University of Piraeus
School of Information and Communication Technologies
Department of Digital Systems

Master Thesis
on

Cyber Risk Management for data-driven enterprises

MIRANDA-MARIA BEKA
AM: MTE1921

Supervisor Professor:
Stefanos Gritzalis

Athens
September 2021

Table of Contents

Acknowledgements

This assignment signifies the completion of an entire cycle of studies at the Department of Digital Systems of the University of Piraeus. A study cycle, initiated 6 years ago when I first selected it for my undergraduate studies. Today, having completed both my Bachelor and my Master's degree I can tell I am more than grateful for the choice I've made back then. Grateful for the people I met, the things I learned and everything I earned, in knowledge and experience.

In risk terms, I challenged my risk thresholds, turning into a risk seeker, in the sense of turning obstacles into opportunities. Not everything has been easy, but I always had the right beacon, at the right time and place to guide me.

My mentors, my family, my friends.

To this point, I would like to thank my professor, supervisor and mentor, Mr. Stefanos Gritzalis for his guidance, his patience and his wisdom (yes, wisdom) that accompanied me throughout my entire MSc journey.

All of my professors for everything they taught me and the challenges they put me through.

My colleagues, for making every day different and letting me know what the real thrill (and responsibility) of being a team "president" is!

Amongst them, mostly, my "Mad Hackz", for every little hack they taught me, and most importantly, the life hack, to protect my smile from malicious situations and circumstances! Thank you, my knights.

My VPN, my Very Personal Network, my closest people, have made it till here together with me, because I have made it thanks to you. I reciprocate by working hard to make you proud every day. I hope this is a little step to this direction.

My whiz(gu)ard, partner in law and ethical crime, each of the goals I have reached by your side would not have been the same without your shines ✧

Thank you for keeping me company throughout this journey.

Last but not least, I am thankful to my family, my 24/7 support line(!), in every thing I go through. Always.

To all
& each every one
of you,

Thank you!

☙ *In every long trip, appreciate your companions. But most of all, appreciate those who stay 'till the end.* ☙

Abstract

The purpose of this thesis is to present and analyze the aspects of risk management concerning the field of cybersecurity and highlight its impact on building resilient business and providing secure services.

In this context, the first chapters aim to clarify basic definitions, required to comprehend the concepts of risk and risk management, in depth. An entire chapter is also dedicated to cybersecurity, including definitions of cyber assets, threats and threat actors, all essential components of cyber risk management, as well as the most common applicable frameworks and standards.

The results of two recent surveys complement the theoretical approach with actual data. The first, regards the latest trends in cyber threat intelligence, while the latter concerns cyber risks and maturity assessments per business sector and per security domain.

The "black swan" phenomenon is also presented as a major concern to be taken into consideration, especially in *the era of the unpredicted*, if the latest couple of years affected by the pandemic could be characterized as such.

Critical infrastructures constitute the next and final section of the study, with a special reference to the Financial sector, drawing upon an ongoing H2020 project, EU regulations and proposed best practices regarding their protection.

Key Words

- Risk
- Risk Management
- Risk Analysis
- Cyber Risk
- Cyber Asset
- Cyber Threat
- Black swans
- Zero-day attacks
- Cybersecurity Posture
- Cyber Insurance
- Awareness
- Critical infrastructure
- Threat Intelligence
- Resilience
- FinSec
- Security Analytics

Introduction

The recent years, more than ever, the world goes cyber. The way we communicate, the way we work, they way we live is more and more reliant on technology and IoT. Conditions such as the Covid-19 pandemic lead to an acceleration of the cyber revolution, since remote is the new trend and wireless is gaining ground.

Despite the fact that this trend has brought many facilities and ease to the table, it does not lack risks. Cyber risks lurk down the corner and just like any other type of risk, it is vital to have the ability to manage them, either by foreseeing them and acting proactively, either by detecting them and reacting effectively.

Cyber risk management is the process of identifying potential cyber risk. In this essay, the importance of managing cyber risk will be thoroughly analyzed, by examining all the correlate issues such as:

- *Why is Risk Management necessary and what does it consist of?*
- *What are the assets to protect?*
- *What are the threats to be protected from?*
- *Where can we refer to, for best practices?*
- *How do we build a robust cybersecurity posture?*
- *Are "Black Swans" the new era of risks and how can they be dealt with?*
- *What is more or less "critical" to protect?*

All of the above are the questions I wish to answer through a multilateral approach in my thesis. But, before the answer hunt begins, let's explore the dimensions of risk management.

The trail will start by setting some basic definitions that will be our first addendum in our toolkit. Besides, awareness is and will always be the No1 defense tool…

Chapter 01:

Risk
&
Risk Management

Risk & Risk Management

Defining Risk and Risk Management

Definition of Risk

An exact definition for risk is hard to find and its measurement is controversial as well. In literature, the word "risk" is used with many different meanings. The Oxford English Dictionary defines risk as "chance or possibility of danger, loss, injury, etc.”.

Most of the definitions are focused on the probability or likelihood of the event. For example, the OECD defines risk as the probability that the actual outcome (for example, sales, costs, and profits) will deviate from the expected outcome. A definition from Australia is as follows: ‘the chance of an event occurring which would cause actual project circumstances to differ from those assumed when forecasting project benefit and costs.

According to the International Organization for Standardization (ISO), the risk would be defined as a "combination of the probability of an event and its consequences". Consequently, a potentially dangerous event, the “hazard” , is not transformed into “risk” only if it applies to a zone where human, economic or environmental “stakes” are in presence and this zone has a certain degree of “vulnerability”.

In the UK’s Orange Book, risk is defined as the “uncertainty of outcome, whether positive opportunity or negative threat, of actions and events”. As the UK’s Orange Book also states, “the risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact which arises if it does actually happen. Risk management includes identifying and assessing risks (the ‘inherent risks’) and then responding to them”.

Risk is not a synonym of uncertainty. The risk concept is inclusive of the uncertainty concept. Risk can be measurable or immeasurable, the latter also being referred to as uncertainty.

As explained in OECD (2008), “uncertainty should be distinguished from measurable risk” (*Fourie and Burger 2000; Grimsey and Lewis 2005*). Uncertainty is defined as a case in which measurable objective or subjective probabilities cannot be calculated and then ascribed to the range of possible and foreseeable outcomes.

Therefore, the essence of risk is characterized by two factors:

1. The *likelihood*: The probability of the risk event occurring within the time period of the project; and
2. The *impact*: The value of the risk event’s effect.

The value of the risk can therefore be calculated using the following “risk formula”:

Risk (Expected Loss) = likelihood x impact = probability of risk occurring x value of effects

Prioritization is a must have in proper risk management. Therefore, the management should be focused on risks that have a high degree of expected loss defined as a combination of probability and potential impact.

Risks should be addressed in an organized and structured approach, which is defined as the risk strategy. Risk management should follow the Risk Management Cycle , which, in sequence, includes: a profound effort to foresee such events (identification) a rigorous analysis of their implications (assessment of likelihood and size of consequences if they materialize), and an analysis and implementation of possible mitigating measures or remedies.

Mitigation measures will provide feedback into the assessment so as to finalize a set of risks that will be the object of the allocation exercise and, subsequently, the risk structuring and incorporation of that structure into the contract. Through this process, some risks are transferred to the private partner, some risks are retained by the public partner, and some risks are shared.

Once risks are allocated and structured, an effective management strategy will be implemented (also known as treatment of risk).[1,2]

IT Risk

Information technology or IT risk in particular, is basically any threat to business data, critical systems and business processes. It is the risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an organization.

IT risks have the potential to damage business value and often come from poor management of processes and events.

Categories of IT risks

IT risk spans a range of business-critical areas, such as:

- *security* – e.g., compromised business data due to unauthorized access or use
- *availability* - e.g., inability to access IT systems needed for business operations
- *performance* - e.g., reduced productivity due to slow or delayed access to IT systems
- *compliance* - e.g., failure to follow laws and regulations (e.g., data protection)

IT risks vary in range and nature. It's important to be aware of all the different types of IT risk potentially affecting the business.

Potential impact of IT failure in business

For businesses that rely on technology, events or incidents that compromise IT can cause many problems. For example, a security breach can lead to:

- identity fraud and theft
- financial fraud or theft
- damage to reputation
- damage to brand
- damage to the business's physical assets

Failure of IT systems due to downtime or outages can result in other damaging and diverse consequences, such as:

- lost sales and customers
- reduced staff or business productivity
- reduced customer loyalty and satisfaction
- damaged relationship with partners and suppliers

If IT failure affects the ability to comply with laws and regulations, then it could also lead to:

- breach of legal duties
- breach of client confidentiality
- penalties, fines and litigation
- reputational damage

If technology is enabling connection to customers, suppliers, partners and business information, managing IT risks in the business should always be a core concern.[3]

Definition of Risk Management

Risk Management is the process of looking at all the essentials and seeing what could go wrong. There is no way to plan for all risks, however identifying the major ones to include likelihood and impact, can increase chances of project success. It involves analyzing schedule, scope, budget and quality factors and identifying pitfalls through lessons learned.

Risk management exists to help us to create plans for the future in a deliberate, responsible, and ethical manner. This requires risk managers to explore what could go right or wrong in an organization, a project or a service, and recognizing that we can never fully know the future as we try to improve our prospects.

Risk management is about analyzing our options and their future consequences, and presenting that information in an understandable, usable form to improve decision making.

The starting point of risk management is an acceptance that risk can't simply be abolished. Risk must be recognized and then managed in some way or other (classically to either avoid, reduce, transfer or retain). This can be easier said than done, particularly when confronted with a demand to 'abolish risk', as if that were an easy and simple option.

Risk Management often requires a relationship between people who analyze risks and people who make decisions based on that analysis. Communication between these two groups must be clear, understandable, and useful. If the people who make decisions can't interpret the analysis they're presented with, then there is little point in doing risk analysis at all.

Paradoxically, we see the lack of a clear definition as an essential aspect of risk management. The fact that organizations won't necessarily know exactly how everyone defines 'risk' forces us to explain to each other what we mean. It makes us ask questions and challenge assumptions.

This is the fundamental strength of risk management; it provides a way of talking about the future, the outcomes we care about, and how to work to towards them. If we could all agree a universal definition of risk, then this could reduce the need for those crucial discussions about the future, uncertainty and risk.

Of course, it may be worthwhile for individual organizations to define, for themselves (and maybe for their supply chains), what they mean by the concept. After all, risks are often analyzed from the perspective of organizations, so it is sensible to develop a local definition which is agreed by anyone working on behalf of that organization.

The purpose of risk management is to enable us to make the best possible decisions, based on our analysis of future events and outcomes. The future can be anticipated, but within limits defined by our uncertainty in our analysis.

Risk is a part of everything we do. People do not only 'take risks' that they are aware of, but they also 'run risks' that they are unaware of all the time. This introduces an important point about risk; because of this uncertainty, it is impossible to know and understand all of the risks that any person, organization, or network is running at any one time.

There are some overly bold standards and frameworks out there which claim all risks will be finally known if a certain set of procedures is diligently and comprehensively followed. That is a false and dangerous notion. Instead, risk management should be approached with a sense of realism and pragmatism. Breaches of cyber security can and do happen to anyone, even the most diligent. The purpose of risk management is not to chase the unattainable goal of perfectly secure systems and a risk-free business; it is to make sure that what can go wrong has been taken into consideration, and that this thinking has influenced the organization's decisions.[4]

7 processes of Risk Management

Risk management is a wide concept, applicable to many, if not all sectors and it consists of 7 main phases (or sub-processes):

1. Establishing scope, context and criteria – Plan Risk Management
2. Identifying risks and/or threats
3. Performing Qualitative Risk Analysis
4. Performing Quantitative Risk Analysis
5. Plan Risk Responses
6. Risk Treatment – Implement Risk Responses
7. Monitoring, Control & Review of Risks

Risks can be identified by any member of the project team. They can be sent via email or raised during a team meeting. The project manager is responsible for logging the risks and assigning a team member to analyze. Risk owners and team members can recommend that a risk be closed; but the Steering Committee must authorize the closure of high and medium level risks.

The flow is simply depicted below:

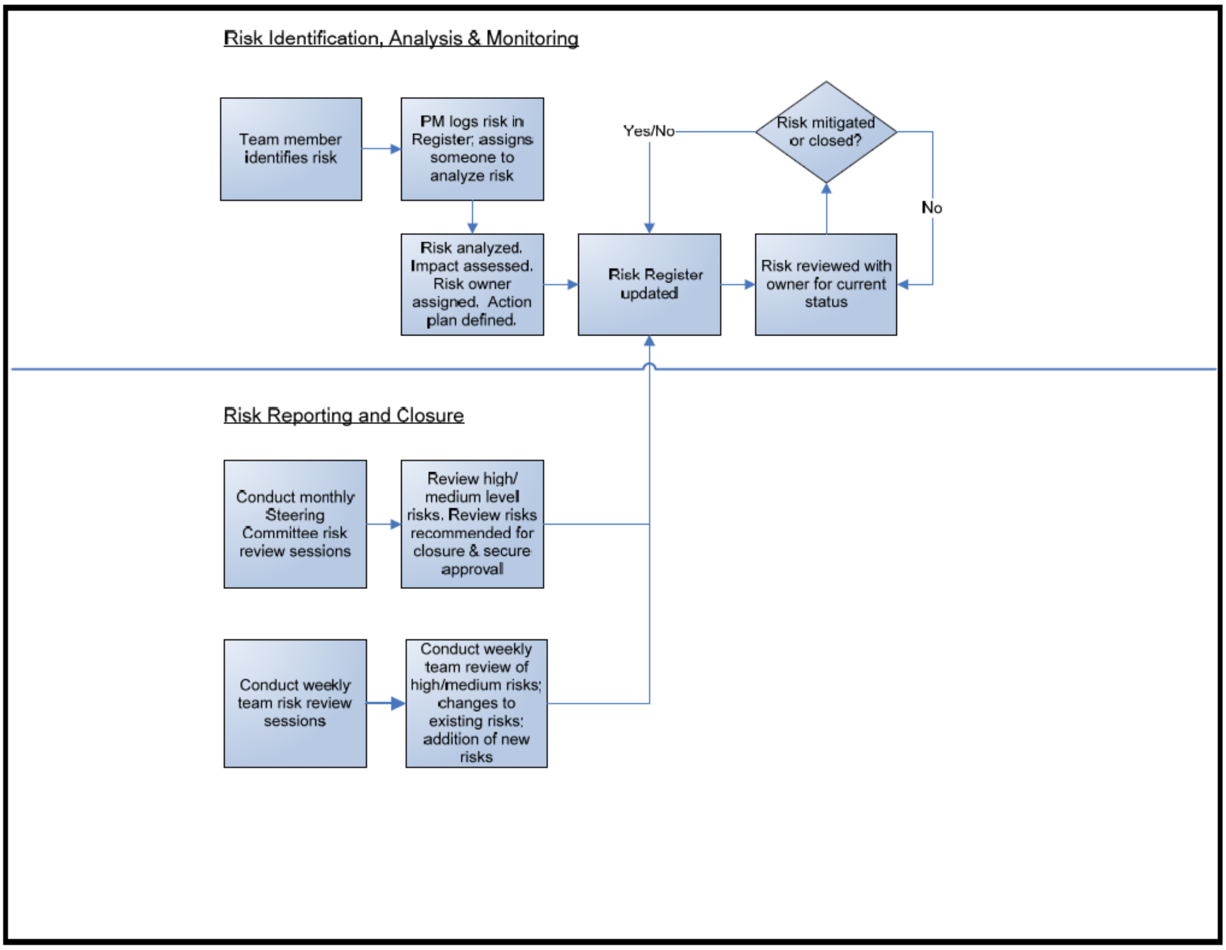

Risk Identification, Analysis & Monitoring
Team member identifies risk
PM logs risk in Register; assigns someone to analyze risk
Yes/No
Risk mitigated or closed?
No
Risk analyzed. Impact assessed. Risk owner assigned. Action plan defined.
Risk Register updated
Risk reviewed with owner for current status
Risk Reporting and Closure
Conduct monthly Steering Committee risk review sessions
Review high/ medium level risks. Review risks recommended for closure & secure approval
Conduct weekly team risk review sessions
Conduct weekly team review of high/medium risks; changes to existing risks; addition of new risks

Fig.1.1: Risk Management Process Flow Diagram

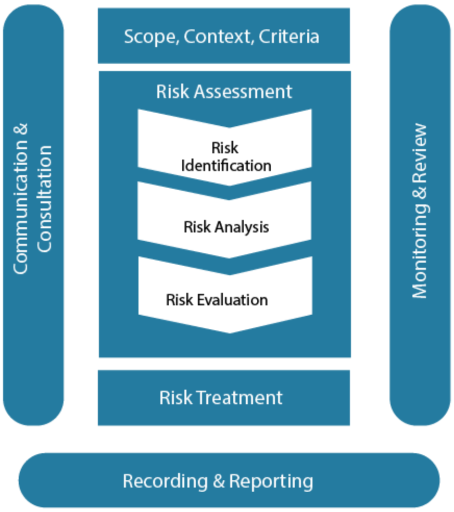


Fig.1.2: Risk Management sub-processes

Plan Risk Management

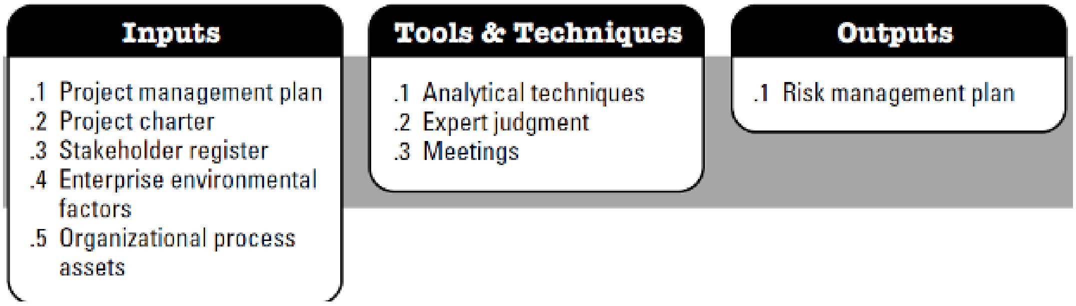
This is the process of defining how to conduct risk management activities for a project. The planning process illuminates the approach for project teams and establishes ground rules for risk management. The output from this process is the risk management plan.

The Risk Management Plan describes the risk management and control: workflows, assessment processes, supplementary tools, roles and responsibilities.

The Project Manager completes the Risk Management Plan during the planning stage of the project and reviews the plan with the entire team to secure buy-in. The Risk Register is also created during the planning stage and updated through standard risk management processes throughout the life of the project. Review of risks, their impacts and status should are to be built into regular team work sessions or supplementary risk management sessions depending upon the nature of the project.

All sections must be completed for all projects, regardless of level. The intricacies of the plan are contingent upon the complexity level of the project.

Below are the main inputs, tools & techniques and outputs of the process:



Inputs	Tools & Techniques	Outputs
.1 Project management plan .2 Project charter .3 Stakeholder register .4 Enterprise environmental factors .5 Organizational process assets	.1 Analytical techniques .2 Expert judgment .3 Meetings	.1 Risk management plan

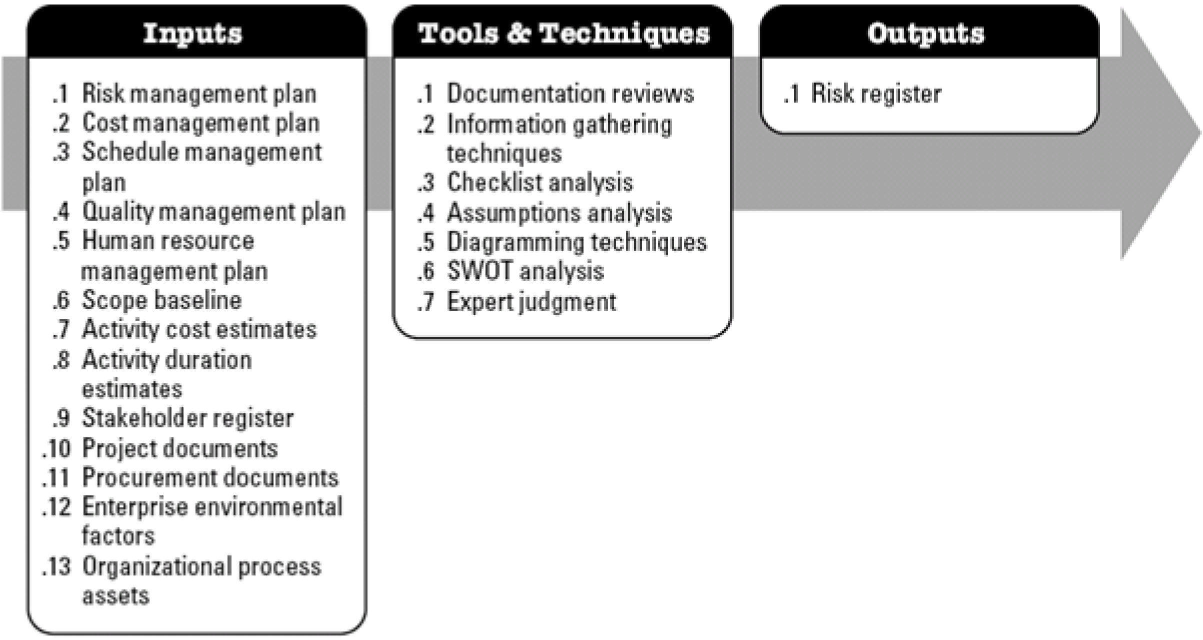
Fig.1.3: Inputs, Outputs, Tools & Techniques of Risk Management Phase 1: Plan Risk Management

Identifying Risks

Risk identification occurs at the beginning of the project, as well as throughout the project. While many risks are considered “known risks,” others might require additional research to discover.

This process is critical and probably the most important in the risk management process. It requires extensive experience as well as calling upon lessons learned to identify all potential risks. In my work organization, the same issues usually arise, however there are always new, unforeseen risks that have an impact in some way.

Below are the main inputs, tools & techniques and outputs of the process:



Inputs

.1 Risk management plan
.2 Cost management plan
.3 Schedule management plan
.4 Quality management plan
.5 Human resource management plan
.6 Scope baseline
.7 Activity cost estimates
.8 Activity duration estimates
.9 Stakeholder register
.10 Project documents
.11 Procurement documents
.12 Enterprise environmental factors
.13 Organizational process assets

Tools & Techniques

.1 Documentation reviews
.2 Information gathering techniques
.3 Checklist analysis
.4 Assumptions analysis
.5 Diagramming techniques
.6 SWOT analysis
.7 Expert judgment

Outputs

.1 Risk register

Fig.1.4: Inputs, Outputs, Tools & Techniques of Risk Management Phase 2: Identifying Risks

Risks are to be identified and dealt with as early as possible in the project. Risk identification is done throughout the project life cycle, with special emphasis during the key milestones.

Risk identification is one of the key topics in the regular project status and reporting meetings. Some risks may be readily apparent to the project team—known risks; others will take more rigor to uncover, but are still predictable.

The medium for recording all identified risks throughout the project is the risk register, which is stored in the central project server.

The following are used to identify risks in a structured and disciplined way, which ensures that no significant potential risk is overlooked.

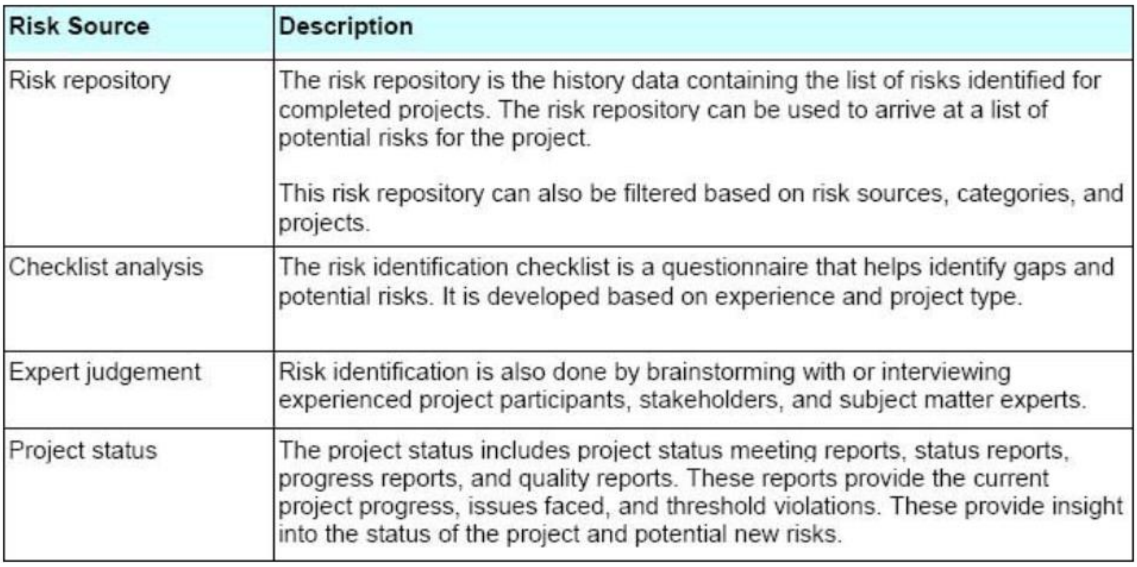
Risk sources

Risk sources may vary and may derive either from the internal or the external environment of the organization. Some indicative results are depicted below:

Scope risks
Resource risks
Performance risks
Quality risks
Schedule risks
Budget risks
Technical risks
Operational risks
Strategic risks
Environmental risks
Market risks
Legal risks

Figs. 1.5a, 1.5b, 1.5c: Risk Sources

Sources of identification may also vary. Here are some examples:

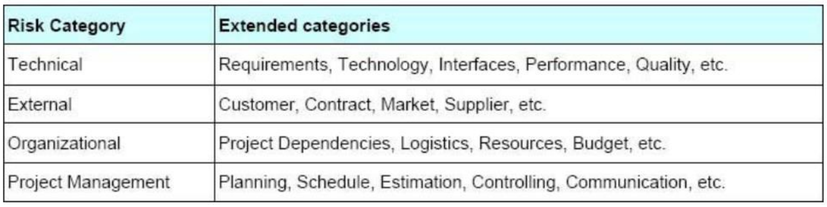


Risk Source	Description
Risk repository	The risk repository is the history data containing the list of risks identified for completed projects. The risk repository can be used to arrive at a list of potential risks for the project. This risk repository can also be filtered based on risk sources, categories, and projects.
Checklist analysis	The risk identification checklist is a questionnaire that helps identify gaps and potential risks. It is developed based on experience and project type.
Expert judgement	Risk identification is also done by brainstorming with or interviewing experienced project participants, stakeholders, and subject matter experts.
Project status	The project status includes project status meeting reports, status reports, progress reports, and quality reports. These reports provide the current project progress, issues faced, and threshold violations. These provide insight into the status of the project and potential new risks.

Fig. 1.6: Risk Sources of Identification

Risk Categorization

Risk category provides a list of areas that are prone to risk events. The organization recommends high-level, standard categories, which have to be extended based on the project type.



Risk Category	**Extended categories**
Technical	Requirements, Technology, Interfaces, Performance, Quality, etc.
External	Customer, Contract, Market, Supplier, etc.
Organizational	Project Dependencies, Logistics, Resources, Budget, etc.
Project Management	Planning, Schedule, Estimation, Controlling, Communication, etc.

Fig. 1.7: Risk Categories

Risk Analysis

Risk analysis involves examining how project outcomes and objectives might change due to the impact of the risk event.

Once the risks are identified, they are analyzed to identify the qualitative and quantitative impact of the risk on the project so that appropriate steps can be taken to mitigate them.

The following, are used to analyze risks.

Probability of Risk Occurrence

An indication of how to calculate the probability of risk occurrence is the following:

- High probability – (80 % ≤ x ≤ 100%)
- Medium-high probability – (60 % ≤ x < 80%)
- Medium-Low probability – (30 % ≤ x < 60%)
- Low probability (0 % < x < 30%)

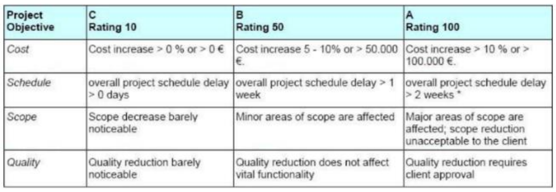
Risk Impact

In addition to classifying risks according to the above guidelines, it is also necessary to describe the impact on cost, schedule, scope, and quality in as much detail as possible based on the nature of the risk.

An indication of how to calculate the risk impact is the following:

- High – Catastrophic (Rating A – 100)
- Medium – Critical (Rating B – 50)
- Low – Marginal (Rating C – 10)

As a guideline for Impact Classification the following matrix can be used:



Project Objective	**C** **Rating 10**	**B** **Rating 50**	**A** **Rating 100**
Cost	Cost increase > 0 % or > 0 €	Cost increase 5 - 10% or > 50.000 €.	Cost increase > 10 % or > 100.000 €.
Schedule	overall project schedule delay > 0 days	overall project schedule delay > 1 week	overall project schedule delay > 2 weeks *
Scope	Scope decrease barely noticeable	Minor areas of scope are affected	Major areas of scope are affected; scope reduction unacceptable to the client
Quality	Quality reduction barely noticeable	Quality reduction does not affect vital functionality	Quality reduction requires client approval

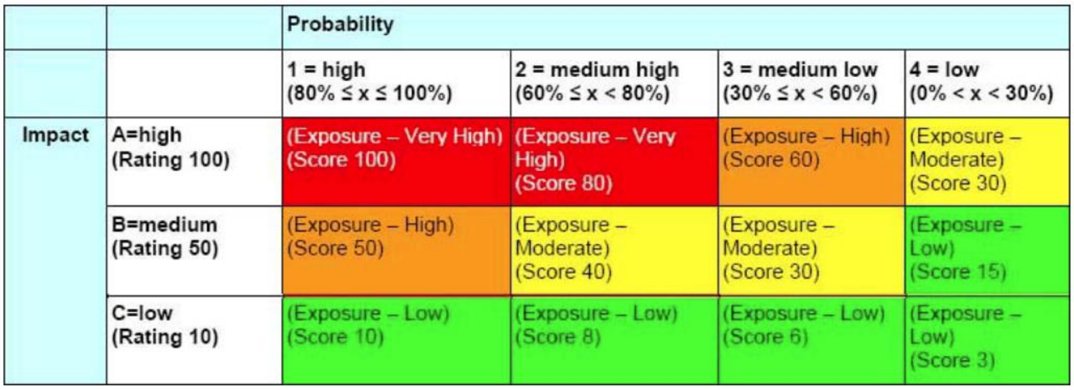
Fig. 1.8: Indicative Impact Classification Table

The score represents bottom thresholds for the classification of risks assuming "normal" conditions. An upgrade of the score to the next or even next + 1 level is necessary, if the risk is impacted by critical factors such as:

- How important the specific customer is
- Whether the project is critical for the further development of the relationship with the customer
- The risk is already in the focus of the customer
- Specific penalties for deviations from project targets are agreed in the contract with the customer

Risk Exposure

Risk Exposure or Risk Score is the value determined by multiplying the Impact Rating with Risk Probability as indicatively shown below:



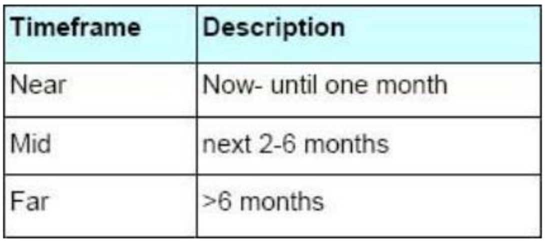
		Probability			
		1 = high (80% ≤ x ≤ 100%)	2 = medium high (60% ≤ x < 80%)	3 = medium low (30% ≤ x < 60%)	4 = low (0% < x < 30%)
Impact	A=high (Rating 100)	(Exposure – Very High) (Score 100)	(Exposure – Very High) (Score 80)	(Exposure – High) (Score 60)	(Exposure – Moderate) (Score 30)
	B=medium (Rating 50)	(Exposure – High) (Score 50)	(Exposure – Moderate) (Score 40)	(Exposure – Moderate) (Score 30)	(Exposure – Low) (Score 15)
	C=low (Rating 10)	(Exposure – Low) (Score 10)	(Exposure – Low) (Score 8)	(Exposure – Low) (Score 6)	(Exposure – Low) (Score 3)

Fig. 1.9: Indicative P& I Matrix

The colours represent the urgency of risk response planning and determine reporting levels.

Risk Occurrence Timeframe

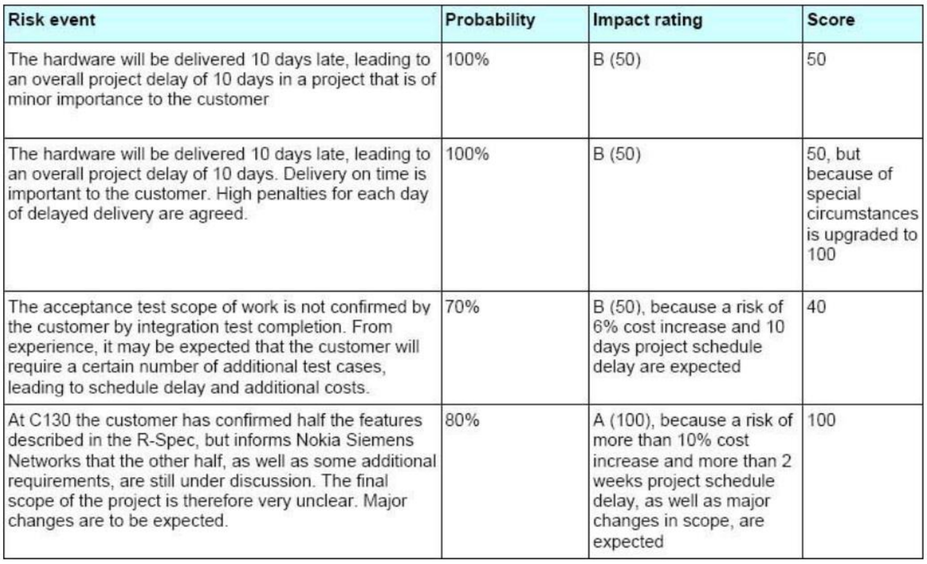
The timeframe in which this risk will have an impact is identified. This can be classified into one of the following:



Timeframe	Description
Near	Now- until one month
Mid	next 2-6 months
Far	>6 months

Fig. 1.10: Risk Occurrence indicative timeframe

Below are some risk classification examples:



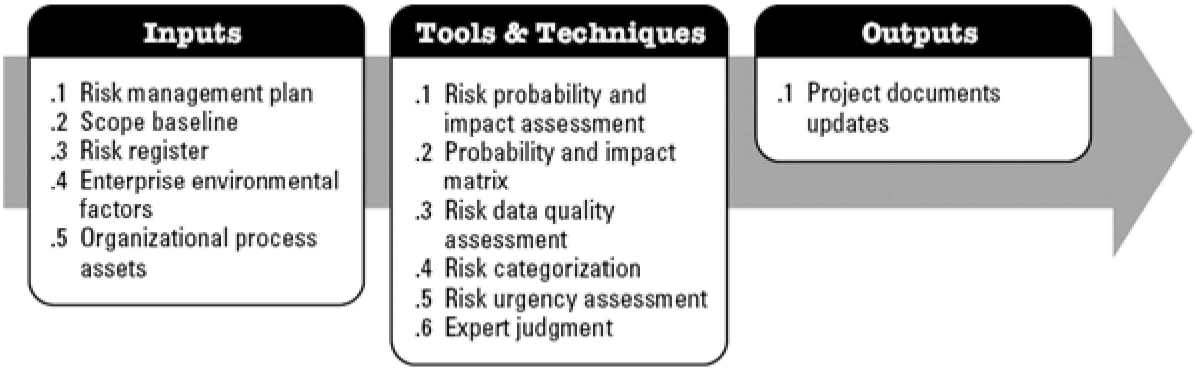
Risk event	Probability	Impact rating	Score
The hardware will be delivered 10 days late, leading to an overall project delay of 10 days in a project that is of minor importance to the customer	100%	B (50)	50
The hardware will be delivered 10 days late, leading to an overall project delay of 10 days. Delivery on time is important to the customer. High penalties for each day of delayed delivery are agreed.	100%	B (50)	50, but because of special circumstances is upgraded to 100
The acceptance test scope of work is not confirmed by the customer by integration test completion. From experience, it may be expected that the customer will require a certain number of additional test cases, leading to schedule delay and additional costs.	70%	B (50), because a risk of 6% cost increase and 10 days project schedule delay are expected	40
At C130 the customer has confirmed half the features described in the R-Spec, but informs Nokia Siemens Networks that the other half, as well as some additional requirements, are still under discussion. The final scope of the project is therefore very unclear. Major changes are to be expected.	80%	A (100), because a risk of more than 10% cost increase and more than 2 weeks project schedule delay, as well as major changes in scope, are expected	100

Fig. 1.11: Risk Classification Examples

Performing Qualitative Risk Analysis

Qualitative Risk Management is the process of analyzing and prioritizing risks based on their probability that they may occur along with their impact. This process will prioritize them on how impactful the risks are.

Below, inputs, tools & techniques and outputs of the process are al depicted:



Inputs

.1 Risk management plan
.2 Scope baseline
.3 Risk register
.4 Enterprise environmental factors
.5 Organizational process assets

Tools & Techniques

.1 Risk probability and impact assessment
.2 Probability and impact matrix
.3 Risk data quality assessment
.4 Risk categorization
.5 Risk urgency assessment
.6 Expert judgment

Outputs

.1 Project documents updates

Fig.1.12: Inputs, Outputs, Tools & Techniques of Risk Management Phase 3: Qualitative Analysis

Probability Rating

The following probability ratings are indicative and may be integrated into the Risk Register. These default ratings may be used as they are or be refined as desired by the project.

Table 1.1: Indicative Probability Rating

Probability	Score	Description
Low	10	Unlikely to occur (*e.g. less than a 25% chance of occurring during the course of the project*).
Medium	20	Likely to occur (*e.g. > 25% and < 75% chance of occurring during the course of the project*).
High	30	Highly likely to occur (*e.g. >75% and < 100% chance of occurring during the course of the project*).

Impact Rating

The following impact ratings are indicative as well and may be integrated into the Risk Register. These default ratings may be used as they are or be refined as desired by the project.

Table 1.2: Indicative Impact Rating

Impact	Score	Description
Low	10	Minor impact on the project *(e.g. no impact to any milestone or deliverable dates)*
Medium	20	Measurable impact on a specific milestone or deliverable and/or budget impact
High	30	Significant impact on key milestones, deliverables, and/or budget

Priority Score & Priority Rating

The following Priority Score and Priority Ratings are automatically calculated in the Risk Register based upon the Probability Ratings referred above. In general, default Priority Scores and Priority Ratings may be used or they can be refined as desired by the project.

Table 1.3: Indicative Risk Priority Rating

Probability Rating	Impact Rating	Priority Score	Priority Rating
Low	Low	10	Low
Low	Medium	15	Medium
Low	High	20	High
Medium	Low	15	Medium
Medium	Medium	20	Medium
Medium	High	25	High
High	Low	20	High
High	Medium	25	High
High	High	30	High

A certain trend that seems to be establishing itself more and more is the traffic light model with the colours green, yellow and red. After all, most questions about possible hazards cannot simply be answered with yes or no, since these answers do not yet contain any evaluation or even measures.

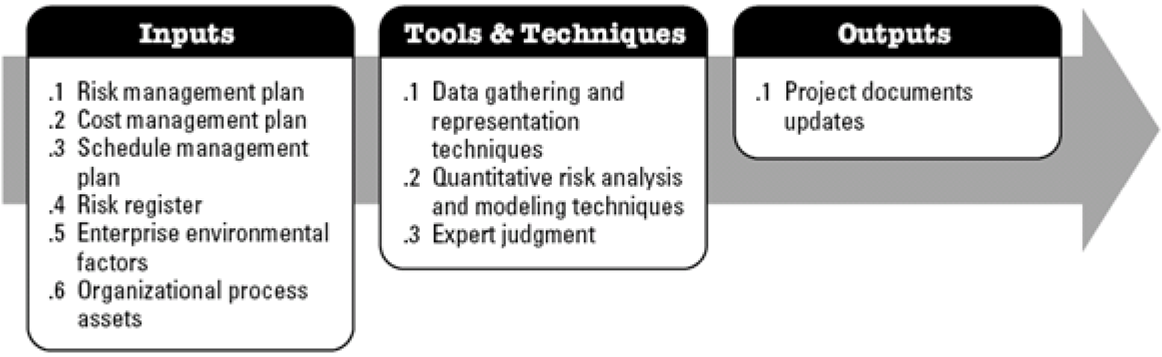
- Green colour indicates that the risk is (very) low (or does not exist at all). It is used if the hazard does not apply or applies, but to such an extent that no serious consequences are to be expected.

- Yellow colour indicates that the risk is medium, therefore protective measures are necessary. It is used in cases when, if the hazard applies, there are specific protective measures that make it possible to continue working on this activity. The indications marked with yellow already contain suggestions for measures.

- Finally, red indicates that the risk is high and may lead to serious consequences. It is used when the hazard applies and no protective measures are available. [5]

Performing Quantitative Risk Analysis

This is the process of numerically analyzing the effect of identified risk on overall project objectives. The techniques for this analysis include expected monetary value, sensitivity analysis and Monte Carlo modeling.



Inputs

.1 Risk management plan
.2 Cost management plan
.3 Schedule management plan
.4 Risk register
.5 Enterprise environmental factors
.6 Organizational process assets

Tools & Techniques

.1 Data gathering and representation techniques
.2 Quantitative risk analysis and modeling techniques
.3 Expert judgment

Outputs

.1 Project documents updates

Fig.1.13: Inputs, Outputs, Tools & Techniques of Risk Management Phase 4: Quantitative Analysis

A quantitative risk analysis is a further analysis of the highest priority risks during a which a numerical or quantitative rating is assigned in order to develop a probabilistic analysis of the project.

A quantitative analysis:

- Quantifies the possible outcomes for the project and assesses the probability of achieving specific project objectives
- Provides a quantitative approach to making decisions when there is uncertainty
- Creates realistic and achievable cost, schedule or scope targets

In order to conduct a quantitative risk analysis, need high-quality data, a well-developed project model, and a prioritized lists of project risks (usually from performing a qualitative risk analysis) are needed.[6]

Quantitative risk analysis is a numeric estimate of the overall effect of risk on the project objectives such as cost and schedule objectives. The results provide insight into the likelihood of project success and is used to develop contingency reserves.
Individual risks are evaluated in the qualitative risk analysis. But the quantitative analysis allows us to evaluate the overall project risk from the individual risks plus other sources of risks.
Business decisions are rarely made with all the information or data we desire. For more critical decisions, quantitative risk analysis provides more objective information and data than the qualitative analysis.

Quantitative Risk Analysis is suggested for:

- Projects that require a Contingency Reserve for the schedule and budget.
- Large, complex projects that require Go/No Go decisions (the Go/No Go decision may occur multiple times in a project).

- Projects where upper management wants more detail about the probability of completing the project on schedule and within budget.

Quantitative Risk Analysis tools and techniques include but are not limited to:

- Three Point Estimate – a technique that uses the optimistic, most likely, and pessimistic values to determine the best estimate.
- Decision Tree Analysis – a diagram that shows the implications of choosing one or other alternatives.
- Expected Monetary Value (EMV) – a method used to establish the contingency reserves for a project budget and schedule.
- Monte Carlo Analysis – a technique that uses optimistic, most likely, and pessimistic estimates to determine the total project cost and project completion dates. For example, we could estimate the probability of completing a project at a cost of $20M. Or what is a company wanted to have an 80% probability of achieving its cost objectives. What is the cost to achieve 80%?
- Sensitivity Analysis – a technique used to determine which risks have the greatest impact on a project.
- Fault Tree Analysis (FMEA) – the analysis of a structured diagram which identifies elements that can cause system failure.[7]

The table below summarizes the key differentiators between qualitative and quantitative risk analysis[8]:

Table 1.4: Qualitative Vs. Quantitative Analysis

Qualitative	Quantitative
risk-level	project-level
subjective evaluation of probability and impact	probabilistic estimates of time and cost
quick and easy to perform	time consuming
no special software or tools required	may require specialized tools

Plan Risk Responses

Planning this process involves choosing which response approach to use for each identified risk, then creating a plan for that risk.

Below, inputs, tools & techniques and outputs of the process are al depicted:

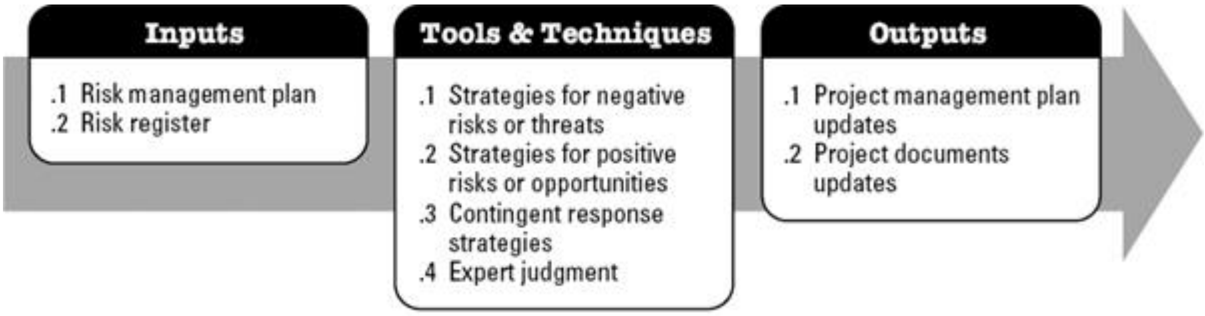

Inputs
.1 Risk management plan
.2 Risk register
Tools & Techniques
.1 Strategies for negative risks or threats
.2 Strategies for positive risks or opportunities
.3 Contingent response strategies
.4 Expert judgment
Outputs
.1 Project management plan updates
.2 Project documents updates

Fig.1.14: Inputs, Outputs, Tools & Techniques of Risk Management Phase 5: Plan Responses

There may not be quick solutions to reduce or eliminate all the risks facing a project. Some risks may need to be managed and reduced strategically over longer periods. Therefore, action plans should be worked out to reduce these risks. These action plans should include:

- Risk description with risk assessment
- Description of the action to reduce the risk
- Owner of the risk action
- Committed completion date of the risk action

All risk action plans should be allotted to the person identified to carry out the action plan.

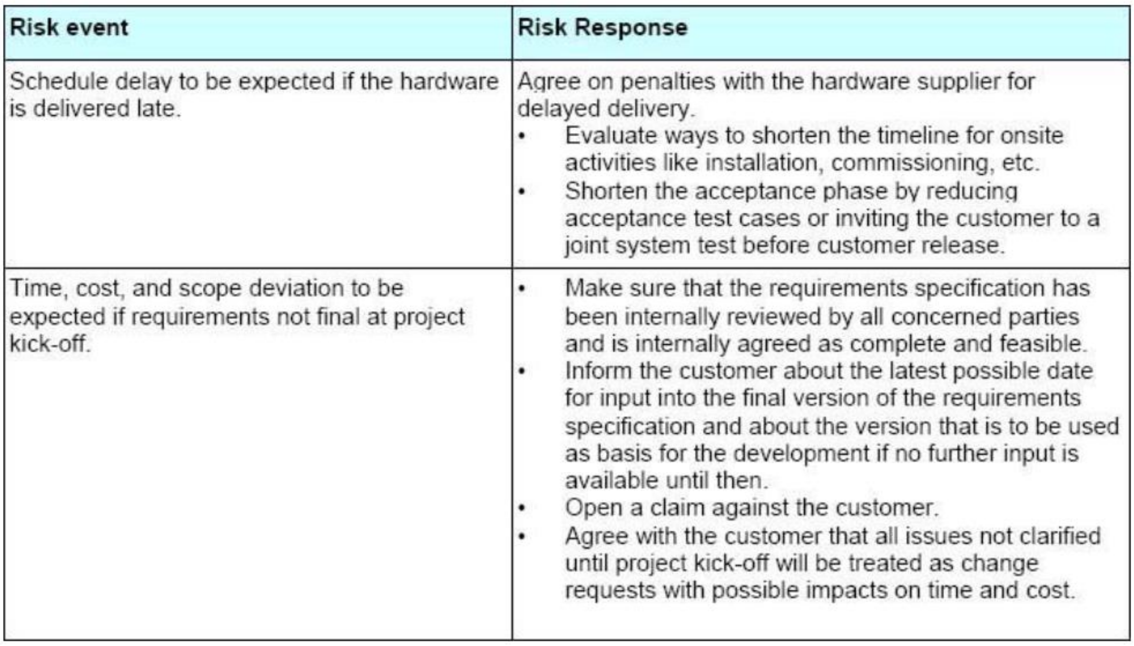
Risk Response Plans

For each risk, a risk response must be documented in the risk register in agreement with the stakeholders. This should be ensured by the project manager.

Risk response plans are aimed at the following targets:

- Eliminating the risk
- Lowering the probability of risk occurrence
- Lowering the impact of the risk on the project objectives

Risk response plans usually impact time and costs. It is therefore mandatory that the time and cost for the defined response plan are calculated as precisely as possible. This also assists in selecting a response plan from the alternatives, and in verifying whether the response plan is costlier or has more impact on one of the project objectives than the risk itself.

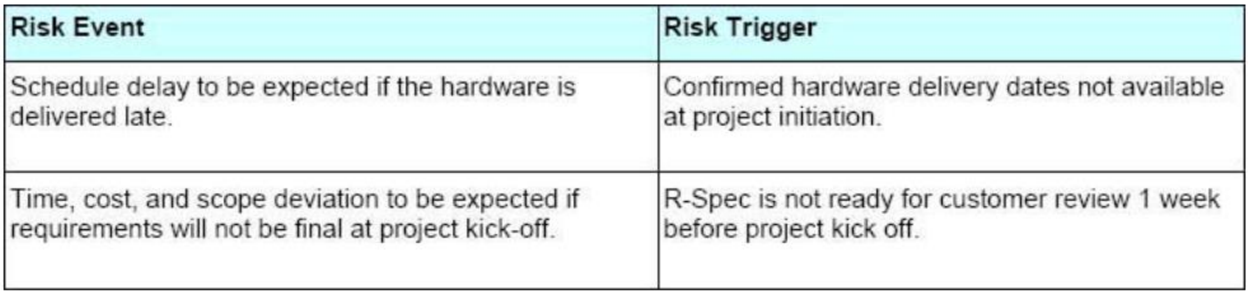


Risk event	Risk Response
Schedule delay to be expected if the hardware is delivered late.	Agree on penalties with the hardware supplier for delayed delivery. • Evaluate ways to shorten the timeline for onsite activities like installation, commissioning, etc. • Shorten the acceptance phase by reducing acceptance test cases or inviting the customer to a joint system test before customer release.
Time, cost, and scope deviation to be expected if requirements not final at project kick-off.	• Make sure that the requirements specification has been internally reviewed by all concerned parties and is internally agreed as complete and feasible. • Inform the customer about the latest possible date for input into the final version of the requirements specification and about the version that is to be used as basis for the development if no further input is available until then. • Open a claim against the customer. • Agree with the customer that all issues not clarified until project kick-off will be treated as change requests with possible impacts on time and cost.

Fig.1.5: Risk Responses by Risk Events

Risk Triggers

For each risk a trigger must be documented in the risk register. The trigger identifies the risk symptoms or warning signs. It indicates that a risk has occurred or is about to occur. The risk trigger also gives an indication of when a certain risk is expected to occur.

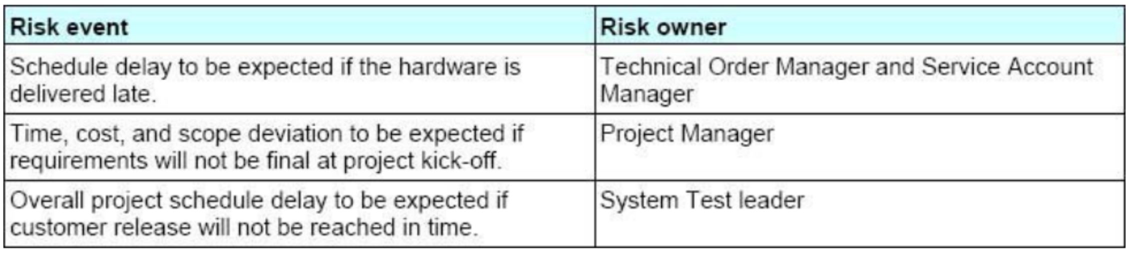


Risk Event	Risk Trigger
Schedule delay to be expected if the hardware is delivered late.	Confirmed hardware delivery dates not available at project initiation.
Time, cost, and scope deviation to be expected if requirements will not be final at project kick-off.	R-Spec is not ready for customer review 1 week before project kick off.

Fig.1.16: Examples of Risk Triggers and Events

Risk Ownership

The ground rule is that responsibility for managing all risks in the project lies with the project manager. Based on this ground rule a Risk Owner (who is not necessarily the project manager) must be determined and named in the Risk Register. The Risk Owner is normally the one who can best monitor the risk trigger, but can also be the one who can best drive the defined countermeasures. The Risk Owner is responsible for immediately reporting any changes in the risk trigger status and for driving the defined countermeasures.



Risk event	Risk owner
Schedule delay to be expected if the hardware is delivered late.	Technical Order Manager and Service Account Manager
Time, cost, and scope deviation to be expected if requirements will not be final at project kick-off.	Project Manager
Overall project schedule delay to be expected if customer release will not be reached in time.	System Test leader

Fig.1.17: Examples of Risk Owners by Risk Events

Risk Treatment – Implement Risk Responses

The process of Implementing Risk Responses is the process of planning and implementing actions and plans in response to project risks. The purpose of this process is to ensure that each of the identified risks on the Risk Register has appropriate actions or plans to mitigate or avoid a risk before it happens or to provide a response when a risk occurs and turns into a project issue.

The idea is to reduce the exposure to risks in the project and minimize threats to the delivery in terms of time, cost or quality.

The inputs to the process are primarily the Risk Register and Assumptions Log but can also be the Lessons Learnt Register. The risks should be sorted into those which present the biggest threat to the project and a process of deciding how to respond to the risk is then undertaken.

The Risk Response Process is used throughout the project lifecycle from the time that the risks are first identified and reviewed regularly to include new risks and also ensure that the response to existing risks remains relevant.

Deciding on a response to a risk utilizes several project management techniques including input from experts in the risk topic, project team members and lessons learnt from previous projects. In some cases, a valid risk response could be to ignore or defer the response if it isn’t a significant risk to the project.

Responses can also be proactive and deal with the risk now, undertaking some activities to prevent or minimize the impact of it. In other cases, a risk response plan will only be executed as and when the risk materializes on the project. For some risks, there may be more than one risk response.

The results of the Risk Response Process should be documented in the project Risk Register. Depending on the response plan, Change Requests can be issued and updates to the project plan are made to reflect the Risk Response activities[9].

There are generally four types of risk responses an organization can take:

- *Avoid*: Change the strategy to avoid the risk. Avoiding risk is usually considered when there is no cost-effective method for reducing the cybersecurity risk to an acceptable level as defined by the unit's or the organization's risk acceptance and tolerance.

- *Mitigate*: Apply risk treatment that reduces the threats, vulnerabilities, likelihood, or impact of a given risk so that the residual risk is within risk acceptance and tolerance.

- *Transfer*: Most organizations consider sharing a part of the risk with another when it does not have complete control over the risk. Think outsourcing to a SaaS or investing in cyber insurance

- *Accept*: Accept the risk as-is because the risk falls within risk acceptance and tolerance but continue to monitor the risk if the risk falls outside of approved tolerance.[10]

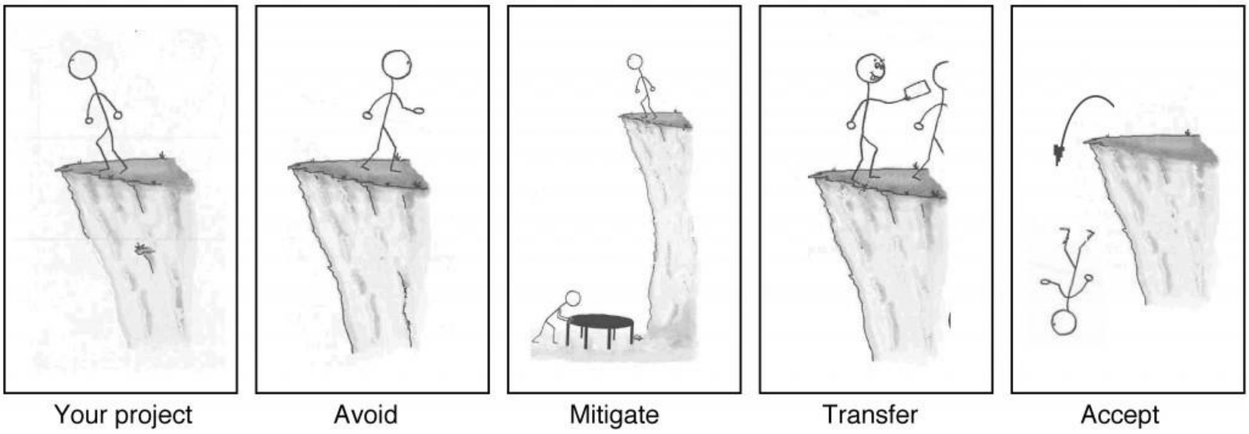


Fig.1.18: Risk Responses Depiction

After successfully implementing a set of response plans, the score of a risk could be lowered in consultation with the stakeholders.

Monitoring, Control & Review of Risks

Risk monitoring and control includes:

- Identifying new risks and planning for them
- Keeping track of existing risks to check if:
  - Reassessment of risks is necessary
  - Any of risk conditions have been triggered
  - Monitor any risks that could become more critical over time

    - Tackle the remaining risks that require a longer-term, planned, and managed approach with risk action plans

- Risk reclassification

For the risks that cannot be closed, the criticality has to go down over a period of time due to implementing the action plan. If this is not the case then the action plan might not be effective and should be re-examined.

- Risk reporting

The risk register is continuously updated, from risk identification through risk response planning and status update during risk monitoring and control. This project risk register is the primary risk reporting tool and is available in the central project server, which is accessible to all stakeholders.

Risk monitoring and controlling or risk review is an iterative process that uses progress status reports and deliverable status to monitor and control risks. This is enabled by various status reports, such as quality reports, progress reports, follow-up reports, and so forth.

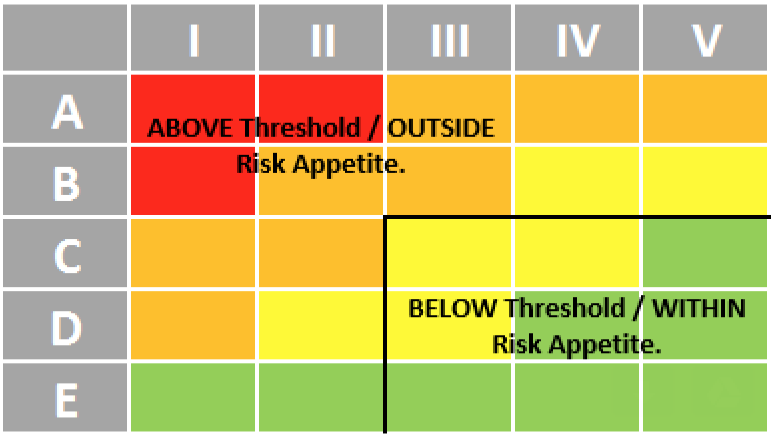
Risk Reviews are a mandatory item of milestone meetings and/or regular project meetings, but they can also be executed during separately planned risk review meetings. These risk reviews must be held regularly. The frequency could also be determined based on the overall risk level of a project.

Risk Threshold

The risk priorities have to be set to direct focus where it is most critical. The risks with the highest risk exposure rating are the highest priority.

Risks with Exposure Low can be dropped from the mitigation plans, but may need to be revisited later in the project.

The organizational mandate is that if the projects have at least one "Very High" risk or more than 3 "High" risks, guidance should be sought from management and stakeholders, as the project may be at high risk of failure. This is the recommended risk threshold. Projects can customize the threshold based on project needs.



	I	II	III	IV	V
A	🟥	🟥	🟧	🟧	🟧
B	🟥	🟧	🟧	🟨	🟨
C	🟧	🟧	🟨	🟨	🟩
D	🟧	🟨	🟨	🟩	🟩
E	🟩	🟩	🟩	🟩	🟩

ABOVE Threshold / OUTSIDE Risk Appetite.
BELOW Threshold / WITHIN Risk Appetite.

Fig.1.19: The threshold concept

Risk Efficiency measurement

Risk Metrics

The efficiency of risk analysis and management is measured by capturing the following metrics during project closure. The analysis results are used to decipher lessons learned, which is updated in the organization's lessons learned database.

- Number of risks that occurred / Number of risks that were identified
- Was the impact of the risks as severe as originally thought?
- How many risks recurred?
- How do the actual problems and issues faced in a project differ from the anticipated risks?

Risk Audit

This is an independent expert analysis of risks, with recommendations to enhance maturity or effectiveness of risk management in the organization. This evaluates:

- How good are we at identifying risk?
- Exhaustiveness and granularity of risks identified
- Effectiveness of mitigation or contingency plan
- Linkage of project risks to organizational risks

This is not a "process adherence" audit, but an aid to enhance the quality of risk identification and risk analysis. This is also used as a forum to benchmark and identify good practices of risk management among various projects in the organization.

The risk audit is done by a group of independent domain or technical experts through documentation review and interviews. The key deliverables of this risk audit are:

- Customized checklist to evaluate the risks of a project
- Identify areas of importance for risk analysis for a project (risk taxonomy)
- Risk radar – risk-prone areas of the product group
- Potential additional risks identified based on the review
- Top 10 risks in the organization from key projects, which requires management attention.[11]

Risk Management Roles & Responsibilities

In order to identify and depict all responsible and accountable key risk management participants as well as their role in the risk management process, it is helpful to use a table, such as the one below[12]:

Table 1.5: Risk Management Roles & Responsibilities

Roles	Responsibilities
Team Members	▪ Raise risks. ▪ Ensure the PM is informed of the risks.

Project Manager	▪ Logs risks. ▪ Assigns an analyst to assess impact, probability and develop an action plan. ▪ Maintains the risk log including detailed status information from each review session in the ▪ register. ▪ Conducts regular risk review sessions with steering committee and project team to review risks. ▪ Follows-through with risk owners independently of team meetings. ▪ Escalates high impact risks to senior management for awareness and assistance.
Steering Committee	▪ Address high impact risks that the PM and team cannot manager on their own. ▪ Must be aware of significant project risks and costs associated with the risks. ▪ Authorize the closure of high/medium level risks.
Risk Originator	▪ The person who informs the risk team about the new risk
Risk Owner	▪ Responsible for planning the response, tracking the risk, monitoring for risk triggers, recommend execution of the risk response plan and monitoring the effectiveness of the response plan ▪ Regularly update team on status, action plans and state of risk. ▪ Accountable point of contact for an enterprise risk at the senior leadership level, who coordinates efforts to mitigate and manage the risk with various individuals who own parts of the risk ▪ Ensures that the agreed-upon risk responses are carried ▪ Accountable for ensuring that the risk response is effective and for planning additional risk responses if required
Risk Action Owner	▪ Assigned by Risk Owner to execute the risk response and reports to him ▪ Helps the risk owner manage the risk ▪ Responsible for ensuring that the agreed-upon risk responses are carried out as planned, in a timely manner.

Describing Risks (Cause-Risk-Effect format)

Every risk has a root cause. In the case of projects, the risk root cause will originate from one or more of three sources: Process, People or Product. The majority of risks that are causing a project to fail are associated with Process and/or People root causes.

It is crucial during the Identify phase to register identified risks with the Cause-Risk-Effect format in order to show that they have been clearly understood. Moreover, this helps at the Risk Response Planning to properly select the right response strategy.

Below are some samples of how to express identified risks in the above-mentioned format[13]:

Table 1.6: Risk Metalanguage: Risks in the Cause-Risk-Effect Format

Situation	Cause	Risk	Effect
Root cause: Process			
Business Case	As a result of not having a business case for the project,	a lack of clarity among stakeholders regarding the project's objectives may occur	which would lead to the project not meeting its objectives and placing its success in jeopardy.
No Change Control Process	As a result of not having a change control process in place,	an inadequate evaluation of a changed requirement on the project may occur,	which would lead to uncontrolled changes impacting the project's schedule, cost and/or quality.
No Governance Structure	As a result of not having a governance structure in place,	addressing project issues and strategic decisions without involving the appropriate parties may occur,	which would lead to project deliverables not being accepted by management, the sponsor or the user community.
Poor Requirements	As a result of having poorly written requirements,	a misunderstanding regarding what the stakeholder wants may occur,	which would lead to the delivered product not being accepted and the team needing to perform rework.
Lack of Resources	As a result of the allocated resources not having the required skill sets,	delays completing project tasks may occur,	which would lead to the project completion date being jeopardized and the quality of the deliverables being compromised.
Lack of User Involvement	As a result of users not validating the project's requirements,	rejection of the delivered product may occur,	which would lead to rework, delays, increased costs and an unhappy user community.
Scope Creep	As a result of not following a formal change control process,	sponsor rejection of a scope change after it has been built may occur,	which would lead to the sponsor's expectations not being met and the project running late and incurring cost overruns.
Poor Stakeholder Management	As a result of not involving key stakeholders in a design demonstration ,	development of a system whose design is not formally approved may occur,	which would lead to the system being rejected by some/all stakeholders.

Situation	Cause	Risk	Effect
Root cause: People			
Poor Communication	As a result of not having a detailed communication plan,	confusion among key stakeholders regarding the	which would lead to poor, delayed or nonexistent decision making.

		project objectives and deliverables may occur,	
Inaccurate Estimation	As a result of poor estimation,	agreement to an unrealistic timeline may occur,	which would lead to work not being delivered in the time allocated.
Being Overly Ambitious	As a result of aggressive scope planning,	delays in delivery or cancellation of the project may occur,	which would lead to a delay or non-realization of any benefit from the project.
Poor Sponsorship	As a result of having a sponsor who is unwilling to participate in project meetings,	scope reviews without sponsor participation may occur,	which would lead to the scope being misinterpreted and the formal sign-off of requirements being delayed .
Poor Project Management	As a result of the project manager not having the skills required to handle a conflict between two resources,	distracting and ongoing disputes between team members may occur ,	which would lead to tasks being completed late and the quality of the deliverables suffering.
Root cause: Product			
Poor Technology Selection	As a result of not researching multiple technology options,	the selection of unsuitable technology may occur,	which would lead to lost functionality, increased costs, support issues and ultimately project cancellation.
No Quality Measures	As a result of not having defined a process to log and communicate code defects during testing,	misunderstandings regarding the issues that are being found may occur,	which would lead to delays in bug fixes.
New Technology	As a result of depending on a technology that is still under development,	delays in delivery may occur,	which would lead to extend the schedule.

Enterprise risk management and strategy

Risk management is a strategic process.

Enterprise risk management helps an organization better understand how its mission, vision and core values provide the foundation for understanding what types and amount of risk are acceptable when setting strategy. That foundation results in three distinctively different ways that risk arises in the process:

- The possibility that strategy and business objectives may not align with the mission, vision and core values
- The types and amount of risk that the organization potentially exposes itself to by choosing a particular strategy
- The types and amount of risk inherent in carrying out its strategy and achieving business objectives and the acceptability of this level of risk and, ultimately, value

The figure below, illustrates strategy in the context of mission, vision and core values and as a driver of an entity's overall direction and performance.

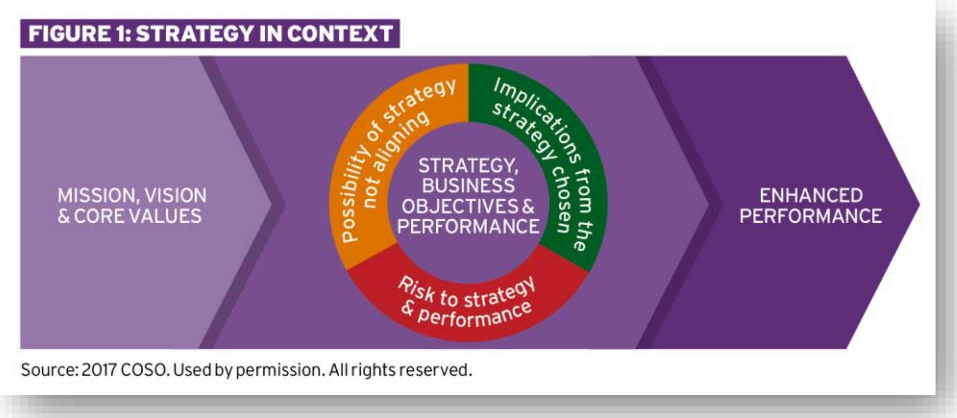


FIGURE 1: STRATEGY IN CONTEXT

MISSION, VISION & CORE VALUES
Possibility of strategy not aligning
Implications from the strategy chosen
STRATEGY, BUSINESS OBJECTIVES & PERFORMANCE
Risk to strategy & performance
ENHANCED PERFORMANCE

Source: 2017 COSO. Used by permission. All rights reserved.

Fig.1.20: Strategy in context

The figure starts with the organization's mission, vision and core values, which define what it wants to be and how it wants to conduct business. Essentially, these three make up its basic business model and reason for existence. The middle of the figure depicts the ongoing operations of the business, focusing on the establishment of strategy and business objectives and day-today performance of activities to achieve the strategy and objectives. Effective strategy, business objectives and performance will drive enhanced performance, which, ultimately, leads to the creation of enhanced value. When conducting strategic planning, it's easy to see the future through rose-colored glasses. That is, imagining the possibilities for success isn't that difficult. But recognizing the potential challenges to that success is much harder. However, studies have shown that the most significant causes of value destruction are embedded in the possibility of the strategy not supporting the organization's mission and vision and the implications from the strategy.

Implications from the strategy chosen

Enterprise risk management does not create the organization's strategy, but it helps in understanding the risks associated with alternative strategies being considered and, ultimately, with the adopted strategy. Decisions must be made on the trade-offs inherent in development of a strategy. Each alternative strategy has its risks – these are the implications arising from the strategy. The board of directors and management need to determine if the strategy works in alignment with the organization's risk appetite and how it will help enable the establishment of business objectives and allocation of resources that, ultimately, will lead to value creation and enhanced performance. Stated differently, the organization needs to evaluate how the chosen strategy could affect the entity's risk profile, specifically the types and amount of risk to which the organization is potentially exposed. Failure to properly consider such implications may result in unintended consequences.

When evaluating potential risks that may arise from strategy, management also must consider any critical assumptions that underlie the chosen strategy. These assumptions form an important part of the strategy and may relate to any of the considerations that form part of the entity's business context.

Enterprise risk management provides valuable insight into how sensitive changes to assumptions would affect achieving the strategy. Understanding the risks and their implications is not easy. By definition, risk involves uncertainty and, therefore, no board can be certain that all three types of risk are comprehensively considered at the culmination of the strategic planning process. However, taking the time to consider the three ways risk can arise in strategic planning will increase the likelihood that the chosen strategies and business objectives are successful. [14,15]

Chapter 02:

Cybersecurity

Cybersecurity

Definition of Cybersecurity

Before going into deep with risk management issues, it is considered important to give an accurate definition of the term ‘cybersecurity’. Cybersecurity is usually confused with information security, while there needs to be a distinction between these two terms. As well described in a paper published in Elsevier[1], cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him/herself. This additional dimension has ethical implications for society as a whole, since the protection of certain vulnerable groups, for example children, could be seen as a societal responsibility.

Cybersecurity is defined as “*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets*”. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

Information security, on the other hand, is defined as “*the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information*”.[2] The aim of information security is to ensure business continuity and minimize business damage by limiting the impact of security incidents.

It is important to note that there is also a difference between information security and information technology (or information and communication technology) security.

Information and communication technology (ICT) security deals with the protection of the actual technology-based systems on which information is commonly stored and/or transmitted. The definition of ICT security is thus very similar to that of information security. However, additional characteristics, which in this context could be better described as services that should be provided by secure information resources, are added to the definition. These include non-repudiation, accountability, authenticity, and reliability.[1]

So, it should be clear that there is a difference between securing information resources and securing ICT resources. A secure information resource could include any entity from which information is received or to which information is sent. A secure information technology resource is a secure information resource that happens to reside on an information technology system. It is also important to note that, in terms of ICT-based systems, the information alone cannot be deemed to be secure unless all resources and processes dealing with that information are secure as well.

When analyzing ICT security, as described above, various threats are targeting related vulnerabilities and, eventually, have a negative impact on ICT infrastructure. In this case the technological infrastructure is deemed to be the asset that needs protection. Accordingly, in ICT security the ICT is the asset that is secured. Fig. 2.1 depicts this relationship.

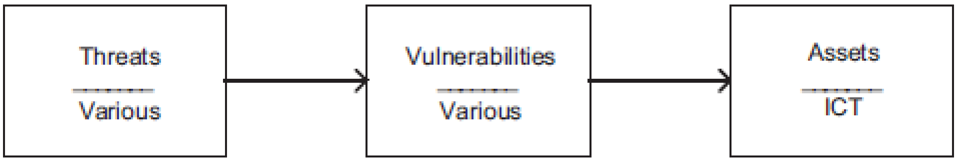


Fig. 2.1: ICT security

In the case of information security, ICT is the infrastructure that processes, stores and communicates information. In this case, it is information that is deemed to be the asset that requires protection, as depicted in Fig. 2.2. Information and communication technology can in this case be classified as, among other things, a vulnerability that is targeted by various threats in an attempt to compromise the asset, that is, information. Thus, it is important to note that, in the case of information security, information is the asset that is to be secured.

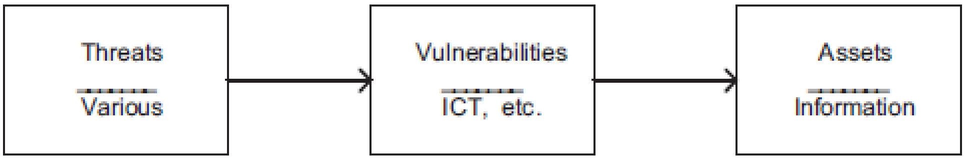


Fig. 2.2: Information security

In order to make it even clearer that cybersecurity differs from information and ICT security, there are cyber security threats to be taken into consideration, that do not form part of the formally defined scope of information security. These include the cases of cyber bullying, home automation, digital media, cyber terrorism and more:

- Being bullied in cyberspace does not constitute a loss of confidentiality, integrity, or availability of information. Instead, the target of such activities is the user him/herself. Accordingly, cyber bullying results in direct harm to the person being bullied.
- The increased convenience of managing one's home via the web is accompanied by the increased risk that someone might gain unauthorized access to such systems and cause harm. This harm could range from "pranks" like turning off the hot water, to serious crimes like turning off the security system in order to burgle the home. Once again, in this case one can argue that the victim's information is not necessarily negatively affected. Instead, other assets of the victim are the target of the cybercrime.
- Every year enormous amounts of potential revenue are lost to the sharing of illegal movies, music, and other forms of digital media. This illegal sharing does not

necessarily affect the confidentiality, integrity, or availability of the shared media; however, it does directly affect the financial wellbeing of the legal owner of the rights to the specific media.

- Cyber terrorists or enemy specialists may target a country's critical infrastructure via cyberspace. This could either be indirectly, for example by influencing the availability of information services using denial-of-service attacks or, more directly, through an attack on the national electricity grid. In this case, it is neither the information itself nor the individual information user that is at risk, but rather the wellbeing of society as a whole. the interests of a person, society, or nation, including their non-information-based assets, need to be protected from risks stemming from interaction with cyberspace. This serves to highlight the difference between information security and cyber security.

As demonstrated in the scenarios above, in cyber security the assets that need to be protected can range from the person him/herself to common household appliances, to the interests of society at large, including critical national infrastructure. In fact, such assets include absolutely anyone or anything that can be reached via cyberspace. In cyber security, information and ICT are the underlying cause of the vulnerability. All assets that should be protected need to be protected because of the vulnerabilities that exist as a result of the use of the ICT that forms the basis of cyberspace. These vulnerabilities can even affect intangible assets. In cybersecurity, assets include the personal or physical aspects, both tangible and intangible, of a human being. Cyber security also includes the protection of societal values (intangible) and national infrastructure (tangible).[16]

Summarizing the above, cyber security can be defined as the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace. The human element, including national interests, is playing an ever-increasing role in cyber security and certainly the current set of international standards and best practices is not comprehensive enough to secure cyberspace.

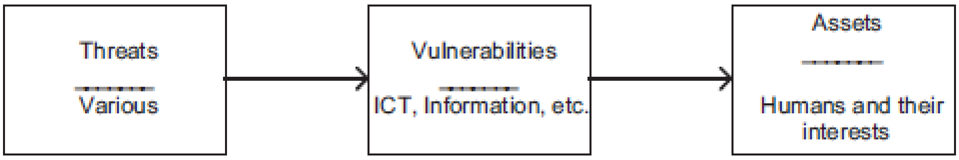


Fig. 2.3: Cyber security

Information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities. Cyber security, on the other hand, is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace.

Just as information security expanded on the concepts of ICT security in order to protect the information itself, irrespective of its current form and/or location, cyber security needs to be seen as an expansion of information security. Cyber security should be about protecting more than just the information, or information systems resources, of a person/ organization. Cyber security is also about the protection of the person(s) using resources in a cyber environment and about the protection of any other assets, including those belonging to society in general, that have been exposed to risk as a result of vulnerabilities stemming from the use of ICT[17].

The relationship between these three overlapping concepts is illustrated in Figure 2.4:

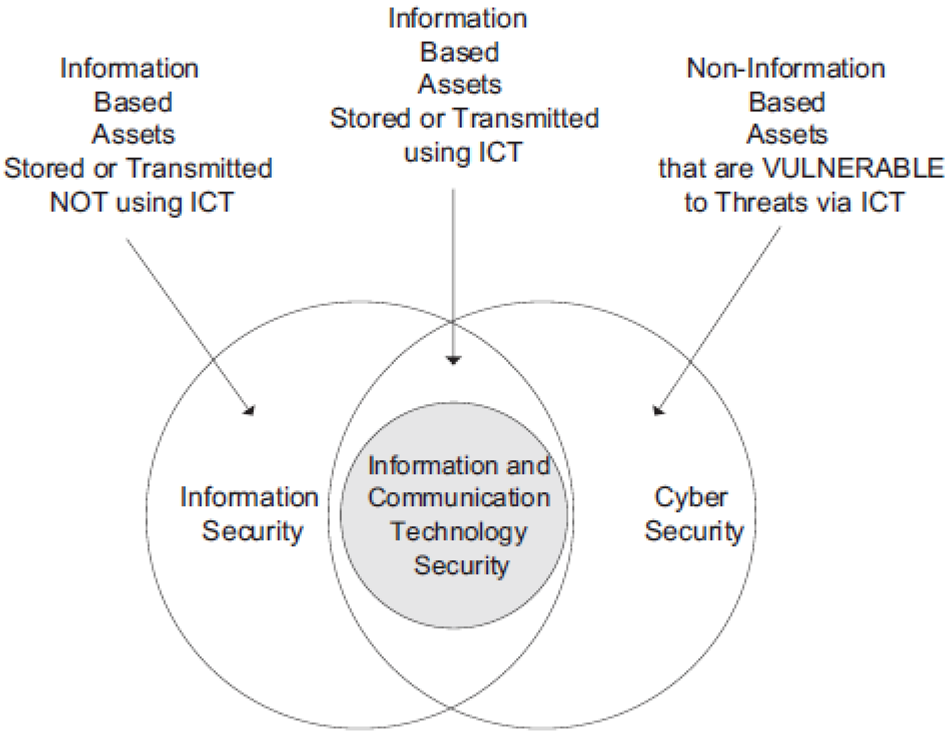

Information Based Assets Stored or Transmitted NOT using ICT
Information Based Assets Stored or Transmitted using ICT
Non-Information Based Assets that are VULNERABLE to Threats via ICT
Information Security
Information and Communication Technology Security
Cyber Security

Fig. 2.4: The relationship between ICT security, information security, and cybersecurity

Now, assuming that the core differences between information, ICT and cyber security have been well defined and the concept of cybersecurity has been clarified, it is time to proceed to the main section of this work, cybersecurity strategy.

In the following chapters, there will be an in-depth analysis of what components a strategy consists of and how its role is related to risk management, how it is structured and implemented in the cybersecurity sector and who are the stakeholders involved.

Moreover, relevant initiatives will be discussed in the context of both prevention and response to cybersecurity incidents.

Cyber Assets

Cyber Asset means any programmable electronic device, including hardware, software, information, or any of the foregoing, which are components of such devices or enable such devices to function.[18]

In information security, computer security and network security, an asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware (e.g., servers and switches), software (e.g. mission critical applications and support systems) and confidential information. [19,20]

Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization[21]

How is a Cyber Security Asset defined?

This can be a tricky question to answer as one navigates the many regulations of the industry, which are regularly updated to adjust to the changing needs of systems per sector. There are a few things to consider while attempting to define cyber security assets, that can be summarized in the five steps that follow:

1. Identify Cyber Assets Associated with a Critical Asset.

A responsible entity should inventory and evaluate cyber assets in order to identify those that might impact any of their critical assets. Cyber assets to consider include, but are not limited to:

- Control systems
- Data acquisition systems
- Networking equipment
- Hardware platforms for virtual machines or storage
- Secondary or supporting systems such as virus scanners, HVAC systems, and uninterruptible power supplies (UPS)

2. Group Cyber Assets.

In order to simplify the process of cyber security asset definition, cyber assets can be grouped according to various functions and characteristics. One category might include cyber assets that communicate with a particular software. Other examples would be groups based on functions that support specific critical assets.

3. Determine Cyber Assets Which are Essential.

Evaluate an asset's impact on critical assets according to the following criteria:

- Is it essential to the reliable operation of a critical asset?
- Does it display, transfer, or contain information necessary for real-time operational decisions?
- Would its loss, degradation, or compromise affect the reliability or operability of the bulk power system?

4. Identify Cyber Assets with Qualifying Connectivity.

According to standard CIP-002 R3, cyber assets that meet any of the following requirements are "critical":

- It uses a routable protocol to communicate outside the Electronic Security Perimeter (ESP).
- It uses a routable protocol within a Control Center.
- It is dial-up accessible.

5. Compile the List of Critical Cyber Assets.

Once cyber assets have been evaluated and it has been determined which of those are essential to the security of critical assets, they should be documented in a list in order to comply with NERC-CIP standards.

When it comes to critical cyber assets, knowing is half the battle. Keeping up with regulations can be challenging, but essential. [22]

The CIA triad

The goal of information security is to ensure the confidentiality, integrity and availability (CIA) of assets from various threats. For example, a hacker might attack a system in order to steal credit card numbers by exploiting a vulnerability. Information Security experts must assess the likely impact of an attack and employ appropriate countermeasures. In this case they might put up a firewall and encrypt their credit card numbers.

Assets, critical assets, cyber assets, and critical cyber assets

An asset is simply a term for a component that is used within an industrial control system. Assets are often "physical," such as a workstation, server, network switch, or PLC. Physical assets also include the large quantity of sensors and actuators used to control an industrial process or plant. There are also "logical" assets that represent what is contained within the physical asset, such as a process graphic, a database, a logic program, a firewall rule set, or firmware. When thinking about it, cyber security is usually focused on the protection of "logical" assets and not the "physical" assets that contain them. Physical security is that which tends to focus more on the protection of a physical asset. Security from a general point-of-view can therefore effectively protect a "logical" asset, a "physical" asset, or both.

The Critical Infrastructure Protection (CIP) standard by the North American Electric Reliability Corporation (NERC) through version 4 has defined a "critical cyber asset" or "CCA" as any device that uses a routable protocol to communicate outside the electronic security perimeter (ESP), uses a routable protocol within a control center, or is dial-up accessible. This changed in version 5 of the standard by shifting from an individual asset approach, to one that addresses groupings of CCAs called bulk electric system (BES) cyber "systems." This approach represents a fundamental shift from addressing security at the component or asset level, to a more holistic or system-based one.

A broad and more generic definition of "asset" is used in this book, where any component—physical or logical; critical or otherwise—is simply referred to as an "asset." This is because most ICS components today, even those designed for extremely basic functionality, are likely to contain a commercial microprocessor with both embedded and user-programmable code that most likely contains some inherent communication capability. History has proven that even single-purpose, fixed-function devices can be the targets, or even the source of a cyber-attack, by specifically exploiting weaknesses in a single component within the device (See Chapter 3, "Industrial Cyber Security History and Trends"). Many devices ranging from ICS servers to PLCs to motor drives have been impacted in complex cyber-attacks—as was the case during the 2010 outbreak of Stuxnet . Regardless of whether a device is classified as an "asset" for regulatory purposes or not, they will all be considered accordingly in the context of cyber security.[23,24,25]

Cyber Threats

Cyber Threat Actors

Threat actors or malicious actor is outlined as an entity that's utterly or partly liable for an incident that may influence the safety of an organization's network. in contrast to hacker or attacker, it's not necessary for the Threat actor to possess technical skills. Threat actors can be an individual or a company, having an intention to hold out an event which will have a malicious or benign result on the security of an organization's infrastructure or systems.

Discussed below are the most common types of threat actors:

- *Hacktivists*

Hacktivism is an attack wherever hackers break into a government's or company's systems as an act of protest. Hacktivists use hacking to extend awareness of their social or political agendas, also as themselves, in both web (online) and offline arenas.

Common hacktivist targets embody government agencies, international firms, or the other emits that they understand as a threat. It remains a truth, however, that gaining unauthorized access could be a crime, no matter their intentions.

- ✧ *Cyber Terrorists*

Cyber terrorists square people with a good vary of skills, intended by non-secular or affairs of state tolerate concern of large-scale disruption of pc networks.

- ✧ *Suicide Hackers*

Suicide hackers are unit people who aim to bring down the crucial infrastructure for a "cause" and don't seem to be upset concerning facing jail terms or the other reasonably penalty. Suicide hackers square measure like suicide bombers, who sacrifice their lives for an attack and are therefore not involved with the implications of the in actions.

- ✧ State-Sponsored Hackers

State-sponsored hackers square people utilized by the government to penetrate and gain classified info and to break info systems of alternative governments.

- ✧ Organized Hackers

Organized hackers square skilled hackers having the aim of assault a system for profits. They hack to get confidential information like Social Security numbers, personal recognizable info (PlI), health records, and monetary info such as bank records, and MasterCard info.

- ✧ Script Kiddies

Script kiddies are a unit unskilled hackers who compromise systems by running scripts, tools, and software package developed by real hackers. they sometimes target the number of attacks instead of the standard of the attacks that they initiate.

- ✧ Industrial Spies

Industrial spies are people who attempt to attack the businesses for industrial functions. Business competitors typically rent hackers or people who are typically known as industrial spies, United Nations agency attack the target organization to steal direction like business strategy, money records, and employees' data.

- ✧ Insider Threat

Insider threat refers to a threat that originates from people within the organization it's usually administrated by a privileged user, discontent worker, terminated worker, inclined worker, third party, or under-trained workers. the most objective of such attacks is either to require revenge on a corporation by damaging its name or gain monetary edges.

Motives, Goals, and Objectives of Cyber Security Attacks

Attackers usually have motives (goals) and objectives behind cybersecurity attacks. A motive originates out of the notion that a target system stores or processes one thing valuable that ends up in the threat of an attack on the system. the aim of the attack could also be to disrupt the target organization's business operations, to steal valuable data for the sake of curiosity, or perhaps to actual revenge. Therefore, these motives or goals rely upon the attacker's state of mind, his/her reason for closing such an activity, and his/her resources and capabilities. Once the wrongdoer determines his/her goal, he/she will use varied tools, attack techniques, and ways to use vulnerabilities in a very computer system or security policy and controls.

Attacks = Motive (Goal) + technique + Vulnerability

Motives behind data security attacks are usually:

- Disrupting business continuity
- Performing info theft
- Manipulating knowledge
- Creating concern and chaos by disrupting vital infrastructure s
- Bringing loss to the target
- Propagating non-secular or politics
- Achieving state's military objectives
- Damaging name of the target
- Taking revenge
- Demanding ransom

Threat actors can be internal or external to the organization being targeted, and they may or may not possess the technical skillsets needed to infiltrate and compromise networks and corporate data.[26]

Cyber Threat Reporting

Cybersecurity related companies and/or organizations regularly publish cyber threat intelligence reports that describe the members of Advanced Persistent Threat (APT) groups, how they work and how to recognize their tactics, techniques and procedures. They gather and publicize threat intelligence gathered from millions of virtual machines in customer deployments. Expert analysts monitor, interpret, and package the data to better arm the public against cyber attackers. These annual threat reports include global and regional threat intelligence on industry trends as well as detailed malware analyses.

Cyber threat intelligence reports also cover vulnerabilities of specific business technologies, such as email, sandboxes and mobile devices. With access to such details cyber security experts can build better defenses against these APT groups and advanced cyber attacks.

Below, we will examine the results of Netwrix's Cyber Threat Report for the past year (2020). Netwrix is a cybersecurity vendor that empowers information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers. [27]

Netwrix Cyber Threat Report

When the 2020 pandemic hit organizations around the world, many of them scrambled to enable their employees to work from home. Almost immediately, news outlets were reporting a skyrocketing number of cyberattacks on the newly broadened IT infrastructures, as well as targeted attacks on employees trying to adjust to their new work-from-home environment.

In June 2020, 937 IT professionals from all over the globe were surveyed by Netwrix to learn how their threat landscape and priorities have changed due to this massive shift to remote work. The findings, which are presented here, aim to help organizations re-assess their security risks and identify new security gaps.

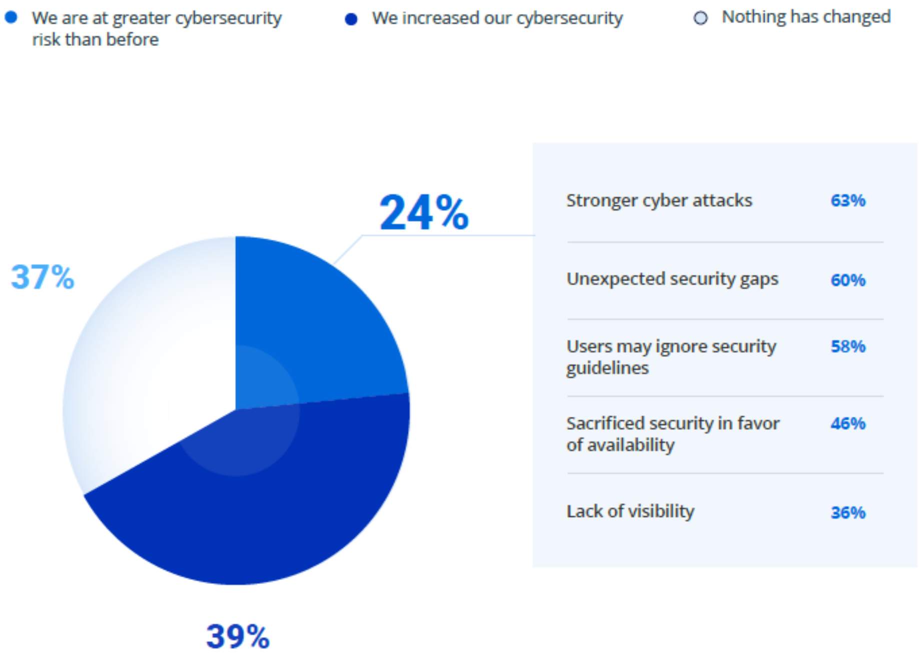


Fig.2.5: Survey participants' answers regarding their cybersecurity posture turnaround due to COVID-19

About half of small organizations (those with up to 100 employees) said that the pandemic didn't have any impact on their data security, and the other half were fairly evenly split between saying they are at greater risk and saying they have improved their cybersecurity. In contrast, about half of medium and large organizations claimed that the rapid transition to remote work actually helped them strengthen their security controls.

Most organizations, regardless of size, based on the same report, say that they are at greater risk cited increased intensity of cyberattacks and employee negligence in following corporate cybersecurity guidance.

Table.2.1: Survey participants' answers regarding their cybersecurity posture turnaround due to COVID-19

	SMALL 1-100	MEDIUM 101-1,000	LARGE 1,001+
WE ARE AT GREATER CYBERSECURITY RISK THAN BEFORE	21%	29%	23%
WE HAVE INCREASED OUR CYBERSECURITY	28%	43%	47%
NOTHING HAS CHANGED	51%	28%	30%

Employee mistakes, including accidental improper sharing of data by employees and errors by admins, remain key concerns, holding nearly steady at over 60% of respondents. Both ransomware and phishing dropped slightly in the threat ranking but remain firmly on organizations' radar, with over 60% still naming them. That's wise, given how actively hackers have been employing these techniques to exploit people's fear and confusion, such as by distributing malicious emails that mention COVID-19.

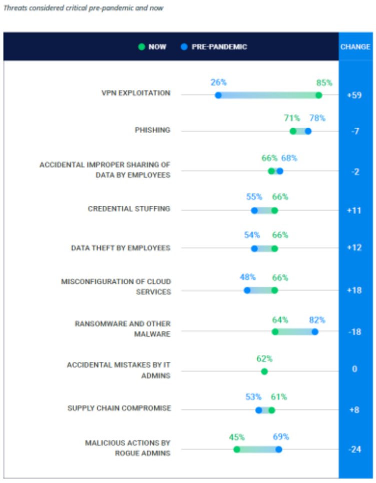


Fig.2.6: Survey participants' cybersecurity posture turnaround due to COVID-19, based on threats

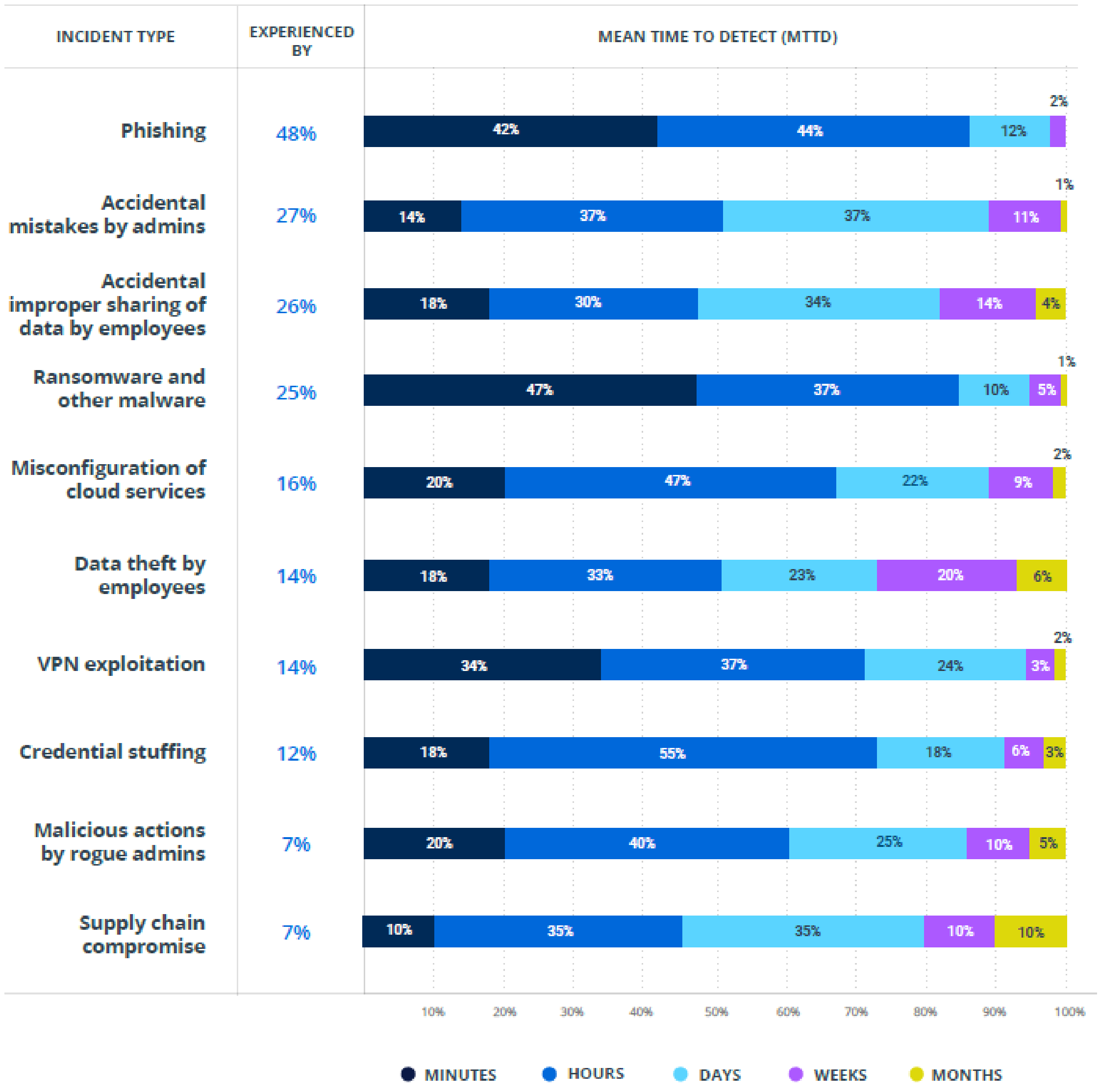


Fig.2.7: Most common cybersecurity incidents since organizations went remote

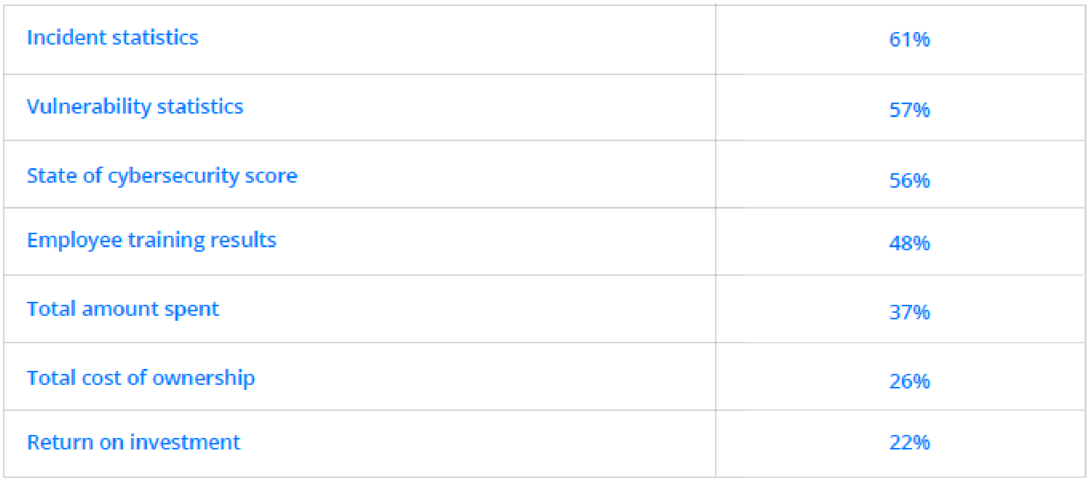
Regarding threat reporting, as data claim, the majority (66%) of IT professionals regularly report on the state of cybersecurity to their leadership. Mainly these reports include:

- Incident statistics, such as number of incidents detected, number responded to, and mean time to resolve
- Vulnerability statistics, such as the number of vulnerabilities identified or patched, and the average time to patch
- General "state of cybersecurity" score, an average figure that sums up several cybersecurity metrics to track overall success

Incident and vulnerability statistics are raw numbers often present limited value for decision-making. Therefore, many IT leaders are trying to create their own "state of cybersecurity score" to report on the success or failure of their implemented security measures. However, there are no standards, so each IT leader is left to their own devices. The survey shows that

56% of security professionals are trying to calculate some sort of average score. We expect that such high demand for an integral metric of cybersecurity will be addressed by the professional community and experts in the near future. 48% of respondents report the results of employee training, a major metric for tracking cybersecurity.

As the economic downturn unfolds, we expect more CFOs to be asking IT leaders to justify proposed expenses via a ROI analysis before approving the budget. 37% of organizations already try to calculate the total amount their organizations spend on cybersecurity. However, only about a quarter of respondents report detailed financial metrics like return on investment (ROI) and total cost of ownership (TCO).



Incident statistics	61%
Vulnerability statistics	57%
State of cybersecurity score	56%
Employee training results	48%
Total amount spent	37%
Total cost of ownership	26%
Return on investment	22%

Fig.2.8: Most common metrics to report on the state of cybersecurity

One reason that just 22% of IT organizations report on the ROI of their security investments is the complexity of the calculation. However, providing clear ROI figures makes it much easier to win budget approvals from senior leaders, since it reveals the probable costs of a breach and therefore the hard dollar savings they will reap by avoiding one.

Cyber Predictions for 2021

Netwrix, has also recently released predictions about key trends that will impact organizations in 2021 and beyond. Most of them arise from the digital transformation and new workflows required by the rapid transition to remote work in 2020. Ilia Sotnikov, cybersecurity expert and Netwrix Vice President of Product Management, recommend that IT and security professionals refine their risk management and business continuity strategies with these seven predictions in mind.

1. Ransomware will do more damage in order to motivate payments.

Next-gen ransomware will be designed to do damage that is more difficult to recover from in order to force organizations into paying the ransom. One example is “bricking” devices by modifying the BIOS or other firmware. Cybercriminals will also be expanding to new targets, such as operational technology and IoT devices, which may have a much more visible impact on the physical world.

2. Cloud misconfigurations will be one of the top causes of data breaches.

A lack of clear understanding of the shared responsibility model due to the rapid transition to the cloud will backfire in 2021. The speed of transition coupled with prioritizing productivity over security has made misconfigurations inevitable, resulting in overexposed data.

3. Hackers will increasingly target service providers.

The shortage of cybersecurity experts will lead more organizations to turn to managed service providers (MSPs). In response, hackers will conduct targeted attacks on MSPs in order to get access to not just one organization but all of the MSP's customers.

4. The rapid digital transformation in 2020 will have a delayed impact on cybersecurity in 2021.

In 2020, organizations were forced to quickly adapt to new ways of working and implement new technologies; and through their own admission via the upcoming Netwrix survey with little experience and nearly no time for planning and testing. In 2021, the security gaps caused by the inevitable mistakes during this rapid transition will be exploited, and we will see new data breach patterns like the recent Twitter hacks.

5. Proof of value will drive business conversations.

Executives will be looking for specific metrics in order to assess the value delivered by the products and security measures the company is using. The practice of justifying the value of current investments and the necessity of new investments will become more generally accepted.

6. Companies will balance cybersecurity and business needs by focusing on risk.

The challenges of the pandemic will force organizations to reassess their priorities. In particular, IT teams will have to find the right balance between ensuing strong security and serving business needs like scalability and accessibility. Expectations will shift from the unrealistic notion of ensuring 100% security to determining and meeting acceptable levels of risk and resilience.

7. Insurance and legislation will drive mass adoption of core security best practices.

To minimize the risk of incurring steep fines for compliance failures, businesses will turn to cyber insurance. However, those policies will come with their own security standards and requirements, such as regular risk assessment and effective detection and response capabilities. As a result, organizations will focus as much on meeting those criteria as much as they do on complying with the regulatory standards themselves.

Cyber Risk

Considering all the above, cyber risk is the fastest growing enterprise risk and organizational priority today. According to the 2019 Global Risk Perception Survey, cyber risk was ranked as a top 5 priority by 79% of global organizations.

The growth of cyber risk is in large part tied to the increasing use of technology as a value driver. Strategic initiatives—such as outsourcing, use of third-party vendors, cloud migration, mobile technologies, and remote access—are used to drive growth and improve efficiency, but also increase cyber risk exposure. Cyber risk has evolved from a technology issue to an organizational problem. In short, cyber risk is everyone's problem.

A compounding factor here is over the last two decades, cyber crime has grown exponentially. According to the IC3, the FBI's cyber crime reporting mechanism, monetary damages from reported cyber crime totaled $3.5 billion in 2019, while Cybersecurity Ventures project that the global costs of cybercrime will double to $6 trillion in 2021, up from $3 trillion in 2015.

Definition of Cyber Risk

Cyber risk, or cybersecurity risk, is the potential exposure to loss or harm stemming from an organization's information or communications systems. Cyber attacks, or data breaches, are two frequently reported examples of cyber risk. However, cybersecurity risk extends beyond damage and destruction of data or monetary loss and encompasses theft of intellectual property, productivity losses, and reputational harm.

Examples of Cyber Risk

Cyber risk can be faced by any organization and can come from within the organization (internal risk) or from external parties (external risk). Both internal and external risks can be malicious or unintentional.

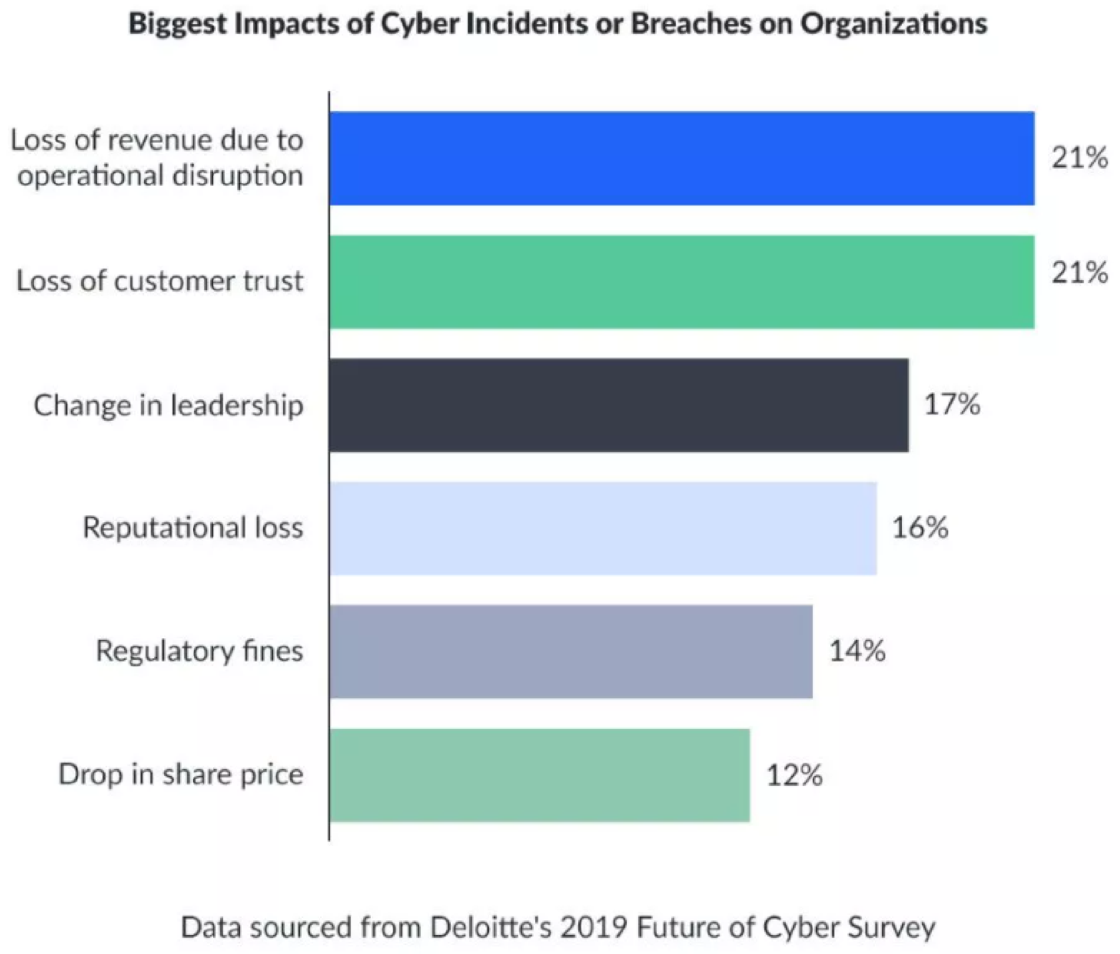
Internal risks stem from the actions of employees inside the organization. An example of malicious, internal cyber risk would be systems sabotage or data theft by a disgruntled employee. An example of unintended, internal risk would be an employee who failed to install a security patch on out-of-date software.

External risks stem from outside the organization and its stakeholders. An external, malicious attack could be a data breach by a third party, a denial-of-service attack, or the installation of a virus. An unintentional, external attack usually stems from partners or third parties who are outside yet related to the organization - a vendor whose systems outage results in an operational disruption to the organization.

Impact of Cyber Risk

According to Deloitte Advisory Cyber Risk Services, “Cyber risk is an issue that exists at the intersection of business risk, regulation, and technology.” In their 2019 Future of Cyber Survey,

Deloitte found that the impact of security incidents varied from real monetary costs, including financial loss due to operational disruptions and regulatory fines, to intangible costs, including the loss of customer trust, reputational loss or a change in leadership.



Biggest Impacts of Cyber Incidents or Breaches on Organizations

Data sourced from Deloitte's 2019 Future of Cyber Survey

Fig.2.9: Biggest impacts of cyber incidents or breaches on organizations

Cybersecurity risks can result in both quantitative loss and qualitative impact. Realized costs may include lost revenue due to disruptions to productivity or operations, incident mitigation and remediation expenses, legal fees, or even fines. Less tangible impacts of cybersecurity incidents, which are difficult to quantify and generally take longer to rectify, include loss of goodwill, diminished brand reputation, or a weakened market position.

Managing Cyber Risk

Cyber risk has the potential to affect every aspect of an organization, including its customers, employees, partners, vendors, assets, and reputation. As such, an effective cyber risk management program involves the entire organization. Although IT or Infosec may ultimately own cybersecurity risk management, cyber risk is dispersed throughout the organization, requiring an integrated approach and cross-divisional collaboration to effectively manage and mitigate exposure.

Below are 4 key steps an organization can take to implement a robust cyber risk management strategy.

- Understand their Risk Profile: Understanding the organization's risk profile and potential exposure requires an enterprise-wide threat assessment.
    - Identify critical enterprise risks to determine the applications, systems, databases, and processes subject to cyber risk. Consider the array of external and internal threats, from unintentional user error to third-party access to malicious attacks.
    - Undertake risk assessments with all stakeholders to assess the likelihood and potential impact of cyber risk exposure, including cross-divisional and secondary effects and technology dependencies. Consider third-party exposure, as they have increasingly become vectors for cyber incidents, and the risk posed by the expanding technology perimeter due to work from home requirements.
    - Quantify risks including the potential financial, operational, reputational, and compliance impact of a cyber risk incident. A risk scoring framework can help provide a more holistic ranking of threats.
- Set a Firmwide Strategy: Establish a firmwide strategic framework for cyber risk management
    - Prioritize risks by employing a shared risk measurement framework and reporting systems to effectively prioritize risks across the organization and enable informed resource allocation.
    - Consider industry-specific risk standards and incorporate any specific compliance requirements into the cyber risk management practice.
    - Set and communicate an enterprise-wide IT and cyber risk management strategy. Technology infrastructure and application use is critical throughout every organization. Therefore, cyber risk exposure can occur in any division, making it an organizational priority, rather than an IT one.
- Invest in Cyber Risk Management Infrastructure
    - Assess system requirements to understand where organizational cyber threats originate and provide a guidepost to the types of systems required. A distributed, cloud-based organization will have different needs from a physical asset intensive organization. Consider how the company currently operates to ensure that a GRC platform will accommodate evolving needs.

    - Potential investment in GRC software or other cyber risk management tools should also consider risk reporting and incident management requirements, workflows, ease of use, flexibility, and future expansion capability.
- Establish a Dynamic Cyber Risk Management Process
    - Establish robust oversight by maintaining an updated inventory of potential threats and dynamic quantification of the potential impact and mitigation costs of cyber incidents.
    - Communicate with third parties to ensure their security protocols align with organizational standards and practices.
    - Invest in Training - With rapid evolution of technology and related cybersecurity risks, cyber risk management is not a static, tick the box solution. Organizations can spend large sums on state of the art security infrastructure, but a truly effective cyber risk management program requires effective stakeholder training.[28]

Cyber Risk analysis

When performing risk analysis, it is important to weigh how much to spend protecting each asset against the cost of losing the asset. It is also important to take into account the chance of each loss occurring. Intangible costs must also be factored in. If a hacker makes a copy of all a company's credit card numbers it does not cost them anything directly but the loss in fines and reputation can be enormous.

In Information security, Risk factor is a collective name for circumstances affecting the likelihood or impact of a security risk. Factor Analysis of Information Risk (FAIR) is devoted to the analysis of different factors influencing IT risk. It decompose at various levels, starting from the first level Loss Event Frequency and Probable Loss Magnitude, going on examining the asset, the threat agent capability compared to the vulnerability (computing) and the security control (also called countermeasure) strength, the probability that the agent get in contact and actually act against the asset, the organization capability to react to the event and the impact on stakeholders.

Risk factors are those factors that influence the frequency and/or business impact of risk scenarios; they can be of different natures, and can be classified in two major categories:

- Environmental, further subdivided in:
    - Internal environmental factors are, to a large extent, under the control of the enterprise, although they may not always be easy to change
    - External environmental factors are, to a large extent, outside the control of the enterprise.
- Capability of the organization, further subdivided in:
    - IT risk management capabilities—To what extent is the enterprise mature in performing the risk management processes defined in the Risk IT framework
    - IT capabilities—How good is the enterprise at performing the IT processes defined in COBIT

    - IT-related business capabilities (or value management)—How closely do the enterprise's value management activities align with those expressed in the Val IT processes

An IT risk scenario is a description of an IT related event that can lead to a business impact, when and if it should occur. Risk factors can also be interpreted as causal factors of the scenario that is materializing, or as vulnerabilities or weaknesses. These are terms often used in risk management frameworks. Risk scenario is characterized by:

- a threat actor that can be:
    - Internal to the organization (employee, contractor)
    - External to the organization (competitor, business partner, regulator, act of god)
- a threat type
    - Malicious,
    - Accidental
    - Failure
    - Natural
- Event
    - Disclosure,
    - Modification
    - Theft
    - Destruction
    - Bad design
    - ineffective execution
    - inappropriate use
- asset or resource
    - People and organization
    - Process
    - Infrastructure or facilities
    - IT infrastructure
    - Information
    - Application
- Time
    - Duration
    - Timing of occurrence (critical or not)
    - Timing to detect
    - Timing to react

The risk scenario structure differentiates between loss events (events generating the negative impact), vulnerabilities or vulnerability events (events contributing to the magnitude or frequency of loss events occurring), and threat events (circumstances or events that can trigger loss events). It is important not to confuse these risks or throw them into one large risk list.[29]

Cyber risk analysis and management will further be explained in the following chapter.

Chapter 03:

Cyber Risk Management

Cyber Risk Management

The strategic concept

Cyber threats are constantly evolving. The most effective way to protect an organization against cyber-attacks is to adopt a risk-based approach to cyber security, where risks, as well as current measures' effectiveness and appropriateness can be regularly reviewed.

A risk-based approach means that the implemented cyber security measures are based on the organization's unique risk profile, so there is no waste of time, effort or expense addressing unlikely or irrelevant threats.

IT Governance can help to this direction, ensuring a cyber threat management strategy development, which enables a systematic approach to managing security challenges.[30]

The 3-pillar approach

There is a three-pillar approach to cyber security. This, consists of people, process, and data and information, as depicted in the figure below:

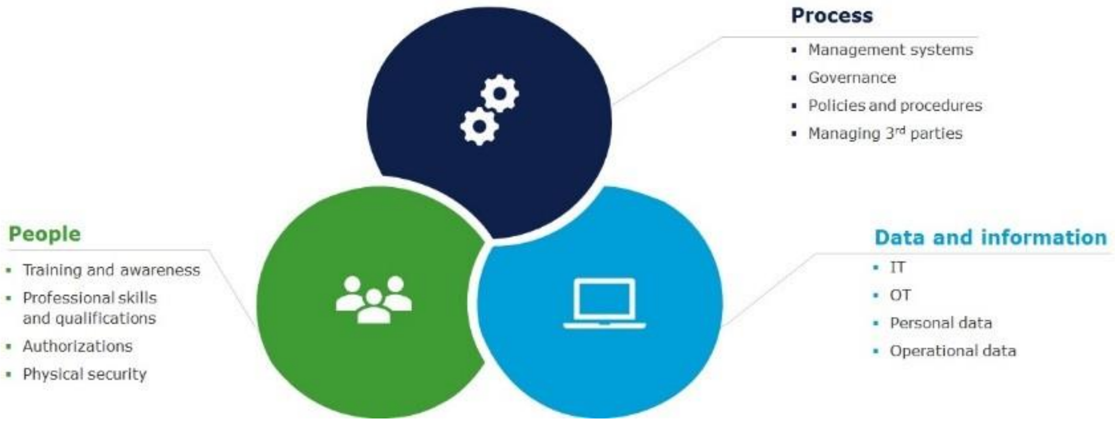


Fig. 3.1: The 3-pillar approach to cybersecurity

1st pillar: People

People are known to be the weak link in the whole process; implying, the biggest risk. People may contain staff, as well as other individuals an organization may come into contact with – i.e. contractors.

According to Verizon's 2018 Data Breach Investigations Report, phishing or other forms of social engineering cause 93% of all data breaches. For phishing or social engineering attacks to be successful, the attacker needs a target, which most often are employees. Therefore, in conjunction with the implementation of IT security measures, training employees is crucial to preventing these types of cyber security attacks. Employers must make employees aware of any possible risks associated with clicking on a link in a phishing email, downloading an attachment from an unknown sender or responding to requests for credential/login information or other data.

Employee training is one of the least expensive and most effective tools an organization can use to reduce the risk of a cyberattack. This training can be both formal and informal. Formal training would include training on the organization's policies and procedures as well as specific incident response training. For informal training, organizations should consider periodic e-mail blasts to employees detailing current threats and simulated phishing attacks with follow-up feedback.

Practical training methods should not stop with an organization's general workforce. In addition to the employee training described above, companies should consider engaging in tabletop exercises that prepare an organization to react in the unfortunate event it experiences a breach. Specifically, these exercises simulate a data breach incident and allow an organization's executives to test the organization's ability to respond in the event of an attack using its formal policies and procedures. Overall, through frequent exposure and regular training, any organization is able to develop a culture of cyber security awareness.[31]

2nd pillar: Processes

The second pillar is processes. Processes are key to the implementation of an effective cyber security strategy. They are crucial in defining how an organization's activities, roles and documentation are used to mitigate information risks. Processes also need to be continually reviewed.

The process pillar is made up of multiple parts: management systems, governance, policies, procedures and managing third parties. All of these parts must be addressed for the process pillar to be effective.

Management systems

To strengthen the second pillar in a cyber security strategy, a proper management system must be put in place. Management systems are key to the second pillar.

Everyone in the organization should understand their duties and responsibilities when it comes to cyber security. For a large and diverse organization, the level of competence and interest in cyber security will vary greatly between employees, but a good management system can increase the security awareness and increase the organization's resilience. Without a clear management system in place, issues and data will fall through the cracks, making the entire company vulnerable to cyber security problems, up to and including a data breach.

Enterprise security governance activities

Governance is a company's strategy for reducing the risk of unauthorized access to information technology systems and data. Enterprise security governance activities involve the development, institutionalization, assessment and improvement of an organization's enterprise risk management (ERM) and security policies. Governance of enterprise security includes determining how various business units, personnel, executives and staff should work together to protect an organization's digital assets, ensure data loss prevention and protect the organization's public reputation.

Enterprise security governance activities should be consistent with the organization's compliance requirements, culture and management policies. The development and sustainment of enterprise security governance often involve conducting threat, vulnerability and risk analysis tests that are specific to the company's industry.

Enterprise security governance is also a company's strategy for reducing the chance that physical assets owned by the company can be stolen or damaged. In this context, governance of enterprise security includes physical barriers, locks, fencing and fire response systems as well as lighting, intrusion detection systems, alarms, cameras and so on.

Link between vision and daily operations

A ‘policy’ is a predetermined course of action, which is established to provide a guide toward accepted business strategies and objectives. In other words, it is a direct link between an organization’s ‘vision’ and their day-to-day operations. Policies identify the key activities and provide a general strategy to decision-makers on how to handle issues as they arise. This is accomplished by providing the reader with limits and a choice of alternatives that can be used to guide their decision-making process as they attempt to overcome problems. Policies can be thought of as a globe, where national boundaries, oceans, mountain ranges and other major features are easily identified.

The goal of every procedure is to provide the reader with a clear and easily understood plan of action required to carry out or implement a policy. A well-written procedure will also help eliminate common misunderstandings by identifying job responsibilities and establishing boundaries for the job-holders. Good procedures allow managers to control events in advance and prevent the organization (and employees) from making costly mistakes. A procedure can be considered as a road map where the trip details are highlighted to prevent a person from getting lost or ‘wandering’ off an acceptable path identified by the company’s management team.

Managing third parties

Third party management is better known as vendor management. It is a discipline that enables organizations to control costs, drive service excellence and mitigate risks to gain increased value from their vendors throughout the deal life cycle.

When selecting a vendor to work with, it must be ensured that they meet the same levels of cyber security as required by the company. Many companies have had data breaches that started by a vendor being hacked, allowing the attackers to gain access to their system.[32]

3rd pillar: Technology

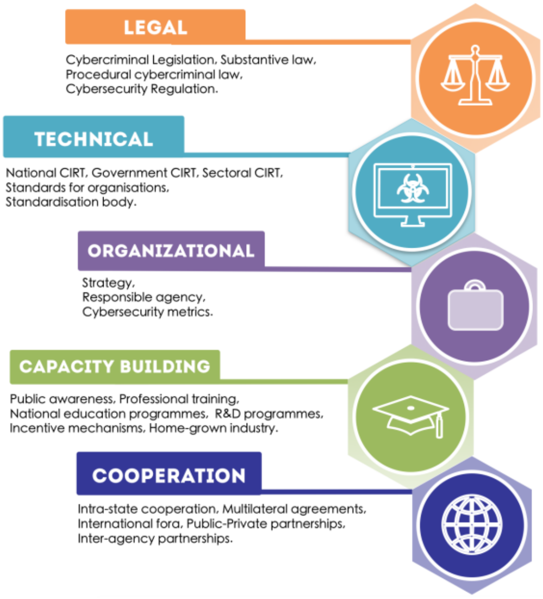
The third pillar deals with data and information protection and it is the most important of a sound cyber security strategy. It is crucial to consider the ‘CIA triad’ when considering how to protect data.

Data and information protection is the most technical and tangible of the three pillars. The gathered data comes from multiple sources, such as information technology (IT), operational technology (OT), personal data and operational data. It must be properly managed and protected every step of the way.

The GCI overall approach

Besides the before-mentioned 3-pillar approach, there is also one provided by ITU (International Telecommunication Union), the GCI overall approach. GCI stands for Global Cybersecurity Index and it is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States cybersecurity commitment with regard to the five pillars identified by the High-Leve Experts and endorsed by the GCA (Global Cybersecurity Agenda). It basically is a capacity building tool, to support countries to improve their national cybersecurity.

The five pillars of this approach are:


LEGAL
Cybercriminal Legislation, Substantive law,
Procedural cybercriminal law,
Cybersecurity Regulation.
TECHNICAL
National CIRT, Government CIRT, Sectoral CIRT,
Standards for organisations,
Standardisation body.
ORGANIZATIONAL
Strategy,
Responsible agency,
Cybersecurity metrics.
CAPACITY BUILDING
Public awareness, Professional training,
National education programmes, R&D programmes,
Incentive mechanisms, Home-grown industry.
COOPERATION
Intra-state cooperation, Multilateral agreements,
International fora, Public-Private partnerships,
Inter-agency partnerships.

i. Legal Measures

ii. Technical and Procedural Measures

iii. Organizational Structure

iv. Capacity Building

v. International Cooperation

Fig. 3.2: The GCI 5-pillar approach to cybersecurity

This is not precisely a documented strategy, as much as an approach that aims to help countries identify areas for improvement, motivate action to improve relative GCI rankings, raise the level of cybersecurity worldwide, help to identify and promote best practices and generally, to foster a global culture of cybersecurity.[33]

Risk management during the strategic planning process

As already mentioned before in brief, risk management is strongly correlated to the strategic concept.

Risk is a consideration in many strategy-setting processes. But risk is often evaluated primarily in relation to its potential effect on an already-determined strategy. In other words, the discussions focus on risks to the existing strategy: we have a strategy in place, so what could affect the relevance and viability of that strategy?

There is always risk to carrying out a strategy. An organisation must consider whether it has the capabilities (for example, people, processes, systems and information) to carry out the strategy. Lack of the necessary resources creates a risk to strategy achievement. Sometimes, the risks become important enough that an organisation may wish to revisit its strategy and consider revising it or selecting one with a more suitable risk profile.

There are two other aspects of risk that arise during the strategic planning process: The first, the possibility of misaligned strategy and objectives, relates to the risks that arise when a seemingly sound strategy doesn't align with the organization's mission, vision and core values. Such misalignment can result in tragic consequences, as evidenced by many examples of corporate failures in the past decades. The second, relates to the potential unintended consequences of a strategy chosen. A strategy viewed through one lens may seem appropriate, but there may be hidden risks that could have dire consequences to the organisation. The extra step in strategic planning of considering potential implications of unintended scenarios is a prudent step.

By definition, risk involves uncertainty and, therefore, no board can be certain that all three types of risk are comprehensively considered at the culmination of the strategic planning process. However, taking the time to consider the three ways risk can arise in strategic planning will increase the likelihood that the chosen strategies and objectives are successful.[33]

Information security risk management is the process of identifying, quantifying, and managing the information security risks that an organisation faces; it is a process aimed at obtaining an efficient balance between realizing opportunities for gains and minimizing vulnerabilities and losses. As an integral part of management practices and an essential element of good governance, security risk management needs to be recurrent seeking to support organizational improvement, performance and decision making.[34]

A risk management process comprises four key phases:

- Risk assessment
- Risk treatment
- Risk acceptance
- Risk communication

The evaluation of impact can only be qualitative. There are four levels of impact:

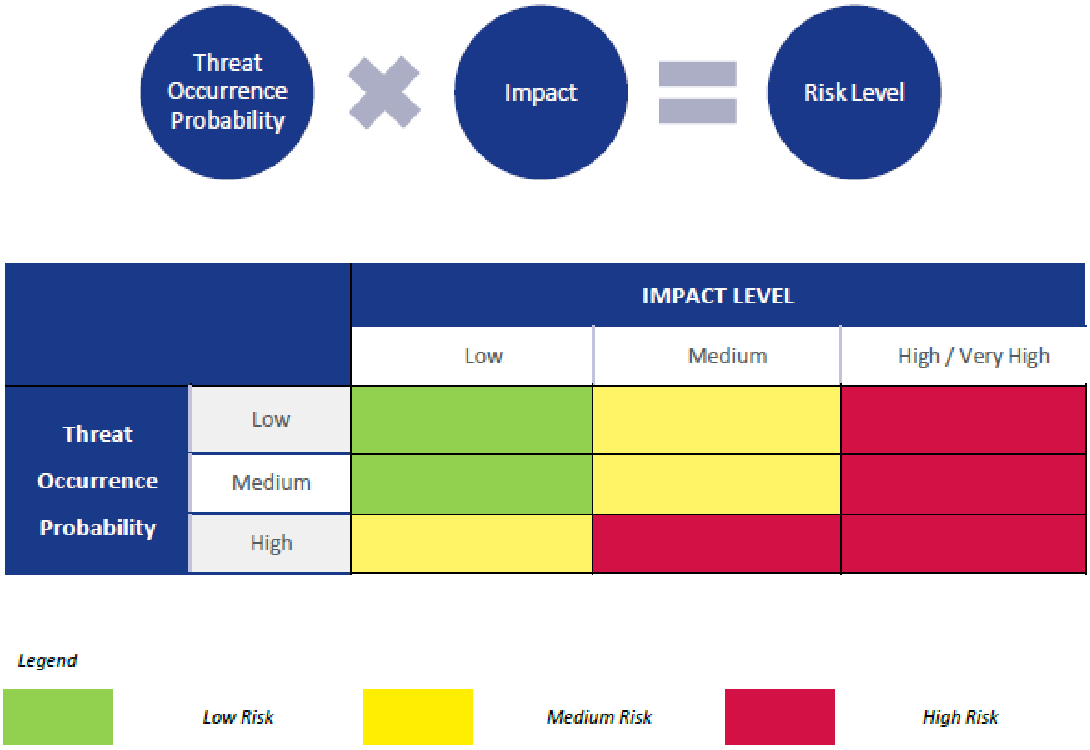
- Low
- Medium
- High
- Very high

The level of impact is always co-related to the consequences that a security incident may have to individuals or/and organizations.

It is also important to define the possible threats and evaluate their likelihood. There are three levels of threat occurrence probability:

- Low
- Medium
- High

The threat occurrence probability multiplied with the impact gives the risk level as a result, as designated by ENISA[35]:



		IMPACT LEVEL		
		Low	Medium	High / Very High
Threat Occurrence Probability	Low	🟩	🟨	🟥
	Medium	🟩	🟨	🟥
	High	🟨	🟥	🟥

Legend

🟩 *Low Risk* 🟨 *Medium Risk* 🟥 *High Risk*

Fig. 3.3: Risk level estimation by ENISA

Templates – Frameworks & Best Practices

NIST frameworks

Regarding available frameworks in correspondence, NIST (U.S. National Institute of Standards and Technology) provides a series of frameworks regarding cybersecurity and privacy, that prove to be quite useful in building a cybersecure environment by illustrating an appropriate corresponding strategy. NIST Frameworks can support the creation of a new cybersecurity/ privacy program or improvement of an existing one.

The goal of publishing the *Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* (Privacy Framework), has been to enable better privacy engineering practices that support privacy by design concepts and help organizations protect individuals' privacy. The Privacy Framework follows the structure of the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) to facilitate the use of both frameworks together.

The Privacy Framework[36] is intended to be widely usable by organizations of all sizes and agnostic to any particular technology, sector, law, or jurisdiction. Using a common approach—adaptable to any organization's role(s) in the data processing ecosystem—the Privacy Framework's purpose is to help organizations manage privacy risks by:

- Taking privacy into account as they design and deploy systems, products, and services that affect individuals;
- Communicating about their privacy practices; and
- Encouraging cross-organizational workforce collaboration—for example, among executives, legal, and information technology (IT)—through the development of Profiles, selection of Tiers, and achievement of outcomes.

The Cybersecurity Framework[37], on the other hand, since its release in 2014, has helped organizations to communicate and manage cybersecurity risk.[34] While managing cybersecurity risk contributes to managing privacy risk, it is not sufficient, as privacy risks can also arise by means unrelated to cybersecurity incidents, as illustrated below:

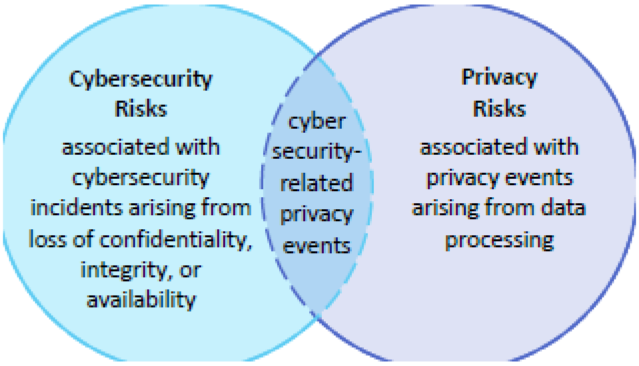

Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

Fig. 3.4: Cybersecurity and Privacy Risk Relationship

Said this, it is implied that both frameworks are useful to the same extent and may be taken into consideration for advice, interchangeably.

Having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks. Organizations may choose to prioritize and respond to cybersecurity and/or privacy risk in different ways, depending on the potential impact to individuals and resulting impacts to organizations. Response approaches include:

- *Mitigating the risk* (e.g., organizations may be able to apply technical and/or policy measures to the systems, products, or services that minimize the risk to an acceptable degree);
- *Transferring or sharing the risk* (e.g., contracts are a means of sharing or transferring risk to other organizations, privacy notices and consent mechanisms are a means of sharing risk with individuals);
- *Avoiding the risk* (e.g., organizations may determine that the risks outweigh the benefits, and forego or terminate the data processing); or
- *Accepting the risk* (e.g., organizations may determine that problems for individuals are minimal or unlikely to occur, therefore the benefits outweigh the risks, and it is not necessary to invest resources in mitigation).

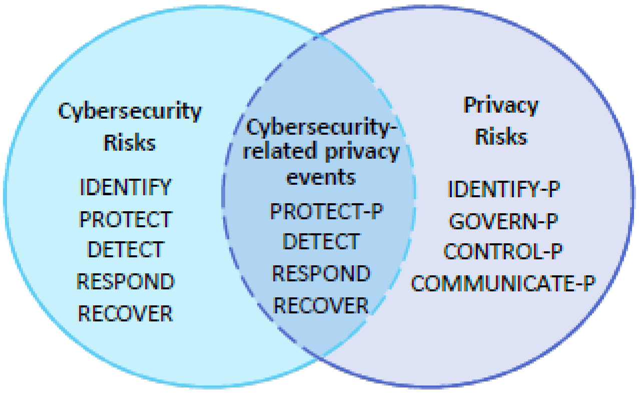


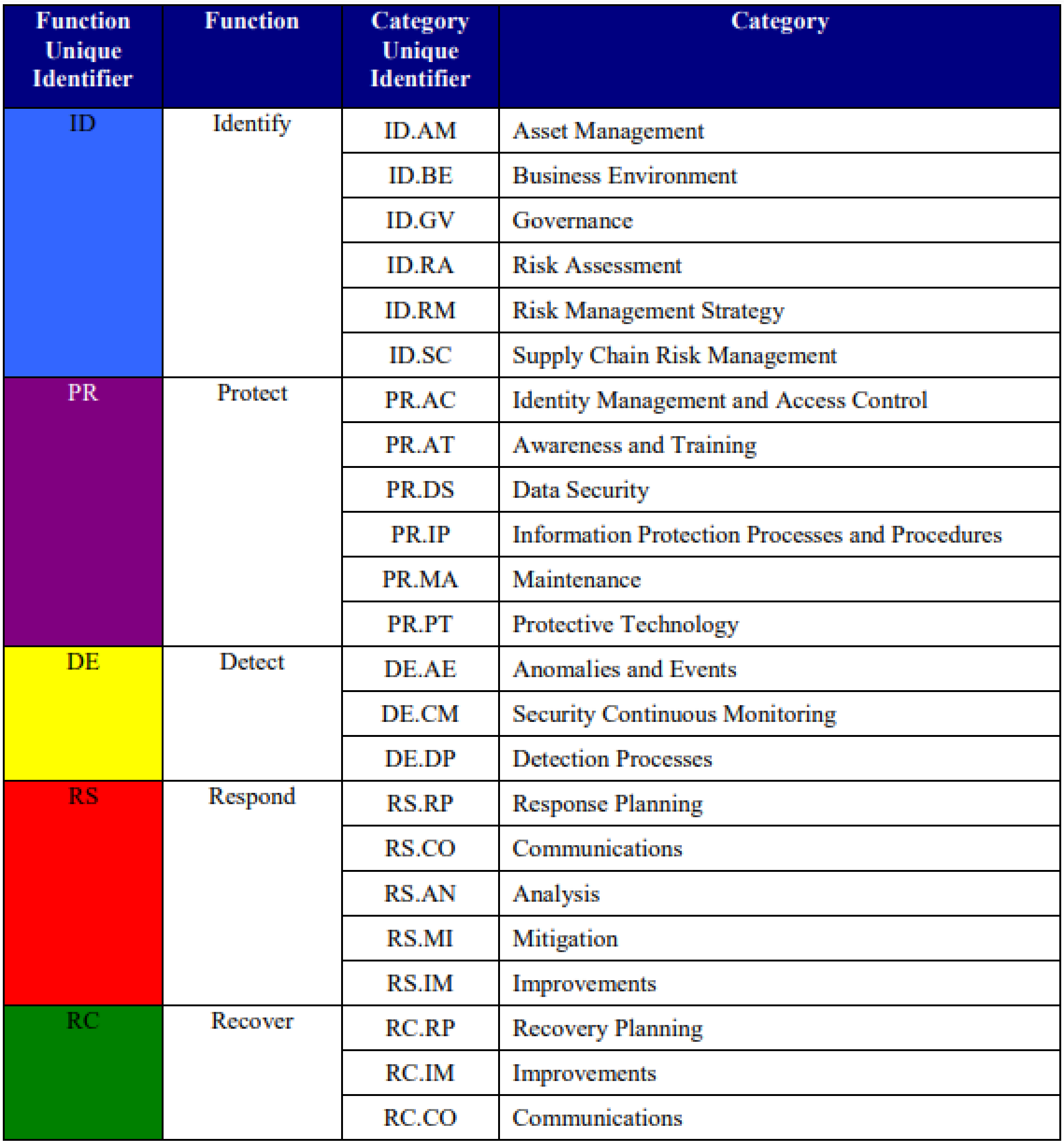
Fig. 3.5: NIST Framework's Functions to Manage Cybersecurity and Privacy Risks

In the figure above, the Functions that the Frameworks propose to manage risks are presented. As far as cybersecurity is concerned, these include the following functions/actions:

- *Identify* – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
- *Protect* – Develop and implement appropriate safeguards to ensure delivery of critical services
- *Detect* – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event
- *Respond* – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
- *Recover* – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The corresponding particular activities (*Categories*) for each Function are presented in the Table below:

Table 3.1: NIST Cybersecurity Framework Function and Category Unique Identifiers



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

In the risk management strategy phase, a key factor is an entity's role(s) in the data processing ecosystem, which can affect not only its legal obligations, but also the measures it may take to manage (privacy) risk. As depicted in Figure 10, the data processing ecosystem encompasses a range of entities and roles that may have complex, multi-directional relationships with each other and individuals. Complexity can increase when entities are supported by a chain of sub-entities; for example, service providers may be supported by a series of service providers, or manufacturers may have multiple component suppliers.

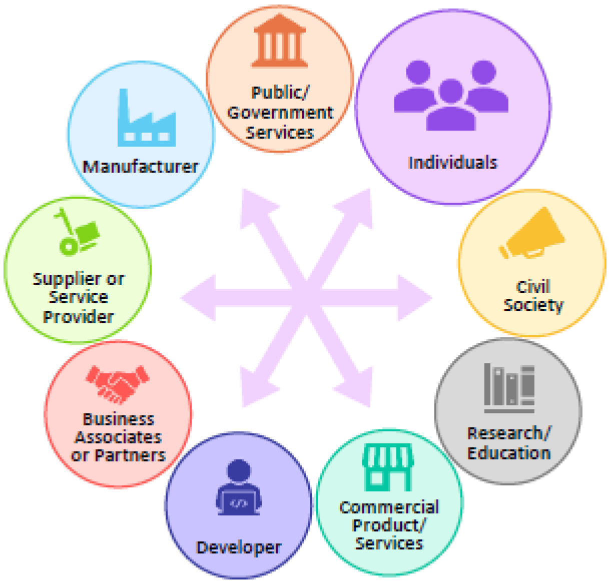

Public/ Government Services
Individuals
Manufacturer
Supplier or Service Provider
Civil Society
Business Associates or Partners
Research/ Education
Developer
Commercial Product/ Services

Fig. 3.6: Data Processing Ecosystem Relationships

Risk management practices include:

- *organizing the preparatory resources*: The appropriate resources facilitate informed decision-making about risks at all levels. Resources that build a foundation for better decision-making are risk management role assignments, taking into consideration that diverse and cross-functional teams are the most effective, enterprise risk management strategy establishment, key stakeholders' and corresponding requirements' definition as long as strategic control tools such as product design artifacts, data maps and data flow diagrams (depending on the case).

- *determining capabilities regarding privacy and cybersecurity:* An organization may use the privacy engineering objectives as a high-level prioritization tool. Systems, products, or services that are low in predictability, manageability, or disassociability may be a signal of increased privacy risk, and therefore merit a more comprehensive privacy risk assessment

- *defining requirements*: Given the applicable limits of an organization's resources, organizations prioritize the risks to facilitate communication about how to respond. Once an organization has determined which risks to mitigate, it can refine the privacy requirements and then select and implement controls (i.e., technical, physical, and/or policy safeguards) to meet the requirements. After implementation, an organization iteratively assesses the controls for their effectiveness in meeting the requirements and managing risk. In this way, an organization creates traceability between controls and requirements, and demonstrates accountability between its systems, products, and services and its organizational goals.

- *conducting risk assessments:* Conducting a risk assessment demands an appropriate risk model. Risk models define the risk factors to be assessed and the relationships among those factors. Although cybersecurity has a widely used risk model based on the risk factors of threats, vulnerabilities, likelihood, and impact, there is not one commonly accepted privacy risk model. NIST has developed a privacy risk model to calculate risk based on the likelihood of a problematic data action multiplied by the impact of a problematic data action.

- *monitoring change, where necessary*: Risk management is not a static process. It should always be monitored how changes in the environment take place – including new laws and regulations as long as emerging technologies – so as to implement corresponding changes to systems, products, services and processes affecting privacy and cybersecurity risk.

Regarding the coordination of the frameworks' implementation, it is described in the figure below:

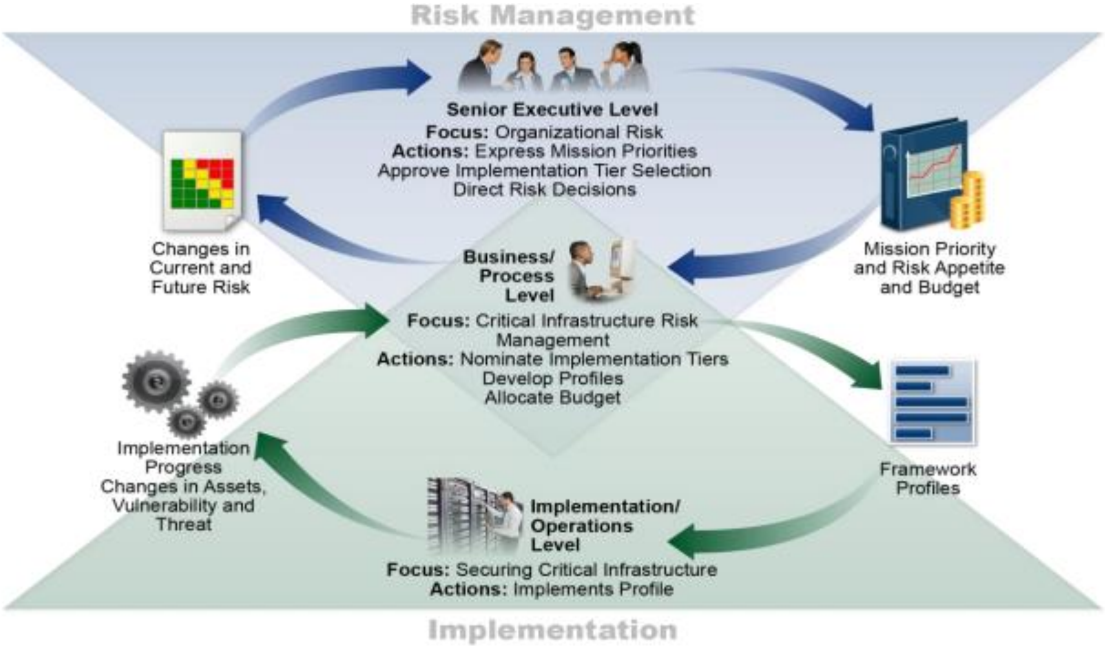

Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget
Implementation Progress
Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Fig. 3.7: Notional Information and Decision Flows within an Organization

Figure 3.7 describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile (customized solution design). The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact.[37]

As it can be assumed from this procedure, communication is a core process, not to be underestimated. Both communication and awareness training are essential parts of a cybersecurity strategy implementation. Therefore, amongst other technical and managerial measures the following should also be taken into consideration, summarizing the actions that are necessary for the scope of any relevant strategy:

- ✓ Governance of cybersecurity risk
- ✓ Approaches to identifying, authenticating, and authorizing individuals to access organizational assets and systems
- ✓ Awareness and training measures
- ✓ Anomalous activity detection and system and assets monitoring
- ✓ Response activities, including information sharing or other mitigation efforts.[34]

All the above, together with appropriate coordination and cooperation of entities in charge might lead to a promising future in terms of cyberspace safety and security.

NIST 800-37 Risk Management, as the name suggests, is a framework for identifying and addressing risks within any organization. It is mandated for DOD organizations (within the US Department of Defense), but anyone can use it. The Risk Management Framework is all about risk management being an integral part of the entire organization. Not just something a risk department handles or the cybersecurity department handles. But something that is integrated into policies, procedures, training in the entire organization. Information system boundaries, today's information systems tend to be quite complex. Responsibilities need to be detected and defined.

Simply identifying information system boundaries is one of the elementary steps in identifying and managing risks. Systems development life cycle. Whether we are developing a new app for a smart phone or a complex enterprise wide application risk management has to be baked in to the entire SDLC. Now, what that means in more practical term is simply this, risk management needs to begin when we are doing the design in the first place, when the requirements are being gathered. And then comes, design, development, deployment, maintenance.

And even before requirements, when we are first contemplating just general ideas, sitting around and brainstorming, we should think about risk management.

Security control allocation. Budget is not unlimited. So where are we going to allocate the most effort in security mitigating controls? Where is the highest risk? That is where focus should be set. So first, most risk sensitive areas will be tested. And then lesser risky. Because even though they get less security control allocation, they should not have zero allocation. All this risk management can be really informative, especially for ethical hacking.

The process is fairly straightforward.

We categorize the information systems. That starts with identifying what it is. A database? A domain controller?

And then we start categorizing its importance to the organization, the sensitivity level of information, etc.

Fig. 3.8: Notional Information and Decision Flows within an Organization

ISO/IEC 18045

Evaluation is an elementary part in this standard. We have an entire process where by we evaluate. What are we evaluating? Well, the things we are trying to protect. Existing security controls, risks, threats, everything gets evaluated. There is lots of input into that evaluation. Input can come from stakeholders, from various relevant standards like PCI-DSS or HIPAA, it can come from security consultants. As much input as possible is desired because without that, we may not be evaluating everything we should. Ultimately, we are going to output a report that is going to indicate our risk levels.

What are we protecting? How well is it protected? What are our threats? Are there recommendations to improve? Or are we sufficient as we are?

So this evaluation process is probably more detailed in this standard rather than in other standards. They all include some evaluation, but this standard puts a lot more focus on evaluation.

There are four major elements.

- Protection profile evaluation. A protection profile is what its name indicates, a profile that indicates what is being protected, the sensitivity of the data, existing controls, threats etc.
- Life cycle support. We must support risk management of protection throughout the entire life cycle, from conceptualization, requirements gathering, design, development. All the way through development, maintenance and retirement.
- Security target evaluations. There are specific targets of security levels that we attempt to achieve. Now, these have been determined through a combination of evaluation inputs, regulatory requirements, threat modeling, sensitivity of data will determine what security level we are targeting and whether we have reached it.
- Finally, assessment of vulnerabilities.

Now, this is a great place to point out that these various models, tools and standards are not mutually exclusive. We could incorporate CVSS here to do a vulnerability assessment. We could incorporate CIA triangle or McCumber cube throughout all of this.

So we bring it altogether. Free to mix and match these different thing to obtain the most robust risk management process possible, but this standard is one that might inform the whole process.

COBIT

COBIT (Control Objectives for Information and Related Technology) helps organisations meet business challenges in the areas of regulatory compliance, risk management and aligning IT strategy with organisational goals.

COBIT 5

COBIT 5 is based on five principles that are essential for the effective management and governance of enterprise IT:

- Principle 1: Meeting stakeholder needs
- Principle 2: Covering the enterprise end to end
- Principle 3: Applying a single integrated framework
- Principle 4: Enabling a holistic approach
- Principle 5: Separating governance from management

These five principles enable an organisation to build a holistic framework for the governance and management of IT that is built on seven 'enablers':

- People, policies and frameworks
- Processes
- Organisational structures
- Culture, ethics and behaviour
- Information
- Services, infrastructure and applications
- People, skills and competencies

Together, the principles and enablers allow an organisation to align its IT investments with its objectives to realise the value of those investments.

The COBIT 5 framework can help organisations of all sizes:

- Improve and maintain high-quality information to support business decisions;
- Use IT effectively to achieve business goals;
- Use technology to promote operational excellence;
- Ensure IT risk is managed effectively;
- Ensure organisations realise the value of their investments in IT; and
- Achieve compliance with laws, regulations and contractual agreements.

COBIT 5 has been designed with integration at its heart. It is aligned with numerous best-practice frameworks and standards, such as ITIL®, ISO 20000 and ISO 27001. It may be best to take an integrated approach when implementing an IT governance framework, using parts of several different frameworks and standards to deliver the results needed. In Pragmatic Application of Service Management, Suzanne Van Hove and Mark Thomas provide an approach to integrating COBIT 5, ITIL and ISO 20000 that delivers better return on investment and alignment of IT with organisational objectives.[38]

COBIT '19

COBIT 2019 is an updated version of COBIT 5. It is built on the solid foundation of its predecessor while integrating the latest developments affecting enterprise information and technology.

In addition to the updates we will detail in a bit, the latest framework offers certificate candidates implementation resources, guidance and insights, as well as training opportunities. It further positions businesses for future success through:

- Coverage of the critical elements to an enterprise, i.e. data, projects and compliance
- An open-source model which allows the global governance community to propose enhancements for updating the framework
- Flexible framework implementation for either specific problem solving or enterprise-wide adoption

The release of COBIT 2019 was necessary as COBIT 5 was introduced more than seven years ago in 2012. Since then, the trends, technologies, and security needs for organisations have dramatically changed. Organisations which fail to adapt with time become obsolete easily. This is especially true when it comes to the evolution of IT as it plays a vital role in almost all the processes across a business.

Upgrading COBIT was also necessary to ensure better alignment with global standards, frameworks, and best practices such as ITIL®, CMMI®, and TOGAF®. In this context, alignment means not contradicting any guidance or copying the contents of related standards. That way, COBIT can maintain its positioning as an umbrella framework.

According to ISACA, COBIT 2019 introduces new concepts, adds updates to enhance the relevancy of COBIT, rolls out an 'open-source' model for global governance, and offers new guidance and tools for a best-fit governance system.

COBIT 2019 has classified principles into two areas: Governance Systems Principles and Governance Framework Principles. COBIT 5 defined five principles that are now part of the Governance System Principles.

COBIT 2019 introduces 11 design factors which are broadly categorised as:

- Contextual (i.e. outside the control of the enterprise)
- Strategic (reflect the decisions the enterprise makes)
- Tactical (based on implementation choices regarding resourcing models, IT methods, and technology adoption choices).

With these design factors, organisations can tailor their governance systems to realise the most value.

"Focus areas" are part of the new COBIT® iteration. These describe governance topics and issues which can be addressed by management or governance objectives. Some examples of these areas include small and medium enterprises, cybersecurity, and cloud computing.

An interesting fact on focus areas is that there is a virtually unlimited number of these concepts. Focus areas will be added and changed based on trends, research, and feedback. This is why COBIT has become an open-ended model.

Demystifying the Cyber Risk Management Process

Enterprise Risk Management

First and foremost, for long of the twentieth century, far too many firms and other types of organizations had any formal idea of "risk management." As interest in corporate risk management developed in the 1990s, this began to alter. Even back then, however, risk analysis was limited to the type of insurance-related risk analysis mentioned above, which was tied to specific types of activity. The limitations of this vision became apparent near the end of the 1990s, when businesses were buffeted by a slew of changes that drastically transformed the environment in which they operated and thrived: economic booms and busts, more competition, and a dramatically changed technological landscape, including the Internet

Real estate markets, credit institutes, rating agencies, and investors became increasingly aware of the various types of risks to which businesses were exposed, and demanded that they implement improved internal controls to pro-actively identify and manage changes that could affect them – not only to avoid negative consequences, but also to use change to their strategic advantage.

As a result of this realization, a strategy was developed that views risk management as an inherent component of the overall competitive and strategic framework within which a company functions in accordance with standard entrepreneurial practice. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) study "Enterprise Risk Management - Integrating with Strategy and Performance" reflects this new approach. In this research, Enterprise Risk Management is defined as "... the culture, capabilities, and practices that businesses rely on to manage risk in creating, conserving, and realizing value, integrated with strategy-setting and performance."

As a result, the COSO model effectively promotes the concept of integrated and comprehensive management of all types of business risk in order to arrive at a global risk profile. This gives it a strategic dimension, allowing it to have a favorable impact on the entire process of creating value for the organization.

The Risk Management Process

Let's look at the aspects of a risk analysis and management process now that we've seen the overall backdrop of cyber risk management within the organization. They entail the following at their most basic level:

- Identify risks
- Assess risks
- Identify possible mitigation measures
- Decide what to do about the residual risk

Let's take a look at each one separately:

Identify Risks. The risks to face will always be determined by what we are seeking to safeguard – assets. A health insurer may recognize smoking as a hazard to our health if we are trying to protect our health. In case of a company attempting to defend its revenues, competition can be seen as a threat. The next step is to figure out how to identify weaknesses to the risks we are up to against, such as weak passwords. Identifying all of the dangers to face is a difficult task that demands rigorous, organized investigation.

Assess risks. A health insurer may recognize smoking as a risk factor, but it must also determine (evaluate) the severity of the risk: what would the consequences of developing lung disease be? However, the chance of an incidence is also important: some very efficient medicines can have major adverse effects, but these are known to be quite rare. Risk assessment is all about striking a balance between impact and likelihood.

Identify possible mitigation measures. What can be done once the risks have been identified? There are two types of measurements. Some hazards, such as having the most up-to-date technology, can be minimized with technical solutions. Others can be mitigated by following best practices, such as not smoking and otherwise living a healthy lifestyle. However, some risks are unavoidable. The term "residual risk" refers to this crucial aspect. The risk of business failure is always present, and there isn't much to do to avoid it. It's a necessary aspect of doing business.

Decide what to do about the residual risk. What to do with the danger that remains after all other options are exhausted? That depends on how concerned one is. It's possible to just accept it. If entering a new market with the risk of failure as well as the possibility of extraordinary success, it can be determined that the upside "risk" outweighs the downside "risk" (in an integrated enterprise risk management context, risk is managed also for competitive advantage, not just for avoiding problems).

Insurance is all about covering residual risk – After all viable mitigation measures have been identified, it is the "last line of defense." Even yet, the quantity of insurance purchases will be determined by how much we are willing to accept the residual risk. However, how do insurance companies determine how much to charge? Years of experience have helped well-established insurers create reliable estimates. Actuarial tables are used by life insurance companies. Accident statistics are available from auto insurers. Hospitalization costs are well-known to health insurance.

Those are the four fundamental steps in every risk management process in which insurance plays a role. Let's take a look at how a cybersecurity risk management process might work.

The Cyber Security Risk Management Process

In recent years, organizations have come to realize that cybersecurity risk management must be integrated into the overall enterprise risk management context.

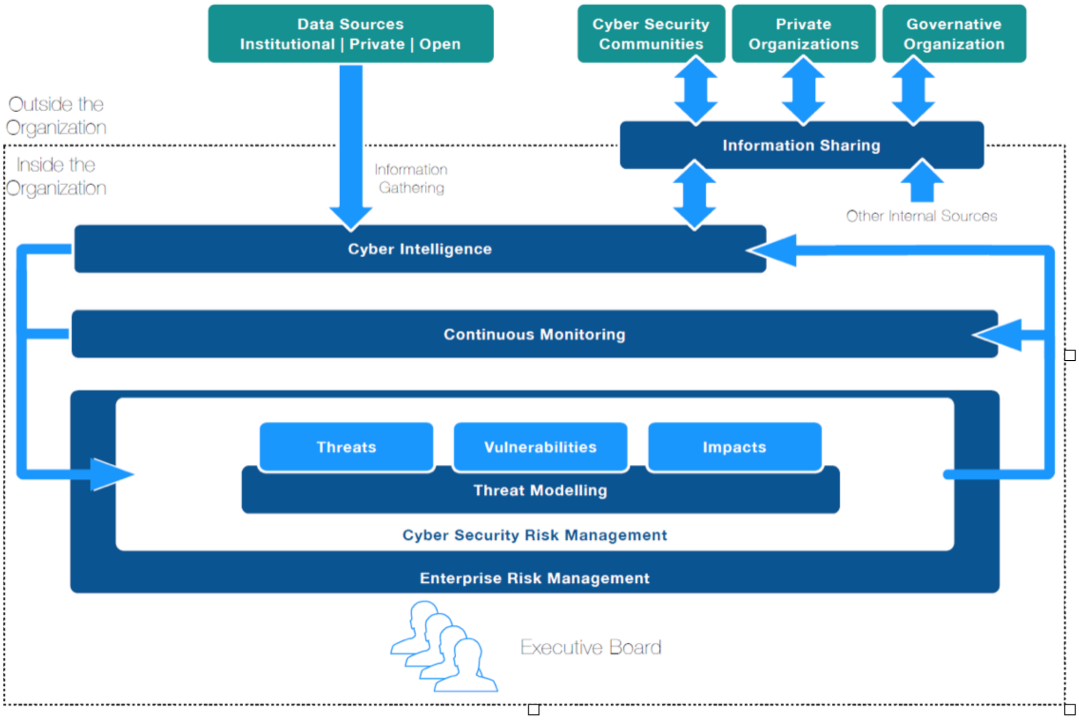


Fig.3.8: The Cybersecurity Risk Management Process Roadmap

A good example of this is illustrated by the Italian National Cybersecurity Framework, shown in the figure. Within this framework, let us see how the four essential steps of risk management are implemented for cybersecurity.

Identify cybersecurity risks. As previously stated, established industries such as healthcare and the automobile industry have years of combined experience in identifying and classifying hazards. However, because cybersecurity is a relatively new field, most of what is depicted

in the diagram relates to this issue. Information sharing is common in various industries (for example, statistics on automobile accidents), but it is especially crucial in cybersecurity because there is so much that is new and continually growing.

Assess cybersecurity risks. There are also organizations in the community working to develop clear criteria for defining and evaluating cybersecurity threats. To get at more specific estimations of the impact and likelihood of a cyber incident, it is necessary to learn what the costs and frequency of occurrences have been for others in the community.

Identify possible cybersecurity risk mitigation measures. There are two types of mitigation measures: technology and best practices, as we learnt before. The latest encryption devices, the greatest firewalls, and other technological steps to combat cybersecurity dangers could be used. Best practices, on the other hand, are just as important – and frequently the only measurements available. This might involve providing employees with a good cybersecurity training program to help them avoid harmful practices like using easy passwords. They could include policies and processes for establishing and implementing supply chain security in the company and its supply chain.

Estimating how much cyber danger someone is still exposed to after having taken all the possible precautions is difficult. An important feature here is community information sharing on occurrences that may still occur despite installed controls and best practices. This is where continuous monitoring comes into play, providing a more precise view of the organization's cyber risk exposure at any given point in time.

Decide what to do about residual cyber risk. Depending on the organization's objectives, it may choose to address residual cyber risk in a variety of ways. As previously said, a good assessment of the cost of losses caused by cyber incidents is a vital component in the decision-making process. Some, such as lost operational time, may be quite simple to assess. However, other expenses, such as "reputation harm," may be difficult to quantify and may vary depending on the individual company sector. Deep expertise of specific business sectors may be required to make a credible estimate, as will a thorough understanding of the always changing cyber incident landscape.

Cyber security insurance is one of most popular solutions. This form of insurance will become more appealing as assessments of the possible damage from cyber catastrophes grow more exact. The nature of a cybersecurity risk management approach as described above should make it evident that going it alone is difficult. The industry is simply too young.

Cybersecurity Posture

An enterprise’s security posture refers to the overall status of an organization’s cybersecurity readiness.

With tens of thousands of assets in every enterprise and each susceptible to a myriad of attack vectors, there are practically unlimited permutations and combinations in which an organization can be breached. With the sharp increase in attack surface size, cybersecurity teams have a lot of complexity to deal with: vulnerability management, security controls, detecting attacks, incidence response, recovery, compliance, reporting and much more. The first line of defense against the adversary is a good security posture.

What is cybersecurity posture?

Security posture is a measure of:

- The level of visibility people have into their organization’s asset inventory and attack surface
- The controls and processes in place to protect the enterprise from cyber-attacks
- The ability to detect and contain attacks

- The ability to react to and recover from security events
- The level of automation in the established security program

A conceptual picture of the various elements of an organization's security posture is shown in the figure below:

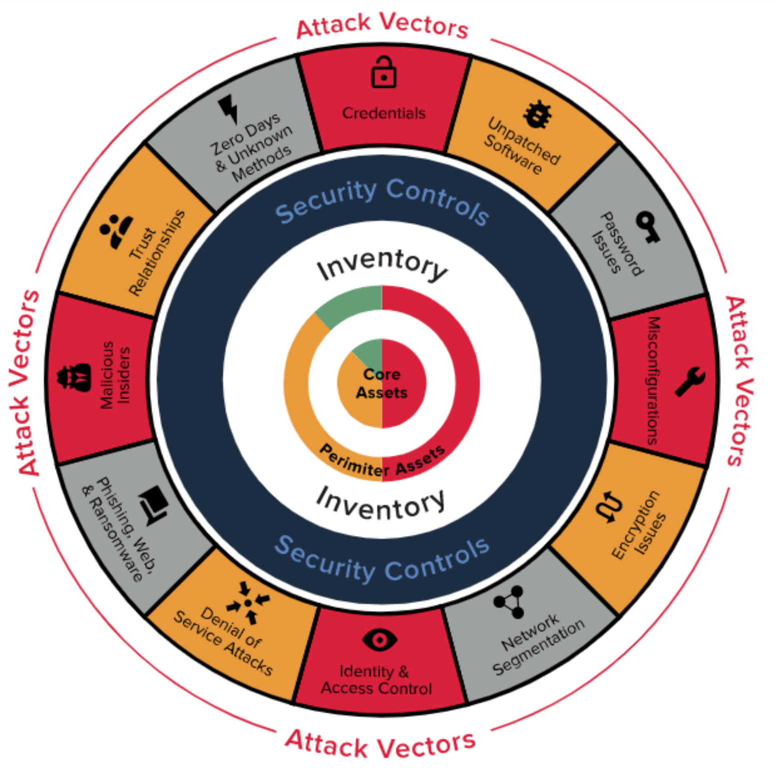


Fig.3.9: Cyber Attack Vectors

Inventory of IT Assets

We can't protect what we don't know about. At the center of the security posture is an accurate inventory of all assets. This includes all on-prem, cloud, mobile, and 3rd party assets; managed or unmanaged assets; applications and infrastructure, catalogued based on geographic location, and whether they are Internet facing (Perimeter assets) or not (Core assets). It is also very important to understand the business criticality of each asset, as this is an important component of calculating breach risk.

Security Controls and Effectiveness

Surrounding this central core is an enumeration of the cybersecurity controls that has been deployed. Some controls, such as firewalls and endpoint are deployed with a goal of preventing attacks. Others, such as intrusion detection systems (IDSes) and SIEMs are involved in detecting attacks that get past protective controls. Additional tools and processes are needed for response and recovery from such attacks. It is important to not just be able to enumerate controls, but also have an understanding of the effectiveness of each control in reducing cyber risk.

Attack Vectors & Surface

The next ring lists the various attack vectors. Attack vectors are the methods that adversaries use to breach or infiltrate the network. Attack vectors take many different forms, ranging from malware and ransomware, to man-in-the-middle attacks, compromised credentials, and phishing. Some attack vectors target weaknesses in the security and overall infrastructure, others target the human users that have access to the network.

And keep in mind that risk extends beyond unpatched software vulnerabilities (CVEs). The ability to monitor assets in risk areas such as unpatched software, password issues, misconfigurations, encryption issues, phishing, web and ransomware, denial of service attacks and many others is the mainstay of the organization's security posture.

The stronger and more resilient the security posture, the lower the cyber risk and greater the cyber-resilience.

Therefore, understanding the full scope of security posture and correctly prioritizing areas of relevant risk is essential to protecting the organization against breaches.

The combination of asset inventory and attack vectors makes up the attack surface. The attack surface is represented by all of the ways by which an attacker can attempt to gain unauthorized to any of the organization's assets using any breach method.

Automation of Security Posture

A critical aspect of security posture is the degree of automation. Attackers are constantly probing defenses using automated techniques. 100s of new vulnerabilities are disclosed every month. It is not enough to simply be able to list an inventory, fix vulnerabilities and review controls from time to time. Security posture management needs to be automated in order to stay ahead of any adversary.

How to assess security posture

Security posture assessment is the first step in understanding where an organization is in its cybersecurity maturity journey and the cyber breach risk. The following questions need to be answered:

- How secure is the organization?
- Do we have the right cybersecurity strategy?
- How good are our security controls?
- Can we accurately measure breach risk and cyber-resilience?
- How vulnerable are we to potential breaches and attacks?
- How effective is our vulnerability management program?
- How can we scorecard and benchmark different risk owners in the organization?
- What is the best way to discuss the organization's security posture with the board of directors?

Assessing cybersecurity postures can take place in 3 steps:

Step 1. Get an accurate IT asset Inventory

The first step in security posture assessment is getting a comprehensive inventory of all assets. An asset is any device, application, service, or cloud instance that has access to enterprise network or data.

An accurate and up to date count of all hardware, software, and network elements in enterprise is necessary. However, just being aware of an asset isn't sufficient. Detailed information about each asset which can help in the understanding of the risk associated with the asset is needed. This involves:

- Categorizing assets by type of asset, sub-type, role, Internet-facing or not, and location
- In-depth information like software and hardware details, status of open ports, user accounts, roles, and services linked to that asset
- Determining the business criticality of each asset
- Ensuring that all assets are running properly licensed and updated software while adhering to overall security policy
- Continuously monitoring them to get a real time picture of their risk profile
- Creating triggered actions whenever an asset deviates from enterprise security policy
- Deciding which assets should be decommissioned if no longer updated or being used

Getting an accurate asset inventory is foundational to security posture. The ability to track and audit the inventory is a baseline requirement for most security standards, including the CIS Top 20, HIPAA, and PCI. Having an accurate, up-to-date asset inventory also ensures that the company can keep track of the type and age of hardware in use. By keeping track of this information, it becomes easier to identify technology gaps and refresh cycles. As systems begin to age, and are no longer supported by the manufacturer, they present a security risk to the organization as a whole. Unsupported software that no longer receives updates from the manufacturer brings the risk of not being monitored for new vulnerabilities and implementation of patches.

Step 2. Map the attack surface

The second step in security posture assessment is mapping an attack surface. The attack surface is represented by all of the points on the network where an adversary can attempt to gain entry to the organization's information systems.

The x-y plot in the figure below represents the attack surface. In a typical breach, the adversary uses some point on this attack surface to compromise an (Internet facing) asset. Other points are then used to move laterally across the enterprise to some valuable asset, compromise that asset, and then exfiltrate data or do some damage.

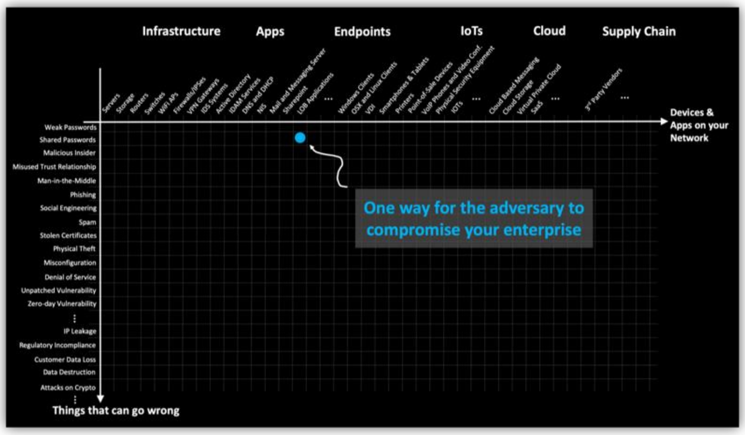


Fig.3.10: Attack Surface Mapping

For a medium to large sized enterprise, the attack surface can be gigantic. Hundreds of thousands of assets potentially targeted by hundreds of attack vectors can mean that the attack surface is made up of tens of millions to hundreds of billions of data points that must be monitored at all times.

Step 3. Understanding cyber risk

The final step in security posture assessment is understanding cyber risk. Cyber risk has an inverse relationship with security posture. As the security posture becomes stronger, cyber risk decreases.

Mathematically, risk is defined as the probability of a loss event (likelihood) multiplied by the magnitude of loss resulting from that loss event (impact). Cyber risk is the probability of exposure or potential loss resulting from a cyberattack or data breach.

An accurate cyber risk calculation needs to consider 5 factors as show in the figure below:

$$\text{risk} = \underbrace{\text{likelihood}}_{\text{likelihood} = f(\textit{vulnerabilities, exposure, threats, mitigating controls})} \times \overbrace{\text{impact}}^{\text{impact} = g(\textit{business criticality})}$$

Fig.3.11:Cyber Risk Calculation Factors & Formula

For each point of the attack surface picture of the figure above, we must consider:

- The severity of a known vulnerability relevant to the asset. e.g., CVSS score of an open CVE on the asset
- Threat level. Is the attack method currently being exploited in the wild by attackers.
- Exposure/usage to the vulnerability. Based on where the asset is deployed and used, vulnerabilities are exploitable or not.
- Risk-negating effect of any security controls in place
- Business criticality of the asset.

This calculation needs to be performed for all points of the attack surface. This result in an accurate picture of where the cyber-risk is and helps prioritize risk mitigation actions while avoiding busy work fixing low risk issues.

How to improve security posture

To improve security posture, the following steps are suggested:

- Automate real-time inventory for all enterprise assets
- Define risk ownership hierarchy and assign owners.
- Continuously monitor assets for vulnerabilities across a broad range of attack vectors like unpatched software, phishing, misconfigurations, password issues etc., evaluate these vulnerabilities based on risk, and dispatch to owners for supervised automatic mitigation.
- Continuously review gaps in security controls and make appropriate changes
- Define metrics and target SLAs for visibility, resolution of vulnerabilities and risk issues, and security control effectiveness; and continually measure and track them

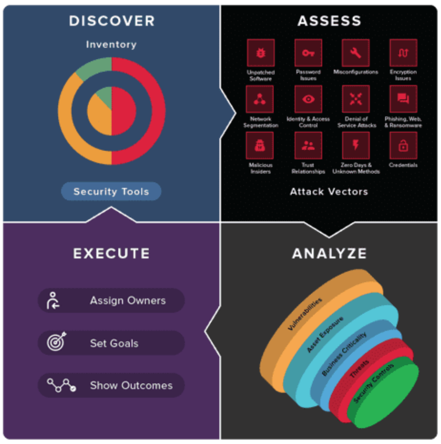


Fig.3.12: Cybersecurity Posture Assessment Key Phases

Step 2 above is key to improving security posture. It is critical that risk ownership organization chart be defined and actively managed. Most risk mitigation tasks need to be executed or approved by individuals who are not part of the Infosec organization. It is important to provide actionable dashboards and reports to each risk owner that contain information about the security issues that they own, associated risk and risk mitigation options.

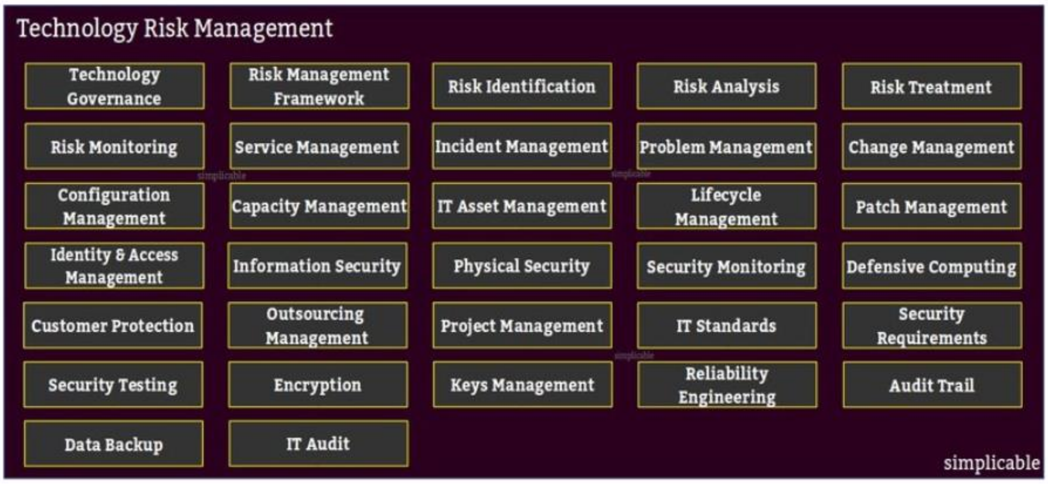
With a well-understood risk ownership hierarchy, it is also feasible to compare and scorecard owners and drive them to do their part in maintaining a good security posture.

Once the organization gains visibility into security posture, the security program governance will need to set and periodically adjust security posture goals. There needs to be a continuous monitoring of the attack surface in the context of the ever-evolving cyber threat landscape as well as automated processes in place for maintaining good cybersecurity posture.

Security posture is an organization's overall cybersecurity strength and resilience in relation to cyber-threats. The complexity and variety of modern cyber-attacks makes analyzing and improving security posture quite challenging. As organizations move away from last generation security strategies and fragmented solutions, they are transitioning to an automated architecture for managing security posture that can protect against a fast-changing threat landscape.[39]

Technology Risk Management

Technology risk management is the direction and control of an organization to manage technology risk. This includes a standard risk management process of identifying and treating risk. Technology risk management also involves oversight of technology development and operations in areas such as information security, reliability engineering and service management. The following are common elements of technology risk management [40]:



Technology Risk Management

Technology Governance	Risk Management Framework	Risk Identification	Risk Analysis	Risk Treatment
Risk Monitoring	Service Management	Incident Management	Problem Management	Change Management
Configuration Management	Capacity Management	IT Asset Management	Lifecycle Management	Patch Management
Identity & Access Management	Information Security	Physical Security	Security Monitoring	Defensive Computing
Customer Protection	Outsourcing Management	Project Management	IT Standards	Security Requirements
Security Testing	Encryption	Keys Management	Reliability Engineering	Audit Trail
Data Backup	IT Audit			

simplicable

Fig.3.13: Technology Risk Management Elements

- ✓ Technology Governance

The board of directors and senior management of an organization are accountable for technology risk and are expected to direct and monitor risk management efforts.

✓ Risk Management Framework

Implementing structures, roles e& responsibilities, practices and processes for controlling technology risks.

✓ Risk identification

The continuous process of identifying technology risks.

✓ Risk analysis

Developing an understanding of the context, impact and probability of each identified risk.

✓ Risk treatment

Developing and implementing treatments for identified risks. Common treatments include risk avoidance, mitigation, transfer, sharing and acceptance.

✓ Risk monitoring

Monitoring and reporting of risk.

✓ Service management

The structures, processes and tools for operating technology services.

✓ Incident management

Handling failures that occur. A tactical process that seeks to quickly minimize impact.

✓ Problem management

The process of identifying and addressing the root cause of failures. A strategic process that learns from failure to drive improvement.

✓ Change management

Controlling change to technology environments.

✓ Configuration management

Ensuring that changes to technology are traceable.

✓ Capacity management

The process of efficiently scaling technology to meet business demands.

✓ IT asset management

Control of technology assets including financial, contractual and lifecycle considerations.

✓ Lifecycle management

Identifying and managing risks related to aging technologies and equipment. For example, planning to replace software that is no longer supported by its vendor.

✓ Patch management

Tracking and implementing patches, particularly security patches.

✓ Identity & access management

Secure processes for granting access to technology and information resources include appropriate separation of concerns.

- ✓ Information security

The defense of information and information systems from unauthorized access, use, disclosure, modification or disruption. Includes system security, data loss prevention, technology infrastructure security and network security.

- ✓ Physical security

Physically securing information resources and related facilities such as offices and data centers.

- ✓ Security monitoring

Security monitoring of platforms, hosts, networks, systems, applications and databases. Large organizations may have a dedicated information security operations center for this purpose.

- ✓ Defensive computing

Training all employees to be aware of defensive computing practices.

- ✓ Customer protection

Extending security efforts to customers. For example, helping customers to secure clients such as web browsers that are used to access the organization's services.

- ✓ Outsourcing management

Managing technology risks related to external partners. This includes due diligence in selecting partners and monitoring their performance.

- ✓ Project management

Controlled planning and execution of technology projects.

- ✓ IT standards

Developing and operating technology resources according to standard policies and practices such as secure coding guidelines.

- ✓ Security requirements

Developing and implementing security requirements for technology projects.

- ✓ Security testing

Code reviews and security testing including penetration tests.

- ✓ Encryption

Adequate encryption of sensitive information in transit, use and storage.

- ✓ Key management

The process of securing encryption keys.

- ✓ Reliability engineering

Designing platforms, systems, applications, infrastructure and facilities for resilience.

- ✓ Audit trail

Ensuring that technology operations and events are recorded with sufficient detail to be reconstructed for the purposes of investigation and audit.

- ✓ Data backup

Secure and resilient processes for backing up data.

- ✓ IT audit

Periodic or ongoing evaluations of technology controls.

Cyber Insurance

Insurance is all about reducing or eliminating a perceived risk. When we get health insurance, we are reducing the risk of being ill. When we purchase automobile insurance, we are reducing the chances of being involved in an accident. Cyber insurance is no different: it is about controlling the risk of a cybersecurity-related incident.

However, there is one question that remains unanswered: *how much insurance is required?*

A little consideration should reveal that the amount of insurance required is proportional to the danger to face. Insurance firms use a risk analysis technique that they are always refining to try to evaluate risk. They are aware of the fundamental factors that influence risk.

So, the first thing to do is a cyber security risk assessment in order to determine how much and what type of cyber insurance the company needs.

The vast majority of businesses will rely on IT systems to store and process valuable operational data and customer information. IT systems are vulnerable to cyber security risks such as scams, fraud, information theft and malware or virus attacks. A business is responsible for its own cyber security but in the event of a cyber attack the right insurance policy that covers cyber liabilities may help business recover.

Cyber insurance or cyber liability insurance is a type of insurance cover that aims to protect businesses from IT threats and covers client once their systems or data has been lost, damaged or stolen in the event of a cyber attack.

Most cyber insurance policies generally cover first party and third party costs relating to a cyber-attack. [41]

- ➢ First-party insurance covers the business's own assets. This may include:
  - Loss or damage to digital assets such as data or software programmes
  - Business interruption from network downtime
  - Cyber exhortation where third parties threaten to damage or release data if money is not paid to them

    - Customer notification expenses when there is a legal or regulatory requirement to notify them of a security or privacy breach
    - Reputational damage arising from a breach of data that results in loss of intellectual property or customers
    - Theft of money or digital assets through theft of equipment or electronic theft.
- Third-party insurance covers the assets of others, typically customers. This may include:
    - Security and privacy breaches, and the investigation, defense costs and civil damages associated with them
    - Multi-media liability, to cover investigation, defense costs and civil damages arising from defamation, breach of privacy or negligence in publication in electronic or print media
    - Loss of third-party data, including payment of compensation to customers for denial of access, and failure of software or systems [42]

If a business uses, sends or stores electronic data it could be vulnerable to cyber crime. Cyber insurance could help with financial and reputational costs if the business is ever the victim of a cyber attack.

As well as putting adequate insurance in place, it is important for organizations to manage their own cyber risks as a business. This includes:

1. Evaluating first and third party risks associated with the IT systems and networks in the business
2. Assessing the potential events that could cause first or third party risks to 84aterialize
3. Analysing the controls that are currently in place and whether they need further improvement [43]

Cyber Risk Report 2021 by AON

Survey Context

In 2020, the speed of digital transformation exceeded the speed of security across industries, with businesses giving up ground to keep the lights on and maintain momentum. The majority of cyber dangers that businesses face today aren't new — linked gadgets, ransomware, and insider risk will all continue to e -19, on the other hand, brought about a 180-degree revolution in the nature of business and enormously increased cyber risk. This was evidenced by an increase in the frequency and intensity of ransomware cases, as well as weaknesses in supply chains and support vendors.

Mimecast, SolarWinds, Accellion, and Microsoft Exchange were among the successful cyber attacks that surfaced at the end of 2020 and the beginning of 2021, highlighting vulnerabilities connected with interacting with third-parties. As activity increased 400 percent from the first quarter of 2018 to the fourth quarter of 2020, ransomware became a headline risk for insurers and insureds alike. Underwriters who saw their cyber insurance portfolios lose money primarily due to ransomware saw the crucial need to better evaluate cyber insurance and charge a higher premium.

The stakes are high and the difficulties are numerous. Global organizations are not in the midst of digital transformation, which suggests that there is a beginning, middle, and finish to the process. Organizations are undergoing a digital transformation, and new dangers emerge on a daily basis.

Clients are always asking themselves, "*How can we make informed decisions around our cyber budget to accommodate evolving business models while protecting our people, clients, partners, and balance sheet?*"

Aon's 2021 *Cyber Security Risk Report: Balancing Risk and Opportunity Through Better Decisions*, is a yearly examination of the state of cyber risk. This research focuses on four major risks today:

- Navigate new exposures,
- Know your partners,
- Focus on controls, and
- Perfect the basics, and concludes with a discussion on developing risks.

The report intends to assist firms in assessing their cyber risk maturity and making smarter corporate risk decisions by utilizing our cutting-edge data, analytics, and expert insights.

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. It has 50,000 colleagues in 120 countries empowering results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Aon's Cyber Quotient Evaluation (CyQu), a comprehensive risk assessment that evaluates cyber risk maturity across nine crucial domains, is new this year. CyQu assists businesses in comprehending cyber dangers from both a commercial and information security standpoint. According to the 2020 data, firms across many geographies, industries, and revenue bands are performing below baseline, with only a minimum degree of cyber maturity and preparation.

As an example, only two out of every five businesses claim to be equipped to deal with new risks posed by rapid digital change. Worse yet, only 17% of firms claim to have effective application security protections in place. When it comes to third-party risk, only 21% of companies say they have baseline controls in place to monitor essential suppliers and vendors. Overall, the CyQu data indicates that cyber security risk management processes and technologies are not institutionalized, and risk is managed haphazardly and reactively.

Regulatory agencies, insurers, partners, and customers will be scrutinizing enterprises in 2021 and beyond, and organizations will have a lot of work ahead of them. This study will assist firms in empowering results and guiding them as they transition to managing cyber risk as an enterprise risk.

Methodology

Aon's Cyber Quotient Evaluation (CyQu), an online cyber risk assessment, provided data on security performance trends. Data was submitted from 996 organizations from North America, Europe, the Middle East & Africa, and Asia-Pacific, representing 20 industry groups. More than

111,552 data points were collected, and security performance trends were organized using the CyQu methodology's nine security domains and 35 essential control areas.

COVID-19 joined the C-suite in 2020, leading change as organizations were forced to rapidly set up remote work environments and enable digital customer experiences.

In the name of survival, any concept of a planned and strategic digital agenda was cast aside. Change appears to be unavoidable, and it is. Organizations are undergoing a digital transformation. In 2021, the continuing push for innovation, such as the Internet of Things (IoT), Internet of Bodies (IoB), and Smart City programs, will increase cyber risk. In this context, businesses must assess the anticipated benefits of a digital agenda against the potential risk posed by adopting new technology or business models.

It is critical to identify cyber risks and threats as part of an enterprise-wide approach, mitigate risks as appropriate through best cyber security practices, prepare and be ready for incidents, and consider which part of the risk to transfer off the balance sheet through insurance, before scrutinizing current and available policies to ensure new risks are covered.

CyQu risk maturity scoring

The risk maturity scoring follows the scale that is described below.

- Initial | 1-1.9

Organizational cyber security risk management practices are not performed. If the organization identifies and addresses risks, it is done within silos only; components and activities of the risk management process are limited in scope and implemented in an ad hoc manner.

- Basic | 2-2.5

Organizational cyber security risk management practices and technologies are not formalized. Risk is managed in an ad hoc and sometimes reactive manner. Risk management practices and technologies are not established organization-wide.

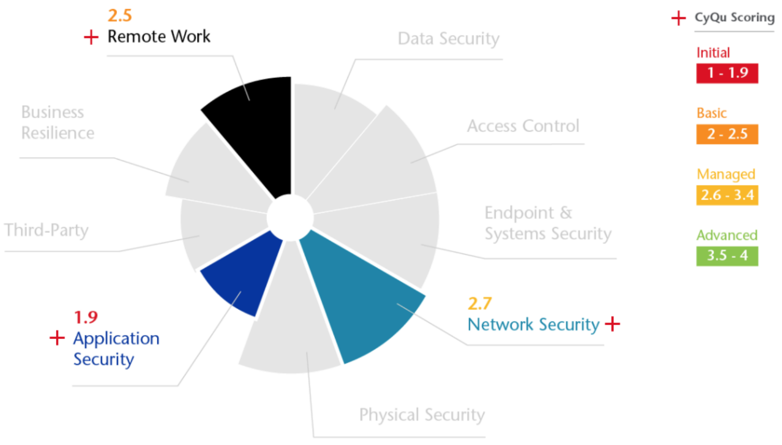
- Managed | 2.6-3.4

Risk management practices and technologies are performed and established throughout the majority of the organization. It adapts cyber security practices based on best practices and predictive indicators throughout the majority of the business. Policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk.

- Advanced | 3.5-4

Adopts an organization-wide approach to manage cyber security risk. Organizational cyber security practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape. Process of continuous improvement incorporating advanced cyber security technologies and practices.

Results per category



*Aon's Cyber Quotient Evaluation (CyQu) is a comprehensive cyber risk assessment that evaluates cyber risk across 9 security domains and 35 critical control areas.

Fig.3.14: Cyber Risk Report scoring for the security domains: Remote Work, Application Security, Network Security

Remote work

Enables users to remotely access corporate systems and data securely to deliver on their roles and responsibilities when outside of of corporate working environments.

CyQu global average | 2.5

*Basic (2-2.5) | Organizational cyber security risk management practices and technologies are not formalized and risk is managed in an ad hoc and sometimes reactive manner.

Remote working is here to stay, yet only 40% of organizations report having adequate remote work strategies to manage this new risk.

These measures include:

- Remote Connectivity
- Authentication and Identity
- Device Vulnerability and Monitoring
- Remote Business Continuity
- Remote Security Awareness

Application security

Protects applications from threats by requiring measures or checks during each stage of the application development life cycle.

CyQu global average | 1.9

*Initial (1-1.9) | Organizational cyber security risk management practices are not performed.

Only 17% of organizations report having adequate application security measures for the rapid pace of digital evolution.

These measures include:

- Training
- Secure Development
- Software Management

How to close the gaps:

Organizations that are not adequately managing application security risks should consider secure development security training for all developers and perform application penetration testing on critical digital services.

Network security

Delivers infrastructure services including enterprise defense for network, compute, physical presence, cloud, storage management and operations.

CyQu global average | 2.7

*Managed (2.6 - 3.4) | Risk management practices and technologies are performed and established throughout the majority of the organization.

Positively 60% of organizations report having sufficient network security measures to manage new digital connectivity.

These measures include:

- Network Environment
- Wireless Security
- Network Penetration Testing
- Network Capacity

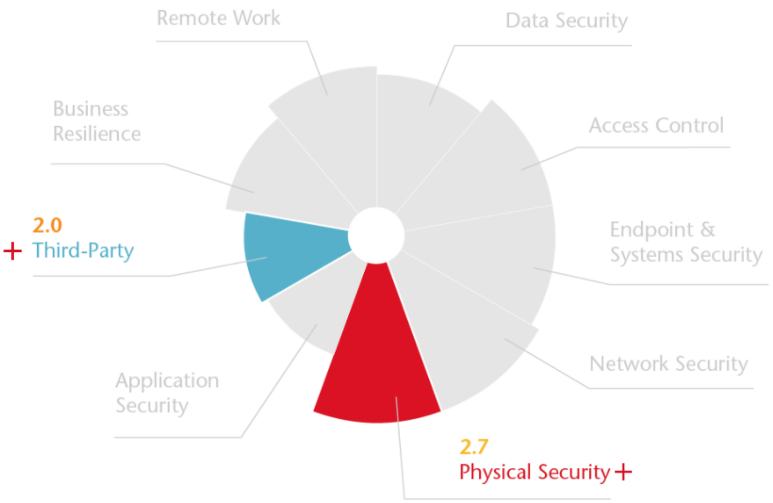


Fig.3.15: Cyber Risk Report scoring for the security domains: Third-Party, Physical Security

Third-party

Monitors relationships with third-parties to ensure provided services adhere to defined security policies.

CyQu global average | 2.0

*Basic (2.0 - 2.5) | Organizational cyber security risk management practices and technologies are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.

An alarmingly low 21%, or one in five organizations, report having adequate third-party management measures to oversee critical suppliers and vendors.

These measures include:

- Third-Party Contracts
- Due Diligence
- Third-Party Inventory

How to Close the gap:

Organizations that are not adequately managing third-party risks should consider a range of due diligence, onboarding, and contract risk management measures. Perform cyber security assessments on third-parties during the vetting stage, and onboarding processes. Require third-parties to agree to Service Level Agreements (SLAs) to periodically perform cyber security assessments, penetration testing, and business continuity management and response exercises.

Physical security

Protects facilities, equipment, resources, and personnel from unauthorized access, damage or harm.

CyQu global average | 2.7

*Managed (2.6 - 3.4) | Risk management practices and technologies are performed and established throughout the majority of the organization.

Positively 60% of organizations report having adequate physical security strategies.

These measures include:

- Physical Access
- Physical Penetration Testing
- Tampering and Alteration Controls
- Environmental Controls

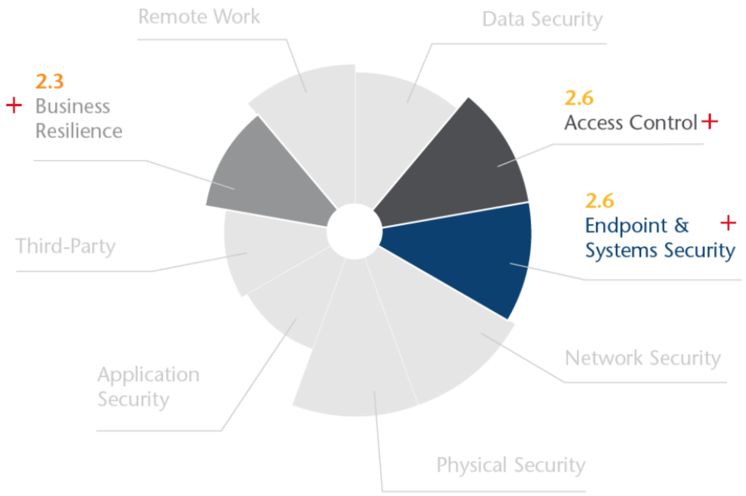


Fig.3.16: Cyber Risk Report scoring for the security domains: Business Resilience, Access Control, Endpoint & Systems Security

Business resilience

Plans for prompt and effective continuation of business critical services in the event of a disruption.

CyQu global average | 2.3

*Basic (2.0-2.5) | Organizational cyber security risk management practices and technologies are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.

Ransomware poses a business interruption and balance sheet risk, but only 31% of organizations report having adequate business resilience measures in place.

These measures include:

- Business Continuity and Disaster Recovery
- Incident Response
- Backup

How to close the gap:

Organizations that are not adequately managing disruptive cyber risks should consider a business continuity strategy that encompasses analysis, planning, testing, and governance. It is critical to build a Business Continuity Plan (BCP) that explicitly addresses disruptive cyber risk scenarios that consider both internal technology, and third-party services.

Access control

Grants authorized users the right to use a service while preventing access to non-authorized users.

CyQu global average | 2.6

*Managed (2.6-3.4) | Risk management practices and technologies are performed and established throughout the majority of the organization.

44% of organizations report having adequate access management measures in place, yet insurers see this control as critical.

These measures include:

- Two-Factor Authentication
- Password Configuration
- Access Management

Endpoint & systems security

Delivery and administration of infrastructure services, systems monitoring, endpoint protection, configuration management, storage management and infrastructure operations.

CyQu global average | 2.6

*Managed (2.6-3.4) | Risk management practices and technologies are performed and established throughout the majority of the organizations.

Positively 49% of organizations report having sufficient endpoint & systems security.

These measures include:

- Endpoint Protection
- Vulnerability Management
- Asset Inventory
- Secure Configuration
- Logging and Monitoring

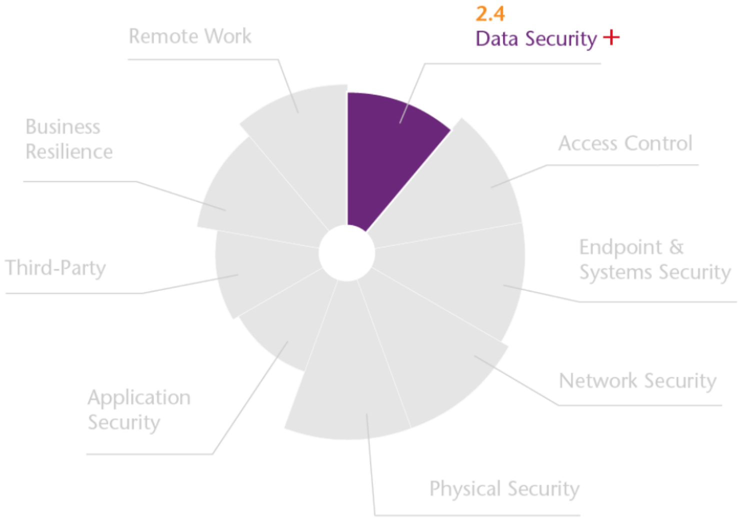


Fig.3.17: Cyber Risk Report scoring for the security domain: Data Security

Data security

Manages safeguards to protect the confidentiality, integrity, and availability of information.

CyQu global average | 2.4

*Basic (2.0-2-5) | Organizational cyber security risk management practices and technologies are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.

Less than two in five organizations (36%) report they have adequate levels of data security preparedness.

These measures include:

- Data Classification
- User Awareness and Training
- Data Protection
- Governance
- Risk Management

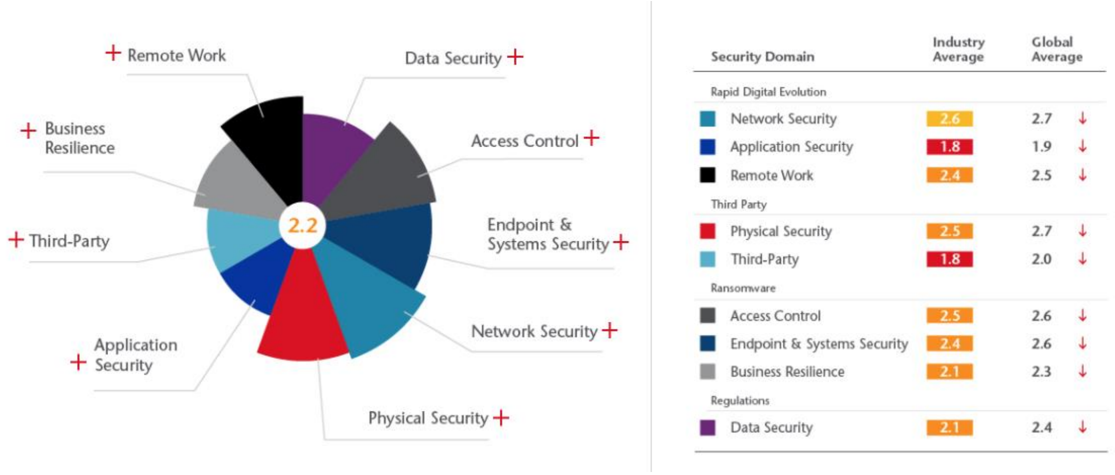
How to close the gap:

Organizations that do not have adequate risk management approaches for data privacy and regulations should consider integrating data privacy and cyber security regulatory risk into the enterprise risk management framework. Appoint an executive-level champion, e.g. CIO, CISO, or GC, to sponsor and promote cyber security matters to the board.

Results per sector

Manufacturing sector

Manufacturing organizations do not have the same legacy experience as data-intensive industries, such as financial institutions. Today, manufacturing is seeing an acceleration in the pace of technological change evidenced by the digital global supply chain, connected devices such as Human Machine Interfaces (HMI), Industrial Control Systems (ICS), and the Industrial Internet of Things (IIoT).



	Security Domain	Industry Average	Global Average	
	Rapid Digital Evolution			
■	Network Security	2.6	2.7	↓
■	Application Security	1.8	1.9	↓
■	Remote Work	2.4	2.5	↓
	Third Party			
■	Physical Security	2.5	2.7	↓
■	Third-Party	1.8	2.0	↓
	Ransomware			
■	Access Control	2.5	2.6	↓
■	Endpoint & Systems Security	2.4	2.6	↓
■	Business Resilience	2.1	2.3	↓
	Regulations			
■	Data Security	2.1	2.4	↓

Fig.3.18: Cyber Risk Report scoring for the Manufacturing sector

How does the manufacturing industry stack up? → 2.2 (basic)

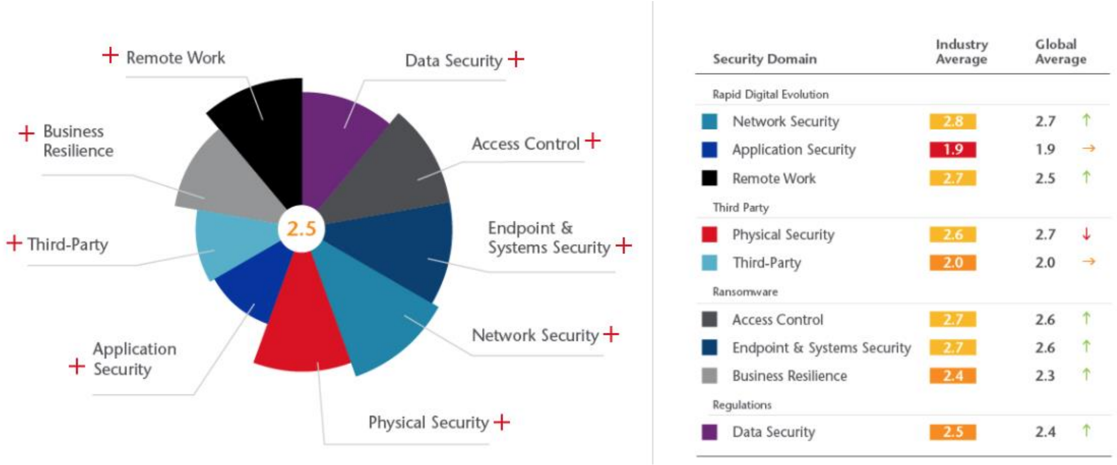
The average CyQu rating for manufacturing organizations globally is 2.2/4 (basic).

What this means

This rating indicates that cyber security maturity is at a basic level. Organizational cyber security risk management practices and technologies are not formalized. Risk is managed in an ad hoc and sometimes reactive manner. Risk management practices and technologies are not established.

Professional Services

Compared to many industries, professional services has weathered the COVID-19 pandemic relatively well. This is partly due to continued demand for its services, and also the ability for workers to shift to remote working with relative ease. This does not mean that cyber risk is irrelevant. The industry is a target for ransomware attacks, and firms report they are not managing cyber risk beyond the basic level.



Security Domain		Industry Average	Global Average	
Rapid Digital Evolution				
🟦	Network Security	2.8	2.7	↑
🟦	Application Security	1.9	1.9	→
■	Remote Work	2.7	2.5	↑
Third Party				
🟥	Physical Security	2.6	2.7	↓
🟦	Third-Party	2.0	2.0	→
Ransomware				
■	Access Control	2.7	2.6	↑
🟦	Endpoint & Systems Security	2.7	2.6	↑
■	Business Resilience	2.4	2.3	↑
Regulations				
🟪	Data Security	2.5	2.4	↑

Fig.3.19: Cyber Risk Report scoring for the Professional Services sector

How does the professional services industry stack up? → 2.5 (basic)

The average CyQu rating for professional services organizations globally is 2.5/4 (basic).

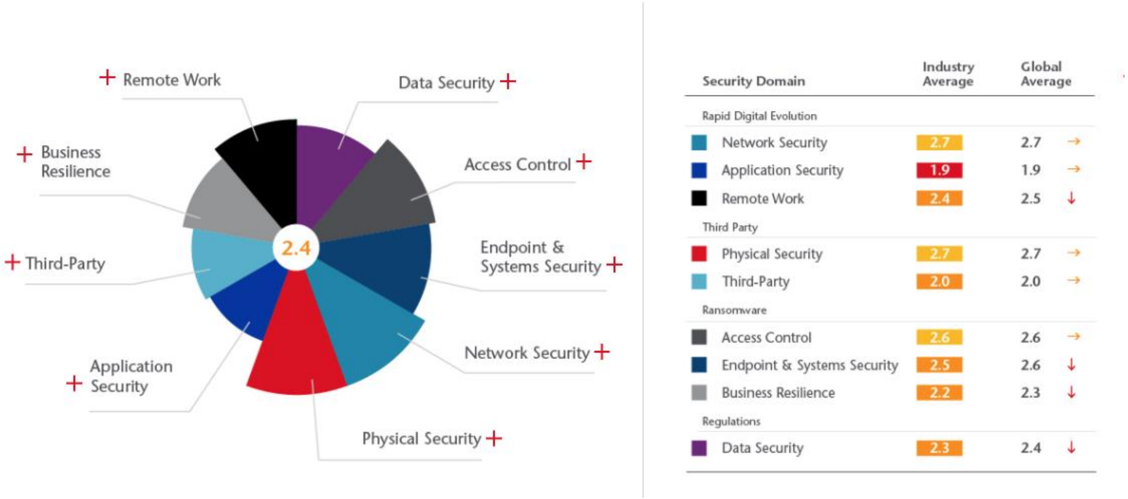
What this means

This rating indicates that cyber security maturity is at a basic level. Organizational cyber security risk management practices and technologies are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.

Risk management practices and technologies are not established organization-wide.

Retail Sector

Online everything was the theme for 2020, and retailers are continuing to see a demand for digital customer experiences. Already an industry fraught with cyber risk and under the watch of regulators, retailers now must identify and close the gaps resulting from rapid technology innovations and continue to painstakingly protect sensitive customer data.



Security Domain	Industry Average	Global Average	
Rapid Digital Evolution			
Network Security	2.7	2.7	→
Application Security	1.9	1.9	→
Remote Work	2.4	2.5	↓
Third Party			
Physical Security	2.7	2.7	→
Third-Party	2.0	2.0	→
Ransomware			
Access Control	2.6	2.6	→
Endpoint & Systems Security	2.5	2.6	↓
Business Resilience	2.2	2.3	↓
Regulations			
Data Security	2.3	2.4	↓

Fig.3.20: Cyber Risk Report scoring for the Retail sector

How does the retail industry stack up? → 2.4 (basic)

The average CyQu rating for retail organizations globally is 2.4/4 (basic).

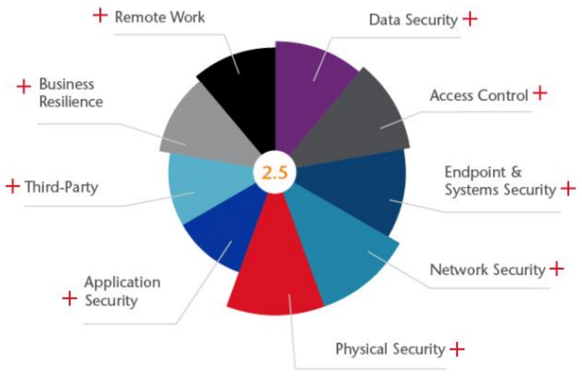
What this means

This rating indicates that cyber security maturity is at a basic level. Organizational cyber security risk management practices and technologies are not formalized. Risk is managed in an ad hoc and sometimes reactive manner.

Risk management practices and technologies are not established.

Technology, media and telecommunications

Technology, media and telecommunications (TMT) organizations serve as an underpinning to all other industries, and demand for their products and services is more pronounced than ever. From electronic signature software, to 5G infrastructure implementation, and the Internet of Things (IoT), this industry is fundamental to the future of work. This is increasing the spotlight on cyber security, magnified by major recent events exposing vulnerabilities in global operating systems and supply chains.



	Security Domain	Industry Average	Global Average	
	Rapid Digital Evolution			
■	Network Security	2.8	2.7	↑
■	Application Security	2.2	1.9	↑
■	Remote Work	2.5	2.5	→
	Third Party			
■	Physical Security	2.8	2.7	↑
■	Third-Party	2.2	2.0	↑
	Ransomware			
■	Access Control	2.7	2.6	↑
■	Endpoint & Systems Security	2.6	2.6	→
■	Business Resilience	2.4	2.3	↑
	Regulations			
■	Data Security	2.6	2.4	↑

Fig.3.21: Cyber Risk Report scoring for the TMT sector

How does the technology, media and telecommunications industry stack up? → 2.5 (basic)

The average CyQu rating for technology, media and telecommunications organizations globally is 2.5/4 (basic).

What this means

This rating indicates that cyber security maturity is at a basic level. Organizational cyber security risk management practices and technologies are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.

Risk management practices and technologies are not established organization-wide.

Takeaways - The opportunity

Predictions abound regarding the future of cyber risk. Instead of focusing on 'what's next?', this report has so far focused on 'what's now?'— in terms of what organizations should do to focus on risks today. To answer this, we relied on practical insight and hard data to explore the questions: What are the most pertinent cyber risks today, and how prepared are organizations across industries and regions, to manage these risks?

Now, we present the opportunities. Armed with knowledge, organizations have the ability to methodically ask the right questions to address cyber risk as an enterprise risk—to conduct a thorough assessment of cyber maturity and close the gaps that exist today.

Organizations also have an opportunity to become ready for tomorrow—to look to the future, and the changing cyber risk landscape. New risks are emerging daily and vigilance is essential.

Keeping the focus on today: making better decisions

The Cyber Quotient Evaluation (CyQu) data told us that organizations are performing under baseline when it comes to managing cyber risk. So, how do organizations become more prepared and protected?

Below is a blueprint to help organizations make better decisions by asking the right questions.

Assessment

- ✓ What is the state of our security and controls, in particular as they apply to digital evolution, third-party risk, ransomware, and regulatory risk?
- ✓ What are the most important assets we need to protect?
- ✓ What are the most likely threats?
- ✓ How do we balance business needs with cyber risks?

Quantification

- ✓ Do we know the type and materiality of our potential losses? For ransomware, do we know this beyond risk of data encryption?
- ✓ Do we understand key regulatory requirements and costs associated with
- ✓ non-compliance?
- ✓ How are we making security investment decisions?
- ✓ Can we measure the effectiveness of our current risk management and insurance, in terms of total cost of risk (TCOR)?

Insurance

- ✓ Do we understand our exposures?
- ✓ Do we have an effective strategy to mitigate loss?
- ✓ Should we transfer a portion of our risk to the insurance market, or consider alternative risk transfer strategies?

Incident Response Readiness

- ✓ Do we have an appropriate, usable incident response plan? If yes, is the response team trained and ready to act?
- ✓ Do we have the right security and forensic tools, processes and procedures?
- ✓ Have we properly configured our cyber security technology?
- ✓ Can we quickly and effectively respond to an incident?

An eye on the horizon: getting ready for tomorrow

Leaders from across Aon’s Cyber Solutions singled out five notable risks that are critical in the near future. Being educated in these risks is essential.

1. Artificial Intelligence (AI)

Machine learning is evolving at a rapid pace, and it will become an inextricable component of how businesses operate. AI will make decisions for us at some time, and any decision that can be swayed or attacked poses a substantial risk.

2. Alternative Payments

There is a cyber risk everywhere there is a financial transfer. Alternative payments and innovative strategies to accumulate and store wealth are desperately needed in the developing countries. Organizations will come into contact with counterparts who do not use banks, and business-to-consumer models will eventually be devoid of traditional currencies.

3. Technology Supply Chain

Every year, technology vendors bring new exposures. Organizations must become more attentive in identifying vulnerabilities and exposure to cyber risk as more sensitive data and intellectual property is transmitted via third-party software.

4. Retirement Plans

Retirement plans contain a plethora of information and provide access to large quantities of money. Organizations need to know who has access to employee retirement data and what the plan provider's fiduciary responsibilities are. As more people access their plans online and via mobile devices, this information is becoming more vulnerable to hacking.

5. The Dark Web

Criminal markets are getting more powerful, thanks to the rise of bitcoin, the usage of browser technologies like TOR, and the sophistication of ransomware gangs. Their workstation is the dark web, and it is here to stay. Without a map or guide, organizations should not attempt to navigate this environment on their own. Maintain a continual state of alertness. [44]

Chapter 04:

Black Swans

Black Swans

Cost & prediction

A black swan is a highly unlikely major risk event that deviates from the usual, is exceedingly difficult to forecast, and has a large impact. The global economic crisis brought this concept to light, and Nassim Taleb wrote a popular book called «*The Black Swan: The Impact of the Highly Improbable*», in which he demonstrates how trying to foresee random events is futile. As a result, in addition to typical hazards, risk management techniques have been tuned to target black swans. In this section, two common mistakes made by executives and managers in addressing major risk event or black swans will be examined.

Risk Management Cost

"A penny saved is a penny earned," declared Benjamin Franklin. When our favorite team overcomes a league opponent in football (soccer for our American readers), we call it a "six-pointer." This perspective should be applied to the organization's risk management activities. Risk management activities are frequently perceived solely as an expense, and as a result, are sometimes avoided.

Most firms' risk management initiatives should be considered as profit-generating activities, according to this concept. We've heard from risk managers that it's difficult to persuade executives to allocate greater resources. Nine times out of ten, this is followed by the statement, "If they only knew how much it would cost without a risk management program."

Attempting to Predict Black Swans

By definition, black swans are difficult to predict. Executives and managers focus on less frequent, less destructive threats and vulnerabilities when projecting a large risk occurrence.

Organizations expose themselves and become more exposed to common events and threats by focusing on anticipating black swans and establishing procedures that are supposed to avoid their existence (albeit an anticipated occurrence). Black swans are unusual and out of the ordinary.

As a result, statistical analysis and historical events cannot be used to predict the occurrence of a black swan, which are rare occurrences.

Rather than attempting to foresee the occurrence of a black swan, it is better for a company to focus on the results and repercussions of a black swan and establish a business continuity and recovery plan (BCP). Understanding the organization's potential impact and vulnerability to a black swan and using this information to design a BCP, an organization is better equipped to address a major risk event if it occurs.

The concept of black swans and risk management is much broader than what is covered here. This is only a starting point...[45]

Preparing for a Black Swan Cyberattack

Major institutions such as banks have a long history of developing redundant systems to withstand cyber-attacks. However, as catastrophic cyber-attacks affect businesses, governments, utilities, and hospitals more frequently, it's becoming evident that organizations now need two playbooks: one for ordinary cyber threats like malware, phishing, and denial-of-service assaults, and another for more serious cyber-attacks. As well as a new one that deals with something considerably worse. They must be prepared for cyber-attacks that could impair not only their own operations, but also their entire industry and others.

Companies must adopt the playbooks used for other types of disasters, so-called "black swan" events that can happen abruptly and have far-reaching consequences, to stay ahead of today's changing cyber challenges. Despite the fact that catastrophic cyber-attacks are becoming more regular, a recent poll performed by Marsh, Oliver Wyman's sister business, found that over half of companies had not even identified cyber scenarios that potentially damage them. One-quarter of respondents do not consider cyber hazards to be significant business risks at all.

This means that businesses must devote time to researching the various forms of cyber catastrophes they may face, no matter how unlikely. Cyber-attacks, like other calamities, can strike with the force of a 100-year storm. They can also arise slowly at first, like a pandemic that builds and spreads over time before exploding into a full-blown crisis — when it is too late to stop it. As a result, businesses must have procedures in place to address both acute cyber attacks and slow-burning, growing cyber risks.

Companies must then determine if cyber dangers can be contained or if they will spread like a contagion within their sector – and maybe outside. Some organizations have already built severe contingency and fallback strategies, such as preparing to function offline. Some people are even choosing to work offline as their preferred method. Three years after hacktivists disrupted the government's websites through a series of cyber-attacks, Singapore has chose to cut off internet connection for practically all of its computers. Infected healthcare providers and hospitals in the United States and Germany are taking vital systems offline and preparing to go back to pen and paper if a ransomware assault disrupts their digital operations.

Considering many operations are now networked, most organizations will need to go above and beyond to prepare for cyber-attacks that could have industry-wide ramifications, such as forming alliances with competitors, regulators, and industry groups. Industry stakeholders can develop specific channels and systems that ensure a quick and effective reaction by working together.

Some banks, for example, are partnering with competitors to act as proxies in the case of a cyber-attack, because they recognize that the consequences of a cyber-attack on their systems might have far-reaching consequences. If banks were suddenly unable to provide millions of businesses and individuals with access to their accounts, stopping them from paying salaries and bills, an economic crisis could occur.

Other major organizations are looking into creating "cyber pool funds," which are akin to money set aside to help victims of terrorist acts or natural disasters. These funds could help to mitigate the aftershocks of cyber-attacks that spread to the point where they become total cyber meltdowns that affect several industries.

Another important step could be to establish industry-wide or cross-industry "SWAT" teams to monitor and respond to prevalent cyber threats on a regular basis. These groups would look into what cyber hazards should be covered and to what extent. They'd look for trigger points that could prevent full-fledged cyber-crises: Which data and services are acceptable to lose for a few hours? What losses would quickly trigger a cyber-meltdown?

These SWAT teams might also undertake cross-industry cyber-attack post mortems, allowing industries to improve their cyber defenses over time. These groups would help organizations not just establish best practices, but also integrate lessons learnt from previous breaches into their systems.

One thing is certain: the consequences of cyber-attacks will only spread, and the sophistication of these attacks will only increase. The White House recently produced its first emergency response plan for a major cyber-attack in reaction to the publication of crucial Democratic National Committee emails in order to influence the US presidential election. While that hack is low-level, the government is preparing for higher-level cyber threats to infrastructure, stability, and human life.

Extraordinary circumstances necessitate extreme means. Cyber risks that were once inconceivable for many businesses are now an everyday occurrence. Organizations should take a cue from governments' growing concern and start forming the connections needed to create a second playbook aimed at preventing cyber meltdowns.[46]

Cyber Situational Awareness

Can it prevent the Next Black Swan Cyber Event?

The black swan concept is especially important when it comes to cybersecurity. As the size and scope of cyberspace expands, it gets more entangled with various elements of daily life. Because of this increased integration, a black swan event might have massive ramifications due to the multiplier effect.

A black swan occurrence is impossible to predict and can only be explained with hindsight wisdom. However, certain high-impact, low-probability scenarios might be simulated or conceived in order to build an incident response plan.

The high-profile breaches at Yahoo, Target, and Sony were not black swan events since they could have been expected and prepared for. Target's 2013 data breach, which exposed 40 million debit and credit card numbers, was caused by a third-party HVAC vendor's inadequate security standards. Similarly, insufficient access control protocols have been blamed for the Sony incident. Meanwhile, an unprotected cellular modem allegedly allowed threat actors to seize control of key infrastructure in a 2013 attack on a dam in New York.

If atypical security vulnerabilities had been considered, these high-impact, low-probability incidents could have been averted. Security situations that are unlikely but possibly harmful must be considered in an effective incident response plan.

The Ponemon Institute issued a fascinating report titled "Efficacy of Emerging Network Security Technologies" in 2013. The majority of security professionals around the world think that the threat landscape is changing and becoming more complicated every day, according to the survey. As a result, most businesses, particularly those in banking, finance, health care, and manufacturing, are implementing the most up-to-date security solutions to prevent incidents.

Surprisingly, some study respondents who claimed positive security solution results also said their firms were vulnerable to cybercrime. The situation offered a bleak picture of the security landscape, implying that many businesses are unable to deal with unusual and unexpected threats that could trigger a black swan cyber event.

Only recognized risks are detected and contained by the solutions that organizations use. Intrusion prevention systems (IPS) can only protect against attacks that match a database of known threat way, these solutions don't cover the complete danger environment since they don't account for dynamically emerging threats and don't offer any protection against the unknown. Cybercriminals will continue to enter networks until all attack paths are insulated by security obstacles, and the risk of high-impact scenarios will persist.

Embracing Cyber Situational Awareness

Extraordinary dangers necessitate extraordinary responses. Noone can't forecast a black swan occurrence, but it is possible to estimate its likelihood and possible impact by designing a security architecture that adapts as the threat landscape changes. To establish a dynamic, not static security posture, organizations must look beyond traditional techniques of defense. This necessitates cyber situational awareness and sharing of data.

Situational awareness, according to Dr. Mica Endsley, former top scientist of the United States Air Force, is the perception of environmental variables, the interpretation of their meaning, and the projection of their condition in the near future. Cyber situational awareness's perception, comprehension, and projection components can effectively follow, evaluate, and deliver actionable intelligence on new threats, threat actors, vulnerabilities, and malware. This allows businesses to assess their own security readiness and take proactive steps to mitigate the dangers posed by emerging attacks.

Securing Human Endpoints

All levels of an organization's hierarchy, including board members and executives, IT experts, security analysts, human resources, finance, sales, marketing, and third-party vendors and clients, must be trained in situational awareness. All of them are human endpoints with awareness gaps that could be exploited by scammers.

If these vulnerabilities are patched in real time, cybercriminals will have a hard time increasing their level of sophistication. Like an exponential curve, their novel tactics would reach a peak and then plateau, giving organizations enough time to regulate their awareness levels. Furthermore, to defend the whole industrial security framework, the actionable information created by situational awareness must be communicated in real time with industry colleagues and clients.

Butterflies and Black Swans

The butterfly effect argues that every minute, localized action can have major implications elsewhere in a complex system, and it's equally vital to view an organization's security posture through this lens. Consider the numerous instances of bad cyber hygiene that employees engage in daily; these blunders can lead to a major black swan event.

Considering that most corporate assets are networked across organizations, malevolent actors can use a localized action to cause catastrophic outcomes within a network and even throughout cyberspace at large. To avoid black swan events, individuals must practice good cyber hygiene. User education, like software, necessitates routine patching, which can only be accomplished through cyber situational awareness.[47]

Is 2021 the Black Swan Event Year?

Stealthbits Technologies, a cybersecurity software company focused on protecting an organization’s sensitive data and the credentials attackers use to steal that data, has recently unveiled its predictions on what security teams would face in 2021. The company believes that fueled by the pandemic, next year will see organizations challenged by unpredictable events with potentially severe consequences, often referred to as “black swan events.” Stealthbits cites a resurgence in outsourcing to meet security needs, the continued struggle to adhere to a growing list of global privacy regulations and a twist on ransomware targets as other hallmarks of the year ahead.

“The events of 2020 forced organizations to do things they weren’t necessarily ready to do to support a remote, global workforce,” said Jim Barkdoll, CEO of Stealthbits. *“As a result, security teams are playing a high-stakes game of whack-a-mole, as they are forced into the almost untenable position of force fitting what they have to meet new challenges without the time, budget or resources to properly execute it. Whether it is digital transformation, cloud adoption or adhering to privacy regulations, we believe 2021 will see global organizations grappling with what the next attack will be and where and how it will hit.”*

Stealthbits predicts that the inevitability of a Black Swan event in security will be impacted by the following in 2021:

1. Ransomware will become cloud aware.

In 2020, ransomware breaches moved away from locking environments, toward data breaches and demanding payment to prevent bad actors from leaking information. In 2021, ransomware will not only become more advanced, it will adapt to target the new data stores in SaaS and cloud.

Enterprises that don’t protect the new perimeter will fall victim to attackers.

As the world faced a global pandemic, enterprises were forced into a corner, acting quickly to extend their perimeters to accommodate a remote workforce. In 2021 organizations must move quickly to control the new perimeter they jammed into place in 2020. Moreover, organizations will be forced to either address all the gaps in their technology architecture resulting from missed or skipped steps for the sake of expediency, or face breaches as threat actors will quickly identify and capitalize on these vulnerabilities.

2. Popularization of Privacy.

As awareness of Data Privacy becomes more mainstream, this will put more pressure on organizations to respond faster than they have previously. If we look at documentaries like The Social Dilemma by Netflix, or cinema-like shows like Identity Thief or UK-produced thriller, Black Mirror, privacy is permeating pop culture. This mainstream shift will drive more accountability through organizations and in turn, their vendors, to become more compliant.

3. Rising, complex global privacy regulations will make data breaches a cost of doing business.

In the next three years, 65% of the world’s population will be living in countries that demand personal data privacy protections for their citizens. That’s up from just 10% this year, according to a recent study by Gartner. 2021 will see an increase in compliance failure and regulatory fines. Even if every organization takes action to implement strategies to address the growth in regulations, it takes time to achieve any effectiveness. Organizations will acknowledge a data breach and/or compliance fine as a cost of doing business.

4. Cloud creates a new skills gap

Rapid cloud adoption and the acceleration of digital transformation initiatives have been the hallmark of 2020 for many organizations. While these initiatives are significant, the pace in which SaaS evolves makes it incredibly difficult for existing security resources to keep abreast of capabilities – it’s creating a new level of skills gap. Cloud experts are challenged to keep pace with the rate of change and that introduces risk.

5. Outsourcing will struggle to deliver due to accelerated cloud adoption and digital transformation.

The acceleration of aggressive cloud adoption and digital transformation combined with the skills gap mentioned above means MSSPs will struggle to meet the demands of the market and keep the security promises to their customers. The increasing demand to secure newly adopted infrastructure results from the same challenge that faces many organizations: they simply can’t hire or train fast enough to keep pace with the demand.[48]

Fortunately or not, most predictions have fallen into place as we are crossing over 2021. What will come remains to be seen, however, it is obvious already that awareness and continuous education are our defense weapons against black swan events regarding emerging technologies. We should keep vigilant in order to predict and prevent events, rather than just learn from them, after having them occurred already, following relevant consequences.

Chapter 05:

Critical Infrastructures Threat Intelligence

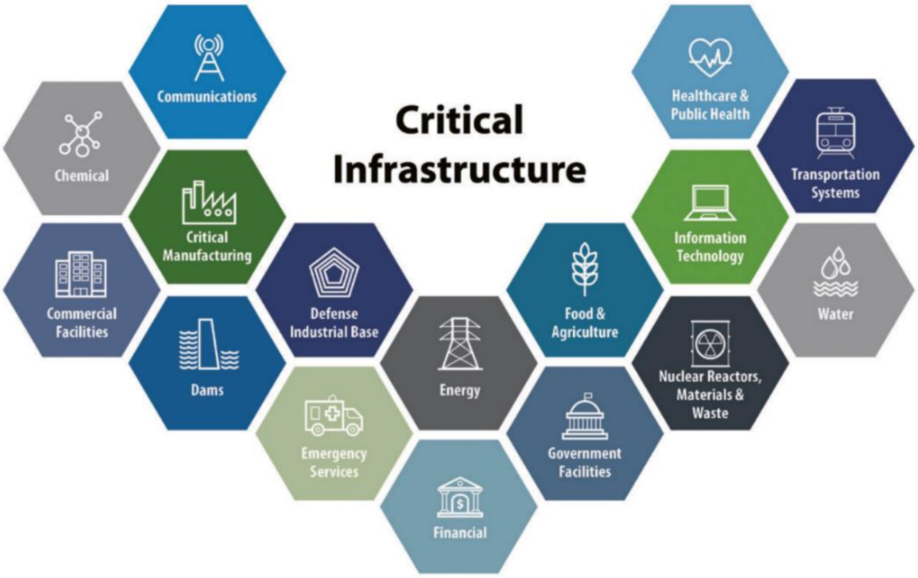
Critical Infrastructures Threat Intelligence

Definitions

Threat intelligence, or cyber threat intelligence, is information an organization uses to understand the threats that have, will, or are currently targeting the organization. This info is used to prepare, prevent, and identify cyber threats looking to take advantage of valuable resources.

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy – the infrastructure. Most commonly associated with the term are facilities for:

- Shelter; Heating (e.g. natural gas, fuel oil, district heating);
- Agriculture, food production and distribution;
- Water supply (drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices));
- Public health (hospitals, ambulances);
- Transportation systems (fuel supply, railway network, airports, harbours, inland shipping);
- Security services (police, military).
- Electricity generation, transmission and distribution; (e.g. natural gas, fuel oil, coal, nuclear power)
- Renewable energy, which are naturally replenished on a human timescale, such as sunlight, wind, rain, tides, waves, and geothermal heat.
- Telecommunication; coordination for successful operations
- Economic sector; Goods and services and financial services (banking, clearing); [49]



© US Cybersecurity &
Infrastructure Security Agency (CISA)

Fig.5.1: Critical Infrastructures Map

EU Security Union Strategy

In 2020, the European Commission sets out a new EU Security Union Strategy for the period 2020 to 2025, focusing on priority areas where the EU can bring value to support Member States in fostering security for all those living in Europe. From combatting terrorism and organised crime, to preventing and detecting hybrid threats and increasing the resilience of our critical infrastructure, to promoting cybersecurity and fostering research and innovation, the strategy lays out the tools and measures to be developed over the next 5 years to ensure security in our physical and digital environment.

This strategy lays out 4 strategic priorities for action at EU level:

1. A future-proof security environment

Individuals rely on key infrastructures, online and offline, to travel, work or benefit from essential public services; and attacks on such infrastructures can cause huge disruptions. Preparedness and resilience are key for quick recovery. The Commission will put forward new EU rules on the protection and resilience of critical infrastructure, physical and digital.

Recent terrorist attacks have focused on public spaces, including places of worship and transport hubs, exploiting their open and accessible nature.The Commission will promote stepped up public-private cooperation in this area, to ensure stronger physical protection of public places and adequate detection systems.

Cyberattacks have become more frequent and sophisticated. By the end of the year, the Commission should complete the review of the Network and Information Systems Directive (the main European cybersecurity legislation) and outline strategic cybersecurity priorities to ensure the EU can anticipate and respond to evolving threats.

In addition, the Commission has also identified the need for a Joint Cyber Unit as a platform for structured and coordinated cooperation.

Lastly, the EU should continue building and maintaining robust international partnerships to further prevent, deter and respond to cyberattacks, as well as promote EU standards to increase the cybersecurity of partner countries.

2. Tackling evolving threats

Criminals increasingly exploit technological developments to their ends, with malware and data theft on the rise. The Commission will make sure that existing EU rules against cybercrime are fit for purpose and correctly implemented, and will explore measures against identity theft.

The Commission will look into measures to enhance law enforcement capacity in digital investigations, making sure they have adequate tools, techniques and skills. These would include artificial intelligence, big data and high performance computing into security policy.

Concrete action is needed to tackle core threats to citizens, such as terrorism, extremism or child sexual abuse, under a framework ensuring the respect of fundamental rights. The Commission is putting forward today a strategy for a more effective fight against child sexual abuse online.

Countering hybrid threats that aim to weaken social cohesion and undermine trust in institutions, as well as enhancing EU resilience are an important element of the Security Union Strategy. Key measures include an EU approach on countering hybrid threats, from early detection, analysis, awareness, building resilience and prevention to crisis response and consequence management – mainstreaming hybrid considerations into broader policy-making. The Commission and the High Representative will continue to jointly take forward this work, in close cooperation with strategic partners, notably NATO and G7.

3. Protecting Europeans from terrorism and organised crime

Fighting terrorism starts with addressing the polarisation of society, discrimination and other factors that can reinforce people's vulnerability to radical discourse. The work on anti-radicalisation will focus on early detection, resilience building and disengagement, as well as rehabilitation and reintegration in society. In addition to fighting root causes, effective prosecution of terrorists, including foreign terrorist fighters, will be essential – to achieve this, steps are under way to strengthen border security legislation and better use of existing databases. Cooperation with non-EU countries and international organisations will also be key in the fight against terrorism, for instance to cut off all sources of terrorism financing.

Organised crime comes at huge costs for victims, as well as for the economy, with €218 to €282 billion estimated to be lost every year. Key measures include an Agenda for tackling organised crime, including trafficking in human beings for next year. More than a third of organised crime groups active in the EU are involved in trafficking illicit drugs. The Commission is today putting forward a new EU Agenda on Drugs to strengthen efforts on drug demand and supply reduction, and reinforce cooperation with external partners

Organised crime groups and terrorists are also key players in the trade of illegal firearms. The Commission is presenting today a new EU Action Plan against firearms trafficking. To ensure that crime does not pay, the Commission will review the current framework on seizing criminals' assets.

Criminal organisations treat migrants and people in need of international protection as a commodity. The Commission will soon put forward a new EU Action Plan against migrant smuggling focussing on combatting criminal networks, boosting cooperation and support the work of law enforcement.

4. A strong European security ecosystem

Governments, law enforcement authorities, businesses, social organisations, and those living in Europe all have a common responsibility in fostering security.

The EU will help promote cooperation and information sharing, with the aim to combat crime and pursue justice. Key measures include strengthening Europol's mandate and further developing Eurojust to better link judicial and law enforcement authorities. Working with partners outside of the EU is also crucial to secure information and evidence. Cooperation with Interpol will also be reinforced.

Research and innovation are powerful tools to counter threats and to anticipate risks and opportunities. As part of the review of Europol's mandate, the Commission will look into the creation of a European Innovation hub for internal security.

Skills and increased awareness can benefit both law enforcement and citizens alike. Even a basic knowledge of security threats and how to combat them can have a real impact on society's resilience. Consciousness of the risks of cybercrime and basic skills to protect oneself from it can work together with protection from service providers to counter cyber-attacks. The European Skills Agenda, adopted on 1 July 2020, supports skills-building throughout life, including in the area of security. [50]

Critical Infrastructure Protection and Resilience

As outlined in the Security Union Strategy, protection and resilience of critical infrastructures remains among the top priorities of the European Union. European critical infrastructure sectors find themselves in the midst of rapid digitization that is accelerated by the growth of technologies like cyber-physical systems (CPS), the Internet of Things (IoT) and artificial intelligence (AI). Besides this, critical infrastructure operators today are confronted with different types of risks in both the cyber- and physical domain. Notable attacks like the "Wannacry" ransomware and the "Mirai" botnet cyber-attacks, which affected critical infrastructure operations across different Member States and in multiple sectors, remind us of the risks that we face. This situation calls for innovative security concepts that take us beyond conventional policies that have been addressing either the physical or cyber-security domain. Currently, the ongoing COVID-19 pandemic shows us the vital role that digital critical infrastructure play in keeping different sectors like telecommunications, finance, energy, and health care running in the time of crisis.

The European Commission (EC) is supporting the Member States to protect and ensure the resilience of critical infrastructures. It has adopted an integrated framework based on both strong physical and cyber-security measures. Key pillars of this framework include the Directive on security of network and information systems (NIS Directive), the Directive on protecting European Critical Infrastructures, the General Data Protection Regulation (GDPR), and the Cybersecurity Act Regulation.

Furthermore, under the Commission's new digital strategy, additional actions are being considered. The EC is emphasizing the consistency and complementarity of these and other ongoing initiatives, including the revision of the EUs overall approach to critical infrastructure protection and resilience, notably the European Programme for Critical Infrastructure Protection (EPCIP). A package of measures has started to be put forward during the fall of 2020.

Besides policy development, the EC supports research and innovation projects under Horizon 2020 looking for innovative approaches to the protection and resilience in different sectors

It is important to underline that research plays a vital strategic role for security policy in the EU. In this respect, the EC has encouraged and supported the clustering between projects, as a means of boosting their cooperation. As such, we welcome the creation of the European Cluster for Securing Critical infrastructures (ECSCI), which seeks to bring the many projects working to improve critical infrastructure protection and resilience together.

Based on results that have been achieved in EU-funded projects, this chapter describes innovative approaches to enhancing the protection of critical infrastructures. It also presents approaches that reduce fragmentation in security operations and improve the implementation of existing European regulation. It provides insights of relevance to policy makers, researchers and practitioners who are working to ensure the functioning of digitally-enabled critical infrastructures that our societies rely on.

At the dawn of the fourth industrial revolution, governments and enterprises are increasingly deploying Cyber-physical Systems (CPS) as part of their critical infrastructures. CPS systems blur the boundaries between the physical and digital worlds and enable digital control of physical processes in sectors like healthcare, finance, energy, and industry. CPS systems are a core element of the popular Internet of Things (IoT) paradigm, which has a transformational impact on the critical infrastructures that support the functioning of our societies and economies. Based on CPS and IoT systems, critical infrastructures operators leverage large amounts of field data in order to optimize business processes and decisions associated with the operation of their infrastructures. Furthermore, the rapid digitalization of critical infrastructures facilitates their interconnection and the seamless exchange of information across different stakeholders and value chains.

Along with these benefits, the expanded deployment of CPS and IoT technologies within critical infrastructures introduces various cybersecurity challenges, which add up to conventional physical security issues. This is evident in some of the recent large-scale security incidents against critical infrastructures, which include attacks against both cyber and physical assets. In several cases, adversaries exploit vulnerabilities in the digital parts of the infrastructures in order to attack their physical parts and vice versa. Therefore, critical infrastructures security must be implemented based on a holistic, integrated approach that protects cyber and physical assets at the same time. This is increasingly acknowledged by critical infrastructures operators and supported by recent regulatory efforts as well. As a prominent example, in Europe, the NIS Directive (EU 2016/1148) underlines the importance of cybersecurity for critical market operators and instructs EU Member states to supervise cybersecurity for the critical infrastructures of key sectors (e.g., telecommunications, finance, energy, healthcare, transport) in their country.

Overall, critical infrastructures security is currently redefined in order to address cyber and physical aspects in an integrated way. Cyber and physical security functions are no longer “siloed,” but rather combined in the scope of integrated security policies. This integration introduces new requirements such as the need to model security knowledge in an unified way, the need to address cascading effects between the two different types of attacks (i.e. cyber and physical attacks), as well as the need to integrate solutions for cybersecurity and physical security within commonly used security platforms. Likewise, integrated platforms for critical infrastructures security must provide functionalities for preventing, detecting, and responding to security incidents in a proactive and cost-effective manner. Moreover, they should provide the means for sharing information across security stakeholders [e.g. Security Teams, First Responders, Computer Emergency Response Teams (CERT)] to facilitate their effective collaboration.

The above-listed requirements are common to the critical infrastructures of the different sectors of the economy (e.g., finance, healthcare, energy, and transport).
Nevertheless, there are also sector-specific security requirements, stemming from the different devices, control processes, and business operations of the various sectors. Moreover, installations in different sectors are interconnected in different ways and are subject to diverse sets of cascading effects.

The critical infrastructure cybersecurity dilemma

Critical infrastructure is vital to the functioning of modern societies and economies, yet often these systems are not properly protected or are easily accessed and exploited, and thus remain a key target for threat actors. Although awareness around the severity of operational technology (OT) cyber risks is on the rise, the fact is, OT environments remain vulnerable.

In the first few months of the year, we've already seen news of several vulnerabilities in the sector exploited, such as the Florida water plant breach and most recently, the ransomware attack on Colonial Pipeline, one of the United States' most critical fuel pipelines.

Given the longevity of the systems and technology implemented in industrial settings, security has historically been relegated to a second tier of priorities compared to uptime, reliability and stability. It comes as no surprise that 56 percent of the world's gas, wind, water and solar utilities experience at least one shutdown or operational data loss per year, according to a Ponemon Institute report. That number has likely grown because of the pandemic, as many organizations weren't prepared for remote management of critical systems. In fact, although leaders agree on the importance of remote access, Claroty reported last year that 26 percent of organizations struggled with the newly dispersed workforce and 22 percent did not have a pre-existing secure remote access solution that is secure enough for OT.

As OT environments continue to evolve in the face of new potential disruptions, it is time for leaders to prioritize security and understand implications so they can act to protect their organizations and nations' critical infrastructure.

Understanding the New OT landscape

In the past few years, we have seen a convergence between OT and IT-based security infrastructures and processes. However, as we saw in the Colonial Pipeline attack, these integrated ecosystems have become considerably more difficult to secure, from misconfiguration, vulnerable hardware/software components and poor cybersecurity practices to the lack of visibility into connected assets and poor network segmentation.

Beyond the OT-IT environment convergence, the pandemic pushed many organizations to alter their cybersecurity processes to accommodate the new needs of remote work. However, adversaries quickly realized that targeting workers at home provided a viable path into OT networks, and turned to exploiting work from home, leveraging unpatched virtual private network (VPN) systems, interconnected IT and OT environments, and exploiting vulnerabilities in legacy Windows and OT systems.

OT has fast become a prime target for motivated and well-resourced threat actors who continue to redesign their tactics to penetrate new and enhanced security measures. In fact, 2020 saw a significant increase in exploitable vulnerabilities in OT. ICS-CERT advisories increased by more than 32 percent last year compared to 2019, and more than 75 percent of advisories were about "high" or "critical" severity vulnerabilities. Threat actors are also using ransomware campaigns to target OT environments because they understand how mission-critical these environments are. For example, if a pipeline carrying 45 percent of the United States' East Coast's fuel is shut down, it costs the pipeline operator millions of dollars per day.

The specialized and mission-critical nature of OT infrastructure technologies means that most security and threat intelligence solutions don't have visibility into potential vulnerabilities, let alone the ability to defend against attacks.

Preventing and Mitigating Risks

So, what can be done to enhance security in today's OT landscape? To protect, prevent and mitigate risks, there are several important steps organizations can take to improve their security posture.

- ✓ Implement a risk management program: OT is built around complex systems that oftentimes are not properly tracked in traditional asset management systems. Designing an effective OT security program requires a risk model that specifically maps the functional requirements of these systems while providing a holistic image of the potential real-world consequences of compromise. As part of the program, organizations that leverage the Purdue Model should ensure they're documenting the number of traffic flows between levels, especially if the flow is across more than one Purdue level.
- ✓ Build a cyber incident response plan: If there was something we should have learned from the COVID-19 pandemic, it is that we need to be ready for anything. A comprehensive cyber incident response plan that includes both proactive and reactive measures is required to help prevent incidents and better allow the organization to respond if one does occur. Make sure to print the response plan and have it handy. What happens if the systems that store the incident response plan are encrypted or unavailable due to an attack?
- ✓ Protect third-party remote access: Organizations regularly rely on third-party vendors to complement their business; however, many do not have uniform cybersecurity policies and practices. Many OT sites even have third party vendors regularly conduct maintenance via remote access technology, which creates exploitable weaknesses in the operations chain. Establishing a supply chain management program that vets external vendors' security standards and provides better control of third-party access is critical to reducing the risks third parties introduce.
- ✓ Enhance system monitoring procedures: It is no longer enough to simply build a network with a hardened perimeter. Securing OT systems against modern threats requires well-planned and well-implemented strategies that will allow defense teams to quickly and effectively detect, counter and respond to adversaries. At a minimum, corporate IT and OT domains should be physically and logically separated, networks must be segmented, and critical parts of the network isolated from untrusted networks, especially the

internet. It is also important to deploy monitoring tools such as passive intrusion detection systems (IDS) specifically designed for OT environments. Passive systems are key because proactive systems may present false positive detection that could lead to downtime of critical systems.

✓ Develop informed security controls: To establish the required controls, we have to start with an asset inventory. Once the assets have been identified, organizations at a minimum need to implement the security features provided by device and system vendors. However, to deal with some critical vulnerabilities, we recommend turning on security features that apply Common Industrial Protocol (CIP) security controls, a fairly universal standard. Many PLC vendors also have physical switches on their appliances that prevent the changing of the PLC' configurations, which should be used appropriately. We see many plants and OT sites with these switches always set to "config mode," which allows for the PLC configuration to be changed (potentially by an attacker). These should be complemented with secure and hardened configurations (read/write protections, memory protection, etc.). Managing controls over time can be daunting and time intervals between OT system upgrades can be years long, so organizations need an effective change management program. The program should be able to identify compensatory controls that can be applied to remediate critical vulnerabilities that cannot be patched immediately. These controls can include a host monitoring system that detects and alerts when unauthorized changes are made to Human Machine Interfaces (HMIs), engineering workstations or to PLCs.

✓ Establish audits and security assessments: Finally, numerous factors affect the security of a system throughout its life cycle, so periodic testing and verification of the system are essential. Timely audits and assessments help eliminate the "path of least resistance" that an attacker could exploit.[51]

The Ethical Aspects of Critical Infrastructure Protection

Critical infrastructures across different sectors are being strongly affected by the introduction of the IoT paradigm, CPS systems, intelligent digitally empowered devices, Big Data analytics, AI, and machine learning. Alongside an array of benefits, this transformational path also poses not only additional risks to their operation and security but also legal and ethical challenges and concerns for developers, practitioners, participants, and policy-makers, ranging from data protection and privacy preservation, to dataveillance, social cooling and dictatorship of data, to data ownership and access aspects, to safety, responsibility and liability, algorithmic bias and others.

The regulatory landscape is fragmented and runs at a much lower pace than technological development. Novel "soft law" tools, capable of giving granular and practical guidance, as well as ethics-related standardization initiatives, like the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, provide complementary rules and useful insights to traditional legal instruments to overcome or mitigate the given challenges raised by these technologies.

Other driving factors towards legal compliance and ethically-sound design, development, and operation of such developments are the Privacy and security by design and ethics & rule of law by design approaches, the regulatory sandboxes, and the cross-fertilization of law and technology, such as certain forms of automated compliance tools.

Critical infrastructures that support the operation and development of our societies across several sectors, like finance, healthcare, and energy, are being strongly affected by the introduction of the IoT paradigm, CPS systems and intelligent digitally empowered devices, such as sensors, to robots, smart wearables, smartphones, and drones, as well as by other emerging ICT technologies, like Big Data analytics, AI, and machine learning. Furthermore, critical infrastructures' digitalized and interconnected operations, business processes, and decision-making imply large collection and processing of increasingly amount of field data, often exchanged between relevant stakeholders within the given value chain. The boundaries between the physical and digital worlds are vanishing, and the digital control of physical processes is a reality.

This transformational path has multiple benefits, in terms of increasing the efficiency and sustainability of current practices and better performance gains, for instance, unfolding a range of possibilities to discover, manage, orchestrate, and control physical space to realize coordinated behaviors within and across devices. At the same time, this metamorphosis also poses additional risks to critical infrastructures' operation and security. A novel range of cybersecurity challenges sums up to the traditional physical security ones faced by critical infrastructure operators, giving rise to the emergence of integrated approaches for critical infrastructures security, simultaneously protecting cyber and physical assets. The introduction of integrated security systems into critical infrastructures poses ethical and legal challenges for developers, practitioners, participants, and policymakers. In conjunction with the array of expected benefits of these systems, unintended negative effects might occur and need to be avoided, or at least minimized, by thinking ahead, while at the same time ensuring that these technologies can benefit everyone, upholding legal concepts and ethical values, protecting human safety, physical integrity, dignity, intimacy, autonomy, and self-determination. One of the challenges related to these systems is to maximize security, and therefore the utility of the overall systems towards this direction, while protecting human rights, preserving ethical values, and respecting the regulatory framework.

The ethical dimensions of these systems need to be explored in an attempt to balance them with the protection of the critical infrastructures against physical and cyberattacks within the EU. Ethical risks, including data-related risks, have to be mitigated both at design time and run time, ensuring that architectures are safe and secure but also adhere to and promote European values (e.g., democracy, privacy safeguards, equal opportunities). Fair, trustworthy, ethical, and regulatory frameworks aimed at ensuring the compliance to the legislation enforcing these values should be perceived, rather than as restrictive, as an opportunity and competitive advantage, even more if taking place alongside technological developments.

In fact, an adequate ethical and legal framework, properly tackling with human-centered challenges and which would ensure that the solutions and services are designed and used in an ethical manner, is therefore critical to ensure trust in the security ecosystem around critical infrastructures, which, in turn, is essential to the acceptability of the technological artifacts, offering services and experimentation opportunities to the whole range of stakeholders across the critical infrastructure value chain.

Legal and Ethical Challenges

As underlined in the previous paragraph, the technological changes related to the Cyber-Physical System (CPS), Artificial Intelligence (AI), Internet of Things (IoT), and integrated security systems introduction in the critical infrastructures, while carrying the potential to yield new solutions and opportunities for business, government, and societies, also generate new risks, concerns, and challenges in multiple contexts.

IoT, AI, blockchain and Distributed Ledger Technology (DLT), collaborative and intelligent devices, cyber ranges, cyber-physical systems are expected to optimize and make more secure and more efficient the critical infrastructures' processes. These processes and the operation of the system are fueled by digital assets like digital twins, operational data, and machine learning models. They manifest both in the cyberspace and in the physical world, depending on underlying cloud-based infrastructure and other operational and information technology infrastructures, often geographically spread.

Being such digital assets and infrastructure increasingly interconnected, automated, and geographically distributed, not only the security challenges are greater but also ethical concerns and the risk of non-compliance with internationally recognized human rights, such as the right to privacy. The same apply to AI-supported technology with, for instance, facial recognition and emotion detection.

The increasing fragmentation in the legal and regulatory landscape at global, regional, and national level contributes to make the situation even more complex and to the emergence of novel accountability challenges. Without claiming to be complete, the following list provides hints on some of the most pressing legal and ethical issues and concerns that need to be addressed, ranging from privacy and data protection rights, to liability, inequality, discrimination, algorithmic bias and non-transparency, safety, personal autonomy, and identity.

Data protection and privacy

CPS extract, collect, and share vast amounts of data to operate effectively, including sensitive information, especially in the healthcare and financial sectors. This raises privacy concerns.

The areas of interest or concern and possible issues and challenges include:

- Data practices in relation to obtaining and ensuring informed consent
- Ensuring transparency of the process by which the tools collect, process, and make use of personal data, including the terms of use of algorithms
- Materialization of the concept of privacy by design and by default in IoT, CPS, and AI applications
- Concepts of sensitiveness and vulnerability, especially in case of patients and/or people under constant direct observation or surveillance
- Sharing of private individual information collected by IoT devices with other systems and preventing the potential misuse of data
- Data collection and processing during the research, development, and testing of AI-empowered tools and CPS
- Tackling inverse privacy and safeguarding personal data rights, filling the gap between the rights enacted by the GDPR (and its 28 national implementations) and the average understanding of their implications, both from citizens and businesses, as well as their operationalization in IoT and AI settings, where sticky policies, dynamic user consent, and

other developments could be further explored to to develop legally compliant, smart solutions.

- The awareness of the kind of data that is being collected and processes is often scarce, and this diminishes an individual's power and freedom.
- Considering that the human-data relation is asymmetric, individuals can feel powerless in the relation to data, and there is the risk of leading to a loss of control over the access to one's own personal data, including the so-called right to be forgotten, which is considered in the EU as one of the pillars of an individual's control over their personal data.

Dataveillance, social cooling, and dictatorship of data

The risk of dataveillance and intrusive big data practices, due to the availability of more and more data sources and the easier and faster data analysis to generate insights. For instance, for addressing the security challenges posed by the critical infrastructures protection, one's position can be tracked over time, through toolslike the ubiquitous use of Closed-circuit Television (CCTV) circuits, coupled with Global Positioning System (GPS) positioning in mobile devices, as well as the use of credit cards and Automated TellerMachine (ATM) cards for payments and withdrawals.

People's awareness of the possibility of being watched at any moment might result, as shown by field experiments, in the so-called social cooling, which is a side effect of Big Data, and refers to the individuals' attitude to conform to the expected norm, especially considering that our society makes extensive use of scoring systems, where critical life changing opportunities are increasingly determined by such scoring systems, often obtained through opaque predictive algorithms applied to data to determine the value of an individual or social group. This is capable of limiting people's desire to take risks or exercise free speech. Over the long term, these self-censorship, risk aversion, and waiver to the exercise of free speech might "cool down" society and produce increased social rigidity and have an impact on human ability to evolve as an inclusive society, where minority views and vulnerable people are still able to flourish.

In strict correlation with dataveillance and social cooling, another ethical concern arises. Despite the undoubted advantages of digital identities, for example, in terms of possibility to access to online contents and all related services through them, the widespread use of such identities makes possible retrieving from the web publicly available information on an individual and generating insights. This might determine the dictatorship of data, with discriminating effects, based on the representation of a person as portrayed by his/her data, as opposed to the real self. In other words, individuals are treated as mere aggregates of data and are therefore no longer respected.

Data ownership and access aspects

Data ownership, control, and access aspects need to be investigated, as regards the claimed property right on data and information, in relation to human data interaction and interconnected devices, that is the case of data retrieved by the sensors of the objects connected to the Internet of Things, with even more complexity when the information is personal or financial data. Radio-frequency identification (RFID), GPS, and Near Field Communication (NFC) technologies allow to track the geographic place where a person is and his movements from one place to another, without his knowledge.

Ubiquitous devices embedded in daily lives in a IoT landscape, primarily collect data that is about or produced by people, either explicitly produced by themselves (such as location data in case of sharing location while running through wearable accessories) or implicitly inferred by the sensing infrastructures, in cases such as monitoring critical infrastructures. Data collection and processing serves them in a broad range of purposes in everyday life in connection, for instance, with the operation of the critical infrastructures in the health, energy and financial sectors, ranging from personal healthcare to tailored smart city services for energy savings, processing data on energy footprint of an individual's home or other situational context. In relation to the unprecedented amount of data collected by these devices, the fundamental research questions are who owns this data and who might have access to it.

The data ownership claims are also related with the risk of data monopolies and with the theme of asymmetries of powers. In fact, data ownership might be referred also to proprietary data, not only to personal data: data producers have the interest to remain in control of their data and to retain their rights as the original owners and therefore demand for the recognition of ownership claims. However, the legal framework is uncertain and fragmented, and it is difficult to apply legal categories: for instance, data is an intangible good difficult to define, and it is not clear the legal concept itself of data ownership. Many questions arise, such as if the EU's existing law provides sufficient protection for data and, if not, what more is needed; if data is capable of ownership (sui generis right or copyright law); if and which is the legal basis for claims of ownership of data. Meanwhile, there are solutions, such as those reflecting the IDSA Data Sovereignty paradigm, that provide the factual exclusivity of data through flexible and pragmatic tools, combining agile contracting with enabling technological artifacts, able to provide certainty and predictability.

Accessibility of information

In relation to accessibility of information, a cyberattack in IoT employed in critical infrastructures, which makes the system vulnerable, might have a direct influence on people's lives, and this might happen in electric heating systems, bank and insurance IT infrastructures, food distribution networks, hospitals, transport networks, and many others.

Safety, responsibility, and liability

One of the main concerns, especially in relation to AI and human–machine interaction, refers to safety aspects, which are especially important as the complex, intelligent, and self-learning CPS increasingly operate in close proximity to humans. Furthermore, also finding the initial cause and the allocation of liability might prove complex. In case of malfunctioning, who can we hold accountable and responsible for failure? Which is the position of the developer or producer of the CPS?

The theme of liability, including the identification of who is responsible – andliable – for failures and insurance instruments for products/users, is a key issue for CPS systems and their integrated security solutions to reach their full potential, especially in contexts with multiple stakeholders and decisions being made by artificial intelligence.

Increase of Digital divide

Another concern regards the difficulty of some individuals in understanding and accessing services delivered through the use of these new technologies, not being familiar with them.

Algorithmic bias

Another issue pertains to the risk of algorithmic bias and in general the risk of discrimination, manipulation, misuse, and technological determinism.

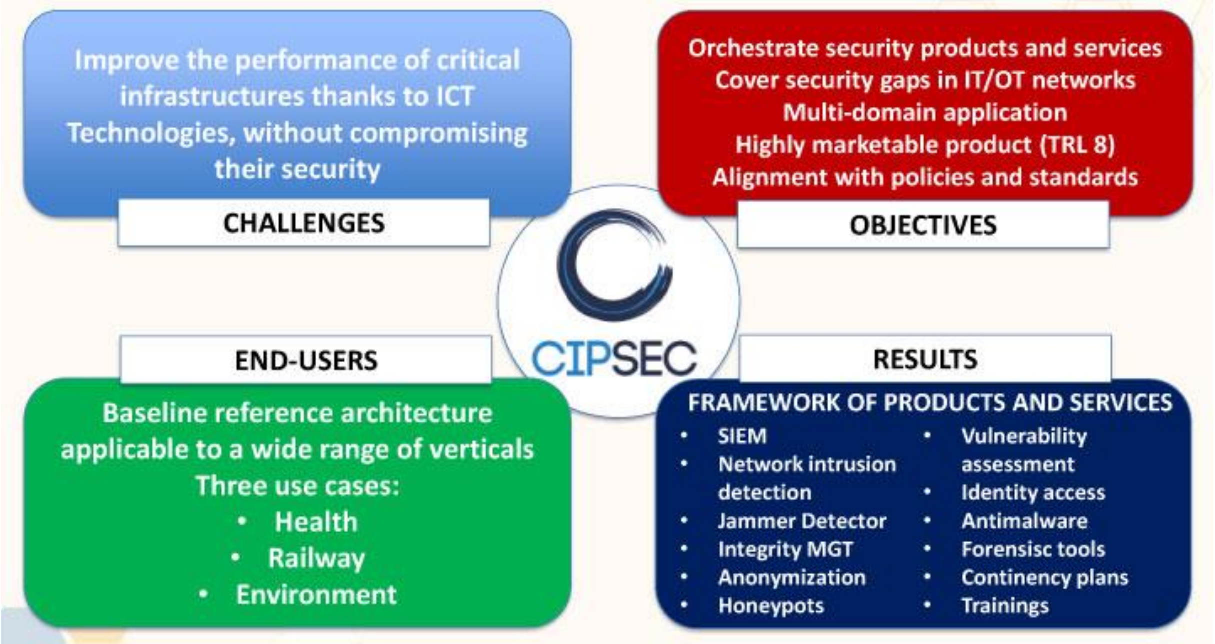

Improve the performance of critical infrastructures thanks to ICT Technologies, without compromising their security
CHALLENGES
Orchestrate security products and services
Cover security gaps in IT/OT networks
Multi-domain application
Highly marketable product (TRL 8)
Alignment with policies and standards
OBJECTIVES
CIPSEC
END-USERS
Baseline reference architecture applicable to a wide range of verticals
Three use cases:
• Health
• Railway
• Environment
RESULTS
FRAMEWORK OF PRODUCTS AND SERVICES
• SIEM
• Network intrusion detection
• Jammer Detector
• Integrity MGT
• Anonymization
• Honeypots
• Vulnerability assessment
• Identity access
• Antimalware
• Forensisc tools
• Continency plans
• Trainings

Fig.5.2: Components of Critical Infrastructures Protection

With a glance at the (critical) future

The world has recently witnessed large-scale security incidents. These incidents indicate that despite the ever-increasing investments in security solutions, industrial organizations and critical infrastructures remain vulnerable against adversarial attacks. Several of the proclaimed vulnerabilities of critical infrastructures stem from their complexity and their cyber-physical nature. Modern critical infrastructures comprise both cyber and physical assets and, as such, can be considered as large-scale cyber-physical systems. Hence, the conventional approach of addressing cybersecurity and physical security separately is no longer effective. On the contrary, more integrated approaches that address the security of cyber and physical assets at the same time are required. Even though the merit of such integrated approaches is acknowledged, their implementation is in its infancy.

Here we have presented integrated (i.e., cyber and physical) security approaches and technologies for some of the most important infrastructures that underpin our societies. Specifically, we presented advanced techniques for threat detection, risk assessment, and security information sharing, based on leading edge technologies like machine learning, security knowledge modeling, IoT security, and distributed ledger infrastructures. Likewise, it has introduced how established security technologies like SIEM, pen-testing, vulnerability assessment, and security data analytics can be used in the context of integrated Critical Infrastructure Protection.

The advent of the fourth industrial revolution (Industry 4.0) is expected to increase the cyber-physical nature of critical infrastructures as well as their interconnection in the scope of sectorial and cross-sector value chains. Therefore, the demand for solutions that foster the interplay between cyber and physical security and enable Cyber-physical Threat Intelligence is likely to explode. In this chapter, we have shed light on the structure of such integrated security systems, as well as on the technologies that will underpin their operation, aiming to raise awareness and enhance the development of future cyber strategies. [52]

A new generation of critical infrastructures to secure

COVID lockdowns and social distancing have exacerbated our dependence on digital, bringing organizations into the critical infrastructure equation that would not have been considered essential before. It is time for governments and organizations to reassess what companies and infrastructures are paramount to national welfare.

While most attacks on enterprises result in a loss of data, financial information, and possibly reputation, attacks on critical national infrastructures can impact society's health and safety.

The European Union puts the power grid, the transport network and information and communications systems among so-called "critical infrastructures," which are crucial to maintaining vital functions in society. The Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. outlines 16 critical infrastructures, including communications, critical manufacturing, emergency services, healthcare and agriculture.

However, according to the World Economic Forum, international and national policies are not keeping up with technological advances. "Digital dependency is changing the nature of international and national security, raising three urgent issues: how to protect critical infrastructure, uphold societal values and prevent the escalation of state-on-state conflicts," argues the WEF Global Risks Report.

Critical infrastructure should be a priority for cybersecurity budgets

According to Mckinsey, if a dedicated national security agency can focus on one aspect of cybersecurity, it should protect the country's critical infrastructure. Critical infrastructure is a prime target for hostile state actors.

"Critical infrastructure typically consists of both information technology and operational technology, which makes it harder and more complicated to protect," argues McKinsey, which recommends that the best-in-class national critical infrastructure protection programs embrace the prioritization of critical sectors and assets, compliance with globally recognized cybersecurity standards, such as the ones defined in the U.S. National Institute of Standards and Technology's Cybersecurity Framework and the adoption of robust governance mechanisms. This may involve additional sector-specific cybersecurity standards.

Leaving the doors open to malevolent actors

Critical infrastructures today are connected to the global digital ecosystem. This has brought with it greater control, easier management, and above all, convenience. But it has also exposed vulnerabilities. Take the recent attack on the water supply of Oldsmar, Florida, which has highlighted concerns about critical infrastructure security. The attackers briefly multiplied the amount of sodium hydroxide used in the city's water supply. The biggest shock about this attack was that it was not complex. It was carried out through software that enables the plant's managers to access the system remotely.

In 2019, the American Water Works Association (AWWA) noted that the resources and capabilities "for preventing, detecting and mitigating cyber risk fall short, particularly given the significance of the threat and potential harm." Two years on, and there is still much progress to make.

As the AWWA points out, much of this is down to fractured organizational infrastructures, shared infrastructures with different levels of risks, and legacy systems. These challenges are not unique to the water industry. Take the municipal computers at Riviera Beach, a suburb of Palm Beach, Florida, which went down in a ransomware attack. The attack disabled communications and forced staff to revert to paper-based systems. The community was so desperate that they opted to pay the hackers $600,000 to restore services.

Digitalization and remote working a considerable challenge

Digitalization and enforced homeworking are significant challenges for those managing critical national infrastructures. According to ABI Research, cybersecurity spending for critical infrastructure is forecast to hit $106 billion this year, a $9 billion increase on 2020. Much of the spending growth is on ensuring that infrastructure operations can be securely monitored remotely.

"There is no denying that secure connectivity has become a key focus, not least with the revelations late last year of the SolarWinds Orion hack, which has brought into sharp focus the need for better vetting of services offered by third-party contractors and remote update processes," explains Michela Menting, Digital Security Research Director at ABI Research.

"The implications for national security are significant, and critical infrastructure operators and governments worldwide are now re-evaluating and reassessing the risks as they relate to remote management," adds Menting.

Fig.5.3: Global spending 2021 for Critical Infrastructure protection

How digital is changing the face of critical national infrastructure

Digital transformation is changing the face of critical national infrastructure as we traditionally know it. Microsoft, Google and Amazon are hyperscale cloud providers, such as providing content and products for consumers that many would consider making them part of the new critical infrastructure. Automating processes is creating greater efficiencies, but with this increasing connectedness comes increased risk.

“In short, we are wrestling with what is critical national infrastructure. Traditionally it has been areas such as power stations, airports and hospitals. Big physical things which governments have always treated differently when it comes to security,” explains Nicolas Arpagian, VP Strategy and Public Affairs at Orange Cyberdefense. “Today’s digital world makes the differentiation even harder. What about Swift bank transfers, electronic trading at the New York Stock Exchange or Amazon and its servers, for example.”

“COVID has accelerated digital transformation process in critical national infrastructure that was already happening and will continue to happen,” adds Arpagian. “We are more and more dependent on digital, and you can’t tease the digital infrastructure apart. The challenge for those working in critical national infrastructure security moving forward is how they can balance the benefits of interconnectivity without significantly opening up risks to cyberattacks.”

One of the most drastic solutions is to move back to analog and away from digitalization in some critical areas where the risks from cyberattacks are too great. In 2019, the U.S. senate went as far as passing a bipartisan cybersecurity bill looking at ways of replacing automated systems with low-tech redundancies to protect the nation’s electric grid from malevolent actors. The aim is to thwart sophisticated nation-state attacks.

Closing the visibility gap

Increased digitalization will force governments to reassess their definition of critical national infrastructure. Across the entire critical infrastructure landscape, greater visibility will be paramount to stopping cyber aggressors from getting into systems without being seen and mounting attacks. “The definition of what is critical is now being tested more than ever before. At the same time, the threats to critical infrastructures are only going to get bigger. Organizations will need to reassess their processes and cyber risks to cope with a more hyper-connected world,” concludes Arpagian. This will require greater collaboration from critical national infrastructure agencies, governments and cybersecurity experts moving forward if we are to keep key critical assets safe in what is an increasingly borderless landscape. [53]

Chapter 06:

Case Study: FinSec

Case Study: FinSec

Securing Critical Infrastructures of the Financial Sector

Security Challenges for the Critical Infrastructures of the Financial Sector

In the era of globalization, the financial sector comprises some of the most critical infrastructures that underpin our societies and the global economy. In recent years, the critical infrastructures of the financial sector have become more digitalized and interconnected than ever before. Advances in leading edge ICT technologies like Big Data, Internet of Things (IoT), Artificial Intelligence (AI), and blockchains, coupled with a wave of Financial Technology (FinTech) innovations, has resulted in an explosion of the number of financial transactions. Furthermore, the critical assets of financial institutions are no longer only physical (e.g., bank branches, buildings, ATM machines, computer rooms), but rather comprise many different types of cyber assets (e.g., computers, networks, IoT devices) as well.

The increased digitization and sophistication of the critical infrastructures of the financial sector has also raised the importance of cybersecurity in the financial sector. Nevertheless, despite significant investments in cybersecurity, recent large-scale incidents demonstrate that financial organizations remain vulnerable against cyberattacks. As a prominent example, the fraudulent SWIFT (Society for Worldwide Interbank Financial Telecommunication) transactions cyberattack back in February 2016 resulted in $81 million being stolen from the Bangladesh Central Bank. Likewise, the famous "WannaCry" ransomware attacked financial institutions and had a significant adverse impact on Russian and Ukrainian banks. Another major attack took place in 2017, when a data breach at Equifax created a turmoil in the global markets and affected more than 140 million consumers. In addition to these major incidents, smaller scale attacks against financial institutions happen daily. While most of them are confronted, there are still many cases where these attacks affect the operations of banks and financial institutions, as well as their customers. For instance, back in February 2019,Metro bank was named as a victim of a cyberattack that targeted the codes sent via text messages to customers, as part of the transactions' verification process. A small number of customers of the bank were potentially affected, while the bank reported the issue to relevant security authorities. During the same month, the Bank of Valletta had to shut down all its operations after hackers broke into its systems and moved e13 million into foreign accounts. Specially, the bank shut down all the bank's functions, including branches, ATMs, mobile banking, as well as email services and the website of the bank.

In general, the financial sector suffers from security attacks (notably cybersecurity attacks) more than other sectors. During 2016, financial services customers suffered over 60% more cyberattacks than customers in any other sector, while cyberattacks against financial services firms increased by over 70% in 2017. Moreover, a 2018 analysis from the IMF (International Monetary Fund) estimated that emerging cyberattacks could put at risk a significant percentage of the financial institutions' profits, which ranges from 9% to even 50% in worst-case scenarios.

In response to the rising number of attacks against financial institutions and their cyber assets, financial sector organizations are allocating more money and effort in increasing their cyber resilience. According to Netscribes, the global cybersecurity market for in financial services is expected to expand at a CAGR (Compound Annual Growth Rate) of 9.81%, leading to a global revenue of USD 42.66 billion by 2023. Other studies reflect a similar estimation, e.g., a Compound Annual Growth Rate (CAGR) of 10.2% during 2018–2023 and a cybersecurity market growth from USD 152.71 billion in 2018 to USD 248.26 billion by 2023.

This section introduces the main challenges that are associated with physical security and cybersecurity for the critical infrastructures of the financial sector. The chapter presents recent security incidents against financial institutions as a main motivation behind integrated security. Moreover, it also outlines the main building blocks of integrated security solutions for the financial sector.

The main challenges can be listed as follows:

1. Limited Integration Between Physical Security and Cybersecurity

Even though the critical infrastructures of the financial sector comprise both physical and cyber assets, physical security and cybersecurity are still handled in isolation from one another. Specifically, cybersecurity and physical security processes in financial organizations remain “siloed” and fragmented. The latter fragmentation concerns both the technical and the organizational levels, i.e., physical and cybersecurity are handled by different security technologies and different security teams. For instance, physical security systems such as CCTV (Closed Circuit Television) systems, intelligent visual surveillance, security lighting, alarms, access control systems, and biometric authentication are not integrated with cybersecurity platforms like SIEM (Security Information and Event Management) and IDS (Intrusion Detection Systems). Likewise, processes like vulnerability assessment, threat analysis, risk mitigation, and response activities are carried out separately by physical security officers and cybersecurity teams.

This “siloed” nature of systems and process leads to several inefficiencies, including:

- Inefficient security measures that consider the state of the cyber or the physical assets alone, instead of considering the global security context. There are specific types of security attacks (e.g., ATM Network attacks), where security processes like risk assessment and mitigation should consider the status of both types of assets.
- Inability to cope with combined cyber/physical attacks, which are set to proliferate in the years to come. For example, a physical security attack (e.g., unauthorized access to a device or data center) is nowadays one of the best ways to gain access to internal resources and launch a cybersecurity attack as an insider.
- Increased costs as several processes are duplicated and overlapping. In this context, an integrated approach to security could help financial organizations streamline their cyber and physical security resources and processes, towards achieving greater efficiencies at a lower cost.

2. Poor Stakeholders' Collaboration in Securing Financial Services

In an era where financial infrastructures are more connected than ever before, their vulnerabilities are likely to impact other infrastructures and systems in the financial chain, having cascading effects. In this context, stakeholders' collaboration can be a key towards identifying and alleviating issues in a timely manner. However, collaboration is currently limited to exchanging data as required by relevant security regulations and do not extend to join security processes like (collaborative) risk assessment and mitigation. Information sharing between stakeholders of the financial supply chain is a first and prerequisite step to their collaboration in security issues. In the financial sector, the Financial Services Information Sharing and Analysis Center (FS-ISAC) has been established, as an industry forum for sharing data about critical cybersecurity threats in the financial services industry. FS-ISAC provides its members with access to threat reports with tactical, operational, and strategic levels of analysis for a greater understanding of the tools, methods, and actors targeting the sector. This allows them to better mitigate risk. Information sharing (e.g., as implemented by FS-ISAC) is a foundation for collaboration in security processes like joint risk scoring for assets and services that are part of the financial services supply chain. Such IT-supported collaborative workflows have been demonstrated in many sectors, including the financial sector. Nevertheless, there are still trust barriers to information sharing and collaboration, especially when data must be shared across private enterprises. Recent advances in IT technologies like blockchain and cloud computing could facilitate the sharing of information and the implementation of collaborative security functionalities.

3. Compliance to Stringent Regulatory Requirements and Directives

Financial institutions are nowadays faced with a need of complying with a host of regulations, which has a severe impact on their security strategies.
For example:

- The Second Payment ServicesDirective (PSD2): Compliance to the 2nd Payment Services Directive (PSD) demands for banks to be able to interact with multiple Payments Services Providers (PSPs) in the scope of an API-based Open Banking approach. This raises more cybersecurity concerns and asks for strong security measures like pentesting and vulnerability assessment on the APIs.

- The General Data Privacy Regulation (GDPR): As of May 2018, financial organizations have to comply with the General Data Privacy Regulation (GDPR), which asks for stricter and effective security measures for all assets where personal data are managed and exchanged. Note that GDPR foresees significant penalties for cases of non-compliance, which is one of the reasons why financial organizations are heavily investing in security systems and measures that boost their compliance.

- The Network Information Systems (NIS) Directive [i.e., Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016]. The NIS Directive prescribes security measures for the resilience of the IT systems and networks that support Europe's critical infrastructures, including infrastructures in the financial sector. The prescribed measures include the establishment of risk-driven security polices, as well as the collaboration between security teams (including CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams) at national and international level. The directive defines entities in the Financial services as 2 of the 7 critical sectors and called the member states upon actions to protect and guarantee the availability of their services. Financial organizations are therefore investing in the implementation of the NIS Directive's mandates.

- The EU legislative framework for electronic communications (EU Directive 2009/140/EC) was reformed in 2009 and Article 13a introduced into the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC). Article 13a concerns security and integrity of electronic communications networks and services. The first part of Article 13a requires that providers of networks and services manage security risks and take appropriate security measures to guarantee the security and integrity of these networks and services. The second part of Article 13a requires providers to report significant security breaches and losses of integrity to competent national authorities, who should report about these security incidents to ENISA and the European Commission annually.

4. The Need for Continuous Monitoring of Transaction and Limited Automation

Financial organizations are nowadays required to secure their infrastructures in a fast moving and volatile environment, which is characterized by a proliferating number of threats and vulnerabilities that are likely to emerge and affect critical infrastructures. Hackers and adversaries are continually taking advantage of leading-edge technologies in order to exploit the rising number of vulnerabilities of the physical and cyber assets of the critical infrastructures. Therefore, it is not practical, and in several cases not possible, to manually carry out all security and protection tasks such as detection, monitoring, patching, reporting, and security policy enforcement activities.

In this context, one of the main challenges faced by the security officers of financial organizations is the poor automation of security functions. To confront this challenge, there is a need for solutions that offer immediate mitigation actions, as well as (semi)automated enforcement of security policies. To this end, financial organizations can take advantage of recent advances in technologies like Artificial Intelligence, Machine Learning and automated orchestration of security functions.

The lack of significant automation is also a setback to fulfilling one of the main security requirements of the financial institutions, which is the ability to monitor transactions without interruptions, i.e. on a 24/7 basis. This is challenging as it requires significant amounts of human resources, including cybersecurity experts and members of security teams. However, it is an essential requirement given that adversarial attacks can happen at any time during the day. Some of the recent attacks against the SWIFT system might have been avoided should a close 247 monitoring of transactions and security events was in place.

5. Lack of Flexibility in Coping with a Proliferating and Dynamic Number of Threats

In addition to automation, security officers of financial organizations are very keen on being flexible when dealing with the proliferating number of threats, including the emergence of several new cyber threats every year. Hence, security departments must be able to deploy new security functions (such as patches or protection policies) very frequently, e.g., daily or even several times per day. In this direction, financial organizations could benefit from latest developments in software engineering practices and methodologies such as the DevOps (Development and Operations) paradigm. Recent research initiatives are exploring the use of DevOps in security systems engineering, which is sometimes called DevSecOps.

6. Digital Culture and Education

The human factor plays a significant role in alleviating cybersecurity attacks. Proper digital culture and education can provide a sound basis for complying with the mandates of security policies, while avoiding mistakes that could open backdoors to malicious parties. Nevertheless, there is currently a proclaimed gap in digital knowledge in general and specifically in cybersecurity. This holds true for physical security teams as well. Hence, the cybersecurity knowledge gap hinders the implementation of integrated security strategies, while being a setback to the cyber resilience of modern financial institutions.

Solution Guidelines

For the above mentioned challenges, there are some key factors that could possibly enhance the cybersecurity posture and mitigate relevant risks.

- *Structuring and Developing Integrated Security Systems*

The design and implementation of integrated security policies requires rethinking of the architecture of the various security platforms, to a direction that considers physical information and devices. Thus, there is a need for new security architectures. The latter can take advantage of the recent advances in Industry 4.0 and the Industrial IoT, including relevant reference architectures such as the Industrial Internet Security Framework (IISF) of the Industrial Internet Consortium.

- *Integrated Security Knowledge Modeling*

There is need for extending existing security models and format, with constructs that enable them to represent integrated security knowledge. State-of-the-art knowledge bases for cybersecurity consolidate several sources of knowledge for Cyber Threat Intelligence (CTI), such as:

- ✓ CPE (Common Platform Enumeration), which is a structured naming scheme for IT software, systems, and packages.

- ✓ CWE (Common Weakness Enumeration), which lists common software's vulnerabilities.
- ✓ CAPEC (Common Attack Pattern Enumeration and Classification), which lists common attack patterns on software and their taxonomy.
- ✓ CVE (Common Vulnerabilities and Exposures), which lists all publicly known cybersecurity vulnerabilities and exposures.

- ▪ *Automation and Flexibility*

To increase the automation of security processes, financial organizations are nowadays offered with the opportunity of leveraging Machine Learning (ML) and Artificial Intelligence (AI) on large volumes of security data. AI and ML algorithms can boost not only the intelligence and proactiveness of the security processes, but also their automation as well. Specifically, they can automate security and surveillance processes through obviating manual surveillance and tracking of security information streams (e.g., from CCTV systems). Furthermore, they can boost the continuous, 247, monitoring of financial systems and transactions, through lowering the human resources needed for the surveillance tasks.

- ▪ *Information Sharing and Collaboration Across the Financial Services Supply Chain*

Interconnected enterprises are vulnerable to attacks that originate from attacks against other stakeholders in the value chains where they participate. Specifically, financial organizations should not only consider the status of their assets and infrastructures. Rather, they should keep an eye on the status of interconnected infrastructures as well. A potential vulnerability in a connected infrastructure can influence other stakeholders in the supply chain.

Moreover, to address supply chains security, stakeholders had better collaborate in their security processes. As a prominent example, enterprises could engage in collaborative assessments of the risk factors that are associated with their assets. Such processes can be empowered by the automated and seamless sharing of information across stakeholders of the supply chain.

Currently, financial organizations share such information as part of regulatory mandates and in the scope of their participation in initiatives like the Financial Services Information Sharing and Analysis Center (FS-ISAC). Nevertheless, the level of security information sharing is still quite low. Lack of trust is one of the reasons that make organizations reluctant to share security information. In recent years, distributed ledger technologies (i.e., blockchain technologies) are explored as a means of sharing information across financial organizations in a decentralized and trustworthy way.

- *Regulatory Compliance Technologies*

To confront the challenges of regulatory compliance, financial organizations need technologies that facilitate the implementation of relevant technical measures. As a prominent example, data anonymization and data encryption can be used to facilitate adherence to GDPR principles. Likewise, SIEM systems can be used to collect and analyze information about access, transfer, and use of data in an organization, towards identifying potential data breaches.

- *Security-by-Design and Privacy-by-Design*

Beyond regulatory compliance, financial organizations need to adopt new principles regarding the design and implementation of their applications. Specifically, they are expected to adhere to the security-by-design and privacy-by-design principles. The latter should become the preferred path of the software design and development cycle for financial organizations like banks. Likewise, traditional serialized development approaches should be updated towards more flexible and responsive approaches that involve the design and implementation of security controls early in the application development life cycle. Given that privacy-by-design is referenced in the text of the GDPR regulation, it can serve as a basis for achieving GDPR compliance as well.

- *Security Education and Training*

Financial organizations should heavily invest in security education and training with a twofold objective: First to close the knowledge gap about cybersecurity issues, and second towards engaging the organization's personnel in IT security, regardless of their background and security knowledge. Such measures will help ensuring that employees are no longer one of the weakest links in the security value chain. Along with investments in training and education, financial organizations should be investing in IT security awareness campaigns.

The critical infrastructures of the financial sector are increasing in size, complexity, and sophistication, while at the same time comprising both cyber and physical elements. At the same time, financial organizations are obliged to comply with many and complex regulations and directives about security, privacy, and data protection. As a result, financial enterprises must deal with increased security vulnerabilities and threats in a rapidly evolving regulatory environment. To this end, they are increasing their investments in cybersecurity and its intersection with physical security. Despite the rising investments, they remain vulnerable to security and privacy threats, as evident in several notorious incidents that have occurred during the last couple of years.

In order to properly secure the critical infrastructures for the financial sector, there is a need for new integrated approaches that addresses physical and cybersecurity together rather than dealing with them in a "siloed" fashion. To this end, financial organizations should benefit from the capabilities of emerging technologies like Big Data and AI analytics for security monitoring and automation, while at the same time leveraging the flexibility of the DevOps paradigm that provides opportunity for frequent changes to security measures and policies (e.g., patching on a daily basis). Likewise, integrated approaches to security knowledge modeling and information sharing can be employed. Following chapters of the first part of the book will illustrate novel technologies for cyber-physical threat intelligence, which address several of the security challenges that are currently faced by financial organizations.[54-60,]

The FINSEC Project

The Project

FINSEC is a security innovation project funded by the European Commission under the H2020 project. FINSEC, (*Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures*), is a flagship project which aims to develop, demonstrate and bring to market an integrated, intelligent, collaborative and predictive approach to the security of critical infrastructures in the financial sector. To this end, FINSEC aims to introduce, implement and validate a novel reference architecture for integrated physical and cyber security of critical infrastructures, which will enable handling of dynamic, advanced and asymmetric attacks, while at the same time boosting financial organizations' compliance to security standards and regulations. As a result, FINSEC will provide a blueprint for the next generation security systems for the critical infrastructures of the financial sector.

FINSEC considers the critical infrastuctures of the financial sector as large-scale cyber-physical systems, which must be protected based on a holistic approach that considers both physical security risks and cyber-security risks, along with their interrelationships, interactions and cascading effects across the financial services supply chain.

FINSEC introduces a novel, standards-based Reference Architecture (RA) for combined cyber and physical security of critical infrastructures in the financial services industry. This reference architecture is integrated, as it considers critical infrastructures as cyber-physical systems, while integrating technologies and measures for cyber and physical security. It is driven by standards for cyber security and physical security in general (e.g. ISO 27000 and ISO 28000) and financial services standards (e.g. ISO/TC 68/SC 2). Mechanism for intelligent and adaptive monitoring and data collection will be difined taking in account the physical-cyber security context.

The project has a three-layer approach:

- Integrated

  FINSEC's unified approach is motivated by the need to reduce the fragmentation of the security systems and teams in financial organizations, while at the same time streamlining their activities and gaining extra efficiencies from possible correlations between cyber security and physical security incidents

- Predictive

FINSEC's predictive approach is based on the collection and analysis of security related data as a means of anticipating security incidents before they actually occur. This apporach enables financial organisations to plan for mitigations activities earlier and in the proper context

- Collaborative

FINSEC's collaborative approach is based on stakeholders' collaboration across the financial services supply chain in the identification, assessment and mitigation of risks, including their cascading effects. FINSEC provides tools based on Blockchain technology to facilitate information exchange.[67]

In the following section, comes a description of the most common standards and regulations, applicable in the FinSec sector. Consequently, follows a reference to some methods and techniques, based on machine learning and deep learning that are proposed by FINSEC project as state-of-the-art tools for predictive security analytics.

FinSec Applicable Standards and Regulations

Financial regulations, supervising authorities and regulatory bodies

Markets in Financial Instruments Directive II

MiFiD II MiFiD II encapsulates both legislations on Markets in Financial Instruments Directive ("MiFID") and the Regulation on Markets in Financial Instruments and Amending Regulation ("MiFIR"). MiFiD has been generated by the European Commission and it relates to a Europe-wide legislative framework for regulating the operation of financial markets in the European Union. The framework was put in force in January 2018. It represents a major overhaul of the existing law, building on and extending the scope of the first MiFID. MiFID regards the framework of trading venues/structures in which financial instruments are traded, whereas MiFIR focuses on regulating the operation of those trading venues/structures, looking to processes, systems and governance measures adopted by market participants and to their future supervision.

Scope of the Regulation.

The legislation aims to establish a safer, sounder, more transparent and more responsible financial system. More specifically, MiFID II includes objectives which are relevant to Fintech and Financial Security, including algorithmic trading activities, which are enhanced by MiFID II as the directive introduces trading controls for algorithmic trading activities, which have led to much increased speed of trading and thus the possibility of causing systemic risks. Investment firms that are providing direct electronic access to trading venues are enforced to have in place systems and risk controls such that they could effectively prevent trading that may contribute to a disorderly market or involve market abuse.

Impact on financial service providers.

MiFID II is widely viewed as significant legislation which will fundamentally reshape European financial markets. For the financial sector and trading in particular, one of the main MiFiD II effects is that traders are provided with enhanced transparency as the system enforces the brokers to increase the information reported. It also has a major impact on algorithmic trading, as it mandates the testing of algorithms and the need to add new tags to precisely identify the origins of an order.

Payments Services Directive (PSD 2) - Directive 2015/2366

The revised Payment Services Directive (PSD2) enhances innovation potential, competition and efficiency in electronic markets. It offers consumers more and better choice in the EU retail payment market. At the same time, it introduces higher security standards for online payments. The directive's deadline to transpose PSD2 in member states was January 2018, whereas it is expected to be put into force in April 2019. Reflecting the challenges of digital economy, the actions of all the active members of the payments value chain are affected.

Scope of the Regulation.

PSD2 will bring changes with respect to the range of transactions, the scope of stakeholders, liability and information and security assessment. In particular, PSD2 will extend the EU's regulatory framework on transactions and will also enhance the Payment Service Provider (PSP) with an additional category, the Third-Party Service Providers (TPSPs) – including Account Information Service Providers (AISPs) and Payment Information Service Providers (PISPs). AISPs will provide a complete view of the payer's accounts to any relevant financial institution. Information Service Providers (ISPs) will connect the payer's and the payee's banking platforms.

To enable the operation of TPSPs, financial institutions will be required to fulfil account information and payment initiation requests by providing TPSPs with the necessary information via Application Programming Interfaces (APIs)—given that they will be authorised by the payer. In this way, the directive will allow the payers to gain additional protection for the case of any incorrectly executed payments as payments will need to be processed through "strong customer authentication" and hence it will be impossible, for information related to the payer that will be exchanged through APIs, to be retained for any other purposes than completing the payment.

Impact on financial institutions and service providers.

Financial institutions will have to ensure their compliance with additional information and technology requirements. This will be relevant to setting up APIs such that it will encapsulate specific monetised services, existing margins, and simplified and optimised infrastructure. PSD2 will also contribute on setting up the mechanisms that will foster strong customer authentication. In the case of Third Party Service Providers (TPSPs) PSD2 will enable TPSPs to extend their consumer base as consumers are expected to increase their interest in initiating their payments through TPSPs. TPSPs will have to as a payment institution with the local regulator, set up risk and control frameworks, comply with all relevant reporting obligations, and perform AML and KYC controls.

PCI DSS and PCI 3DS

The Payment Card Industry Data Security Standard (PCI DSS) issued by the Payment Card Industry Security Standards Council, is a worldwide information security standard, for securing card payments. It was originally designed for the handling of credit card information by payment companies such as Visa and MasterCard and its main purpose is to prevent credit card fraud. Among the main goals of the standard is to ensure that 'cardholder data' as the full Primary Account Number (PAN) or the full PAN along with Cardholder name, the expiration date, the service code and sensitive authentication data (full magnetic stripe data, CAV2, CVC2, CVV2, CID, PINs, PIN blocks) are protected.

The Three-Domain Secure (3DS) is a messaging protocol that enables consumers to authenticate themselves with their card issuer when making e-commerce purchases. The additional security layer helps prevent unauthorized transactions where the "Card is not Presented" (e-commerce transactions also called CNP transactions in the industry) and protects the merchant from fraud.

Scope

The PCI DSS is very specific to the payment card sector and it is relevant to the payment functions of business systems. Compliance of PCI DSS is imposed by Credit card processors to card issuers and merchant banks. The standard introduces a number of requirements, which include the establishment of an effective operational and security risk management framework; processes that detect, prevent and monitor potential security breaches and threats; risk assessment procedures; regular testing; and processes that raise awareness to Payment Service Users on security risks and risk-mitigating actions. Additionally, specific Vulnerability Scans must be conducted by a PCI Approved Scanning Vendor (ASV) at Payment gateways.

Impact on financial services.

The requirements of the directive aim to establish that any physical access to data or systems that house cardholder data should be appropriately restricted. These requirements have significant impact on the protection expected from cyber-physical threats.

European Banking Authority III

The European Banking Authority (EBA) is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector.

As part of its task of establishing consistent, efficient and effective supervisory practices across the EU and ensure uniform application of Union law, the European Banking Authority (EBA) issues regulatory guidelines and recommendations in its fields of competence. Regulation (EU) No 1093/2010 establishing the EBA requires that competent authorities and financial institutions make every effort to comply with the EBA guidelines and recommendations (Article 16).

Scope of the regulation: The Article 9(2) of the EBA's Founding Regulation mandates the Authority to monitor new and existing financial activities. This obligation extends to all areas of the EBA's competence, including the field of activities of credit institutions, financial conglomerates, investment firms, payment institutions, and electronic money institutions.

Regulation for insurance security

The directives affecting the operation of the insurance sector are presented below, along with the guidance from the national and European supervision authorities.

IVASS is the Italian Institute for the Supervision of Insurance. It pursues the stability of the financial system and markets. National regulation 38/2018 is particularly important and imposes a series of obligations for the insurance companies, impacting the following functions: Board of Directors; Corporate Bodies; Internal Controls System; Risk Management System; Fundamental SII Functions (Risk Management, Compliance, Actuarial Function, Internal Audit); ICT / Cyber security; Reinsurance; Capital Management; Professionalism, integrity and independence; Compensation; Outsourcing; Corporate Group Governance.

With regard to the strategic Information and Communication Technology plan, the definition and approval by the Board of a corporate governance policy, including data quality and cyber security profiles, are of particular importance. The regulation states that IVASS will receive notification of any serious IT security incident. The European Insurance and Occupational Pensions Authority (EIOPA) is a European Agency commissioned aiming to monitor and identify trends, potential risks and vulnerabilities stemming from the micro-prudential level, across borders and across sectors. Its core responsibilities are to support the stability of the financial system, transparency of markets and financial products as well as the protection of policyholders, pension scheme members and beneficiaries. Solvency is a Directive in European Union law that codifies and harmonises the EU insurance regulation. The framework states that insurance organizations must guarantee business continuity through the development of business continuity plans which should include cyber security implementation measures.

European Central Bank (ECB) cyber incident reporting regime

The ECB cooperates with EU national central banks to ensure the confidentiality, availability and integrity of data. Its aim is to protect against cyber-attacks, limit the impact of a data breach and ensure that the bank system continues to operate. ECB collaborates with other EU institutions such as the EU Computer Emergency Response Team (CERT-EU); CERT EU warns its members about new threats, provides testing and offers advisory services. The ECB facilitates exchanges of security information among a global network of central banks and international financial organisations.

The ECB confirmed that the mandatory cyber incident reporting requirements do not stem directly from a specific EU directive (e.g. NIS) or regulation. Instead, it states that the requirements were developed by its Governing Council, using requirements set out in two previous regulations, including the REGULATION OF THE EUROPEAN CENTRAL BANK (EU) No 795/2014 of 3 July 2014, on oversight requirements for systemically important payment systems.

The ECB's responsibility for determining the security of network and information systems or the notification of cyber-security incidents, is indeed recognized by the NIS Directive (presented in section 3.3 of the report). The NIS Directive specifically allows the exemption of organizations who might otherwise be classed as "operators of essential services" from the NIS regime, if there are already "Union legal acts" that set out sector-specific security requirements. It is clearly indicated that the sector specific requirements "are at least equivalent in effect" to the obligations set out in the NIS Directive.

The ECB has not however (as of the time of writing of this report) published the cyber incident reporting requirements that it has issued for the banks, as the documents are deemed confidential.

Information Security Standards and Directives

ISO/IEC 27000 standards' family

The ISO/IEC 27000-series comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The series provides best practice recommendations on information security management - the management of information risks through information security controls - within the context of an overall Information security management system (ISMS), similar in design to the management systems for quality assurance (the ISO 9000 series), environmental protection (the ISO 14000 series) and other management systems. The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT/technical/cyber-security issues. It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information risks, then treat them (typically using information security controls) according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information risk and security, the ISMS concept incorporates continuous feedback and improvement activities to respond to changes in the threats, vulnerabilities or impacts of incidents.

Scope of the Standard.

ISO/IEC 27000 describes the fundamentals on information technology with respect to security techniques and information security management systems. In particular, the ISO/IEC 27000 provides additional support to the financial industry to set up an appropriate information security management system for the provisioning of their financial services, while giving more confidence to their customers.

The adoption of the standard is not universal in the finance and banking sector, although the compliance of financial organisations is recommended. The benefits of implementing an ISMS will primarily result from a reduction in information security risks (i.e. reducing the probability of, and/or impact caused by, information security incidents). However, a supplement to the ISO/IEC 27001 family of standards, ISO/IEC TR 27015: 2012 "Information technology – Security techniques – Information security management guidelines for financial services" (more details at section 3.2), provides sector-specific guidance for the financial sector with respect to information security of assets, as well as information processing for organizations providing financial services, in order to support the information security management of their assets and processed information. Financial services organisations process sensitive financial and customer data and ISO/IEC 27002:2005 can contribute by providing additional guidance to the information security of financial services organisations such that they can effectively manage their information security risks.

The ISO 27000 series includes a sequence of standards with respect to some particular areas of information security. In particular, ISO/IEC 27001 regards information security management and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of information security controls, customized to the needs of individual organizations or parts thereof. ISO/IEC 27001 provides normative requirements for the development and operation of an Information System Management Systems, including a set of controls for the control and mitigation of the risks associated with the information assets, which the organization seeks to protect by operating its Information System Management Systems. Organizations operating an Information System Management Systems may have its conformity audited and certified.

ISO/IEC 27001 formally defines the mandatory requirements for an Information Security Management System (ISMS). However, ISO/IEC 27002 provides a code of practice certification standard with respect to Information Security Management System (ISMS). It outlines recommendations on information security controls such that information security control objectives arising from risks to the confidentiality, integrity and availability of information can be addressed. Organizations that adopt

ISO/IEC 27002 are required to own information risks, clarify their control objectives and apply suitable controls (or indeed other forms of risk treatment) using the standard for guidance.

The standard is structured logically around groups of related security controls. Many controls could have been put in several sections but, to avoid duplication and conflict, they were arbitrarily assigned to one and, in some cases, cross-referenced from elsewhere. For example, a card-access-control system for, say, a computer room or archive/vault is both an access control and a physical control that involves technology plus the associated management/administration and usage procedures and policies. This has resulted in a few oddities (such as section 6.2 on mobile devices and teleworking being part of section 6 on the organization of information security) but it is at least a reasonably comprehensive structure. It may not be perfect but it is good enough on the whole.

ISO/IEC 27015:2012 Information technology - Security techniques – Information security management guidelines for financial services

Continuous developments in the information technology have led to an increased reliance by organizations providing financial services on their assets processing information.

Consequently, management, customers and regulators have heightened expectations regarding an effective information security protection of these assets and of processed information.

Whereas ISO/IEC 27001:2005 and ISO/IEC 27002:2005 address information security management and controls, they do so in a generalized form. Organizations providing financial services have specific information security needs and constraints within their respective organization or while performing financial transactions with business partners, which require a high level of reliance between involved stakeholders.

ISO/IEC 27015:2012 is a technical report which is intended, as a supplement of the ISO/IEC 270xx family of International Standards, to be used by organizations providing financial services. In particular, the guidance contained in this technical report complements and is in addition to information security controls defined in ISO/IEC 27002:2005.

ISO/IEC 27033 - Information technology — Security techniques — Network security

ISO/IEC 27033 aims to provide guidance on the management, operation and use of information system networks, and their inter-connections from a security perspective. In particular, it provides advice on implementing the network security controls of ISO/IEC 27002. It includes an overview of network security and related definitions, as well as advice on identifying and analyzing network security risks and then define network security requirements. It also provides guidance on how to develop good quality technical security architectures. This standard is applicable to the security of networked devices and the management of their security, network applications/services and users of the network. This is additional to the security of information that is being transferred and is more relevant to network security architects, designers, managers and officers.

ISO27034 - Information technology — Security techniques — Application security

ISO/IEC 27034 is relevant to information security with respect to the design and development or procurement, implementation and use of application systems. In particular, it provides guidance on specifying, designing/selecting and implementing information security controls. This includes all aspects including the identification of information security requirements, protection of information accessed by an application and prevention of unauthorized use and/or actions of an application. The standard complements other systems development standards and methods without conflicting with them. Guidance provided in this standard is more relevant to business and IT managers, developers and auditors, and end-users. Its objectives is to ensure that computer applications deliver the desired or necessary level of security in support of the organization's Information Security Management System and addressing security risks arising.

ISO/IEC 27038 - Information technology — Security techniques — Specification for digital redaction

The standard is relevant to removal of confidential (or sensitive in general) content from documents as well as indicating the location in the document where content was removed. In other words, this standard regards redaction, defined as the "permanent removal of information within a document". It specifies, redaction requirements and describes the process for redaction, reflects on techniques for conducting digital redaction on documents as well as defines the requirements for tools in charge of testing that digital reduction was successfully and securely done. It also provides guidance on keeping records so as to justify or explain redaction decisions. Although the standard regards information redaction, it does not encapsulate database redaction.

ISO/IEC 27041 - Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative methods

ISO/IEC 27041 is relevant to the mechanisms employed to ensure the adequacy of the methods and processes followed to investigate Information Security Incidents. The standard provides guidance on best practices with respect to the elicitation analysis of functional and non-functional requirements relating to an Information Security (IS) incident investigation, provide guidance and describe the use of validation means to indicate the suitability of processes involved in the investigation. It also aims at the delivery of evidence that implementations of methods meet the requirements and guide the assessment the levels of validation required and also provide advice on incorporating how to external testing and documentation in the validation process. It also reflects on vendor and third-parties with respect to the testing approaches that can be employed to assist this assurance process.

ISO/IEC 27042 - Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence

This standard emphasizes on the forensics process. It particular, it focuses on providing guidance on the process of analyzing and also interpreting digital evidence. It includes insights on how evidential controls such as the maintenance of chain of custody or scrupulous documentation is managed. Additionally, it focuses on analytical and interpretational processes so as to ensure their integrity in case different investigators are working on the same digital evidence. It also provides guidance on the selection and use of forensic tools, plus proficiency and competency of the investigators.

ISO/IEC 27043 - Information technology — Security techniques — Incident investigation principles and processes

ISO/IEC 27043 provides guidance on idealized models with respect to common incident investigation processes. It reflects on the processes followed for investigating various incident scenarios involving digital evidence. It captures the processes from pre-incident preparation to providing returning evidence in order for it to be stored and disseminated. It also provides dissemination as well as any general advice and caveats on such processes. It provides an overview of all incident investigation principles that could be applicable to various kinds of investigations, however, it does not focus on proscribing particular details to specific categories or groups of incident.

Directive on security of network and information systems (NIS Directive)

The Directive on security of network and information systems (NIS Directive), provides legal measures to boost cyber-security in the EU. The directive requires Operators of Essential Services (OESs) to implement appropriate and proportionate security measures to achieve the outcomes set out by the NIS principles and notify the relevant national authorities of serious incidents and events.

The NIS Directive is the first EU-wide legislation on cyber-security. It aims to achieve harmonization of the levels of protection of the Network and Information Services (the internet as a whole).

The NIS Directive needs to be transposed into national legislation by 9 May, 2018. The deadline for the identification of operators of essential services by 9 November, 2018, i.e. 21 months after the deadline.

Scope

Financial services and financial market infrastructure providers (including trading venues and central counterparties) are included in the scope of the new NIS Directive — in Article 3, they are specifically defined as “Operators of Essential Services” (OES). OES are private businesses or public entities with an important role for the society and economy. According to NIS, the entities have several obligations in case of a cyber-attack. The OES have to take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of networks and information systems that they use in their operations (according to Article 14). They need to prevent and minimize the impact of cyber incidents. Serious incidents need to be notified to the relevant national authority (i.e. Computer Security Incident Response Teams) that each EU country will need to set up. An incident can be classified as “significant” depending on the number of people affected by it, the duration of the incident, and the geographical spread (for example, whether the incident affects services in several branches of a bank). The final text places a great deal of responsibility on the essential services providers. For example, even if a financial services company has outsourced the cloud computing services to a third party, the delegating entity still holds the main responsibility of any cyber attack data breach.

It is understood in NIS that harmonization in the banking sector has been achieved. According to the statutory statements of the directive, "*Regulation and supervision in the sectors of banking and financial market infrastructures is highly harmonized at Union level, through the use of primary and secondary Union law and standards developed together with the European supervisory authorities*". It is understood that "*Within the banking union, the application and the supervision of those requirements are ensured by the single supervisory mechanism*" and thus the requirements of NIS have been mostly reached or even exceeded by the banking and financial infrastructure.

Impact on banking and financial services.

The approach towards the banking sector considers the particularities of the business environment. The notification about incidents in the banking sector is indicated to be specified by member states: "*requirements for notification of incidents are part of normal supervisory practice in the financial sector and are often included in supervisory manuals. Member States should consider those rules and requirements in their application of lex specialis*". Furthermore, as noted by the European Central Bank in its opinion of 25 July 2014 , "*this Directive does not affect the regime under Union law for the Eurosystem's oversight of payment and settlement systems. It would be appropriate for the authorities responsible for such oversight to exchange experiences on matters concerning security of network and information systems with the competent authorities under this Directive*".

NIST Cybersecurity framework

In the US, the National Institute of Standards and Technology (NIST) released in 2018 the version 1.1 of the "Framework for Improving Critical Infrastructure Cybersecurity", commonly referred to as the "Cybersecurity Framework" . The version 1.1 refines, clarifies, and enhances Version 1.0, which was issued in February 2014.

The NIST Cybersecurity Framework provides a common language and mechanism for organizations to describe current cybersecurity posture; describe their target state for cybersecurity; identify and prioritize opportunities for improvement within the context of risk management; assess progress toward the target state; foster communications among internal and external stakeholders. The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.

The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

Scope

The framework addresses the needs of industries that are important to the national and economic security, including energy, financial services and communications. Although it originates from the US and is not a mandatory requirement for European organizations, corporations, organizations and countries around the world, including Italy and Israel, have built on the NIST framework. It has proven flexible enough to be adopted by large and small companies and organizations across all industry sectors.

Impact on banking and financial services

The version 1.1 has significant correlation to FINSEC goals and objectives as (among others) it contains greatly expanded explanation of using Framework for Cyber Supply Chain Risk Management purposes. In the most advanced level, the Tier 4 ("Adaptive"), the organization is expected to consider the External Participation; it understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. According to NIST, The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses.

General purpose Regulations & Standards

EU Privacy Rules – GDPR

The General Data Protection Regulation (GDPR) 2016/679 of the European Parliament and of the European Council, finalized on the 27th April 2016 was put in full effect on the 25th of May 2018. This Regulation was designed in order to adapt the existing data protection legislation with respect to the way in which data is currently being used in the digital setting. The objective of the Regulation is to empower EU citizens by making them aware of the kind of data held by institutions and the rights of the individual to protect their personal information. In this way it provides additional control to EU residents on over how their personal information is accessed, communicated and stored. All organisations must ensure compliance by 25th May 2018. Failure to comply with the GDPR principles will incur significant penalties for the institution. This will be discretionary and, depending on the nature of the breach, it will range between 2% and 4% of its worldwide revenue, with upper limits of Euros 10m and Euros 20m.

Scope of the regulation

This regulation will be extremely useful in protecting EU citizens and making them feel more secure on their data, and in creating a simpler and clearer legal environment for companies to operate in it. However, GDPR prompts serious consequences for companies. As GDPR standardises data privacy laws and mechanisms across industries, regardless of the nature or type of operations, financial institutions are equally affected by this Regulation. Given that financial organizations collect large amounts of customer data which are used in a variety of processes and activities, such data may easily be collated. Such processes may include client or customer on boarding, relationship management, trade-booking, and accounting. In these processes customer data is exposed to different people, at different stages, and hence GDPR needs to be applied in any of the processes that requires the handling of any type of customer data.

Impact on banking and financial services

Overall, GDPR impacts significantly the financial institutions, especially with respect to the collection of customer information. Institutions need to demonstrate the integrity and validity of their customer's consent with respect to how their data is shared and used for marketing and commercial purposes. They also need to inform customers on how they plan to process and use the data. Additionally, each institution needs to appoint a Data Protection Officer (DPO).

The rest of this subsection outlines the areas of the GDPR that are relevant to the financial services domain.

- Data subject consent: GDPR ensures that customers retain the rights over their own data. This concerns personal data and mandates firms to gain customer consent from their customers about the personal data that is gathered, such that customers are aware of what information organisations are holding. This data might be related but not limited to anything that could be used to identify an individual (or to keep them anonymous via pseudonymisation as defined by GDPR but deduce their core propensities to invest, to vote and other personal characteristics), e.g. including as data sources their neighbours, colleagues and friends), as well as their GDPR-related data such as name, email address, IP address, social media profiles or social security numbers. Firms are obliged to provide a clear outline of the purpose for which the data is being collected and gain additional customer consent especially for the case that the firm wants to share some of the customer information with third-parties.

- Right to data erasure and right to be forgotten: Beyond the right to data privacy, GDPR, under the terms, also allows Data Portability. Data Portability implies that individuals can request access to, or the removal of, their own personal data from financial institutions. Financial institutions may keep some data to ensure compliance with other regulations, but in all other circumstances where there is no valid justification, the individual's right to be forgotten applies.

- Minimizing the possibility of a breach: The DPO must report a data breach to the supervisory authority of personal data within 72 hours. The information to be communicated by the DPO includes details on the nature of the breach, the categories and approximate number of individuals impacted, and contact information of the DPO. As soon as the possible outcomes of the breach become clear, the company is required to inform impacted customers 'without undue delays' (if needed). Penalties in cases of serious violations such as failing to gain consent to process data or a breach of privacy by design, could be up to €20 million, or 4 per cent of the company's global turnover (whichever is greater). Lesser violations, such as records not being kept in order or failure to notify the supervisory authorities, will incur fines of 2 per cent of global turnover. Hence, financial organisations need to ensure that there is an adequate level of security with respect to the risk. Firms need to act with consciousness, diligence and proactive attitude towards data processing and apply the necessary security measures.

- Vendor management: GDPR is a regulation that relates to the personal data of clients. Hence, it is essential for firms to understand all their data flows across their various systems. Given the wide deployment of outsourcing development and support functions, firms need to ensure that personal client data is not accessible to external vendors, thus significantly increasing the data's net exposure. According to GDPR, vendors cannot disassociate themselves from obligations towards data access. Additionally, it is essential for Non-EU organisations that collaborate with EU banks or serving EU citizens, to ensure vigilance while sharing data across borders. GDPR in effect imposes end-to-end accountability to ensure client data stays well protected by enforcing not only the bank, but all its support functions to embrace compliance.

- Privacy by design: Under GDPR (Article 25, Recital 78) controllers should embed privacy features and functionalities into products, systems from the time that are first designed throughout all the processing operation. It suggests that appropriate measures can be applied such as minimizing the collected data, pseudonymisation techniques (replacing personally identifiable material with artificial identifies) and improved security features, like encryption (encoding messages so only those authorized can read them).

- Pseudonymisation: GDPR applies to all potential client data wherever it is found, whether it's in a live production environment, during the development process or in the middle of a testing programme. It is quite common to mask data across non-production environments to hide sensitive client data. Under GDPR, data must also be pseudonymised into artificial identifiers in the live production environment. These data-masking or pseudonymisation rules, aim to ensure the data access stays within the realms of the 'need-to-know' obligations.

- Impact assessment: Another new obligation established by the GDPR is to carry out an impact assessment (Privacy Impact Assessment - PIA) for organizations that perform data processing that may involve a high risk for the rights and freedoms of natural persons. The origin, nature, particularity and severity of such risk must be assessed (Recital 84 of the GDPR).

- Data Protection Officer (DPO): GDPR requires that a responsible individual is identified as the Data Protection Officer within each organisation. The DPO is expected to be the company's advisor on Data Protection and they should be competent in the matters of coordination and control of compliance with data protection regulations. Although not mandatory in all organizations, this role is considered as necessary for public firms, firms that have large-scale processing or firms that collect particularly sensitive data or data related to convictions or criminal offenses. A dedicated DPO is required for large organisations with more than 250 employees. Beyond the main duties of the D P O, this role also encapsulates several additional functions including: monitoring the implementation and application of internal policies, training staff with respect to GDPR, organizing and coordinating audits, managing the data subjects' data and the requests presented in the exercise of their rights, ensuring the conservation of documentation, supervising the execution of the impact evaluation and acting as point of contact for the supervisory authority.

- Biometrics as identifiers for financial transactions*:* Financial services may consider the use of biometrics, such as for example fingerprints and eye scans to identify their customers. In this respect, beyond obtaining the explicit consent for the use of biometric data of their customers, financial institutions are also required to have controls in place that protect them. Such controls will ensure that data controllers take the necessary technical and organizational measures to prevent this special data from being exposed, as a consequence their systems being poorly managed.

US Privacy Rules - Gramm-Leach-Bliley Act

Gramm-Leac-Bliley (GLB) Act refers to the corresponding U.S. regulatory framework with respect to customer data protection in the financial sector.

Scope of the Act

The Gramm-Leach-Bliley (GLB) Act requires financial institutions to provide information to their customers regarding their information-sharing practices as well as to safeguard sensitive data. In particular, the GLB Act requires financial institutions to take measures such that customer information is safeguarded. This is implemented by deriving a written information security plan that describes the company’s plan to protect customer information. The plan is based on the company’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company needs to identify employees that are coordinating this information security program, identify and assess the risk to customer information in each operation of the company and evaluate the effectiveness of current safeguard measures, design and implement a safeguards program, select service providers that can maintain appropriate safeguards, evaluate and adjust the program in light of relevant circumstances, including changes in the firm’s business or operations, or the results of security testing and monitoring.

Impact on financial institutions

The GLB Act does not have a direct impact on the FINSEC project, as the latter is implemented in the European regional area, where the GDPR regulation is applicable. However, the GLB Act has been included in this deliverable as the Act is explicitly addressing financial institutions and therefore provides additional support for the sections of the GDPR that have been identified as relevant to FINSEC in the previous section.

e-Privacy

e-Privacy regards a proposal for regulation concerning the respect for private life and protection of personal data in electronic communications. This proposal repeals Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, e-Privacy directive). The e-Privacy directive will come into force towards the end of 2018 or the beginning of 2019.

Scope of the Regulation

The provisions included in this proposal particularise and complement the GDPR by identifying certain rules for the rights of natural and legal persons on electronic communication. In particular, the e-Privacy proposal (finalized in March 2017) identifies the rules regarding the protection of fundamental rights and freedoms of natural and legal persons with respect to the use of electronic communications services. It regards the rights of natural and legal persons for respect on private life and communications and the protection of natural persons with regard to the processing of personal data. The proposal also encapsulates the free movement of electronic communications data and electronic communications services within the EU territory.

The proposal defines electronic communications data in a broad and technology neutral way such that it includes any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content.

This also includes data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. As the content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment, e-Privacy aims to provide additional provisions for natural and legal persons.

Similarly, e-Privacy is also relevant to any metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata may include the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication.

Additionally e-Privacy also aims to provide protection for electronic communication data that may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value, and thus the provisions of this Regulation apply to both natural and legal persons.

Overall, the regulation provisions that legal persons have the same rights as end-users that are natural persons regarding e-Privacy. Supervisory authorities in charge of this regulation should also be responsible for monitoring the application of this regulation regarding legal persons.

Impact on financial institutions

The scope of e-Privacy is to particularize and complement the GDPR with respect the entire content of any electronic communication. To this end, e-Privacy will impact the financial services sector with respect to the following:

- Protection of legal persons: All electronic communications exchanged in the financial sector are subject to stricter requirements, especially in the case that they contain personal or confidential data. This translates into additional measures to ensure the protection of such data.
- Protection of electronic communication*:* e-Privacy aims to protect all kinds of data processing within electronic communications. Hence, additional security requirements for the transmission of personal and confidential data through electronic means might need to be developed in the financial sector. Beyond email communication, this might prompt changes in existing processes such as fund transfers (where the data of the payer and payee is transferred between banks) or information exchanges related to regulations such as AEI (Automatic Exchange of Information), FATCA (Foreign Account Tax Compliance Act) or MiFID (Markets in Financial Instruments Directive).
- Protection of terminal equipment information: The e-Privacy also refers to the information related to the terminal equipment of end-users. Hence, financial institutions will have to consider these requirements in applications developed (such as web-banking or mobile banking apps) where data such as transaction details are stored by the user.
- Metadata restrictions: The processing and/or storage of metadata is restricted by e-Privacy and hence this may affect the ability of the financial institutions to use and analyse such data.
- Effects on internal screenings: The regulation will prohibit the processing of electronic communications without prior consent. Hence, internal screenings of e-mails and other electronic files will require the prior consent by any user communicating with the institution.

eIDAS

eIDAS (electronic IDentification, Authentication and trust Services) is an EU regulation on a set of standards for electronic identification and trust services for electronic transactions in the European Single Market.

Scope of the Regulation

Electronic identification (eID) and electronic Trust Services (eTS) are key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market. eIDAS took effect on July 2016. In particular, the eIDAS Regulation aims to ensure that individuals and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU member states if the eID schemes are available. Along the same lines, it creates a European internal market for eTS - namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication - by ensuring that they will work across borders and have the same legal status as traditional paper based processes. Therefore, these regulations provide certainty on the legal validity of all these services, businesses and citizens that will use the digital interactions as their natural way of interaction. To this end, through eIDAS, it has allowed the EU to provide right foundations and a predictable legal framework for people, companies (in particular SMEs) and public administrations, to safely access services and do transactions online and across border in just "one click". Indeed, the release of eIDAS provides higher security and more convenience for any online activity.

Impact on financial institutions

eIDAS is the last step in the process of converting all paper-based processes to e-processes. In particular it provides the financial sector with:

- • Legal effects for qualified electronic signatures, seals, certificates for electronic seals, timestamps and documents, as well as e-signature and e-seal creation devices.
- • A legal framework for e-registered delivery services and website authentication services.
- • The basis for eID schemes notified under the regulation in one member state to be recognised in one another.
- • Security of personal data and breach notification requirements for all trust service providers.
- • Supervision for Qualified Trust Service Providers (QTSPs), trusted lists and a trust mark for QTSPs to demonstrate compliance with the regulation.

Specification for security management systems for the supply chain (ISO 28000:2007)

ISO 28000:2007 specifies the requirements for a security management system, including those aspects critical to the security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain. The standard was last confirmed in 2014 and still applies today.

Scope of the standard

Security Management is a challenge within supply chains, as the supply chain partners are often located in varying locations worldwide, meaning that they are subject to varying regulations and processes. The benefits associated with complying with the standard include identifying potential threats which originate from outside the organization, control and influence activities that impact on supply chain security and ensure continuity of business. A certified ISO 28000 management system can reduce a company's liability for security incidents.

Impact on banking and financial services

The primary focus and interest of the standard is on the transportation and logistics businesses and not in banking. The standard requires the organization to review and document the processes and procedures and identify the areas that do not meet the standard requirements with regard to the security of the supply chain. Nevertheless, the standard in case it is adopted by a financial organization would primarily indicate the special emphasis placed on identifying threats from the external environment that affect the internal operation of the organization and ensure the continuity of business. FINSEC places specific emphasis on the inter-organization sharing of information about threats and vulnerabilities as a means for collaborative risk assessment. It will implement a supply chain collaboration module that specifically addresses the financial supply chain.

Business continuity management systems (ISO 22301:2012)

Business continuity is the planning and preparation of a company to cope with serious incidents or disasters and resume its normal operations within a reasonably short period. It is deemed nowadays the essential complementary stage to an integrated risk management approach. Business Continuity Management (BCM) includes the following three key elements:

- *Resilience*, i.e. the design of critical business functions and of the supporting infrastructure that makes sure that they are not affected by disruptions; for example through the use of redundancy and spare capacity;
- *Recovery*, i.e. the arrangements planned to recover or restore critical and less critical business functions that have failed; and
- *Contingency*, i.e. the readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been, foreseen. Contingency preparations constitute a last-resort response if resilience and recovery arrangements should prove inadequate in practice.

The ISO 22301:2012 standard sets out the requirements for a best-practice business continuity management system (BCMS). A BCMS is by itself a comprehensive approach to organisational resilience and helps organisations cope with incidents that affect their business-critical processes and activities. It provides a structure for organisations to update, control and deploy effective plans, taking into account organisational contingencies and capabilities, as well as business needs.

The ISO22301:2012 standard specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

While ISO 22301 may be used for certification and therefore includes rather short and concise requirements describing the central elements of BCM, a more extensive guidance standard (ISO 22313) is being developed to provide greater detail on each requirement in ISO 22301.

Scope of the standard

The requirements specified in ISO 22301:2012 are generic and intend to be applicable to all organizations, or parts thereof, regardless of their nature. The extent of application of these requirements depends on the organization's operating environment and complexity. Those businesses that recognize their dependence on each other and seek assurance that their key suppliers and partners continue to operate and provide their products and services, even when incidents occur, seem to be the ones that pursue certification.

Impact on Banking and Financial Services

The adoption of the standard is not universal in the finance and banking sector. However, given the advent of new directives such as the EU General Data Protection Regulation (GDPR) and the NIS Directive, ISO 22301, compliance is recommended as a useful tool for implementing a well-defined incident response and reporting structure, so organisations can demonstrate they are taking steps to comply with regulatory requirements. Thus we expect that the standard will increasingly be adopted by the financial sector and lead to the development of service models that adhere to its principles by adopting best practices fault-tolerance and resilience.

Impact of Regulations and Standards on FinSec components

The regulations and directives reviewed in the previous sections prompt a number of implications for the components of the FINSEC project and the design of the project's architecture.

The following is a preliminary logical view of the FINSEC platform architecture.

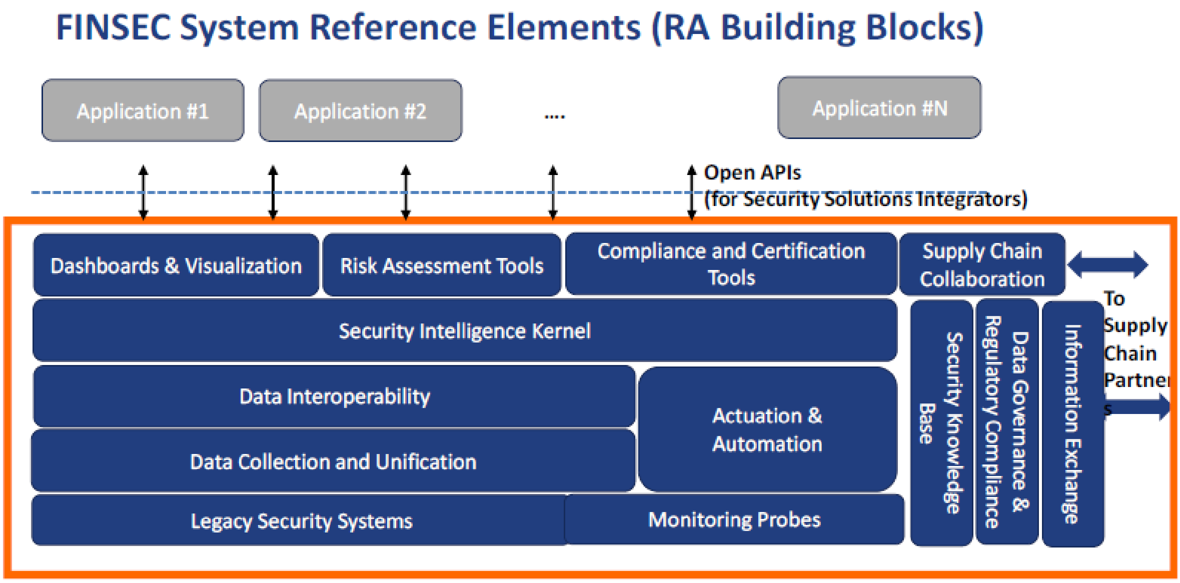

FINSEC System Reference Elements (RA Building Blocks)
Application #1
Application #2
....
Application #N
Open APIs
(for Security Solutions Integrators)
Dashboards & Visualization
Risk Assessment Tools
Compliance and Certification Tools
Supply Chain Collaboration
To Supply Chain Partner s
Security Intelligence Kernel
Data Interoperability
Data Collection and Unification
Actuation & Automation
Legacy Security Systems
Monitoring Probes
Security Knowledge Base
Data Governance & Regulatory Compliance
Information Exchange

Fig.6.1: FINSEC System Reference Elements

The FINSEC RA defines a set of building blocks for building data-intensive security monitoring systems including:

(i) Monitoring probes, which interface to cyber and physical security systems towards collecting security-related information

(ii) Data Collection mechanisms will ensure data quality, data filtering, as well as adaptive selection of the needed data sources based on dynamic changes to the configuration of the critical infrastructures

(iii) Actuation and Automation module, builds on predictive security and machine learning to achieve the identification and correlation of events

(iv) Security Intelligence Kernel, which identifies known and potential new security attack patterns by means of advanced data analytics and matching of identified evens against the security knowledge base

(v) Risk Assessment Tools include a range of background security technologies, including a risk assessment engine, Security Information and Event Management (SIEM) technologies, anomaly detection technologies, predictive CCTV analytics, a Risk Assessment Engine (RAE), vulnerability assessment services and more

(vi) Supply Chain Collaboration, are tools facilitating the collaborative assessment and mitigation of risks by participants in the financial sector supply chain.

(vii) Security Knowledge Base that holds Information gathered a-priori (databases, etc.) on known attacks against critical infrastructures

(viii) Open APIs are Open programming interfaces dedicated to each single service within the RA

The following table summarizes the main impacts of each regulation or directive with respect to the building block being affected.

Table 6.1: Regulations impact on security monitoring systems building blocks

Building Block	Role within the RA	Regulations	Main Impacts
Data collection – CCTV	Monitoring for physica security level – raw data extraction	GDPR	• Minimisation: not exceeding needed amount of acquired data; •Impact Assessment on Data Protection; • Control Authority consultation
Data collection - Access control			• Minimisation: not exceeding needed amount of acquired data;

	Monitoring for physica security level – raw data extraction	GDPR NIS	• Transparency in the use of personal data; • Privacy by design; • Personal data usage acceptance; • Right of deletion; • Need for mechanisms such as Multi-Factor Authentication, Single Sign-On, User Behavior Analysis, etc.
		ISO 27001	• Physical security perimeter with physica barriers; • Physical entry controls; • Removal of access rights at the end o employment; • Isolation between delivery/loading area and information processing facilities; • Written access control policy accordin to business and security requirements
Logs control	Monitoring for logical security level – raw data extraction	GDPR	• Minimisation: not exceeding needed amount of acquired data • Pseudonymisation • Personal Data encryption; • Need for role-based access controls
		NIS	Notification of significant security incidents to authorities
		ISO 27001	Event records shall be synchronized with an agreed accurate time source

Risk Assessment Tools: SIEM	Existing security tools, which collects, analyses and correlates security events within a critical infrastructure, with generation of alarms and reports	GDPR	• Need for automated reporting, ensuring that data handling is in compliance with security by design (pseudonymisation, encryption, minimization of data); • Automated measure inside the SIEM to correct activities violating GDPR-compliance controls; • Flexibility to quickly process any kind of data generated by different applications; • Need for data destruction policies; • Need for role-based access controls
		NIS	Need for traceability and communicability of number of users affected by an incident and its duration;
		ISO 27001	Third party service must be in compliance with the service delivery agreement; reports of service to be periodically reviewed
Data collection module	Ensures that data from different data sources (security monitoring data, assets monitoring data, user behaviours, customer interaction data, publicly available security threat knowledge bases, vulnerabilities knowledge bases, sensor data) are correctly gathered together	GDPR	• Minimisation: not exceeding needed amount of acquired data; • Accountability (e.g. control logs as evidence of compliance of data usage); • Data Security test procedure; • Need for network firewall/antivirus; • Need for Data Leakage Protection measures • Automatization to avoid human errors in data management
		ISO 27001	

			Classify collected data in terms of their value, sensitivity and criticality
Data Storage module	Big data infrastructure where FINSEC data are saved	GDPR	• Storage time no longer than needed; • Privacy by design; • Accountability (e.g. control logs as evidence of compliance of data usage); • Resilience-based design against physical and logical damages; • Data Security test procedure; • Need for Data Leakage Protection measures
		ISO 27001	Classify stored data in terms of their value, sensitivity and criticality; • System resource in terms of data storage must be constantly monitored; • Back-up of data; • Written procedures for the management of removable media
Data interoperability module	Ensures that data ar unified and complian with data format selected for FINSE purposes	GDPR	Automation to avoid human errors in data management
Actuation & automation module	Semi-automated intelligence module t interact with dat collection settings	GDPR	Avoid the use of data collected to extract intelligence that may be used for personalised behavior analysis
Security Intelligence Kernel	Analytics tool, extracting information about abnormal or suspicious behaviours	GDPR NIS	• Minimisation: not exceeding needed amount of acquired data; • Storage time should not be longer thar required;

		ISO 27001	System resource in terms of information extraction must be constantly monitored
Security Knowledge Base	Information gathered a-priori (databases, etc.) on known attacks against cyber critical infrastructures	GDPR	• Minimisation: not exceeding needed amount of acquired data; • Storage time no longer than required.
		NIS	Ensure a network security level adequate to the estimated level of risk.
Dashboard & visualization Dashboard & visualization	Visualization and interaction between the user and the applications (Risk Assessment tools, Compliance and Certification tools)	GDPR	Minimisation: the required amount of visualized data should not exceed purpose;
		ISO 27001	• Implement measures to ensure responsibilities of users are clear, to reduce the risk of misuse of the services • Removal of access rights at the end of employment
Risk Assessment Tools	Application delivered as a service for risk prediction and mitigation	GDPR	Need for prediction of economic and reputational impacts of cyber and physical attacks
		NIS	Ensure a network security level adequate to the estimated level of risk
		ISO 22301	Resilience, include business continuity management aspects

Supply Chain Collaboration module	Ensures Security data sharing and information exchange between different end-user organizations	GDPR	•Accountability (e.g. control logs as evidence of compliance of data usage); • Pseudonymisation; • Personal Data encryption; • Need for network firewall/antivirus; • Need for Data Leakage Protection measures
		ISO 27001	• System resource in terms of data exchange (network resources) must be constantly monitored; • Information exchange agreements have to be foreseen between different parties
APIs	Open programming interfaces dedicated to each single service within the RA	ISO 27001	• Implement measures to ensure responsibilities of users are clear, to reduce the risk of misuse of the services • Removal of access rights at the end of employment

CCTV systems

Video monitoring systems constitute one of the main physical security tools within the FINSEC architecture. Such systems are subject to both general European regulations and national laws about privacy and data usage. In particular, the CCTV systems are significantly affected by the GDPR regulation. Although GDPR was discussed earlier in this deliverable (section 4.1), this section discusses its impact on the use of CCTV systems. Annex 1 includes more information on national regulations relevant to this topic.

The new GDPR regulation impacts on some aspects of a CCTV system design and usage. In particular, the following principles have to be taken into account:

Minimization: CCTV devices have to be installed in order to ensure the amount of data processed is the minimum needed for the purposes of monitoring. For instance, CCTV cameras are supposed to monitor only the portion of space which is strictly correlated to the physical access to the monitored area, avoiding to register the surrounding zones.

Right to be forgotten: A data subject has the right to obtain from the data controller the deletion of their personal information from the system as soon as the data is no longer necessary for the purpose it was collected for.

Data portability: the CCTV system should allow the data subject to receive its own data in a portable and standard format

Data Protection Impact Assessment: this can be undertaken before installing a new CCTV system; it is aimed at identifying the most effective way to comply with GDPR requirements, thus reducing the risks of misuses of personal information. The DPIA can be needed for a CCTV system, as specified in Article 35 of GDPR, mentioning the "large scale, systematic monitoring of public areas (CCTV)".

Physical access controls – biometric measures

Use of biometric measures is another possible way to control physical access to sensitive areas of critical infrastructures within the scope of FINSEC. The following paragraphs discuss the main restrictions and recommendations to system designers for compliance with the current regulations and laws.

Any physical access control system must be designed in compliance with both the GDPR regulation, and the NIS, mainly under the following points of view:

Data Treatment Registry: the purpose for the use of biometric data has to be specified in a written registry. The registry should be available to the authorities for audit purposes.

Data Protection Impact Assessment: as explained for the CCTV case, this measure is aimed at identifying the most effective way to comply with GDPR requirements, thus reducing the risks of misuses of personal information. This assessment evaluates the effective need of all the foreseen biometric data treatments, and related risks.

Data Protection Officer: biometric data treatment forces the organization to appoint a Data Protection Officer, whose roles are ensuring the compliance of treatments to the GDPR, supporting the activities related to the Data Protection Impact Assessment and being a contact point for the control authorities.

Right to be forgotten: the data subject has the right to request from the data controller to delete all of his personal information - biometric data from the system, once the data is no longer necessary for the purpose it was collected for.

Data portability: the access monitoring system should allow the data subject to receive its own biometric data in a portable and standard format.

Information protection: Furthermore any information stored will need to be protected (application of the NIS directive as transposed to national laws), so that data breach may be avoided in the first place. Thus there is the need for mechanisms such as Multi-Factor Authentication that will protect the information.

Blockchain infrastructure

The Peer-to-Peer payment solution regulatory and law compliance requirements fall under several categories.

First, in terms of regulators, regulations and directives, the Smart Contracts need to be put under control either by a private company or consortium that must be, based on regulatory requirements, accepted as a "Trust”, subject to relevant conditions, controls and inspections.

Second, effective controls need to be formulated for all encompassing prevention of risks (money laundering, terrorism, illegal activities, market manipulation, etc.), possibly granting CBs the same level of risk decision making they’d have in a “standard” payments scenario (for AML and other).

Third, end-to-end transactions tracking must be enabled. This could be achieved by leveraging on inherent CB KYC (Know Your Customer) provisions, granting them visibility on all CBs, on demand or automatically (for AML).

Finally, the GB and the Trust must accept being auditable by an independent and established audit firm.

Blockchain transactions ensure the privacy of end-users. Hence, end-users' transactions are inherently anonymously stored on the Blockchain. However, the privacy of end-users is protected as long as their CBs preserve separation of their network and real identities from other circuit participants or attackers. Along the same lines, cyber-security and in particular, the Digital Wallet (the mobile app) must be capable of safely storing end-user’s credentials, leveraging on specific end-user’s device features on platform provisions or on additional app components. The CB and GB must be able to adopt IT security best practices for their systems hosting dashboards. Similarly, peer-to-peer payment solution Smart Contract software should be protected, possibly by a continuous review by a third party that will be defined.

Finally, end-users must know about implications of using an easy and innovative, yet regulated, payment solution, where any DCASH and/or its equivalent flat currency may be forfeited or seized if illegal activities are performed using DCASH (also by other End-users) and unusable DCASH results in unusable or non/existing corresponding flat currency (however exchanged with it), and this possibly implies a new framework of usage terms and conditions.

Cloud technology

The FINSEC architecture foresees the use of a private cloud system to exchange data and information between the different security control centers. The cloud technology can be used in FINSEC in both the PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) perspectives. The compliance with current GDPR regulation and NIS directive foresees the following measures:

- Clear definition of the cloud provider: who handles the infrastructures;
- Clear definition of data storage physical location;
- A priori definition of risks: assessment of how cloud deployment introduces data loss and data breach risks;
- Use of secure data transmission protocols;
- Store only encrypted data in the cloud; and
- Adequate logging procedures to monitor data access.

General recommendations for FINSEC

Based on the information presented above, we provide a digest of the regulatory (RR) and standardization requirements (SR) that impact the design of the FINSEC platform (including the individual components) and the execution of the pilots.

RR1. Minimization of data collected.

Adding more layers of security and collecting more data than what is really required to face the existing challenges, is a temptation for system designers, especially in an environment exposed to a number of different and largely unknown threats; however, GDPR clearly states that the amount of data (personal data in this case) processed is "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".

The data being collected in FINSEC should not exceed the minimum required. While this may put a limit to the further exploitation of the data collected, it does not prohibit a well-defined reason for collecting them in the first place (e.g. "extended CCTV coverage" may be justified for establishing a "soft" perimeter around ATMs, if the public is notified, privacy is respected and passers-by are not recorded).

RR2. Pseudonymisation.

The processing of personal data should be performed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately. Pseudonymisation is different from anonymization, as in the latter the detailed information about the owner of the data is lost (as in the USA and UK voting-influence crisis with Cambridge Analytics), while in the former the data can be traced back to their owners.

The need for pseudonymisation will influence the way the FINSEC pilots are implemented.

RR3. Purpose limitation.

Additionally the data collection goals should be consistent with the (initially defined) purpose set for the system and should be erased after that purpose is fulfilled.

Purpose limitation means that "*They should be collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*" which limits the opportunities for exploiting data collected by one system for another (initially unforeseen) purpose, unless explicit notification is issued.

RR4. Increased incident reporting and notification needs.

The NIS requires that "incidents having a significant impact on the continuity of the essential services they provide" are disclosed to the supervising authorities without undue delay. In determining the significance of security incidents operators of essential services will need to consider factors such as how many users are affected by disruptions to essential services, how long such an incident lasts and the "geographic spread" of the impact from such an incident. In contrast to GDPR, all incidents need to be reported including even the outages affecting availability that meet the stated threshold.

The need for notification, required by NIS and GDPR, is thus a major driver for the selection of features that will need to be present in the FINSEC Knowledge Base.

RR5. User profiling.

Controllers may continue to carry out profiling and automated decision-making if the processing doesn't produce legal or similar significant effect on the individuals, but always follow the GDPR principles.

Any profiling activity implemented within FINSEC (e.g. analytics-based profiling on a CCTV stream) is prohibited, in case it leads to an individualized assessment and a recommendation about an individual.

RR6. Periodic Data Privacy Impact Assessment need to be foreseen.
An obligation established by the GDPR is to carry out an impact assessment (Privacy Impact Assessment - PIA) for organizations that perform data processing that may involve a high risk for the rights and freedoms of natural persons. The origin, nature, particularity and severity of such risk must be assessed (Recital 84 of the GDPR).
A periodic assessment of the impact to user data privacy should be facilitated by the design of every FINSEC component. DPIA should precede any actual use of the component.

RR7. The design of FINSEC (input, data models, application logic) should respect individual privacy rights.
The structure of the information should guarantee that the right to be informed about the information processed and stored as well as the right to be forgotten, are maintained by the users.

RR8. Data processing contracts are required.
The contracts should state the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data to be processed and categories of data subjects and the obligations and rights of the controller.
Data processing contracts need to be established between data owners (controllers) and data processors (technical partners). If vendors are involved in the execution of a pilot, vendor contracts need to be updated prior to the FINSEC pilots to comply with GDPR privacy requirements.

SR1. Collaboration is critical to assess emerging threats.
The ISO28000 standard indicates the need for collaboration between peer organizations as well as partners in a supply chain (suppliers-customers) as a significant opportunity for an organization to be better informed and equipped for the threats emerging. This was vividly understood e.g. during the WannaCry crisis.
Collaboration based on information exchange is an important consideration in FINSEC. The data model for information sharing should be based on the insights about threats and vulnerabilities that the financial institutions can offer.

SR2. Business Continuity, operational resilience.

Financial services are mission-critical activities that should continue no matter how serious the threat it is exposed to. Anticipating failure and pursuing fault tolerance in the system design and implementation is a primary goal.

Business continuity (itself a standard, ISO/IEC 22301) is a central element of the whole Information Security Management System and should be a key consideration for the FINSEC implementation.

SR3. Information about vulnerabilities needs to be obtained.

ISO/IEC 27001 indicates in its A12.6 section "*Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk*".

Thus information exchange (as will be pursued by the FINSEC Collaboration Module) that will lead to timely assessment of vulnerabilities as new threats emerge is important to achieve compliance with the standard.

SR4. Proportionality is important.

The security strategy should adapt to the magnitude and impact of the risks, considering the practical constraints imposed by the business needs and the environment in which the business operates. In terms of resources spent (time, money, effort) the amount to be spent on mitigating a risk should be proportional to the risk. Proportionality is thus an important design consideration for the Security-as-a-Service (SECaaS) product and service offering.

The security requirements expected from a Fintech service provider (an SME) with a very specific business model, well-controlled service endpoints and a limited number of clients should be less stringent than the ones expected from a bank which offers a multitude of services, web-based transactions including payments to millions of users. [61]

Predictive Security Analytics

Predictive Analytics algorithms and methods

The methods of security data analytics with the purpose of detecting attacks can be classified into three main categories (statistical methods, machine learning/deep learning methods, and knowledge-based methods) as described in the followings.

Statistical methods

In these approaches, network traffic activity is captured and a profile representing its normal behaviour is generated. This is done using metrics such as packet level data and flow level data. For instance, a statistical inference is applied to calculate an anomaly score which is generated based on currently observed traffic. If the score is upper than a given threshold, then an alarm of anomaly is generated. We distinguish three relevant models applied in statistical methods: Univariate models, multivariate models and time series models. We describe briefly each of the cited models as follows:

1. *Univariate models*

These models need prior knowledge of an underlying distribution of data and estimate parameters (mean and standard deviation) from given data.

2. *Multivariate models*

They consider correlations between two or more metrics and do not need prior knowledge of an underlying distribution.

3. *Time series models*

These models use an interval time combining with an event counter or a resource measure, and they consider inter-arrivals times of observations as well as their values.

There are several used examples of statistical methods in attack detection. One can cite the information entropy, which consists of summarizing the traffic distribution by capturing the important characteristics of traffic features. Entropy-based methods are suitable for detecting attacks launched by Botnet based on anomalous patterns in networks.

Another statistical method is Cumulative Sum (or CUSUM) algorithm which is a sequential technique used to detect irregular changes in traffic traces.

The statistical methods have some number of advantages. We can cite:

- They do not require prior knowledge of network attacks. Hence, they are capable to detect zero-day attacks
- They use few features to characterize the network traffic leading to considerable reduction of their time and space complexity

These methods have also some drawbacks that we cite below:

- These methods can be trained by an attacker
- An appropriate threshold is difficult to set in order to better balance false positives and false negatives

Machine learning and deep learning methods

Machine Learning

The aim of machine learning is to establish an explicit or implicit model of analysed patterns. Machine learning approach can be divided into three categories:

1. *Supervised learning*

In this type of machine learning, the used algorithm will learn knowledge from labelled data and then uses the obtained knowledge to classify the unknown data. There are various supervised learning algorithms such as:

- Support Vector Machine (SVM)
- K-Nearest Neighbour (KNN)
- Artificial Neural Network (ANN)
- Decision Tree (Random Forests)

2. Unsupervised learning

In this family of learning techniques, the used algorithms can find the underlying data structure without the need for the user to annotate ("label") the data used in the training process. The most used methods or algorithms in this category are:

- K-means
- K-medoids
- BIRCH
- Chameleon
- DBSCAN
- OPTICS
- STING
- CLIQUE

3. Semi-supervised learning

In this type of learning, we consider a portion of labelled data mixed into a large amount of unlabelled data to generate training datasets for unsupervised learning.

The machine learning methods have a certain number of advantages and we cite some of them in the following:

- These methods have high detection rate
- They are adaptive: they are capable of updating their execution processes according to the new traffic

Nevertheless, they have also some disadvantages such as:

- The supervised learning cannot detect unknown attacks until relevant information is fed for retraining
- These methods consume more resources in both training and updating processes

4. Deep learning

Deep Learning is a subfield of machine learning whose algorithm is inspired by the structure and function of the brain called artificial neural networks. The algorithm takes metadata as an input and processes the data through a number of layers of the non-linear transformation of the input data to compute the output. It has a unique feature i.e. automatic feature extraction, which enables it to automatically grasp the relevant features required for the solution of the problem, reducing the burden on the programmer to select the features explicitly. The algorithm can be used to solve supervised, unsupervised or semi-supervised type of problems. Deep learning-based systems using self-taught learning have proved promising in detecting unknown network intrusions.

Knowledge-based methods

In these approaches, network or host events are matched with predefined attack rules or signatures to examine them for the presence of known attack instances. The most used knowledge-based methods is the *Expert System*. This extracts the specific features from training data and builds a rule classifying new coming data. There exists also another approach noted by *ontology analysis* and consists of expressing the relationships between collected data and using them to infer particular attack types. Another approach is noted by *logic analysis* and consists of expressing logic structure and using this structure to determine whether network events are legal.

As we discussed the advantages and drawbacks of the cited methods, the knowledge-based methods have also some advantages such as:

- They are simple and robust
- They have a high detection rate

Unfortunately, these methods have also some drawbacks such as:

- They cannot detect unknown attacks
- These methods may trigger some false alarms due to non-availability of attack datasets.

Machine Learning/Deep Learning for FINSEC

Machine Learning/Deep Learning for FINSEC

One of the most relevant components in the data collection and analysis architecture consists of analysing and processing the data in the Data Processing Layer. This component noted by “Machine Learning” in the “Global Analysis System” will be used to analyse the collected data provided and normalized by the “Data Collector” on the cyber physical system.

A big picture, and without loss of generality, on how machine learning algorithms are working on a given data set, is depicted in the figure below:

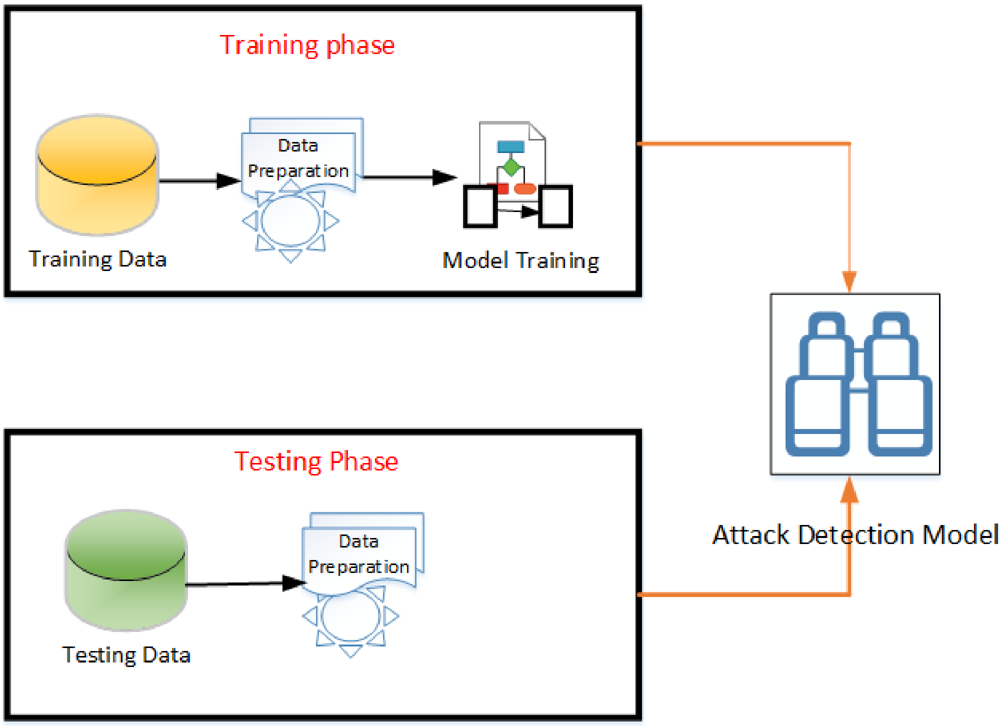


Fig.6.2: Machine Learning algorithms functioning model

Indeed, and after data normalization and filtering, one can observe two essential steps that should be used before proposing an attack detection model:

- Training phase: this phase consists of collecting security event data for training our model. Our ML/DL algorithms and their combination will be applied on the prepared training data to detect eventual anomalies or attacks according to some added rules. This phase will result in an attack detection model that will be validated and approved by the data testing set.
- Testing phase: This phase proposes a data set to test the detection model found in the Training phase. When the data preparation is complete, then we apply the learning algorithms adjusted in the previous phase, to validate and improve the accuracy and the message/decision to be highlighted.

Nevertheless, and despite the performance that can be guaranteed by the attack detection model illustrated in Figure 1, some applied machine learning or deep learning algorithms can be inconsistent for different problems or for some data sets. Therefore, a machine learning algorithm may perform well for one type of cybersecurity analysis but may not perform well in another type of problems or data sets. Then, the algorithms selection is challenging in this context and has the merit to be addressed carefully and in a dynamic manner to improve the attack detection model performance and accuracy. In other words, the algorithms selection consists of identifying a good trade-off among various system's qualities (performance, accuracy ...).

Thus, we can compare various types of machine learning algorithms, but also combine some of them to improve the quality of the expected result.

Machine learning tools: state of the art

To operate and run machine learning algorithms, different frameworks exist in the literature, and each framework may be performant for some data analytics objectives but this can change when addressing different data sets.

In the following, we summarize the most well known frameworks for machine learning in general and for Deep Learning in particular. These frameworks are described as follows:

1. Apache Singa: is a general distributed deep learning platform for training big deep learning models over large datasets. It is designed with an intuitive programming model based on the layer abstraction. A variety of popular deep learning models are supported, namely feed-forward models including convolutional neural networks (CNN), energy models like restricted Boltzmann machine (RBM), and recurrent neural networks (RNN)

2. Amazon Machine Learning: is a service that makes it easy for developers of all skill levels to use machine learning technology. Amazon Machine Learning provides visualization tools and wizards that guide users through the process of creating machine learning (ML) models without having to learn complex ML algorithms and technology. It connects to data stored in Amazon S3, Redshift, or RDS, and can run binary classification, multiclass categorization, or regression on said data to create a model.

3. Azure ML Studio: allows Microsoft Azure users to create and train models, then turn them into APIs that can be consumed by other services. Users get up to 10GB of storage per account for model data, although they can also connect their own Azure storage to the service for larger models. A wide range of algorithms are available, courtesy of both Microsoft and third parties.

4. Caffe: is a deep learning framework made with expression, speed, and modularity in mind. It is developed by the Berkeley Vision and Learning Center (BVLC) and by community contributors. Models and optimization are defined by configuration without hard-coding & user can switch between CPU and GPU. Speed makes Caffe perfect for research experiments and industry deployment. Caffe can process over 60M images per day with a single NVIDIA K40 GPU.

5. Massive Online Analysis (MOA): is the most popular open source framework for data stream mining, with a very active growing community. It includes a collection of machine learning algorithms (classification, regression, clustering, outlier detection, concept drift detection and recommender systems) and tools for evaluation.

6. Spark: is Apache Spark's machine learning library. Its goal is to make practical machine learning scalable and easy. It consists of common learning algorithms and utilities, including

classification, regression, clustering, collaborative filtering, dimensionality reduction, as well as lower-level optimization primitives and higher-level pipeline APIs.

7. MLpack: a C++-based machine learning library originally rolled out in 2011 and designed for "scalability, speed, and ease-of-use," according to the library's creators. Implementing mlpack can be done through a cache of command-line executables for quick-and-dirty, "black box" operations, or with a C++ API for more sophisticated work. Mlpack provides these algorithms as simple command-line programs and C++ classes which can then be integrated into larger-scale machine learning solutions.

8. Scikit-Learn: leverages Python's breadth by building on top of several existing Python packages — NumPy, SciPy, and matplotlib — for math and science work. The resulting libraries can be used either for interactive "workbench" applications or be embedded into other software and reused. The kit is available under a BSD license, so it's fully open and reusable. Scikit-learn includes tools for many of the standard machine-learning *tasks* (such as clustering, classification, regression, etc.).

9. Theano: is a Python library that lets users define, optimize, and evaluate mathematical expressions, especially ones with multi-dimensional arrays (numpy.ndarray). Using Theano it is possible to attain speeds rivalling hand-crafted C implementations for problems involving large amounts of data. It was written at the LISA lab to support rapid development of efficient machine learning algorithms. Theano is named after the Greek mathematician, who may have been Pythagoras' wife. Theano is released under a BSD license.

10. TensorFlow: is an open source software library for numerical computation using data flow graphs. TensorFlow implements what are called data flow graphs, where batches of data ("tensors") can be processed by a series of algorithms described by a graph. The movements of the data through the system are called "flows" — hence, the name. Graphs can be assembled with C++ or Python and can be processed on CPUs or GPUs.

11. TensorBoard is a set of tools that allows graphical representation of different aspects and stages of machine learning in TensorFlow. The graphical interface facilitates the model training monitoring. A graph visualizer shows the model structure with graphs, allowing to ensure that the model components are located and connected properly. This approach simplifies the user experience during the performance evaluation of the model, especially for models of complex structures. In addition, TensorBoard allows to monitor how a model performs when its hyperparameters slightly change, making it possible to choose the hyperparameters that make the model perform best.[62]

12. H20.ai: makes it possible for anyone to easily apply mathematics and predictive analytics to solve today's most challenging business problems. It intelligently combines unique features not currently found in other machine learning platforms including: Best of Breed Open Source Technology, Easy-to-use WebUI and Familiar Interfaces, Data Agnostic Support for all Common Database and File Types. With H2O, users can work with their existing languages and tools. Further, they can extend the platform seamlessly into their Hadoop environments.

13. Keras: is an open-source Python deep learning library which can run on top off Theano and TensorFlow. It was developed with the objective of increasing the execution speed of machine learning experiments. Its user-friendly interface and the division of networks into sequences of separate modules simplifies the user experience during the design of the prototype. Modules are easy to create and add to the networks models.[63]

14. PyTorch: is an open-source machine learning framework for deep neural networks built on Torch that supports GPUs acceleration and Python language. Unlike other tools (such as TensorFlow, Theano and Caffe) PyTorch models are built as dynamic computational graphs, thus supporting the change of the neural network behaviour at runtime without the need of static rebuilding of the whole model. This choice allows reduced lags and computational overhead. [64]

15. Shogun: is one of the oldest tool for machine learning, written in C++, although it supports a plethora of programming languages such as C#, Octave, Python, Java, Ruby, R. Shogun is open-source and provides data structures and algorithms for regression (such as Kernel Ridge Regression), pre-processing, visualization, model selection strategies (such as forward selection, Least Angle Regression), clustering algorithms (such as k-means and Gaussian Mixture Model), one-time classification and multi-class classification (such as Support Vector Machines and K-Nearest Neighbor).[65]

Machine learning algorithms to detect innovative attacks

Machine learning algorithms are used in many contexts where statistical based methods are required to progressively improve performance and efficiency. In the intrusion detection system area, machine learning is usually adopted for anomaly-based detection. Machine learning algorithms may be adopted indeed to identify running Cyber and Physical Attacks, although detection in real-time may not be possible in some cases. In particular, two algorithms have been studied that can be used to identify attacks in progress by analyzing network traffic. These algorithms are called Principal Component Analysis and Mutual Information.

The Principal Component Analysis (PCA) is a statistical function already known in the intrusion detection field. It maps a coordinate space into a new coordinate system with axes commonly known as principal components (PCs). Such axes point in the direction of maximum variance of the original data. In particular, the first PC identifies the greatest data variance in a single direction, the second one is relative to the second greatest degree of variance, and so on. The retrieved PCs are ordered by the amount of data variance they identify. Typically, the first PCs contribute most of the variance in the original data set so that we can describe them with only these PCs, neglecting the others, with minimal loss of variance. Once the PCA is computed, given a set of data and its associated coordinate space, it is possible to perform a data transformation by projecting them onto the new axes.

Also Mutual information is not new in intrusion detection applications. This metric may help the traffic profiling in the presence of anomalies. Mutual Information could be adopted to understand the dependence between the analyzed variables. By combining these two approaches, it may be possible to implement intrusion detection systems able to identify innovative attacks.[66]

Conclusions

As critical as the aforementioned infrastructures are, more is their protection. The reason is more than obvious. Our lives today are reliant on them, and thus, they ought to be resilient.

Cyberspace is our contemporary (and seems like non-temporary) habitat. As we seek for safety in our house, we similarly ask for security in our digital, shared environment. The available frameworks, tools and methodologies are plenty, yet not enough. It is common truth that a chain is as strong as its weakest link. Which, in this case, is the human factor.

Not for lack of awareness. The latest years (and attacks) seem to have contributed to this direction. But, for manageability of arisen risk. Especially when they cannot be predicted.

Risk management is science, theory, practice and skills, all in one.

It takes experience to come up with results. It takes critical thinking, acute perception of the context, threats and opportunities, strong knowledge base and theoretical background, as well as managerial and communication skills.

But, most of all, risk management is about leading the way to the destination, even without having clear view of the road, which is full of both threats and opportunities. Good news are that we are not blind nor totally unaware of the road. Through continuous education, information and alert attitude, consequences can be reduced and chances be leveraged.

Cyber risk management in precise, additionally requires a strong technical background and knowledge of state-of-the-art technologies, from which risks but also countermeasures may arise.

As Robert E. Davis has stated, "*To competently perform rectifying security service, two critical incident response elements are necessary: information and organization*". And Daniel Wagner has complemented: "*Some risks that are thought to be unknown, are not unknown. With some foresight and critical thought, some risks that at first glance may seem unforeseen, can in fact be foreseen. Armed with the right set of tools, procedures, knowledge and insight, light can be shed on variables that lead to risk, allowing us to manage them.*"

My journey in risk management has just began, yet, I may conclude to the following:

"Keep your knowledge sharpened - it's your shield and your weapon.

There will always be competent warriors.

Keep informed, stay vigilant and be proactive."

Bibliography

[1]https://ppp-certification.com/ppp-certification-guide/52-defining-risk-risk-management-cycle36

[2] https://www.coe.int/en/web/europarisks/concept-of-risk

[3] https://www.nibusinessinfo.co.uk/content/what-it-risk

[4]https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/fundamentals

[5]https://www.uni-konstanz.de/en/occupational-safety-health-and-environmental-protection/occupational-safety/risk-assessment/making-a-risk-assessment/

[6]https://www.pmlearningsolutions.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1

[7] https://projectriskcoach.com/evaluating-risks-using-quantitative-risk-analysis/

[8]https://www.pmlearningsolutions.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1

[9] https://project-management-knowledge.com/definitions/i/implement-risk-response/

[10] https://www.rockcyber.com/blog/implementing-risk-responses

[11] https://www.pmi.org/learning/library/risk-analysis-project-management-7070

[12] Risk Management Plan, Private Placement Content Management System, Commonwealth of Massachusetts Information Technology Division CW Risk Management Plan, Kathy Cibotti, 9/15/2009

[13] https://humanassetrm.wordpress.com/2014/05/28/cause-risk-effect-format-in-identify-risks/

[14] https://ethicalboardroom.com/understanding-risk-in-the-strategy-setting-process/

[15] https://erau.instructure.com/eportfolios/8791/Planning_Process_Group/

[16] Rossouw von Solms*, Johan van Niekerk, From information security to cyber security, Elsevier Journal, April 2013

[17] Whitman ME, Mattord HJ., Principles of information security, 3rd ed., Thompson Course Technology; 2009; p.8

[18]https://www.lawinsider.com/dictionary/cyber-asset

[19] ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management

[20] "ENISA Glossary". *Archived from* the original *on 2012-02-29. Retrieved 2010-11-21.*

[21]"An Introduction to Factor Analysis of Information Risk (FAIR)", Risk Management Insight LLC, November 2006 Archived 2014-11-18 at the Wayback Machine;

[22] https://www.versify.com/how-do-i-define-a-cyber-security-asset/

[23] Eric Knapp, in Industrial Network Security, 2011

[24] Eric D. Knapp, Joel Thomas Langill, in Industrial Network Security (Second Edition), 2015

[25] https://www.sciencedirect.com/topics/computer-science/critical-cyber-asset

[26] https://info-savvy.com/cyber-threat-actors/

[27] https://www.netwrix.com/company.html

[28] https://www.logicgate.com/blog/grc-101-what-is-cyber-risk/

[29] https://en.wikipedia.org/wiki/Risk_factor_(computing)

[30] https://www.itgovernance.co.uk/cyber-security-risk-management

[31] https://www.dnvgl.com/article/the-three-pillar-approach-to-cyber-security-starts-with-people-134252

[32] https://www.dnvgl.com/article/the-three-pillar-approach-to-cyber-security-processes-are-crucial-162890

[33] https://ethicalboardroom.com/understanding-risk-in-the-strategy-setting-process/

[34] Sameer Sharma, *Cybersecurity : ITU Initiatives*, Tehran , Iran 12-16 May 2018

[35] ENISA, Guidelines for SMEs on the security of personal data processing, December 2016

[36] NIST, NIST Privacy Framework: A tool for improving privacy through enterprise risk management, Version 1.0, January 2020

[37] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[38] https://www.itgovernance.co.uk/cobit

[39] https://www.balbix.com/insights/what-is-cyber-security-posture/

[40] https://simplicable.com/new/technology-risk-management

[41] https://www.nibusinessinfo.co.uk/content/cyber-insurance

[42] https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/

43https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/

[44] https://www.aon.com/2021-cyber-security-risk-report/

[45] https://www.riskmanagementstudio.com/black-swans-cost-and-prediction/

[46] https://hbr.org/2016/09/preparing-for-a-black-swan-cyberattack

[47] https://securityintelligence.com/can-cyber-situational-awareness-prevent-the-next-black-swan-cyber-event/

[48] https://www.businesswire.com/news/home/20201102005334/en/Stealthbits-Predicts-2021-to-be-the-Year-of-the-Black-Swan-Event

[49] https://en.wikipedia.org/wiki/Critical_infrastructure

[50] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

[51] https://www.securityinfowatch.com/critical-infrastructure/article/21223544/the-critical-infrastructure-cybersecurity-dilemma

[52] Cyber-Physical Threat Intelligence for Critical Infrastructures Security A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures

[53]https://www.orange-business.com/en/magazine/new-generation-critical-infrastructures-secure

[54] Cyber-Physical Threat Intelligence for Critical Infrastructures Security A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures

[55] Natasha Bernal, "Metro Bank hit by cyber-attack used to empty customer accounts," The Telegraph, February, 2019, available at: https://www.telegraph.co.uk/technology/2019/02/01/metro-bank-hit-cyber-attack-used-emptycustomer-accounts/

[56] "BOVgoes dark after hackers go aftere13 m," Time ofValletta, February 2019, available at: https://timesofmalta.com/articles/view/bank-of-valletta-goes-dark-after-detecting-cyber-attack.701896

[57] Antoine Bouveret, "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," International Monetary Fund (IMF) Paper, July 2018

[58] "Cyber security in Financial ServicesMarket:Market players,Market Research, Growth During, to 2018–2023,"Marketwatch Press Release, September 2019, available at: https://www.marketwatch.com/press-release/cyber-security-in-financial-services-market-market-players-market-research-growth-during-to-2018-2023-2019-09-17

[59] European Parliament and Council. Directive (EU) 2016/1148, measures for a high common level of security of network and information systems across the Union, 2016

[60]The Industrial Internet Security Framework Technical Report, available at: htsps://www.iiconsortium.org/IISF.htm

[61] Project Number: 786727 - FINSEC D2.2 Report on applicable Standards and Regulations FINSEC, Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures, Start Date of Project: 2018-05-01 ,Duration: 36 months

[62] https://www.tensorflow.org/guide/summaries_and_tensorboard

[63] https://keras.io/

[64] https://pytorch.org/

[65] http://www.shogun-toolbox.org/

[66] Project Number: 786727 D3.4 Predictive Security Analytics Infrastructure, Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures, Start Date of Project: 2018-05-01, Duration: 36 months

[67] https://www.finsec-project.eu/

If you don't invest in risk management, it doesn't matter what business you're in, it's a risky business.

Gary Cohn