Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνίων
Τμήμα Ψηφιακών Συστημάτων

Επίπεδο: Προπτυχιακό/Μεταπτυχιακό Πρόγραμμα Σπουδών

Μάθημα -Τίτλος Μαθήματος
Μεταπτυχιακή Διπλωματική Εργασία

Τίτλος -Ατομικής Άσκησης
Διοίκηση Επιχειρησιακής Συνέχειας
Επιβλέπων Καθηγητής: Στέφανος Γκρίτζαλης

Ονοματεπώνυμο	E-mail	Α.Μ.
Κουκουρής Γεώργιος	georgios.koukouris@ssl-unipi.gr	MTE2111

Πειραιάς
12/02/2023

Περίληψη

Οι οργανισμοί εκτίθενται όλο και συχνότερα σε ένα ευρύ φάσμα διαταραχών και καταστροφών με ελάχιστη έως καθόλου προβλεψιμότητα, με αποτέλεσμα οι συνέπειες να είναι μεγάλες. Η ικανότητα ενός οργανισμού να αντιδρά γρήγορα και αποτελεσματικά είναι απαραίτητη για την επιβίωσή του στην περίπτωση μιας απρόβλεπτης καταστροφής. Οι οργανισμοί είναι σε θέση να υιοθετούν και να κωδικοποιούν τις θεμελιώδεις αρχές ενός Συστήματος Διαχείρισης Επιχειρηματικής Συνέχειας με τη χρήση προτύπων, όπως το ISO 22301. Οι οργανισμοί ενισχύοντας την αντοχή τους σε κινδύνους ποικίλων μορφών, που ενδέχεται να επηρεάσουν την ικανότητα τους να διεξάγουν επιχειρησιακές δραστηριότητες, αποκτούν την δυνατότητα να προστατεύσουν τους υπαλλήλους τους, τα συμφέροντα όλων των εμπλεκόμενων μελών και να διατηρούν τη φήμη και την εμπορική τους αξία. Σκοπός της παρούσας μελέτης είναι η παρουσίαση προτάσεων με σκοπό την διασφάλιση της επιχειρηματικής συνέχειας βάσει της μελέτης των αντίστοιχων προτύπων ISO και NIST.

Abstract

Organizations are more frequently and with greater consequence exposed to a wide range of disruptions and catastrophes with little to no predictability. The ability of an organization to react swiftly and effectively is essential to its survival in the event of an unforeseen catastrophe or catastrophic events. Organizations can adopt and codify the fundamentals of a Business Continuity Management (BCM) System with the use of standards like ISO 22301. By strengthening their resistance to risks and other business hazards that can have an impact on their ability to conduct business, organizations can protect their employees, protect the interests of all parties involved, and maintain their reputation and commercial activity. This study makes recommendations of how to ensure business continuity by looking into ISO and NIST standards.

Περιεχόμενα

Εισαγωγή

Σήμερα ο σχεδιασμός των επιχειρησιακών διαδικασιών καθοδηγείται από στόχους, όπως η διαθεσιμότητα των υπηρεσιών, η έγκαιρη παράδοση τους και η ικανοποίηση των προσδοκιών των πελατών. Για τη βιωσιμότητα των οργανισμών είναι απαραίτητο να μπορούν σε συνεχή να βάση να παραδίδουν με συνέπεια το σωστό προϊόν στους τελικούς τους πελάτες, την κατάλληλη στιγμή και στην τιμή που του αναλογεί. Προκειμένου να διασφαλιστεί η διαθεσιμότητα της εκάστοτε υπηρεσίας οι οργανισμοί οφείλουν να είναι σε θέση να την σχεδιάζουν σε μεγαλύτερη κλίμακα από το καθιερωμένο, με σκοπό να αντιμετωπιστούν όλες οι πιθανές απειλές. Οι περισσότερες επιχειρήσεις και οργανισμοί αντιμετωπίζουν κινδύνους οι οποίοι χωρίζονται στις παρακάτω κατηγορίες:

- Φυσικοί κίνδυνοι π.χ. σεισμοί
- Ανθρωπογενείς κίνδυνοι π.χ. τρομοκρατία
- Λειτουργικοί κίνδυνοι π.χ. προβλήματα στην ποιότητα παραγωγής
- Στρατηγικοί κίνδυνοι π.χ. τεχνολογική πρόοδος
- Ρίσκα που αφορούν πληροφορίες π.χ. κυβερνοέγκλημα , μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, malware
- Ρίσκα συμμόρφωσης π.χ. ποινές που αφορούν μη συμμόρφωση .

Οι διαδικασίες και οι σχετικές υπηρεσίες βρίσκονται στο επίκεντρο της υλοποίησης της στρατηγικής μιας επιχείρησης. Οι διαδικασίες αποτελούνται από σύνολα δραστηριοτήτων που έχουν σχεδιαστεί για να προσφέρουν αξία στους πελάτες. Αυτές οι διαδικασίες εξαρτώνται από ανθρώπινους πόρους για την έναρξη, τη θέσπιση και τον έλεγχο συγκεκριμένων δραστηριοτήτων. Επιπλέον, εξαρτώνται από υποδομές, υλικούς, οικονομικούς και πληροφοριακούς πόρους για την παροχή του πλαισίου (context) και των εισροών από τις οποίες μπορεί να δημιουργηθεί αξία [1].

Οι διεργασίες βρίσκονται στα παραδοσιακά λειτουργικά και οργανωτικά όρια και πρέπει να ενσωματώνονται αποτελεσματικά, να παρακολουθούνται και να προστατεύονται, εάν πρόκειται να αποφευχθούν βλάβες σε παραγωγικά συστήματα και σημεία παράδοσης. Οι διαδικασίες εξαρτώνται επίσης σε μεγάλο βαθμό από τις πληροφορίες και την τεχνολογία και οι αστοχίες των υποκείμενων συστημάτων μπορεί

να είναι δαπανηρές για έναν οργανισμό. Μερικές από τις επιπτώσεις που μπορεί να έχει η διακοπή παροχής υπηρεσιών σε ένα οργανισμό είναι οι παρακάτω:

- οικονομικές: π.χ. απώλεια παραγγελιών για μια χρονική περίοδο, πρόσθετο κόστος για την ανάκτηση της υπηρεσίας, απώλεια μεριδίου αγοράς κ.λπ.
- αναξιοπιστία ή εταιρική δυσφήμιση π.χ. απώλεια αξιοπιστίας, πολιτική ή εταιρική δυσφήμιση κ.λπ.
- νομικές ενέργειες εναντίων του οργανισμού για συμβατικές παραβιάσεις, δημοσιοποίηση προσωπικών στοιχείων και παραβίαση της νομοθεσίας περί προστασίας δεδομένων κ.λπ.

Παρόλη την σημαντικότητα της συνεχόμενης και αδιάληπτης διάθεσης προϊόντων και υπηρεσιών είναι αρκετά τα παραδείγματα όπου η συγκεκριμένη απαίτηση δεν καλύφθηκε με αποτέλεσμα την διακοπή παροχής υπηρεσιών. Μερικά παραδείγματα αποτελούν:

- Το 2010 λόγω ενός προβλήματος στο σύστημα ψύξης σε datacenter της εταιρίας Wikipedia προκλήθηκε ο τερματισμός λειτουργίας του. Η εταιρία χρησιμοποίησε μηχανισμό failover σε άλλο datacenter, όμως η διαδικασία δεν λειτούργησε με αποτέλεσμα να πέσει η ιστοσελίδα της [2].
- Το 2012 λόγω καιρικών φαινομένων υπήρξε διακοπή ρεύματος στο data center της εταιρίας Cogeco Peer 1. Η εταιρία διέθετε γεννήτριες οι οποίες ενεργοποιήθηκαν. Παρόλα αυτά η δεξαμενή καυσίμων εξαιτίας των καιρικών φαινομένων αποσυνδέθηκε, με αποτέλεσμα η εταιρία να αναγκαστεί να απενεργοποιήσει τα συστήματά της [3].
- Το 2013 λόγω ενός αποτυχημένου software update η θερμοκρασία στο datacenter της εταιρείας Microsoft ανέβηκε σε τέτοιο σημείο που τα μέτρα αποτροπής του φαινομένου που είχε σχεδιάσει η εταιρία δεν μπορούσαν να εφαρμοστούν. Μέχρι να διορθωθεί το πρόβλημα οι υπηρεσίες Hotmail και Outlook ήταν εκτός λειτουργίας [4].
- Το 2016 λόγω ενός προβληματικού UPS της εταιρείας Telecity LD8 προκλήθηκε outage το οποίο είχε ως αποτέλεσμα προβλήματα σύνδεσης σε όσους καταναλωτές χρησιμοποιούσαν το δίκτυο οπτικών ινών [5].
- Το 2021 προκλήθηκε φωτιά σε datacenter του cloud provider OVH. Η φωτιά προκάλεσε την καταστροφή του datacenter, ζημιές στο διπλανό datacenter της

εταιρίας καθώς και την παύση λειτουργίας 2 άλλως κοντινών datacenter για προληπτικούς λόγους [6].

Εικόνα 1 Το datacenter της εταιρίας OVH μετά το πέρας της πυρκαγιάς

- Το 2021 η μη κερδοσκοπική οργάνωση Scripps δέχτηκε επίθεση ransomware που οδήγησε στην κλοπή στοιχείων 150 χιλιάδων ασθενών. Εν συνεχεία βρέθηκε ότι η επίθεση επηρέασε και 2 νοσοκομεία του οργανισμού κι έτσι αναγκάστηκαν σε παύση της λειτουργίας τους για αρκετές εβδομάδες [7].
- Το 2022 εξαιτίας της ασυνήθιστης αύξησης της θερμοκρασίας οι εταιρείες Google και Oracle αναγκάστηκαν να διακόψουν την λειτουργία ενός μέρους των συστημάτων τους λόγω της ανεπάρκειας των συστημάτων ψύξης να καλύψουν τις απαιτήσεις ψύξης στα datacenter τους [8].

Βάσει των παραπάνω παραδειγμάτων δύναται κανείς να συμπεράνει ότι τα θέματα επιχειρησιακής συνέχειας απασχολούν ακόμα και σήμερα εταιρείες και οργανισμούς ανεξαρτήτως μεγέθους και φύσης των παρεχόμενων υπηρεσιών.

Σκοπός της εργασίας είναι η μελέτη μεθόδων ασφάλειας και ανθεκτικότητας οργανισμών και διαδικασιών, όπως και μεθόδων ασφάλειας και τεχνικών αποκατάστασης πληροφοριακών συστημάτων. Η μελέτη των συγκεκριμένων θεμάτων βασίζεται πάνω στα υπάρχοντα πρότυπα ISO τα οποία σχετίζονται με την επιχειρησιακή συνέχεια. Τα πρότυπα αυτά είναι τα ISO 22300 [9], 22301 [10], 22316 [11], 22320 [12], 24762 [13], 27031 [14].

1 Ασφάλεια και Ανθεκτικότητα Οργανισμών και Διαδικασιών

Οι διακοπές και οι αναταραχές χαρακτηρίζουν τις σύγχρονες επιχειρήσεις παροχής υπηρεσιών. Οι αναταραχές αυτές μπορούν να προκαλέσουν ανησυχία στις επιχειρήσεις όσον αφορά την επιβίωσή τους καθώς και την βιωσιμότητα των επιχειρήσεων.

Σε αυτό το δύσκολο περιβάλλον, οι οργανισμοί πρέπει να είναι ανθεκτικοί. Η ανθεκτικότητα (Resilience) προέρχεται από την λατινική λέξη «resiliere» και αναφέρεται στην ικανότητα ανάκαμψης. Εμφανίστηκε στην ακαδημαϊκή βιβλιογραφία χάρις στο έργο του Holling [15] στον τομέα της οικολογίας και των οικοσυστημάτων. Στη συνέχεια, οι μελέτες ανθεκτικότητας εξαπλώθηκαν σε ένα πλήθος ερευνητικών πεδίων, ως γενική ιδιότητα πολλών διαφορετικών συστημάτων, που ορίζεται ως η ικανότητα ανάκαμψης και αντίστασης σε διαταραχές.

Όσον αφορά την επιχειρησιακή ανθεκτικότητα, δύναται να οριστεί ως «η ικανότητα του οργανισμού να αντιμετωπίζει διακοπές και απροσδόκητα γεγονότα χάρη στη στρατηγική ενημέρωση και τη διασυνδεδεμένη επιχειρησιακή διαχείριση εσωτερικών και εξωτερικών διαταραχών» [16]. Επιπλέον, είναι σημαντικό να επισημανθούν δύο ιδιαίτερα χαρακτηριστικά της ανθεκτικότητας που προέρχονται από τη στατική και τη δυναμική της φύση. Η στατική ανθεκτικότητα βασίζεται κυρίως στην ετοιμότητα και τα προληπτικά μέτρα για την ελαχιστοποίηση των απειλών όσον αφορά την πιθανότητα εμφάνισης και τον πιθανό αντίκτυπο, ενώ η δυναμική ανθεκτικότητα επικεντρώνεται περισσότερο στην αποτελεσματική διαχείριση ατυχημάτων και απρόβλεπτων γεγονότων για να συντομεύσει τα δυσμενή επακόλουθα και να μεγιστοποιήσει την ταχύτητα ανάκαμψης του οργανισμού [17, 18] .

Ως εκ τούτου, είναι ζωτικής σημασίας για τις εταιρείες να λάβουν μέτρα για την οικοδόμηση οργανωτικής ανθεκτικότητας, για τη διατήρηση της ανταγωνιστικότητας και τη διασφάλιση της βιωσιμότητας των επιχειρήσεων. Στο γενικό πλαίσιο που περιγράφεται παραπάνω, οι εταιρείες αντιμετωπίζουν μια σειρά από νέες απειλές που σχετίζονται με επιθέσεις στον κυβερνοχώρο. Οι απειλές που αφορούν το cybersecurity παρουσιάζονται όλο και πιο συχνά [19]. Στο παρελθόν, η βιβλιογραφία για την οργανωτική ανθεκτικότητα επικεντρωνόταν κυρίως σε εταιρείες προϊόντων και αλυσίδες εφοδιασμού. Ωστόσο, έχει αυξηθεί η ανάγκη να διερευνηθεί με μεγαλύτερη λεπτομέρεια η ανάπτυξη της ανθεκτικότητας στις εταιρείες παροχής υπηρεσιών [20].

1.1 Τεχνικές Ενίσχυσης Της Επιχειρησιακής Ανθεκτικότητας

Οι κρίσεις και τα ανησυχητικά γεγονότα είναι ένας τρόπος δοκιμασίας και ελέγχου μέσω του οποίου επικυρώνεται εάν οι οργανισμοί είναι αρκετά ανθεκτικοί για να αντέξουν τις αντιξοότητες και να ευημερήσουν. Για τους περισσότερους οργανισμούς η μεγαλύτερη δυσκολία έγκειται στην καθιέρωση επιπέδων ωριμότητας της οργανωτικής ανθεκτικότητας. Η δυσκολία αυτή δεν οφείλεται απαραιτήτως στην απουσία προτύπων καθώς μέχρι στιγμής υπάρχουν δύο τέτοια πρότυπα. Συγκεκριμένα, υπάρχει το Βρετανικό πρότυπο 65000, Organizational resilience (BS 65000:2022) [21] και το ISO 22316 Security and resilience — Organizational resilience — Principles and attributes (ISO 22316:2017). Για το κεφάλαιο αυτό έχει πραγματοποιηθεί μελέτη του ISO 22316.

Σύμφωνα με το ISO 22316 ως οργανωτική ανθεκτικότητα ορίζεται η ικανότητα ενός οργανισμού να απορροφά και να προσαρμόζεται σε ένα μεταβαλλόμενο περιβάλλον για να του επιτρέψει να επιτύχει τους στόχους του και να επιβιώσει και να ευημερήσει. Οι πιο ανθεκτικοί οργανισμοί μπορούν να προβλέψουν και να ανταποκριθούν σε απειλές και ευκαιρίες, που προκύπτουν από ξαφνικές ή σταδιακές αλλαγές στο εσωτερικό και εξωτερικό τους πλαίσιο. Η ανθεκτικότητα ενός οργανισμού επηρεάζεται την αλληλεπίδραση και τον συνδυασμό στρατηγικών και οργανωτικών παραγόντων. Η δέσμευση ενός οργανισμού για ενίσχυση της οργανωτικής ανθεκτικότητας συμβάλλει:

- Βελτιωμένη ικανότητα πρόβλεψης και αντιμετώπισης κινδύνων και τρωτών σημείων.
- Αυξημένο συντονισμό και ενοποίηση των κλάδων διαχείρισης για τη βελτίωση της συνοχής και της απόδοσης.
- Μεγαλύτερη κατανόηση των ενδιαφερομένων μερών και των εξαρτήσεων που υποστηρίζουν στρατηγικούς στόχους και στόχους.

Στο στάνταρντ καθιερώνονται οι αρχές για την οργανωτική ανθεκτικότητα. Επιπλέον, προσδιορίζονται τα χαρακτηριστικά και οι δραστηριότητες που υποστηρίζουν έναν οργανισμό στην ενίσχυση της ανθεκτικότητάς του. Σκοπός του στάνταρντ είναι η παροχή καθοδήγησης για την επίτευξη οργανωτικής ανθεκτικότητας σε οργανισμούς

,ανεξαρτήτως μεγέθους. Στο στάνταρντ περιγράφονται οι αρχές (principles), τα γνωρίσματα (attributes) , οι τρόποι αξιολόγησης και οι διοικητικές απαιτήσεις για την επίτευξη της οργανωτικής ανθεκτικότητας.

1.1.1 Αρχές Της Επιχειρησιακής Ανθεκτικότητας

Στην παράγραφο 4 του ISO 22316 περιγράφονται οι αρχές οι οποίες παρέχουν τη βάση πάνω στην οποία μπορεί να αναπτυχθεί, να εφαρμοστεί και να αξιολογηθεί ένα πλαίσιο και μια στρατηγική για την επίτευξη μιας ενισχυμένης κατάστασης οργανωτικής ανθεκτικότητας.

Η αποτελεσματικότητα της οργανωτικής ανθεκτικότητας ενισχύεται όταν η συμπεριφορά (ενέργειες) του οργανισμού συμβαδίζει με το κοινό όραμα και σκοπό του οργανισμού. Επιπλέον, επηρεάζεται από την ικανότητα του συντονισμού μεταξύ του διοικητικού κλάδου σε συνδυασμό με ανατροφοδότηση που δέχεται από τεχνολογικούς και επιστημονικούς τομείς.

Επιπρόσθετα, η αποτελεσματικότητα της διαδικασίας βασίζεται στην ικανότητα αποτελεσματικής προσαρμογής του οργανισμού στις αλλαγές, στις διοικητικές και διαχειριστικές αποφάσεις στην αποτελεσματική διαχείριση του ρίσκου και στην κατανόηση του πλαισίου (context) του οργανισμού.

Ως context ορίζονται οι εσωτερικοί και εξωτερικοί παράγοντες οι οποίοι καθορίζουν την λειτουργία ενός οργανισμού. Σε αυτό το σημείο πρέπει να τονιστεί πως οι οργανισμοί οφείλουν να προσέχουν ιδιαίτερα τους εξωτερικούς παράγοντες. Μερικοί από αυτούς είναι οι γεωγραφικοί, περιβαλλοντικοί, κοινωνικοί και οι νομικές απαιτήσεις και συμβάσεις με προμηθευτές ή πελάτες. Οι εξωτερικοί αυτοί παράγοντες είναι συνεπώς υποχρεώσεις/στοιχεία που ο οργανισμός δεν μπορεί να ελέγξει, πρέπει όμως να συμμορφώνεται και να προσαρμόζεται σε αυτά.

Οι οργανισμοί οφείλουν να αναπτύξουν μία συντονισμένη προσέγγιση που να παρέχει μία εντολή η οποία να δεσμεύει την διοίκηση με σκοπό την εξασφάλιση, πως το διοικητικό προσωπικό θα αφοσιωθεί στην ενίσχυση της οργανωτικής ανθεκτικότητας. Επίσης, οι οργανισμοί θα χρειαστεί να διαθέσουν τους απαραίτητους πόρους, δομές διακυβέρνησης, μηχανισμούς και συστήματα ελέγχου και αξιολόγησης. Τέλος, ο οργανισμός θα πρέπει να αναπτύξει αποτελεσματικές μεθόδους επικοινωνίας με σκοπό την βελτίωση κατανόησης και λήψης αποφάσεων.

1.1.2 Γνωρίσματα Της Επιχειρησιακής Ανθεκτικότητας

Οι οργανισμοί που υιοθετούν τις αρχές της ανθεκτικότητας επιδεικνύουν κοινά χαρακτηριστικά που υποστηρίζονται από δραστηριότητες, τα οποία καθοδηγούν τη χρήση, την αξιολόγηση και την βελτίωσή τους. Τέτοια χαρακτηριστικά περιλαμβάνουν:

- Το κοινό όραμα και τη σαφήνεια του σκοπού. Η οργανωτική ανθεκτικότητα ενισχύεται όταν υπάρχει ένας σαφώς διατυπωμένος και κατανοητός σκοπός, όραμα και αξίες προκειμένου να επιτυγχάνεται η σαφήνεια κατά την λήψη αποφάσεων σε όλα τα επίπεδα της επιχείρησης. Οι οργανισμοί εκτός από την διατύπωση είναι αναγκαίο να φροντίσουν και για την επικοινωνία των κύριων αξιών σε όλα τα ενδιαφερόμενα μέρη [22]. Επιπλέον, πρέπει να βεβαιωθούν και να παρακολουθούν ότι οι επιμέρους στόχοι συμβαδίζουν με τις αξίες που έχουν αναφερθεί. Σημαντικό ρόλο παίζει και η αναγνώριση της ανάγκης αναθεώρησης των αξιών, καθώς και η αναζήτηση καινοτόμων μέσων και ιδεών για την για την ανάπτυξη στρατηγικών ,για την επιχείρηση, στόχων.
- Κατανόηση και επιρροή του context. Η πιο ολοκληρωμένη κατανόηση των εσωτερικών και εξωτερικών περιβαλλόντων της επιχείρησης οδηγεί στην ενίσχυση της ικανότητας σκέψης και σχεδιασμού πέρα από τις υπάρχουσες διαδικασίες, στρατηγικές όπως και στην καλύτερη κατανόηση, συνεργασία με τα ενδιαφερόμενα μέρη με στόχο την επίτευξη των στόχων του οργανισμού. Οι οργανισμοί πρέπει να παρακολουθούν και να αξιολογούν συνεχώς τις αλληλεξαρτήσεις, το πολιτικό και ρυθμιστικό περιβάλλον τους και τις δραστηριότητες των ανταγωνιστών τους. Επίσης, οι οργανισμοί είναι αναγκαίο να διατηρούν καλές σχέσεις με τα συνεργαζόμενα μέλη, ειδικά με αυτά που μοιράζονται το ίδιο όραμα και στόχους, δημιουργώντας συνεργασίες σε όλα τα επίπεδα.
- Αποτελεσματική ηγεσία. Η επιχειρησιακή ανθεκτικότητα ενισχύεται όταν η ηγεσία ενός οργανισμού ενθαρρύνει άλλους να ηγηθούν σε ένα εύρος καταστάσεων και συνθηκών, συμπεριλαμβανομένων συνθηκών αβεβαιότητας και διαταραχών. Ο οργανισμός επιβάλλεται να δώσει προτεραιότητα και πόρους στην ανάπτυξη έμπιστων και αξιοσέβαστων αρχηγών οι οποίοι δρουν

για την επίτευξη των στόχων της επιχείρησης. Επιπρόσθετα, πρέπει να διαμοιράζει ρόλους και καθήκοντα με σκοπό την ενίσχυση της επιχειρησιακής ανθεκτικότητας, να ενθαρρύνει την δημιουργία μάθησης βασισμένη σε προηγούμενα περιστατικά και να ενδυναμώνει όλα τα επίπεδα του οργανισμού με σκοπό τη λήψη αποφάσεων για προστασία του.

- Κουλτούρα υποστήριξης της οργανωτικής ανθεκτικότητας. Μια κουλτούρα που υποστηρίζει την οργανωτική ανθεκτικότητα δείχνει δέσμευση και ύπαρξη κοινών πεποιθήσεων και αξιών. Οι οργανισμοί είναι ουσιαστικό να δώσουν προτεραιότητα στον καθορισμό των πεποιθήσεων, των αξιών και συμπεριφορών οι οποίες καθορίζουν την κουλτούρα του οργανισμού. Επιπλέον, πρέπει να αναγνωρίσουν τις αξίες και συμπεριφορές που ενισχύουν την επιχειρησιακή ανθεκτικότητα, να παροτρύνουν το προσωπικό να προβάλουν σε όλα τα επίπεδα τις συγκεκριμένες αρχές, να το εμψυχώσει με σκοπό να αναγνωρίζουν και επικοινωνούν απειλές και ευκαιρίες και να δρουν ως προς όφελος του οργανισμού. Εν συνεχεία, είναι ανάγκη να προάγει την δημιουργικότητα και την καινοτομία, να παρακολουθεί και να αξιολογεί αλλαγές στην κουλτούρα του οργανισμού οι οποίες μπορεί να επηρεάσουν την οργανωτική ανθεκτικότητα.
- Διαμοιρασμένη πληροφορία και γνώση. Όταν η γνώση μοιράζεται ευρέως, είναι κατάλληλη και εφαρμόζεται, έτσι η οργανωτική ανθεκτικότητα βελτιώνεται. Ενθαρρύνεται η μάθηση από την εμπειρία καθώς και η μάθηση του ενός από την γνώση του άλλου. Ο οργανισμός οφείλει να επιδεικνύει και να ενισχύει την αξία της πληροφορίας, της μάθησης και της γνώσης και ότι η μάθηση προέρχεται από όλες τις διαθέσιμες πηγές. Ακόμη, ο οργανισμός θα πρέπει να διασφαλίζει ότι οι πληροφορίες είναι εύκολα προσβάσιμες, κατανοητές, αποτελεσματικά κοινοποιημένες, ότι χρησιμοποιούνται στην οργανωτική μάθηση και αναγνωρίζονται ως κρίσιμοι πόροι.
- Διαθεσιμότητα πόρων. Οι άνθρωποι, οι εγκαταστάσεις, η τεχνολογία, τα οικονομικά και οι πληροφορίες είναι σημαντικό να αναπτυχθούν και να διατεθούν από τον οργανισμό για την αντιμετώπιση των τρωτών σημείων και την παροχή της ικανότητας προσαρμογής στις μεταβαλλόμενες συνθήκες. Για να αποφευχθούν μεμονωμένα σημεία αποτυχίας και να ανταποκριθεί σε ορισμένα περιστατικά και αλλαγές, ο οργανισμός θα πρέπει να δώσει

προτεραιότητα και να τροφοδοτήσει τη λήψη των κατάλληλων αποφάσεων σχετικά με τους πόρους και τη χωρητικότητα, τη διαφοροποίηση, την αναπαραγωγή και τον πλεονασμό, έτσι ώστε οι βασικές υπηρεσίες να διατηρούνται σε αποδεκτό, προκαθορισμένο επίπεδο . Για να συμβάλουν στην ικανότητα του οργανισμού να ανταποκρίνεται και να προσαρμόζεται στην αλλαγή, οι επιλεγμένοι υπάλληλοι θα πρέπει να αναπτύξουν ένα ποικιλόμορφο σύνολο δεξιοτήτων και γνώσεων. Συμπληρωματικά, προκειμένου να προσαρμοστεί στις νέες συνθήκες, ο οργανισμός θα πρέπει να αναπτύξει την ικανότητα να εντοπίζει και να ανταποκρίνεται στην αλλαγή με ευέλικτο τρόπο.

- Ανάπτυξη και συντονισμό των πειθαρχιών διαχείρισης. Ο σχεδιασμός, η ανάπτυξη και ο συντονισμός των κλάδων διαχείρισης, όπως και η ευθυγράμμισή τους με τους στρατηγικούς στόχους του οργανισμού, είναι κρίσιμες για την αύξηση της οργανωτικής ανθεκτικότητας. Ο οργανισμός θα είναι σημαντικό να επιδεικνύει και να βελτιώνει συντονισμένους κλάδους διαχείρισης που συμβάλλουν ατομικά και συλλογικά στον σκοπό του οργανισμού και στην προστασία αυτού. Επιπλέον, ο οργανισμός θα πρέπει να διαχειρίζεται τον αντίκτυπο της αβεβαιότητας στους στόχους του σε όλους τους κλάδους διαχείρισης. Ο οργανισμός οφείλει να δώσει προτεραιότητα στον εντοπισμό και το σχεδιασμό των κλάδων διαχείρισης που συμβάλλουν στην ανθεκτικότητα του οργανισμού, να αξιολογεί πώς κάθε κλάδος διαχείρισης συμβάλλει στην ανθεκτικότητα του οργανισμού σε τακτική βάση, να δημιουργεί ευελιξία στους κλάδους διαχείρισης και να βελτιώνει την επικοινωνία, τον συντονισμό και τη συνεργασία μεταξύ των κλάδων διαχείρισης, ώστε να δημιουργήσει μια συνεκτική προσέγγιση.
- Υποστήριξη της συνεχούς ανάπτυξης. Η οργανωτική ανθεκτικότητα ενισχύεται όταν οι οργανισμοί παρακολουθούν συνεχώς την απόδοσή τους με βάση προκαθορισμένα κριτήρια, με σκοπό να μάθουν και να βελτιωθούν από την εμπειρία και να αξιοποιήσουν τις ευκαιρίες. Ο οργανισμός θα πρέπει να παρουσιάζει μια κουλτούρα συνεχούς βελτίωσης για να διασφαλίσει ότι οι οργανωτικοί στόχοι, στρατηγικές και διαδικασίες παραμένουν συναφείς και κατάλληλες για την υποστήριξη των μεταβαλλόμενων αναγκών του οργανισμού. Επιπλέον, ο οργανισμός πρέπει να επιδείξει δέσμευση ως προς την επικύρωση και τη συνεχή βελτίωση των δραστηριοτήτων και ικανοτήτων της

οργανωτικής ανθεκτικότητας. Για να υποστηρίξει τη συνεχή βελτίωση και να διασφαλίσει ότι τα κριτήρια διαχείρισης απόδοσης ανταποκρίνονται σε αλλαγές που επηρεάζουν τους στόχους του οργανισμού, ο οργανισμός προέχει να δώσει προτεραιότητα στους μηχανισμούς παρακολούθησης και αξιολόγησης της απόδοσης.

- Ικανότητα πρόβλεψης και διαχείριση της αλλαγής. Η οργανωτική ανθεκτικότητα αυξάνεται όταν ένας οργανισμός μπορεί να προβλέψει, να σχεδιάσει και να ανταποκριθεί στην αλλαγή. Ο οργανισμός θα πρέπει να επιδεικνύει και να βελτιώνει την ικανότητά του να εκπληρώνει με συνέπεια τις δεσμεύσεις του υπό μεταβαλλόμενες συνθήκες και να προσαρμόζει τις δραστηριότητές του ανάλογα. Εκτός από αυτό, οφείλει να παρουσιάζει την ικανότητά του να απορροφά και να προσαρμόζεται στις επιπτώσεις ξαφνικών και απροσδόκητων συμβάντων, όπως και την ετοιμότητά του να ανταποκριθεί ή να ασκεί επιρροή στις αλλαγές εάν είναι απαραίτητο. Ο οργανισμός θα πρέπει να δίνει προτεραιότητα και να προμηθεύει δραστηριότητες που αυξάνουν την επίγνωση καταστάσεων που είναι πιθανό να επηρεάσουν την αλλαγή, να προσαρμόζεται όταν είναι απαραίτητο χωρίς να έχει σημαντικό αντίκτυπο στις υπηρεσίες του, να δεσμεύεται για προστασία, απόδοση και προσαρμογή. Ταυτόχρονα να μπορεί να μετατοπίζει την εστίαση χωρίς να διακυβεύεται το όραμά του και βασικές αξίες και να διασφαλίζει ότι οι πειθαρχίες διαχείρισης είναι επαρκώς αποτελεσματικές για να ανταποκρίνονται στις αλλαγές.

1.1.3 Αξιολόγηση Των Παραγόντων Που Συμβάλουν Στην Ανθεκτικότητα

Τα μέτρα απόδοσης που χρησιμοποιούνται στη διαδικασία αξιολόγησης είναι πιθανό να επιλέγονται βάσει του κλάδου στον οποίο δραστηριοποιείται ο οργανισμός, των κριτηρίων ανώτατης διοίκησης και της οργανωτικής κουλτούρας. Οι περισσότερες επιχειρήσεις συλλέγουν ήδη δεδομένα απόδοσης που μπορούν να χρησιμοποιηθούν για την αξιολόγηση της ανθεκτικότητάς τους. Πηγές μπορεί να είναι οι υπάρχουσες πληροφορίες διαχείρισης και οι εκθέσεις εσωτερικού ελέγχου, όπως η διαδικασία επισκόπησης της επιχείρησης και η αναφορά έργων. Η ανώτατη διοίκηση είναι ουσιαστικό να καθορίζει, να αναπτύσσει κριτήρια μέτρησης, να παρακολουθεί, να αξιολογεί και να ορίζει το εύρος των κατάλληλων στόχων οργανωτικής ανθεκτικότητας. Η ανώτατη διοίκηση θα πρέπει επίσης να αποφασίζει σχετικά με τα

αποδεκτά όρια εκροών αξιολόγησης, πώς θα εφαρμοστούν οι ρυθμίσεις αξιολόγησης και παρακολούθησης και πώς θα αναλυθούν, θα αξιολογηθούν και θα προσδιοριστούν τα παραγόμενα αποτελέσματα.

Η προκαταρκτική αξιολόγηση της οργανωτικής ανθεκτικότητας είναι δυνατόν να χρησιμοποιηθεί για την ενημέρωση της επείγουσας εργασίας και για την ενίσχυση της έννοιας της οργανωτικής ανθεκτικότητας με τα ενδιαφερόμενα μέρη. Πριν από την εφαρμογή αλλαγών, ο οργανισμός οφείλει να επανεξετάσει τις συμφωνημένες μετρήσεις, για να προσδιορίσει την ανθεκτικότητα του οργανισμού, να καθορίσει εάν η ανθεκτικότητα είναι αποδεκτή από την ανώτατη διοίκηση και να εξετάσει τις κατάλληλες στρατηγικές για την αντιμετώπιση τυχόν σημαντικών κενών που εντοπίστηκαν στην αξιολόγηση.

Για να διασφαλιστεί ότι η ανθεκτικότητα του οργανισμού συνεχίζει να ανταποκρίνεται στις προσδοκίες, η ανώτατη διοίκηση θα πρέπει να διεξάγει περιοδική αναθεώρηση. Αλλαγές στο οργανωτικό πλαίσιο, όπως αλλαγές στο οργανωτικό όραμα, το επιχειρηματικό μοντέλο, τις νέες αγορές, το προσωπικό, τους κινδύνους, την αποτελεσματικότητα και ανατροφοδότηση σχετικά με την ανθεκτικότητα του οργανισμού, είναι χρήσιμο να λαμβάνονται υπόψη στην ανασκόπηση. Η παρακολούθηση της οργανωτικής ανθεκτικότητας δύναται να οδηγήσει σε συνοπτική αναφορά που παρέχει στην ανώτατη διοίκηση μια αξιολόγηση της ανθεκτικότητας σε σχέση με τα χαρακτηριστικά που είναι πιο σημαντικά για τον οργανισμό. Η ανώτατη διοίκηση θα πρέπει να παρακολουθεί τις τάσεις στα δεδομένα που χρησιμοποιούνται για την αξιολόγηση της οργανωτικής ανθεκτικότητας και να διασφαλίζει ότι τα συστήματα διαχείρισης πληροφοριών παρέχουν τα απαραίτητα δεδομένα για την υποστήριξη των εισροών που απαιτούνται για την παρακολούθηση της ανθεκτικότητας. Τα αποτελέσματα της διαδικασίας υποβολής εκθέσεων είναι απαραίτητο επίσης να χρησιμοποιηθούν από την ανώτατη διοίκηση για την ανάπτυξη πρόσθετων σχεδίων δράσης με στόχο τη βελτίωση της οργανωτικής ανθεκτικότητας.

1.2 Απαιτήσεις Συστημάτων Διαχείρισης Επιχειρησιακής Συνέχειας

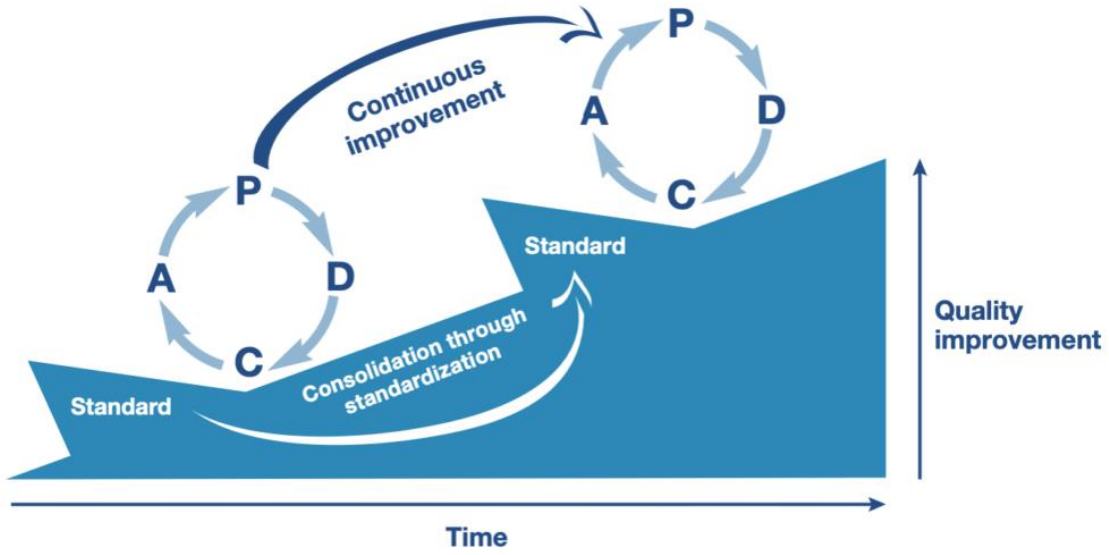
Οι οργανισμοί είναι ευάλωτοι σε ένα ευρύ φάσμα καταστροφών, με ελάχιστη ή καθόλου προβλεψιμότητα. Παραβιάσεις ασφαλείας, οικονομικές κρίσεις, εκρήξεις ηφαιστείων, σεισμοί, συμβάντα που σχετίζονται με τις καιρικές συνθήκες, όπως τυφώνες και ανεμοστρόβιλοι και η έναρξη πανδημιών όπως ο Covid-19 είναι όλα παραδείγματα καταστροφικών γεγονότων. Τις τελευταίες τρεις δεκαετίες, οι παγκόσμιες αλυσίδες εφοδιασμού έχουν εκτεθεί σε ένα ευρύ φάσμα καταστροφών, οι οποίες τείνουν να συμβαίνουν με αυξανόμενη συχνότητα και επιπτώσεις.

Ο σχεδιασμός της επιχειρησιακής συνέχειας είναι ο πιο αποτελεσματικός τρόπος προετοιμασίας για πιθανές κρίσεις και μείωση των επιπτώσεων της διακοπής παροχής προϊόντων και υπηρεσιών. Όταν συμβαίνει ένα περιστατικό, η χρήση ενός αποτελεσματικού σχεδιασμού έκτακτης ανάγκης διασφαλίζει ότι όλοι στην εταιρεία ακολουθούν το συγκεκριμένο σχέδιο. Οι πρακτικές ιδέες έκτακτης ανάγκης και τα σχέδια ανάκτησης επιτρέπουν την συνέχιση των παραγωγικών λειτουργιών το συντομότερο δυνατό μετά από διακοπή ή αποτυχία των επιχειρηματικών διαδικασιών, υπηρεσιών, υπηρεσιών πληροφορικής ή συστημάτων ενός οργανισμού. Μέσω ενός σχεδίου επιχειρησιακής συνέχειας είναι πιθανό να μειωθεί αποτελεσματικά το κόστος που σχετίζεται με καταστροφές, να ικανοποιηθούν οι απαιτήσεις συμμόρφωσης και να δημιουργηθεί ένα ολοκληρωμένο σύστημα διαχείρισης κινδύνου που παρέχει ασφάλεια δικαίου και ανταγωνιστικό πλεονέκτημα. Αυξάνοντας τη διαθεσιμότητά των υπηρεσιών , ένας οργανισμός μπορεί να αποκτήσει σημαντικό ανταγωνιστικό πλεονέκτημα, επειδή οι πελάτες και οι επιχειρηματικοί εταίροι μπορούν να βασιστούν στην επιχείρηση για να παραμείνει λειτουργική ακόμη και σε περιόδους κρίσης.

Η έρευνα για αυτό το κεφαλαίο βασίστηκε σε ένα τυπικό πλαίσιο για το BCM το οποίο είναι το ISO 22301:2019 . Το ISO 22301 καθορίζει τη δομή και τις απαιτήσεις για την εφαρμογή και τη διατήρηση ενός συστήματος διαχείρισης επιχειρησιακής συνέχειας (business continuity management system - BCMS[23]) που αναπτύσσει την κατάλληλη επιχειρηματική συνέχεια ως προς το μέγεθος και τον τύπο του αντίκτυπου που μπορεί ή όχι να δεχτεί ένας οργανισμός μετά από μια διακοπή. Ένα σύστημα διαχείρισης επιχειρησιακής συνέχειας είναι ένα σύστημα διαχείρισης που συνδυάζει αλληλένδετες μεθόδους, διαδικασίες και κανόνες ώστε να διασφαλίσει ότι οι κρίσιμες

επιχειρηματικές διαδικασίες συνεχίζουν να λειτουργούν σε περίπτωση ζημιάς ή έκτακτης ανάγκης, τις αναπτύσσει και τις βελτιώνει συνεχώς.

Το ISO 22301 εφαρμόζει το μοντέλο Plan, Do, Check, Act (PDCA) [24] . Το PDCA είναι ένα μοντέλο τεσσάρων βημάτων για την πραγματοποίηση της αλλαγής. Όπως ένας κύκλος δεν έχει τέλος, ο κύκλος του PDCA είναι επιτακτική ανάγκη να επαναλαμβάνεται ξανά και ξανά για την επίτευξη της συνεχούς βελτίωσης.



Εικόνα 2 Χρήση του μοντέλου PDCA με σκοπό την συνεχή βελτίωση

Κατά την υιοθέτηση του ISO 22301, ένας οργανισμός πρέπει να εντοπίζει εξωτερικές και εσωτερικές προκλήσεις που σχετίζονται με τον σκοπό του και επηρεάζουν την ικανότητά του να επιτύχει τα επιδιωκόμενα αποτελέσματα του BCMS του. Ο οργανισμός οφείλει να αξιολογήσει εάν τα ενδιαφερόμενα μέρη και οι ανάγκες τους σχετίζονται ή όχι με το BCMS. Επιπρόσθετα, η επιχείρηση πρέπει να δημιουργήσει μια διαδικασία αναγνώρισης, τεκμηρίωσης και επαλήθευσης της εφαρμογής όλων των νομικών και κανονιστικών υποχρεώσεων που σχετίζονται με τη συνέχιση των προϊόντων και των υπηρεσιών της. Ο προσδιορισμός του πεδίου εφαρμογής είναι επίσης μια ουσιαστική πτυχή της διαδικασίας σχεδιασμού του BCMS. Επίσης είναι απαραίτητος από τον οργανισμό ο ορισμός του πεδίου εφαρμογής του BCMS. Λαμβάνοντας υπόψη εξωτερικές και εσωτερικές προκλήσεις, απαιτήσεις και στόχους, ο οργανισμός θα καθορίσει τα μέρη, τα αγαθά και τις υπηρεσίες που θα συμπεριληφθούν στο BCMS με βάση το μέγεθος, τον τύπο και την πολυπλοκότητα των τοποθεσιών του.

Το top management διαδραματίζει σημαντικό ρόλο στο σχεδιασμό του BCMS αφού είναι υπεύθυνο για τη διασφάλιση πως η πολιτική και οι στόχοι της επιχειρηματικής συνέχειας έχουν θεσπιστεί και είναι συμβατοί με τη στρατηγική κατεύθυνση του οργανισμού, την ενσωμάτωση των απαιτήσεων BCMS στις επιχειρηματικές διαδικασίες του οργανισμού, τη διαθεσιμότητα των απαραίτητων πόρων για το BCMS και πως το BCMS επιτυγχάνει το επιδιωκόμενο αποτέλεσμα. Είναι πρωταρχικής σημασίας επίσης η ανώτατη διοίκηση να σχεδιάσει μια πολιτική επιχειρηματικής συνέχειας που να είναι προσαρμοσμένη στην αποστολή του οργανισμού να παρέχει ένα πλαίσιο και να περιλαμβάνει δέσμευση για συμμόρφωση με τους ισχύοντες κανονισμούς. Αυτή η πολιτική θα πρέπει στη συνέχεια να διαδοθεί ως γραπτή πληροφορία σε ολόκληρο τον οργανισμό και σε κάθε ενδιαφερόμενο μέρος. Επιπρόσθετα το top management είναι ανάγκη να αναθέσει καθήκοντα για να εγγυηθεί ότι το BCMS συμμορφώνεται με τις απαιτήσεις του και την ανατροφοδότηση στην ανώτατη διοίκηση.

Ο προγραμματισμός και η υποστήριξη είναι κρίσιμα στοιχεία της εφαρμογής ενός BCMS. Κατά τον προγραμματισμό, αναπτύσσονται οι προϋποθέσεις για τους στρατηγικούς στόχους και τις κατευθυντήριες αρχές του BCMS. Κατά την ανάπτυξη ενός BCMS, η υποστήριξη παίζει κρίσιμο ρόλο. Κατά τον προγραμματισμό, ο οργανισμός πρέπει να καθορίσει τι θα γίνει, ποιος θα είναι υπεύθυνος για αυτό, πότε θα ολοκληρωθεί, πώς θα αξιολογηθούν τα αποτελέσματα και ποιοι πόροι απαιτούνται. Οι οργανισμοί είναι σημαντικό να υποστηρίζουν αυτή τη διαδικασία παρέχοντας τους πόρους που απαιτούνται για την υλοποίησή της, διασφαλίζοντας την ικανότητα των ατόμων και, εάν είναι απαραίτητο, λαμβάνοντας μέτρα για την απόκτηση της απαιτούμενης ικανότητας και αξιολογώντας την αποτελεσματικότητα των μέτρων που εκτελούνται.

Τα άτομα που εκτελούν εργασίες υπό την επίβλεψη του οργανισμού οφείλουν να γνωρίζουν την πολιτική της επιχειρησιακής συνέχειας, τους ρόλους και τα καθήκοντά τους, τη συμβολή τους στην αποτελεσματικότητα του BCMS και τις συνέπειες της μη συμμόρφωσης με τις απαιτήσεις του BCMS. Επιπλέον, τα άτομα πρέπει να κατανοούν τι, πότε, με ποιον και πώς να μοιράζονται πληροφορίες που σχετίζονται με το BCMS. Ο οργανισμός είναι υποχρεωμένος να παρέχει όλες αυτές τις πληροφορίες σε γραπτή μορφή. Η διαχείριση των τεκμηριωμένων πληροφοριών πρέπει να γίνεται με σκοπό να είναι προσβάσιμες όταν και αν χρειάζονται και να προστατεύονται επαρκώς. Για να

εκπληρώσει αυτούς τους στόχους, ο οργανισμός πρέπει να διαχειριστεί τη διανομή, την αποθήκευση, τον έλεγχο αλλαγών και τη διατήρηση.

Αφού σχεδιάσει το BCMS του, ένας οργανισμός είναι ουσιαστικό να εξετάσει πώς θα λειτουργήσει. Η παράγραφος 8 του ISO 22301 περιγράφει όλες τις πρακτικές ενέργειες που θα πρέπει να ληφθούν υπόψη για να λειτουργήσει το BCMS όπως προβλέπεται. Είναι ένα από τα πιο ολοκληρωμένα και ουσιαστικά τμήματα του προτύπου.

Αποτελεί αναγκαιότητα οι οργανισμοί να ορίζουν, να εκτελούν, να παρακολουθούν και να τεκμηριώνουν τις διαδικασίες που διασφαλίζουν ότι το BCMS τους ικανοποιεί τις απαιτήσεις ISO, επιτυγχάνει όλα τα επιθυμητά αποτελέσματα, αποφεύγει τις αρνητικές παρενέργειες και βελτιώνεται συνεχώς. Οι επιχειρήσεις πρέπει να κατανοήσουν ακριβώς πώς οι επιχειρηματικές διαταραχές μπορούν να επηρεάσουν και να δημιουργήσουν κινδύνους για τις δραστηριότητές τους. Αυτό απαιτεί τη θέσπιση και την εκτέλεση ενδελεχών διαδικασιών ανάλυσης επιχειρηματικών επιπτώσεων και αξιολόγησης κινδύνου. Η ανάλυση επιχειρηματικού αντίκτυπου θα βοηθήσει τον οργανισμό να καθορίσει προτεραιότητες και απαιτήσεις για την επιχειρησιακή συνέχεια. Είναι πρωταρχικής σημασίας οι οργανισμοί να ξεκινήσουν με τον εντοπισμό των πιθανών επιπτώσεων που θα μπορούσαν να τους προκαλέσουν προβλήματα. Στη συνέχεια, θα πρέπει να εξεταστούν οι συγκεκριμένες δραστηριότητες που θα μπορούσαν να επηρεάσουν και να δημιουργηθεί ένα χρονοδιάγραμμα για τα πιθανά ζητήματα που είναι πιθανό να προκαλέσουν. Αυτό το χρονοδιάγραμμα θα βοηθήσει να τον οργανισμό να προσδιορίσει ακριβώς πότε αυτά τα ζητήματα γίνονται μη ανεκτά.

Μέχρι εκείνο το σημείο, υπάρχει η μέγιστη ανεκτή περίοδος διακοπής (maximum tolerable period of disruption MTPD). Αυτό είναι το σημείο μετά το οποίο η ανάκαμψη της επιχείρησης είναι αδύνατη. Ένας οργανισμός είναι δυνατόν να έχει ένα MTPD για ολόκληρο τον οργανισμό ή πολλαπλά MTPD για διάφορα προϊόντα και υπηρεσίες. Σειρά, έχει ο ορισμός ενός συγκεκριμένου στόχου, του χρόνου ανάκτησης (recovery time objective RTO). Σε αυτό το σημείο η επιχείρηση θα είναι και πάλι λειτουργική. Συμπληρωματικά, οι οργανισμοί πρέπει να ορίσουν τον στόχο του σημείου ανάκτησης (recovery time objective RTO). Το RTO είναι ένα σημείο στο παρελθόν στο οποίο η επιχείρηση θέλει να επιστρέψει, δηλαδή η τελευταία επιβεβαιωμένη κατάσταση του οργανισμού στην οποία είχε πλήρη ακεραιότητα.

Μετά την ανάλυση του τρόπου με τον οποίο μια κρίση θα μπορούσε να επηρεάσει και να δημιουργήσει κινδύνους και της κατανόησης της φύσης αυτών των επιπτώσεων

και κινδύνων, οι οργανισμοί είναι ζωτικής σημασίας να σχεδιάσουν ακριβώς τι πρέπει να κάνουν πριν, κατά τη διάρκεια και μετά από μία κρίση. Οι επιχειρήσεις θα πρέπει να διερευνήσουν πιθανές στρατηγικές και λύσεις που θα τους επιτρέψουν να συνεχίσουν τις κύριες δραστηριότητες τους, να μειώσουν την πιθανότητα και τη διάρκεια οποιασδήποτε διακοπής, να περιορίσουν τον αντίκτυπό της στον οργανισμό και να διασφαλίσουν ότι όλοι οι απαραίτητοι πόροι είναι έτοιμοι να διατεθούν. Οι οργανισμοί θα πρέπει να λαμβάνουν τις αποφάσεις τους ώστε να είναι σε θέση να συνεχίσουν ή να επανεκκινήσουν τις καθορισμένες βασικές τους δραστηριότητες εντός των καθορισμένων χρονικών πλαισίων.

Όταν καθορίσουν τις στρατηγικές και τις λύσεις της επιχειρηματικής τους συνέχειας, οι οργανισμοί είναι έτοιμοι να εφαρμόσουν και να διατηρήσουν μια λύση επιχειρηματικής συνέχειας που δύναται να αναπτυχθεί άμεσα, κατά τη διάρκεια μιας κρίσης. Αυτό απαιτεί σχεδιασμό όλων των διαδικασιών διαχείρισης διαταραχών του οργανισμού και καθορισμό σαφών κριτηρίων ενεργοποίησης. Αυτές οι διαδικασίες είναι σημαντικό να ευθυγραμμίζονται με την προηγούμενη στρατηγική σκέψη και ανάπτυξη λύσεων. Η λύση για την επιχειρησιακή συνέχεια πρέπει να ορίζει άμεσες ενέργειες για την επίλυση της κατάστασης, γρήγορη προσαρμογή σε μεταβαλλόμενους εσωτερικούς και εξωτερικούς παράγοντες, μηδενισμό συμβάντων που μπορεί να οδηγήσουν σε αναστάτωση, μετριασμό των επιπτώσεών τους με αποτελεσματικές λύσεις και ανάθεση συγκεκριμένων καθηκόντων και ευθυνών. Επιπρόσθετα, πρέπει να προετοιμαστούν ομάδες διαχείρισης διαταραχών. Όλα αυτά είναι απαραίτητο να αποτελούνται από σαφώς προσδιορισμένο προσωπικό και να υποστηρίζονται από διεξοδικά τεκμηριωμένες διαδικασίες. Αυτό θα τους βοηθήσει να αξιολογήσουν τη φύση, το μέγεθος και τις πιθανές επιπτώσεις οποιασδήποτε κρίσης.

Η αποτελεσματική αντιμετώπιση κρίσεων χρειάζεται εξαιρετική επικοινωνία. Οι οργανισμοί οφείλουν να εξετάσουν πώς θα επικοινωνούν σε δύσκολες καταστάσεις. Οι εσωτερικές και εξωτερικές διαδρομές επικοινωνίας πρέπει να είναι καταγεγραμμένες. Επίσης, πρέπει να διασφαλίζεται ότι υπάρχει ο απαραίτητος εξοπλισμός. Όλες οι εισερχόμενες και εξερχόμενες επικοινωνίες προέχει να είναι καταγεγραμμένες σωστά και, όπου χρειάζεται, να λειτουργούν σύμφωνα με το πρωτόκολλο. Μια ευρύτερη επικοινωνιακή στρατηγική είναι σημαντικό να περιλαμβάνει τα πάντα, από τη συνεργασία με τους ανταποκριτές έκτακτης ανάγκης έως τις σχέσεις με τα μέσα ενημέρωσης.

Κάθε σχέδιο επιχειρησιακής συνέχειας επιβάλλεται να περιλαμβάνει το σκοπό, το πεδίο εφαρμογής και τους στόχους, τους ρόλους και τις ευθύνες της ομάδας που θα εφαρμόσει το σχέδιο, τις απαιτήσεις πόρων, τις απαιτήσεις αναφοράς, μια διαδικασία απόσυρσης και τα υποστηρικτικά δεδομένα που απαιτούνται για την ενεργοποίηση, λειτουργία , συντονισμό και επικοινωνία των ενεργειών της ομάδας. Επιπλέον, το σχέδιο επιχειρηματικής συνέχειας πρέπει να περιέχει λεπτομέρειες σχετικά με τον τρόπο με τον οποίο οι ομάδες θα συνεχίσουν ή θα ανακτήσουν δραστηριότητες προτεραιότητας μέσα σε προκαθορισμένα χρονικά πλαίσια, καθώς και να παρακολουθεί τις επιπτώσεις της διακοπής και την απόκριση του οργανισμού. Στο BCMS, είναι κοινωφελές να τεκμηριώνονται ελάχιστα κατώτατα όρια και οι διαδικασίες για την ενεργοποίηση της απόκρισης και τη δυνατότητα παράδοσης προϊόντων και υπηρεσιών στη συμφωνημένη δυναμικότητα.

Το πρότυπο απαιτεί από τους οργανισμούς να καθιερώνουν και να διατηρούν ένα πρόγραμμα τακτικής αξιολόγησης και δοκιμών για να επιβεβαιώνουν την αξιοπιστία των σχεδίων και των λύσεων τους για την επιχειρηματική συνέχεια. Αυτό συνεπάγεται τη διεξαγωγή δραστηριοτήτων και αξιολογήσεων που ευθυγραμμίζονται με τους στόχους επιχειρηματικής συνέχειας του οργανισμού και επικεντρώνονται σε ρεαλιστικά, καλά δομημένα σενάρια με σαφώς καθορισμένες προτεραιότητες και στόχους. Πρέπει να έχουν θετική αντήχηση στο BCMS, να ενισχύουν τις σχέσεις, τις γνώσεις και τις δεξιότητες όλων των εμπλεκόμενων ομάδων και να καταλήγουν σε εποικοδομητικές, ολοκληρωμένες αξιολογήσεις και σχόλια που βελτιώνουν το σύστημα. Εξάλλου, το πρότυπο καθορίζει πως ένας οργανισμός πρέπει να αξιολογεί κάθε πτυχή του BCMS του και κάθε παράγοντα που μπορεί να έχει αντίκτυπο. Η ανταπόκριση του BCMS στις ανάγκες και τα ζητήματα του οργανισμού, η σχέση του με εξωτερικούς συνεργάτες και προμηθευτές και η συμμόρφωσή του με όλες τις σχετικές πολιτικές, κανονισμούς και πρότυπα του κλάδου θα πρέπει να αξιολογούνται σε τακτική βάση. Το BCMS επιβάλλεται να επαναξιολογείται μετά από τυχόν περιστατικά ή ενεργοποιήσεις, καθώς και κάθε φορά που υπάρχουν σημαντικές αλλαγές στον οργανισμό ή το επιχειρηματικό περιβάλλον.

Τα παραπάνω αποτελούν τις βασικές αρχές ενός συστήματος διαχείρισης κρίσεων. Οι αρχές και τεχνικές σχεδιασμού ενός συστήματος διαχείρισης κρίσεων περιγράφονται στο ISO 22320.

1.3 Διαχείριση Κρίσεων

Τα τελευταία χρόνια, υπήρξαν πολλές φυσικές και ανθρωπογενείς καταστροφές και άλλα μεγάλα περιστατικά που απέδειξαν τη σημασία της διαχείρισης συμβάντων για τη διάσωση ζωών, τον μετριασμό τραυματισμών και ζημιών και τη διατήρηση της συνέχειας των βασικών κοινωνικών υπηρεσιών.

Η υγεία, η επικοινωνία με απαραίτητους φορείς , η παροχή νερού και τροφίμων και η πρόσβαση σε ενέργεια και καύσιμα αποτελούν τέτοια παραδείγματα. Στο παρελθόν, η διαχείριση συμβάντων είχε εθνική, περιφερειακή ή ενιαία οργανωτική εστίαση. Ωστόσο, μια πολυεθνική και πολυοργανωτική στρατηγική είναι απαραίτητη σε τωρινά και μελλοντικά σχέδια διαχείρισης κρίσεων.

Η αυξημένη αστικοποίηση, οι απαραίτητες συνιστώσες λειτουργίας κρίσιμων υποδομών, η κοινωνικοοικονομική δυναμική, η περιβαλλοντική αλλαγή, οι ασθένειες των ζώων και των ανθρώπων και η αυξημένη παγκόσμια κυκλοφορία ανθρώπων και αγαθών έχουν αυξήσει την πιθανότητα διαταραχών και καταστροφών που υπερβαίνουν τα γεωγραφικά και πολιτικά όρια και την ικανότητα διαχείρισης τους.

Το ISO 22320 παρέχει στους οργανισμούς κατευθύνσεις για τον καλύτερο τρόπο διαχείρισης όλων των τύπων καταστάσεων. Το έγγραφο περιέχει συστάσεις διαχείρισης συμβάντων, συμπεριλαμβανομένων των εννοιών επικοινωνίας, των βασικών αρχών διαχείρισης συμβάντων και της συνεργασίας μέσω κοινής κατεύθυνσης.

Το ISO 22320, σε αντίθεση με το ISO 22301, τονίζει τη σημαντικότητα των ανθρώπων κατά τη διάρκεια ενός περιστατικού. Μεταξύ των εννοιών που περιγράφονται στο πρότυπο είναι η σημασία της ασφάλειας τόσο για όσους ανταποκρίνονται όσο και για εκείνους που επηρεάζονται, όπως επίσης και ο σεβασμός της υπεροχής της ανθρώπινης ζωής και της ανθρώπινης αξιοπρέπειας μέσω της αμεροληψίας.

Επιπλέον, το πρότυπο καθορίζει μια μέθοδο για τη διαχείριση συμβάντων. Πιο συγκεκριμένα, οι ειδικοί διαχείρισης συμβάντων ενθαρρύνονται να υιοθετήσουν μια στρατηγική για όλους τους κινδύνους σε αντίθεση με την εστίαση σε έναν συγκεκριμένο κίνδυνο. Αυτή η στρατηγική οφείλει να ενσωματώνει περιστατικά που ο οργανισμός δεν έχει ακόμη αντιμετωπίσει.

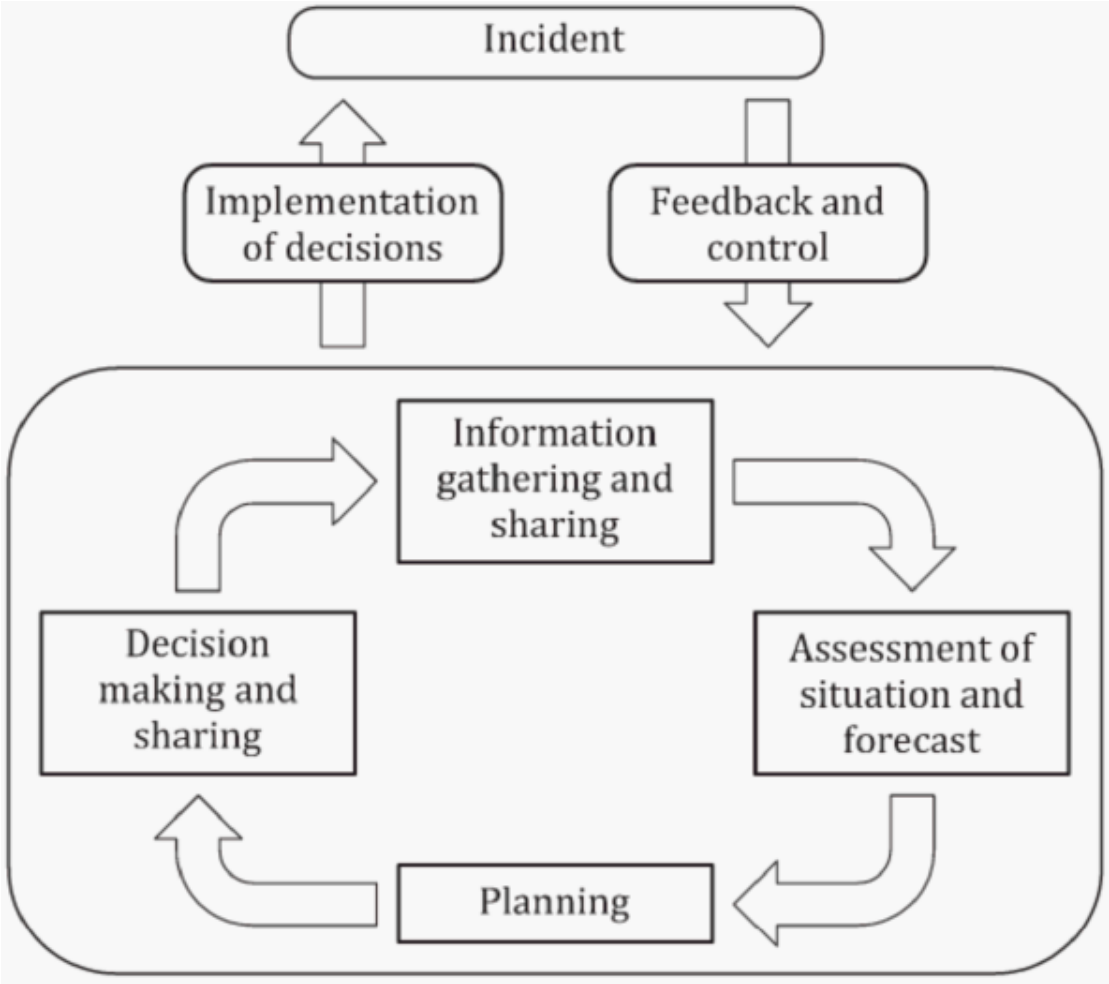
Οι εγκαταστάσεις, ο εξοπλισμός, οι εργαζόμενοι, η οργανωτική δομή, οι διαδικασίες και οι επικοινωνίες θα πρέπει να λαμβάνονται υπόψη κατά τη διαχείριση συμβάντων. Αυτή η μέθοδος βασίζεται σε στόχους που διαμορφώνονται με τη συλλογή και την ανταλλαγή πληροφοριών προληπτικά, ώστε να αξιολογηθεί η κατάσταση, να εντοπιστούν πιθανά σενάρια και να εμπλακούν σε δραστηριότητες σχεδιασμού ως μέρος της ετοιμότητας και της αντίδρασης σε καταστάσεις έκτακτης ανάγκης.

Είναι αποτελεσματικό ο οργανισμός να δημιουργήσει μια δομή για τη διαχείριση συμβάντων με στόχο να εκτελεί τις ευθύνες που σχετίζονται με διάφορα περιστατικά. Μια δομή για τη διαχείριση συμβάντων θα πρέπει να περιλαμβάνει ηγεσία, σχεδιασμό, λειτουργίες και οικονομικά στοιχεία. Ο οργανισμός επιβάλλεται να έχει εξουσία και έλεγχο επί του συμβάντος, να συλλέγει, να αξιολογεί και να διαδίδει έγκαιρα πληροφορίες και πληροφορίες για το περιστατικό και να περιλαμβάνει τακτικούς στόχους, μείωση κινδύνου και προστασία ανθρώπων, ιδιοκτησίας και περιβάλλοντος. Ακόμη, ο οργανισμός θα πρέπει να προσφέρει βοήθεια και πόρους για περιστατικά, όπως εγκαταστάσεις, μεταφορές, προμήθειες, καύσιμα, τρόφιμα και ιατρικές υπηρεσίες, καθώς και να διαχειρίζεται το κόστος και το χρόνο αποζημίωσης και προμήθειας.

Επιπλέον, είναι πρωτεύον οι οργανισμοί να προσπαθήσουν να κατανοήσουν τις προοπτικές εκείνων που βρίσκονται τόσο εντός όσο και εκτός της εταιρείας. Επιπλέον, ο οργανισμός θα πρέπει να αξιολογήσει μια ποικιλία σεναρίων αντίδρασης, αναγκών, απαιτούμενων ενεργειών, οργανωτικής κουλτούρας και στόχων. Είναι ωφέλιμο να ληφθεί υπόψιν ότι ο οργανισμός πρέπει να έχει μια κουλτούρα να ενεργεί νωρίτερα παρά αργότερα. Ο χρόνος είναι κρίσιμος όταν ανταποκρίνεται σε καταστάσεις. Οι οργανισμοί οφείλουν να είναι σε θέση να προβλέπουν κλιμακωτά αποτελέσματα, να λαμβάνουν υπόψη τα χρονοδιαγράμματα άλλων οργανισμών, να αξιολογούν τον αντίκτυπο των διαφορετικών χρονικών πλαισίων και να προσαρμόζουν ανάλογα το χρονοδιάγραμμά τους.

Επιπρόσθετα, το να είναι ο οργανισμός προορατικός μπορεί να είναι απαραίτητο όταν ανταποκρίνεσαι σε καταστάσεις. Οι οργανισμοί είναι ανάγκη να αναλάβουν την πρωτοβουλία να αναλύσουν τους κινδύνους και να συντονίσουν τις αντιδράσεις, να προβλέψουν πώς μπορεί να εξελιχθούν τα περιστατικά, να διαχειριστούν τα προβλήματα έγκαιρα, να προσδιορίσουν ποια ανταλλαγή πληροφοριών είναι απαραίτητη και να ξεκινήσουν μια συλλογική απάντηση. Επιπλέον, πρέπει να ειδοποιούν και να κατευθύνουν τρίτα μέρη.

Η διαδικασία διαχείρισης συμβάντων θα πρέπει να ισχύει για όλα τα μέλη της ομάδας διοίκησης συμβάντος, ανεξάρτητα από το επίπεδο ευθύνης τους, και όχι μόνο για τον διοικητή του συμβάντος. Το πλαίσιο για τη διαδικασία διαχείρισης συμβάντων που παρέχεται στο πρότυπο φαίνεται παρακάτω.



Εικόνα 3 Διαδικασία διαχείρισης συμβάντων

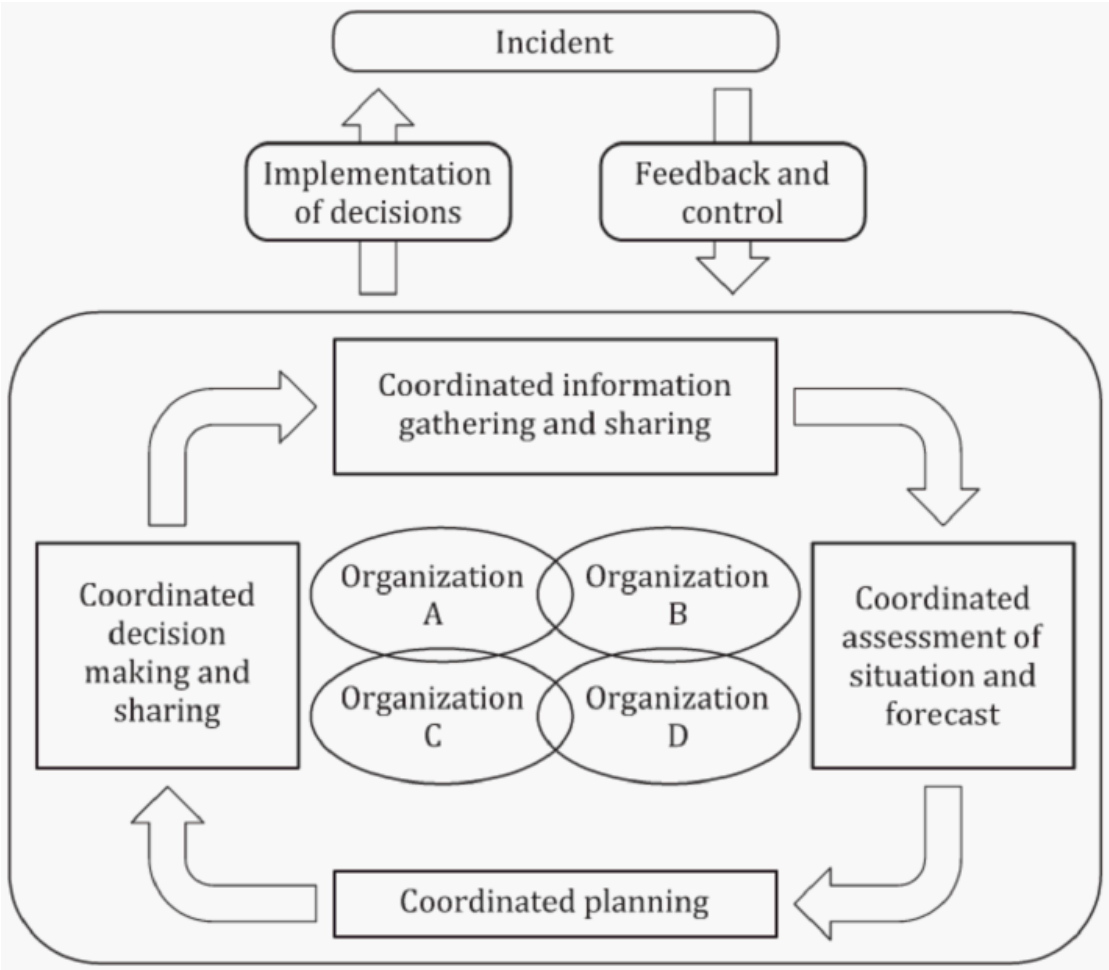
1.3.1 Συντονισμένη Διαδικασία Διαχείρισης Συμβάντων

Η συνεργασία απαιτεί συντονισμό και συνεργασία μεταξύ πολλών τμημάτων ή οργανωτικών επιπέδων και οργανισμών. Αποτελεί ανάγκη η εκτελεστική ηγεσία κάθε οργανισμού να δεσμευτεί να συνεισφέρει και να επιδιώξει την κοινή κατεύθυνση. Η συνεργασία απαιτεί από τις εταιρείες να χρησιμοποιούν τη διαδικασία διαχείρισης συμβάντων. Η εταιρεία θα πρέπει να σχεδιάζει τη διαχείριση ταυτόχρονων συμβάντων, καθώς οι επιπτώσεις ενός περιστατικού μπορεί να εξελιχθούν ταυτόχρονα σε πολλά επίπεδα και σε πολλούς δημόσιους τομείς. Η ενεργή κοινή χρήση και η διασφάλιση της

διαθεσιμότητας πληροφοριών για λήψη και ανάλυση θα βοηθήσει τον οργανισμό να αναπτύξει μια ενοποιημένη άποψη των λειτουργιών του. Μια σαφής και διαφανής διαδικασία λήψης αποφάσεων να βοηθά τον οργανισμό να λαμβάνει αποφάσεις και να τις κοινοποιεί εντός της επιχείρησης, σε άλλους εμπλεκόμενους οργανισμούς και στο ευρύ κοινό.

Η ανταλλαγή πληροφοριών με άλλους οργανισμούς είναι δυνατή με τη δημιουργία συμφωνιών συνεργασίας, τη δημιουργία μιας εξειδικευμένης λειτουργίας και την κατανομή ειδικών πόρων. Ένα τέτοιο στοιχείο αποτελεί ο τεχνικός εξοπλισμός.

Ο οργανισμός είναι απαραίτητο να χρησιμοποιεί τεχνικό εξοπλισμό για την επίτευξη διαλειτουργικότητας διασφαλίζοντας με αυτόν τον τρόπο τη λειτουργία του εξοπλισμού μεταξύ των οργανισμών και σε διάφορα πλαίσια, μεγιστοποιώντας τη χρήση του διαθέσιμου εξοπλισμού και λαμβάνοντας υπόψη τη χρήση του εξοπλισμού από εταιρείες με μικρότερη εμπειρία. Λαμβάνοντας υπόψη αυτές τις πληροφορίες, το πρότυπο εμπλουτίζει τη διαδικασία που απεικονίζεται στην εικόνα 3, όπως φαίνεται στην εικόνα 4.



Εικόνα 4 Συντονισμένη διαδικασία διαχείρισης συμβάντων για πολλούς οργανισμούς

2 Ασφάλεια και Τεχνικές Αποκατάστασης Πληροφοριακών Συστημάτων

Αναμφίβολα, ένας πιο διασυνδεδεμένος κόσμος συνοδεύεται από ορισμένα πλεονεκτήματα, όπως και κάποιους κινδύνους. Ένας από αυτούς τους κινδύνους είναι οι διαταραχές, οι οποίες ορίζονται ως «γεγονότα που σταματούν την κανονική ροή εμπορευμάτων ή υπηρεσιών μέσα σε ένα σύστημα» [25]. Τις τελευταίες δύο δεκαετίες, οι εταιρείες εξαρτώνται περισσότερο από την τεχνολογία πληροφοριών (IT) για τη βελτίωση των επιχειρηματικών λειτουργιών, τον εξορθολογισμό της λήψης αποφάσεων διαχείρισης και την εφαρμογή εταιρικών στρατηγικών [26,27]. Αυτό έχει ως συνέπεια, η διαθεσιμότητα των συστημάτων πληροφορικής να έχει γίνει ένα από τα

πιο πιεστικά ζητήματα που έχουν συγκεντρώσει την προσοχή τόσο των μελετητών πληροφορικής όσο και των επαγγελματιών. Ορισμένοι οργανισμοί (π.χ. χρηματοπιστωτικά ιδρύματα, οργανισμοί υγειονομικής περίθαλψης, διαδικτυακοί λιανοπωλητές μεγάλου όγκου, κυβερνητικά γραφεία, εταιρείες κοινής ωφέλειας κ.λπ.) απαιτούν ένα σύστημα πληροφορικής για να λειτουργεί συνεχώς. Δεν δύνανται να δεχτούν κανένα χρόνο διακοπής της λειτουργίας του [28]. Επομένως, η αυξανόμενη ζήτηση για συνεχή λειτουργία συστημάτων πληροφορικής έχει προκαλέσει ενδιαφέρον για τοποθεσίες αποκατάστασης καταστροφών (ονομάζονται επίσης και «απομακρυσμένες τοποθεσίες δημιουργίας αντιγράφων ασφαλείας»). Ένα μέρος αποκατάστασης καταστροφών για IT είναι μια δευτερεύουσα τοποθεσία με αντίγραφα ασφαλείας για το κύριο κέντρο δεδομένων σε περίπτωση αποτυχίας της κύριας τοποθεσίας [29]. Οι τοποθεσίες ανάκτησης καταστροφών πληροφορικής έχουν τη δυνατότητα να επαναφέρουν δεδομένα για την εταιρεία σε περίπτωση σοβαρών αστοχιών που θα μπορούσαν να καταστήσουν ανενεργή μία ολόκληρη τοποθεσία και στην οποία η τοπική επαναφορά ενδέχεται να είναι ανεπαρκής.

Ωστόσο, οι προκλήσεις που προκύπτουν στην επιλογή του τόπου αποκατάστασης από καταστροφή είναι πρακτικές, πολύπλοκες και μπορεί να περιλαμβάνουν σημαντική υποκειμενικότητα και αβεβαιότητα [30,31]. Ένας λόγος είναι ότι οι τοποθεσίες ανάκαμψης από καταστροφές θεωρούνται μερικές φορές ως «αναγκαίο κακό», ένα κόστος που οι περισσότερες εταιρείες θα ήθελαν να κρατήσουν στο ελάχιστο και όχι ως λειτουργία δημιουργίας εσόδων. Οι αποφάσεις σχετικά με την επιλογή μιας τοποθεσίας για ανάκαμψη από καταστροφές είναι επίσης εξαρτώμενες από τους διαθέσιμους, τις επιπτώσεις τους και την τεχνολογία τους. Συνεπώς, η αξιολόγηση και η επιλογή των τόπων αποκατάστασης από καταστροφές έχουν γίνει τα πιο ουσιαστικά ζητήματα τόσο για τους δημόσιους όσο και για τους ιδιωτικούς οργανισμούς.

Λόγω της σημασίας των συστημάτων αποκατάστασης καταστροφών για τη συνεχή λειτουργία των data center, αρκετοί ερευνητές έχουν αρχίσει πρόσφατα να εξετάζουν σχετικά θέματα [32,33]. Στον πραγματικό κόσμο, τα κριτήρια αξιολόγησης για τοποθεσίες data center και τοποθεσίες αποκατάστασης καταστροφών είναι διαφορετικά. Ειδικότερα, μια μελέτη για την αξιολόγηση και την επιλογή των τοποθεσιών αποκατάστασης από καταστροφές μπορεί να βοηθήσει τη διαχείριση στη λήψη πιο ενημερωμένων αποφάσεων σχετικά με τα συστήματα ανάκαμψης από καταστροφές.

Αυτό το κεφάλαιο περιγράφει τις έννοιες και τις αρχές της ετοιμότητας της τεχνολογίας πληροφοριών και επικοινωνιών (information and technology ICT) για επιχειρηματική συνέχεια και παρέχει κατευθυντήριες γραμμές για την παροχή υπηρεσιών ανάκαμψης από καταστροφές τεχνολογίας πληροφοριών και επικοινωνιών (ICT DR) ως μέρος της διαχείρισης επιχειρηματικής συνέχειας, με βάση το ISO 27301 και το ISO 24762.

2.1 Αξιολόγηση Ετοιμότητας Πληροφοριακών Συστημάτων Ως Προς Τεχνολογίες Επιχειρησιακής Συνέχειας

Η ικανότητα ενός οργανισμού να ανταποκρίνεται και να ανακάμπτει από ένα γεγονός που επηρεάζει αρνητικά τις δραστηριότητές του είναι γνωστή ως «αποκατάσταση από καταστροφή». Μετά από μια κρίση, ένας οργανισμός έχει τη δυνατότητα να αποκαταστήσει γρήγορα την πρόσβαση στα ζωτικά συστήματα και την υποδομή του χάρις στις τεχνικές αποκατάστασης καταστροφών. Ένας οργανισμός προετοιμάζεται για αυτό κάνοντας μια ολοκληρωμένη αναθεώρηση των συστημάτων του και καταρτίζοντας ένα επίσημο έγγραφο που πρέπει να ακολουθείται σε περιόδους καταστροφής. Αυτό το έγγραφο παρέχει μια στρατηγική αποκατάστασης καταστροφών για το IT.

Η αποκατάσταση καταστροφών πληροφορικής (IT disaster recovery) βασίζεται σε καταστροφικά περιστατικά. Αυτά τα γεγονότα συνδέονται συνήθως με φυσικές καταστροφές, αλλά μπορεί επίσης να είναι αποτέλεσμα συστήματος, τεχνικής βλάβης ή εσκεμμένης επίθεσης από ανθρώπους. Είναι σημαντικά περιστατικά που μπορούν να εμποδίσουν ή ακόμα και να σταματήσουν βασικές επιχειρηματικές δραστηριότητες. Ορισμένα τυπικά συμβάντα μπορεί να περιλαμβάνουν:

- Κυβερνοεπιθέσεις όπως κακόβουλο λογισμικό, DDoS και επιθέσεις ransomware
- Σαμποτάζ
- Διακοπές ρεύματος
- Αστοχία εξοπλισμού
- Επιδημίες ή πανδημίες, όπως ο COVID-19
- Τρομοκρατικές επιθέσεις ή απειλές

- Ανεμοστρόβιλους
- Σεισμούς
- Πλημμύρες
- Φωτιές
- Βιομηχανικά ατυχήματα

Η ενότητα Α.17.1 του Παραρτήματος Α του ISO 27001 έχει ως στόχο της ότι ένας οργανισμός επιβάλλεται να ενσωματώσει τη συνέχεια της ασφάλειας των πληροφοριών στα συστήματα διαχείρισης της επιχειρησιακής συνέχειας. Αυτή η ενότητα περιέχει στοιχεία ελέγχου που σχετίζονται με τις διαδικασίες επιχειρηματικής συνέχειας (BCP), τα σχέδια ανάκτησης και τις αποκλίσεις για την υποστήριξη αυτού του στόχου.

Ωστόσο, το ISO 27001, όπως όλα τα πρότυπα συστημάτων διαχείρισης, απλώς καθορίζει τι πρέπει να επιτευχθεί και όχι το πώς θα επιτευχθεί. Η συλλογή βέλτιστων πρακτικών που υποστηρίζει το ISO 27001, το ISO 27002, είναι ελάχιστη βοήθεια.

Το ISO 27031, το οποίο καλύπτει την ετοιμότητα Τεχνολογίας Πληροφοριών και Επικοινωνιών (Information and Communication Technology ICT) για Επιχειρησιακή Συνέχεια (IRBC) και παρέχει καθοδήγηση σχετικά με το τι πρέπει να λαμβάνεται υπόψη κατά την ανάπτυξη επιχειρηματικής συνέχειας για τις ΤΠΕ – γνωστό και ως «ανάκτηση καταστροφών» – είναι ένα από τα πρόσθετα των προτύπων του ISO 2700 που στοχεύουν συγκεκριμένες περιοχές.

Το ISO 27031 προτείνει μια προσέγγιση συστημάτων διαχείρισης ICT για την υποστήριξη του συστήματος διαχείρισης επιχειρησιακής συνέχειας του ISO 22301. Το ISO 27031 καθορίζει ένα σύστημα διαχείρισης για την ετοιμότητα επιχειρησιακής συνέχειας του ICT (IRBC). Το IRBC είναι ένα σύστημα διαχείρισης που εστιάζει στην αποκατάσταση καταστροφών. Το IRBC ακολουθεί το ίδιο μοντέλο Plan-Do-Check-Act (PDCA) με το σύστημα διαχείρισης επιχειρηματικής συνέχειας που περιγράφεται σύμφωνα με το ISO 22301. Το IRBC έχει ως στόχο η εταιρεία να υιοθετήσει μέτρα που περιορίζουν τον κίνδυνο διακοπής των ICT, και επίσης μέτρα για να ανταποκρίνεται και να ανακάμπτει από διακοπές.

Τα Συστήματα Διαχείρισης IRBC χρησιμοποιούν την ίδια θεμελιώδη μέθοδο διαχείρισης PDCA με το ISO 22301, αλλά την τροποποιούν για να καλύψει την τεχνική πτυχή του IRBC. Εκτός από τις τεχνικές τροποποιήσεις στο PDCA, το ISO 27031 εξαρτάται από τα αποτελέσματα της ανάλυσης επιχειρηματικών επιπτώσεων (business

impact analysis BIA) που δημιουργούνται και γίνονται αποδεκτά ως μέρος του ευρύτερου BCMS ενός οργανισμού. Το σύστημα διαχείρισης PDCA στο IRBC αναλύεται ως εξής.

Ως μέρος των στρατηγικών τους για την ανάκαμψη από καταστροφές τεχνολογίας πληροφοριών (information disaster recovery ITDR), πολλές εταιρείες μπορεί ήδη να εφαρμόζουν ορισμένα από τα στοιχεία του "Plan" του ISO 27031. Το ISO 27031 θεωρεί το ITDR ως υποσύνολο του IRBC, βέβαια στην πράξη, υπάρχουν σχετικά λίγες διακρίσεις . Κατά τη φάση του σχεδιασμού, ο οργανισμός θεσπίζει μια πολιτική για τον έλεγχο των διαδικασιών και των απαιτήσεων IRBC. Η πολιτική περιγράφει τη δομή διακυβέρνησης του συστήματος διαχείρισης IRBC. Χρησιμοποιώντας εισροές από το BIA του οργανισμού, το IRBC μεταφράζει τις επιχειρηματικές απαιτήσεις σε κριτήρια απόδοσης ICT για υπηρεσίες ICT. Η φάση του σχεδίου ολοκληρώνεται με τη δημιουργία εναλλακτικών στρατηγικών IRBC για εφαρμογή στη φάση Do.

Η διαμόρφωση στρατηγικής IRBC ουσιαστικά σηματοδοτεί τη δημιουργία προσφορών υπηρεσιών πληροφορικής που το προσωπικό του ICT θα συμπεριλάβει στον κατάλογο υπηρεσιών ή, πιο γενικά, ως επιλογές για επιχειρηματικό παράγοντα και επιλογή. Ένας οργανισμός που έχει μια καταχώρηση καταλόγου υπηρεσιών για έναν εικονικό διακομιστή, για παράδειγμα, θα προσθέσει καταχωρήσεις για να αντιμετωπίσει τη δυνατότητα ανάκτησης ενός εικονικού διακομιστή μέσω μιας ποικιλίας τεχνικών προκειμένου να επιτύχει μια ποικιλία στόχων ανάκτησης. Για την επίτευξη των επιχειρηματικών στόχων που προσδιορίζονται από την BIA, ο οργανισμός μπορεί να επιλέξει να παρέχει δύο μεθοδολογίες ανάκτησης για την ανάκτηση μιας εικονικής μηχανής με διαφορετικές περιόδους ανάκτησης. Αυτές οι δύο στρατηγικές ανάκτησης προστίθενται εν συνεχεία στον κατάλογο υπηρεσιών του οργανισμού, είτε ως διακριτές καταχωρήσεις είτε ως τροποποιήσεις σε υπάρχουσες καταχωρήσεις.

Σύμφωνα με το ISO 27031, για να είναι αποτελεσματικές οι στρατηγικές IRBC, πρέπει να έχουν έξι στοιχεία για την παρακολούθηση, την απόκριση και την ανάκαμψη από διακοπές στις τεχνολογίες πληροφοριών και επικοινωνιών. Οι έξι παράγοντες είναι:

- Ικανότητα και γνώση: Οι μέθοδοι ανάκτησης αντιπροσωπεύουν τις τεχνικές δεξιότητες και γνώσεις που απαιτούνται για τη λειτουργία των υπηρεσιών ICT

πριν, κατά τη διάρκεια και μετά από μια διακοπή. Οι στρατηγικές που λαμβάνουν υπόψη τις δεξιότητες και τη γνώση διασφαλίζουν ότι κανένα άτομο δεν υπολείπεται συγκεκριμένων δεξιοτήτων των και γνώσεων που απαιτούνται για τη διαχείριση των συστημάτων ICT του οργανισμού.

- Εγκαταστάσεις: Οι στρατηγικές ανάκαμψης περιλαμβάνουν τη μείωση του κινδύνου λειτουργίας συστημάτων ICT από μία μόνο εγκατάσταση. Οι στρατηγικές που ενσωματώνουν ανησυχίες για τις εγκαταστάσεις διασφαλίζουν ότι τα συστήματα ICT έχουν την ικανότητα να συνεχίσουν να λειτουργούν σε περίπτωση που μια βασική εγκατάσταση καταστεί μη λειτουργική.
- Τεχνολογία: Οι στρατηγικές ανάκαμψης προβλέπουν τις τεχνολογικές ανάγκες που είναι απαραίτητες για την επίτευξη των απαιτήσεων ανάκτησης του οργανισμού, ιδίως το Recovery Time Objective (RTO) και το Recovery Point Objective (RPO). Οι στρατηγικές με γνώση της τεχνολογίας περιλαμβάνουν τη διασφάλιση ότι το υλικό και οι εφαρμογές μπορούν να ανακτηθούν εντός του χρόνου και των απαιτήσεων ανάκτησης δεδομένων της επιχείρησης. Τα συστήματα υποστήριξης όπως η τροφοδοσία, η ψύξη, το ανθρώπινο δυναμικό, η υποστήριξη από τον προμηθευτή και η συνδεσιμότητα WAN επιβάλλεται να περιλαμβάνονται σε αυτές τις σκέψεις.
- Δεδομένα: Οι μέθοδοι ανάκτησης περιλαμβάνουν μελέτες για την προστασία των βασικών δεδομένων του οργανισμού. Στις στρατηγικές εξέτασης δεδομένων περιλαμβάνονται η ασφάλεια, η ακρίβεια και η προσβασιμότητα στα δεδομένα που απαιτούνται από τους τελικούς χρήστες.
- Διαδικασίες: Οι στρατηγικές ανάκτησης οφείλουν να αφορούν τον τρόπο διατήρησης των διαδικασιών που απαιτούνται για την παρακολούθηση, τη λειτουργία και την ανάκτηση συστημάτων ICT προκειμένου να ικανοποιηθούν οι επιχειρηματικές απαιτήσεις. Οι στρατηγικές που εξετάζουν τις διαδικασίες προσδιορίζουν τις διαδικασίες ICT που απαιτούνται πριν, κατά τη διάρκεια και μετά από μια διακοπή συστήματος ICT.
- Προμηθευτές: Οι στρατηγικές ανάκαμψης εμπεριέχουν εξέταση του τρόπου ενημέρωσης και εμπλοκής των προμηθευτών που χρειάζονται για την ανάκτηση και τη λειτουργία συστημάτων ICT. Οι στρατηγικές που ενσωματώνουν ζητήματα προμηθευτών καθορίζουν ποιοι προμηθευτές

εμπλέκονται στη λειτουργία και την ανάκτηση συστημάτων ICT πριν, κατά τη διάρκεια και μετά από μια διακοπή.

Κάθε επιλογή στρατηγικής IRBC λαμβάνει υπόψη τα έξι στοιχεία και συχνά καταλήγει στην κατασκευή βαθμίδων για την ταξινόμηση της τεχνολογίας πληροφοριών και επικοινωνιών του οργανισμού. Κατά τη φάση Do, οι υπηρεσίες ICT θα εκχωρηθούν σε ένα επίπεδο, το οποίο θα επιτρέψει την επιλογή στρατηγικής. Μόλις το IT βρει τις δυνατότητες στρατηγικής, η διοίκηση του οργανισμού είναι απαραίτητο να σταθμίσει το ποσό του κινδύνου που μετριάζεται από τη στρατηγική έναντι του κόστους υλοποίησης. Το τελικό αποτέλεσμα της φάσης Plan είναι μια λίστα στρατηγικών για προσθήκη ή αλλαγή στον κατάλογο υπηρεσιών, επιτρέποντας στην εταιρεία να επιλέξει το κατάλληλο επίπεδο ανάκτησης.

Η φάση Do του συστήματος διαχείρισης IRBC περιλαμβάνει την εφαρμογή των στρατηγικών που καθορίστηκαν στη φάση Plan, την υλοποίηση σχεδίων ανάκαμψης για υπηρεσίες ICT και την πραγματοποίηση εκπαίδευσης και ευαισθητοποίησης για να διασφαλιστεί ότι το προσωπικό που συμμετέχει στο πρόγραμμα IRBC είναι καταρτισμένο και ενημερωμένο. Το πρόγραμμα IRBC εκτελεί τις σχετικές λύσεις που καθορίστηκαν στη φάση του Σχεδίου για την αύξηση της ετοιμότητας ICT για υπηρεσίες εντός του πεδίου εφαρμογής του προγράμματος.

Όταν οι καταστάσεις που προκαλούν διακοπές γίνονται πραγματικότητα, το προσωπικό πληροφορικής εφαρμόζει τεχνικές και εκπονεί σχέδια για τον μετριασμό του υπολειπόμενου κινδύνου. Η τεκμηρίωση του σχεδίου απόκρισης και ανάκαμψης είναι σημαντική για να διασφαλιστεί ότι οι εμπλεκόμενοι κατανοούν τις δραστηριότητες που απαιτούνται για την εκπλήρωση των επιχειρηματικών προσδοκιών. Το ISO 27031 καλύπτει πολλά από τα ίδια στοιχεία με το ISO 22301, όπως ο στόχος και το πεδίο εφαρμογής του σχεδίου, καθορισμένοι ρόλοι και ευθύνες, αναπληρωματικά πρόσωπα, κριτήρια επίκλησης σχεδίου και στοιχεία επικοινωνίας.

Το τελευταίο βήμα της φάσης Do είναι η εκτέλεση διαδικασιών εκπαίδευσης και ευαισθητοποίησης για να διασφαλιστεί ότι όλο το προσωπικό που συνδέεται με το σύστημα διαχείρισης IRBC (συμπεριλαμβανομένων εκείνων με ρόλους σε σχέδια απόκρισης και αποκατάστασης) γνωρίζει τα καθήκοντά του πριν, κατά τη διάρκεια και μετά από μια διακοπή.

Η φάση Check του συστήματος διαχείρισης IRBC καλύπτει συμβατικές δραστηριότητες της φάσης Check, όπως η αναθεώρηση της διαχείρισης και η δοκιμή

και η άσκηση. Επιπροσθέτως, η φάση Check εισάγει συνεχείς λειτουργίες που παρακολουθούν για διακοπές στις υπηρεσίες ICT και αξιολογούν την απόδοση που σχετίζεται με την ετοιμότητα ICT.

Η φάση Act περιλαμβάνει μια αξιολόγηση διαχείρισης της απόδοσης του προγράμματος IRBC, την απόδοση ετοιμότητας ICT και την κατανομή πόρων. Εκτός από τη διεξαγωγή μιας διαχειριστικής ανασκόπησης, το πρόγραμμα IRBC εφαρμόζει διορθωτικά μέτρα που ανακαλύφθηκαν σε άλλες φάσεις του συστήματος διαχείρισης. Ο στόχος των διορθωτικών ενεργειών είναι να ενσταλάξει μια κουλτούρα συνεχούς βελτίωσης σε ολόκληρο τον οργανισμό και να εμπλακεί η διοίκηση, ώστε να θέσει τη συνεχή βελτίωση ως κορυφαία προτεραιότητα.

Το πρόγραμμα IRBC που περιγράφεται στο ISO 27031 βοηθά τους επαγγελματίες πληροφορικής και επιχειρηματικής συνέχειας να διατηρήσουν ένα καλό επίπεδο ανθεκτικότητας στο ICT. Οι ειδικοί της πληροφορικής και της επιχειρησιακής συνέχειας βοηθούν τον οργανισμό τους στην παρακολούθηση, την ανταπόκριση και την ανάκαμψη από μια διακοπή στο ICT, αναπτύσσοντας ένα σύστημα διαχείρισης IRBC. Το ISO 27031 χρησιμοποιεί και τροποποιεί τις έννοιες BCM που περιγράφονται στο ISO 22301 για να βοηθήσει στον μετριασμό του κινδύνου διαταραχών στις τεχνολογίες πληροφοριών και επικοινωνιών και στην επιχείρηση στο σύνολό της.

2.2 Εφαρμογή Τεχνολογιών Επιχειρησιακής Συνέχειας Σε Πληροφοριακά Συστήματα

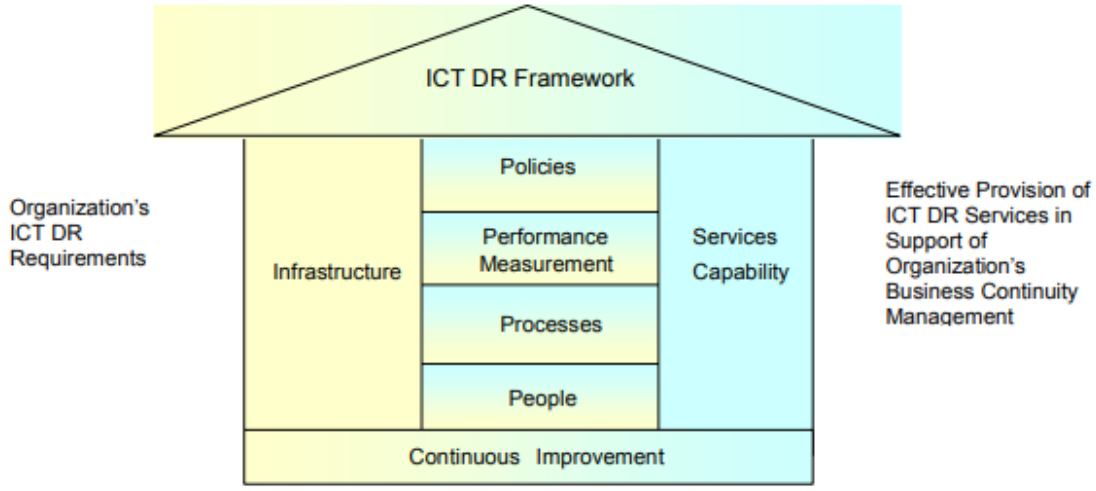
Οποιαδήποτε μορφή καταστροφής είναι δυνατόν να συμβεί οπουδήποτε και ανά πάσα στιγμή. Οι καταστροφές είναι σχεδόν αδύνατο να αποφευχθούν, αλλά οι εταιρείες μπορούν τουλάχιστον να έχουν μια κατάλληλη στρατηγική αποκατάστασης από καταστροφές.

Ο σχεδιασμός για την αποκατάσταση από καταστροφές είναι ο παράγοντας διάκρισης μεταξύ των επιχειρήσεων που μπορούν να διαχειριστούν κρίσεις με το μικρότερο κόστος και προσπάθεια, μέγιστη ταχύτητα και εκείνων που αναγκάζονται

να λάβουν αποφάσεις από απελπισία και είναι πρόθυμοι να πληρώσουν οποιοδήποτε τίμημα για την ανάκαμψή τους.

Το ISO 24762 σχεδιάστηκε για να περιγράφει τις υπηρεσίες ICT Disaster Recovery που θα οφείλουν να παρέχουν τρίτες επιχειρήσεις. Το πρότυπο παρέχει μια δομή για επιχειρήσεις, όπως εταιρείες παροχής backup-hot site [34], εταιρείες παροχής cold site, παρόχους υπηρεσιών συνεγκατάστασης και παρόχους εναλλακτικών χώρων εργασίας. Το πρότυπο αντιμετωπίζει μια μεγάλη ποικιλία προκλήσεων που καλούνται να αντιμετωπίσουν οι πωλητές για να προστατεύσουν την προσφορά υπηρεσιών τους. Αυτά περιλαμβάνουν την κατασκευή κτιρίων, τα μέτρα ασφαλείας, την παροχή υπηρεσιών υποδομής όπως ρεύμα, νερό και τηλεπικοινωνίες και περιβαλλοντικούς ελέγχους.

Όπως φαίνεται στην εικόνα 5, αυτό το πρότυπο βασίζεται σε μια αρχιτεκτονική πολλαπλών επιπέδων που αποτελείται από πολλά στοιχεία για την παροχή υπηρεσιών ICT DR. Το επίπεδο «θεμελίωσης» περιέχει τα βασικά στοιχεία των υπηρεσιών ICT DR: Πολιτικές, Μέτρηση Απόδοσης, Διαδικασίες και Άνθρωποι. Οι πολιτικές επιτρέπουν στους παρόχους υπηρεσιών ICT DR να καθορίζουν την κατεύθυνση για άλλους, συναφείς τομείς των υπηρεσιών τους ICT DR, καθώς και να παρέχουν σαφή επικοινωνία με τα κατάλληλα μέρη σχετικά με τις ανάγκες που μπορούν να ικανοποιηθούν από τις εγκαταστάσεις παρόχων υπηρεσιών ICT DR. Το επίπεδο «θεμελίωσης» συμβάλλει στον ορισμό της υποκείμενης υποδομής και της χωρητικότητας υπηρεσιών. Το επίπεδο «συνεχούς βελτίωσης» υπογραμμίζει τεχνικές που συμβάλλουν στη βελτίωση των δραστηριοτήτων ICT DR σε συγκεκριμένους τομείς και αποτελεί ένα επιπλέον επίπεδο παροχής υπηρεσιών. Ως αποτέλεσμα προκύπτει ότι οι συστάσεις σε αυτό το Διεθνές Πρότυπο προέρχονται από μια σύνθετη άποψη αυτών των στρωμάτων, διατηρώντας παράλληλα μια ισορροπία μεταξύ της σχέσης κόστους-αποτελεσματικότητας και της τυπικής αυστηρότητας.



Εικόνα 5 Πλαίσιο παροχής υπηρεσιών ICT DR

2.2.1 Ανάκτηση Υπηρεσιών Τεχνολογίας Πληροφοριών Και Υπηρεσιών Από Καταστροφές

Η περιβαλλοντική σταθερότητα είναι απαραίτητη για την άμεση λειτουργία μιας εγκατάστασης αποκατάστασης καθώς και για τα ταξίδια/μετακινήσεις, την ασφάλεια και την ευημερία των εργαζομένων. Οι επιχειρήσεις κοινής ωφέλειας που είναι απαραίτητες για τη λειτουργία ενός κέντρου αποκατάστασης, όπως η ηλεκτρική ενέργεια και οι τηλεπικοινωνίες, είναι ευαίσθητες στην περιβαλλοντική αστάθεια. Η ασφάλεια του προσωπικού που ταξιδεύει από και προς ένα κέντρο ανάκτησης μπορεί να τεθεί σε κίνδυνο εάν διαταραχθεί η υποδομή μεταφοράς. Η περιβαλλοντική αστάθεια μπορεί να προκληθεί από την τακτική εμφάνιση περιστατικών μεγάλης κλίμακας όπως απεργίες, βίαια εγκλήματα, φυσικές καταστροφές, πανδημίες και προγραμματισμένες επιθέσεις π.χ. τρομοκρατία.

Οι πάροχοι υπηρεσιών επιβάλλεται να διασφαλίζουν ότι τα περιουσιακά στοιχεία που τοποθετούνται στις εγκαταστάσεις ICT DR, όπως το λογισμικό εφαρμογών και οι βασικές πληροφορίες που είναι αποθηκευμένες σε υλικά μέσα. Αυτές οι πληροφορίες είναι αναγκαίο να μπορούν να εντοπιστούν, και να ανακτηθούν εγκαίρως από εξωτερικούς συνεργάτες όταν ζητηθούν από εταιρείες ή παρόχους υπηρεσιών. Για να διασφαλιστεί ότι ο ζωτικός εξοπλισμός και οι υπηρεσίες δύνανται να παρέχονται από τους προμηθευτές τους εντός καθορισμένων και συμφωνηθέντων χρονικών πλαισίων, πρέπει να αξιολογούνται όλοι οι κίνδυνοι. Προκειμένου να

επιτευχθεί αυτός ο στόχος, θα πρέπει να δημιουργηθεί ένα σύστημα προμηθειών για τη διαχείριση των τρόπων παράδοσης, του χρόνου παράδοσης και της διάρκειας εγγύησης των περιουσιακών στοιχείων, του εξοπλισμού και των ανταλλακτικών. Πιο αναλυτικά , όλα τα εξωτερικά μέρη, συμπεριλαμβανομένων των υπεργολάβων, είναι ωφέλιμο να ενημερώνονται για τα συμφωνημένα χρονοδιαγράμματα και τα καθήκοντα των παρόχων υπηρεσιών. Τουλάχιστον μία φορά το χρόνο, ο οργανισμός οφείλει να αξιολογεί την οικονομική, φυσική και βιωσιμότητα των υφιστάμενων προμηθευτών, καθώς και νέες διαδρομές για εναλλακτικές προμήθειες.

Επιπλέον, διαγράφεται έντονα η ανάγκη να εξεταστεί η θέση των συστημάτων ICT DR του οργανισμού. Οι οργανισμοί θα πρέπει να γνωρίζουν τη θέση των συστημάτων DR τους και να ειδοποιούνται όταν τα περιουσιακά τους στοιχεία μεταφέρονται. Δεν θα πρέπει να λησμονηθεί ότι οι επιχειρήσεις θα πρέπει να αξιολογούν τις συνέπειες των δεδομένων ανάκτησης και άλλων περιουσιακών στοιχείων από καταστροφές. Είναι πρωταρχική ανάγκη επίσης, να αποφευχθεί η αποθήκευση δεδομένων και άλλων περιουσιακών στοιχείων κατά μήκος εθνικών συνόρων ή σε άλλων γεωγραφικών περιοχών που είναι επιρρεπείς στις ίδιες απειλές καταστροφής/αστοχίας με τις κύριες τοποθεσίες ενός οργανισμού.

Επιπλέον, οι πάροχοι υπηρεσιών χρειάζεται να διασφαλίζουν την ακεραιότητα και την ασφάλεια των αποθηκευμένων δεδομένων και περιουσιακών στοιχείων και να εφαρμόζουν διαδικασίες και ελέγχους για τον σκοπό αυτό. Για να διασφαλιστεί η φυσική πρόσβαση σε εγκαταστάσεις που στεγάζουν συστήματα ICT και το απόρρητο των χώρων εργασίας τους, οι πάροχοι υπηρεσιών θα πρέπει να εφαρμόσουν περιορισμούς. Επίσης, οφείλουν να απαγορεύσουν τη μη εξουσιοδοτημένη πρόσβαση ή η αποκάλυψη πληροφοριών από το σύστημα ICT ενός οργανισμού στο σύστημα ICT άλλου οργανισμού. Όλα τα συμβάντα ασφαλείας και τα τρωτά σημεία πρέπει να αναφέρονται γρήγορα στην αρμόδια αρχή και πρέπει να λαμβάνονται τα κατάλληλα μέτρα αναπτύσσοντας ένα σαφές σύνολο διαδικασιών για τη διαχείριση ζητημάτων ασφάλειας πληροφοριών. Η εξέταση των αρχείων καταγραφής που σχετίζονται με τον εντοπισμό, την ειδοποίηση, την αντίδραση και την αποτελεσματικότητα περιστατικών ασφαλείας είναι μία από τις μεθόδους που πρέπει να ακολουθήσουν οι πάροχοι υπηρεσιών ή οι υπεργολάβοι τους.

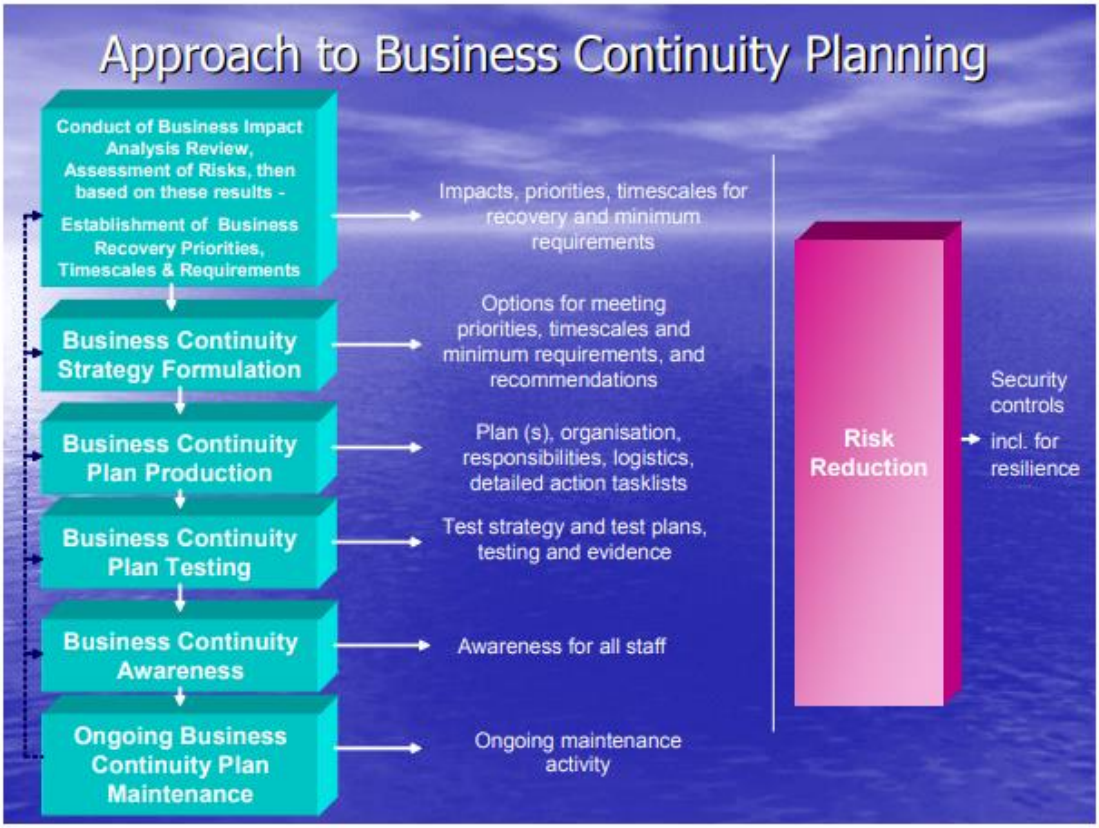
Με σκοπό αυτοί οι έλεγχοι να είναι αποτελεσματικοί, οι πάροχοι υπηρεσιών πρέπει να δημιουργήσουν ένα «σύστημα» που θα διασφαλίζει ότι όλο το προσωπικό που εμπλέκεται άμεσα στην παροχή υπηρεσιών ICT DR σε επιχειρήσεις,

συμπεριλαμβανομένων εκείνων που διαχειρίζονται τις φυσικές εγκαταστάσεις, έχει τα κατάλληλα προσόντα και εκπαίδευση. Οι οργανισμοί , για παρόμοιους λόγους, επιβάλλεται να δημιουργήσουν προγράμματα για την εκπαίδευση των ανθρώπων που θα ανατεθούν κατά τη διάρκεια μιας καταστροφής ή αποτυχίας και να αναθέσουν προσωπικό να συμμετάσχει σε ασκήσεις του σχεδίου disaster recovery. Και τα δύο μέρη θα πρέπει να αξιολογήσουν όλη την εκπαίδευση. Ως εκ τούτου, οι πάροχοι υπηρεσιών και οι οργανισμοί οφείλουν να διασφαλίζουν ότι το προσωπικό τους κατανοεί τις διαδικασίες.

Εκτός από αυτές τις πολιτικές και τους ελέγχους, οι πάροχοι υπηρεσιών είναι επιτακτική ανάγκη να καθορίσουν με τους πελάτες τους τα κριτήρια και τις διαδικασίες για την ενεργοποίηση και απενεργοποίηση των υπηρεσιών αποκατάστασης από καταστροφές. Για να αποφευχθεί η αβεβαιότητα και τυχόν παρεξηγήσεις, οι εκπρόσωποι των παροχών υπηρεσιών πρέπει να ανακοινώσουν στους εκπροσώπους του οργανισμού τη συμφωνία που έχει συναφθεί και συμφωνηθεί. Αυτές οι συμφωνίες θα ήταν καλό να καταγράφονται και να κοινοποιούνται σε όλο το σχετικό προσωπικό. Σύμφωνα με την αρχική συμφωνία, οι εκπρόσωποι των παρόχων υπηρεσιών είναι σημαντικό να επικυρώσουν τη συμφωνία με τον οργανισμό. Επιπλέον, ο πάροχος υπηρεσιών επιβάλλεται να ενημερώνει τους εργαζόμενους και τους εξωτερικούς προμηθευτές που εμπλέκονται άμεσα στις υπηρεσίες αυτές. Κατά την ενεργοποίηση, ο πάροχος υπηρεσιών οφείλει, εάν είναι απαραίτητο, να συλλέξει στοιχεία ώστε να προετοιμάσει και να μεταφέρει συνδρομητικές υπηρεσίες. Σε περίπτωση που ληφθεί απόφαση για απενεργοποίηση συνδρομητικών υπηρεσιών, οι πάροχοι πρέπει να εγγυηθούν ότι οι συμφωνίες με οργανισμούς περιλαμβάνουν διαδικασίες για την ομαλή μεταφορά των εγκαταστάσεων και του εξοπλισμού από τους οργανισμούς πίσω σε αυτούς.

Οι πάροχοι υπηρεσιών είναι απαραίτητο να εγγυώνται ότι όλα τα συστήματα ict που είναι υπεύθυνα για την αποκατάσταση από καταστροφές αξιολογούνται τακτικά με στόχο να επαληθευτεί ότι μπορούν να συνεχίσουν να υποστηρίζουν σχέδια αποκατάστασης από καταστροφές. Συμπληρωματικά, θα πρέπει να διενεργούνται δοκιμές κάθε φορά που υπάρχουν σημαντικές αλλαγές στις απαιτήσεις του οργανισμού ή και στην ικανότητα και τις δυνατότητες του παρόχου υπηρεσιών που έχουν απήχηση στις υπηρεσίες που παρέχονται στην εταιρεία. Όλες οι επιχειρηματικές λειτουργίες είναι ωφέλιμο να περιλαμβάνονται στα σχέδια επιχειρηματικής συνέχειας που αναπτύσσονται, δοκιμάζονται, συντηρούνται και ενημερώνονται από τους παρόχους

υπηρεσιών. Ωστόσο, οι πάροχοι υπηρεσιών θα ήταν καλό να αποφεύγουν να παράγουν τις στρατηγικές χωρίς πρώτα να διεξαγάγουν κρίσιμη έρευνα. Αρχικά, οι πάροχοι υπηρεσιών θα πρέπει να καθορίσουν τις προτεραιότητες της εταιρείας τους, ακολουθούμενες από την πιο κατάλληλη και οικονομικά αποδοτική στρατηγική επιχειρηματικής συνέχειας για το επιχειρηματικό τους περιβάλλον. Όταν οι πάροχοι υπηρεσιών έχουν συμφωνήσει σε στρατηγικές επιχειρηματικής συνέχειας και γνωρίζουν την καλύτερη πορεία δράσης τους, μόνο τότε υποχρεούνται να αναπτύξουν, να δοκιμάσουν και να εφαρμόσουν σχέδια επιχειρηματικής συνέχειας. Ακόμα, θα πρέπει να διαχειρίζονται τους κινδύνους για να μειώσουν την πιθανότητα ανάγκης εφαρμογής των σχεδίων ή/και να μετριάσουν τις επιπτώσεις μιας καταστροφής ή αποτυχίας, σε περίπτωση που συμβεί κάτι τέτοιο. Στην εικόνα 6 παρουσιάζεται η προτεινόμενη συνολική προσέγγιση για τον προγραμματισμό της επιχειρησιακής συνέχειας.



Εικόνα 6 Προσέγγιση Σχεδιασμού Επιχειρηματικής Συνέχειας

2.2.2 Πολιτικές Και Μέτρα Ασφαλείας Των Υποδομών Ανάκτησης Υπηρεσιών Τεχνολογίας Πληροφοριών Και Υπηρεσιών

Οι πάροχοι υπηρεσιών ICT DR είναι απαραίτητο να πληρούν θεμελιώδεις απαιτήσεις προκειμένου να παρέχουν ασφαλή, φυσικά και λειτουργικά περιβάλλοντα που υποστηρίζουν τις προσπάθειες ανάκτησης του οργανισμού. Εκτός από την παροχή θεμελιωδών φυσικών απαιτήσεων του κτιρίου, είναι χρήσιμο να ληφθούν υπόψη οι περιβαλλοντικοί έλεγχοι, οι τηλεπικοινωνίες, η συνεχής παροχή ρεύματος και λοιπές ανέσεις, όπως η στάθμευση και η πρόσβαση σε τρόφιμα και ποτά.

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, η τοποθέτηση υποδομών αποκατάστασης από καταστροφές αποτελεί μία σημαντική απόφαση όσον αφορά την αποτελεσματικότητά τους. Οι φυσικές καταστροφές ενδέχεται να δημιουργούν κινδύνους που δεν είναι δυνατόν να μετριαστούν ή να γίνουν αποδεκτοί. Επιπροσθέτως, ο καιρός, ιδίως οι δραματικές διακυμάνσεις του, μπορούν να δημιουργήσουν πολλά προβλήματα σε τοποθεσίες αποκατάστασης καταστροφών. Συνεπώς, οι επιχειρήσεις είναι πρωταρχικής σημασίας να αποφεύγουν να τοποθετούν τα συστήματα DR τους σε περιοχές επιρρεπείς σε φυσικές καταστροφές όπως ανεμοστρόβιλοι και σεισμοί, καθώς και ξαφνικές αλλαγές θερμοκρασίας ή ακραίες επιπτώσεις όπως καταρρακτώδεις βροχές.

Καταστροφές όπως αυτές που αναφέρονται παραπάνω όχι μόνο δύνανται να δημιουργήσουν προβλήματα στις υποδομές αποκατάστασης καταστροφών, αλλά και στις μεθόδους προσβασιμότητας. Όλοι οι χώροι είναι αναγκαίο να βρίσκονται σε κοντινή απόσταση από περιοχές που έχουν προσβασιμότητα με διάφορα μέσα και να διαθέτουν όλες τις απαραίτητες ανέσεις για τη φιλοξενία του προσωπικού.

Συμπληρωματικά, η ασφάλεια του εξοπλισμού και των εργαζομένων είναι απαραίτητη. Οι πάροχοι υπηρεσιών είναι επιβεβλημένη ανάγκη να αποφεύγουν περιοχές κάτω από χώρους προσγείωσης ή κοντά σε πολυσύχναστα νοσοκομεία, ειδικά εκείνα που αντιμετωπίζουν πανδημίες και άλλες καταστροφές. Επίσης, οι δημόσιες εγκαταστάσεις όπως οι σταθμοί ηλεκτροπαραγωγής και οι πύργοι αναμετάδοσης μπορούν να προκαλέσουν παρεμβολές. Οι παρεμβολές αυτές μπορούν να μετριαστούν θάβοντας τα καλώδια τηλεπικοινωνιών και τροφοδοσίας των παροχών. Γενικά, τα καλώδια δεν πρέπει να εκτίθενται σε υπερβολική εξωτερική φυσική φθορά.

Πιθανός κίνδυνος θεωρείται ακόμη το ανθρώπινο στοιχείο. Οι πάροχοι υπηρεσιών είναι σημαντικό να ορίσουν ζώνες ασφαλείας και να ταξινομήσουν τους

εργαζομένους με στόχο να εφαρμόζουν καλύτερα πολιτικές και ελέγχους διαχείρισης των εργαζομένων και των επισκεπτών. Ο διαχωρισμός των ζωνών ασφαλείας σε περιορισμένες εγκαταστάσεις και κοινές εγκαταστάσεις είναι απαραίτητος. Περιορισμένης πρόσβασης θεωρούνται οι χώροι που στεγάζουν εγκαταστάσεις και εξοπλισμό, όπως διακομιστές. Οι κοινές εγκαταστάσεις, από την άλλη πλευρά, είναι χώροι ή δωμάτια που χρησιμοποιούνται από όλο το προσωπικό και δεν υπόκεινται σε εσωτερικούς περιορισμούς ασφαλείας. Αυτοί οι χώροι είναι πιθανό να περιλαμβάνουν χώρους υποδοχής, καφετέριες και τουαλέτες. Όσον αφορά το προσωπικό επιβάλλεται να υπάρχουν τέσσερις κατηγορίες. Αυτές οι ομάδες περιέχουν προσωπικό σέρβις, εργαζόμενους του οργανισμού, εργαζομένους παροχών υπηρεσιών και επισκέπτες.

Το προσωπικό του παρόχου υπηρεσιών είναι αναγκαίο να έχει πρόσβαση όλο το εικοσιτετράωρο στις εγκαταστάσεις που αναπτύσσονται και επιβάλλονται για κάθε ζώνη ασφαλείας με βάση την κατάταξη ασφαλείας τους. Αυτός ο βαθμός πρόσβασης παρέχεται από τον πάροχο υπηρεσιών σε νεοπροσλαμβανόμενο προσωπικό. Μετά την παραίτηση, όλες οι εξουσιοδοτήσεις πρόσβασης που σχετίζονται με το προσωπικό είναι απαραίτητο να ανακληθούν αμέσως. Εκτός αυτού, ο πάροχος υπηρεσιών επιβάλλεται να σχεδιάσει τα απαραίτητα πρωτόκολλα ώστε οι εργαζόμενοι να έχουν πρόσβαση εκτός των κανονικών ωρών λειτουργίας, όπως απαιτείται, κατά τη διάρκεια επιτόπιας αποκατάστασης από καταστροφές.

Η σύμβαση με τον πάροχο υπηρεσιών επιτρέπει στο προσωπικό του οργανισμού να επισκέπτεται τον χώρο ανάκτησης σε προκαθορισμένα χρονικά διαστήματα. Κατά τη διάρκεια μιας καταστροφής, το προσωπικό του οργανισμού είναι ζωτικής σημασίας να έχει πρόσβαση 24 ώρες την ημέρα, επτά ημέρες την εβδομάδα.

Εκτός από το προσωπικό του παρόχου υπηρεσιών και του οργανισμού, σαφείς πολιτικές και διαδικασίες θα πρέπει να διέπουν όλο το υπόλοιπο προσωπικό. Ορισμένες πολιτικές εμπεριέχουν αιτήματα για είσοδο στις εγκαταστάσεις του παρόχου υπηρεσιών και πρόσβαση σε ιδιόκτητες εγκαταστάσεις, συνοδεία και παρακολούθηση από το προσωπικό του παρόχου υπηρεσιών, σήματα/κάρτες μοναδικές για τον κάθε εξωτερικό επισκέπτη που εισέρχεται στις εγκαταστάσεις του παρόχου υπηρεσιών και καταγραφή της εισόδου τρίτων, συμπεριλαμβανομένων των μόνιμων εργολάβων, στις εγκαταστάσεις του παρόχου υπηρεσιών.

Με σκοπό να εξασφαλιστεί ο έλεγχος εισόδου όπως αναφέρεται παραπάνω βασική προϋπόθεση είναι η ασφάλεια και άρτια λειτουργία των κτηριακών εγκαταστάσεων και συστημάτων ασφαλείας. Όλες οι πιθανοί είσοδοι πρέπει να είναι

προστατευμένοι. Η προστασία είναι απαραίτητη και στους χώρους φύλαξης όπου οι οργανισμοί αποθηκεύουν ευαίσθητα δεδομένα τους, όπως μαγνητικά μέσα και προμήθειες .Επιπλέον, πρέπει να υπάρχουν συστήματα ανίχνευσης και συναγερμού σε όλους του χώρους περιορισμένης πρόσβασης. Οι αισθητήρες ανίχνευσης εκτός από διαρρήξεις θα πρέπει να είναι ικανοί να εντοπίσουν καπνό, φωτιά και διαρροές νερού.

Όλες οι έννοιες προστασίας είναι αναγκαίο να χρησιμεύουν ως θεμέλια προστασίας στις διαδικασίες φυσικής ασφάλειας, ενσωματώνοντας και συμπληρώνοντας η μία την άλλη. Μια στρατηγική προστασίας που εστιάζει αποκλειστικά σε έναν ψηλό περιμετρικό τοίχο, για παράδειγμα, μπορεί να είναι ανεπαρκής έναντι άλλων τύπων εισβολής. Το στάνταρντ προτείνει τρεις τρόπους προσέγγισης. Την πολυεπίπεδη προσέγγιση, κατά την οποία οι χώροι είναι χωρισμένοι σε πολλαπλά στρώματα από την εξωτερική περίμετρο έως τον εσωτερικό πυρήνα, με αντίστοιχα αυξανόμενους περιορισμούς που επιβάλλονται σε κάθε διαδοχική βαθμίδα. Ή τον διαχωρισμό ανά τμήμα-τομέα όπου υπάρχουν διακριτοί τομείς για τα κτίρια. Κάθε κτήριο/τομέας είναι δυνατόν να υπόκειται σε διαφορετικά κριτήρια προστασίας πρόσβασης. Τελευταία είναι η σύνθετη προσέγγιση στην οποία υπάρχει συνδυασμός των τεχνικών πολλαπλών επιπέδων και τομέων. Οι εγκαταστάσεις είναι χωρισμένες σε διάφορους τομείς με αυξανόμενους περιορισμούς από την εξωτερική περίμετρο έως το κέντρο κάθε τομέα.

Όποια μέθοδο και να ακολουθήσουν οι πάροχοι υπηρεσιών είναι υποχρεωμένοι να εφαρμόσουν κάποιες κοινές πολιτικές. Οι χώροι τους οποίους παρέχουν οι πάροχοι υπηρεσιών στον οργανισμό για δραστηριότητες αποθήκευσης και ανάκτησης επιβάλλεται να είναι επαρκείς, ώστε οι οργανισμοί να μπορέσουν να συγκεντρώσουν και να ενημερώσουν όλο το προσωπικό ανάκτησης σε αυτούς . Οι χώροι αυτοί θα πρέπει να περιλαμβάνουν χώρους συναρμολόγησής, χώρους αποθήκευσης, εκφόρτωσης και φόρτωσης καθώς και χώρους δοκιμών του εξοπλισμού .Επίσης, οι πάροχοι υπηρεσιών οφείλουν να αποφεύγουν την αποθήκευση εύφλεκτων υλικών και να απαγορεύσουν κινητές συσκευές όπως PDA, κάμερες και αναιρούμενα μέσα αποθήκευσης από περιοχές/δωμάτια στα οποία στεγάζονται ευαίσθητες εγκαταστάσεις όπως data rooms. Όλες οι ευαίσθητες πληροφορίες του οργανισμού είναι αναγκαίο να μπορούν να καταστραφούν βάσει διαδικασιών και παρεχόμενων μέσων(π.χ. καταστροφείς εγγράφων) διαθέσιμα από τον πάροχο υπηρεσιών. Επιπρόσθετα, όλα τα κλειδιά ή άλλα μέσα πρόσβασης όπως μαγνητικές κάρτες και ψηφιακά κλειδιά πρέπει να καταγράφονται να οργανώνονται και να διαχειρίζονται κεντρικά από τον

οργανισμό. Όλος ο εξοπλισμός που παρέχει περιβαλλοντικούς ελέγχους είναι σημαντικό να είναι εξοπλισμένος σε μεγαλύτερο βαθμό από τον απαιτούμενο, λαμβάνοντας υπόψη τη συντήρηση ή/και την αστοχία του εξοπλισμού με στόχο να, ελαχιστοποιηθούν οι αρνητικές συνέπειες σε επίπεδο υπηρεσιών. Τα έγγραφα που μπορούν να συσχετίσουν ή να προσδιορίσουν ευαίσθητες εγκαταστάσεις επεξεργασίας πληροφοριών θα πρέπει να είναι διαθέσιμα μόνο σε κατάλληλα εξουσιοδοτημένα άτομα.

Οι πάροχοι υπηρεσιών υποχρεούνται να εγγυώνται ότι ελαχιστοποιούνται τα μεμονωμένα σημεία αστοχίας στις τηλεπικοινωνίες, παρέχοντας εναλλακτικές πηγές τηλεπικοινωνιών για ανακατεύθυνση. Οποιαδήποτε εναλλακτική πηγή είναι αναγκαίο να είναι μια ανεξάρτητη, διακριτή και μη κοινόχρηστη συλλογή τηλεπικοινωνιακών υποδομών και γραμμών που οδηγούν σε μια τοποθεσία ανάκτησης παρόχου υπηρεσιών. Τα καλώδια που διασχίζουν χώρους/δωμάτια προσβάσιμα στο κοινό ή που δεν μπορούν να φυλαχτούν, προστατεύονται με διάφορα μέσα όπως κρυφές καλωδιώσεις γραμμών, αγωγών ή/και δίσκων με επαρκή αντοχή υλικού για την προστασία των γραμμών από φυσικές βλάβες, γραμμές κίνησης σε μηχανικά συμπαγείς αγωγούς και αγωγούς που κλειδώνουν. Οι πάροχοι υπηρεσιών οφείλουν να διατηρούν τα ακριβή και τρέχοντα σχέδια τοποθεσίας για όλες τις καλωδιώσεις. Τέτοια σχέδια παρέχουν βασικές πληροφορίες για την εγκατάσταση καλωδίων, τη συντήρηση, την αντιμετώπιση προβλημάτων και την επισκευή, αφού βοηθούν στον εντοπισμό πιθανών ζωνών κινδύνου.

Συμπληρωματικά, οι πάροχοι υπηρεσιών οφείλουν να εγγυώνται ότι οι τοποθεσίες ανάκτησης διαθέτουν εναλλακτικές πηγές ενέργειας για προσωρινή χρήση (όταν οι κανονικές πηγές ενέργειας αποτυγχάνουν) που είναι ικανές να ικανοποιήσουν όλες τις απαιτήσεις ανάκτησης του οργανισμού, μέχρι να αποκατασταθούν οι κανονικές πηγές ενέργειας. Προκειμένου να αποφευχθούν σημαντικές διακοπές ρεύματος, που εμποδίζουν τις προσπάθειες ανάκτησης, είναι υποχρεωτικό να εγκατασταθούν εφεδρικές γεννήτριες. Επιπλέον, οι μονάδες UPS θα πρέπει να εγκατασταθούν με τέτοιο τρόπο, που να παρέχονται και να συντηρούνται έτσι ώστε τα κρίσιμα για την αποστολή δίκτυα και ο εξοπλισμός υπολογιστών να δύνανται να λειτουργούν και να τερματίζονται με τακτικό τρόπο. Κατά τη διάρκεια διακοπών ρεύματος, είναι σημαντικό για τους παρόχους υπηρεσιών να εγγυώνται ότι η μετάβαση από τις τυπικές πηγές ενέργειας στις γεννήτριες πραγματοποιείται με ασφάλεια και χωρίς να διακόπτονται οι συνήθεις λειτουργίες. Αυτές οι μεταβάσεις είναι σημαντικό

επίσης να εντοπιστούν. Από την άλλη πλευρά, όταν ζητηθεί από τους οργανισμούς, οι πάροχοι υπηρεσιών είναι υποχρεωμένοι να εγγυώνται ότι παρέχονται διακόπτες κυκλώματος έκτακτης ανάγκης σε σημεία που έχουν καθοριστεί από τον οργανισμό όπου η θερμότητα που παράγεται από ηλεκτρικές συσκευές θα μπορούσε να αποτελέσει κίνδυνο πυρκαγιάς.

Οι πάροχοι υπηρεσιών επιβάλλεται να διασφαλίζουν ότι υπάρχουν κατάλληλα συστήματα πυρανίχνευσης και καταστολής στους χώρους ανάκτησής τους για την προστασία του εξοπλισμού, των υπολογιστών και των εργαζομένων. Η χωρητικότητα αυτών των συστημάτων θα πρέπει να είναι ανάλογη με το απαιτούμενο επίπεδο προστασίας και τα μεγέθη της περιοχής/δωματίου. Οι πάροχοι υπηρεσιών οφείλουν να διασφαλίζουν ότι οι οδοί διαφυγής πυρκαγιάς σχεδιάζονται, καταγράφονται και κοινοποιούνται σε όλους τους εργαζόμενους, και ότι υπάρχουν σχέδια και διαδικασίες για την αντιμετώπιση εστιών πυρκαγιάς και καπνού. Περιοδικά, είναι θετικό να πραγματοποιούνται ασκήσεις εκκένωσης που σχετίζονται με πυρκαγιές με στόχο την δοκιμή διάφορων στοιχείων αυτών των σχεδίων και διαδικασιών αντιμετώπισης πυρκαγιάς/καπνού. Τα σημεία παροχής νερού για την πυρόσβεση θα πρέπει να έχουν καθοριστεί κατάλληλα, με σκοπό να είναι εύκολο να ανακαλυφθούν αμέσως σε περίπτωση πυρκαγιάς και, εάν απαιτείται από τους τοπικούς κανονισμούς. Αντίγραφα των σχεδίων που καθορίζουν τα σημεία παροχής νερού είναι υποχρεωτικό να υποβάλλονται στις τοπικές υπηρεσίες έκτακτης ανάγκης .

Οι πάροχοι υπηρεσιών θα πρέπει να παρέχουν κέντρα λειτουργίας εκτακτης ανάγκης (Emergency Operation Centers EOC) στους χώρους ανάκτησής τους που είναι επαρκώς προετοιμασμένα, ώστε να επιτρέπουν στις εταιρείες να διαχειρίζονται και να διατηρούν συνδέσεις με τις επιχειρηματικές τους μονάδες και τους εξωτερικούς συνεργάτες τους κατά τη διάρκεια καταστροφών ή διακοπών λειτουργίας. Αυτός ο εξοπλισμός περιλαμβάνει τηλεπικοινωνιακό εξοπλισμό, εξοπλισμό γραφείου και προμήθειες γραφείου. Επιπλέον, τα EOC είναι πρωταρχικής σημασίας να είναι εξοπλισμένα με ειδικές φυσικές εγκαταστάσεις. Αυτές περιλαμβάνουν αίθουσες φωνητικών επικοινωνιών, αίθουσες συσκέψεων, αίθουσες ενημέρωσης μέσων και χώρους εργασίας για την ομάδα αποκατάστασης της περιοχής εργασίας.

Ακόμη έλεγχοι υγείας και ασφάλειας για το προσωπικό περιλαμβάνουν τον συνεχή αερισμό, τον κατάλληλο φωτισμό, τις ηλεκτρικά ελεγχόμενες πόρτες που μπορούν να ανοίγουν χωρίς ηλεκτρικό ρεύμα, τα σύστημα δημόσιας αναγγελίας (Public Announcement PA) και σύστημα συναγερμού.

Όλες οι φυσικές εγκαταστάσεις και ο εξοπλισμός είναι απαραίτητο να εξετάζονται σε τακτική βάση από κατάλληλα έμπειρους εσωτερικούς ή εξωτερικούς επαγγελματίες. Το πεδίο εφαρμογής αυτών των ανασκοπήσεων θα πρέπει να περιλαμβάνει τη φυσική προστασία των χώρων και της περιμέτρου του χώρου ανάκτησης, τον εξοπλισμό φυσικής ασφάλειας, τον εξοπλισμό περιβαλλοντικού ελέγχου, τον εξοπλισμό και τις εγκαταστάσεις ICT, τον εξοπλισμό και εγκαταστάσεις τηλεπικοινωνιών, την προστασία από πυρκαγιά και καπνό τροφοδοσίας ρεύματος και προστασία νερού/υγρού. Η δημιουργία αναφορών είναι σημαντικό να ακολουθεί κάθε επανεξέταση. Αυτές οι αξιολογήσεις επιβάλλεται να καλύπτουν το πεδίο εφαρμογής, τις διαδικασίες που ακολουθήθηκαν, τα ευρήματα και τα συμπεράσματα, τις αποκλίσεις και τα απαραίτητα διορθωτικά μέτρα. Όταν υπάρχουν σημαντικές αλλαγές στις ανάγκες του οργανισμού, είναι απαραίτητο να πραγματοποιούνται επιθεωρήσεις φυσικών κτιρίων και εξοπλισμού. Για την επίτευξη αυτού του στόχου, οι πάροχοι υπηρεσιών οφείλουν να διασφαλίζουν ότι διατηρούν τρέχοντα αποθέματα των ειδών φυσικών εγκαταστάσεων και εξοπλισμού τους και ότι παρακολουθούνται συνεχώς τα σημαντικά είδη φυσικών εγκαταστάσεων και εξοπλισμού. Επιπροσθέτως, οι πάροχοι υπηρεσιών υποχρεούνται να επαληθεύουν ότι η λειτουργία των στοιχείων φυσικής εγκατάστασης και εξοπλισμού δύναται να εφαρμοστεί στο υπάρχων firmware και λογισμικό (software). Τα ανταλλακτικά και αξεσουάρ θα πρέπει να διατηρούνται σε ετοιμότητα και να είναι επαρκή για να διευκολύνεται η επισκευή, η συντήρηση και η αντικατάσταση των φυσικών εγκαταστάσεων και εξοπλισμού με ελάχιστη διακοπή στις συνήθεις λειτουργίες. Επιπλέον, τυχόν φυσικές εγκαταστάσεις και εξοπλισμός που έχουν φτάσει στο τέλος της ωφέλιμης ζωής τους παροπλίζονται ή/και αφαιρούνται από κατάλληλα καταρτισμένο προσωπικό και σύμφωνα με τις τρέχουσες συστάσεις του κατασκευαστή, επαγγελματικά πρότυπα/πρακτικές και κανονιστικές απαιτήσεις.

2.2.3 Επιλογή Κατάλληλων Θέσεων Για Τις Υποδομές Ανάκτησης Υπηρεσιών Τεχνολογίας Πληροφοριών Και Υπηρεσιών

Όπως περιγράφεται στο κεφάλαιο 2, οι τοποθεσίες των υποδομών disaster recovery αποτελούν κρίσιμο συστατικό των συνεχιζόμενων λειτουργιών του συστήματος πληροφορικής. Κατά τη διάρκεια φυσικών ή ανθρωπογενών καταστροφών, αυτά τα μέτρα μπορούν να διατηρήσουν την προσβασιμότητα των

συστημάτων/υποδομών IT και να μετριάσουν τις οικονομικές απώλειες. Όσον αφορά το κόστος και τον κίνδυνο, οι δυσκολίες επιλογής τοποθεσίας ανάκτησης από καταστροφές συστημάτων πληροφορικής είναι ένα από τα προβλήματα απόφασης πολλαπλών κριτηρίων. Εκτός από τη σταθερότητα του εξωτερικού περιβάλλοντος, η επαρκής υποδομή και η διαθεσιμότητα εκπαιδευμένου τοπικού εργατικού δυναμικού θα συμβάλουν σε ένα κατάλληλο περιβάλλον για τους παρόχους υπηρεσιών ICT DR για τη λειτουργία τοποθεσιών ανάκτησης. Επιπλέον, η παρουσία άλλων παρόχων υπηρεσιών ICT DR και των προμηθευτών στην περιοχή θα δημιουργήσει την κρίσιμη μάζα που απαιτείται για έναν ακμάζοντα τοπικό τομέα. Το ιστορικό εξυπηρέτησης/συνεργασίας με άλλες σημαντικές εταιρείες/πελάτες είναι ένα επιπλέον μέτρο της ωριμότητας και της ζωτικότητας της τοπικής αγοράς ICT DR. Εκτός από τα κριτήρια που δίνονται στο κεφάλαιο 2, το κεφάλαιο 8 του ISO παρέχει πρόσθετα κριτήρια.

Η εξωτερική υποδομή της περιοχής στην οποία οι εξωτερικοί πάροχοι υπηρεσιών τοποθετούν τις υποδομές disaster recovery επηρεάζει το εύρος και την ποιότητα των υπηρεσιών που μπορούν να παρασχεθούν. Εκτός από την προσβασιμότητα, οι λειτουργίες ανάκτησης από τις τοποθεσίες συστημάτων DR ενδέχεται να επηρεαστούν εάν υπάρχουν αβεβαιότητες, συχνές διακυμάνσεις ή διακοπές στις επικοινωνίες, στην παροχή ρεύματος ή την χερσαία μεταφορά. Τα προαναφερθέντα στοιχεία υποδομής επηρεάζονται και από τις αεροπορικές ή θαλάσσιες συνδέσεις και τις μεταφορές.

Είναι αναγκαίο να υπάρχει μια τοπική ομάδα εκπαιδευμένων και έμπειρων ειδικών στον τομέα του ICT στη στοχευμένη τοποθεσία. Για να είναι σε θέση να αναλάβει επιχειρησιακούς ρόλους ICT DR, το διαθέσιμο εργατικό δυναμικό θα πρέπει να αποτελείται από επαγγελματίες υψηλού επιπέδου οι οποίοι εκπαιδεύονται πιο γρήγορα, όπως και από ένα ευρύ φάσμα παρόχων εκπαίδευσης και κατάρτισης ICT DR. Το προφίλ των παρόχων υπηρεσιών ICT DR σε μια περιοχή είναι ενδεικτικό του επιπέδου ανάπτυξης της τοπικής βιομηχανίας ICT DR. Το προφίλ είναι πιθανό να περιλαμβάνει πληροφορίες όπως τον αριθμό των ετών που πραγματοποιήθηκαν τοπικές λειτουργίες, τον αριθμό των δοκιμών ανάκτησης που πραγματοποιήθηκαν κατά τη διάρκεια τοπικών λειτουργιών, το πλήθος των οργανισμών στους οποίους έχουν πραγματοποιήσει ανάκτηση από τοπικούς εγκαταστάσεις και το προφίλ των οργανισμών που βοήθησαν/συνεργάστηκαν.

Ένας ελάχιστος/απαιτούμενος αριθμός πωλητών και προμηθευτών είναι ωφέλιμο να υποστηρίζει την τοποθεσία DR και όλες τις σχετικές δραστηριότητες. Θα πρέπει να υπάρχει μια κρίσιμη ποσότητα και ποικιλία προμηθευτών ICT DR και προμηθευτών στην περιοχή, ώστε να δύναται να παρέχουν τις απαιτούμενες συμβουλές, εξοπλισμό, υλικό και λογισμικό υποστήριξης και αντικατάστασης 24 ώρες την ημέρα, επτά ημέρες την εβδομάδα. Οι προμηθευτές ICT DR αποτελούνται από συμβούλους και παρόχους υλικού και υπηρεσιών, όπως εταιρείες hardware, λογισμικού, τεχνολογίας και τηλεπικοινωνιών.

Εκτός από το τοπικό εργατικό δυναμικό, τους παρόχους υπηρεσιών και τους προμηθευτές, τη χώρα στην οποία βρίσκεται η τοποθεσία ανάκτησης, το πολιτικό της περιβάλλον και τις σχετικές ευκαιρίες, η υποστήριξη των τοπικών και εθνικών αρχών μπορεί να διαδραματίσει ζωτικό ρόλο στην ανάπτυξη και την εξέλιξη του ICT DR μίας επιχείρησης. Ανάλογα με το ρόλο των τοπικών και εθνικών αρχών σε μια χώρα, η τοπική υποστήριξη θα μπορούσε να περιλαμβάνει την ανάπτυξη ενός προτύπου ICT DR και προγράμματος πιστοποίησης, την υποστήριξη μεγάλων προμηθευτών ICT DR με σκοπό την εγκαθίδρυση και ενίσχυση των δραστηριοτήτων τους σε τοπικό επίπεδο, την εφαρμογή μιας προληπτικής στρατηγικής τηλεπικοινωνιών για την ενθάρρυνση μεγάλων πωλητών ICT DR να δημιουργήσουν τις δραστηριότητές τους σε τοπικό επίπεδο και την εκχώρηση και τον προσχεδιασμό γης για χρήση ως τοποθεσίες disaster recovery.

Διάφορες ομάδες έχουν εργαστεί σε ζητήματα επιλογής τοποθεσιών και οι ιδέες σχετικά με το "πού είναι ο κατάλληλος ιστότοπος" και "πώς να επιλεχθεί μία τοποθεσία" ποικίλλουν. Ορισμένοι συγγραφείς πίστευαν ότι η επιλογή μιας κατάλληλης τοποθεσίας απαιτούσε την εξέταση πολλών χαρακτηριστικών και κριτηρίων, ιδιαίτερα της τοποθεσίας της εγκατάστασης. Για παράδειγμα, ο Wang όπως και άλλοι ερευνητές [35] αξιολόγησαν τις περιβαλλοντικές και οικονομικές πτυχές, όπως η τιμή και η απόσταση, και ανέπτυξαν ένα ιεραρχικό πλαίσιο λήψης αποφάσεων για την επίλυση του προβλήματος της επιλογής του χώρου διάθεσης στερεών αποβλήτων. Ο Covas [36] τόνισε ότι η ενεργειακή απόδοση θα πρέπει να λαμβάνεται υπόψη κατά την εξέταση μιας νέας τοποθεσίας κέντρου δεδομένων, κυρίως επειδή τα κέντρα δεδομένων απαιτούν μεγάλη ισχύ για τον εξοπλισμό επεξεργασίας και την υποδομή τους. Άλλοι μελετητές δίνουν μεγαλύτερη έμφαση στην τεχνική επιλογής τοποθεσίας, θεωρώντας την ως το αρχικό βήμα μιας διεξοδικής διαδικασίας λήψης αποφάσεων [37,38]. Μια πληθώρα μελετών αξιολογεί τις βέλτιστες τοποθεσίες

χρησιμοποιώντας διάφορες στρατηγικές λήψης αποφάσεων. Αυτές οι τεχνικές εμπεριέχουν τις προσεγγίσεις διευρυμένης ταξινόμησης ή βαθμολόγησης [39], τη διαδικασία Analytic Hierarchy Process (AHP) [40] και την προσέγγιση Linear Programming(LP) [52].

Σύμφωνα με τους Herbane και άλλους ερευνητές [42], πολλές εταιρείες υιοθέτησαν/εγκατέστησαν διαδικασίες διαχείρισης επιχειρηματικής συνέχειας για να αποφύγουν την απώλεια πελατών, την ανθεκτικότητα της διαμόρφωσης ή για λόγους υποχρέωσης/συμμόρφωσης. Για αυτούς τους λόγους, η ευθύνη για την επιλογή ενός τόπου για αποκατάσταση από καταστροφές είναι ένα από τα πιο σημαντικά στοιχεία για την διαχείριση της επιχειρησιακής συνέχειας. Λόγω νομικής υποχρέωσης, ορισμένες εταιρείες (υπηρεσίες κοινής ωφέλειας, τηλεπικοινωνίες, δημόσιος τομέας, χρηματοπιστωτικά ιδρύματα, υγειονομική περίθαλψη κ.λπ.) διαθέτουν χώρους αποκατάστασης καταστροφών ή, γενικότερα εγκαταστάσεις/υπηρεσίες BCM. Τέτοιοι χώροι αποκατάστασης καταστροφών πρέπει να είναι διαπιστευμένοι βάσει διεθνών προτύπων ή εθνικών κανόνων [43] είτε αυτό είναι το ISO 22301 είτε κάποιο άλλο διεθνές πρότυπο/στάνταρντ.

3 Σχεδιασμός Μηχανισμών Έκτακτης Ανάγκης Για Ομοσπονδιακά Πληροφοριακά Συστήματα

Στα προηγούμενα κεφάλαια αναφέρθηκε η σημαντικότητα και τα πλεονεκτήματα της διαχείρισης της επιχειρησιακής συνέχειας. Ακόμα, στο κεφάλαιο 2.2.3 αναφέρθηκαν τα πλεονεκτήματα που ενδέχεται να έχει η κρατική/τοπική υποστήριξη στους παρόχους υπηρεσιών, τους προμηθευτές και το εργατικό δυναμικό. Στο κεφάλαιο αυτό θα πραγματοποιηθεί ανάλυση των μεθόδων απαιτήσεων της επιχειρησιακής συνέχειας σε κρατικά συστήματα/υπηρεσίες. Σύμφωνα με τον οργανισμό NIST (National Institute of Standards and Technology) ως δημόσιο πληροφοριακό σύστημα ορίζεται ένα πληροφοριακό σύστημα που χρησιμοποιείται ή λειτουργεί από εκτελεστικό οργανισμό, από ανάδοχο εκτελεστικού οργανισμού ή από άλλο οργανισμό για λογαριασμό εκτελεστικού οργανισμού [44].

Η ανάλυση των συγκεκριμένων μεθόδων/απαιτήσεων βασίζεται στο πρότυπο 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems το οποίο έχει

εκδώσει ο οργανισμός NIST. Ο σχεδιασμός έκτακτης ανάγκης (contingency planning) αναφέρεται σε ενδιάμεσες προσπάθειες για την ανάκτηση των λειτουργιών του συστήματος πληροφοριών μετά από μια διακοπή. Τα προσωρινά μέτρα είναι πιθανό να περιλαμβάνουν τη μετεγκατάσταση συστημάτων και δραστηριοτήτων πληροφοριών σε διαφορετική τοποθεσία, την ανάκτηση λειτουργιών συστημάτων πληροφοριών με χρήση εναλλακτικής τεχνολογίας ή τη μη αυτόματη εκτέλεση λειτουργιών συστημάτων πληροφοριών.

Η διαμόρφωση λεπτομερών σχεδίων, διαδικασιών και τεχνικών βημάτων για τη δημιουργία αντιγράφων ασφαλείας ενός συστήματος και τη λειτουργία του όσο το δυνατόν πιο γρήγορα και αποτελεσματικά μετά από διακοπή της υπηρεσίας συνιστά σχεδιασμό έκτακτης ανάγκης. Ένα σχέδιο έκτακτης ανάγκης είναι μια στρατηγική που επιτρέπει στην κυβέρνηση, έναν οργανισμό ή μια επιχείρηση να ανταποκριθεί αποτελεσματικά σε απρόβλεπτα γεγονότα.

Κατά συνέπεια, ο οδηγός σχεδιασμού έκτακτης ανάγκης για το ομοσπονδιακό σύστημα πληροφοριών είναι μια δημοσίευση που περιλαμβάνει σχέδια που παρέχουν συγκεκριμένες οδηγίες για την αντίδραση σε περίπτωση παραβίασης των ομοσπονδιακών συστήματα πληροφοριών. Εξ ορισμού, η δημοσίευση περιέχει σχέδια, συστάσεις και οδηγίες για τον τρόπο ανάπτυξης ενός σχεδίου έκτακτης ανάγκης. Το έγγραφο δημιουργήθηκε για την ομοσπονδιακή κυβέρνηση, αλλά οι κανονισμοί της ισχύουν και για ιδιωτικές επιχειρήσεις.

Ο οδηγός σχεδιασμού έκτακτης ανάγκης εξυπηρετεί πολλαπλές λειτουργίες. Ο επιτυχημένος σχεδιασμός έκτακτης ανάγκης δίνει τη δυνατότητα στους κυβερνητικούς οργανισμούς να ανακάμψουν γρήγορα από καταστροφές και να προστατεύσουν ευαίσθητα δεδομένα, από το να πέσουν σε λάθος χέρια, καθώς υπάρχουν προεγκατεστημένες διαδικασίες για την αντιμετώπιση παραβιάσεων ασφάλειας. Επιπλέον, ο σχεδιασμός έκτακτης ανάγκης ελαχιστοποιεί τον αντίκτυπο ατυχών καταστάσεων.

Η ανάπτυξη σχεδίου είναι η καρδιά του σχεδιασμού έκτακτης ανάγκης του συστήματος πληροφοριών και αποτελείται από τα συστατικά μέρη του σχεδίου. Το πρότυπο του NIST παρέχει συστάσεις για την ανάπτυξη αυτών των σχεδίων, τα οποία θα πρέπει να προσαρμοστούν στις ανάγκες του οργανισμού. Ο στόχος της στρατηγικής είναι να διασφαλίσει ότι το σύστημα πληροφοριών είναι ικανό να ανακτηθεί μετά από μια διακοπή. Το πρώτο βήμα στην κατασκευή μιας στρατηγικής είναι ο εντοπισμός των

βασικών στοιχείων του συστήματος. Πιο συγκεκριμένα, ο καθορισμός του ελάχιστου αποδεκτού επιπέδου εξυπηρέτησης οφείλεται να διατηρηθεί ως το επόμενο στάδιο.

Αφού καθοριστούν αυτά τα κριτήρια, το πρότυπο συνιστά την εξέταση πολλών μεθόδων ανάκτησης, συμπεριλαμβανομένων των πλεονασμάτων, εναλλακτικών τοποθεσιών και συστημάτων δημιουργίας αντιγράφων ασφαλείας. Τρίτο στάδιο αποτελεί η καθιέρωση διεξοδικών διαδικασιών ανάκτησης και ο τακτικός έλεγχος. Τηρώντας αυτά τα βήματα, οι εταιρείες είναι σε θέση να διασφαλίσουν ότι τα πληροφοριακά τους συστήματα είναι έτοιμα για κάθε ενδεχόμενο.

Το εγχειρίδιο περιγράφει ένα σχέδιο έκτακτης ανάγκης επτά βημάτων που επιβάλλεται να αναπτύξουν οι επιχειρήσεις προκειμένου να προετοιμαστούν για διάφορους κινδύνους. Σύμφωνα με αυτό, η ευθύνη για τη διαδικασία σχεδιασμού ανήκει στον συντονιστή του σχεδίου έκτακτης ανάγκης πληροφοριακού συστήματος. Τα επτά βήματα περιγράφονται παρακάτω.

Το πρώτο βήμα αφορά την ανάπτυξη μίας δήλωσης πολιτικής σχεδίου έκτακτης ανάγκης. Η δήλωση πολιτικής για το σχέδιο έκτακτης ανάγκης καθορίζεται συνήθως σε επίπεδο φορέα, σε αυτήν την περίπτωση από το NIST. Αυτή η δήλωση περιγράφει την αποστολή, τους στόχους και το πεδίο εφαρμογής του οργανισμού. Η πολιτική θα πρέπει να προσδιορίζει τις απαιτήσεις και τα πρότυπα του σχετικού πληροφοριακού συστήματος.

Οι εργαζόμενοι είναι απαραίτητο να ενημερώνονται για τα καθήκοντα και τις ευθύνες τους, ώστε να διασφαλίζεται ότι οι κρίσιμες για την αποστολή λειτουργίες διατηρούνται ανά πάσα στιγμή. Οι εργαζόμενοι οφείλουν να γνωρίζουν ποιος είναι υπεύθυνος για τη συντήρηση εφεδρικών γεννητριών και πώς να τις χειρίζονται σε περίπτωση διακοπής ρεύματος. Ομοίως, το προσωπικό πρέπει να γνωρίζει ποιος είναι υπεύθυνος για την εκκένωση των χώρων και πώς να το κάνει με ασφάλεια σε περίπτωση πυρκαγιάς.

Αυτή η δήλωση πολιτικής θα διασφαλίσει ότι όλοι οι εργαζόμενοι κατανοούν την ευθύνη τους για τη διατήρηση της επιχειρηματικής συνέχειας σε περίπτωση σημαντικής διακοπής. Καθορίζοντας σαφώς τους ρόλους και τα καθήκοντα, οι επιχειρήσεις δύνανται να μειώσουν τον αντίκτυπο των καταστροφών και να συνεχίσουν τις δραστηριότητές τους.

Το δεύτερο βήμα αφορά την διεξαγωγή ανάλυσης επιχειρηματικού αντίκτυπου. Η μελέτη επιπτώσεων της επιχείρησης χρησιμοποιείται για τον προσδιορισμό των λειτουργικών διαταραχών και του χρόνου ανάκαμψης ενός οργανισμού. Αυτός ο τύπος

μελέτης είναι απαραίτητος, ώστε οι επιχειρήσεις να είναι προετοιμασμένες για μια ποικιλία σεναρίων, συμπεριλαμβανομένων των παραβιάσεων δεδομένων και των φυσικών καταστροφών.

Τέσσερα βήματα περιλαμβάνουν τη διαδικασία ανάλυσης επιχειρηματικών επιπτώσεων. Συγκεκριμένα τα βήματα αυτά είναι ο εντοπισμός διαταραχών, η διαπίστωση της επίδρασης των διακοπών στις λειτουργίες, η ποσοτικοποίηση του αντίκτυπου της διακοπής και η ανάπτυξη ενός σχεδίου για τον μετριασμό των επιπτώσεων της διακοπής. Ολοκληρώνοντας μια ανάλυση επιχειρηματικού αντίκτυπου, οι οργανισμοί είναι σε θέση να προετοιμαστούν καλύτερα για απρόβλεπτα γεγονότα και να περιορίσουν τις αρνητικές επιπτώσεις τους.

Το τρίτο βήμα είναι ο προσδιορισμός προληπτικών ελέγχων. Οι δραστηριότητες που εκτελούνται πρέπει να διασφαλίζουν ότι το σύστημα επιστρέφει στην κανονική λειτουργία όσο το δυνατόν γρηγορότερα, ενώ ταυτόχρονα συνεπάγονται ελάχιστες δαπάνες για το σχέδιο έκτακτης ανάγκης. Αυτή η φάση απαιτεί τη διασφάλιση ότι το κόστος των προληπτικών ελέγχων είναι ανάλογο με το κόστος μιας πιθανής διακοπής.

Το τέταρτο βήμα αφορά την δημιουργία στρατηγικών έκτακτης ανάγκης. Όπως γνωρίζουν όλοι όσοι έχουν αντιμετωπίσει απώλεια ρεύματος ή σφάλμα υπολογιστή, η συνέχεια των μέτρων λειτουργίας είναι απαραίτητη. Αυτές οι λύσεις οφείλουν να είναι άμεσα εκτελέσιμες με σκοπό να επιστρέψει το σύστημα στην κανονικότητα.

Έχοντας μια στρατηγική έκτακτης ανάγκης, είτε πρόκειται για ένα απλό εφεδρικό σχέδιο ενέργειας είτε για ένα πιο ολοκληρωμένο σχέδιο αποκατάστασης από καταστροφές, διασφαλίζει ότι ο οργανισμός μπορεί να συνεχίσει να λειτουργεί σε περίπτωση διακοπής ρεύματος ή άλλου απρόβλεπτου συμβάντος.

Προφανώς, όσο καλά προετοιμασμένος και είναι ένας οργανισμός, ο χρόνος διακοπής είναι πάντα μια πιθανότητα. Ωστόσο, εάν ο οργανισμός έχει εφαρμόσει στρατηγική για τη συνέχεια, μπορεί να ελαχιστοποιήσει το αντίκτυπο οποιουδήποτε χρόνου διακοπής λειτουργίας και να επαναφέρει την επιχείρησή σας σε λειτουργία το συντομότερο δυνατό.

Το πέμπτο βήμα αφορά την ανάπτυξη ενός σχεδίου έκτακτης ανάγκης για το πληροφοριακό σύστημα. Είναι ζωτικής σημασίας για τη συνέχιση των εργασιών και τη διαφύλαξη των δεδομένων σε περίπτωση απροσδόκητης διακοπής. Το αρχικό στάδιο είναι ο καθορισμός των συστημάτων που είναι απαραίτητα για τον οργανισμό. Η επιχείρηση πρέπει στη συνέχεια να υπολογίσει τον χρόνο που είναι δυνατόν να αντέξει

οικονομικά να μείνει χωρίς κάθε σύστημα. Αυτό θα βοηθήσει στον προσδιορισμό των συστημάτων τα οποία είναι αναγκαίο να είναι αρχικά λειτουργικά σε περίπτωση διακοπής.

Σε κάθε σύστημα είναι απαραίτητο στη συνέχεια να έχει αναπτυχθεί μια εφεδρική στρατηγική. Αυτό θα πρέπει να περιλαμβάνει αντίγραφα ασφαλείας επιτόπου και εκτός τοποθεσίας σε περίπτωση ολικής διακοπής ρεύματος ή φυσικής ζημιάς στην ιδιοκτησία. Τέλος, ο οργανισμός πρέπει να δοκιμάζει συχνά το σχέδιο για να διασφαλίσει ότι εξακολουθεί να είναι αποτελεσματικό και ότι όλοι γνωρίζουν τις ευθύνες τους σε περίπτωση έκτακτης ανάγκης.

Το έκτο βήμα αφορά την δοκιμή, εκπαίδευση και άσκηση του σχεδίου έκτακτης ανάγκης. Οποιοδήποτε σχέδιο επιχειρησιακής συνέχειας είναι τόσο αποτελεσματικό όσο το πρόγραμμα δοκιμών, εκπαίδευσης και άσκησης. Πολύ συχνά, οι οργανισμοί αναπτύσσουν σταθερά σχέδια συνέχειας, αλλά αποτυγχάνουν να αφιερώσουν τον απαραίτητο χρόνο και πόρους για τη δοκιμή και την άσκησή τους. Αυτό έχει ως συνέπεια, όταν συμβαίνει μια πραγματική καταστροφή, η στρατηγική συνέχειας σύντομα διαπιστώνεται ότι είναι ανεπαρκής. Προκειμένου να αποφευχθεί αυτή η περίσταση, οι επιχειρήσεις θα πρέπει συχνά να αξιολογούν τα σχέδια συνέχειας.

Αυτό είναι ζωτικής σημασίας να περιέχει τόσο δοκιμές μικρής κλίμακας που μπορούν να διεξαχθούν εσωτερικά όσο και ασκήσεις μεγάλης κλίμακας που απαιτούν τη συμμετοχή εξωτερικών εταίρων. Με τη δοκιμή και την άσκηση των σχεδίων συνέχειας, οι οργανισμοί είναι σε θέση να εξασφαλίσουν ότι είναι προετοιμασμένοι για κάθε ενδεχόμενο.

Το έβδομο βήμα αφορά την λήψη μέτρων συντήρησης του σχεδίου έκτακτης ανάγκης. Δεν υπάρχει τέτοιο πράγμα όπως ένα υπερβολικά διατηρημένο σχέδιο έκτακτης ανάγκης. Είτε ο οργανισμός είναι προετοιμασμένος για φυσική καταστροφή, διακοπή εργασιών ή οποιαδήποτε άλλη μορφή κρίσης, είναι σημαντικό τα σχέδια έκτακτης ανάγκης να είναι τρέχοντα και έτοιμα να εφαρμοστούν αμέσως.

3.1 Σχεδιασμός Και Ανάπτυξη Πλάνου Αντιμετώπισης Εκτάκτων Αναγκών Πληροφοριακών Συστημάτων

Σε αντίθεση με τα πρότυπα ISO, το πρότυπο 800-34 δίνει μεγάλη έμφαση στην ανθεκτικότητα και τον σχεδιασμό έκτακτης ανάγκης. Ο σχεδιασμός έκτακτης ανάγκης

του συστήματος πληροφοριών περιλαμβάνει ένα ευρύ φάσμα λειτουργιών που αποσκοπούν στη διατήρηση και αποκατάσταση βασικών λειτουργιών του συστήματος μετά από μια καταστροφή. Αντί να εστιάζει μόνο στον εντοπισμό και τον μετριασμό των απειλών, των τρωτών σημείων και των κινδύνων, το πρότυπο συμβουλεύει ότι οι κρατικές υπηρεσίες οφείλουν να αναπτύξουν ανθεκτική υποδομή που ελαχιστοποιεί τον αντίκτυπο των διακοπών σε υπηρεσίες ζωτικής σημασίας για την αποστολή. Θα πρέπει να καταβάλλονται συνεχείς προσπάθειες από τους οργανισμούς για να προσαρμοστούν στις αλλαγές και τις καταστάσεις που απειλούν την ικανότητά τους να συνεχίσουν τις βασικές τους λειτουργίες. Ο αποτελεσματικός σχεδιασμός έκτακτης ανάγκης ξεκινά με τη διαμόρφωση της πολιτικής σχεδιασμού έκτακτης ανάγκης ενός οργανισμού και τη μελέτη επιχειρηματικών επιπτώσεων κάθε πληροφοριακού συστήματος (BIA). Αυτό διευκολύνει την ιεράρχηση συστημάτων και διαδικασιών σύμφωνα με το επίπεδο επιπτώσεων FIPS 199. Το FIPS 199 παρέχει πρότυπα για την ανάλυση του αντίκτυπου των συστημάτων πληροφοριών και πληροφοριών σε οργανωτικές λειτουργίες και περιουσιακά στοιχεία, πρόσωπα, άλλους οργανισμούς και το έθνος εξετάζοντας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα ως στόχους ασφαλείας.

Ο σχεδιασμός στρατηγικών για τα πληροφοριακά συστήματα υψηλού αντίκτυπου υποχρεούται επίσης να ενσωματώνει επιλογές για υψηλή διαθεσιμότητα και πλεονασμό. Οι επιλογές περιλαμβάνουν εντελώς πλεονάζοντα (redundant) συστήματα εξισορρόπησης φορτίου σε άλλες τοποθεσίες, κατοπτρισμό δεδομένων και απομακρυσμένη αναπαραγωγή βάσεων δεδομένων. Αυτό όμως δεν σημαίνει ότι όλα τα κυβερνητικά πληροφοριακά συστήματα πρέπει να δημιουργηθούν με στόχο την επίτευξη υψηλής διαθεσιμότητας. Η διαθεσιμότητα των συστημάτων θα πρέπει να είναι ανάλογη της κρισιμότητας/σημαντικότητας του πληροφοριακού συστήματος. Αυτή η προσέγγιση μειώνει το κόστος, καθώς ο εξοπλισμός πληροφορικής υψηλής διαθεσιμότητας είναι συνήθως ακριβός. Λόγω της εγγενούς σχέσης μεταξύ ενός πληροφοριακού συστήματος και της αποστολής/επιχειρηματικής διαδικασίας που υποστηρίζει, αυτή η δημοσίευση συνιστά συντονισμό μεταξύ των σχεδίων κατά την ανάπτυξη και των ενημερώσεων προκειμένου να μειωθεί το κόστος. Αυτό θα διασφαλίσει ότι οι στρατηγικές ανάκαμψης και οι πόροι υποστήριξης δεν έρχονται σε αντίθεση μεταξύ τους ούτε διπλές προσπάθειες. Η δημοσίευση NIST 800-53 προσδιορίζει εννέα κανόνες ασφαλείας για τον σχεδιασμό έκτακτης ανάγκης σε συστήματα πληροφοριών. Όπως αναφέρθηκε προηγουμένως, η σημασία των

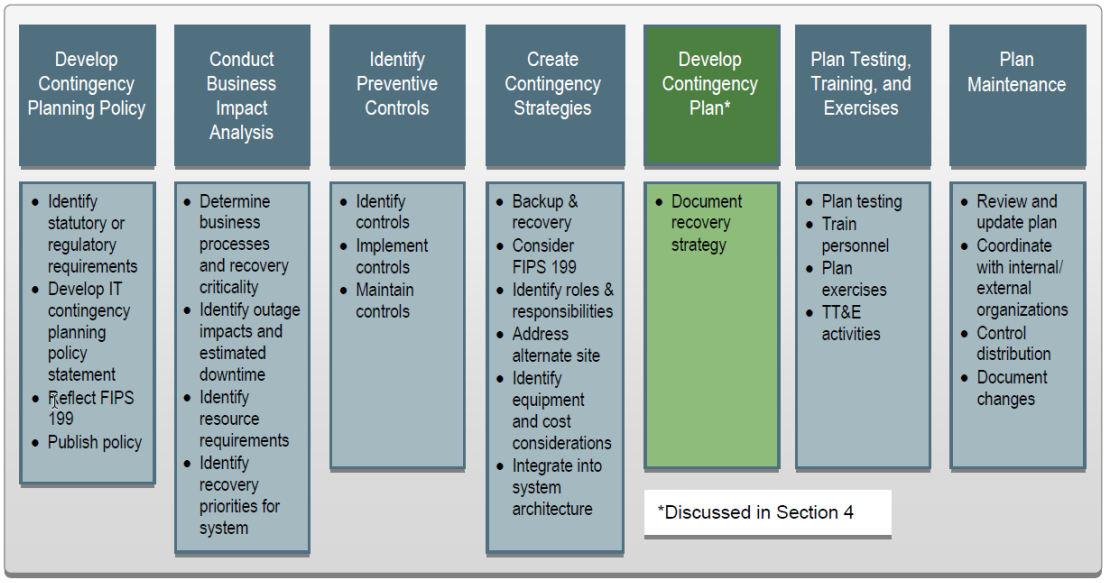
συστημάτων πληροφοριών υπαγορεύει τις βασικές γραμμές ελέγχου ασφαλείας. Η παρακάτω εικόνα/πίνακας απεικονίζει αυτά τα μέτρα ασφαλείας σχεδιασμού έκτακτης ανάγκης και τις αντίστοιχες βασικές απαιτήσεις τους.

Control No.	Control Name	Security Control Baselines		
		Low	Moderate	High
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2) (3)
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercise	CP-4	CP-4 (1)	CP-4 (1) (2) (4)
CP-5	Contingency Plan Update (Withdrawn)	------	-----	------
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3) (5)	CP-7 (1) (2) (3) (4) (5)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 (2) (3)	CP-10 (2) (3) (4)

Εικόνα 7 Σύνοψη του ελέγχου σχεδιασμού έκτακτης ανάγκης συστημάτων 53 χαμηλού, μέτριου και υψηλού αντίκτυπου του NIST SP 800-53

Στο πρότυπο παρέχεται μια διαδικασία επτά βημάτων για τη διαδικασία σχεδιασμού έκτακτης ανάγκης πληροφοριών για το σχεδιασμό και τη διαχείριση ενός αποτελεσματικού σχεδίου έκτακτης ανάγκης συστήματος πληροφοριών:

- Ανάπτυξη την πολιτικής σχεδιασμού έκτακτης ανάγκης
- Διεξαγωγή της ανάλυσης επιχειρηματικού αντίκτυπου (BIA)
- Προσδιορισμός προληπτικών ελέγχων
- Δημιουργία στρατηγικών έκτακτης ανάγκης
- Ανάπτυξη σχέδιού έκτακτης ανάγκης για το πληροφοριακό σύστημα
- Εξασφάλιση δοκίμων, εκπαίδευσης και ασκήσεων του σχεδίου
- Εξασφάλιση της συντήρησης του σχεδίου



Εικόνα 8 Διαδικασία σχεδιασμού πλάνου έκτακτης ανάγκης

Αυτή η δημοσίευση, όπως και τα πρότυπα ISO, υπογραμμίζει τη σημασία της κατανόησης των απαιτήσεων σχεδιασμού έκτακτης ανάγκης του οργανισμού από το προσωπικό. Για να επιτευχθεί αυτός ο στόχος, το σχέδιο έκτακτης ανάγκης είναι σημαντικό να βασίζεται σε μια καλά καθορισμένη πολιτική, να έχει καταγεγραμμένο το οργανωτικό πλαίσιο και τις ευθύνες για τον προγραμματισμό έκτακτης ανάγκης του συστήματος και να περιγράφει τους συνολικούς στόχους έκτακτης ανάγκης του οργανισμού. Οι ενέργειες έκτακτης ανάγκης του συστήματος πληροφοριών πρέπει να συμβαδίζουν με τις απαιτήσεις του προγράμματος για την ασφάλεια του συστήματος πληροφοριών, τη φυσική ασφάλεια, τους ανθρώπινους πόρους, τις λειτουργίες του συστήματος και τις λειτουργίες ετοιμότητας και ανάκτησης σε περίπτωση καταστροφών. Για να ενημερωθεί για νέες ή αναδυόμενες πολιτικές, πρωτοβουλίες ή δυνατότητες, το προσωπικό οφείλει να συνεργάζεται με εκπροσώπους από κάθε τομέα.

Η επακόλουθη φάση στη διαδικασία του σχεδιασμού έκτακτης ανάγκης είναι η διενέργεια μελέτης επιχειρηματικών επιπτώσεων (BIA). Το BIA είναι ένα κρίσιμο βήμα για την εφαρμογή των ελέγχων CP που περιγράφονται στο NIST SP 800-53 και στην ευρύτερη διαδικασία σχεδιασμού έκτακτης ανάγκης. Το BIA επιτρέπει στον συντονιστή των σχεδίων έκτακτης ανάγκης του συστήματος πληροφοριών να χαρακτηρίζει τα στοιχεία του συστήματος, τις υποστηριζόμενες διαδικασίες αποστολής/επιχειρήσεων και τις αλληλεξαρτήσεις. Κατά τη διάρκεια της φάσης

έναρξης του κύκλου ζωής ανάπτυξης (System Development Life Cycle SDLC) του συστήματος, θα πρέπει να διεξάγεται BIA . Συνήθως, αποτελείται από τρία βήματα.

Το πρώτο στάδιο είναι ο προσδιορισμός της σημασίας των επιχειρησιακών διαδικασιών και της ανάκαμψης. Μέσω αυτού του βήματος εντοπίζονται οι επιχειρηματικές λειτουργίες που υποστηρίζονται από το σύστημα και υπολογίζεται ο αντίκτυπος μιας διακοπής στην λειτουργία του συστήματος σε αυτές τις διαδικασίες, καθώς και ο προβλεπόμενος χρόνος διακοπής λειτουργίας. Κατά τη διάρκεια αυτής της διαδικασίας, ο οργανισμός είναι υποχρεωμένος να καθορίσει το μέγιστο χρονικό διάστημα που μπορεί να αντέξει χωρίς να διακυβεύσει τον στόχο του.

Το δεύτερο βήμα περιλαμβάνει τον προσδιορισμό των αναγκών σε πόρους. Μέσω αυτής της διαδικασίας αξιολογούνται οι πόροι που απαιτούνται για την επανέναρξη των διαδικασιών του οργανισμού καθώς και οι αλληλεξαρτήσεις τους.

Το τρίτο στάδιο εμπεριέχει τον προσδιορισμό των προτεραιοτήτων ανάκτησης για τους πόρους του συστήματος και τη σύνδεσή τους με βασικές επιχειρηματικές δραστηριότητες και λειτουργίες. Είναι δυνατό να τεθούν αποτελεσματικές προτεραιότητες ανάκτησης λαμβάνοντας υπόψη την κρισιμότητα της επιχειρηματικής διαδικασίας, τις επιπτώσεις διακοπών, τον αποδεκτό χρόνο διακοπής λειτουργίας και τους πόρους του συστήματος. Το αποτέλεσμα είναι μια ιεραρχική δομή προτεραιότητας ανάκτησης για το πληροφοριακό σύστημα.

Ο συντονιστής των σχεδίων έκτακτης ανάγκης πληροφοριακών συστημάτων είναι απαραίτητο να συνεργάζεται με τη διοίκηση και τα εσωτερικά και εξωτερικά σημεία επαφής για τον εντοπισμό και την επικύρωση των αποστολών/επιχειρηματικών λειτουργιών και διαδικασιών που εξαρτώνται ή υποστηρίζουν το πληροφοριακό σύστημα, με αποτέλεσμα την καλύτερη κατανόηση του BIA. Στη συνέχεια, ο συντονιστής των σχεδίων έκτακτης ανάγκης του πληροφοριακού συστήματος οφείλει να συνεχίσει να αναλύει με τη διοίκηση τον επιτρεπόμενο χρόνο διακοπής λειτουργίας των επιχειρηματικών διαδικασιών του οργανισμού. Υπάρχουν τρεις διαφορετικοί τρόποι για να οριστεί ο χρόνος διακοπής λειτουργίας. Ο συνολικός χρόνος που είναι διατεθειμένος να δεχτεί ο κάτοχος του συστήματος/εξουσιοδοτημένος υπάλληλος για διακοπή ή διακοπή της αποστολής/επιχειρηματικής διαδικασίας, συμπεριλαμβανομένων όλων των παραμέτρων του αντίκτυπου, είναι ο μέγιστος χρόνος που ένας πόρος συστήματος μπορεί να παραμείνει μη διαθέσιμος πριν υπάρξει καταστροφικός αντίκτυπος σε άλλο σύστημα πόρων και υποστηριζόμενες επιχειρηματικές διαδικασίες, καθώς και το σημείο, πριν από μια διακοπή του

συστήματος, στο οποίο μπορούν να ανακτηθούν δεδομένα αποστολής/επιχειρηματικής διαδικασίας (δεδομένων των πιο ευνοϊκών συνθηκών). Ο μέγιστος αποδεκτός χρόνος διακοπής λειτουργίας, ο στόχος χρόνου ανάκτησης και ο στόχος σημείου ανάκτησης είναι τα ονόματά των αντίστοιχων τεχνικών τους. Σε αυτή την προσέγγιση, θα πρέπει να εξεταστεί το κόστος των απαιτούμενων πόρων για την ανάκτηση του συστήματος και τη γενική του υποστήριξη, καθώς και των απωλειών του οργανισμού τη στιγμή που μια διαδικασία ή λειτουργία δεν λειτουργεί. Όταν απεικονίζονται τα σημεία ισοζυγίου κόστους, είναι δυνατόν να προσδιοριστεί το καλύτερο σημείο μεταξύ του κόστους διακοπής και ανάκτησης. Αυτό είναι πρωτεύον να λαμβάνεται υπόψη κατά την ανάπτυξη ενός σχεδίου έκτακτης ανάγκης.

Οι μέθοδοι δημιουργίας αντιγράφων ασφαλείας και ανάκτησης αποτελούν παράδειγμα των προαναφερθέντων. Οι μέθοδοι και οι τακτικές για τη δημιουργία αντιγράφων ασφαλείας και την ανάκτηση είναι ένας τρόπος για την επαναφορά των λειτουργιών του συστήματος γρήγορα και αποτελεσματικά μετά από μια διακοπή της υπηρεσίας. Κατά τη φάση ανάπτυξης/απόκτησης του κύκλου ζωής ανάπτυξης του συστήματος, οι μεθοδολογίες και οι τακτικές θα πρέπει να ενσωματωθούν στην αρχιτεκτονική του συστήματος για την αντιμετώπιση των επιπτώσεων διακοπής και των επιτρεπόμενων χρόνων διακοπής λειτουργίας που ορίζονται στην BIA. Για τα δεδομένα συστήματος είναι σημαντικό να δημιουργούνται συχνά αντίγραφα ασφαλείας. Οι πολιτικές θα πρέπει να καθορίζουν την ελάχιστη συχνότητα και το εύρος των αντιγράφων ασφαλείας (π.χ. ημερήσια ή εβδομαδιαία, incremental ή full) με βάση τη σημασία των δεδομένων και τον ρυθμό με τον οποίο προστίθενται νέα δεδομένα. Η μέθοδος που επιλέγεται για τη δημιουργία αντιγράφων ασφαλείας είναι αναγκαίο να βασίζεται στις απαιτήσεις διαθεσιμότητας και ακεραιότητας του συστήματος και των δεδομένων. Ανάλογα με την κρισιμότητα και τον αντίκτυπο των συστημάτων, ορισμένα εφεδρικά σχέδια θα πρέπει να περιλαμβάνουν μια στρατηγική ανάκτησης και εκτέλεσης λειτουργιών συστήματος για μεγάλο χρονικό διάστημα σε μια εναλλακτική εγκατάσταση. Αυτές οι πρόσθετες τοποθεσίες μπορεί να είναι cold sites, warm sites ή hot sites. Τα cold sites είναι συνήθως εγκαταστάσεις με επαρκή χώρο και υποδομή για την υποστήριξη δραστηριοτήτων ανάκτησης συστημάτων πληροφοριών. Τα hot sites είναι μερικώς εξοπλισμένοι χώροι γραφείων που περιέχουν μέρος ή όλο το υλικό, το λογισμικό, τις τηλεπικοινωνίες και τις πηγές ενέργειας του συστήματος. Το κόστος είναι πιθανό να ποικίλλει σημαντικά με βάση την ανάπτυξη της εφεδρικής λύσης που αποφασίζει να εφαρμόσει η εταιρεία. Ορισμένες λύσεις (hot sites) μπορεί να εγγυώνται

σχεδόν εκατό τοις εκατό χρόνο λειτουργίας, αλλά είναι σημαντικά πιο ακριβές από άλλες (π.χ. δημιουργία αντιγράφων ασφαλείας σε tape) όπου τα συστήματα απαιτούν χρόνο για να λειτουργήσουν ξανά.

Η αντικατάσταση εξοπλισμού είναι μια άλλη λειτουργία που είναι δυνατό να αυξήσει το κόστος μιας προσέγγισης εφεδρικής και εναλλακτικής τοποθεσίας. Εάν το σύστημα πληροφοριών έχει καταστραφεί ή εάν το cold site δεν είναι προσβάσιμο, το κατάλληλο υλικό και λογισμικό πρέπει να ενεργοποιηθεί ή να προμηθευτεί και να μεταφερθεί στην εναλλακτική τοποθεσία το συντομότερο δυνατό. Επομένως, μπορούν να δημιουργηθούν SLA (Service Level Agreement) με προμηθευτές υλικού, λογισμικού και υποστήριξης για υπηρεσίες συντήρησης έκτακτης ανάγκης. Διαφορετικά, ο βασικός εξοπλισμός είναι δυνατό να αγοραστεί εκ των προτέρων και να αποθηκευτεί σε μια ασφαλή τοποθεσία εκτός του εργοταξίου ή ο οργανισμός μπορεί να χρησιμοποιήσει εξοπλισμό που στεγάζεται και χρησιμοποιείται επί του παρόντος από το συμβεβλημένο hot site ή άλλο οργανισμό εντός του οργανισμού. Κατά την επανεξέταση των επιλογών, ο συντονιστής των σχεδίων έκτακτης ανάγκης του συστήματος πληροφοριών είναι υποχρεωμένος να σημειώσει ότι η απόκτηση εξοπλισμού, όπως απαιτείται, είναι οικονομικά αποδοτική και μπορεί να μειώσει τον χρόνο διακοπής λειτουργίας, αλλά ότι η αναμονή για αποστολή και εγκατάσταση μπορεί να προσθέσει σημαντικό γενικό χρόνο στη διαδικασία ανάκτησης.

Μετά την επιλογή και την εφαρμογή σχεδίων δημιουργίας αντιγράφων ασφαλείας και ανάκτησης συστήματος, ο συντονιστής των σχεδίων έκτακτης ανάγκης του συστήματος πληροφοριών οφείλει να ορίσει σχετικές ομάδες για την υλοποίηση της στρατηγικής. Κάθε ομάδα θα πρέπει να εκπαιδεύεται και να προετοιμάζεται να ανταποκριθεί σε περίπτωση ανατρεπτικού σεναρίου που απαιτεί ενεργοποίηση σχεδίου. Τα άτομα ανάκτησης είναι υποχρεωτικό να σταλούν σε μία από τις πολλές εξειδικευμένες ομάδες που θα ανταποκριθούν στο συμβάν, θα ανακτήσουν τις δυνατότητες και θα επαναφέρουν το σύστημα στην κανονική του κατάσταση. Για να επιτευχθεί αυτό, τα μέλη της ομάδας αποκατάστασης πρέπει να έχουν πλήρη κατανόηση του στόχου της προσπάθειας αποκατάστασης της ομάδας, των επιμέρους διαδικασιών που θα εκτελέσει η ομάδα και των αλληλεξαρτήσεων που μπορεί να υπάρχουν μεταξύ των ομάδων αποκατάστασης όσον αφορά τις συνολικές στρατηγικές. Το προσωπικό κάθε ομάδας είναι ωφέλιμο να επιλέγεται με βάση τις γνώσεις και τα ταλέντα του. Στην ιδανική περίπτωση οι ομάδες θα ήταν καλό να αποτελούνται από άτομα τα οποία, υπό κανονικές συνθήκες, είναι υπεύθυνα για τα ίδια ή παρόμοια

καθήκοντα. Οι διαχειριστές διακομιστή είναι αναγκαίο να περιλαμβάνονται ως μέλη της ομάδας ανάκτησης διακομιστή. Κάθε ομάδα καθοδηγείται από έναν αρχηγό ομάδας που ηγείται των γενικών λειτουργιών της ομάδας, ενεργεί ως εκπρόσωπος της ομάδας στη διοίκηση και διατηρεί επικοινωνία με άλλους ηγέτες της ομάδας. Ο αρχηγός της ομάδας κοινοποιεί πληροφορίες στα μέλη της ομάδας και εγκρίνει τυχόν επιλογές που είναι απαραίτητες να ληφθούν εντός της ομάδας. Οι ηγέτες μιας ομάδας θα πρέπει να ορίσουν έναν εκπρόσωπο που θα αναλάβει ηγετικές ευθύνες σε περίπτωση απουσίας του αρχηγού. Επιπλέον, απαιτείται μια ομάδα διαχείρισης για την πλειονότητα των συστημάτων προκειμένου να παρέχει γενική κατεύθυνση μετά από μεγάλη διακοπή λειτουργίας συστήματος ή έκτακτη ανάγκη. Ένα ανώτερο στέλεχος της διοίκησης, όπως ο Chief Information Officer (CIO), έχει την τελική ικανότητα να ενεργοποιήσει τη στρατηγική και να κάνει επιλογές σχετικά με τα επίπεδα προϋπολογισμού, τον αποδεκτό κίνδυνο και το συντονισμό μεταξύ των υπηρεσιών.

Ένας συντονιστής των σχεδίων έκτακτης ανάγκης συστημάτων πληροφοριών είναι απαραίτητο να διατηρείται κατάσταση ετοιμότητας, η οποία περιλαμβάνει εκπαίδευση του προσωπικού για την εκπλήρωση των ρόλων και των ευθυνών του στο πλαίσιο του σχεδίου, την άσκηση σχεδίων για την επικύρωση του περιεχομένου τους και τη δοκιμή συστημάτων και στοιχείων του συστήματος για τη διασφάλιση της λειτουργικότητάς τους στο περιβάλλον που καθορίζεται στο τα σχέδια έκτακτης ανάγκης του πληροφοριακού συστήματος. Περιοδικά, μετά από οργανωτικές αλλαγές ή αλλαγές στο σύστημα, τη δημοσίευση νέων οδηγιών δοκιμών, εκπαίδευσης και άσκησης ή, όπως απαιτείται άλλως, οι οργανισμοί θα πρέπει να διεξάγουν και να τεκμηριώνουν εκδηλώσεις δοκιμών, εκπαίδευσης και άσκησης (test, training, and exercise TT&E). Η εκτέλεση των εκδηλώσεων TT&E βοηθά τους οργανισμούς να προσδιορίσουν την αποτελεσματικότητα του σχεδίου και διασφαλίζει ότι όλοι οι άνθρωποι γνωρίζουν τις ευθύνες τους στην εφαρμογή κάθε σχεδίου συστήματος πληροφοριών. Ένα πρόγραμμα TT&E παρέχει μια δομή για τον εντοπισμό, τον προγραμματισμό και τον καθορισμό στόχων για τις λειτουργίες TT&E. Όλες οι δοκιμές και οι ασκήσεις είναι σημαντικό να περιλαμβάνουν αξιολόγηση των επιπτώσεων στις λειτουργίες του οργανισμού και μια διαδικασία ενημέρωσης και βελτίωσης του σχεδίου ως αποτέλεσμα.

Μια tabletop άσκηση με συχνότητα που καθορίζεται από τον οργανισμό είναι αρκετή για συστήματα χαμηλής πρόσκρουσης. Οι επιτραπέζιες ασκήσεις είναι ασκήσεις που βασίζονται σε συζήτηση στις οποίες τα άτομα συγκεντρώνονται σε μια

τάξη ή σε μικρές ομάδες για να εξερευνήσουν τους ρόλους τους κατά τη διάρκεια μιας έκτακτης ανάγκης και τις απαντήσεις τους σε μια συγκεκριμένη κατάσταση έκτακτης ανάγκης.

Σε συχνότητα που καθορίζεται από τον οργανισμό, θα πρέπει να εκτελείται λειτουργική άσκηση σε συστήματα μέτριας σημαντικότητας. Εκτελώντας τα καθήκοντά τους σε ένα προσομοιωμένο επιχειρησιακό περιβάλλον, το προσωπικό είναι σε θέση να επιδείξει την επιχειρησιακή του ετοιμότητα για καταστάσεις έκτακτης ανάγκης κατά τη διάρκεια λειτουργικών ασκήσεων.

Μια λειτουργική άσκηση πλήρους κλίμακας είναι ωφέλιμο να πραγματοποιείται με συχνότητα που καθορίζεται από τον οργανισμό για συστήματα με σημαντικό αντίκτυπο. Η άσκηση λειτουργίας πλήρους κλίμακας πρέπει να ενσωματώνει ένα σύστημα failover στο hot site.

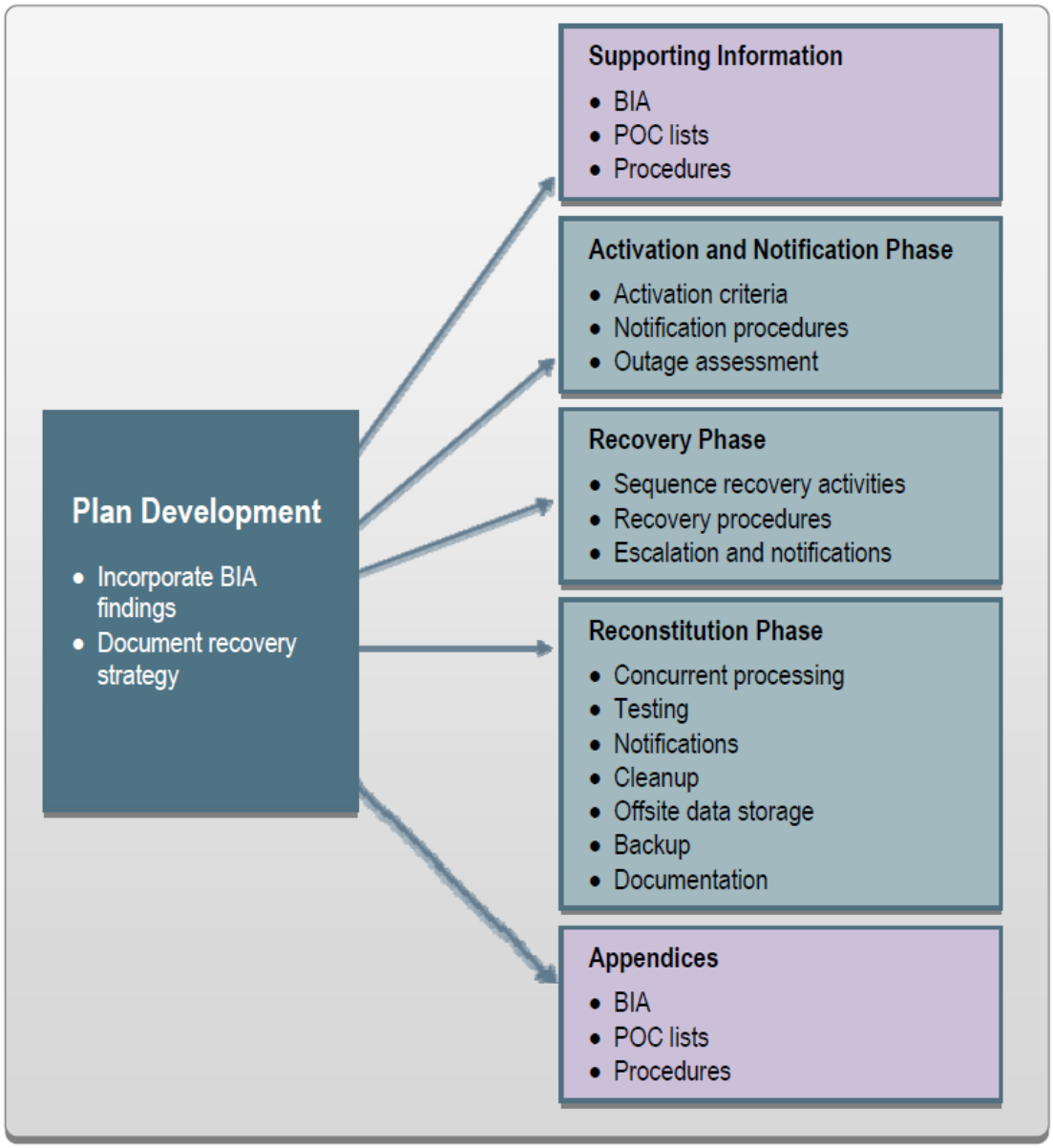
Τα σχέδια έκτακτης ανάγκης για δοκιμές συστημάτων πληροφοριών αποτελούν βασικό συστατικό μιας αποτελεσματικής ικανότητας έκτακτης ανάγκης. Επικυρώνοντας ένα ή περισσότερα στοιχεία του συστήματος και τη λειτουργικότητα του σχεδίου, ο έλεγχος επιτρέπει τον εντοπισμό και την αποκατάσταση των ελλείψεων του σχεδίου. Οι δοκιμές είναι δυνατό να λάβουν ποικίλα σχήματα και να επιτύχουν διάφορους στόχους, αλλά θα πρέπει πάντα να εκτελούνται σε ένα περιβάλλον που είναι όσο το δυνατόν παρόμοιο με ένα περιβάλλον παραγωγής. Κάθε στοιχείο ενός συστήματος πληροφοριών θα πρέπει να αξιολογείται για να επικυρώνεται η ακρίβεια των χωριστών λειτουργιών ανάκτησης. Σε μια δοκιμή ενός σχεδίου έκτακτης ανάγκης, κατά περίπτωση, θα πρέπει να καλύπτονται οι ακόλουθοι τομείς:

- Διαδικασίες ειδοποίησης.
- Ανάκτηση συστήματος σε εναλλακτική πλατφόρμα μέσω εφεδρικών μέσων.
- Εσωτερική και εξωτερική συνδεσιμότητα.
- Απόδοση συστήματος με χρήση εναλλακτικού εξοπλισμού.
- Αποκατάσταση κανονικών λειτουργιών.

Για να είναι ένα σχέδιο χρήσιμο με οποιονδήποτε τρόπο, είναι επιτακτική ανάγκη να διατηρείται σε κατάσταση ετοιμότητας που να αντιπροσωπεύει κατάλληλα τις ανάγκες του συστήματος, τις διαδικασίες, την οργανωτική δομή και τις πολιτικές. Κατά τη φάση λειτουργίας/συντήρησης του κύκλου ζωής ανάπτυξης του συστήματος, τα πληροφοριακά συστήματα υφίστανται συχνές αλλαγές ως αποτέλεσμα των κυμαινόμενων επιχειρηματικών απαιτήσεων, των τεχνολογικών εξελίξεων και των

νέων εσωτερικών και εξωτερικών πολιτικών. Άρα, είναι σημαντικό τα σχέδια έκτακτης ανάγκης του συστήματος πληροφοριών να επανεξετάζονται και να ενημερώνονται σε τακτική βάση ως μέρος της διαδικασίας διαχείρισης αλλαγών του οργανισμού, ώστε να διασφαλίζεται ότι οι νέες πληροφορίες τεκμηριώνονται και τα απαιτούμενα μέτρα έκτακτης ανάγκης τροποποιούνται όπως απαιτείται.

Όταν πρόκειται για τη διαδικασία δημιουργίας ενός ολοκληρωμένου προγράμματος σχεδιασμού έκτακτης ανάγκης, ένα από τα πιο σημαντικά βήματα είναι η ολοκλήρωση της κατασκευής του εφεδρικού σχεδίου του συστήματος πληροφοριών. Μετά από μια διακοπή σε ένα σύστημα πληροφοριών, το σχέδιο περιγράφει με μεγάλη λεπτομέρεια τους ρόλους, τις ευθύνες, τις ομάδες και τις διαδικασίες που σχετίζονται με την επαναφορά του συστήματος στο διαδίκτυο. Η τεκμηρίωση των τεχνολογικών δυνατοτήτων που έχουν δημιουργηθεί για την υποστήριξη λειτουργιών έκτακτης ανάγκης είναι σημαντικό μέρος του σχεδίου έκτακτης ανάγκης του πληροφοριακού συστήματος, το οποίο επιβάλλεται επίσης να προσαρμοστεί στην εταιρεία και τις απαιτήσεις που έχει. Αυτό το άρθρο παραθέτει πέντε κύρια στοιχεία που συνθέτουν το σχέδιο έκτακτης ανάγκης, όπως φαίνεται στο σχήμα που ακολουθεί. Το συμπληρωματικό υλικό και τα παραρτήματα του σχεδίου περιέχουν επίσης σημαντικές πληροφορίες που είναι απαραίτητες για την ανάπτυξη μιας εμπεριστατωμένης στρατηγικής. Μετά από διακοπή του συστήματος ή έκτακτη ανάγκη, ο οργανισμός πρέπει να εκτελέσει μια σειρά από συγκεκριμένες δραστηριότητες, οι οποίες αντιμετωπίζονται σε όλες τις φάσεις ενεργοποίησης και ειδοποίησης, ανάκτησης και ανασύστασης.



Εικόνα 9 Δομή Σχεδίου Έκτακτης Ανάγκης

Μια εισαγωγή και μια ενότητα σχετικά με την ιδέα των λειτουργιών περιλαμβάνονται στην ενότητα του υποστηρικτικού υλικού. Αυτές οι ενότητες παρέχουν ζωτικής σημασίας πληροφορίες για το υπόβαθρο που διευκολύνουν την κατανόηση, την εφαρμογή και τη διατήρηση του σχεδίου έκτακτης ανάγκης. Αυτές οι ιδιαιτερότητες βοηθούν στην κατανόηση του βαθμού εφαρμογής των συστάσεων, στον προσδιορισμό του καλύτερου τρόπου υλοποίησης του σχεδίου και στην απόκτηση γνώσεων σχετικά με τη διαθεσιμότητα των σχετικών σχεδίων και πληροφοριών που δεν εμπίπτουν στο πεδίο εφαρμογής του σχεδίου. Στην ενότητα με τίτλο "Έννοια των Λειτουργιών", θα βρείτε πρόσθετες πληροφορίες σχετικά με το πληροφοριακό σύστημα, περιγραφή των ρόλων και των ευθυνών που εμπλέκονται στο σχέδιο

έκτακτης ανάγκης του πληροφοριακού συστήματος, καθώς και τις τρεις φάσεις του σχεδίου έκτακτης ανάγκης (Ενεργοποίηση και ειδοποίηση, Ανάκτηση και Ανασύσταση). Αυτή η ενότητα είναι πιθανό να περιλαμβάνει τα στοιχεία της περιγραφής του συστήματος, μια επισκόπηση των τριών φάσεων (ενεργοποίηση και ειδοποίηση, ανάκτηση και ανακατασκευή) και ανάλυση των ρόλων και των ευθυνών της συνολικής δομής των ομάδων έκτακτης ανάγκης, συμπεριλαμβανομένης της ιεραρχίας και της συντονιστικών μηχανισμών και απαιτήσεων μεταξύ των ομάδων.

Η φάση ενεργοποίησης και ειδοποίησης είναι αυτή που περιγράφει τις αρχικές δραστηριότητες που πραγματοποιήθηκαν, αφού διαπιστωθεί ότι η επικείμενη διακοπή ή διακοπή του συστήματος έχει ανακαλυφθεί. Σε περίπτωση που ικανοποιούνται μία ή περισσότερες από τις απαιτήσεις ενεργοποίησης του πληροφοριακού συστήματος, επιβάλλεται να τεθεί σε εφαρμογή το εφεδρικό σχέδιο του συστήματος πληροφοριών. Εάν πληρούνται ένα από τα κριτήρια ενεργοποίησης, η ορισθείσα αρχή οφείλει να θέσει σε εφαρμογή το σχέδιο. Είναι πιθανό να υπάρξει διακοπή ή διακοπή ανά πάσα στιγμή, με ή χωρίς προηγούμενη ειδοποίηση. Για παράδειγμα, η προηγούμενη προειδοποίηση παρέχεται συνήθως όταν αναμένεται ότι ένας τυφώνας θα επηρεάσει μια συγκεκριμένη περιοχή ή όταν ένας ιός υπολογιστή θα είναι παρών σε μια συγκεκριμένη ημερομηνία. Από την άλλη πλευρά, ενδέχεται να μην υπάρχει ένδειξη ότι η συσκευή απέτυχε ή ότι διαπράχθηκε έγκλημα. Και τα δύο είδη σεναρίων θα πρέπει να έχουν στις αντίστοιχες μεθόδους ειδοποίησης λεπτομερώς καθορισμένες στη στρατηγική. Οι ειδοποιήσεις είναι δυνατό να αποστέλλονται από διάφορα κανάλια, όπως το τηλέφωνο, το ηλεκτρονικό ταχυδρομείο (email), το κινητό τηλέφωνο και η ανταλλαγή μηνυμάτων κειμένου. Υπάρχει η δυνατότητα αυτά τα κανάλια να προγραμματιστούν να στέλνουν ειδοποιήσεις αυτόματα ή μη αυτόματα. Τα συστήματα ειδοποιήσεων που είναι αυτοματοποιημένα συμμορφώνονται με προκαθορισμένους κανόνες και κριτήρια και συχνά προσφέρουν γρήγορο έλεγχο ταυτότητας και έγκριση, εκτός από ασφαλείς επικοινωνίες. Μετά τη διακοπή, θα πρέπει να εκδοθεί ειδοποίηση στην ομάδα αξιολόγησης διακοπών, ώστε να αξιολογήσει την τρέχουσα κατάσταση και να αποφασίσει για τα επόμενα βήματα που πρέπει να γίνουν. Είναι ανάγκη επίσης να εκδίδονται ειδοποιήσεις σε σημεία επαφής εξωτερικών οργανισμών ή συνεργατών διασυνδεδεμένων συστημάτων που ενδέχεται να επηρεαστούν αρνητικά εάν δεν είναι ενημερωμένοι για την κατάσταση. Εάν δεν γνωρίζουν την κατάσταση, δεν θα μπορούν να λάβουν τα κατάλληλα μέτρα. Τα αυτοματοποιημένα συστήματα ειδοποιήσεων χρειάζονται μια αρχική επένδυση και μια καμπύλη εκμάθησης, αλλά θα μπορούσαν να

είναι μια αποτελεσματική μέθοδος για ορισμένες εταιρείες, ώστε να διασφαλίζουν την έγκαιρη και ακριβή παράδοση των μηνυμάτων τους. Αντίθετα, οι ειδοποιήσεις που εκδίδονται μέσω email οφείλουν να γίνονται με εξαιρετική προσοχή, επειδή δεν υπάρχει τρόπος να διασφαλιστεί η λήψη ή η επιβεβαίωση του μηνύματος. Είναι ζωτικής σημασίας να αξιολογηθεί τόσο το είδος όσο και η έκταση της διακοπής με σκοπό να καθοριστεί πως θα λειτουργήσει το εφεδρικό σχέδιο για το σύστημα πληροφοριών σε περίπτωση που το σύστημα καταστεί ανενεργό. Η αξιολόγηση της διακοπής θα πρέπει να ολοκληρωθεί όσο πιο γρήγορα το επιτρέπουν οι τρέχουσες συνθήκες, με τη συνεχή προστασία των ανθρώπων να αποτελεί κορυφαία προτεραιότητα σε όλη τη διάρκεια.

Μετά την εφαρμογή του σχεδίου έκτακτης ανάγκης του συστήματος πληροφοριών, έχουν ολοκληρωθεί οι αξιολογήσεις διακοπών (εάν είναι εφικτό), έχει ειδοποιηθεί το προσωπικό και έχουν κινητοποιηθεί κατάλληλες ομάδες, μπορούν να ξεκινήσουν επίσημες δραστηριότητες αποκατάστασης. Οι ενέργειες που λαμβάνουν χώρα κατά τη διάρκεια της Φάσης Ανάκτησης επικεντρώνονται στην εφαρμογή μεθόδων ανάκτησης με στόχο την αποκατάσταση των δυνατοτήτων του συστήματος, την αποκατάσταση ζημιών και την επανεκκίνηση των λειτουργικών δυνατοτήτων είτε στην αρχική τοποθεσία είτε σε νέα εναλλακτική τοποθεσία. Το σχέδιο έκτακτης ανάγκης του συστήματος πληροφοριών πρέπει να παρέχει οδηγίες βήμα προς βήμα για την επαναφορά του συστήματος πληροφοριών ή των στοιχείων του σε αναγνωρισμένη κατάσταση, ώστε να μπορεί να κάνει τις λειτουργίες της φάσης ανάκτησης πιο ομαλά. Η ενσωμάτωση ενός στοιχείου κλιμάκωσης και ειδοποίησης στη φάση ανάκτησης βοηθά να διασφαλιστεί ότι λαμβανομένων υπόψη όλων των πραγμάτων, ακολουθείται μια διαδικασία ανάκτησης που είναι επαναχρησιμοποιήσιμη, δομημένη, συνεπής και μετρήσιμη. Όταν ολοκληρωθεί η φάση ανάκαμψης, το σύστημα πληροφοριών θα λειτουργεί πλήρως και θα είναι σε θέση να εκτελεί όλες τις λειτουργίες που περιγράφονται στο σχέδιο. Κατά την ανάκτηση ενός πολύπλοκου συστήματος, όπως ένα δίκτυο ευρείας περιοχής (WAN) ή ένα εικονικό τοπικό δίκτυο (VLAN) που περιλαμβάνει πολλά ανεξάρτητα στοιχεία, οι τεχνικές ανάκτησης πρέπει να αντικατοπτρίζουν τις προτεραιότητες του συστήματος που αναφέρονται στο BIA. Παραδείγματα τέτοιων πολύπλοκων συστημάτων περιλαμβάνουν την αποτροπή σημαντικών αρνητικών επιπτώσεων στα συνδεδεμένα συστήματα, τη σειρά με την οποία εκτελούνται οι λειτουργίες είναι σημαντικό να αντικατοπτρίζει τον μέγιστο χρόνο διακοπής του συστήματος.

Στην τρίτη και τελευταία φάση της υλοποίησης του σχεδίου έκτακτης ανάγκης του πληροφοριακού συστήματος, που είναι γνωστή ως φάση ανασύστασης, ορίζονται τα βήματα που διεξάγονται για τη δοκιμή και επιβεβαίωση της ικανότητας και της λειτουργικότητας του συστήματος. Κατά τη φάση της ανασύστασης, οι δραστηριότητες ανάκτησης ολοκληρώνονται και η κανονική λειτουργία του συστήματος επανέρχεται στο διαδίκτυο. Οι λειτουργίες που λαμβάνουν χώρα κατά τη διάρκεια αυτής της φάσης μπορούν επίσης να χρησιμοποιηθούν για την προετοιμασία μιας νέας μόνιμης τοποθεσίας για την υποστήριξη των απαιτήσεων επεξεργασίας του συστήματος σε περίπτωση που η πρώτη εγκατάσταση καταστραφεί χωρίς επισκευή. Η επικύρωση ότι η ανάκαμψη ήταν αποτελεσματική και η απενεργοποίηση του σχεδίου είναι οι δύο κύριες λειτουργίες που συνθέτουν αυτήν τη φάση. Η διαδικασία επαναφοράς του συστήματος στην κανονική του λειτουργία και ολοκλήρωσης των απαραίτητων διαδικασιών για την ανασύστασή του προκειμένου να είναι έτοιμο για μελλοντική διακοπή ή διακοπή αναφέρεται ως "απενεργοποίηση του σχεδίου". Αυτές οι δραστηριότητες συνίστανται για την ειδοποίηση των κατάλληλων μερών κατά την επιστροφή του συστήματος στην κανονική λειτουργία, τον καθαρισμό του χώρου εργασίας ή την αποσυναρμολόγηση τυχόν θέσεων προσωρινής ανάκτησης, την ανανέωση προμηθειών, την επιστροφή εγχειριδίων και άλλης τεκμηρίωσης στις τοποθεσίες από τις οποίες ελήφθησαν και την προετοιμασία του συστήματος για άλλη κατάσταση έκτακτης ανάγκης.

Τα παραρτήματα ενός σχεδίου έκτακτης ανάγκης εμπεριέχουν βασικές λεπτομέρειες που δεν περιλαμβάνονται στο κύριο σώμα του σχεδίου. Μερικά από τα παραρτήματα του σχεδίου έκτακτης ανάγκης περιέχουν λεπτομερείς διαδικασίες ανάκτησης και λίστες ελέγχου, λεπτομερείς διαδικασίες δοκιμών επικύρωσης και λίστες ελέγχου, λίστες απαιτήσεων εξοπλισμού και συστήματος του υλικού, λογισμικού και άλλων πόρων που απαιτούνται για την υποστήριξη λειτουργιών συστήματος, δοκιμές σχεδίου έκτακτης ανάγκης συστημάτων πληροφοριών και διαδικασίες συντήρησης και συμφωνίες επιπέδου υπηρεσιών προμηθευτή, αμοιβαίες συμφωνίες με άλλους οργανισμούς και άλλα ζωτικής σημασίας αρχεία. Αυτά τα παραρτήματα βρίσκονται στο σχέδιο έκτακτης ανάγκης του συστήματος πληροφοριών.

3.2 Επιλογή Πλάνου Αντιμετώπισης Εκτάκτων Αναγκών Πληροφοριακών Συστημάτων

Αυτό το κεφάλαιο έχει τη χρήση συμπληρώματος στη διαδικασία και τις συστάσεις πλαισίου που προσφέρθηκαν σε προηγούμενες ενότητες. Το κάνει αντιμετωπίζοντας τις τεχνικές πτυχές σχεδιασμού έκτακτης ανάγκης που είναι μοναδικές για συγκεκριμένα είδη συστημάτων πληροφοριών. Επειδή κάθε σύστημα είναι διαφορετικό, οι εκτιμήσεις που προσφέρονται είναι γραμμένες σε ένα επίπεδο που μπορεί να γίνει κατανοητό και να εφαρμοστεί από τους περισσότερους δυνατούς ανθρώπους. Η λίστα των πλατφορμώνν δεν περιέχει όλες τις διαθέσιμες επιλογές, αλλά είναι αντιπροσωπευτική των ειδών συστημάτων που χρησιμοποιούνται συνήθως στην παραγωγή ή την ανάπτυξη. Είναι πιθανό ότι μόνο ορισμένες από τις πληροφορίες που παρέχονται είναι σχετικές με το εν λόγω σύστημα πληροφοριών. Ο συντονιστής του σχεδίου έκτακτης ανάγκης για το πληροφοριακό σύστημα θα πρέπει να χρησιμοποιεί τις εκτιμήσεις, κι όταν είναι κατάλληλο και να τις τροποποιεί έτσι ώστε να ανταποκρίνονται στις ιδιαίτερες ανάγκες έκτακτης ανάγκης του συστήματος. Τα συστήματα πελάτη/διακομιστή, τα συστήματα τηλεπικοινωνιών και τα συστήματα mainframe [45] είναι οι αντιπροσωπευτικοί τύποι πλατφόρμας που συζητούνται σε αυτό το έγγραφο. Ανεξαρτήτως από την πλατφόρμα ή το είδος του συστήματος που χρησιμοποιείται, υπάρχουν μερικές διαφορετικές πτυχές που πρέπει να ληφθούν υπόψη κατά τη διαμόρφωση λύσεων για τεχνικά σχέδια έκτακτης ανάγκης. Οποιοδήποτε είδος προετοιμασίας για μια έκτακτη ανάγκη είναι αναγκαίο να ξεκινά με αυτούς τους παράγοντες, γιατί αποτελούν τη βάση για τη διαδικασία. Υπάρχουν πολλές από αυτές τις προληπτικές διαδικασίες που είναι τυπικές σε όλους τους τομείς για τα πληροφοριακά συστήματα. Τα ακόλουθα είναι μερικά παραδείγματα κοινών θεωρήσεων:

- Χρήση πληροφοριών που συλλέγονται από τη διαδικασία BIA.
- Ανάπτυξη πολιτικών και διαδικασιών ασφάλειας, ακεραιότητας και δημιουργίας αντιγράφων ασφαλείας δεδομένων.
- Προστασία του εξοπλισμού και των πόρων συστήματος.
- Τήρηση και συμμόρφωση με τους ελέγχους ασφαλείας του NIST SP 800-53.

- Ανάπτυξη πρωτογενών και εναλλακτικών τοποθεσιών με κατάλληλα μεγέθους και διαμορφωμένα συστήματα διαχείρισης ενέργειας και περιβαλλοντικούς ελέγχους.
- Χρήση διαδικασιών υψηλής διαθεσιμότητας (High Availability HA) για την παροχή διαδικτυακής πρόσβασης σε πραγματικό χρόνο σε εναλλακτικούς πόρους του συστήματος.

Στον προγραμματισμό έκτακτης ανάγκης, μία από τις πιο σημαντικές πτυχές είναι η διασφάλιση ότι τα δεδομένα και το λογισμικό στο σύστημα διατηρούνται ασφαλή και άθικτα. Η προστασία και η ενημέρωση δεδομένων στις κύριες συσκευές αποθήκευσης ενός συστήματος είναι ένα ουσιαστικό μέρος της διατήρησης της ακεραιότητας των δεδομένων του. Όπως συζητήθηκε στο κεφάλαιο 3.1, υπάρχουν περισσότεροι από ένας τρόποι για να διασφαλιστεί ότι τα δεδομένα που έχουν αποθηκευτεί δεν θα χάσουν την ακεραιότητά τους. Η προστασία των ευαίσθητων πληροφοριών απαιτεί να διατηρούνται ασφαλείς από μη εξουσιοδοτημένη πρόσβαση ή χρήση τόσο σε τοπικό όσο και σε απομακρυσμένο περιβάλλον.

Η κρυπτογράφηση είναι μια τυπική τεχνολογία που χρησιμοποιείται για την ασφάλεια των δεδομένων που διατηρούνται στα συστήματα. Όταν εφαρμόζεται τόσο στην κύρια συσκευή αποθήκευσης δεδομένων όσο και στο εφεδρικό μέσο που αποστέλλεται σε τοποθεσία εκτός έδρας, η κρυπτογράφηση λειτουργεί στο μέγιστο επίπεδο της αποτελεσματικότητάς της. Εάν επιλέξετε να κρυπτογραφήσετε τα δεδομένα σας πριν τα αποθηκεύσετε εκτός τοποθεσίας, είναι απαραίτητο να βεβαιωθείτε ότι υπάρχουν προγράμματα ανάγνωσης πολυμέσων στην εναλλακτική τοποθεσία του ιστότοπου, ώστε να μπορείτε να διαβάσετε σωστά τα κρυπτογραφημένα δεδομένα όταν προσπαθείτε να τα ανακτήσετε. Απαιτείται η καθιέρωση μιας αξιόπιστης στρατηγικής διαχείρισης κλειδιών προκειμένου να είναι προσβάσιμα τα κρυπτογραφημένα δεδομένα όποτε απαιτείται. Απαιτείται διαχείριση του υλικού κλειδώματος, που χρησιμοποιείται στη διαδικασία δημιουργίας και διατήρησης των κλειδιών, και κατά προτίμηση θα πρέπει να πραγματοποιείται σε κεντρικό χώρο εντός της επιχείρησης. Όταν τα αντίγραφα ασφαλείας των δεδομένων αποθηκεύονται σε μια ασφαλή περιοχή εκτός από την κύρια τοποθεσία, μπορεί να είναι γρήγορη και εύκολη η πρόσβαση σε αυτά σε περίπτωση έκτακτης ανάγκης. Μια αποτελεσματική μέθοδος δημιουργίας αντιγράφων ασφαλείας δεδομένων είναι απαραίτητη για τη συνολική στρατηγική ανάκτησης που πρέπει να αναπτυχθεί από έναν συντονιστή ενός σχεδίου

έκτακτης ανάγκης συστήματος πληροφοριών. Σε σταθερή βάση, είναι επιτακτική ανάγκη να γίνονται αντίγραφα ασφαλείας των δεδομένων που είναι αποθηκευμένα σε κάθε σύστημα. Η δημιουργία αντιγράφων ασφαλείας συστημάτων σε μεμονωμένους υπολογιστές ή σε μια κεντρική συσκευή αποθήκευσης, όπως ένα δίκτυο storage area network(SAN) ή network attached storage (NAS), είναι και οι δύο βιώσιμες επιλογές.

Μια εργασία δημιουργίας αντιγράφων ασφαλείας μπορεί να εκτελέσει ένα πλήρες αντίγραφο ασφαλείας όλων των αρχείων στο δίσκο ή στον φάκελο που έχει επιλεγεί για δημιουργία αντιγράφων ασφαλείας. ένα σταδιακό αντίγραφο ασφαλείας μόνο των αρχείων που έχουν δημιουργηθεί ή τροποποιηθεί από το προηγούμενο αντίγραφο ασφαλείας ή μπορεί να αποθηκεύσει μόνο αρχεία που έχουν δημιουργηθεί ή τροποποιηθεί μετά το πιο πρόσφατο πλήρες αντίγραφο ασφαλείας (differential backup). Είναι δυνατό να χρησιμοποιηθεί ένας συνδυασμός διεργασιών δημιουργίας αντιγράφων ασφαλείας, αλλά αυτό θα εξαρτηθεί από τη διαμόρφωση του συστήματος και τις απαιτήσεις για ανάκτηση. Κατά τη διαδικασία δημιουργίας της πολιτικής δημιουργίας αντιγράφων ασφαλείας Το πόσο σύντομα θα ανακτηθούν τα αντίγραφα ασφαλείας σε περίπτωση έκτακτης ανάγκης, πόσο καιρό θα διατηρηθούν τα εφεδρικά μέσα και ποιο είναι το σωστό μέσο δημιουργίας αντιγράφων ασφαλείας για τους τύπους των αντιγράφων ασφαλείας που πρέπει να πραγματοποιηθούν είναι όλα ερωτήματα που μπορεί να βοηθήσει στη δημιουργία της κατάλληλης πολιτικής δημιουργίας αντιγράφων ασφαλείας για τον οργανισμό. Εκτός από τη δημιουργία αντιγράφων ασφαλείας των δεδομένων τους, οι οργανισμοί θα πρέπει ακόμη να δημιουργούν αντίγραφα ασφαλείας των προγραμμάτων οδήγησης και του λογισμικού του συστήματος. Αποτελεί βέλτιστη πρακτική για τις εταιρείες το να διατηρούν το λογισμικό τους και τις άδειες χρήσης λογισμικού σε ξεχωριστό χώρο. Αυτό περιλαμβάνει τον αρχικό δίσκο εγκατάστασης, τους όρους και τις προϋποθέσεις της άδειας χρήσης και τυχόν κλειδιά άδειας χρήσης που μπορεί να είναι απαραίτητα.

Συνιστάται τα εφεδρικά μέσα να φυλάσσονται εκτός τοποθεσίας, σε τοποθεσία που είναι ασφαλής και ελεγχόμενη από το κλίμα. Κατά την επιλογή της τοποθεσίας εκτός τοποθεσίας, είναι σημαντικό να λαμβάνονται υπόψη οι ώρες λειτουργίας της τοποθεσίας, η ευκολία με την οποία είναι δυνατή η πρόσβαση στα εφεδρικά μέσα, οι περιορισμοί της φυσικής αποθήκευσης και οι όροι της σύμβασης. Για να βοηθήσει στον προσδιορισμό του πόσο συχνά θα πρέπει να ελέγχονται τα εφεδρικά μέσα, ο συντονιστής ISCP οφείλει να συμβουλεύεται την πολιτική ανθεκτικότητας του οργανισμού και την BIA. Η επισήμανση κάθε εφεδρικής ταινίας, κασέτας ή δίσκου με

ένα μοναδικό αναγνωριστικό είναι απαραίτητη για να διασφαλιστεί ότι τα αναγκαία δεδομένα μπορούν να εντοπιστούν αμέσως σε περίπτωση απροσδόκητης καταστροφής. Εξαιτίας αυτού, ο οργανισμός επιβάλλεται να επινοήσει μια μέθοδο προσθήκης ετικετών και παρακολούθησης μέσων που να είναι ταυτόχρονα αποτελεσματική και αποτελεσματική. Συμπληρωματικά, εναλλακτικές εγκαταστάσεις επεξεργασίας μπορούν να παρέχουν μια τοποθεσία για έναν οργανισμό για να συνεχίσει τις λειτουργίες του συστήματος σε περίπτωση που ένα καταστροφικό συμβάν απενεργοποιήσει ή καταστρέψει την κύρια εγκατάσταση του συστήματος. Αυτή η τοποθεσία είναι δυνατό να παρέχεται από μια εναλλακτική εγκατάσταση επεξεργασίας. Οι τρεις βασικές ποικιλίες εναλλακτικών εγκαταστάσεων επεξεργασίας αναφέρονται ως ψυχρές τοποθεσίες και θερμές τοποθεσίες και συζητούνται στο κεφάλαιο 3.1. Ο συντονιστής του σχεδίου έκτακτης ανάγκης για το σύστημα πληροφοριών οφείλει να εξετάσει τις πληροφορίες που παρέχονται στο BIA για να προσδιορίσει ποια κρίσιμη αποστολή ή επιχειρηματικές διαδικασίες υποστηρίζει ένα σύστημα, το μέγιστο χρονικό διάστημα που υπάρχει η δυνατότητα να διακοπεί το σύστημα και τον αντίκτυπο της απώλειας του συστήματος που θα είχε η εταιρεία προκειμένου να καθοριστεί τι είδους τοποθεσία ανάκτησης απαιτείται. Είναι δυνατό μια στρατηγική ανάκτησης για ένα σύστημα πληροφοριών να περιλαμβάνει ένα ή περισσότερα από αυτά τα διαφορετικά είδη εναλλακτικών δυνατοτήτων επεξεργασίας.

Η δημιουργία μιας πολιτικής για επιτυχημένο σχεδιασμό έκτακτης ανάγκης συνεπάγεται την ανθεκτικότητα ενός συστήματος σε αστοχίες σε επίπεδο περιβάλλοντος και εξαρτημάτων, που ελλείψει αυτής της πολιτικής, θα προκαλούσαν διακοπές στο σύστημα. Υπάρχουν μερικές διαφορετικές προσεγγίσεις που οφείλουν να ακολουθηθούν προκειμένου να γίνει πιο ανθεκτικό το πολύτιμο υλικό και λογισμικό. Οι αποφάσεις που λαμβάνουν υπόψη τους πιθανούς κινδύνους θα πρέπει να χρησιμεύουν ως βάση για τον καθορισμό των κατάλληλων προσεγγίσεων. Η δυνατότητα εφαρμογής αυτών των στρατηγικών σε ένα δεδομένο σύστημα εξαρτάται από τα αποτελέσματα της διαδικασίας διαχείρισης κινδύνου και είναι πιθανό να μην ισχύουν καθόλου.

Η απώλεια ηλεκτρικής ενέργειας είναι δυνατό να καταστρέψει τόσο την ακεραιότητα του συστήματος όσο και τα δεδομένα που είναι αποθηκευμένα σε αυτό. Για την προστασία των δεδομένων από την καταστροφή, βασικό υλικό όπως οι διακομιστές μπορούν να εξοπλιστούν με ένα ζεύγος ανεξάρτητης παροχής ρεύματος. Οι δύο πηγές τροφοδοσίας είναι αναγκαίο να χρησιμοποιούνται ταυτόχρονα, έτσι ώστε

σε περίπτωση υπερθέρμανσης ή μη λειτουργίας του πρωτεύοντος τροφοδοτικού, η δευτερεύουσα μονάδα να μπορεί να παρέμβει ως κύρια πηγή ενέργειας. Αυτό θα διασφαλίσει ότι δεν θα υπάρξει καμία διαταραχή στο σύστημα. Σε περίπτωση όμως απώλειας ισχύος, ένα UPS μπορεί να προστατεύσει το σύστημα. Στις περισσότερες περιπτώσεις, ένα UPS θα προσφέρει μεταξύ τριάντα και εξήντα λεπτών προσωρινής εφεδρικής ισχύος για να διευκολύνει την ομαλή απενεργοποίηση. Ελέγχοντας την εισερχόμενη ηλεκτρική ενέργεια και παρέχοντας μια σταθερή πηγή ρεύματος, ένα αδιάλειπτο τροφοδοτικό (UPS) μπορεί επιπλέον να προστατεύσει από τις διακυμάνσεις του ρεύματος. Εάν υπάρχει ανάγκη για υψηλή διαθεσιμότητα, είναι πιθανό να είναι απαραίτητη μια γεννήτρια που να λειτουργεί είτε με φυσικό αέριο είτε με ντίζελ. Η γεννήτρια μπορεί να συνδεθεί απευθείας στο σύστημα τροφοδοσίας της τοποθεσίας και μπορεί να προγραμματιστεί να ξεκινά να λειτουργεί αυτόματα κάθε φορά που υπάρχει διακοπή στην παροχή ρεύματος. Εφόσον υπάρχει καύσιμο για τη γεννήτρια, μια αδιάλειπτη παροχή ρεύματος (UPS) που περιλαμβάνει επίσης μια γεννήτρια μπορεί να τροφοδοτεί ένα σύστημα με καθαρό και αξιόπιστο ηλεκτρικό ρεύμα.

Η υψηλή διαθεσιμότητα, συχνά γνωστή ως HA, είναι μια τεχνική που περιλαμβάνει τη δημιουργία μηχανισμών πλεονασμού και ανακατεύθυνσης σε ένα σύστημα προκειμένου να αυξηθεί ο χρόνος λειτουργίας και η διαθεσιμότητα του συστήματος. Ο στόχος της υψηλής διαθεσιμότητας (HA) είναι να έχουμε χρόνο λειτουργίας 99,999 % ή μεγαλύτερο, που μεταφράζεται σε μόνο λίγα λεπτά διακοπής λειτουργίας ετησίως. Η υψηλή διαθεσιμότητα (HA) είναι μια επιλογή που μπορεί να είναι ακριβή για συστήματα, καθώς απαιτεί διπλό υλικό και εξειδικευμένο λογισμικό ανακατεύθυνσης για την αφαίρεση όλων των πιθανών μεμονωμένων σημείων αστοχίας. Στις περισσότερες περιπτώσεις, το κόστος συντήρησης και υποστήριξης για συστήματα ΥΑ είναι σημαντικά μεγαλύτερο από αυτό για άλλους τύπους συστημάτων. Εξαιτίας αυτού, το HA δεν είναι μια εφαρμόσιμη επιλογή για πολλά συστήματα και θα πρέπει να λαμβάνεται υπόψη μόνο για εκείνα τα συστήματα που δεν είναι σε θέση να διατηρήσουν οποιοδήποτε χρόνο διακοπής λειτουργίας. Είναι δυνατό να δημιουργηθεί HA σε μια ενιαία τοποθεσία, με όλο τον πλεονασμό του συστήματος να βρίσκεται σε αυτήν τη θέση. Με την προϋπόθεση ότι δεν υπάρχει διακοπή στη λειτουργία της εγκατάστασης στην οποία στεγάζεται το σύστημα, αυτό θα διασφαλίσει ότι το σύστημα θα συνεχίσει να λειτουργεί σε επίπεδο ΥΑ. Ως εκ τούτου, όταν ασχολούμαστε με συστήματα υψηλής πρόσκρουσης, είναι σημαντικό να λαμβάνεται υπόψη η διαδικασία επέκτασης του HA σε διαφορετική τοποθεσία.

Τόσο σε επίπεδο συστήματος διακομιστή όσο και σε επίπεδο πελάτη, οι ανησυχίες για ένα τέτοιο ενδεχόμενο θα πρέπει να δίνουν έμφαση στη διαθεσιμότητα, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Με σκοπό να ικανοποιηθούν αυτές οι απαιτήσεις, συνιστάται να αποθηκεύονται τακτικά και συχνά αντίγραφα ασφαλείας των δεδομένων μακριά από την κύρια τοποθεσία. Για αρχιτεκτονικές πελάτη-διακομιστή, υπάρχει μια τεράστια ποικιλία από πιθανές επιλογές δημιουργίας αντιγράφων ασφαλείας και ανάκτησης λογισμικού και υλικού. Στις συσκευές-πελάτες, η κρυπτογράφηση είναι μια κοινή μορφή προστασίας δεδομένων που χρησιμοποιείται. Υπό το πρίσμα της αυξανόμενης επικράτησης της χρήσης ψηφιακών υπογραφών για τη μη απόρριψη και τη χρήση της κρυπτογράφησης για σκοπούς μυστικότητας ή/και ακεραιότητας, οι επιχειρήσεις είναι απαραίτητο να εξετάσουν σοβαρά την ενσωμάτωση της κρυπτογράφησης στη στρατηγική τους για τη δημιουργία αντιγράφων ασφαλείας. Για την προστασία των δεδομένων σε περίπτωση που τοποθετηθούν λάθος ή κλαπούν κατά τη μεταφορά τους ή όταν φτάσουν στη δευτερεύουσα θέση, είναι σημαντικό να κρυπτογραφήσετε τυχόν εφεδρικά μέσα που αποστέλλονται μακριά από την κύρια τοποθεσία για αποθήκευση. Σε περίπτωση που τα κρυπτογραφημένα δεδομένα αποστέλλονται εκτός τοποθεσίας για αποθήκευση, θα πρέπει να υπάρχει ένα σύστημα διαχείρισης κρυπτογραφικού κλειδιού για να διασφαλίζεται ότι τα δεδομένα μπορούν να αποκρυπτογραφηθούν και να διαβαστούν σε περίπτωση που χρειαστεί να ανακτηθούν σε νέο ή διαφορετικό σύστημα. Οι διακομιστές συνήθως αποθηκεύουν πολύ μεγαλύτερες ποσότητες δεδομένων, τα οποία οφείλουν να διαχειρίζονται, να προστατεύονται και να ενημερώνονται όλα. Συνιστάται ότι σε ρυθμίσεις με πολλούς διακομιστές, ο χώρος αποθήκευσης δεν πρέπει να αφιερώνεται σε κάθε μεμονωμένο διακομιστή, αλλά μάλλον να βρίσκεται συγκεντρωμένος, ώστε να μπορεί να χρησιμοποιηθεί από έναν αριθμό διακομιστών ταυτόχρονα. Τόσο το SAN όσο και το NAS είναι παραδείγματα δημοφιλών αρχιτεκτονικών αποθήκευσης πολλών διακομιστών. Η δυνατότητα δημιουργίας κεντρικού αντιγράφου ασφαλείας δεδομένων για αποθήκευση εκτός τοποθεσίας καθίσταται δυνατή με τη συγκέντρωση των δεδομένων σε πολλούς διακομιστές. Συνιστάται ανεπιφύλακτα να χρησιμοποιείται ένα ξεχωριστό και αποκλειστικό δίκτυο ειδικά για τις μεταφορές δεδομένων που απαιτούνται για τη διαδικασία δημιουργίας αντιγράφων ασφαλείας δεδομένων. Αυτό οφείλεται στον τεράστιο όγκο δεδομένων που πρέπει να δημιουργηθούν αντίγραφα ασφαλείας. Κατά τη διάρκεια του σχεδιασμού και της εκτέλεσης του συστήματος πελάτη/διακομιστή, πιθανές εναλλακτικές λύσεις

θα μπορούσαν να ενσωματωθούν στο σύστημα. Για παράδειγμα, μια αρχιτεκτονική πελάτη-διακομιστή θα μπορούσε να κατασκευαστεί με τέτοιο τρόπο με στόχο όλα τα δεδομένα να αποθηκεύονται σε μια ενιαία τοποθεσία και στη συνέχεια να διανέμονται στις διάφορες τοπικές τοποθεσίες.

Σε αντίθεση με τον σχεδιασμό πελάτη/διακομιστή, η αρχιτεκτονική του mainframe είναι μια κεντρική μορφή οργάνωσης υπολογιστών. Οι πελάτες είναι τερματικά που δεν έχουν ούτε την ικανότητα να επεξεργάζονται δεδομένα ούτε να τα αποθηκεύουν και χρησιμοποιούνται για πρόσβαση στον κεντρικό υπολογιστή. Η μοναδική πηγή υπολογιστικής ικανότητας για το σύστημα περιέχεται στον ίδιο τον κεντρικό υπολογιστή. Η μόνη πηγή εξόδου που θα πάρουν τα τερματικά είναι το mainframe. Παρά το γεγονός ότι η επεξεργασία σε έναν κεντρικό υπολογιστή είναι πιο ισχυρή και συγκεντρωτική από την επεξεργασία σε άλλους τύπους πλατφορμών, πολλές από τις ανάγκες έκτακτης ανάγκης παραμένουν οι ίδιες. Ένα mainframe δεν διαθέτει τον ενσωματωμένο πλεονασμό που παρέχεται από ένα κατανεμημένο σύστημα ή δίκτυο λόγω του γεγονότος ότι ένας κεντρικός υπολογιστής έχει κεντρική αρχιτεκτονική. Ως συνέπεια αυτού, η διαθεσιμότητα του mainframe, καθώς και τα αντίγραφα ασφαλείας δεδομένων είναι εξαιρετικά σημαντικά. Εξαιτίας αυτού τα δεδομένα αποθηκεύονται μόνο σε μία τοποθεσία, τα mainframes απαιτούν διαφορετικό σύνολο τεχνικών έκτακτης ανάγκης από τα κατανεμημένα συστήματα. Οι στρατηγικές για απρόβλεπτα γεγονότα είναι απαραίτητο να δίνουν έμφαση στις δυνατότητες αποθήκευσης δεδομένων του mainframe καθώς και στην υποκείμενη αρχιτεκτονική του. Είναι αναγκαίο να υπάρχουν πλεονάζοντα εξαρτήματα συστήματος για να διασφαλιστεί ότι η απώλεια ενός μεμονωμένου στοιχείου του συστήματος, όπως ένα τροφοδοτικό, δεν θα οδηγήσει σε αστοχία ολόκληρου του συστήματος. Ένα UPS, καθώς και εργαλεία παρακολούθησης και ελέγχου ισχύος, θα πρέπει επίσης να χρησιμοποιούνται για να διασφαλιστεί ότι ο κεντρικός υπολογιστής δεν θα επηρεαστεί αρνητικά από τις διακυμάνσεις στην παροχή ρεύματος. Είναι πιθανό να απαιτηθεί μια μακροπρόθεσμη εφεδρική λύση ισχύος για τους μεγάλους υπολογιστές, επειδή συχνά επεξεργάζονται τεράστιες βασικές εφαρμογές. Σε περίπτωση διακοπής ρεύματος, μια γεννήτρια που τροφοδοτείται είτε με φυσικό αέριο είτε με ντίζελ έχει τη δυνατότητα να διατηρήσει την ομαλή λειτουργία της επεξεργασίας του mainframe. Επιπλέον, μπορεί να δοθεί πλεονασμός δίσκου για συσκευές αποθήκευσης άμεσης πρόσβασης δημιουργώντας μια λύση RAID. Αυτό μπορεί να γίνει με πολλούς διαφορετικούς τρόπους. Ένα σύστημα αντικατάστασης θα πρέπει πάντα να είναι έτοιμο για χρήση σε

εναλλακτικό ζεστό ή ζεστό χώρο ως προληπτικό μέτρο. Αυτό οφείλεται στο γεγονός ότι η αρχιτεκτονική κάθε mainframe είναι ξεχωριστή και συγκεντρωτική. Η απόκτηση και η συντήρηση εφεδρικών πλατφορμών mainframe είναι εξαιρετικά δαπανηρές, γι' αυτό πολλοί κυβερνητικοί οργανισμοί μοιράζονται εμπορικά συστήματα. Επιπλέον, οι αντιπροσωπείες συχνά διατηρούν συμβάσεις υποστήριξης προμηθευτών για να επιδιορθώσουν τα κατεστραμμένα συστήματα. Ωστόσο, το να βασίζεται η επιχείρηση αποκλειστικά στη βοήθεια του προμηθευτή ενδέχεται να μην είναι αρκετή για την αποκατάσταση της λειτουργικότητας του συστήματος εντός του καθορισμένου χρόνου διακοπής λειτουργίας. Σε κάθε περίσταση, είναι σημαντικό να διατηρείται ενημερωμένες τις συμφωνίες επιπέδου υπηρεσιών προμηθευτή (SLA) και να τις αναθεωρείτε τακτικά για να διασφαλίζετε ότι ο προμηθευτής προσφέρει επαρκή βοήθεια για την κάλυψη των αναγκών διαθεσιμότητας συστήματος.

Οι πιο συνηθισμένοι τύποι δικτύων επικοινωνιών είναι γνωστοί ως τοπικά δίκτυα (LAN) και δίκτυα ευρείας περιοχής (WAN). Η ασύρματη επικοινωνία, η οποία είναι κοινή για χρήση με φορητές συσκευές, εφαρμόζεται είτε σε τοπικά δίκτυα (LAN) είτε σε δίκτυα ευρείας περιοχής (WAN). Ένα τοπικό δίκτυο μπορεί να βρεθεί σε περιβάλλον γραφείου ή πανεπιστημιακού περιβάλλοντος. Μπορεί να είναι τόσο απλό όσο δύο προσωπικοί υπολογιστές συνδεδεμένοι σε έναν ενιαίο διακόπτη δικτύου ή θα μπορούσε να υποστηρίζει εκατοντάδες χρήστες και έναν αριθμό διακομιστών. Από την άλλη πλευρά, ένα δίκτυο ευρείας περιοχής (WAN) είναι ένας τύπος δικτύου επικοινωνιών δεδομένων που περιλαμβάνει τη σύνδεση δύο ή περισσότερων συστημάτων που βρίσκονται σε διαφορετικά μέρη μιας μεγάλης γεωγραφικής περιοχής. Η σύνδεση που επιτρέπει σε ένα σύστημα να εμπλέκεται με άλλα συστήματα παρέχεται μέσω συνδέσεων επικοινωνίας. Αυτοί οι σύνδεσμοι παρέχονται συχνά από τον δημόσιο φορέα. Κατά την ανάπτυξη ενός ολοκληρωμένου σχεδίου για την ανάκαμψη των τηλεπικοινωνιακών συστημάτων, ο συντονιστής του σχεδίου έκτακτης ανάγκης του πληροφοριακού συστήματος επιβάλλεται να λαμβάνει υπόψη μια ποικιλία διαφορετικών στρατηγικών και λύσεων, παρά το γεγονός ότι τα συστήματα τηλεπικοινωνιών LAN και WAN υπόκεινται σε παρόμοια είδη έκτακτης ανάγκης.

Κατά την κατασκευή ενός ISCP (information system contingency plan) για ένα LAN, ο συντονιστής ISCP θα πρέπει να προσδιορίζει μεμονωμένα σημεία αστοχίας που επηρεάζουν βασικά συστήματα ή διαδικασίες που περιγράφονται στο BIA. Αυτό είναι δυνατό να επιτευχθεί κάνοντας μια εκτίμηση κινδύνου. Αυτή η ανάλυση μπορεί να λάβει υπόψη πιθανούς κινδύνους για το σύστημα καλωδίωσης, όπως η αποκοπή

καλωδίου, οι ηλεκτρομαγνητικές παρεμβολές και οι παρεμβολές ραδιοσυχνοτήτων και ζημιές που προκαλούνται από φωτιά, νερό και άλλους κινδύνους. Είναι δυνατή η προσθήκη περιττών καλωδίων ως θεραπεία στις κατάλληλες καταστάσεις. Για παράδειγμα, η εγκατάσταση περιττών καλωδίων σε επιτραπέζιους υπολογιστές μπορεί να μην είναι η πιο αποτελεσματική χρήση των πόρων. Η χρήση εξοπλισμού σύνδεσης δικτύου, συμπεριλαμβανομένων των διανομέων, των μεταγωγέων, των δρομολογητών και των γεφυρών θα πρέπει να λαμβάνεται υπόψη κατά τη διάρκεια της διαδικασίας σχεδιασμού έκτακτης ανάγκης. Το BIA οφείλει να παρέχει μια περιγραφή των λειτουργιών που εκτελεί κάθε συσκευή εντός του δικτύου. Επιπλέον, είναι πρωτεύον να προετοιμαστεί ένα εφεδρικό σχέδιο για κάθε συσκευή λαμβάνοντας υπόψη πόσο ζωτικής σημασίας το θεωρεί η BIA.

Είναι σημαντικό να ενσωματωθούν εικονικά ιδιωτικά δίκτυα στον σχεδιασμό έκτακτης ανάγκης για τοπικά δίκτυα (LAN). Οι διακομιστές και άλλες συσκευές στο τοπικό δίκτυο (LAN) προσφέρουν μια υπηρεσία γνωστή ως απομακρυσμένη πρόσβαση. Οι χρήστες που λειτουργούν εκτός τοποθεσίας επωφελούνται από την ευκολία της απομακρυσμένης πρόσβασης και επιτρέπει επίσης στους διακομιστές και άλλες συσκευές να συνδέονται μεταξύ τους σε διάφορες τοποθεσίες. Η πρόσβαση από απόσταση μπορεί να επιτευχθεί με διάφορα μέσα, το πιο συνηθισμένο από τα οποία είναι ένα εικονικό ιδιωτικό δίκτυο (Virtual Private Network VPN). Είναι πιθανό η απομακρυσμένη πρόσβαση να λειτουργεί ως κύριας σημασίας σε περίπτωση έκτακτης ανάγκης ή σημαντικής διακοπής του συστήματος. Αυτό θα επέτρεπε στις ομάδες ανάκτησης ή στους χρήστες να έχουν πρόσβαση σε δεδομένα για ολόκληρο τον οργανισμό από άλλη τοποθεσία. Εάν η απομακρυσμένη πρόσβαση πρόκειται να εφαρμοστεί ως εφεδρικό σχέδιο, τότε πρέπει πρώτα να καθοριστούν οι απαιτήσεις εύρους ζώνης δεδομένων και, στη συνέχεια, η λύση απομακρυσμένης πρόσβασης οφείλει να κλιμακωθεί ανάλογα.

Μετά από διακοπή ενός ενσύρματου τοπικού δικτύου (LAN), ενδέχεται να είναι δυνατή η χρήση ασύρματων τοπικών δικτύων (γνωστά και ως WiFi) ως αποτελεσματικό σχέδιο δημιουργίας αντιγράφων ασφαλείας για την επαναφορά των υπηρεσιών δικτύου. Τα ασύρματα δίκτυα δεν απαιτούν την υποδομή ενσύρματων LAN, επομένως δεν χρειάζονται ούτε καλώδια. Εξαιτίας αυτού, μπορούν εύκολα να αναπτυχθούν ως λύση, είτε είναι προσωρινή είτε μόνιμη. Εντούτοις, τα ασύρματα δίκτυα στέλνουν τα δεδομένα τους μέσω ραδιοφωνικού σήματος, το οποίο καθιστά δυνατή την παραβίαση των δεδομένων. Η χρήση κωδικού πρόσβασης για έλεγχο

ταυτότητας και κρυπτογράφηση μετάδοσης περιλαμβάνεται συνήθως ως τυπική λειτουργία στους ασύρματους δρομολογητές. Απαιτείται η εφαρμογή ορισμένων προτύπων και αρχών ασφαλείας για επιχειρήσεις που εξετάζουν το ενδεχόμενο χρήσης απομακρυσμένης συνδεσιμότητας. Ο ηλεκτρονικός έλεγχος ταυτότητας, συχνά γνωστός ως ηλεκτρονικός έλεγχος ταυτότητας, είναι μια μέθοδος που μπορεί να χρησιμοποιηθεί για την επικύρωση της ταυτότητας ενός χρήστη.

Όλες οι προφυλάξεις που αναφέρθηκαν σε σχέση με συστήματα πελάτη-διακομιστή και τοπικά δίκτυα περιλαμβάνονται στις λύσεις έκτακτης ανάγκης WAN. Εξάλλου, η διαδικασία σχεδιασμού έκτακτης ανάγκης WAN είναι απαραίτητο να λαμβάνει υπόψη τις ζεύξεις επικοινωνίας που χρησιμοποιούνται για τη σύνδεση των διαφόρων συστημάτων. Το είδος των δεδομένων που μεταδίδονται μέσω του δικτύου έχει επίδραση στα σχέδια αποκατάστασης καταστροφών για το δίκτυο ευρείας περιοχής (WAN). Ένα δίκτυο ευρείας περιοχής (WAN) που συνδέει πολλά τοπικά δίκτυα (LAN) με σκοπό την κοινή χρήση πόρων ενδέχεται να απαιτεί μια λιγότερο αυστηρή προσέγγιση ανάκτησης από ένα WAN που φιλοξενεί ένα σύστημα κρίσιμο για την αποστολή. Οι περιττοί σύνδεσμοι επικοινωνίας, οι περιττοί πάροχοι υπηρεσιών δικτύου, οι πλεονάζουσες συσκευές σύνδεσης δικτύου και οι πλεονασμοί που παρέχονται από παρόχους υπηρεσιών Διαδικτύου (ISP) είναι μερικές από τις λύσεις έκτακτης ανάγκης που πρέπει συμπεριλάβουν οι οργανισμοί. Η εγκατάσταση λογισμικού παρακολούθησης είναι ένας τρόπος για να περιοριστεί ο αντίκτυπος μιας διακοπής στις τηλεπικοινωνίες, καθιστώντας δυνατή την έγκαιρη ανίχνευση του προβλήματος. Εάν το λογισμικό παρακολούθησης εντοπίσει ότι ένας κόμβος ή μια σύνδεση αποτυγχάνει ή δεν ανταποκρίνεται, θα δημιουργηθεί συναγερμός. Η αντιμετώπιση προβλημάτων μπορεί να γίνει ευκολότερη με λογισμικό παρακολούθησης, το οποίο επίσης ειδοποιεί τον διαχειριστή για πιθανά ζητήματα στις περισσότερες περιπτώσεις προτού οι χρήστες και άλλοι κόμβοι τα αντιληφθούν.

Συμπεράσματα

Η τρέχουσα κατάσταση του παγκόσμιου επιχειρηματικού περιβάλλοντος είναι ολοένα και πιο απρόβλεπτη/χαοτική. Αυτή η κατάσταση, μαζί με τις ραγδαίες βελτιώσεις στην τεχνολογία και την κοινωνική δυναμική, επηρεάζουν σχεδόν όλους τους τομείς, συμπεριλαμβανομένης της κάθε επιχείρησης στον πλανήτη. Ως εκ τούτου, οι επιχειρήσεις οφείλουν να προστατεύονται αποτελεσματικά μέσω της αυξημένης ανθεκτικότητας, προκειμένου να συνεχίσουν να λειτουργούν επικερδώς σε περίπτωση

σοβαρής επιχειρηματικής διαταραχής. Οι οργανισμοί τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα πρέπει να είναι καλύτερα εξοπλισμένες για να διαχειρίζονται τυχόν δυσμενείς κρίσεις και να διασφαλίζουν, ότι οι διαταραχές στις καθημερινές τους λειτουργίες περιορίζονται στο ελάχιστο. Οποιαδήποτε σημαντική λειτουργική αστοχία μπορεί να οδηγήσει σε μείωση της ποιότητας των υπηρεσιών και, σε ακραίες περιπτώσεις, σε οικονομική ζημία λόγω παρατεταμένης ή σοβαρής διακοπής της λειτουργίας της εταιρείας.

Η ανθεκτικότητα είναι μια κρίσιμη ποιότητα για τις επιχειρήσεις, απαραίτητη για να προστατεύουν τις δραστηριότητές τους και να διασφαλίζουν τη βιωσιμότητα και τη συνέχειά τους, παραμένοντας ωστόσο ανταγωνιστικές. Εκτός από τη βοήθεια στη δημιουργία και την οικοδόμηση ανθεκτικότητας, ορισμένες από τις προτεινόμενες ενέργειες—όπως η συνεχής παρακολούθηση, οι δεξιότητες αυτοσχεδιασμού και η ικανότητα πρόβλεψης—μπορούν επίσης να είναι χρήσιμες σε άλλους επιχειρηματικούς τομείς και δραστηριότητες.

Οι στρατηγικές που προτείνονται σε αυτή τη μελέτη για την εφαρμογή της διαχείρισης επιχειρηματικής συνέχειας είναι βασισμένες στην στρατηγική που αντιπροσωπεύεται στην καθιέρωση προτύπων όπως τα ISO 22301, 22316, 22320, 24762, 27031 και η δημοσίευση NIST 800-34. Τα ευρήματα της γνωστοποιούν τις διαχειριστικές γνώσεις και τις επιπτώσεις διαχείρισης διαταραχών, καθώς και συμβουλές σχετικά με τα βήματα που πρέπει να ακολουθηθούν και τις μεταβλητές που πρέπει να λαμβάνονται υπόψη κατά τη δημιουργία συστημάτων διαχείρισης διαταραχών. Αυτή η μελέτη σκοπεύει επίσης να καταδείξει την αξία της διαχείρισης επιχειρησιακής συνέχειας ως εργαλείου στρατηγικής διαχείρισης που οφείλουν να χρησιμοποιήσουν οι επιχειρήσεις με σκοπό τη μείωση του λειτουργικού κινδύνου και των επιπτώσεων του στις ζωτικές λειτουργίες της εταιρείας.

Βιβλιογραφία

[1] A. Hiles, P. Barnes (Eds.), The definitive handbook of business continuity management, Wiley, Chichester (2001), pp. 3-24.

[2] Perez, J.C. (2010) Wikipedia suffers global collapse, Network World. IDG News Service. Available at: https://www.networkworld.com/article/2205368/wikipedia-suffers-global-collapse.html (Accessed: September 25, 2022).

[3] Data center disasters Data Center Disasters | Sunbird DCIM. Available at: https://www.sunbirddcim.com/infographic/data-center-disasters (Accessed: November 5, 2022).

[4] 16, R.M.| D. (2013) The Year in downtime: The top 10 outages of 2013, Data Center Knowledge | News and analysis for the data center industry. Available at: https://www.datacenterknowledge.com/archives/2013/12/16/year-downtime-top-10-outages-2013 (Accessed: November 6, 2022).

[5] 21, Y.S.| J. (2016) Equinix data center outage in London blamed on faulty ups, Data Center Knowledge | News and analysis for the data center industry. Available at: https://www.datacenterknowledge.com/archives/2016/07/21/equinix-data-center-outage-in-london-blamed-on-faulty-ups (Accessed: November 6, 2022).

[6] Peter Judge Peter Judge is the global editor at DatacenterDynamics. (2023) OVHcloud's Data Center Fire: One year on, what do we know?, All Content RSS. Available at: https://www.datacenterdynamics.com/en/opinions/ovhclouds-data-center-fire-one-year-on-what-do-we-know/ (Accessed: November 6, 2022).

[7] Landi, H. (2021) Scripps Health was attacked by hackers. now, patients are suing for failing to protect their health data, Fierce Healthcare. Available at: https://www.fiercehealthcare.com/tech/following-ransomware-attack-scripps-health-now-facing-class-action-lawsuits-over-data-breach (Accessed: November 7, 2022).

[8] Swinhoe, D. (2023) Google's London Data Center outage during heatwave caused by "simultaneous failure of multiple, redundant cooling systems", All Content RSS. Available at: https://www.datacenterdynamics.com/en/news/googles-london-data-center-outage-during-heatwave-caused-by-simultaneous-failure-of-multiple-redundant-cooling-systems/ (Accessed: November 7, 2022). [9] https://www.iso.org/standard/77008.html

[10] International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. Retrieved from https://www.iso.org/standard/75106.html
[11] International Organization for Standardization. (2017). ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes. Retrieved from https://www.iso.org/standard/50053.html
[12] International Organization for Standardization. (2018). ISO 22320:2018 Security and resilience — Emergency management — Guidelines for incident management. Retrieved from https://www.iso.org/standard/67851.html
[13] International Organization for Standardization. (2008). ISO/IEC 24762:2008 Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services. Retrieved from https://www.iso.org/standard/41532.html
[14] International Organization for Standardization. (2011). ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity. Retrieved from https://www.iso.org/standard/44374.html
[15] Holling, C.S. Resilience and Stability of Ecological Systems. Annu. Rev. Ecol. Syst. 1973, 4, 1–23.
[16] Annarelli, A.; Nonino, F. Strategic and operational management of organizational resilience: Current state of research and future directions. Omega 2016, 62, 1–18.
[17] Rose, A. Defining and measuring economic resilience to disasters. Disaster Prev. Manag. Int. J. 2004, 13, 307–314.
[18] Rose, A. Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions. Environ. Hazards 2007, 7, 383–398.
[19] Von Solms, R.; Van Niekerk, J. From information security to cyber security. Comput. Secur. 2013, 38, 97–102.
[20] Sheffi, Y.; Rice, J.B., Jr. A supply chain view of the resilient enterprise. MIT Sloan Manag. Rev. 2005, 47, 41–48.
[21] BSI. (2022). BS 65000:2022 Organizational resilience. Code of practice. Retrieved from https://knowledge.bsigroup.com/products/organizational-resilience-code-of-practice/standard?creative=617647803294&keyword=bsi%20organisational%20resilience&matchtype=p&network=g&device=c&gclid=Cj0KCQjw4omaBhDqARIsADX

ULuU8lZxwrOk1n3Lr81k72GhKUpRgsDHwcKsdd-r6r6HlCp8pMxmUKPUaAvxOEALw_wcB&gclsrc=aw.ds

[22] Keen, R. (2022) ISO 9001 - clause 4.2: Understanding the needs and expectations of interested parties, ISO 9001 Checklist. Available at: https://www.iso-9001-checklist.co.uk/4.2-understanding-the-needs-and-expectations-of-interested-parties.htm (Accessed: November 15, 2022).

[23] Rheinland, T.Ü.V. (2022) Business Continuity Management System (BCMS), WO | TÜV Rheinland. Available at: https://www.tuv.com/world/en/business-continuity-management-system-(bcms).html (Accessed: November 16, 2022).

[24] What is the plan-do-check-act (Pdca) cycle? ASQ. Available at: https://asq.org/quality-resources/pdca-cycle (Accessed: November 20, 2022).

[25] Blackhurst, J., Dunn, K. and Craighead, C. (2011). An Empirically Derived Framework of Global Supply Resiliency. Journal of Business Logistics, 32(4), pp.374-391.

[26] Feng, N.; Li, M. An information systems security risk assessment model under uncertain environment. Appl. Soft Comput. 2011, 11, 4332–4340.

[27] Kankanhalli, A.; Teo, H.H.; Tan, B.C.Y.; Wei, K.-K. An integrative study of information systems security effectiveness. Int. J. Inf. Manag. 2003, 23, 139–154.

[28] Sembiring, J.; Siregar, M.I.H. A Decision Model for IT Risk Management on Disaster Recovery Center in an Enterprise Architecture Model. Proc. Technol. 2013, 11, 1142–1146.

[29] Hawkins, S.M.; Yen, D.C.; Chou, D.C. Disaster recovery planning: A strategy for data security. Inf. Manag. Comput. Secur. 2000, 8, 222–230.

[30] Bryson, K.-M.; Millar, H.; Joseph, A.; Mobolurin, A. Using formal MS/OR modeling to support disaster recovery planning. Eur. J. Oper. Res. 2002, 141, 679–688.

[31] Daim, T.U.; Bhatla, A.; Mansour, M. Site selection for a data centre–a multi-criteria decision-making model. Int. J. Sustain. Eng. 2013, 6, 10–22.

[32] Kant, K. Data center evolution: A tutorial on state of the art, issues, and challenges. Comput. Netw. 2009, 53, 2939–2965.

[33] Covas, M.T.; Silva, C.A.; Dias, L.C. On locating sustainable Data Centers in Portugal: Problem structuring and GIS-based analysis. Sustain. Comput. 2013, 3, 27–35.

[34] Reed, J. (2023) Disaster recovery sites comparison: Which One to choose?, Official NAKIVO Blog. Available at: https://www.nakivo.com/blog/overview-

disaster-recovery-sites/ (Accessed: November 25, 2022). [35] Wang, G.; Qin, L.; Li, G.; Chen, L. Landfill site selection using spatial information technologies and AHP: A case study in Beijing, China. J. Environ. Manag. 2009, 90, 2414–2421.
[36] Covas, M.T.; Silva, C.A.; Dias, L.C. On locating sustainable Data Centers in Portugal: Problem structuring and GIS-based analysis. Sustain. Comput. 2013, 3, 27–35.
[37] Rikalovic, A.; Cosic, I.; Lazarevic, D. GIS Based Multi-criteria Analysis for Industrial Site Selection. Proc. Eng. 2014, 69, 1054–1063.
[38] Dermol, U.; Kontić, B. Use of strategic environmental assessment in the site selection process for a radioactive waste disposal facility in Slovenia. J. Environ. Manag. 2011, 92, 43–52.
[39] Herbane, B.; Elliott, D.; Swartz, E.M. Business continuity management: Time for a strategic role? Long Range Plan. 2004, 37, 435–457.
[40] Vahidnia, M.H.; Alesheikh, A.A.; Alimohammadi, A. Hospital site selection using fuzzy AHP and its derivatives. J. Environ. Manag. 2009, 90, 3048–3056.
[41] Dissanayake, S.; Önal, H. Amenity driven price effects and conservation reserve site selection: A dynamic linear integer programming approach. Ecol. Econ. 2011, 70, 2225–2235.
[42] Herbane, B.; Elliott, D.; Swartz, E.M. Business continuity management: Time for a strategic role? Long Range Plan. 2004, 37, 435–457.
[43] Hristidis, V.; Chen, S.-C.; Li, T.; Luis, S.; Deng, Y. Survey of data management and analysis in disaster situations. J. Syst. Softw. 2010, 83, 1701–1714.
[44] Editor, C.S.R.C.C. Federal Information System - Glossary: CSRC, CSRC Content Editor. Available at: https://csrc.nist.gov/glossary/term/federal_information_system (Accessed: December 5, 2022).
[45] What is a mainframe? it's a style of computing IBM. Available at: https://www.ibm.com/docs/en/zos-basic-skills?topic=today-what-is-mainframe-its-style-computing (Accessed: December 6, 2022).