ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ

ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΤΗ ΔΙΟΙΚΗΣΗ

ΕΠΙΧΕΙΡΗΣΕΩΝ ΓΙΑ ΣΤΕΛΕΧΗ (Ε-ΜΒΑ)

Διπλωματική Εργασία

«Η Λειτουργία των Εξωτερικών Αναθέσεων, η περίπτωση της Ασφάλειας Πληροφοριών»

Γεώργιος Ι. Φύσαρης

ΑΜ: EMBA1659

Επιβλέπων Καθηγητής:

κ. Γεώργιος Μποχώρης, Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη Επιτροπής Αξιολόγησης:

κ. Δημήτριος Γεωργακέλλος, Καθηγητής Πανεπιστημίου Πειραιώς

κ. Αθάνασιος Κουρεμένος, Καθηγητής Πανεπιστημίου Πειραιώς

κ. Γεώργιος Μποχώρης, Καθηγητής Πανεπιστημίου Πειραιώς

Πειραιάς, 17 Ιουνίου 2021

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ ΓΙΑ ΣΤΕΛΕΧΗ

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

(περιλαμβάνεται ως ξεχωριστή (δεύτερη) σελίδα στο σώμα της διπλωματικής εργασίας)

«Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, στη Διοίκηση Επιχειρήσεων για Στελέχη : Ε-ΜΒΑ» με τίτλο
Η ΛΕΙΤΟΥΡΓΙΑ ΤΩΝ ΕΞΩΤΕΡΙΚΩΝ ΑΝΑΘΕΣΕΩΝ:Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ
OUTSOURCING OPERATIONS:THE CASE OF INFORMATION SECURITY
έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας, αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Υπογραφή Μεταπτυχιακού Φοιτητή/ τριας.....

Ονοματεπώνυμο.ΓΕΩΡΓΙΟΣ ΦΥΣΑΡΗΣ

Ημερομηνία.17/06/2021

Αφιερώνεται στην οικογένεια μου

για την κατανόηση και την αμέριστη συμπαράστασή της

Σημαντικοί όροι:

Εξωτερική ανάθεση, εξωτερικοί πάροχοι, πληροφοριακά συστήματα, ασφάλεια πληροφοριών, υπηρεσίες, λειτουργίες, κίνδυνοι, απειλές, ευπάθειες, διαχείριση, διαδικασίες, αξιολόγηση, κόστη, οφέλη, απαιτήσεις, απόδοση, επίδοση, εμπιστευτικότητα, ακεραιότητα, αξιοπιστία, εμπιστοσύνη, υποστήριξη, ποιότητα.

Περίληψη

Η Διπλωματική Εργασία που ακολουθεί εκπονήθηκε στα πλαίσια ολοκλήρωσης του μεταπτυχιακού προγράμματος σπουδών «Διοίκηση Επιχειρήσεων για Στελέχη», του τμήματος Οργάνωσης και Διοίκησης Επιχειρήσεων, του Πανεπιστημίου Πειραιώς.

Στην παρούσα εργασία, θα εστιάσουμε στην λειτουργία εξωτερικής ανάθεσης επικεντρώνοντας στα σημεία που αφορούν την ασφάλεια πληροφοριών. Η διασφάλιση της ασφάλειας, αποτελεί έναν από τους μεγαλύτερους κινδύνους για τους οργανισμούς. Αυτό οφείλεται στον υψηλό βαθμό εμπιστοσύνης των οργανισμών προς τους εξωτερικούς παρόχους, οι οποίοι είναι υπεύθυνοι εκτός από τη διαχείριση των ανατεθέντων υπηρεσιών και για τη διαχείριση των υπηρεσιών ασφάλειας. Η απόφαση εξωτερικής ανάθεσης θα πρέπει να βασίζεται σε τεκμηριωμένη ανάλυση και σε συγκεκριμένη μεθοδολογία. Οι οργανισμοί πριν αποφασίσουν να αναθέσουν σε κάποιον εξωτερικό πάροχο, μέρος ή σύνολο εσωτερικών υπηρεσιών, θα πρέπει να απαντήσουν σε πολύ σημαντικά ερωτήματα που αφορούν τους ίδιους, αλλά και τους εξωτερικούς παρόχους. Στα κεφάλαια που ακολουθούν, θα αναφερθούμε στη χρησιμότητα των εξωτερικών αναθέσεων και θα περιγράψουμε τα κόστη και τα οφέλη της διαδικασίας εξωτερικών αναθέσεων. Θα αναλύσουμε τους κινδύνους που καλούνται να αντιμετωπίσουν οι οργανισμοί και θα επεκταθούμε στις απειλές της ασφάλειας των πληροφοριών. Στη συνέχεια, θα επικεντρώσουμε στην διαδικασία που θα πρέπει να ακολουθείται για την αξιολόγηση καταλληλότητας των εξωτερικών αναθέσεων και θα ορίσουμε τις απαιτήσεις και τα κύρια κριτήρια επιλογής εξωτερικών παρόχων. Ολοκληρώνοντας, θα εστιάσουμε στην εξωτερική ανάθεση των λειτουργιών ασφάλειας και θα ορίσουμε τη διαδικασία που θα πρέπει να ακολουθούν οι οργανισμοί από την έναρξη μέχρι την ολοκλήρωση και τη λειτουργία μιας ασφαλούς εξωτερικής ανάθεσης.

Περιεχόμενα

Κατάλογος Πινάκων και Διαγραμμάτων

Διαγράμματα

Πίνακες

Κατάλογος Ακρωνυμίων

BCP Business Continuity Plan - Πλάνο Επιχειρηματικής Συνέχειας
BPI Bank Policy Institute - Ινστιτούτο Πολιτικής Τραπεζών
CBA Cost Benefit Analysis - Ανάλυση Κόστους Ωφέλειας
CBK Common Body of Knowledge - Κοινό Σώμα Γνώσης
CEO Chief Executive Officer - Γενικός Διευθυντής
CIO Chief Information Officer - Υπεύθυνος Πληροφοριών
CISO Chief Information Security Officer - Υπεύθυνος ασφάλειας
COO Chief Operations Officer - Επικεφαλής Λειτουργιών
CSO Chief Security Officer - Επικεφαλής ασφάλειας
DRP Disaster Recovery Plan - Πλάνο Αποκατάστασης από Καταστροφές
EVA Economic value added - Οικονομική Προστιθέμενη Αξία
ISO International Standards Organization - Διεθνής Οργανισμός Τυποποίησης
IRR Internal rate of Return - Εσωτερική Απόδοση Επένδυσης
MTBF Mean Time Between Failures - Μέσος Χρόνος Μεταξύ Βλαβών
MTTF Mean Time To Failure - Μέσος Χρόνος Αστοχίας
MTTR Mean Time To Repair - Μέσος Χρόνος Επιδιόρθωσης
NPV Net Present Value - Καθαρή Παρούσα Αξία
PKI Public Key Infrastructure - Υποδομή Δημόσιου Κλειδιού
PP Payback Period - Περίοδος Αποπληρωμής
RFI Request for Information - Αιτήμα για Πληροφορίες
RFP Request for Proposal - Αιτήμα για Προσφορά
ROI Return on Investment - Απόδοση Επένδυσης
SDLC Systems Development Life Cycle - Κύκλος Ζωής Συστήματος Ανάπτυξης
SLA Service Level Agreements - Συμφωνίες Επιπέδου Υπηρεσιών
SOW Statement of Work - Δήλωση Εργασιών

Πρόλογος

Στις μέρες μας, η επιχειρηματικότητα βασίζεται στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα της πληροφορίας, τα οποία αποτελούν κύρια δομικά στοιχεία της λειτουργίας των σύγχρονων επιχειρήσεων. Η διασφάλιση της ασφάλειας πληροφοριών σε ένα κλειστό περιβάλλον είναι σχετικά απλή. Δεν ισχύει όμως το ίδιο στις εξωτερικές αναθέσεις όπου, οι οργανισμοί για τον εξορθολογισμό των λειτουργιών και τη μείωση του κόστους επιλέγουν την ανάθεση των επιχειρηματικών διαδικασιών και υπηρεσιών, σε εξωτερικό πάροχο.

Οι περισσότεροι οργανισμοί αρχίζουν τώρα να εξετάζουν την ιδέα εκμετάλλευσης των εξωτερικών αναθέσεων. Δείχνουν πρόθυμοι να κατανοήσουν τον τρόπο με τον οποίο μπορεί να διασφαλιστεί η ασφάλεια των πληροφοριών, των απαιτήσεων συμμόρφωσης και της πνευματικής ιδιοκτησίας, εκμεταλλευόμενοι παράλληλα τα οφέλη της μείωσης του λειτουργικού κόστους. Το κύριο ερώτημα είναι, πόσο ασφαλής μπορεί να είναι μια εξωτερική ανάθεση για τον οργανισμό. Υπάρχουν πολλαπλά επίπεδα ασφάλειας από άποψη διαδικασιών και τεχνολογιών που μπορούν να εφαρμοστούν σε έναν οργανισμό ή εξωτερικό πάροχο ώστε να διασφαλιστούν οι επιχειρηματικές σχέσεις, τα δεδομένα και τη πνευματική ιδιοκτησία. Είναι εξίσου σημαντικό, οι οργανισμοί και οι εξωτερικοί πάροχοι να λαμβάνουν τα απαιτούμενα μέτρα προστασίας σε περίπτωση παραβίασης της ασφάλειας, εφόσον έχουν αξιολογήσει το επίπεδο ελέγχου κινδύνων των πληροφοριών και της φύσης των επιχειρηματικών σχέσεων.

Η εξωτερική ανάθεση έχει ρίσκο αναφορικά με τη διαρροή πληροφοριών, τη βιωσιμότητα και την φήμη ενός οργανισμού. Επομένως, η ανάθεση των επιχειρηματικών διαδικασιών και υπηρεσιών σε εξωτερικό πάροχο χρειάζεται να συνοδεύεται από εσωτερική υποστήριξη για την αποφυγή και τον μετριασμό των κινδύνων.

Εισαγωγή

Στις σημερινές αναπτυγμένες κοινωνίες, παρατηρείται το φαινόμενο της επιβίωσης των οργανισμών μέσα από ένα πολύπλοκο σύστημα υποστήριξης από εξειδικευμένες ειδικότητες και τεχνολογίες, για την παροχή αγαθών και υπηρεσιών. Στην παρούσα εργασία, εστιάζουμε στη λειτουργία εξωτερικής ανάθεσης υπηρεσιών επικεντρώνοντας στα σημεία που αφορούν στην ασφάλεια πληροφοριών. Ασχολούμαστε με τους παράγοντες κινδύνου που μπορούν να επηρεάσουν την απόφαση εξωτερικής ανάθεσης και, επεκτείνουμε στο υβριδικό μοντέλο εξωτερικής ανάθεσης στο οποίο η ευθύνη για την παροχή υπηρεσιών μοιράζεται μεταξύ του προσωπικού που διαθέτει ο οργανισμός και ο εξωτερικός πάροχος.

Η εξωτερική ανάθεση είναι μια επιλογή που πρέπει να βασίζεται σε τεκμηριωμένη ανάλυση. Ο οργανισμός που προτίθεται να προβεί σε χρήση εξωτερικών υπηρεσιών, πρέπει πρωτίστως να απαντήσει σε σημαντικά ερωτήματα για την επιλογή παρόχου. Με ποιόν τρόπο θα πραγματοποιηθεί η αξιολόγηση των υπηρεσιών και η επιλογή του παρόχου; Ποιές υπηρεσίες είναι κατάλληλες για εξωτερική ανάθεση; Ποιά είναι τα χαρακτηριστικά (μέγεθος, οικονομική υγεία, στελέχωση, τοποθεσία, χρησιμοποιούμενες τεχνολογίες) που θα πρέπει να διαθέτει ένας πάροχος για να μπορέσει να ανταποκριθεί στις ευθύνες που θα του ανατεθούν; Όλα τα παραπάνω, θα αναλυθούν στα κεφάλαια που ακολουθούν.

Διανύοντας μια εποχή υψηλού κινδύνου με ραγδαία αύξηση των απειλών και τρωτών σημείων σε λογισμικά, θα περίμενε κανείς την αγορά της ασφάλειας πληροφοριών και ειδικά της δικτυακής ασφάλειας στον κυβερνοχώρο, να ακμάζει. Η πραγματικότητα όμως είναι τελείως διαφορετική. Πολλές εταιρείες λογισμικού, εξοπλισμού και υπηρεσιών ασφάλειας αγωνίζονται να επιβιώσουν. Αυτό συμβαίνει λόγο του έντονου ανταγωνισμού που κυρίως καταλήγει στον αφανισμό αδύναμων εταιριών από τις ισχυρότερες. Υπάρχει γενικά μια οικονομική δυσφορία παρά την επιτακτική ανάγκη δημιουργίας ασφαλέστερου περιβάλλοντος. Επικερδής επιχειρήσεις παροχής υπηρεσιών, έχουν αποτύχει να επιβιώσουν στην αγορά και έχουν πτωχεύσει. Οι χαμηλοί προϋπολογισμοί που επενδύονται στην ασφάλεια των πληροφοριών εταιριών, παρουσιάζουν καθοδικές τάσεις. Διοικήσεις εταιριών, προτιμούν την ανάληψη κινδύνων λόγω του χαμηλού κεφαλαίου επένδυσης παρόλο που, η ιστορία των περιστατικών ασφάλειας έχει θέσει υπό αμφισβήτηση τέτοιου είδους αποφάσεις.

Στα κεφάλαια που ακολουθούν, θα περιγράψουμε τη χρησιμότητα των εξωτερικών αναθέσεων στις σύγχρονες επιχειρήσεις και θα επεκταθούμε στα κόστη και στα οφέλη της διαδικασίας των εξωτερικών αναθέσεων. Στην συνέχεια, θα αναλύσουμε τους κινδύνους και τις απειλές ασφάλειας των πληροφοριών και θα επικεντρώσουμε στη διαδικασία αξιολόγησης εξωτερικών αναθέσεων καθώς και στον καθορισμό των κύριων απαιτήσεων και κριτηρίων επιλογής εξωτερικών παρόχων. Τέλος, θα περιγράψουμε την εξωτερική ανάθεση των υπηρεσιών ασφάλειας και θα ορίσουμε τη μεθοδολογία που θα πρέπει να ακολουθούν οι οργανισμοί από την έναρξη μέχρι και τη λειτουργία μιας ασφαλούς εξωτερικής ανάθεσης.

Πριν προχωρήσουμε στο πρώτο κεφάλαιο, είναι σημαντικό να περιγράψουμε τα σημεία στα οποία διασταυρώνεται η εξωτερική ανάθεση με την ασφάλεια πληροφοριών.

Η ανάθεση εξωτερικής ανάθεσης από τον εξωτερικό πάροχο

Στην περίπτωση αυτή, ο εξωτερικός πάροχος αναθέτει υπηρεσίες σε μία ή περισσότερες εταιρείες παροχής υπηρεσιών χωρίς αυτό να συνεπάγεται με την ενημέρωση του τελικού πελάτη. Απαιτείται ιδιαίτερη προσοχή από τους οργανισμούς, προκειμένου να εξασφαλιστεί από τον εξωτερικό πάροχο η διασφάλιση της ασφάλειας των πληροφοριών σε κάθε στάδιο επεξεργασίας αυτών από τους υπεργολάβους.

Η διασφάλιση της ασφάλειας

Η διασφάλιση της ασφάλειας σχετίζεται με το επίπεδο ασφάλειας των προσφερόμενων υπηρεσιών ασφάλειας από τους εξωτερικούς παρόχους. Για παράδειγμα, στον φυσικό κόσμο, πρέπει να διασφαλιστεί ότι οι φύλακες δεν έχουν ποινικό μητρώο ενώ στον ηλεκτρονικό κόσμο, θα πρέπει να ελεγχθεί το επίπεδο ασφάλειας του τείχους προστασίας ενός συγκεκριμένου κατασκευαστή. Η διασφάλιση της ασφάλειας αποτελεί τον μεγαλύτερο από όλους τους κινδύνους, δεδομένου του υψηλού βαθμού εμπιστοσύνης προς τους εξωτερικούς παρόχους οι οποίοι, είναι υπεύθυνοι για τη διαχείριση των υπηρεσιών ασφάλειας.

Η ανάθεσης της ασφάλειας σε εξωτερικό πάροχο

Στο σημείο αυτό αναφερόμαστε στους εξωτερικούς παρόχους υπηρεσιών ασφάλειας. Η ανάθεση της ασφάλειας σε έναν εξωτερικό πάροχο περιλαμβάνει έναν μεγάλο αριθμό προσφερόμενων υπηρεσιών τους οποίους θα αναφέρουμε στη συνέχεια. Οι κίνδυνοι που σχετίζονται με την υπηρεσία αυτή, μπορούν να επιφέρουν μεγαλύτερους κινδύνους στις δραστηριότητες ενός οργανισμού είτε από τον εξωτερικό πάροχο ή, από ανάθεση υπηρεσιών του εξωτερικού παρόχου σε υπεργολάβους.

Η ασφάλεια της εξωτερικής ανάθεσης

Όπως αναφέραμε και παραπάνω, προκύπτουν αρκετά θέματα ασφάλειας κατά την ανάθεση υπηρεσιών σε εξωτερικό πάροχο και δη, όταν επιλέγεται από τον τελευταίο η επικουρική συμμετοχή υπεργολάβων για την ολοκλήρωση ενός έργου. Έτσι λοιπόν, προκειμένου να διασφαλιστεί η ασφάλεια των πληροφοριών και δεδομένων του οργανισμού ο εξωτερικός πάροχος, υποχρεούται να αντιμετωπίσει σοβαρά και υπεύθυνα τους ενδεχόμενους κινδύνους γνωρίζοντας τον τρόπο αντιμετώπισής τους. Είναι πολύ εύκολο να χαθεί ο έλεγχος με τις νέες τεχνολογίες λογισμικών και δικτύων, κυρίως λόγω της εμπλοκής πολλών απομακρυσμένων παρόχων που ενδέχεται να είναι άγνωστοι στον τελικό πελάτη.

1. Βιβλιογραφική Ανασκόπηση

Καθώς το επιχειρηματικό περιβάλλον σε παγκόσμιο επίπεδο κινείται προς μια οικονομία βασισμένη στην γνώση, η τεχνολογία των πληροφοριών και οι τηλεπικοινωνίες αυξάνουν την πολυπλοκότητα, με αποτέλεσμα οι οργανισμοί να αντιμετωπίζουν ολοένα και περισσότερες δυσκολίες στην διαχείριση των υπηρεσιών πληροφορικής. Οι οργανισμοί με τις εξωτερικές αναθέσεις, προσπαθούν να αποκτήσουν ανταγωνιστικό πλεονέκτημα μειώνοντας τα κόστη και εστιάζοντας το εσωτερικό προσωπικό τους στις κύριες επιχειρησιακές δραστηριότητές τους. Ωστόσο, ο έλεγχος της διαχείρισης και η ασφάλεια των δεδομένων από τους εξωτερικούς παρόχους ενέχει διάφορους κινδύνους και κρυφά κόστη για τους οργανισμούς. Ο Victor Wheatman των υπηρεσιών στρατηγικής ασφάλειας πληροφοριών του Ομίλου Gartner (Gartner, Inc, 2020), το 1997 είχε αναφέρει ότι «οι επιχειρήσεις αντιμετωπίζουν αυξανόμενο κίνδυνο για την ασφάλεια των πληροφοριών». Συγκεκριμένα, εκτός από τις τεχνολογικές ευπάθειες, αντιμετωπίζουν και αυξημένο κίνδυνο και λόγω της απουσίας επαρκών μέτρων ασφαλείας.

Η εξωτερική ανάθεση υπηρεσιών πληροφορικής έχει λάβει μεγάλη προσοχή τόσο στον ιδιωτικό όσο και στον δημόσιο (Buck-Lew, 1992) (Currie, 1996). Η ορολογία της εξωτερικής ανάθεσης υπηρεσιών πληροφορικής χρησιμοποιήθηκε για πρώτη φορά το 1989 όταν η εταιρεία Kodak αποφάσισε να συνάψει συμφωνίες εξωτερικής ανάθεσης με τρεις μεγάλους εξωτερικούς παρόχους πληροφορικής (Loh & Venkatraman, 1992b) (De Looff, 1995) (Slaughter & Ang, 1996).

Η παγκόσμια αγορά για τη βιομηχανία εξωτερικής ανάθεσης υπηρεσιών πληροφορικής έχει φτάσει τα 92,5 δισεκατομμύρια δολάρια το 2019 (Statista, 2020) και οι αναλυτές της Technavio (Technavio, 2020) προβλέπουν θα αυξάνεται ετησίως με ρυθμό περίπου 5% την επόμενη πενταετία αγγίζοντας τα 98 δισεκατομμύρια δολάρια το 2020.

Οι Loh και Venkatraman (Loh, L.; Venkatraman, N., 1992a) ορίζουν την εξωτερική ανάθεση υπηρεσιών πληροφορικής ως «τη συμβολή εξωτερικών προμηθευτών στους φυσικούς ή / και στους ανθρώπινους πόρους που σχετίζονται με το σύνολο ή με μέρος της υποδομής πληροφορικής ενός οργανισμού». Η εξωτερική ανάθεση υπηρεσιών πληροφορικής θεωρείται σημαντική διοικητική καινοτομία διότι προκαλεί σημαντική αλλαγή στον τρόπο διακυβέρνησης, στις εσωτερικές διαδικασίες των χρηστών και στις επιχειρησιακές λειτουργίες που χρησιμοποιούνται για την αντιμετώπιση του εξωτερικού περιβάλλοντος.

Ο Jack (Jack, 1992) ορίζει τη σημασία της αντιμετώπισης της «ασφάλειας πληροφοριών» στο πλαίσιο της εξωτερικής ανάθεσης υπηρεσιών πληροφορικής. Ο Radcliff (Radcliff, 2000) υποστηρίζει ότι η μεγαλύτερη ανησυχία των οργανισμών κατά

την ανάθεση υπηρεσιών σε εξωτερικό πάροχο προκύπτει από το «ποιος έχει πρόσβαση στα δεδομένα και με ποιόν τρόπο τα προστατεύει». Στο ίδιο πνεύμα, ο Greenemeier (Greenemeier, 2001) παρατηρεί ότι οι υπηρεσίες ασφαλείας εξωτερικής ανάθεσης είναι ένα «αμφισβητούμενο ζήτημα» επειδή οι οργανισμοί διστάζουν να αναθέσουν στους παρόχους υπηρεσιών πληροφορικής τα κλειδιά για τα συστήματα πληροφορικής και τα δεδομένα τους.

Η αυξημένη έκθεση των πληροφοριακών συστημάτων μέσω του διαδικτύου αυξάνει όλο και περισσότερο τη ζήτηση των υπηρεσιών ασφάλειας πληροφοριών. Ο Vijayan (Vijayan, 2001) επισημαίνει ότι ολοένα αυξανόμενος αριθμός παρόχων υπηρεσιών ασφάλειας μπορεί να καλύψει αυτή τη σημαντική ζήτηση. Οι υπηρεσίες ασφαλείας περιλαμβάνουν τη διαχείριση τείχους προστασίας και των εικονικών ιδιωτικών δικτύων, την εκτέλεση ανάλυσης ευπαθειών, την ανίχνευση εισβολών, την προστασία κατά των ιών και, σε ορισμένες περιπτώσεις, τον σχεδιασμό, την εφαρμογή και τη διαχείριση αρχιτεκτονικών ασφαλείας. Τονίζει επίσης, ότι οι κύριες αιτίες της ζήτησης για αυτές τις υπηρεσίες είναι η έλλειψη εκπαιδευμένων επαγγελματιών ασφάλειας και η πολυπλοκότητα της εφαρμογής και της διατήρησης αρχιτεκτονικών ασφαλείας στους οργανισμούς.

Σε μια παρόμοια ανάλυση, οι Peterson, Brown και Maw (Peterson & Maw, 2002) ορίζουν τις τρεις βασικές ιδιότητες ασφάλειας πληροφοριών:

- Ακεραιότητα: συλλογή και διατήρηση ακριβών πληροφοριών και αποφυγή κακόβουλης τροποποίησης.
- Διαθεσιμότητα: παροχή πρόσβασης στις πληροφορίες όταν και όπου είναι επιθυμητό.
- Εμπιστευτικότητα: αποφυγή αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένα ή ανεπιθύμητα άτομα.

Περαιτέρω και σύμφωνα με το πρότυπο ISO 27001:2013 (ISO/IEC 27001:2013, 2020) , η ασφάλεια των πληροφοριών βασίζεται στη διατήρηση των παρακάτω πτυχών:

- Εμπιστευτικότητα: εξασφάλιση ότι οι πληροφορίες είναι προσβάσιμες μόνο σε εκείνους που έχουν άδεια πρόσβασης.
- Ακεραιότητα: διασφάλιση της ακρίβειας και πληρότητας των πληροφοριών και των μεθόδων επεξεργασίας.
- Διαθεσιμότητα: εξασφάλιση ότι οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε πληροφορίες και σχετικά στοιχεία όταν απαιτείται.

Ο βαθμός στον οποίο διατηρούνται αυτές οι πτυχές πρέπει να βασίζεται στις απαιτήσεις ασφάλειας του κάθε οργανισμού. Οι απαιτήσεις ασφάλειας, προκύπτουν μέσω της ανάλυσης των κινδύνων και των επιπτώσεων. Η διαχείριση της ασφάλειας, αφορά τις ενέργειες που απαιτούνται για τη διατήρηση κινδύνων σε διαχειρίσιμο επίπεδο. Η ασφάλεια δεδομένων αναφέρεται στο επίπεδο προστασίας που παρέχεται για την αποτροπή μη εξουσιοδοτημένης πρόσβασης. Όπως σημειώνεται από τους Fink (Fink, D., 1994) και Sherwood (Sherwood, J. , 1997), η ασφάλεια πληροφοριών είναι ένας τομέας που συχνά παραμελείται στις εξωτερικές αναθέσεις. Η ασφάλεια πληροφοριών καλύπτει τόσο την ασφάλεια δεδομένων όσο και τον προγραμματισμό επιχειρησιακής συνέχειας (Lee, 1995). Η ασφάλεια δεδομένων στοχεύει στη διασφάλιση της ακεραιότητας και της ιδιωτικότητας των δεδομένων που ανήκουν στον οργανισμό, ενώ η επιχειρησιακή συνέχεια στοχεύει στα μέτρα που διασφαλίζουν την ταχεία αποκατάσταση των κανονικών επιχειρησιακών λειτουργιών σε περίπτωση εμφάνισης προβλημάτων που σχετίζονται με την πληροφορική (π.χ. μόλυνση από ιούς, καταστροφή δεδομένων, ξαφνική διακοπή της λειτουργίας συστημάτων πληροφορικής).

Όταν η λειτουργία των πληροφοριακών συστημάτων ανατίθεται σε εξωτερικό πάροχο υπηρεσιών, ο οργανισμός χάνει τον πλήρη έλεγχο της ασφάλειας των πληροφοριών του (Lee, 1995) . Για τους επαγγελματίες και ερευνητές πληροφορικής, ο όρος «εξωτερική ανάθεση ασφάλειας» έχει διπλή έννοια. Την ασφάλεια πληροφοριών και δεδομένων κατά τη μετάδοση, αποθήκευση και τη μεταφορά, και τις ρυθμίσεις ασφαλείας και τα μέτρα που έχουν εφαρμοστεί από τους εξωτερικούς παρόχους. Στην παρούσα διπλωματική εργασία θα βασιστούμε στις δύο αυτές έννοιες, για να απαντήσουμε στο πρόβλημα της ασφάλειας των εξωτερικών αναθέσεων.

2. Χρησιμότητα των Εξωτερικών Αναθέσεων

Όλο και περισσότερες επιχειρήσεις σήμερα επιλέγουν να αναθέσουν σε τρίτους σημαντικές εσωτερικές λειτουργίες πληροφορικής όπως τη διαχείριση του δικτύου, των υπολογιστών, του λογισμικού αλλά και των συστημάτων ασφάλειας. Αναζητούν εξωτερικούς παρόχους με σκοπό να μεταφέρουν την ευθύνη εκτός του οργανισμού, να μειώσουν τα λειτουργικά έξοδα, να εξοικονομήσουν κεφάλαια, να αυξήσουν την παραγωγικότητα (εστιάζοντας σε κύριες δραστηριότητες), να αποκτήσουν πρόσβαση σε νέες τεχνολογίες, να ελευθερώσουν εσωτερικούς πόρους, να επιταχύνουν εργασίες ανασχεδιασμού και να αποφύγουν την εσωτερική διαχείριση. Από όλα τα παραπάνω, η εξοικονόμηση κόστους συνεχίζει να αποτελεί το κυριότερο κίνητρο εξωτερικών αναθέσεων για τους περισσότερους οργανισμούς (T.D. Clark Jr., 1992) (Grover, Cheon, & Teng, 1994) (Saunders, Gebelt, & Hu, 1997) (Robinson & Kalakota, 2004).

Πολλές φορές η εξωτερική ανάθεση δεν αποφασίζεται με τα σωστά κριτήρια και τους απαραίτητους όρους και ως αποτέλεσμα, μέρος της ευθύνης παραμένει στον οργανισμό. Αν συμβεί κάποιο περιστατικό ασφάλειας και διαπιστωθεί ότι δεν τηρούνταν οι απαιτούμενες δικλείδες ασφάλειας από τον εξωτερικό πάροχο, υπεύθυνος είναι ο ίδιος ο οργανισμός. Σε άλλες περιπτώσεις οι οργανισμοί θεωρούν ότι με την εξωτερική ανάθεση εξοικονομούν χρήματα, αλλά στην πραγματικότητα υπάρχουν κρυφά κόστη τα οποία δεν έχουν υπολογιστεί και αλλάζουν εντελώς τα δεδομένα. Επίσης, υπάρχουν κόστη και συνέπειες που μπορεί να προκύψουν με την πιθανή απομάκρυνση του οργανισμού από τον εξωτερικό πάροχο.

Οι οργανισμοί πριν αποφασίσουν να αναθέσουν σημαντικές εσωτερικές λειτουργίες τους σε εξωτερικό πάροχο θα πρέπει να υπολογίσουν όλες αυτές τι παραμέτρους. Είναι επίσης απαραίτητο να έχουν ένα συγκεκριμένο πλάνο ενεργειών για τις περιπτώσεις έκτακτης ανάγκης. Οι εξωτερικές αναθέσεις θεωρείται ότι βοηθάνε τους οργανισμούς απαλλάσσοντάς τους από εσωτερικές λειτουργίες για να επικεντρωθούν στις κύριες επιχειρηματικές δραστηριότητές τους. Η ανάθεση όμως μπορεί να μην έχει τα αναμενόμενα αποτελέσματα για τον οργανισμό.

Η απόφαση για την εξωτερική ανάθεση είναι συχνά πολύ υποκειμενική, ακόμη και στις περιπτώσεις που έχει διενεργηθεί από τον οργανισμό εκτεταμένη ποσοτική ανάλυση και μελέτη. Για τον προσδιορισμό του κόστους μιας εξωτερικής ανάθεσης οι οργανισμοί πολλές φορές, βασίζονται μόνο στα οικονομικά οφέλη της ανάθεσης και το αποτέλεσμα που θα προκύψει μπορεί να είναι εσφαλμένο. Είναι εξαιρετικά δύσκολο να υπολογιστούν με ακρίβεια οι τιμές των άυλων ωφελειών και για αυτόν τον λόγο οι αποτιμήσεις συχνά είναι υποκειμενικές. Πριν εξεταστεί οποιοδήποτε σενάριο εξωτερικής ανάθεσης θα

πρέπει να έχουν συγκεντρωθεί και καταγραφεί οι κύριοι λόγοι για τους οποίους κρίνεται η εξωτερική ανάθεση ως η καλύτερη επιλογή. Αυτοί οι λόγοι μπορεί να είναι προφανείς, αναξιόπιστοι, ασαφείς και αμφισβητήσιμοι (Schniederjans, 2007). Στην συνέχεια θα επεκταθούμε στα κύρια κριτήρια που μπορούν να υποστηρίξουν μια απόφαση εξωτερικής ανάθεσης τα οποία συνδέονται με το κόστος, τις επιδόσεις, την ασφάλεια, την τεχνογνωσία, και την υποστήριξη.

2.1 Εξοικονόμηση κόστους

Η εξοικονόμηση χρημάτων βρίσκεται πολύ κοντά στην κορυφή της λίστας των κριτηρίων επιλογής εξωτερικών αναθέσεων. Είναι αρκετά δύσκολο για έναν οργανισμό να επιλέξει μια υπηρεσία που προσφέρεται από κάποιον εξωτερικό πάροχο και είναι πιο δαπανηρή, σε σχέση με μια υπηρεσία η οποία εκτελείται εσωτερικά. Σε αντίθεση, στις περιπτώσεις που υπάρχει σημαντική διαφορά στον τύπο ή στην ποιότητα των προσφερόμενων υπηρεσιών, η επιλογή εξωτερικής ανάθεσης είναι πολύ πιο εύκολη για τους οργανισμούς (Power, 2006).

2.1.1 Εργασία

Τις περισσότερες φορές, το μεγαλύτερο κόστος της παροχής υπηρεσιών είναι το κόστος εργασίας. Για τον υπολογισμό του κόστους εργασίας εσωτερικά του οργανισμού υπάρχουν διάφορες κατηγορίες κόστους. Αυτές οι κατηγορίες συνήθως είναι οι μισθοί, τα επιδόματα και οι φόροι μισθοδοσίας. Για τους εργολάβους και τους συμβούλους, υπάρχει ωριαία ή ημερήσια βασική τιμή, με πριμοδότηση για υπερωρίες. Για το εσωτερικό προσωπικό, πρέπει να προστεθούν οι διακοπές, καθώς και οι ημέρες ασθένειας, ενώ στους εργολάβους και συμβούλους αυτά περιλαμβάνονται στην συμφωνημένη τιμή. Διάφορα γενικά έξοδα, όπως εκείνα που σχετίζονται με τις εγκαταστάσεις που χρησιμοποιεί το προσωπικό, το διοικητικό κόστος και το κόστος διαχείρισης θα πρέπει επίσης να υπολογιστούν. Στις περιπτώσεις όπου οι εργολάβοι και οι σύμβουλοι συμμετέχουν στην υποστήριξη εσωτερικών λειτουργιών λόγω έλλειψης εσωτερικών πόρων του οργανισμού, το κόστος των υπηρεσιών τους θα πρέπει να συνυπολογιστεί.

Στον Πίνακας 1 απεικονίζεται το εσωτερικό και εξωτερικό προσωπικό που χρησιμοποιείται στις εσωτερικές και εξωτερικές λειτουργίες ενός οργανισμού. Από τον πίνακα, συμπεραίνουμε εύκολα ότι κάποιο μείγμα από το εσωτερικό και εξωτερικό προσωπικό είναι απαραίτητο ανεξάρτητα από την φύση της υπηρεσίας.

Πίνακας 1: *Εσωτερικό και εξωτερικό προσωπικό ανά τύπο υπηρεσίας*

	Λειτουργία εντός του οργανισμού	**Λειτουργία σε εξωτερικό πάροχο**

Εσωτερικό προσωπικό	Εργαζόμενοι πλήρους και μερικής απασχόλησης	Ελάχιστοι (υπεύθυνοι για την επικοινωνία με τους εξωτερικούς συνεργάτες)
Εξωτερικό προσωπικό	Ορισμένοι σύμβουλοι και εργολάβοι	Όλοι είναι σύμβουλοι και εργολάβοι.

Εκτός από τα κόστη που αποδίδονται άμεσα σε πρόσωπα, άλλες δαπάνες μπορούν να αποδοθούν γενικότερα στον ρόλο που έχει ένα συγκεκριμένο πρόσωπο και στις εργασίες που πραγματοποιεί σε σχέση με τον ρόλο αυτό. Τα πιο προφανή από αυτά τα κόστη, είναι έξοδα ταξιδιού που περιλαμβάνουν την μεταφορά, την στέγαση, τα γεύματα, και τα έξοδα που σχετίζονται με την ψυχαγωγία των πελατών. Οι εταιρείες συμβούλων συνήθως χρεώνουν τα έξοδα ταξιδιού που σχετίζονται με έργα ή υπηρεσίες προσθέτοντας και διαχειριστικά κόστη σε αυτά. Αξίζει να σημειωθεί ότι, τα έξοδα μετακίνησης σε έναν κύριο τόπο επιχειρηματικής δραστηριότητας επιβαρύνουν γενικά τους εργαζομένους. Σε αντίθεση αυτού, οι εξωτερικοί συνεργάτες χρεώνουν την μετακίνηση στους πελάτες τους ανεξάρτητα από την απόσταση που απαιτείται να διανύσουν. Για τους υπεράκτιους παρόχους υπηρεσιών, το ταξιδιωτικό στοιχείο μπορεί να είναι σημαντικό, όχι μόνο όσον αφορά στα αεροπορικά εισιτήρια και στα καταλύματα, αλλά τον απαιτούμενο χρόνο για το ταξίδι, το οποίο χρεώνεται στον πελάτη.

Άλλα έξοδα που σχετίζονται με τους εργαζόμενους περιλαμβάνουν τα έξοδα εκπαίδευσης και συμμετοχής σε σεμινάρια και συνέδρια. Τα έξοδα περιλαμβάνουν εκείνα που αποδίδονται άμεσα σε ταξίδια, αλλά και το κόστος του χαμένου χρόνου που δεν εργάζονται κατά τη διάρκεια της περιόδου κατάρτισης. Ωστόσο, η δραστηριότητα της εκπαίδευσης πιθανότατα θα αποδώσει περισσότερο από μόνη της μέσω της υψηλότερης παραγωγικότητας και της αποτελεσματικότητας και μέσω νέων ευκαιριών, με στόχο τη δημιουργία εσόδων και την μείωση του κόστους. Οι εταιρείες διαθέτουν συχνά τυπικά πρότυπα για την εκπαίδευση, όπως η απαίτηση συγκεκριμένων ημερών κατάρτισης ετησίως ή τον ελάχιστο αριθμό μονάδων συνεχιζόμενης εκπαίδευσης. Για τις εταιρείες παροχής συμβουλών, οι δαπάνες αυτές είναι ενσωματωμένες στις χρεώσεις τους.

Επίσης, υπάρχουν εφάπαξ έξοδα ανά άτομο, όπως αυτά για την πρόσληψη και την απόλυση. Μπορεί να είναι πιο δύσκολο για έναν οργανισμό να προσλαμβάνει ειδικούς από ότι για έναν πάροχο υπηρεσιών ή μια εταιρεία παροχής συμβουλών, δεδομένου ότι, ο τελευταίος μπορεί να προσφέρει πιο ενδιαφέρουσα εργασία, με μεγαλύτερη ευθύνη, με περισσότερη ποικιλία εργασίας και περιβάλλοντος και καλύτερη πορεία ανάπτυξης και σταδιοδρομίας. Για τον λόγο αυτόν, οι πάροχοι υπηρεσιών μπορεί να είναι σε θέση

να εξοικονομήσουν τα κόστη αυτά εφόσον μπορούν να προσφέρουν ελκυστικότερο περιβάλλον εργασίας και διαθέτουν χαμηλότερο κύκλο ανακύκλωσης προσωπικού. Τα διάφορα κόστη που σχετίζονται με το εργατικό δυναμικό και ο τρόπος με τον οποίο υπολογίζονται και κατανέμονται για τις υπηρεσίες που παρέχονται εσωτερικά και εξωτερικά του οργανισμού παρουσιάζονται στον Πίνακας 2. Η κύρια διαφορά είναι ότι για τους εσωτερικούς εργαζόμενους οι κατηγορίες μεμονωμένων δαπανών πρέπει να καθοριστούν και να ποσοτικοποιηθούν, ενώ για τους εξωτερικούς παρόχους υπηρεσιών οι περισσότερες κατηγορίες συμπεριλαμβάνονται στην τιμή ανθρωποώρας. Φυσικά, ο εξωτερικός πάροχος υπηρεσιών πρέπει να ακολουθήσει την ίδια λογική για τον ποσοτικό προσδιορισμό των εσωτερικών του δαπανών προκειμένου να υπολογίσει την τιμή χρέωσης (Amant, 2009) (Schniederjans, 2007).

Πίνακας 2: *Κόστη εργασίας ανά τύπο ανάθεσης*

	Εσωτερική ανάθεση	**Εξωτερική ανάθεση**
Τρέχοντα κόστη		
Μισθοί	Συγκεκριμένο κόστος	Περιλαμβάνεται στην συμφωνημένη τιμή
Υπερωρίες	Ποσοστό μισθού (π.χ. 25%)	
Προνόμια	Ποσοστό μισθού (π.χ. 20 %)	Περιλαμβάνεται στην συμφωνημένη τιμή
Φόροι	Ανάλογα με τον νόμο	
Ταξίδια και διασκέδαση	Συγκεκριμένο κόστος	
Εκπαίδευση	Συγκεκριμένο κόστος	Περιλαμβάνεται στην συμφωνημένη τιμή
Παροχές (αυτοκίνητο, κινητό, laptop κτλ.)	Συγκεκριμένο κόστος	Περιλαμβάνεται στην συμφωνημένη τιμή ή χρεώνεται με βάση κάποια κριτήρια (π.χ. αποστάσεις)
Εφάπαξ κόστη		
Πρόσληψη	Συγκεκριμένο κόστος	Περιλαμβάνεται στην συμφωνημένη τιμή
Απόλυση	Συγκεκριμένο κόστος	Περιλαμβάνεται στην συμφωνημένη τιμή
Εγκατάσταση	Συγκεκριμένο κόστος	Περιλαμβάνεται στην συμφωνημένη τιμή
Επιπλέον κόστη		
Εγκαταστάσεις	Συγκεκριμένο κόστος	Περιλαμβάνεται στην συμφωνημένη τιμή
Διαχείριση	Συγκεκριμένο κόστος	Χρεώνεται συνήθως ποσοστιαία (π.χ. +20% στην συμφωνημένη τιμή)

2.1.2 Υπολογιστές, εξοπλισμός δικτύωσης και λογισμικό

Η σύγκριση μεταξύ των δαπανών για εξοπλισμό και λογισμικό που χρησιμοποιούνται εσωτερικά και παρέχονται είτε απευθείας, όπως στην περίπτωση ενός παρόχου

υπηρεσιών εφαρμογών είτε ενσωματώνονται σε μια υπηρεσία, όπως για έναν πάροχο επιχειρηματικών υπηρεσιών, είναι αρκετά δύσκολη διότι αυτά τα προϊόντα μπορούν να αποκτηθούν με ποικίλους τρόπους. Η κύρια διαφορά του κόστους έγκειται στο αν ο οργανισμός επιλέξει να αγοράσει τον εξοπλισμό ή αν θα επιλέξει να τον μισθώσει. Η μίσθωση αντικατοπτρίζεται ως επαναλαμβανόμενο περιοδικό κόστος, συνήθως μηνιαίο. Για τον αγορασμένο εξοπλισμό η εταιρεία θα αποσβέσει το περιουσιακό στοιχείο σε έναν συγκεκριμένο αριθμό ετών. Είτε έτσι είτε αλλιώς, το κόστος περιλαμβάνει τις τρέχουσες χρεώσεις συντήρησης και ενδεχομένως, χρεώσεις ανά παραγόμενη μονάδα, όπως στην περίπτωση ενός εκτυπωτή. Τα τέλη εγκατάστασης και απεγκατάστασης θα πρέπει επίσης να υπολογιστούν.

Το λογισμικό συνήθως δεν μπορεί να αγοραστεί. Αντιθέτως, ο αγοραστής καλείται να πληρώσει ένα περιοδικό τέλος αδείας συν ένα τέλος συντήρησης. Μπορεί ή όχι, να υπάρχουν τέλη εγκατάστασης και απεγκατάστασης για τα προϊόντα λογισμικού, αλλά υπάρχουν σημαντικές χρεώσεις για τις επαγγελματικές υπηρεσίες παραμετροποίησης. Η τιμολόγηση του λογισμικού ποικίλλει σημαντικά, κυμαινόμενη από το κόστος των απεριόριστων αδειών χρήσης μέχρι τις πολύ συγκεκριμένες άδειες, ανάλογα με το μέγεθος και τον αριθμό των κεντρικών συστημάτων στα οποία εκτελείται το λογισμικό, τον αριθμό των τελικών χρηστών και άλλους παράγοντες. Τα δίκτυα επιφέρουν πρόσθετα έξοδα κατά την παραγγελία τους, την εγκατάσταση, την συντήρηση και την αφαίρεσή τους. Γενικά χρεώνονται με ένα προκαθορισμένο τέλος ανά μήνα ή με βάση τις μονάδες χρήσης. Η εύκολη πρόσβαση στο Διαδίκτυο και ο πολλαπλασιασμός των φορητών ασύρματων συσκευών έχει αλλάξει τον τρόπο χρήσης και χρέωσης των επικοινωνιακών τεχνολογιών.

Όλα τα παραπάνω δείχνουν ότι υπάρχουν σίγουρα ευκαιρίες για ποσοτικές εκπτώσεις βάσει του όγκου των προϊόντων που αποκτήθηκαν. Η έκπτωση μπορεί να ισχύσει είτε για τον εξωτερικό πάροχο υπηρεσιών είτε για τον πελάτη, αλλά συχνά ένας πάροχος υπηρεσιών θα αναζητήσει μια καλύτερη συμφωνία από τον πελάτη, ειδικά για προϊόντα ειδικού τύπου. Στους εξωτερικούς παρόχους υπηρεσιών, το κόστος εξοπλισμού, λογισμικού, υπηρεσιών και δικτύων συνήθως μεταφέρεται σε καθορισμένη τιμή ανεξάρτητα από το αν το κόστος θα αλλάξει με την πάροδο του χρόνου ή ο εξοπλισμός θα έχει υποτιμηθεί πλήρως. Στις υπεράκτιες εξωτερικές αναθέσεις, το κόστος των τηλεπικοινωνιών μπορεί να είναι σημαντικό εξαιτίας όχι μόνο των σχετικών αποστάσεων, αλλά και λόγω της αυξημένης ανάγκης επικοινωνίας εξαιτίας των διαφορετικών χρονικών ζωνών. Επιπλέον, διαφορετικές χώρες έχουν διαφορετικές απαιτήσεις εξοπλισμού, τιμολόγια τηλεπικοινωνιών και κανονισμούς. Στην εσωτερική χρήση, το κόστος μπορεί

να ποικίλλει ευρέως με βάση όχι μόνο τον τρόπο με τον οποίο τα προϊόντα έχουν αποκτηθεί, αλλά και από το αν μοιράζονται τις ίδιες εφαρμογές (Halvey & Melby, 2007).

2.1.3 Εγκαταστάσεις

Οι άνθρωποι και ο εξοπλισμός χρειάζονται χώρο, έπιπλα, θέρμανση, ψύξη, ηλεκτρική ενέργεια, φως και αέρα. Ειδικότερα, απαιτούν όχι μόνο ένα ρυθμιζόμενο φυσικό περιβάλλον, αλλά και προμήθειες, τρόφιμα, ποτά, εγκαταστάσεις μπάνιου και πολλά άλλα. Ο χώρος, τα εξαρτήματα, ο εξοπλισμός και τα έπιπλα μπορούν να νοικιαστούν ή να αγοραστούν και, εάν αγοραστούν, αποσβένονται για φορολογικούς σκοπούς επί σειρά ετών. Τα κτίρια αποσβένονται επί δεκαετίες σε σχέση με τον υπόλοιπο εξοπλισμό. Εάν αγοραστεί ένα κτίριο, ο ιδιοκτήτης πρέπει να πληρώσει φόρους ακίνητης περιουσίας και τους λογαριασμούς κοινής ωφέλειας, όπως η ηλεκτρική ενέργεια, το φυσικό αέριο και το νερό, καθώς και τη συντήρηση και την υποστήριξη των εγκαταστάσεων, συμπεριλαμβανομένων των δαπανών προσωπικού και του προσωπικού ασφάλειας. Μερικές φορές το κόστος των υπηρεσιών κοινής ωφέλειας και συντήρησης μεταφέρεται στον ενοικιαστή, ενώ σε άλλες περιπτώσεις συμπεριλαμβάνεται στο ενοίκιο. Όλα αυτά τα έξοδα εγκαταστάσεων μπορούν να υπολογιστούν εύκολα στις εσωτερικές αναθέσεις (Halvey & Melby, 2005).

2.1.4 Άλλα κόστη υποδομών

Στο κόστος πρέπει να συμπεριλαμβάνονται και στοιχεία όπως η ασφάλεια, η επιχειρησιακή συνέχεια του οργανισμού και η ανάκαμψη μετά από καταστροφή. Κάποια μερίδα αυτών των εξόδων θα πρέπει να κατανεμηθεί στην συγκεκριμένη υπηρεσία που εξετάζεται για εξωτερική ανάθεση. Συνήθως, οι εξωτερικοί συνεργάτες παρέχουν και έχουν την ικανότητα να καλύψουν τις ανάγκες ασφάλειας του οργανισμού. Ιδιαίτερη προσοχή πρέπει να δοθεί στη διασφάλιση της λειτουργίας των υπηρεσιών δημιουργίας αντιγράφων ασφαλείας, στην περίπτωση που διατηρηθούν εσωτερικά ή, μεταφερθούν σε άλλον πάροχο ή, εάν το περιβάλλον αλλάξει ουσιαστικά, όπως συμβαίνει στην περίπτωση εξαγοράς του πελάτη ή του παρόχου. Πρέπει επίσης να σημειωθεί ότι εάν μια διεργασία μοιράζεται κόστος που είναι σταθερό και δεν μπορεί να μειωθεί σε περίπτωση εξωτερικής ανάθεσης, τότε οι δαπάνες αυτές πρέπει να ανακατανεμηθούν μέσω των υπόλοιπων εσωτερικών λειτουργιών. Στην συνέχεια, θα περιγράψουμε ένα σύνολο άλλων σημαντικών κριτηρίων επιλογής εξωτερικής ανάθεσης, πολλά από τα οποία έχουν επίσης στοιχεία κόστους τα οποία θα πρέπει να συμπεριλαμβάνονται και αυτά στην ανάλυση.

2.2 Επίδοση

Ένα από τα πιο σημαντικά κριτήρια επιλογής εξωτερικής ανάθεσης είναι οι αυξημένες επιδόσεις, που ο εξωτερικός πάροχος υπηρεσιών μπορεί να προσφέρει τόσο λόγω των οικονομιών κλίμακας όσο και, λόγω του μεγέθους του. Για παράδειγμα το μέγεθος, θα μπορούσε να δώσει σε έναν οργανισμό την ευκαιρία να παρέχει επαρκή εργασία για να κρατήσει απασχολημένο το προσωπικό δεύτερης και τρίτης βάρδιας. Επίσης, θα μπορούσε να προσφέρει μια ποικιλία λειτουργιών και ευκαιριών που θα βοηθήσουν στη διατήρηση του καλύτερου διαθέσιμου ανθρώπινου προσωπικού. Επιπλέον, το επίπεδο της τεχνογνωσίας αναμένεται να είναι υψηλότερο στους εξωτερικούς παρόχους υπηρεσιών, λόγω της μεγαλύτερης συγκέντρωσης προσωπικού και της μικρότερης επαναληψιμότητας των εργασιών.

Η σχέση μεταξύ εξωτερικού παρόχου υπηρεσιών και πελάτη βασίζεται σε συμβόλαια με συγκεκριμένες απαιτήσεις και ρήτρες σε περίπτωση που δεν τηρηθούν τα συμφωνηθέντα, στα χρονικά περιθώρια που έχουν οριστεί. Εσωτερικά στον οργανισμό δεν συμβαίνει το ίδιο γιατί είναι πολύ δύσκολο να ασκηθεί πίεση στο προσωπικό της εταιρείας σε περιπτώσεις μη επαρκής απόδοσης. Οι πάροχοι υπηρεσιών έχουν περισσότερα κίνητρα για να τηρήσουν τους όρους μιας συμφωνίας ανάθεσης εργασιών, από ότι το εσωτερικό προσωπικό ενός οργανισμού. Αξίζει να αναφερθεί ότι, έχει σημειωθεί επιδείνωση των επιπέδων εξυπηρέτησης από εξωτερικούς παρόχους στις περιπτώσεις που αντιμετωπίζει οικονομικές δυσκολίες ή, όταν δεσμεύει υπερβολικούς πόρους σε άλλους πελάτες (Solli-Saether H. , 2010).

2.2.1 Αξιοπιστία

Ο βαθμός αξιοπιστίας ως συστατικό στοιχείο της απόδοσης, αποτελεί κριτήριο υψηλής κρισιμότητας για την επιλογή ενός λογισμικού ή εξοπλισμού. Επομένως, η επιλογή πιο αξιόπιστων εξαρτημάτων υλικού και λειτουργιών λογισμικού καθιστά το συνολικό σύστημα πιο αξιόπιστο και αυξάνει το επίπεδο της διαθεσιμότητάς του. Το ίδιο ακριβώς ισχύει και στην επιλογή ενός εξωτερικού παρόχου. Άλλοι παράγοντες που πρέπει να ληφθούν υπόψη όσον αφορά την αξιοπιστία είναι οι μηχανισμοί επιχειρηματικής συνέχειας και αποκατάστασης από καταστροφές. Το πλάνο επιχειρηματικής συνέχειας (Business Continuity Plan - BCP) και το πλάνο αποκατάστασης από καταστροφές (Disaster Recovery Plan - DRP) αποτελούν σημαντικές ευκαιρίες εξωτερικής ανάθεσης καθώς, η κοινή χρήση τέτοιων υπηρεσιών με άλλους πελάτες μπορεί να μειώσει σημαντικά το κόστος. Από την σκοπιά της διαθεσιμότητας, το BCP και το DRP παρέχουν υψηλό επίπεδο διαβεβαίωσης ότι ένας οργανισμός μπορεί να επιβιώσει και να ανακάμψει από μια μεγάλη καταστροφή όπως πυρκαγιά, τυφώνα, σεισμό ή, τρομοκρατική επίθεση.

Από την πλευρά του πελάτη, ο χρόνος στον οποίο συμβαίνουν αυτές οι φαινομενικά τυχαίες αποτυχίες είναι κρίσιμης σημασίας. Η διαθεσιμότητα είναι σημαντική για τον οργανισμό στις περιόδους κατά τις οποίες χρησιμοποιεί τα συστήματα και τα δίκτυα για τις εταιρικές του ανάγκες. Οι βλάβες αυτές, τις ώρες εκτός λειτουργίας ουσιαστικά δεν υπολογίζονται. Αυτός είναι και ο κύριος λόγος για τον οποίο οι οργανισμοί επιθυμούν σύντομους χρόνους απόκρισης κατά τη διάρκεια των κρίσιμων περιόδων λειτουργίας τους και, είναι πρόθυμοι να πληρώσουν για τέτοιες υπηρεσίες ένα σημαντικό ασφάλιστρο το οποίο μπορεί να ισούται με το 20% έως 50% του βασικού τέλους συντήρησης. Στις περισσότερες περιπτώσεις, οι οργανισμοί ενδιαφέρονται μόνο για τη διαθεσιμότητα των υπηρεσιών που υποστηρίζουν τις επιχειρησιακές λειτουργίες τους χωρίς να δίνουν βάρος στις υπόλοιπες απαιτήσεις λειτουργίας όπως είναι, η ασφάλεια και η αξιοπιστία (Sparrow, 2003).

2.2.2 Ακεραιότητα

Η απαίτηση να λειτουργεί σωστά και με ακρίβεια ένα σύστημα αποτελεί σημαντική πτυχή της ακεραιότητας και της χρηστικότητας ενός συστήματος. Για να διατηρηθεί ο σωστός βαθμός ακεραιότητας, ο πάροχος υπηρεσιών πρέπει να αναπτύξει, να υιοθετήσει και να επιβάλει πολιτικές και διαδικασίες για την θέσπιση και εφαρμογή προστατευτικών μέτρων. Ο πάροχος πρέπει να είναι σε θέση να παρακολουθεί και να εξετάζει όλες τις δραστηριότητες των τελικών χρηστών και των προγραμμάτων. Θα δύναται να προσδιορίσει και να εντοπίσει ποιος έχει αποκτήσει πρόσβαση στις εφαρμογές, στις λειτουργίες και στα δεδομένα. Επιπροσθέτως, χρειάζεται να διαθέτει συγκεκριμένα σχέδια απόκρισης σε περιπτώσεις τυχόν ασυνήθιστων δραστηριοτήτων ή εισβολών, προκειμένου να αποφευχθεί η κατάχρηση, να αποκατασταθεί οποιαδήποτε ζημία έχει γίνει και να μπορεί να διώξει ποινικά τους δράστες (Amant, 2009).

2.2.3 Ποιότητα εξυπηρέτησης

Ενώ τα επίπεδα υπηρεσιών, η διαθεσιμότητα και η ακεραιότητα είναι μετρήσιμα, η ποιότητα της υπηρεσίας είναι πολύ δύσκολο να μετρηθεί. Είναι ένας συνδυασμός των προαναφερθέντων ποσοτικών μέτρων μαζί με τις άυλες πτυχές της απόδοσης. Ιδιαίτερα σημαντικός είναι και ο βαθμός στον οποίο ο πάροχος υπηρεσιών είναι προληπτικός όσον αφορά στην επίλυση προβλημάτων προτού αυτά εξελιχθούν σε κρίσιμα για τον οργανισμό. Μέσα από τέτοιες ενέργειες, ένας εξωτερικός πάροχος υπηρεσιών μπορεί να διαφοροποιηθεί από τους ανταγωνιστές του προσφέροντας καλύτερες υπηρεσίες στους πελάτες του. Επειδή η ποιότητα της υπηρεσίας είναι υποκειμενική αλλά και ταυτόχρονα πολύ σημαντική στην επιλογή ενός παρόχου υπηρεσιών, οι οργανισμοί θα πρέπει να αξιολογούν συνεχώς τους εξωτερικούς παρόχους ορίζοντας και εφαρμόζοντας εξ’ αρχής συγκεκριμένα κριτήρια αξιολόγησης. Τέτοια κριτήρια είναι, ο

βαθμός αύξησης του αριθμού των πελατών, ο χρόνος παραμονής των πελατών στον πάροχο, τα παράπονα κ.ά. (Chorafas, 2003) (Sparrow, 2003).

2.3 Ασφάλεια

Ένα άλλο κρίσιμο κριτήριο επιλογής εξωτερικού παρόχου είναι το επίπεδο της ασφάλειάς του. Όπως και η αξιοπιστία, έτσι και η ασφάλεια περιλαμβάνει ένα ευρύ φάσμα χαρακτηριστικών. Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα είναι τα βασικότερα χαρακτηριστικά της ασφάλειας των πληροφοριακών συστημάτων. Έχουμε ήδη αναφέρει την ακεραιότητα και τη διαθεσιμότητα στα προηγούμενα κεφάλαια της απόδοσης και της ποιότητας των υπηρεσιών, οπότε αυτό που θα αναλύσουμε στην συνέχεια είναι η εμπιστευτικότητα (Allen, Gabbard, May, Hayes, & Sledge, 2003).

2.3.1 Εμπιστευτικότητα

Οι όροι εμπιστευτικότητα, προστασία της ιδιωτικής ζωής, πνευματική ιδιοκτησία και ιδιοκτησιακές πληροφορίες χρησιμοποιούνται από τους οργανισμούς για τον χειρισμό θεμάτων που αφορούν τη διαχείριση των πληροφοριών και των δεδομένων. Το ζήτημα της εμπιστευτικότητας λαμβάνει μεγάλη προσοχή από τους νομοθέτες και τις ρυθμιστικές αρχές, ιδίως στις χρηματοπιστωτικές υπηρεσίες και στις υπηρεσίες υγείας. Οι γρήγορες τεχνολογικές εξελίξεις, ιδιαίτερα αυτές που επιτρέπουν την εύκολη απομακρυσμένη πρόσβαση από οπουδήποτε, ξεπέρασαν κατά πολύ τις ικανότητες των οργανισμών για τον έλεγχο και τη διασφάλιση των πληροφορίων. Ο αυξανόμενος αριθμός περιστατικών ασφάλειας που δημοσιεύονται ευρέως, με εκατομμύρια περιπτώσεις κλοπής ταυτότητας και άλλων προσωπικών δεδομένων, έχει προσελκύσει και το ενδιαφέρον των κυβερνήσεων. Το αποτέλεσμα είναι ένας μεγάλος αριθμός νόμων και κανονισμών, που αποσκοπούν στην προστασία των προσωπικών δεδομένων των ατόμων. Οι ρυθμιστικές αρχές σε ορισμένους κλάδους, όπως οι χρηματοπιστωτικές υπηρεσίες, απαιτούν από τους οργανισμούς να εκτελούν εξαντλητικούς ελέγχους στους εξωτερικούς παρόχους υπηρεσιών όσον αφορά στο επίπεδο της ασφάλειάς τους.

Οι τράπεζες συγκεκριμένα, εκτελούν εκτεταμένες αξιολογήσεις και ελέγχους ασφάλειας σε κάθε τομέα ασφάλειας, συμπεριλαμβανομένης της πρόσβασης στο σύστημα, της ευαισθητοποίησης προσωπικού, της επιχειρησιακής συνέχειας, της αποκατάστασης μετά από καταστροφή και της φυσικής ασφάλειας (Solli-Saether & Gottschalk, 2006). Στον Πίνακας 3 παρουσιάζονται οι κύριες κατηγορίες και υποκατηγορίες των μηχανισμών και των μέτρων ασφάλειας που θα πρέπει να αξιολογούνται κατά την επιλογή εξωτερικών παρόχων, σύμφωνα με το Ινστιτούτο Πολιτικής Τραπεζών (Bank Policy Institute - BPI) (BPI BITS, 2020).

Πίνακας 3: *Κύριες κατηγορίες και υποκατηγορίες μέτρων ασφάλειας*

Κατηγορία	**Υποκατηγορία**
Πολιτικές ασφάλειας	
Ασφάλεια οργανισμού	Υποδομή ασφάλειας δεδομένων Μέτρα διασφάλισης πρόσβασης τρίτων Εξωτερική ανάθεση
Ταξινόμηση και έλεγχος περιουσιακών στοιχείων	Λογοδοσία για περιουσιακά στοιχεία Διαβάθμιση πληροφοριών
Ασφάλεια προσωπικού	Ασφάλεια περιβάλλοντος εργασίας Εκπαίδευση προσωπικού Απόκριση προσωπικού σε περιστατικά ασφάλειας και δυσλειτουργίες
Φυσική και περιβαλλοντική ασφάλεια	Ασφαλείς περιοχές Ασφάλεια εξοπλισμού Γενικοί μηχανισμοί ελέγχου
Επικοινωνίες και λειτουργίες διαχείρισης	Λειτουργικές διαδικασίες και ευθύνες Σχεδιασμός συστημάτων και κριτήρια αποδοχής Προστασία από κακόβουλο λογισμικό Διαχείριση δικτύου Διαχείριση αποθηκευτικών μέσων και λογισμικού Διαμοιρασμός πληροφοριών και λογισμικού
Έλεγχος προσβάσεων	Επιχειρησιακές απαιτήσεις για έλεγχο προσβάσεων Διαχείριση προσβάσεων χρηστών Ευθύνες χρηστών Έλεγχος πρόσβασης δικτύου Έλεγχος πρόσβασης λειτουργικών συστημάτων Έλεγχος πρόσβασης εφαρμογών Εποπτεία πρόσβασης και χρήσης συστημάτων Φορητές συσκευές και τηλεργασία
Υλοποίηση συστημάτων και συντήρηση	Απαιτήσεις ασφάλειας συστημάτων Απαιτήσεις ασφάλειας εφαρμογών Εφαρμογή μηχανισμών κρυπτογράφησης Ασφάλεια συστημικών αρχείων Ασφάλεια κατά την υλοποίηση εφαρμογών και την υποστήριξή τους
Διαχείριση επιχειρηματικής συνέχειας	Σχεδιασμός, υλοποίηση και εποπτεία πλάνου επιχειρηματικής συνέχειας
Εναρμόνιση με νομικές απαιτήσεις	Εναρμόνιση με νομικές απαιτήσεις Αξιολόγηση πολιτικής ασφάλειας και τεχνική εναρμόνιση Συστήματα ελέγχου

2.3.2 Εμπιστοσύνη

Όπως προαναφέρθηκε, η εξέταση του επιπέδου ασφάλειας των παρόχων υπηρεσιών εκτείνεται πέραν των συνηθισμένων τεχνικών ελέγχου. Η εξέταση διερευνά τις πρακτικές πρόσληψης και τα προγράμματα ευαισθητοποίησης σχετικά με την

ασφάλεια και τους ελέγχους πρόσβασης σε κτίρια και εγκαταστάσεις (ειδικά σε κέντρα δεδομένων). Οι πάροχοι υπηρεσιών θα πρέπει να μπορούν να αποδείξουν το ότι προστατεύουν επαρκώς τις εμπιστευτικές πληροφορίες των πελατών τους. Για να πετύχουν αυτό, θα πρέπει να συμμορφώνονται με αυστηρές απαιτήσεις ασφάλειας. Η λειτουργία τους, εξαρτάται σε μεγάλο βαθμό από τα πρότυπα ασφάλειας που εφαρμόζουν, από το επίπεδο ασφάλειας των εγκαταστάσεων που διαθέτουν και από το επίπεδο της ασφάλειας των υπηρεσιών τους. Αν κάποιος εξωτερικός πάροχος μπορεί να επιδείξει υψηλές προδιαγραφές ασφάλειας, τότε έχει μεγαλύτερες πιθανότητες να επιλεγεί σε σύγκριση με έναν άλλο πάροχο ο οποίος δεν τις διαθέτει (Karabulut, 2007).

2.4 Εξειδίκευση

Ένας άλλος σημαντικός λόγος για την εξωτερική ανάθεση, είναι η πρόσβαση σε υψηλά ειδικευμένο προσωπικό το οποίο μπορεί να μην είναι διαθέσιμο εσωτερικά στον οργανισμό. Σε ορισμένους τομείς, ιδίως όσον αφορά στην ασφάλεια των πληροφοριών, η ζήτηση για ειδικευμένους και έμπειρους επαγγελματίες υπερβαίνει κατά πολύ την προσφορά. Επίσης, ένας οργανισμός μπορεί να μην έχει το κατάλληλο εύρος εργασίας για να κρατήσει απασχολημένο το προσωπικό υψηλής εξειδίκευσης σε αντίθεση με έναν εξωτερικό πάροχο. Για παράδειγμα, οι ειδικοί ασφάλειας που εργάζονται σε εξωτερικούς παρόχους υπηρεσιών έχουν μεγαλύτερη εμπειρία σε αντίθεση με έναν υπάλληλο που υποστηρίζει μόνο μια εταιρεία. Παρόλο που και οι δύο είναι εξειδικευμένοι, ο πρώτος ωφελείται από την εμπειρία που έχει αποκτήσει. Επίσης, είναι σημαντικό οι εξωτερικοί πάροχοι να ενημερώνουν τους οργανισμούς σε περίπτωση που δεν χρησιμοποιήσουν τα εξειδικευμένα στελέχη που τους υποσχέθηκαν κατά την εξωτερική ανάθεση. Οι οργανισμοί θα πρέπει να γνωρίζουν το προσωπικό στο οποίο πρόκειται να ανατεθεί σε κάθε έργο και τον ρόλο του κάθε εργαζομένου. Στο αρχικό συμφωνητικό παροχής υπηρεσιών θα πρέπει να αναφέρεται το προσωπικό που πρόκειται να απασχοληθεί καθώς οι πιστοποιήσεις που διαθέτει.

Όπως περιγράψαμε και πρωτύτερα, οι εξωτερικοί πάροχοι προσφέρουν στα στελέχη τους καλύτερες προοπτικές εξέλιξης από ότι οι οργανισμοί. Τα εξειδικευμένα στελέχη είναι πιθανό να αποχωρήσουν στις περιπτώσεις που επαναλαμβάνουν μια εργασία, διότι θεωρούν ότι βλάπτεται η καριέρα τους και μειώνεται το γνωστικό τους επίπεδο. Οι εξωτερικοί πάροχοι για να αντιμετωπίσουν αυτού το είδους τα προβλήματα, πολλές φορές μεταφέρουν τους καλύτερους και πιο έμπειρους ειδικούς από τον έναν πελάτη τους σε έναν άλλο. Αυτές οι αλλαγές είναι λογικό να επηρεάζουν το επίπεδο των υπηρεσιών που προσφέρουν στους πελάτες τους. Υπάρχουν πολλές λύσεις σε τέτοια προβλήματα. Μια λύση είναι να διασφαλιστεί ότι ο πάροχος υπηρεσιών δεν έχει το δικαίωμα μαζικών απολύσεων προσωπικού με υψηλό επίπεδο γνώσεων και εκτεταμένη

εμπειρία. Μια άλλη λύση είναι, ο εξωτερικός πάροχος υπηρεσιών να μοιράσει τις αρμοδιότητες σε πολλά άτομα. Επίσης, θα μπορούσε να τεκμηριώσει πλήρως τις λειτουργίες, έτσι ώστε κάποιος με λιγότερη εμπειρία να μπορεί να τις εκτελέσει. Σε κάθε περίπτωση, η πρόσβαση σε εξειδικευμένη τεχνογνωσία μπορεί να αποτελέσει σημαντική κινητήρια δύναμη στην απόφαση για εξωτερική ανάθεση. Αποτελεί έναν από τους σημαντικότερους παράγοντες που οδηγούν στην επιλογή υπεράκτιας ανάθεσης σε χώρες όπως η Ινδία, η Ιρλανδία και η Κίνα, όπου διατίθενται είναι ολοένα και μεγαλύτερες ομάδες χαμηλού κόστους, με υψηλά μορφωμένους επαγγελματίες (Solli-Saether & Gottschalk, 2006) (Power, 2006).

2.5 Λογισμικό

Οι οργανισμοί και οι εξωτερικοί πάροχοι μπορεί να έχουν αναπτύξει εφαρμογές υπολογιστών, από κοινού ή ανεξάρτητα. Μεγάλη βαρύτητα στην απόφαση για εξωτερική ανάθεση έχουν ο σχεδιασμός, η ανάπτυξη, η υλοποίηση, η λειτουργία των εφαρμογών καθώς επίσης και η διασύνδεσή τους με άλλα συστήματα και διαδικασίες. Απαιτεί χρόνο, χρήμα και προσπάθεια πολλών ειδικών σε συστήματα πληροφορικής, τεχνολογία για την ανάπτυξη και τη συντήρηση αυτών των εφαρμογών ηλεκτρονικών υπολογιστών. Οι οργανισμοί για να αποφύγουν το βάρος της υλοποίησης και της υποστήριξης των εφαρμογών τους, αποφασίζουν να αναθέσουν αυτό το έργο σε εξωτερικούς παρόχους (Harold & Krause, 2008). Τα κύρια κριτήρια επιλογής μιας εξωτερικής ανάθεσης που σχετίζεται με τις εφαρμογές υπολογιστών αναλύονται στην συνέχεια.

2.5.1 Ανεπαρκής εσωτερική τεχνογνωσία

Όπως προαναφέραμε, ένας σημαντικός λόγος για την χρήση εξωτερικών παρόχων για την ανάπτυξη και τη λειτουργία συστημάτων πληροφορικής είναι η μη επαρκή τεχνογνωσία και εμπειρία του προσωπικού που διαθέτουν οι οργανισμοί.

2.5.2 Ανακύκλωση προσωπικού

Η ανταγωνιστική αγορά για συγκεκριμένες ειδικότητες προσωπικού δυσχεραίνει τους οργανισμούς στο να διατηρήσουν προσωπικό υψηλής εξειδίκευσης. Η εξωτερική ανάθεση έρχεται να δώσει λύση σε αυτό το δύσκολο πρόβλημα.

2.5.3 Περιορισμοί πληρωμής και αποζημίωσης προσωπικού

Οι οργανισμοί αντιμετωπίζουν δυσκολία στο να στρατολογήσουν το προσωπικό που επιθυμούν λόγω έλλειψης κεφαλαίου. Επίσης, πολλές φορές δεν έχουν την δυνατότητα να προσφέρουν ανταγωνιστικά κίνητρα όπως μετοχές, παροχές κ.ά.

2.5.4 Διαμοιραζόμενα κόστη υλοποίησης

Ένας οργανισμός από μόνος του πιθανών να μην έχει την οικονομική δυνατότητα να υποστηρίξει την υλοποίηση μιας συγκεκριμένης εφαρμογής. Μπορεί όμως να είναι σε θέση να υποστηρίξει οικονομικά το κόστος ανάπτυξης και λειτουργίας εάν το μοιράζεται με άλλους οργανισμούς μέσω ενός εξωτερικού παρόχου. Τα πληροφοριακά συστήματα παρέχουν στους οργανισμούς ανταγωνιστικό πλεονέκτημα. Στην περίπτωση που κάποιος οργανισμός δεν είναι σε θέση να υποστηρίξει οικονομικά κάποιο απαραίτητο για την λειτουργία του πληροφοριακό σύστημα, αυτομάτως οδηγείται σε απώλεια μεριδίου αγοράς και μειωμένα κέρδη. Αυτό όπως καταλαβαίνουμε έχει αρνητικό αντίκτυπο στην εικόνα του οργανισμού. Στις περιπτώσεις όπου ρυθμιστικές αρχές θέτουν προδιαγραφές λειτουργίας συστημάτων εντός συγκεκριμένης προθεσμίας, η υλοποίηση νέων συστημάτων ή η αλλαγή υφιστάμενων συστημάτων ορίζει ποιος θα επιβιώσει και ποιος όχι στην αγορά. Ως παράδειγμα μπορούμε να αναφέρουμε το ζήτημα του 2000, όταν πολλές εταιρείες αποφάσισαν να αναθέσουν σε εξωτερικούς παρόχους την προσαρμογή των συστημάτων τους για να μην χρειαστεί να αλλάξουν οι ίδιοι εκατομμύρια γραμμών κώδικα προγραμμάτων.

2.5.5 Ενημερώσεις εκδόσεων λογισμικού

Στον σημερινό κόσμο οι ιοί μπορούν να εξαπλωθούν παγκοσμίως μέσα σε λίγα δευτερόλεπτα. Ως εκ τούτου, η ενημέρωση του λογισμικού και των συστημάτων είναι ακόμα πιο σημαντική. Αυτό, όχι μόνο διατηρεί την εικόνα του εξωτερικού παρόχου υπηρεσιών ως προοδευτική, αλλά μειώνει επίσης την έκθεσή του στις συνεχώς αυξανόμενες απειλές. Οι εξωτερικοί πάροχοι είναι συχνά πιο κατάλληλοι στο να εκτελούν αναβαθμίσεις, επειδή είναι πιο ευαίσθητοι στα ζητήματα που αφορούν στην ασφάλεια πληροφοριακών συστημάτων. Τα κίνητρα για την επικαιροποίηση του λογισμικού είναι τα ίδια για εσωτερικά και εξωτερικά συστήματα. Συχνά δεν δίδεται η δέουσα σημασία στα εσωτερικά συστήματα των οργανισμών λόγων ανεπαρκών πόρων προσωπικού και χρημάτων. Οι ενημερώσεις λογισμικού ασφάλειας θεωρούνται ως πολυτέλεια στους μικρούς εξωτερικούς παρόχους και παραλείπονται σε αντίθεση με τους μεγάλους σε μέγεθος εξωτερικούς παρόχους για τους οποίους αποτελούν σημαντική λειτουργία ασφάλειας (Halvey & Melby, 2007).

Ταχύτητα

Οι εξωτερικοί πάροχοι διαθέτουν μεγάλες ομάδες ειδικών για την εγκατάσταση ενημερώσεων στους πελάτες τους. Για τον λόγο αυτόν οι ενημερώσεις παραδίδονται στους πελάτες πολύ πιο γρήγορα από ότι αν αναλάμβαναν να τις εγκαταστήσουν οι ίδιοι απασχολώντας δικό τους προσωπικό.

Νέες ευκαιρίες εσόδων

Οι οργανισμοί μπορούν να εκμεταλλευτούν το ευρύτερο φάσμα δυνατοτήτων που προσφέρουν οι εξωτερικοί πάροχοι υπηρεσιών προκειμένου να δημιουργήσουν υψηλότερα έσοδα και κέρδη. Μερικές φορές μια επιχειρηματική ιδέα ξεκινάει σε μικρή κλίμακα και μεγαλώνει με την πάροδο του χρόνου. Σε μια τέτοια περίπτωση, ένας οργανισμός μπορεί να μην είναι πρόθυμος να πραγματοποιήσει την αρχική επένδυση που απαιτείται για την ανάπτυξη των συστημάτων και υπηρεσιών. Επιλέγοντας έναν εξωτερικό πάροχο υπηρεσιών αυτό είναι εφικτό.

Διακυμάνσεις στον όγκο έργων

Ένα σημαντικό πρόβλημα που πρέπει να αντιμετωπίσουν οι οργανισμοί σχετικά με την υλοποίηση εφαρμογών είναι οι διακυμάνσεις στον όγκο εργασίας. Οι πάροχοι έχουν την δυνατότητα να μεταφέρουν προσωπικό από ένα πελάτη τους σε έναν άλλο ανάλογα με τη ζήτηση. Επίσης, με τη χρήση εξωτερικών παρόχων οι οργανισμοί αποφεύγουν τις απολύσεις και τις προσλήψεις προσωπικού στις διακυμάνσεις του φόρτου εργασίας τους.

Χαμηλότερα κόστη παραμετροποιήσεων

Συνήθως είναι πολύ πιο εύκολο για τους εξωτερικούς παρόχους να προσαρμόσουν τα συστήματα που προσφέρουν για να καλύψουν τις έκτακτες ανάγκες των πελατών τους. Τα συστήματά είναι υλοποιημένα με τέτοιο τρόπο προκειμένου να προσαρμόζονται εύκολα στις ατομικές απαιτήσεις των πελατών τους, σε σύγκριση με τα εσωτερικά συστήματα των οργανισμών τα οποία είναι λιγότερο ευέλικτα.

Χαμηλότερα κόστη ενσωμάτωσης

Ο εξωτερικοί πάροχοι θα πρέπει να είναι σε θέση να ενσωματώνουν αποτελεσματικά τα συστήματά τους με τα συστήματα των πελατών τους. Θα πρέπει να έχουν σχεδιαστεί με τέτοιον τρόπο για να προσαρμόζονται εύκολα και γρήγορα σε πολυάριθμα περιβάλλοντα. Η γρήγορη ενσωμάτωση και οι διαδικασίες ενσωμάτωσης αποτελούν επίσης καθοριστικό παράγοντα επιλογής ενός εξωτερικού παρόχου.

2.6 Υποστήριξη

Οι εξωτερικοί πάροχοι χρειάζεται να διαθέτουν ισχυρά τμήματα υποστήριξης πελατών για να επιβιώσουν σε μια ανταγωνιστική αγορά όπως η δική τους. Η υποστήριξη μπορεί να καλύψει διάφορα σημεία σε έναν οργανισμό όπως τις τηλεπικοινωνίες, τα δίκτυα, τα συστήματα, το λογισμικό κ.ά. Η λειτουργία ενός τμήματος υποστήριξης σε έναν εξωτερικό πάροχο μοιάζει αρκετά με ένα εσωτερικό τμήμα

υποστήριξης ενός οργανισμού και η διαφορά τους αφορά κυρίως στο επίπεδο τεχνογνωσίας του προσωπικού που διαθέτει. Το προσωπικό ενός εξωτερικού παρόχου υπηρεσιών αντιμετωπίζει καθημερινά πολλά και διαφορετικά προβλήματα σε διαφορετικούς πελάτες και ως αποτέλεσμα, διαθέτει πολύ μεγαλύτερη εμπειρία σε σχέση με το εσωτερικό προσωπικό ενός οργανισμού. Οι εξωτερικοί πάροχοι θέλουν να παρουσιάζουν καλή εικόνα λειτουργιών υποστήριξης γιατί αν δεν το πράξουν θα μειωθεί το πελατολόγιό τους.

Οι οργανισμοί συνήθως δημιουργούν τα τμήματα υποστήριξης στα κεντρικά σημεία των υποδομών τους, όπου τα εργατικά κόστη είναι συνήθως υψηλά. Σε αντίθεση, οι εξωτερικοί πάροχοι υπηρεσιών επειδή υποστηρίζουν πολλούς πελάτες, λόγω μεγέθους έχουν τη δυνατότητα να δημιουργήσουν αντίστοιχα τμήματα σε περιοχές με χαμηλά εργατικά κόστη και εξειδικευμένο προσωπικό. Η εργασία σε τμήματα υποστήριξης στις περιοχές με μεγάλη ζήτηση προσωπικού, θεωρείται συχνά ως προσωρινή και βαρετή δουλειά που προσελκύει κακή ποιότητα υποψηφίων. Αυτό διαφοροποιείται στις περιπτώσεις που επιλέγεται κάποια περιοχή με υψηλή ανεργία ή κάποια υποανάπτυκτη χώρα (Butler, 2000).

Η πρόοδος της τεχνολογίας των τηλεπικοινωνιών διευκόλυνε την τάση προς την απομακρυσμένη τεχνική υποστήριξη και εξυπηρέτηση. Τα τμήματα τεχνικής υποστήριξης των εξωτερικών παρόχων πλέον μπορούν να λειτουργούν σε τρεις βάρδιες, αξιοποιώντας προσωπικό που βρίσκεται σε ξένες χώρες διαφορετικής ζώνης ώρας. Αυτό επιτρέπει στους οργανισμούς να απολαμβάνουν τις ίδιες υπηρεσίες με λειτουργικά κόστη κανονικών ωρών εργασίας. Με το κόστος των γραμμών επικοινωνίας μεταξύ μεγάλων αποστάσεων να μειώνεται, οι συνδέσεις μεταξύ των οργανισμών και των εξωτερικών παρόχων πλέον είναι οικονομικότερες και τεχνικά εφικτές.

2.7 Οικονομικές διευθετήσεις

Οι επιλογές πληρωμής που προσφέρει ένας εξωτερικός πάροχος υπηρεσιών μπορούν να επηρεάσουν σημαντικά την κερδοφορία ενός οργανισμού. Οι εξωτερικοί πάροχοι διαθέτουν διαφορετικές τιμολογιακές πολιτικές ανά υπηρεσία. Συνήθως οι χρεώσεις υπολογίζονται με βάση την χρήση πόρων σε συνδυασμό με το επίπεδο ποιότητας της προσφερόμενης υπηρεσίας. Οι ίδιοι πόροι (ανθρώπινοι ή συστημικοί), μπορεί να διατίθενται ταυτόχρονα σε πολλούς πελάτες. Σε αυτή την περίπτωση, η κοστολόγηση των υπηρεσιών εξαρτάται από τον βαθμό της κοινής χρήσης. Οι οργανισμοί συνήθως αγοράζουν κάποιον συνδυασμό κοινόχρηστων ή αποκλειστικών υπηρεσιών. Ως παράδειγμα κοινόχρηστων υπηρεσιών, θα μπορούσαμε να αναφέρουμε τις υπηρεσίες αποκατάστασης από καταστροφές.

Ο λόγος ύπαρξης των υπηρεσιών αποκατάστασης από καταστροφές, είναι η αντίληψη ότι σε δεδομένο χρονικό σημείο, μόνο ένα μικρό σύνολο πελατών μπορεί να χρειαστεί να χρησιμοποιήσει αυτές τις υπηρεσίες. Οι εξωτερικοί πάροχοι, για την υποστήριξη αυτού του είδους των υπηρεσιών, βασίζονται στην κοινή χρήση πόρων και στην χαμηλή πιθανότητα να εκδηλωθούν περιπτώσεις καταστροφών ταυτόχρονα σε πολλούς πελάτες. Σε γενικές γραμμές, στις υπηρεσίες αποκατάστασης καταστροφών, οι εξωτερικοί πάροχοι υπερφορτώνουν (αυξάνουν σε μεγάλο βαθμό το ποσοστό κοινής χρήσης) τα συστήματά τους διότι προσπαθούν να υποστηρίξουν όλο και περισσότερους πελάτες.

Θα πρέπει να αναφερθεί ότι υπάρχει πιθανότητα οι συμφωνημένοι πόροι να μην είναι διαθέσιμοι σε περίπτωση που τους χρησιμοποιούν ταυτόχρονα πολλοί πελάτες. Οι εξωτερικοί πάροχοι υπηρεσιών αποκατάστασης καταστροφών για να αντιμετωπίσουν τέτοιες περιπτώσεις παίρνουν διάφορα μέτρα όπως, η ανάθεση κοινών πόρων σε εταιρείες που βρίσκονται σε διαφορετικές γεωγραφικές περιοχές ή, σε εταιρείες με διαφορετικές επιχειρηματικές δραστηριότητες. Με αυτούς τους τρόπους μειώνουν την πιθανότητα των ταυτόχρονων χρήσεων μεγάλου αριθμού πόρων.

Στις περιπτώσεις χρήσης αποκλειστικών πόρων, το κόστος χρήσης είναι υψηλότερο ακόμη και από το κόστος των αντίστοιχων εσωτερικών λειτουργιών. Πολλοί οργανισμοί δεν επιθυμούν να πάρουν το ρίσκο της κοινής χρήσης πόρων λόγω των αυξημένων απαιτήσεων των υπηρεσιών που αναθέτουν στους εξωτερικούς παρόχους. Για ποιον λόγο ένας οργανισμός να επιλέξει να αναθέσει σε εξωτερικό πάροχο μια υπηρεσία αποκατάστασης καταστροφών εφόσον θα του κοστίζει περισσότερο; Η απάντηση συχνά έγκειται σε μη οικονομικά οφέλη όπως η δυνατότητα υποστήριξης της υπηρεσίας από το εσωτερικό προσωπικό του οργανισμού ή, η μη διαθεσιμότητα κατάλληλων κτιριακών και πληροφοριακών υποδομών.

Η δυνατότητα πληρωμής σε μηνιαία βάση, χωρίς μεγάλη αρχική δαπάνη κεφαλαίου, είναι επίσης ένας σημαντικός παράγοντας για τις εξωτερικές αναθέσεις, ιδιαίτερα για τους νεοσυσταθέντες οργανισμούς. Τα παραπάνω ζητήματα είναι πολύ σημαντικά κατά την σύναψη συμφωνιών εξωτερικής ανάθεσης και ισχύουν στον ίδιο βαθμό για τις υπηρεσίες παροχής υπηρεσιών ασφάλειας (Butler, 2000).

2.7.1 Επιλογές πληρωμής

Όπως αναφέρθηκε προηγουμένως, η χρήση εξωτερικών παρόχων προσφέρει στους οργανισμούς περισσότερες και πιο ευέλικτες επιλογές πληρωμής. Η δυνατότητα πληρωμής ανά μονάδα χρήσης, συχνά σε ολισθαίνουσα κλίμακα με μειωμένες τιμές για αυξημένους όγκους συναλλαγών, επιτρέπει στους οργανισμούς να χρησιμοποιήσουν

νέες υπηρεσίες χωρίς υψηλό αρχικό κόστος. Η εξωτερική ανάθεση, σε πολλές περιπτώσεις έχει και φορολογικά οφέλη έναντι της αγοράς εξοπλισμού και λογισμικού, με βάση τους υπολογισμούς απόσβεσης και τις εκτιμήσεις της υπολειμματικής αξίας.

2.7.2 Χρηματοδότηση

Σε πολλές περιπτώσεις οι οργανισμοί καλούνται να χρηματοδοτήσουν την ανάπτυξη και την λειτουργία μια συγκεκριμένης υπηρεσίας αναθέτοντάς την εξ' αρχής σε εξωτερικό πάροχο με προκαθορισμένο κόστος. Αντιθέτως, οι νεοσύστατες επιχειρήσεις δεν έχουν τα κεφάλαια ή τους πόρους διαχείρισης για να πράξουν το ίδιο. Οι πιο μεγάλοι οργανισμοί μπορούν να εκμεταλλευτούν πολύ πιο εύκολα την σημαντική μείωση του κόστους από την εξωτερική ανάθεση. Για παράδειγμα, λίγοι είναι οι μεγάλοι οργανισμοί που έχουν παρουσία σε όλο τον κόσμο ώστε να δικαιολογούν υποστήριξη 24 ώρες το 24ωρο για εργασίες όπως η παρακολούθηση του τείχους προστασίας ή του ιομορφικού λογισμικού τους, διότι αυτό απαιτεί υψηλό επίπεδο τεχνογνωσίας και υψηλά κόστη. Ένας εξωτερικός πάροχος μπορεί να κατανείμει τέτοιες εργασίες σε μεγάλο αριθμό πελατών, το οποίο είναι οικονομικά αποδοτικότερο για κάθε πελάτη και κερδοφόρο για τον ίδιο.

3. Κόστη και Οφέλη Εξωτερικών Αναθέσεων

Όπως προαναφέραμε, με την εξωτερική ανάθεση οι οργανισμοί μπορούν να αποκτήσουν σημαντικά οφέλη και πλεονεκτήματα. Ωστόσο, οι διοικήσεις των οργανισμών επιθυμούν να γνωρίζουν τί θα τους κοστίσει στην πραγματικότητα μια εξωτερική ανάθεση, ποιές εξοικονομήσεις μπορούν να αναμένουν και ποια θα είναι η απόδοση της επένδυσης. Σε αυτό το κεφάλαιο, θα περιγράψουμε τις γενικές κατηγορίες κόστους και οφέλους και θα αναφέρουμε τα κόστη και τα οφέλη που προκύπτουν από τη διαδικασία αξιολόγησης των εξωτερικών παρόχων και από τη διαδικασία της εξωτερικής ανάθεσης.

3.1 Γενικές κατηγορίες κόστους και οφέλους

Ορισμένα κόστη και οφέλη που συνδέονται με την εξωτερική ανάθεση είναι γνωστά με υψηλό βαθμό ακρίβειας και βεβαιότητας. Αυτά περιλαμβάνουν το κόστος εργασίας, τις μισθώσεις εξοπλισμού, τις μισθώσεις κτιρίων κ.ά. Υπάρχουν όμως άλλα κόστη και οφέλη τα οποία είναι πολύ δύσκολο να υπολογιστούν λόγω του βαθμού μεταβλητότητάς τους. Κατά τη διαδικασία αξιολόγησης μιας εξωτερικής ανάθεσης, θα πρέπει να υπολογίζονται εκτός από τα γνωστά και τα απτά έξοδα και οφέλη αλλά και τα αβέβαια, άγνωστα και άυλα (Amant, 2009).

Απτά και άυλα κόστη και οφέλη

Τα απτά κόστη υπάρχουν στα βιβλία των οργανισμών και μπορούν εύκολα να εντοπιστούν και να μετρηθούν. Τα απτά οφέλη, μπορούν να υπολογιστούν εύκολα μέσω των πιθανών εξοικονομήσεων και της αύξησης κερδών. Σε αντίθεση όμως, τα άυλα κόστη και οφέλη δεν μπορούν να προσδιοριστούν εύκολα και είναι πολύ δύσκολο να μετρηθούν με ακρίβεια.

Αντικειμενικά και υποκειμενικά κόστη και οφέλη

Τα απτά κόστη είναι αντικειμενικά και τα απτά οφέλη υποκειμενικά. Η εξοικονόμηση κόστους ή η αύξηση των κερδών μπορεί να είναι πραγματική, αλλά η κατανομή της σε μια συγκεκριμένη προσπάθεια μπορεί να είναι δύσκολη και να βασίζεται ως έναν μεγάλο βαθμό σε εκτιμήσεις. Τα άυλα κόστη και τα οφέλη είναι υποκειμενικά, μερικές φορές πολύ υψηλά, παρόλο που οι εκτιμήσεις μπορούν να γίνουν από αντικειμενικούς εξωτερικούς συμβούλους. Ως παράδειγμα μπορούμε να αναφέρουμε την χρήση στατιστικών στοιχείων για απώλειες εξαιτίας των σκουληκιών υπολογιστών, των ιών και των επιθέσεων χάκερ, για να δικαιολογηθούν δαπάνες για εργαλεία ασφάλειας. Αυτά τα στατιστικά στοιχεία είναι αμφισβητήσιμα ως προς την ακρίβεια και παρέχουν γενικά δεδομένα τάσης.

Άμεσα και Έμμεσα κόστη και οφέλη

Οι δαπάνες και τα οφέλη αντιμετωπίζονται διαφορετικά ανάλογα με το αν είναι άμεσα ή έμμεσα. Τα άμεσα κόστη ή τα οφέλη μπορούν να αποδοθούν σε μια συγκεκριμένη δραστηριότητα ή ομάδα. Από την άλλη πλευρά, τα έμμεσα κόστη και οφέλη αφορούν άλλα τμήματα στα οποία έχουν διατεθεί πόροι όπως προσωπικό, εξοπλισμός κτίρια και εργαλεία.

Ελεγχόμενα και μη ελεγχόμενα κόστη και οφέλη

Τα ελεγχόμενα κόστη και οφέλη είναι αυτά που μπορούν να μεταβληθούν από τον αναλυτή ή τον υπεύθυνο λήψης αποφάσεων. Γενικά, τα απτά, άμεσα και αντικειμενικά κόστη και οφέλη θεωρούνται ελεγχόμενα σε αντίθεση με τα άυλα, έμμεσα και υποκειμενικά που θεωρούνται μη ελεγχόμενα.

Συγκεκριμένα και πιθανά κόστη και οφέλη

Ορισμένα κόστη και οφέλη μπορούν να εκφράζονται με ακριβείς απόλυτους όρους, δηλαδή είναι γνωστά με υψηλό βαθμό βεβαιότητας. Για παράδειγμα, οι πληρωμές για εξοπλισμό και λογισμικό. Τα πιθανά κόστη και οφέλη, στηρίζονται σε προσδοκίες και εκτιμήσεις μεγέθους και πιθανότητας. Σε ορισμένες περιπτώσεις, δημιουργείται ένα δέντρο αποφάσεων στο οποίο αναφέρονται οι πιθανότητες των διαφόρων αποτελεσμάτων και εκτιμάται το μέγεθος κάθε αποτελέσματος.

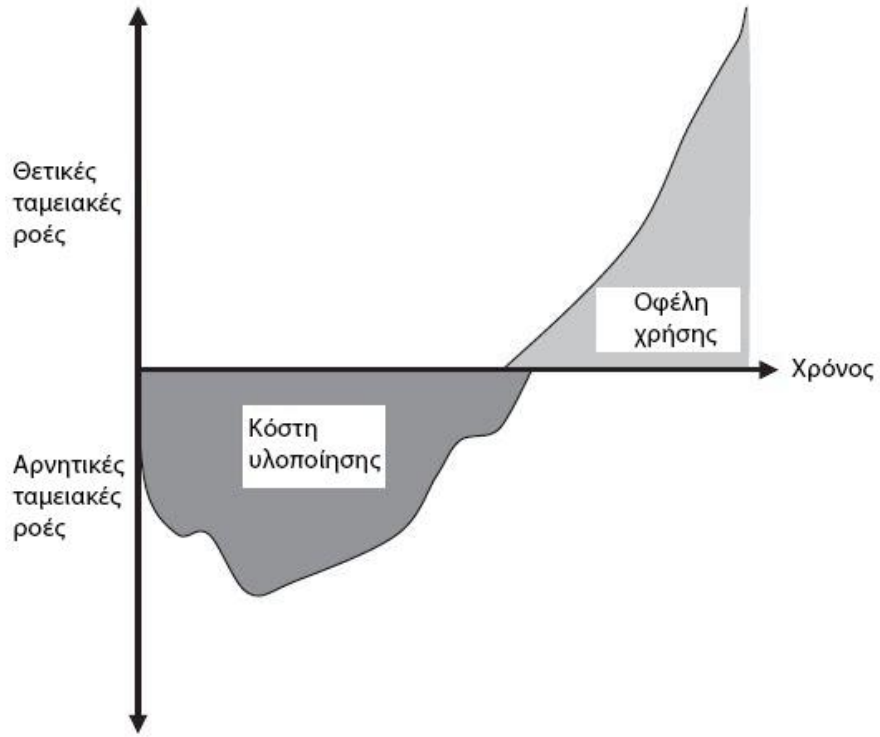
Σταθερά και μεταβλητά κόστη και οφέλη

Μακροπρόθεσμα ισχύει ότι όλα τα κόστη και οφέλη είναι μεταβλητά. Ωστόσο, ο όρος μιας τυπικής σύμβασης υπεργολαβίας, η οποία είναι συνήθως διάρκειας δύο έως τριών ετών, αλλά μπορεί να παραταθεί μέχρι και 10 έτη, επιτρέπει να θεωρηθούν ορισμένα έξοδα και οφέλη σταθερά. Τέτοια μακροπρόθεσμα πάγια έξοδα περιλαμβάνουν μισθώσεις ακινήτων ή πληρωμές υποθηκών. Η μεταβλητότητα είναι συνάρτηση του χρόνου, του επιπέδου πόρων ή και του επιπέδου δραστηριότητας. Εάν το τελευταίο σχετίζεται με κάποιο τρόπο με το κόστος και τα οφέλη, τότε μπορούν να γίνουν υποθέσεις σχετικά με τις λεγόμενες ανεξάρτητες μεταβλητές (επίπεδο δραστηριότητας) και μπορούν να υπολογιστούν οι εξαρτημένες μεταβλητές (κόστος ή οφέλη). Τα σταθερά και μεταβλητά κόστη συχνά, αλλά όχι πάντα, συνίστανται σε εφάπαξ και συνεχιζόμενες δαπάνες, όπως περιγράφουμε στη συνέχεια.

Εφάπαξ και συνεχόμενα κόστη και οφέλη

Είναι σημαντικό να γίνει διάκριση μεταξύ των εφάπαξ και συνεχιζόμενων δαπανών. Εφάπαξ κόστος για παράδειγμα είναι η τιμή αγοράς ενός εξοπλισμού ή ενός λογισμικού,

ενώ συνεχιζόμενο κόστος είναι η τιμή της ετήσιας συντήρησής τους. Τα οφέλη αρχίζουν να εμφανίζονται κατά την εξέλιξη υλοποίησης ενός έργου και μεγιστοποιούνται με την ολοκλήρωσή του. Οι ταμειακές ροές κόστους και οφέλους για ένα τυπικό έργο εσωτερικής ανάπτυξης εφαρμογών απεικονίζονται στο Διάγραμμα 1: Κόστη και οφέλη διαδικασίας υλοποίησης συστημάτων. Αυτός ο τύπος διαγράμματος ισχύει επίσης και για την υλοποίηση προϊόντων που σχετίζονται με την ασφάλεια.



Διάγραμμα 1: *Κόστη και οφέλη διαδικασίας υλοποίησης συστημάτων*

Στον Πίνακας 4 περιγράφονται οι κύριες κατηγορίες και υποκατηγορίες κόστους και οφέλους που προαναφέραμε.

Πίνακας 4:*Κύριες κατηγορίες κόστους και οφέλους εξωτερικών αναθέσεων*

Κατηγορίες	**Κόστη**	**Οφέλη**
Απτά	Κόστη που είναι μετρήσιμα και μπορούν να υπολογιστούν εύκολα	Οφέλη που είναι μετρήσιμα και μπορούν να υπολογιστούν εύκολα
Αντικειμενικά	Δαπάνες όπως αναφέρονται στα βιβλία και αρχεία του οργανισμού	Εξοικονομήσεις κόστους οι οποίες μπορούν να αποδοθούν άμεσα σε συγκεκριμένες αποφάσεις ή ενέργειες

Άμεσα	Συγκεκριμένα και μετρήσιμα έξοδα (εργασία, υλικό, λογισμικό, γραμμές επικοινωνίας)	Μειώσεις κόστους λόγω περικοπών σε προσωπικό, εξοπλισμό, λογισμικό
Έμμεσα	Κόστη άλλων τμημάτων στα οποία έχουν διατεθεί πόροι όπως προσωπικό, εξοπλισμός, κτίρια, εργαλεία	Μειώσεις κόστους λόγω εξοικονόμησης δαπανών (τερματισμός μισθώσεων)
Υποκειμενικά	Κόστη τα οποία δεν ορίζονται σαφώς και υπόκεινται στη διακριτική ευχέρεια του αναλυτή	Οφέλη που δεν είναι σαφώς καθορισμένα και είναι υπό την κρίση του αναλυτή
Άμεσα	Αυξήσεις κόστους ευκαιρίας που οφείλονται στη μη συμμετοχή σε συγκεκριμένη δραστηριότητα ή πόρο	Εξοικονόμηση κόστους ευκαιρίας, από την μη απαίτηση για πρόσληψη και διατήρηση προσωπικού για συγκεκριμένο σκοπό
Έμμεσα	Κόστος ευκαιρίας που δεν αποδίδεται άμεσα σε κάποια συγκεκριμένη δραστηριότητα ή πόρο	Εξοικονόμηση κόστους ευκαιρίας που δεν αποδίδεται άμεσα σε κάποια συγκεκριμένη δραστηριότητα ή πόρο
Άυλα	Κόστη που δεν είναι μετρήσιμα και δεν μπορούν να υπολογιστούν εύκολα	Οφέλη που δεν μπορούν να εκφραστούν με όρους συγκεκριμένης εξοικονόμησης κόστους ή εσόδων
Αντικειμενικά	Οι δαπάνες που προκύπτουν, λόγου χάρη, από την ανεπαρκή τεχνογνωσία και πείρα του προσωπικού	Οφέλη που δεν κερδίζονται όπως αυτά που οφείλονται σε λάθος επιλογή προσωπικού
Άμεσα	Αυξημένο κόστος προσωπικού και άλλων πόρων, για παράδειγμα λόγω ανεπαρκούς ή έλλειψης προγραμμάτων κατάρτισης	Αυξημένη παραγωγικότητα εξαιτίας, για παράδειγμα, ευνοϊκού περιβάλλοντος εργασίας
Έμμεσα	Αυξημένο κόστος λόγω εξωτερικών παραγόντων εκτός του ελέγχου του οργανισμού	Αυξημένη παραγωγικότητα λόγω εξωτερικών παραγόντων εκτός του ελέγχου του οργανισμού
Υποκειμενικά	Κόστη που προκύπτουν από την έλλειψη κινήτρων, πίστης, συντροφικότητας και ούτω	Οφέλη που δεν κερδήθηκαν λόγω έλλειψης πίστης και κινήτρου και υπόκεινται στη διακριτική ευχέρεια του αναλυτή

	καθεξής, και είναι υπό την κρίση του αναλυτή	
Άμεσα	Ενώ οι δαπάνες αυτές είναι ασαφείς, μπορούν να αποδοθούν σε συγκεκριμένες δραστηριότητες ή πόρους	Αν και αυτά τα οφέλη είναι ασαφή, μπορούν να αποδοθούν σε συγκεκριμένες δραστηριότητες ή πόρους
Έμμεσα	Κόστη τα οποία είναι ασαφή και δεν μπορούν να αποδοθούν σε συγκεκριμένες δραστηριότητες ή πόρους (π.χ. κίνδυνος χώρας)	Οφέλη τα οποία είναι ασαφή και δεν μπορούν να αποδοθούν σε συγκεκριμένες δραστηριότητες και πόρους (φήμη, υπεραξία)

3.2 Κόστη και οφέλη διαδικασίας εξωτερικής ανάθεσης

Προηγουμένως, περιγράψαμε τα απτά, άυλα, αντικειμενικά, υποκειμενικά, άμεσα και έμμεσα κόστη και οφέλη που σχετίζονται με την εξωτερική ανάθεση. Στην συνέχεια, θα επικεντρώσουμε στα κύρια κόστη και στα οφέλη που θα πρέπει να υπολογίζονται κατά την φάση της διαδικασίας αξιολόγησης εξωτερικών αναθέσεων και της διαδικασίας επιλογής εξωτερικών παρόχων.

3.2.1 Έναρξη διαδικασίας εξωτερικών αναθέσεων

Υπάρχουν οργανισμοί οι οποίοι δεν έχουν πραγματοποιήσει κάποια εξωτερική ανάθεση και ενδέχεται να το πράξουν στο κοντινό μέλλον. Οι οργανισμοί που έχουν προηγουμένως αναθέσει σε εξωτερικούς παρόχους έργα και λειτουργίες, συνήθως βασίζονται στις προηγούμενες εμπειρίες τους για τις μελλοντικές τους εξωτερικές αναθέσεις. Πολλοί οργανισμοί, δοκιμάζουν αρχικά να αναθέσουν σε εξωτερικό πάροχο μη κρίσιμες λειτουργίες ή υπηρεσίες. Αν αποδειχθεί ότι τα αποτελέσματα αυτών των αναθέσεων είναι τα αναμενόμενα, εξετάζουν το ενδεχόμενο της εξωτερικής ανάθεσης και άλλων πιο σημαντικών υπηρεσιών.

Παρακάτω θα αναφέρουμε επιγραμματικά τους κύριους λόγους οι οποίοι μπορούν να οδηγήσουν έναν οργανισμό στο να εξετάσει την προοπτική εξωτερικής ανάθεσης για πρώτη φορά ή, να εξετάσει το ενδεχόμενο επέκτασης σε περιοχές που δεν είχαν δοκιμαστεί.

- Διαφήμιση από εξωτερικούς παρόχους
- Ενημέρωση από συνεργάτες άλλων εταιρειών
- Άρθρα σε ένα περιοδικό ή εφημερίδα
- Προγράμματα τηλεόρασης
- Σεμινάρια

- Η δυσκολία εύρεσης, πρόσληψης και διατήρησης εξειδικευμένου προσωπικού (ιδιαίτερα στον τομέα της ασφάλειας των πληροφοριών)
- Προβλήματα σε εσωτερικές λειτουργίες που δημιουργούν δυσαρέσκεια
- Η πίεση για μείωση του κόστους και ταυτόχρονα η βελτίωση των υπηρεσιών
- Η μη ικανοποιητική εξυπηρέτηση από τις εσωτερικές μονάδες του οργανισμού

Ο όρος εξωτερική ανάθεση χρησιμοποιείται όλο και περισσότερο στους οργανισμούς και η έννοια χρήσης εξωτερικού παρόχου για κρίσιμες λειτουργίες και τεχνολογίες πληροφορίας είναι πλέον συνήθης. Οι διοικήσεις των οργανισμών έχουν αρχίσει να ζητούν από τα στελέχη τους να αξιολογήσουν και την εξωτερική ανάθεση ως επιλογή κατά την υλοποίηση νέων ή την αναδιάρθρωση υφιστάμενων υπηρεσιών. Τα στελέχη συνήθως έχουν ανεπαρκή γνώση, εμπειρία και κατανόηση για να εκτελέσουν εξαντλητικές αξιολογήσεις επιλογών εξωτερικής ανάθεσης. Όσον αφορά στον τομέα της ασφάλειας, αυτός αναλύεται ανεπαρκώς ανεξάρτητα από το αν είναι ή όχι η κύρια λειτουργία εξωτερικής ανάθεσης.

Ένας οργανισμός μπορεί να μην επιθυμεί να αναλάβει το βάρος της ίδρυσης και λειτουργίας κάποιου εσωτερικού τμήματος, όπως για παράδειγμα της μισθοδοσίας. Επίσης, μπορεί λόγω μικρού μεγέθους να αδυνατεί να υποστηρίξει μια υπηρεσία ακόμη και αν αυτή κρίνεται ως βασική για τη λειτουργία του. Σε άλλες περιπτώσεις ενδέχεται να θεωρήσει ότι η μεταφορά κάποιων εσωτερικών υπηρεσιών σε εξωτερικό πάροχο είναι πιο αποδοτική. Ακόμη, θα μπορούσε να μεταφέρει εσωτερικά εξωτερικές λειτουργίες ή υπηρεσίες λόγω ανεκπλήρωτων προσδοκιών όπως είναι το κόστος, η ποιότητα και τα λειτουργικά οφέλη. Αντιθέτως, στην περίπτωση θετικής εμπειρίας, θα μπορούσε να μεταφέρει όλο και περισσότερες κρίσιμες λειτουργίες ή υπηρεσίες σε εξωτερικούς παρόχους. Σε άλλες περιπτώσεις, με την αλλαγή των συνθηκών, η σχέση κόστους - αποτελεσματικότητας μιας εσωτερικής λειτουργίας μπορεί να κριθεί ως συμφερότερη από εκείνη ενός εξωτερικού παρόχου. Συχνά, η προθυμία για εξωτερική ανάθεση εκφράζεται σε υψηλό εκτελεστικό επίπεδο. Η ευθύνη του αναλυτή είναι να ποσοτικοποιήσει αυτό το ενδιαφέρον στο μέτρο του δυνατού και να ενσωματώσει τα αποτελέσματα σε ανάλυση κόστους - απόδοσης ή επιστροφής στην επένδυση (Sparrow, 2003).

3.2.2 Διαδικασία αξιολόγησης

Ένα συγκεκριμένο γεγονός συνήθως ενεργοποιεί την εξέταση εξωτερικών αναθέσεων για συγκεκριμένες εταιρικές λειτουργίες και δραστηριότητες. Μερικές φορές, λόγω κρίσιμων επιχειρηματικών αναγκών ή πολιτικών παραγόντων, ορισμένα βήματα αξιολόγησης παρακάμπτονται. Ωστόσο, για μια πλήρη και ακριβή αξιολόγηση, θα πρέπει

να ακολουθηθούν συγκεκριμένα βήματα, το πρώτο από τα οποία είναι η διαδικασία αξιολόγησης. Η διαδικασία της αξιολόγησης εκτελείται συνήθως από εσωτερικό προσωπικό, εξωτερικούς συμβούλους ή σε συνεργασία και των δύο. Η χρήση εξωτερικών συμβούλων συνιστάται όταν το εσωτερικό προσωπικό δεν είναι εξοικειωμένο με τις εξωτερικές αναθέσεις για την υπηρεσία που προορίζεται να ανατεθεί ή αν δεν υπάρχουν επαρκείς εσωτερικοί πόροι. Το εσωτερικό προσωπικό που διαχειρίζεται τις εσωτερικές λειτουργίες που ανατίθενται, θα πρέπει να συμμετάσχει στη διαδικασία λήψης αποφάσεων (Schniederjans, 2007) (Sparrow, 2003).

Πολλοί οργανισμοί και ιδίως οι κρατικές υπηρεσίες, χρησιμοποιούν συγκεκριμένα πρότυπα για τη διενέργεια των αξιολογήσεων εξωτερικών αναθέσεων. Ωστόσο, πολλές φορές η τελική απόφαση επηρεάζεται σε μεγάλο βαθμό από το συναίσθημα και την υποκειμενικότητα. Οι προτιμήσεις και οι προδιαθέσεις των αναλυτών συχνά αλλάζουν τα αποτελέσματα των αξιολογήσεων εξωτερικής ανάθεσης. Οι αναλυτές, από καιρό σε καιρό, προσαρμόζουν τα στοιχεία κατάλληλα για να τους δώσουν τα αποτελέσματα που επιθυμούν. Αυτό μπορεί να μην έχει κακόβουλο χαρακτήρα, αφού η προκατάληψη των αναλυτών μπορεί να είναι υποσυνείδητη. Σε άλλη περίπτωση, αν ένας αναλυτής, πιστεύει ότι ο ίδιος θα επηρεαστεί αρνητικά σε προσωπικό επίπεδο από την απόφαση εξωτερικής ανάθεσης, ενδέχεται να προκαλέσει σκοπίμως λανθασμένα αποτελέσματα. Για αυτούς τους λόγους, πολλοί οργανισμοί επιλέγουν να χρησιμοποιήσουν εξωτερικούς συμβούλους για τη διενέργεια αυτών των αναλύσεων οι οποίο τους κοστίζουν ακριβά. Η επιλογή των εξωτερικών συμβούλων θα πρέπει να γίνεται και αυτή προσεκτικά. Οι οργανισμοί θα πρέπει να ελέγχουν αν οι εξωτερικοί σύμβουλοι έχουν κάποιο συμφέρον από την εξωτερική ανάθεση την οποία καλούνται να αναλύσουν (Sparrow, 2003). Τα κύρια κόστη και οφέλη της διαδικασίας αξιολόγησης ακολουθούν στην συνέχεια.

Κόστη κατά την φάση απαιτήσεων

Ενώ, σε ορισμένες περιπτώσεις, οι επιλογές μπορεί να είναι προφανείς, ως επί το πλείστων είναι απαραίτητο να καθοριστούν και να τεκμηριωθούν τυπικά οι απαιτήσεις, ιδιαίτερα οι απαιτήσεις ασφάλειας λειτουργειών, είτε αυτές εκτελούνται εσωτερικά είτε εξωτερικά. Τα κόστη που προκύπτουν από τη φάση των απαιτήσεων απεικονίζονται στον Πίνακας 5.

Πίνακας 5:*Κόστη κατά την φάση απαιτήσεων*

Εσωτερικά κόστη προσωπικού	
Άμεσα	Μισθοί Προνόμια

	Έξοδα ταξιδιών και διαμονής όπως πτήσεις, γεύματα, ξενοδοχεία κ.ά.
Έμμεσα	Διάφορες χορηγήσεις όπως χώροι εργασίας, τηλέφωνα, υπολογιστές, δίκτυα, διαχειριστικά κόστη κ.ά.
Άμεσα έξοδα συμβούλων	Ωριαίες ή ημερήσιες χρεώσεις ανά κατηγορία παρεχόμενης υπηρεσίας Έξοδα ταξιδιών και διαμονής όπως πτήσεις, γεύματα, ξενοδοχεία κ.ά. Διαχειριστικά κόστη Αναλώσιμα, εξοπλισμός, δίκτυα κ.ά.
Άλλα κόστη	
Άμεσα	Άδειες και συντήρηση λογισμικού Συντήρηση και ενοικίαση εξοπλισμού και υπολογιστών Συνδρομή σε υπηρεσίες πληροφόρησης και παροχής συμβουλών
Έμμεσα	Αδυναμία ανταπόκρισης στις προσδοκίες των χρηστών Μείωση του επιπέδου ικανοποίησης πελατών Απώλεια φήμης

Οφέλη κατά την φάση απαιτήσεων

Η φάση των απαιτήσεων είναι εξαιρετικά κρίσιμη για την επιτυχία του έργου εξωτερικής ανάθεσης και αντιπροσωπεύει σε μεγαλύτερο βαθμό την σχέση οφέλους – κόστους από κάθε άλλη φάση κατά τη διαδικασία λήψης αποφάσεων. Τα οφέλη από τον προσεκτικό προσδιορισμό των απαιτήσεων είναι τα παρακάτω:

- Μεγαλύτερη ακρίβεια απαιτήσεων: Οδηγούν σε ρεαλιστικές εκτιμήσεις κόστους, σε σωστό σχεδιασμό και σε αποδοτική υλοποίηση του έργου.
- Χαμηλότερα κόστη υλοποίησης και συντήρησης: Το χαμηλότερο κόστος είναι άμεσο αποτέλεσμα λεπτομερών και συμφωνημένων απαιτήσεων, καθώς υπάρχει μεγαλύτερη πιθανότητα το τελικό αποτέλεσμα να ικανοποιεί τις αρχικές απαιτήσεις και τις προσδοκίες του οργανισμού.
- Ταχύτερος χρόνος εισαγωγής στην αγορά: Η αποφυγή λαθών και διορθωτικών ενεργειών κατά την υλοποίηση του έργου επηρεάζει τον χρόνο ολοκλήρωσης του έργου.

Η εισαγωγή της κατάλληλης εμπειρογνωμοσύνης σε αυτό το στάδιο, ιδιαίτερα από άτομα με μεγάλη εμπειρία στο εξεταζόμενο εγχείρημα, μπορεί να βελτιώσει σημαντικά το τελικό

αποτέλεσμα και να αποφύγει πολλές από τις παγίδες που συναντιούνται στις εξωτερικές αναθέσεις.

3.2.3 Κόστη αιτημάτων προσφορών και πληροφοριών

Η προετοιμασία των αιτημάτων προσφορών (Request for Proposal - RFP) και των αιτημάτων πληροφοριών (Request for Information - RFI) αυξάνει περαιτέρω τις δαπάνες των οργανισμών. Σε αυτές τις δαπάνες περιλαμβάνονται τα κόστη της έρευνας των πληροφοριών, της δημιουργίας εγγράφων, της δημιουργία λίστας παραληπτών, της αναπαραγωγής και διανομής των εγγράφων, της λήψης των απαντήσεων, της παρακολούθησης και την ανάλυσης των αποτελεσμάτων. Αυτές οι διαδικασίες μπορούν να πραγματοποιηθούν από το εσωτερικό προσωπικού του οργανισμού, να ανατεθούν σε εξωτερικούς συμβούλους ή με την συνεργασία και των δύο. Πολλά από αυτά τα κόστη είναι κρυφά, αλλά θα πρέπει να εντοπίζονται και να υπολογίζονται στα έργα εξωτερικής ανάθεσης.

Τα μεγάλα RFI και RFP μπορεί να απαιτούν μήνες υλοποίησης και επιβαρύνουν τους οργανισμούς με σημαντικά συμβουλευτικά έξοδα για την προετοιμασία και τη διαχείρισή τους. Το μέγεθος αυτής της προσπάθειας εξαρτάται από το μέγεθος του έργου. Για ιδιαίτερα κρίσιμες αποφάσεις, όπως αυτή των εξωτερικών αναθέσεων κρίσιμων εσωτερικών υπηρεσιών, η έμφαση στα στάδια συλλογής πληροφοριών και αξιολογήσεων αποδίδει. Οι μικρότεροι οργανισμοί, μπορεί να μην μπορούν να ανταποκριθούν σε RFI ή RFP επειδή το κόστος μπορεί να είναι απαγορευτικό. Σε αυτές τις περιπτώσεις τα έργα συνήθως ανατίθενται στους μεγαλύτερους και πιο γνωστούς εξωτερικούς παρόχους. Κατά συνέπεια, οι μικρότεροι εξωτερικοί πάροχοι υπηρεσιών αποκλείονται αυτομάτως, παρόλο που ενδέχεται να διαθέτουν πολύ μεγάλη εξειδίκευση. Τα RFI και τα RFP κοστίζουν στους οργανισμούς, αλλά παρέχουν σημαντικά οφέλη στη διαδικασία αξιολόγησης και επιλογής εξωτερικών παρόχων, μειώνοντας με αυτόν τον τρόπο τον κίνδυνο μιας κακής επιλογής (Butler, 2000) (Halvey & Melby, 2007).

Τα RFI και RFP, εκτός από τους οργανισμούς, επιβαρύνουν οικονομικά και τους εξωτερικούς παρόχους οι οποίοι συμμετέχουν στην διαδικασία αξιολόγησης μιας εξωτερικής ανάθεσης. Τα κόστη για τους οργανισμούς και για τους εξωτερικούς παρόχους αναλύονται παρακάτω.

Κόστη για τους οργανισμούς

Τα κόστη που σχετίζονται με την προετοιμασία και την υλοποίηση των RFI και RFP περιλαμβάνουν κυρίως τους μισθούς των εσωτερικών υπαλλήλων ή των εξωτερικών συμβούλων. Η διαδικασία συνήθως περιλαμβάνει τα παρακάτω βήματα:

1. Έλεγχος σκοπιμότητας
2. Έγκριση από τη διοίκηση για την υλοποίηση RFI / RFP
3. Δημιουργία RFI / RFP
4. Δημιουργία λίστας υποψήφιων εξωτερικών παρόχων
5. Διανομή των εγγράφων με ηλεκτρονική ή έντυπη μορφή
6. Απάντηση σε ερωτήματα εξωτερικών παρόχων
7. Λήψη απαντήσεων από τους εξωτερικούς παρόχους
8. Ανάλυση των απαντήσεων
9. Προετοιμασία και παρουσίαση αποτελεσμάτων

Άλλα κόστη τα οποία μπορεί να προκύψουν:

- Κόστη ερευνών, συμβουλευτικών υπηρεσιών, βιβλία και συνδρομές
- Κόστη εξοπλισμού, γραμμών επικοινωνίας και γραφείων
- Κόστη μεταφοράς και διαμονής προσωπικού
- Κόστη που αφορούν στην εκτύπωση και την αποστολή εγγράφων

Κόστη των εξωτερικών παρόχων

Τα κόστη που σχετίζονται με την ανταπόκριση των εξωτερικών παρόχων σε RFI και RFP είναι παρόμοια με εκείνα των οργανισμών και περιλαμβάνουν τους μισθούς και τις υπερωρίες του προσωπικού τους για τα παρακάτω:

1. Έλεγχος σκοπιμότητας για την συμμετοχή στο συγκεκριμένο έργο εξωτερικής ανάθεσης
2. Έγκριση από τη διοίκηση για την ανταπόκριση στο συγκεκριμένο RFI ή RFP
3. Ανάλυση του RFI ή RFP και καθορισμός του περιεχομένου ανταπόκρισης
4. Προετοιμασία του εγγράφου ανταπόκρισης και της παρουσίασης αν κρίνεται απαραίτητο
5. Αποστολή των σχετικών εγγράφων στον οργανισμό που διεξάγει τον διαγωνισμό με ηλεκτρονική ή έντυπη μορφή
6. Ανταπόκριση σε ερωτήματα μέσω τηλεφώνου, email ή μέσω συνάντησης
7. Τελικές προσαρμογές στο παραδοτέο έγγραφο ανταπόκρισης

Άλλα κόστη τα οποία μπορεί να προκύψουν:

- Κόστη εξοπλισμού, γραμμών επικοινωνίας και γραφείων
- Κόστη μεταφοράς και διαμονής προσωπικού
- Κόστη που αφορούν στην εκτύπωση και στην αποστολή εγγράφων

3.2.4 Οφέλη αιτημάτων προσφορών και πληροφοριών

Στην συνέχεια θα περιγράψουμε τα οφέλη που προσφέρουν στους οργανισμούς και στους εξωτερικούς παρόχους τα σωστά δομημένα και υλοποιημένα RFI και RFP.

Οφέλη για τους οργανισμούς

Η εφαρμογή σωστά δομημένων και κατασκευασμένων RFI ή RFP προσφέρει πολλαπλά οφέλη στους οργανισμούς. Η εξέταση των απαιτήσεων, μέσω ερωτημάτων, για τον προσδιορισμό του βαθμού στον οποίο οι πάροχοι υπηρεσιών μπορούν να ικανοποιήσουν αυτές τις απαιτήσεις, μειώνει τον κίνδυνο έλλειψης βασικών κριτηρίων απόφασης. Οι απαντήσεις σε αυτά τα ερωτήματα, αποκλείουν γρήγορα τους υποψηφίους που δεν καλύπτουν τα βασικά κριτήρια επιλογής και οδηγούν σε έναν σύντομο κατάλογο τριών ή τεσσάρων σοβαρών υποψηφίων. Αυτό μειώνει την προσπάθεια και περιορίζει την απώλεια χρήσης πόρων προσωπικού τόσο για τους οργανισμούς όσο και για τους εξωτερικούς παρόχους.

Συνήθως, οι μεγάλοι εξωτερικοί πάροχοι αποστέλλουν εντυπωσιακές προτάσεις, οι οποίες είναι χρονοβόρες, λεπτομερείς και δαπανηρές. Η εμφάνιση μιας πρότασης δεν θα πρέπει απαραίτητα να ληφθεί ως δείκτης ικανότητας. Οι οργανισμοί θα πρέπει να είναι σε θέση να αξιολογήσουν αυτές τις προτάσεις και να εντοπίσουν τα σημεία που τους ενδιαφέρουν. Κατά τη διάρκεια των διαπραγματεύσεων συχνά προκύπτουν διαφωνίες μεταξύ των οργανισμών και των εξωτερικών παρόχων ως προς τα ζητούμενα των RFP. Αυτό συνήθως συμβαίνει λόγω ελλιπών στοιχειών και τεκμηρίωσης και από τις δύο πλευρές στα πλαίσια του διαγωνισμού ανάθεσης. Είναι σαφές ότι τα παραπάνω οφέλη είναι άυλα και δεν μπορούν εύκολα να μετρηθούν με συγκεκριμένους όρους χρημάτων. Εντούτοις, μπορούν να συμπεριληφθούν σε μια εκτίμηση κινδύνου με ευρείες εκτιμήσεις για το πόσο μπορεί να μειωθεί ο κίνδυνος των προβλημάτων ως αποτέλεσμα μιας υγιούς διαδικασίας RFI και RFP.

Μια διεξοδική διαδικασία RFI και RFP μπορεί επίσης να συμβάλει στην μείωση της τιμής των προσφερόμενων υπηρεσιών. Οι αναλυτικές οικονομικές προτάσεις επιτρέπουν τους οργανισμούς να εξετάσουν όλο το φάσμα των τιμών προκειμένου να επιλέξουν την υπηρεσία ή την λειτουργία που παρέχει περισσότερα στο μικρότερο κόστος. Η διαπραγμάτευση των τιμών συνήθως είναι ευκολότερη για τους οργανισμούς όταν ο κατάλογος των υποψήφιων εξωτερικών παρόχων είναι μεγάλος (Butler, 2000) (Halvey & Melby, 2007).

Οφέλη για τους εξωτερικούς παρόχους

Όπως προαναφέραμε οι εξωτερικοί πάροχοι καταναλώνουν πολλές ανθρωποώρες για να την εξέταση και την απάντηση σε RFI και RFP. Η εν λόγω διαδικασία δεν θα υπήρχε εάν δεν υπήρχαν σημαντικά οφέλη και για αυτούς. Εάν ένας εξωτερικός πάροχος δεν βρίσκεται στην λίστα υποψηφίων, τότε δεν θα συμμετάσχει στον διαγωνισμό ανάθεσης. Αν συμμετάσχει κάνοντας μια έντιμη και διεξοδική προσπάθεια και αποτύχει, είναι πιθανό να ληφθεί υπόψη σε μελλοντικά RFI και RFP του οργανισμού ή να διαφημιστεί από αυτόν σε άλλους οργανισμούς του κλάδου. Είναι προτιμότερο, από άποψη αξιοπιστίας και φήμης, να αρνηθεί να υποβάλει προσφορές για δεσμεύσεις τις οποίες δεν μπορεί να καλύψει είτε δεν έχει την κατάλληλη τεχνογνωσία ή ικανότητα, παρά να υποβάλει προσφορά, να κερδίσει και στην συνέχεια να αποτύχει. Αντιθέτως, εάν ένας εξωτερικός πάροχος δεν απαντήσει καθόλου, ακόμη και να επιβεβαιώσει την παραλαβή του αιτήματος και την απροθυμία του να υποβάλει προσφορά, είναι πιθανό να αφαιρεθεί από τον κατάλογο υποψηφίων και ως αποτέλεσμα δεν θα συμμετάσχει σε μελλοντικούς διαγωνισμούς (Butler, 2000) (Halvey & Melby, 2007).

3.2.5 Καθορισμός δήλωσης εργασιών

Ο κύριος σκοπός του RFI είναι να συγκεντρώσει επαρκείς πληροφορίες για να αποφασιστεί εάν ο οργανισμός θα προχωρήσει ή όχι σε RFP. Αν αποφασίσει να προχωρήσει, οι πληροφορίες που θα αποκτηθούν μέσω του RFI θα βοηθήσουν τον οργανισμό στην ανάπτυξη του RFP. Το RFP θα πρέπει να περιλαμβάνει την περιγραφή του έργου, τις απαιτήσεις και τη δήλωση εργασιών (Statement of Work - SOW) στα οποία θα βασιστούν οι υποψήφιοι εξωτερικοί πάροχοι για να υλοποιήσουν τις προτάσεις τους. Όσο πληρέστερο και ακριβέστερο είναι το RFP, τόσο πιο πλήρες θα είναι το SOW.

Οι απαντήσεις σε ένα RFP από διάφορους υποψηφίους, αναδεικνύουν τυχόν παραλείψεις στο SOW οι οποίες και ενδέχεται να οδηγήσουν στην αναθεώρηση του. Για την αναθεώρηση του SOW θα δαπανηθούν πόροι και θα υπάρξουν κόστη τα οποία ο οργανισμός ελπίζει να αποσβέσει μέσω της σωστής υλοποίησης του έργου εξωτερικής ανάθεσης. Η επικαιροποιημένη έκδοση του SOW, θα πρέπει να αποσταλεί μόνο στον σύντομο κατάλογο υποψηφίων, υπό την προϋπόθεση ότι οι αλλαγές δεν ήταν αρκετά σημαντικές ώστε να δικαιολογούν την μη επανάληψη ολόκληρης της διαδικασίας του RFP. Αυτό φυσικά δεν συμβαίνει πάντοτε. Στην περίπτωση που πραγματοποιηθούν σημαντικές αλλαγές στο SOW, τότε η επανάληψη της διαδικασίας του RFP θα πρέπει να επιβληθεί.

Οι οργανισμοί είναι προτιμότερο να δαπανήσουν παραπάνω κεφάλαια σε αυτό το στάδιο από το να προχωρήσουν με ένα ελλιπές SOW το οποίο πιθανών θα τους οδηγήσει σε αρνητικά αποτελέσματα. Παρόλο που τα οφέλη για τους οργανισμούς είναι σαφή,

υπάρχουν και οφέλη για τους εξωτερικούς παρόχους υπηρεσιών. Η μεγαλύτερη ικανοποίηση των πελατών τους καθώς και το μικρότερο κόστος υλοποίησης, είναι κάποια από αυτά (Power, 2006).

3.2.6 Συμφωνίες επιπέδου υπηρεσιών

Το SOW όπως αναφέραμε, περιγράφει τις φάσεις υλοποίησης του έργου εξωτερικής ανάθεσης και τον τρόπο με τον οποίον ο εξωτερικός πάροχος θα αποκρίνεται στα αιτήματα υποστήριξης για τις ανατιθέμενες υπηρεσίες. Επομένως, όσο πιο ακριβές είναι το SOW, τόσο δομημένο και δεσμευτικό, ως προς τον εξωτερικό πάροχο, θα είναι και το συμφωνητικό επιπέδου υπηρεσιών. Το SLA πρέπει να εμβαθύνει πολύ περισσότερο από το SOW στην περιγραφή των απαιτήσεων που πρέπει να καλύψει ο εξωτερικός πάροχος υπηρεσιών προκειμένου να ικανοποιήσει τον πελάτη καθώς και, στις συνέπειες της μή τήρησης των απαιτήσεων αυτών.

Το SOW απαιτεί την προσοχή και την εμπλοκή του προσωπικού που βρίσκεται πιο κοντά στη διαδικασία που ανατίθεται σε εξωτερικούς συνεργάτες, όπως το τμήμα πληροφορικής και το τμήμα διαχείρισης έργων. Η οριστικοποίηση του SOW απαιτεί ανασκοπήσεις και απαντήσεις από τα στελέχη και τα διευθυντικά μέλη της ομάδας των εξωτερικών παρόχων. Από την άλλη, για την προετοιμασία και τη διαπραγμάτευση του SLA θα πρέπει να συμμετάσχουν και άλλα τμήματα των οργανισμών όπως το νομικό τμήμα και το τμήμα συμμόρφωσης. Το SLA θα πρέπει να περιγράφει τις προσδοκίες του οργανισμού από τον εξωτερικό πάροχο και τα μέσα απομάκρυνσής του σε περίπτωση αποκλίσεων από αυτές.

Η προετοιμασία ενός ισχυρού SLA μπορεί να είναι μια απαιτητική, χρονοβόρα και δαπανηρή διαδικασία, ανάλογα με την κρισιμότητα και την πολυπλοκότητα των ανατεθέντων υπηρεσιών. Επίσης, το SLA είναι πολύ σημαντικό για την μακροχρόνια λειτουργία της εξωτερικής ανάθεσης. Τα κόστη που σχετίζονται με την προετοιμασία του SLA, είναι κατά βάση ίδια ανά κατηγορία με εκείνα που αφορούν την προετοιμασία των απαιτήσεων RFI και RFP, εκτός από την εμπλοκή των νομικών τμημάτων και των τμημάτων συμμόρφωσης τα οποία θα πρέπει να συμπεριλαμβάνονται (Power, 2006) (Solli-Saether H. , 2010).

Το SOW θα πρέπει να συμπεριλαμβάνει τις παρακάτω φάσεις τους έργου εξωτερικής ανάθεσης.

Φάση υλοποίησης

Η διαδικασία της υλοποίησης περιλαμβάνει διάφορα στάδια, τα κόστη των οποίων, θα πρέπει να εντοπιστούν και να συμπεριληφθούν στον έλεγχο σκοπιμότητας του έργου

εξωτερικής ανάθεσης. Επειδή αυτά τα κόστη συνήθως είναι εκτιμήσεις, ο οργανισμός οφείλει να καταβάλει κάθε δυνατή προσπάθεια για να επιτευχθούν όσο το δυνατόν ακριβέστερες εκτιμήσεις.

Τα κύρια στοιχεία που πρέπει να ληφθούν υπόψιν είναι:

- Η μετάβαση από εσωτερικές υπηρεσίες σε υπηρεσίες εξωτερικών παρόχων
- Η εφαρμογή των ελέγχων διαχείρισης καθώς και, η χρήση συστημάτων μέτρησης, ελέγχου και αναφοράς
- Η εισαγωγή διαδικασιών επίλυσης διαφορών
- Η εφαρμογή και ο έλεγχος των διαδικασιών έκτακτης ανάγκης
- Η ανάπτυξη μιας διαδικασίας τερματισμού λόγω αναμενόμενων ή μή αναμενόμενων γεγονότων

Φάση μετάβασης

Η φάση της μετάβασης στον εξωτερικό πάροχο είναι η λιγότερο κατανοητή και η πιο υποτιμημένη φάσης της διαδικασίας εξωτερικής ανάθεσης. Συχνά συνοδεύεται από αλλαγές στην τεχνολογία των πληροφοριών και τις επιχειρησιακές διαδικασίες, οι οποίες από μόνες τους είναι δύσκολο να αντιμετωπιστούν. Τα οφέλη μιας ομαλής μετάβασης είναι δύσκολο να ποσοτικοποιηθούν, αν και είναι πολύ προφανή για κάποιον που έχει εμπλακεί σε μια κακώς προγραμματισμένη μετάβαση.

Στις περισσότερες φάσεις μετάβασης υπάρχει μια περίοδος παράλληλης λειτουργίας των εσωτερικών και των εξωτερικών υπηρεσιών. Οι οργανισμοί δεν θα πρέπει να υποτιμούν τη διάρκεια αυτής της περιόδου, διότι μπορεί να αυξήσει σημαντικά το συνολικό κόστος του έργου εξωτερικής ανάθεσης. Τα κύρια εμπόδια που μπορούν να επηρεάσουν αρνητικά το κόστος και τον χρόνο υλοποίησης των έργων εξωτερικής ανάθεσης, είναι επιγραμματικά τα παρακάτω:

- Υποεκτίμηση του χρόνου και των απαιτήσεων σε προσωπικό
  Αντιμετώπιση: Πρόσληψη έμπειρων στελεχών που έχουν συμμετάσχει σε αντίστοιχα έργα.
- Αλλαγή της εταιρικής στρατηγικής κατεύθυνσης
  Αντιμετώπιση: Επιλογή εξωτερικού παρόχου ο οποίος παρέχει ευελιξία σε τέτοιου είδους αλλαγές χωρίς απαίτηση για αποζημιώσεις.
- Μεταφορά της διαχείρισης των θεμάτων τεχνολογίας
  Αντιμετώπιση: Διαχωρισμός του έργου υλοποίησης σε πολλά μικρά παραδοτέα με βραχυπρόθεσμες προθεσμίες.
- Ασταθή τεχνολογία

Αντιμετώπιση: Ο οργανισμός θα πρέπει να αποδεχθεί την πιθανότητα να προκύψουν διάφορες τεχνικές δυσκολίες κατά την φάση μετάπτωσης. Η εμπλοκή έμπειρου εσωτερικού και εξωτερικού προσωπικού θα βοηθήσει στην επίλυση των τεχνικών δυσκολιών.

- Υπερεκτιμημένα οφέλη για το έργο
  Αντιμετώπιση: Ο οργανισμός θα πρέπει να επικεντρώσει στις άμεσες εξοικονομήσεις κόστους και να μην «δώσει βάρος» στα άυλα οφέλη.
- Υψηλά κόστη υλοποίησης
  Αντιμετώπιση: Ο οργανισμός θα πρέπει να εξετάσει το έργο μακροπρόθεσμα.

Τα κόστη και τα οφέλη που σχετίζονται με την φάση της μετάβασης είναι τα παρακάτω:

- Κόστη απαξίωσης (στις περιπτώσεις που ο οργανισμός χρησιμοποιεί παλιά τεχνολογία και ο εξωτερικός πάροχος σύγχρονη τεχνολογία)
- Δαπάνες που οφείλονται στην αδυναμία υποστήριξης ή / και διαχείρισης των καινούργιων τεχνολογιών από το εσωτερικό προσωπικό λόγω έλλειψης τεχνογνωσίας
- Υψηλό και αυξανόμενο κόστος συντήρησης για παλαιότερο εξοπλισμό
- Υψηλό και αυξανόμενο κόστος υποστήριξης για παλαιότερο λογισμικό
- Κίνδυνος διακοπής της υποστήριξης από τον κατασκευαστή
- Έλλειψη νέων δυνατοτήτων που μπορεί να θεωρηθούν δεδομένες

Πρόσθετα κόστη μετάβασης:

- Πρόσληψη έμπειρου προσωπικού
- Εκπαίδευση υφιστάμενου και νέου προσωπικού
- Εκμάθηση κατά την εργασία (μειωμένη παραγωγικότητα)
- Κόστη επαναφοράς λειτουργιών σε περίπτωση δυσλειτουργιών
- Απώλεια αξιοπιστίας από χαμένες προθεσμίες και ανεπαρκή συστήματα
- Μη επαρκή διαχείριση έργου μετάπτωσης

Τα πλεονεκτήματα μετάβασης, αν η εξωτερική ανάθεση έχει εγκαταστήσει πιο ευέλικτες και κλιμακούμενες τεχνολογίες, είναι τα παρακάτω:

- Υποδομή και αρχιτεκτονική που μπορεί να υποστηρίξει μελλοντικές λειτουργίες ή υπηρεσίες
- Πιο ευέλικτες, προσαρμόσιμες τεχνολογίες που είναι πιο εύκολο να υποστηριχθούν και να διορθωθούν
- Διαθεσιμότητα προηγμένων εργαλείων σχεδίασης, ανάπτυξης και δοκιμών

- Βελτίωση των δεξιοτήτων του προσωπικού που εμπλέκεται στο έργο

Η ποσοτικοποίηση των δαπανών και οφελών για πολλές από τις παραπάνω κατηγορίες είναι δύσκολη, αλλά ορισμένες εκτιμήσεις είναι δυνατές και πρέπει να γίνουν από τους οργανισμούς για να έχουν μια καλή εικόνα των σχετικών δαπανών και οφελών. Οι οργανισμοί θα πρέπει να κατανοήσουν ότι θα πρέπει να περάσουν από την φάση της μετάβασης ώστε να αξιοποιήσουν τα οφέλη που θα τους δώσει το νέο περιβάλλον και οι νέες τεχνολογίες του εξωτερικού παρόχου.

Παρακολούθηση, αναφορά και ανασκόπηση

Η χρήση SLA απαιτεί τον υπολογισμό και την αναφορά συγκεκριμένων μετρήσεων. Αυτές οι μετρήσεις θα πρέπει να απαιτούνται, τόσο στις φάσεις του RFI όσο και στις φάσεις του RFP, όπως η ασφάλεια, η παρακολούθηση, η αναφορά και η ανασκόπηση που θα πρέπει να ενταχθούν στις διαδικασίες εξ' αρχής. Εντούτοις, υπάρχει κόστος, τόσο για την ανάπτυξη και την εφαρμογή των προγραμμάτων μέτρησης όσο και για την αναθεώρηση, την υποβολή εκθέσεων και την αντιμετώπιση εξαιρέσεων κατά την εφαρμογή της υπηρεσίας. Αυτό το κόστος είναι συνήθως μικρό. Ορισμένες μετρήσεις, όπως αυτές που σχετίζονται με την ασφάλεια, είναι πιο δύσκολο να πραγματοποιηθούν. Στις περιπτώσεις αυτές, το SLA αντί να απαιτεί τη χρήση συγκεκριμένων μέτρων ασφάλειας από τον εξωτερικό πάροχο, απαιτεί τη διεξαγωγή περιοδικών δοκιμών και αξιολογήσεων ασφάλειας.

Επίλυση διαφορών

Οι οργανισμοί θα πρέπει να έχουν στη διάθεσή τους τα μέσα και τις διαδικασίες για την επίλυση τυχών διαφορών με τους εξωτερικούς παρόχους. Το κόστος που περιβάλλει την επίλυση διαφορών, αποτελεί μια από τις πιο ασαφείς απώλειες για τους οργανισμούς και τους εξωτερικούς παρόχους. Και τα δύο μέρη, θα πρέπει να συμφωνήσουν εξ' αρχής για το πώς θα αντιμετωπίζουν αυτές τις διαφορές. Αυτό είναι σαφώς καλύτερο από το να επικαλεστούν τους όρους της συμφωνίας, αντιμετωπίζοντας τις διαφορές τους σε νομικό επίπεδο.

Αντιμετώπιση περιστατικών, αποκατάσταση και δοκιμή

Οι φυσικές καταστροφές και οι τρομοκρατικές ενέργειες τα τελευταία χρόνια ευαισθητοποίησαν τους οργανισμούς και τους οδήγησαν στην αναζήτηση μέτρων ασφάλειας για την αντιμετώπισή τους. Η διασφάλιση της επιχειρησιακής συνέχειας και η ανάκαμψη από καταστροφές αποτελούν βασικές απαιτήσεις των οργανισμών από τους εξωτερικούς παρόχους. Οι απαιτήσεις αυτές, είναι συνήθως εξαιρετικά δαπανηρές και το κόστος τους θα πρέπει να περιλαμβάνεται στο κόστος των προσφερόμενων υπηρεσιών.

Το κόστος των υπηρεσιών για ένα περιβάλλον υψηλής διαθεσιμότητας, είναι κατά 25% έως 50% μεγαλύτερο, ανάλογα με την γεωγραφική κατανομή των υπηρεσιών του εξωτερικού παρόχου. Η κρισιμότητα των ανατεθέντων υπηρεσιών είναι το κύριο κριτήριο για την επιλογή ενός περιβάλλοντος υψηλής διαθεσιμότητας από τους οργανισμούς. Η ανάλυση κινδύνου καθώς και η χρήση υπηρεσιών ασφάλισης για την αντιστάθμιση του κινδύνου, είναι μέθοδοι οι οποίες μπορούν να βοηθήσουν τους οργανισμούς προς αυτή την κατεύθυνση.

Τερματισμός συνεργασίας

Ο τερματισμός της συνεργασίας με τον εξωτερικό πάροχο μπορεί να δημιουργήσει σημαντικά κόστη τόσο για τον οργανισμό, όσο και για τον εξωτερικό πάροχο. Στην αρχική ανάλυση εξωτερικής ανάθεσης, τα ενδεχόμενα κόστη μεταφοράς σε άλλον εξωτερικό πάροχο θα πρέπει να υπολογίζονται. Η μετάβαση σε άλλον εξωτερικό πάροχο μπορεί να εξελιχθεί κανονικά, στις περιπτώσεις που η απομάκρυνση από τον υφιστάμενο εξωτερικό πάροχο γίνεται σύμφωνα με τους όρους και τις προϋποθέσεις της σύμβασης. Υπάρχουν όμως και περιπτώσεις που η απομάκρυνση από τον υφιστάμενο εξωτερικό πάροχο είναι αποτέλεσμα ενός ξαφνικού γεγονότος, όπως για παράδειγμα η πτώχευση, η ολική απώλεια υπηρεσιών του παρόχου λόγω φυσικών καταστροφών, πολέμου κ.ά. Οι οργανισμοί για να είναι καλύτερα προετοιμασμένοι, θα πρέπει να αναλύσουν με βάση τις πιθανότητες κάθε πιθανή έκβαση, υπολογίζοντας παράλληλα το κόστος και τις απώλειες που μπορεί να προκύψουν.

4. Κίνδυνοι των Εξωτερικών Αναθέσεων

Στο προηγούμενο κεφάλαιο περιγράψαμε τα κόστη των εξωτερικών αναθέσεων και τα οφέλη της διαδικασίας εξωτερικής ανάθεσης για τους οργανισμούς. Σε αυτό το κεφάλαιο θα αναλύσουμε τους κύριους κινδύνους των εξωτερικών αναθέσεων όπως η απώλεια ελέγχου, η αθέτηση όρων συμβολαίων ανάθεσης, η βιωσιμότητα, οι λόγοι εγκατάλειψης, η ποιότητα των προσφερόμενων υπηρεσιών, η εμπιστοσύνη, η απόδοση, η έλλειψη τεχνογνωσίας, τα κρυφά κόστη, οι δυνατότητες προσαρμογής , η μετάδοση γνώσης, τα κοινόχρηστα περιβάλλοντα και θα επεκταθούμε σε κανονιστικά και νομικά ζητήματα (O'Leary, 1990) (Lacity & Hirschheim, 1993) (Cross, 1995) (Earl, 1996).

Στον Πίνακας 6 απεικονίζονται οι αντικρουόμενοι και οι κοινοί στόχοι των οργανισμών και των εξωτερικών παρόχων, οι οποίοι επηρεάζουν το επίπεδο κινδύνου των εξωτερικών αναθέσεων.

Πίνακας 6*: Αντικρουόμενοι και κοινοί στόχοι Οργανισμών και Εξωτερικών Παρόχων*

Παράγοντας (Στόχος)	**Οργανισμός**	**Εξωτερικός πάροχος**
Κόστος ανά μονάδα υπηρεσίας (Αντικρουόμενος)	Επιθυμεί να αποκτήσει το μέγιστο από την υπηρεσία στο μικρότερο δυνατό κόστος μέσω: - Προσεκτικού ελέγχου στις υπηρεσίες και στα συναφή κόστη. - Προσφορών από πολλούς εξωτερικούς παρόχους. - Διαπραγμάτευσης για πιο χαμηλές τιμές.	Μακροπρόσθεσμη κερδοφορία μέσω: -Υψηλού λόγου τιμής προς κόστος. - Ευελιξίας στους τρόπους τιμολόγησης για τη δημιουργία πρόσθετων κερδών. - Μεγάλου όγκου τυποποιημένων υπηρεσιών. -Υψηλού επιπέδου διατηρησιμότητας πελατών. - Οικονομιών κλίμακος.
Ποιότητα υπηρεσιών (Αντικρουόμενος)	- Εγγυημένα επίπεδα υπηρεσιών, που τηρούν προκαθορισμένες απαιτήσεις, με υψηλό κόστος προστίμου σε περίπτωση που ο εξωτερικός πάροχος δεν πληροί τις προϋποθέσεις των επιπέδων υπηρεσιών. - Καταβολή αποζημίωσης σε περίπτωση απώλειας επιχειρηματικών λειτουργιών.	- Χαλαρό ή ανύπαρκτο επίπεδο απαιτήσεων υπηρεσιών με ελάχιστο πρόστιμο σε περίπτωση που δεν πληρούνται τα καθορισμένα επίπεδα υπηρεσιών.
Έλεγχος (Αντικρουόμενος)	- Διατηρεί τον έλεγχο διαθέτοντας εσωτερικά προσωπικό με τις απαιτούμενες δυνατότητες. - Παραδίδει τον έλεγχο και την ευθύνη στον εξωτερικό πάροχο.	- Προτιμά να έχει τον έλεγχο για να αποτρέψει τον οργανισμό να εγκαταλείψει (να μεταφέρει τις υπηρεσίες εσωτερικά ή να μεταφερθεί σε ανταγωνιστή).

	- Αποσύρει προσωπικό και συνάπτει σύμβαση παροχής υπηρεσιών με τον εξωτερικό πάροχο.	
Βιωσιμότητα εξωτερικού παρόχου (Κοινός)	- Επιθυμεί να διατηρήσει τον ίδιο εξωτερικό πάροχο και να επεκτείνει την σύμβαση λειτουργίας σε αυτόν. - Δεν επιθυμεί ξαφνικές αλλαγές που επηρεάζουν τον τρόπο λειτουργίας του εξωτερικού παρόχου οι οποίες θα μπορούσαν να οδηγήσουν σε διακοπή κρίσιμων υπηρεσιών (π.χ. αλλαγή ιδιοκτησίας).	- Θέλει να λειτουργεί μακροπρόθεσμα χωρίς λειτουργικά και διοικητικά προβλήματα. Η μακροπρόθεσμη βιωσιμότητα προσελκύει περισσότερους πελάτες.
Βιωσιμότητα οργανισμού (Κοινός)	- Επιθυμεί οικονομικά αποδοτικότερες εξωτερικές αναθέσεις οι οποίες θα του αυξήσουν την κερδοφορία και θα τον κάνουν πιο ανταγωνιστικό.	- Επιθυμεί να διαθέτει οικονομικά εύρωστους πελάτες οι οποίοι μπορούν να πληρώνουν τους λογαριασμούς τους.
Εγκατάσταση (Κοινός)	- Επιθυμεί την ανώδυνη και γρήγορη μεταφορά των υπηρεσιών στον εξωτερικό πάροχο.	- Επιθυμεί αποτελεσματική και γρήγορη εγκατάσταση για να πληρωθεί.
Διακοπή (Αντικρουόμενος)	- Ανώδυνη για τον οργανισμό εφόσον το επιλέξει και το σχεδιάσει σωστά.	- Επώδυνη για τον εξωτερικό πάροχο διότι χάνει πελατολόγιο και κέρδη.
Λειτουργία (Κοινός)	- Επιθυμεί την εύκολη ενσωμάτωση από τον εξωτερικό πάροχο, υπηρεσιών και συστημάτων με άλλους οργανισμούς.	- Επιθυμεί το ίδιο, διότι στόχος του είναι η μακροχρόνια συνεργασία με τους οργανισμούς.
Ευελιξία (Κοινός)	- Επιθυμεί τα συστήματα του εξωτερικού παρόχου να είναι ευέλικτα και να προσαρμόζονται ανάλογα με τις απαιτήσεις του. - Το κόστος των υπηρεσιών θέλει να μεταβάλλεται ανάλογα με τους πόρους του εξωτερικού παρόχου που χρησιμοποιεί.	- Επιθυμεί τα συστήματα και οι υπηρεσίες που προσφέρει να είναι επεκτάσιμα ώστε να μπορούν να καλύψουν επιπλέον ανάγκες των πελατών του. - Παρέχοντας όλο και περισσότερες υπηρεσίες στους πελάτες αυξάνει την κερδοφορία και τον κύκλο εργασιών του.
Πολυπλοκότητα (Αντικρουόμενος)	- Τα συστήματα και οι υπηρεσίες επιθυμεί να έχουν μικρό βαθμό πολυπλοκότητας	- Το κόστος για την υλοποίηση μη πολύπλοκων συστημάτων και υπηρεσιών είναι υψηλό.
Ευκολία χρήσης (Κοινός)	- Προτιμά τα συστήματα και τις υπηρεσίες που είναι απλές στην χρήση και χρειάζονται λιγότερη εκπαίδευση προσωπικού.	- Επιθυμεί τα συστήματα και οι υπηρεσίες που προσφέρει να είναι απλά για να μην χρειάζονται πολλές ώρες τεχνικής υποστήριξης.

Στην συνέχεια, θα περιγράφονται οι κύριοι κίνδυνοι που καλούνται να αντιμετωπίσουν οι οργανισμοί στα πλαίσια των εξωτερικών αναθέσεων.

4.1 Απώλεια ελέγχου

Όπως αναφέραμε και στα προηγούμενα κεφάλαια, ένας από τους σημαντικότερους λόγους επιλογής εξωτερικών αναθέσεων στους οργανισμούς, είναι η ολική ή η μερική μεταφορά της ευθύνης σε τρίτους. Υπάρχουν όμως οργανισμοί, οι οποίοι δεν επιθυμούν να μεταφέρουν σημαντικές λειτουργίες τους σε εξωτερικούς παρόχους διότι κρίνουν ότι με αυτόν τον τρόπο χάνουν τον έλεγχο από τα χέρια τους. Αυτό οφείλεται στις αντιλήψεις που έχει ο κάθε οργανισμός σχετικά με τις υπηρεσίες, τα κέρδη και την επιβίωση. Σαφώς και μεγάλο μέρος της ανησυχίας τους πηγάζει από τις υποψίες ότι, ο εξωτερικός πάροχος δεν θα έχει τον ίδιο βαθμό δέσμευσης για την ικανοποίηση των απαιτήσεων των υπηρεσιών όπως συμβαίνει στο εσωτερικό προσωπικό. Το εσωτερικό προσωπικό είναι πιο ευθυγραμμισμένο με τους στόχους, την αποστολή και την κουλτούρα του οργανισμού. Ωστόσο, αυτό μπορεί να αντισταθμιστεί με την σύναψη κατάλληλων συμφωνιών επιπέδου υπηρεσιών (Service Level Agreements - SLA). Οι συμφωνίες SLA, πραγματοποιούνται μεταξύ των οργανισμών και των εξωτερικών παρόχων και αποτελούν σημαντικό όπλο στα χέρια των οργανισμών.

Υπάρχουν θεμελιώδεις διαφορές στα κίνητρα, τους στόχους και τη στάση μεταξύ του εσωτερικού προσωπικού και του προσωπικού των εξωτερικών παρόχων. Αυτές οι διαφορές δεν είναι οι ίδιες και ποικίλουν ανάλογα με το μέγεθος των οργανισμών και των εξωτερικών παρόχων. Πολλές φορές σχετίζονται με τον τύπο τον παρεχόμενων υπηρεσιών και τις δεξιότητες που απαιτούνται από το εσωτερικό και το εξωτερικό προσωπικό. Οι διαφορές αυτές, επίσης μεταβάλλονται με την πάροδο του χρόνου, επειδή το προσωπικό στους οργανισμούς διαφοροποιείται παράλληλα με την φύση των λειτουργιών και επειδή υπάρχει μεγάλος ανταγωνισμός σε τοπικό, εθνικό και παγκόσμιο επίπεδο (Schniederjans, 2007) (Sparrow, 2003).

4.2 Βιωσιμότητα εξωτερικών παρόχων

Ένας από τους χειρότερους «εφιάλτες» των οργανισμών που αναθέτουν λειτουργίες σε εξωτερικούς παρόχους είναι, η πιθανότητα ο εξωτερικός πάροχος να σταματήσει την επιχειρηματική του δραστηριότητα με αποτέλεσμα να χάσουν την πρόσβαση σε κρίσιμες υπηρεσίες και συστήματα. Έχουν συμβεί αρκετές φορές στο παρελθόν τέτοια περιστατικά τα οποία προκάλεσαν ανεπανόρθωτες ζημιές σε οργανισμούς. Οι οργανισμοί για να μειώσουν αυτόν τον κίνδυνο, θα πρέπει να αξιολογούν πλήρως και λεπτομερέστατα τους εξωτερικούς παρόχους πριν προχωρήσουν σε οποιαδήποτε ανάθεση λειτουργιών. Στην συμφωνία ανάθεσης θα πρέπει να προβλεφθεί η πιθανότητα

τερματισμού λειτουργίας του εξωτερικού παρόχου και θα πρέπει να περιλαμβάνονται κατάλληλες διατάξεις για ένα τέτοιο γεγονός. Ως παράδειγμα θα μπορούσαμε να αναφέρουμε τα σχέδια εκτάκτου ανάγκης τα οποία θα πρέπει να δοκιμάζονται σε τακτική βάση από τους οργανισμούς για να διασφαλιστεί η λειτουργία τους όταν κριθεί απαραίτητο (Sparrow, 2003) (Schniederjans, 2007).

4.3 Αιτίες εγκατάλειψης υπηρεσιών

Υπάρχουν πολλοί λόγοι για τους οποίους ένας οργανισμός μπορεί να αποχωρήσει από έναν εξωτερικό πάροχο. Ορισμένοι από αυτούς οφείλονται σε εσωτερικούς παράγοντες όπως η κακή διαχείριση, η ανεπαρκής χρηματοδότηση και το εργατικό προσωπικό. Άλλοι, οφείλονται σε εξωτερικούς παράγοντες όπως οι τάσεις της τεχνολογίας ή βιομηχανίας, οι κάμψεις της οικονομίας, οι συγχωνεύσεις και οι εξαγορές. Μια από τις πιο «ύπουλες» αιτίες εγκατάλειψης ενός εξωτερικού παρόχου είναι η αρνητική επίπτωση στη φήμη του. Η αποχώρηση υφιστάμενων πελατών, η επιφυλακτικότητα των νέων πελατών στο να τον επιλέξουν, η απώλεια προσωπικού, τα δημοσιεύματα τύπου και η δημοσίευση αρνητικών σχολίων στο διαδίκτυο, είναι αποτελέσματα της αρνητικής φήμης (Sparrow, 2003). Οι συγχωνεύσεις και εξαγορές επίσης μπορούν να επηρεάσουν τους οργανισμούς. Οι εξαγορές θεωρούνται πιο κρίσιμες διότι στα πλαίσια αυτών, τίθεται το ερώτημα κατά πόσο η απορροφούσα εταιρεία επιθυμεί να συνεχίσει να χρησιμοποιεί τις ίδιες υπηρεσίες ή προτιμά να τερματίσει τη λειτουργία τους. Στις συγχωνεύσεις, υπάρχει ο κίνδυνος η απορροφούσα εταιρεία να μεταφέρει τις υπηρεσίες της εξαγοράζουσας εταιρείας στον εξωτερικό πάροχο που ίδια χρησιμοποιεί. Σε άλλες περιπτώσεις, η εξαγοράζουσα εταιρεία μπορεί να θέλει να παρέχει ή ίδια τις υπηρεσίες του εξωτερικού παρόχου για τις εσωτερικές της λειτουργίες. Τέτοιες αλλαγές απειλούν τους εξωτερικούς παρόχους και αντιπροσωπεύουν ρίσκο για τους πελάτες τους.

4.4 Μέγεθος πελατών

Ο κάθε πελάτης ενός εξωτερικού παρόχου κατά πάσα πιθανότητα καταλαμβάνει μόνο ένα μικρό ποσοστό του συνολικού φόρτου εργασίας του. Μερικές φορές οι μικρότεροι πελάτες θεωρούν ότι είναι «πολίτες δεύτερης κατηγορίας» σε σχέση με τους μεγαλύτερους από τους οποίους παράγονται τα περισσότερα κέρδη. Οι μεγαλύτεροι οργανισμοί απολαμβάνουν μεγαλύτερες εκπτώσεις τιμών, και οι υπηρεσίες τους υποστηρίζονται από το πιο εξειδικευμένο προσωπικό.

Στις περιπτώσεις γενικών προβλημάτων, οι μεγαλύτεροι οργανισμοί συνήθως εξυπηρετούνται με προτεραιότητα σε αντίθεση με τους μικρότερους οι οποίο αναμένουν να ελευθερωθεί προσωπικό υποστήριξης. Σε μια τέτοια ανταγωνιστική μάχη για

εξυπηρέτηση, οι οργανισμοί μπορούν να κερδίσουν προτεραιότητα, δημιουργώντας «θόρυβο», μεταφέροντας το ζήτημα στην ανώτερη διοίκηση του εξωτερικού παρόχου. Οι μικρότεροι οργανισμοί, μπορούν να επωφεληθούν, δημιουργώντας επιθετικά αιτήματα ή εκμεταλλεύοντας τυχόν προσωπικές σχέσεις με ανώτερα στελέχη του εξωτερικού παρόχου. Ακόμη, μπορεί να απευθυνθούν σε πρώην εργαζόμενους που έχουν μεταβεί στον εξωτερικό πάροχο, αποκτώντας έτσι προνομιακή πρόσβαση στους υπεύθυνους λήψης αποφάσεων. Επίσης, αξίζει να αναφερθεί, ότι οι μεγαλύτεροι οργανισμοί δημιουργούν οικονομίες κλίμακος οι οποίες μειώνουν το κόστος σε όλους, συμπεριλαμβανομένων των μικρότερων οργανισμών. Το μέγεθός τους και ο όγκος των υπηρεσιών που χρησιμοποιούν τους δίνει μεγάλη διαπραγματευτική δύναμη και ως αποτέλεσμα αυτής συνάπτουν καλύτερες συμφωνίες με τους εξωτερικούς παρόχους (Amant, 2009).

4.5 Ποιότητα υπηρεσιών

Ένας από τους κύριους λόγους εξωτερικών αναθέσεων είναι η προσδοκία για καλύτερη ποιότητα υπηρεσιών. Αυτή η προσδοκία συχνά βασίζεται στο ότι υπάρχει συγκεκριμένο συμβόλαιο SLA το οποίο ορίζει το επίπεδο των προσφερόμενων υπηρεσιών του εξωτερικού παρόχου και τα πρόστιμα τα οποία θα του καταλογίζονται στις περιπτώσεις που αποκλίνει από την τήρηση των όρων αυτού. Πολλές φορές οι οργανισμοί συνάπτουν συμβόλαια SLA και στις εσωτερικές λειτουργίες τους, είναι όμως δύσκολο να εφαρμοστούν εφόσον όλοι είναι «μέλη της ίδιας οικογένειας». Τα συμβόλαια SLA μεταξύ οργανισμών και εξωτερικών παρόχων σε γενικές γραμμές ορίζουν τι είναι αποδεκτό και τι όχι σε μια προσφερόμενη υπηρεσία. Επομένως, διαθέτουν ένα βασικό σύνολο όρων βάση των οποίων ορίζεται η ποιότητα των προσφερόμενων υπηρεσιών από τον εξωτερικό πάροχο. Στον Πίνακας 7 απεικονίζονται οι κύριοι όροι που θα πρέπει να συμπεριλαμβάνονται σε ένα συμβόλαιο SLA με εξωτερικό πάροχο.

Πίνακας 7: *Κύριοι όροι συμβολαίων SLA*

Προδιαγραφές
• Οι φυσικές εγκαταστάσεις και τα πληροφοριακά συστήματα του εξωτερικού παρόχου θα πρέπει να πληρούν τις απαραίτητες προδιαγραφές ασφάλειας και λειτουργίας. • Οι εργαζόμενοι του εξωτερικού παρόχου θα πρέπει να έχουν την κατάλληλη τεχνογνωσία και εξειδίκευση.
Αξιοπιστία
• Ο εξωτερικός πάροχος θα πρέπει να τηρεί τις υποσχέσεις του στους χρόνους που έχουν συμφωνηθεί.

• Ο εξωτερικός πάροχος θα πρέπει να παρέχει τις υπηρεσίες που συμφωνήθηκαν εντός του ορισμένου χρονοδιαγράμματος. • Στις περιπτώσεις δυσλειτουργιών ή σοβαρών προβλημάτων θα πρέπει να δείχνει ειλικρινές ενδιαφέρον για την επίλυσή τους. • Τα πληροφοριακά συστήματα του εξωτερικού παρόχου θα πρέπει να είναι αξιόπιστα. • Οι προσφερόμενες υπηρεσίες θα πρέπει να λειτουργούν σωστά και χωρίς λάθη.
Απόκριση
• Ο εξωτερικός πάροχος θα πρέπει να ενημερώνει τους πελάτες του για οποιοδήποτε ζήτημα προκύψει και αφορά στις υπηρεσίες που προσφέρει. • Το προσωπικό του εξωτερικού παρόχου θα πρέπει να εξυπηρετεί άμεσα τα αιτήματα των πελατών. • Οι υπάλληλοι του εξωτερικού παρόχου θα πρέπει να είναι πάντα πρόθυμοι να βοηθήσουν τους πελάτες. • Οι υπάλληλοι του εξωτερικού παρόχου θα πρέπει να είναι πάντα διαθέσιμοι να ανταποκριθούν στις ανάγκες των πελατών.
Διασφάλιση
• Η συμπεριφορά του προσωπικού του εξωτερικού παρόχου θα πρέπει να δημιουργεί εμπιστοσύνη στους πελάτες. • Οι πελάτες θα πρέπει να αισθάνονται ασφαλείς χρησιμοποιώντας τα πληροφοριακά συστήματα του εξωτερικού παρόχου. • Οι υπάλληλοι του εξωτερικού παρόχου θα πρέπει να είναι ευγενικοί με τους πελάτες. • Οι υπάλληλοι του εξωτερικού παρόχου θα πρέπει να γνωρίζουν καλά τη δουλειά τους.
Εν συναίσθηση
• Οι ώρες λειτουργίας του εξωτερικού παρόχου θα πρέπει να είναι κατάλληλες για όλους τους πελάτες. • Ο εξωτερικός πάροχος θα πρέπει να δίνει σε όλους τους πελάτες τη δέουσα προσοχή. • Ο εξωτερικός πάροχος θα πρέπει να κατανοεί τις ειδικές ανάγκες των πελατών του.

Πολλοί από τους παραπάνω όρους συνήθως δεν αναφέρονται στις συμβάσεις SLA αλλά είναι πολύ βασικοί για τη διαδικασία αξιολόγησης και επιλογής ενός εξωτερικού παρόχου. Οι όροι που αφορούν στην ασφάλεια των πληροφοριακών συστημάτων πολλές φορές δεν συμπεριλαμβάνονται στα συμβόλαια SLA. Αυτό οφείλεται στο ότι δεν υπάρχουν συγκεκριμένα πρότυπα για την μέτρηση του επίπεδου ασφάλειας και ούτε πρόκειται να υπάρξουν διότι το περιβάλλον στους οργανισμούς αλλάζει διαρκώς. Δεδομένου ότι η απόλυτη ασφάλεια δεν είναι εφικτή, τα μέτρα ασφάλειας που περιλαμβάνονται στα συμβόλαια SLA είναι και αυτά σχετικά. Παρόλα αυτά, τα ζητήματα ασφάλειας που σχετίζονται με τον βαθμό διαθεσιμότητας των συστημάτων και των δικτύων των εξωτερικών παρόχων είναι μετρήσιμα και μπορούν να εκφραστούν με ποσοτικούς όρους (Allen, Gabbard, May, Hayes, & Sledge, 2003) (Halvey & Melby, 2007).

4.6 Εμπιστοσύνη

Οι οργανισμοί είναι υπεύθυνοι για τη διασφάλιση και την προστασία των πληροφοριών των πελατών τους. Οι εξωτερικοί πάροχοι θα πρέπει να προστατεύουν αυτές τις πληροφορίες από μη εξουσιοδοτημένη πρόσβαση, κατάχρηση και αποκάλυψη. Όπως προαναφέραμε, οι αναδυόμενοι νόμοι και κανονισμοί προστασίας δεδομένων καθιστούν τα ανώτατα στελέχη των οργανισμών, υπεύθυνα για οποιαδήποτε παραβίαση και αποκάλυψη εμπιστευτικών πληροφοριών. Το ζήτημα της εμπιστοσύνης έχει λάβει κεντρικό ρόλο κυρίως στις υπηρεσίες υγείας και στις υπηρεσίες που προσφέρονται από τα χρηματοπιστωτικά ιδρύματα ανά τον κόσμο. Αρκετοί νόμοι και κανονισμοί θέτουν μέτρα προστασίας για την αποθήκευση, επεξεργασία και μεταβίβαση των δεδομένων των χρηστών. Ακόμη και πριν από την εκτεταμένη νομοθεσία για την προστασία της ιδιωτικής ζωής και την ασφάλεια, υπήρχαν ισχυροί λόγοι για περιορισμό της πρόσβασης σε πληροφορίες που μεταδίδονται και αποθηκεύονται ηλεκτρονικά.

Η προστασία των πληροφοριών είναι ένα από τα δυσκολότερα ζητήματα στις εξωτερικές αναθέσεις. Είναι πολύ πιο δύσκολο να προστατευτούν πληροφορίες όταν αποκτώνται, υποβάλλονται και επεξεργάζονται από εξωτερικούς παρόχους υπηρεσιών οι οποίοι πολλές φορές δε δεσμεύονται από τους ίδιους κανονισμούς και νόμους με τους πελάτες τους. Από όλα τα ζητήματα ασφάλειας που αφορούν τις εξωτερικές αναθέσεις, η προστασία των πληροφοριών είναι η πιο κρίσιμη, ειδικά στις χρηματοπιστωτικές, υγειονομικές υπηρεσίες και κυβερνητικές υπηρεσίες, όπου το απόρρητο των πληροφοριών είναι υψίστης κρισιμότητας. Προκειμένου να ληφθούν επαρκή μέτρα ασφάλειας για την προστασία των πληροφοριών, απαιτούνται μεγάλες επενδύσεις κεφαλαίων από τους εξωτερικούς παρόχους. Οι οργανισμοί θα πρέπει να ελέγχουν ανά τακτά χρονικά διαστήματα εάν η πολιτική και οι διαδικασίες προστασίας δεδομένων των

εξωτερικών παρόχων εφαρμόζονται. Τέλος, με την χρήση εξειδικευμένων εξωτερικών ελεγκτών ή συμβούλων ασφάλειας μπορούν να εκτελέσουν ελέγχους για να αξιολογήσουν το επίπεδο ασφάλειας των πληροφοριακών συστημάτων των εξωτερικών παρόχων (Surja Datta, 2015).

4.7 Απόδοση εφαρμογών και υπηρεσιών

Ένα άλλο ζήτημα που θα πρέπει να ενδιαφέρει τους οργανισμούς που σκοπεύουν να μεταβούν σε εξωτερικό πάροχο, είναι η απόδοση των εφαρμογών και των υπηρεσιών. Και σε αυτήν την περίπτωση, τα συμβόλαια SLA θα πρέπει να σχεδιάζονται έτσι ώστε να λαμβάνουν υπόψη το επίπεδο απόδοσης των ανατεθέντων υπηρεσιών. Οι όροι που αφορούν στην χωρητικότητα, την απόδοση, τον χρόνο απόκρισης και τη διαθεσιμότητα των εφαρμογών και υπηρεσιών, θα πρέπει να συμπεριλαμβάνονται στα συμβόλαια SLA. Δεδομένου ότι ο εξωτερικός πάροχος επιθυμεί όλο και μεγαλύτερη κερδοφορία, στόχος του είναι να παρέχει τις υπηρεσίες στο πλαίσιο των συμφωνημένων όρων αλλά με το ελάχιστο δυνατό κόστος. Αν τα πρόστιμα που ορίζονται στο συμβόλαιο SLA δεν είναι σωστά καθορισμένα, υπάρχει μεγάλη πιθανότητα ο εξωτερικός πάροχος να αθετήσει τους όρους του συμβολαίου SLA για δικό του οικονομικό όφελος. Ως εκ τούτου, είναι σημαντικό να διασφαλιστεί ότι οι τυχόν αποζημιώσεις επαρκούν για να παρακινήσουν τον εξωτερικό πάροχο να ανταποκριθεί στις απαιτήσεις της υπηρεσίας. Είναι επίσης σημαντικό, οι όροι του επιπέδου διαθεσιμότητας των παρεχόμενων υπηρεσιών να τηρούνται στο ακέραιο από τον εξωτερικό πάροχο. Η απώλεια μιας υπηρεσίας για έναν οργανισμό, κατά τη διάρκεια κρίσιμων περιόδων υψηλού τζίρου, έχει μεγαλύτερη επίπτωση από μια αντίστοιχη απώλεια σε ώρες εκτός λειτουργίας του οργανισμού. Για να διατηρηθεί μια σωστή ισορροπία απαιτήσεων και κόστους, είναι απαραίτητο να καθοριστούν εξ αρχής όλα αυτά τα θέματα στο συμβόλαιο SLA. Διαφορετικά, οι ανάγκες των οργανισμών ενδέχεται να μην μπορούν να καλυφθούν επαρκώς από τον εξωτερικό πάροχο ιδιαίτερα όσο αυξάνεται ο όγκος των υπηρεσιών που χρησιμοποιούν (Solli-Saether H. , 2010).

4.8 Έλλειψη τεχνογνωσίας

Συχνά είναι πολύ δύσκολο να βρεθούν εξωτερικοί πάροχοι οι οποίοι να διαθέτουν εξειδικευμένο προσωπικό με εμπειρία και τεχνογνωσία για συγκεκριμένους επιχειρηματικούς κλάδους, γλώσσες προγραμματισμού, εφαρμογές και συστήματα. Οι εξωτερικοί πάροχοι θα πρέπει στις τεχνοοικονομικές τους προτάσεις να συμπεριλαμβάνουν στα στοιχεία του προσωπικού τους και τα βιογραφικά αυτών. Από την άλλη, οι οργανισμοί θα πρέπει να επιμένουν στο να τους ανατεθούν συγκεκριμένα άτομα στο έργο ή την υπηρεσία που πρόκειται να υλοποιηθεί. Ένα άλλο μέτρο είναι να εξασφαλιστεί ότι οι εφαρμογές ή οι λειτουργίες που ανατίθενται σε εξωτερικούς

συνεργάτες, μπορούν εάν χρειαστεί, να ανατεθούν σε άλλο εξωτερικό πάροχο με μεγαλύτερη τεχνογνωσία (Amant, 2009).

4.9 Κρυφά κόστη

Υπάρχουν διάφοροι λόγοι για τους οποίους ορισμένα κόστη μπορεί να παραλειφθούν ή να αποκρυφθούν κατά την αξιολόγηση μιας εξωτερικής ανάθεσης. Κάποια κόστη, είναι πολύ δύσκολο ή πρακτικά αδύνατο να προσδιοριστούν ποσοτικά. Για παράδειγμα, τα άυλα κόστη, τα οποία μπορεί να σχετίζονται με θέματα όπως η ποιότητα των παρεχόμενων υπηρεσιών. Άλλα κόστη είναι ευκολότερα προσδιορίσιμα, αλλά η πιθανότητα εμφάνισής τους είναι πολύ μικρή. Αυτό συμβαίνει κυρίως στις περιπτώσεις που αφορούν στην βιωσιμότητα των εξωτερικών παρόχων. Μπορούν εύκολα να γίνουν καλές εκτιμήσεις για τον οικονομικό αντίκτυπο που θα είχε ο τερματισμός της επιχειρηματικής λειτουργίας ενός εξωτερικού παρόχου, αλλά η πιθανότητα που μπορεί αυτό να συμβεί είναι δύσκολο να υπολογιστεί.

Κατά τη διαδικασία αξιολόγησης, θα πρέπει να ελεγχθεί και η οικονομική βιωσιμότητα των εξωτερικών παρόχων. Αν κάποιος εξωτερικός πάροχος είναι γνωστό ότι αντιμετωπίζει οικονομικό πρόβλημα θα πρέπει να αφαιρεθεί από την λίστα των υποψηφίων προς επιλογή. Ωστόσο, παρόλο που ένας εξωτερικός πάροχος βρίσκεται σε δύσκολη οικονομική θέση, μπορεί να συνεχίσει να παρέχει υπηρεσίες. Μια πρόσθετη χρηματοδότηση, θα μπορούσε να σώσει τον πάροχο ή θα μπορούσε να του επιτρέψει να εξαγοράσει κάποιον ανταγωνιστή του. Οι εξωτερικοί πάροχοι συνήθως εξαγοράζονται από ανταγωνιστές τους οπότε οι τελευταίοι, μπορεί να αποφασίσουν να τερματίσουν μια ή ένα σύνολο προσφερόμενων υπηρεσιών. Ορισμένοι οργανισμοί, συμπεριλαμβάνουν στα συμβόλαια με τους εξωτερικούς παρόχους συγκεκριμένους όρους για την προστασία τους από τέτοιες καταστάσεις.

Στην ανάλυση κινδύνου η οποία θα πρέπει να πραγματοποιείται κατά τη διαδικασία αξιολόγησης, κάποια κόστη μπορεί να αποκρύπτονται ή να αποκλείονται εντελώς, εσκεμμένα ή, λόγω της άγνοιας είτε της απειρίας του αναλυτή. Ένας αναλυτής θα μπορούσε να αποκλείσει εσκεμμένα κόστη για να ευνοήσει μια απόφαση, όπως για παράδειγμα η επιλογή ενός εξωτερικού παρόχου έναντι ενός άλλου. Όποια και αν είναι η προδιάθεση του αναλυτή, αυτές οι εσκεμμένες παραλείψεις ή λάθη θα πρέπει να αντιμετωπιστούν. Υπάρχουν διάφορες περιπτώσεις σημαντικών επιχειρηματικών αποφάσεων που πραγματοποιήθηκαν λόγω σφαλμάτων ή παραλείψεων.

Όπως προαναφέραμε, ορισμένοι εξωτερικοί πάροχοι χρησιμοποιούν προσωπικό και υποδομές σε υποανάπτυκτες χώρες για να μειώσουν τα κόστη λειτουργίας τους. Η πιθανότητα τρομοκρατικών επιθέσεων, πολέμων, εξάπλωσης ασθενειών σε αυτές τις

χώρες εγείρει ανησυχίες για την ομαλή λειτουργία των ανατεθέντων υπηρεσιών. Οι οργανισμοί που χρησιμοποιούν τέτοιους εξωτερικούς παρόχους, θα πρέπει να επιβεβαιώσουν ότι ο εξωτερικός πάροχος διαθέτει κατάλληλα πλάνα έκτακτης ανάγκης, επιχειρηματικής συνέχειας και ανάκαμψης σε περιπτώσεις καταστροφών. Θα πρέπει να γνωρίζουν αν ο εξωτερικός πάροχος έχει τις απαραίτητες εγκαταστάσεις και δυνατότητες για να αντιμετωπίσει τέτοια γεγονότα. Φυσικά, παρόμοιες ανησυχίες υπάρχουν και για την εγχώρια εξωτερική ανάθεση, όπου η πιθανότητα του πολέμου μπορεί να είναι μικρή, αλλά η πιθανότητα ενός τρομοκρατικού χτυπήματος μεγάλη (Power, 2006) (Tho, 2005).

4.10 Περιορισμένες δυνατότητες προσαρμογών και βελτιώσεων

Κατά την σύναψη μιας συμφωνίας εξωτερικής ανάθεσης, τα συστήματα και οι υπηρεσίες που προσφέρει ένας εξωτερικός πάροχος αρχικά φαίνεται ότι καλύπτουν το μεγαλύτερο μέρος των αναγκών του οργανισμού χωρίς να απαιτούνται μελλοντικές βελτιώσεις. Ωστόσο τα δεδομένα αλλάζουν με την πάροδο του χρόνου, τόσο για τον πάροχο όσο και για τον ίδιο τον οργανισμό. Οποιαδήποτε αλλαγή στο καθεστώς της συνεργασίας τους θα πρέπει να επαναδιαπραγματευθεί, εφόσον δεν προβλέπεται στην αρχική σύμβαση. Οι περισσότερες αλλαγές είναι συνήθως εύκολο να πραγματοποιηθούν και να γίνουν αποδεκτές και από τα δύο μέρη. Επίσης, η επιχειρηματική δραστηριότητα του οργανισμού μπορεί να αλλάξει λόγω των δυνάμεων της αγοράς ή λόγω καινούργιων νόμων και κανονισμών. Σε αυτές τις περιπτώσεις αλλάζουν παράλληλα και οι απαιτήσεις προς στον εξωτερικό πάροχο. Αν ο εξωτερικός πάροχος είναι πρόθυμος να καλύψει αυτές τις καινούργιες απαιτήσεις, θα υπάρξουν πρόσθετα κόστη για τον οργανισμό. Σε αντίθετη περίπτωση, ο οργανισμός θα πρέπει να αναζητήσει νέο πάροχο για να καλύψει τις καινούργιες ανάγκες (Axelrod, 2004).

4.11 Μετάδοση γνώσης

Το εσωτερικό προσωπικού ενός οργανισμού, συνήθως είναι πολύ δύσκολο να υποστηρίξει μια υπηρεσία η οποία ενδέχεται να μεταφερθεί από τον εξωτερικό πάροχο εσωτερικά. Για να διατηρήσει ο οργανισμός τη διαπραγματευτική του δύναμη, θα πρέπει να φροντίζει το προσωπικό του να ενημερώνεται ανά τακτά χρονικά διαστήματα από τον εξωτερικό πάροχο για τα τεχνικά θέματα και τις λειτουργίες των ανατεθέντων υπηρεσιών. Κάτι τέτοιο φυσικά δεν συμφέρει τους εξωτερικούς παρόχους και πιθανότατα δε θα επιθυμούν να το υποστηρίξουν. Η μακροπρόθεσμη εξοικονόμηση χρημάτων από την μη διατήρηση εξειδικευμένου προσωπικού είναι σημαντική για τους οργανισμούς. Έχει όμως αρνητικό αντίκτυπο στη διαπραγματευτική τους δύναμη και παράλληλα τους αφαιρεί την δυνατότητα μεταφοράς των υπηρεσιών τους εσωτερικά. Αυτά τα κρυφά κόστη, είναι δύσκολο να υπολογιστούν και συνήθως δε συμπεριλαμβάνονται στην αξιολόγηση εξωτερικής ανάθεσης (Power, 2006) (Solli-Saether & Gottschalk, 2006).

4.12 Κοινόχρηστα περιβάλλοντα

Στα κοινόχρηστα περιβάλλοντα, όπως αυτά που χρησιμοποιούν οι εξωτερικοί πάροχοι, υπάρχει ο κίνδυνος τα δεδομένα ενός πελάτη να διαρρεύσουν σε έναν άλλο πελάτη. Επίσης, υπάρχει η πιθανότητα ο εξωτερικός πάροχος να μην είναι πλήρως εναρμονισμένος με τους υφιστάμενους κανονισμούς και τους νόμους. Στην περίπτωση που διαπιστωθούν παραλείψεις στα μέτρα προστασίας των δεδομένων η ευθύνη μετακυλίεται στις διοικήσεις των οργανισμών. Όταν οι υπηρεσίες ή οι λειτουργίες εξυπηρετούνται από τα εσωτερικά πληροφοριακά συστήματα ενός οργανισμού η πιθανότητα κάτι τέτοιο να συμβεί, είναι μικρότερη. Υπάρχουν διάφορα μέτρα με βάση τα οποία μπορούν οι εξωτερικοί πάροχοι αλλά και οι οργανισμοί να μετριάσουν αυτόν τον κίνδυνο. Οι έλεγχοι ασφάλειας και η εφαρμογή κατάλληλων προτύπων ασφάλειας είναι κάποια από αυτά (Axelrod, 2004).

4.13 Νομικά και κανονιστικά ζητήματα

Οι νομοθέτες και οι ρυθμιστικές αρχές όλο και περισσότερο εξετάζουν τα θέματα που αφορούν στην ασφάλεια πληροφοριακών συστημάτων. Οι κίνδυνοι που σχετίζονται με την μη επαρκή προστασία των δεδομένων των πελατών, επηρεάζουν όχι μόνο τα άτομα που είναι επιφορτισμένα με τη διαχείριση αυτών των δεδομένων, αλλά και τα ανώτερα διοικητικά στελέχη των οργανισμών. Οι κανονισμοί και οι νόμοι, έχουν ισχύ για τους οργανισμούς ανεξάρτητα από το αν επεξεργάζονται εσωτερικά ή από εξωτερικό πάροχο τα δεδομένα των πελατών τους. Αυτό, έχει οδηγήσει τους οργανισμούς σε έναν «αγώνα» επιμέλειας. Για να εναρμονιστούν, θα πρέπει να εφαρμόσουν παγκόσμια αναγνωρισμένα πρότυπα ασφάλειας και να πιστοποιηθούν σε αυτά. Η διαδικασία της πιστοποίησης και η ανανέωσή τους ανά τακτά χρονικά διαστήματα, απαιτεί επιπλέον κεφάλαια. Τα κόστη των νέων απαιτήσεων ασφάλειας για την τήρηση των κανονιστικών απαιτήσεων θα πρέπει να συμπεριλαμβάνονται και αυτά στην αξιολόγηση των εξωτερικών αναθέσεων (Butler, 2000).

5. Απειλές της Ασφάλειας Πληροφοριών

Εκτός από τους κύριους κινδύνους εξωτερικών αναθέσεων που αναλύσαμε στο προηγούμενο κεφάλαιο, οι οργανισμοί καλούνται να αντιμετωπίσουν και τις απειλές που σχετίζονται με την ασφάλεια των πληροφοριών όταν συνεργάζονται με εξωτερικούς παρόχους. Οι επαγγελματίες ασφάλειας πληροφοριακών συστημάτων θεωρούν ότι, οι μεγαλύτερες απειλές βρίσκονται μέσα στους ίδιους τους οργανισμούς και όχι έξω από αυτούς. Οι οργανισμοί χρησιμοποιούν προστατευτικά και αμυντικά μέτρα για να αποτρέψουν τις επιθέσεις και, διορθώνουν τα τρωτά σημεία των συστημάτων τους για να μειώσουν την έκθεσή τους στον κίνδυνο, το ίδιο ισχύει και για τους εξωτερικούς παρόχους υπηρεσιών. Στη συνέχεια, θα περιγράψουμε τις απειλές και τα ευάλωτα σημεία των σύγχρονων πληροφοριακών συστημάτων που καλούνται να αντιμετωπίσουν οι οργανισμοί στις εξωτερικές αναθέσεις (Jouini, 2014) (McCarthy, 2002).

5.1 Εσωτερικές απειλές

Οι εσωτερικές απειλές προέρχονται από ανθρώπους του οργανισμού οι οποίοι διαθέτουν εσωτερικές πληροφορίες για τις λειτουργίες, τα δεδομένα, τα συστήματα και τις υποδομές του οργανισμού. Αυτές οι απειλές είναι πιο επιβλαβείς σε σχέση με αυτές που προέρχονται από κακόβουλους εξωτερικούς παράγοντες. Συνήθως υπαίτιοι για την πραγματοποίηση τέτοιων απειλών είναι, οι εργαζόμενοι του οργανισμού (υφιστάμενοι και μη), οι υπεργολάβοι και οι συνεργάτες, οι οποίοι διαθέτουν νόμιμη πρόσβαση στα συστήματα πληροφορικής για την εκτέλεση των καθηκόντων τους. Οι κύριες κατηγορίες αυτών των ανθρώπων αναλύονται παρακάτω.

Ο δυσαρεστημένος υπάλληλος

Ο τυπικός δυσαρεστημένος υπάλληλος, μπορεί να έχει απολυθεί ή να συνεχίζει να εργάζεται στην επιχείρηση και συχνά ως μέλος του τμήματος μηχανογράφησης. Έχει όλα τα προσόντα που απαιτούνται για να προκαλέσει καταστροφές, που είναι η καλή γνώση των εφαρμογών υπολογιστών, δικτύων, συστημάτων και διαδικασιών της επιχείρησης. Επίσης μπορεί να διαθέτει φυσική πρόσβαση στις εγκαταστάσεις της εταιρείας και πρόσβαση σε εφαρμογές και συστήματα.

Ο πληροφοριοδότης

Ο πληροφοριοδότης μπορεί να είναι υπάλληλος, εξωτερικός συνεργάτης ή σύμβουλος ο οποίος, είναι πολύ εξοικειωμένος με τις εφαρμογές, τα συστήματα και τις διαδικασίες του οργανισμού. Μπορεί να χρησιμοποιήσει τη γνώση αυτή για προσωπικό όφελος μέσω απάτης, υπεξαίρεσης χρημάτων και νομιμοποίησης εσόδων από παράνομες δραστηριότητες και άλλων μεθόδων.

Ο τυχοδιώκτης

Ο τυχοδιώκτης είναι ο εργαζόμενος ή ο εξωτερικός συνεργάτης που εντοπίζει ένα ελάττωμα ή μια ευπάθεια σε μια εφαρμογή ή σύστημα, συχνά τυχαία και αντί να αναφέρει το ελάττωμα, αποφασίζει να το εκμεταλλευτεί για προσωπικό όφελος. Λόγω των κινδύνων που σχετίζονται με τον οπορτουνισμό, πολλά συστήματα ηλεκτρονικών υπολογιστών εμφανίζουν ενημερωτικά μηνύματα ως αποτρεπτικό μέσο, δηλώνοντας ότι οι πληροφορίες που είναι διαθέσιμες μέσω του συστήματος είναι εμπιστευτικές. Αυτή η ειδοποίηση ενδέχεται επίσης να αναφέρει ότι η επιχείρηση θα αναλάβει πειθαρχική και νομική δράση, εάν κάποιος υποκλέψει ή χρησιμοποιήσει παράνομα πληροφορίες από το σύστημα.

Ο ακούσιος καταστροφέας

Ο ακούσιος καταστροφέας, είναι ο υπεύθυνος για την παραβίαση πληροφοριακών συστημάτων και για την καταστροφή δεδομένων. Ένα τέτοιο άτομο μπορεί να είναι κάποιος εργαζόμενος ή ανάδοχος με νόμιμη πρόσβαση σε διάφορα συστήματα ή ένας πελάτης που δικαιούται να έχει πρόσβαση σε εφαρμογές και πληροφορίες για να εκτελεί διάφορες εργασίες. Μπορεί επίσης να είναι ένα άτομο υποστήριξης ή ένας διαχειριστής, που δεν είναι εξοικειωμένος με ένα σύστημα και τις λεπτομέρειες λειτουργίας του. Ο ακούσιος καταστροφέας μπορεί να ακολουθεί τις συνήθεις διαδικασίες και στη συνέχεια, είτε τυχαία είτε, λανθασμένα να εκτελέσει εντολή ή σειρά εντολών εκτός του εύρους των τυποποιημένων λειτουργιών. Οι νέες εντολές ενδέχεται να προκαλέσουν ακατάλληλες αποκρίσεις του συστήματος ή να προκαλέσουν βλάβη στο σύστημα. Δεδομένου ότι ο ίδιος δεν σκόπευε να παραβιάσει ή να προκαλέσει σφάλμα, είναι πιθανό να αναφέρει το περιστατικό, να ζητήσει επίσημα βοήθεια ή απλώς, να μην επαναλάβει την ενέργεια σε αντίθεση με την εκμετάλλευσή του, την οποία θα έκανε ο οπορτουνιστής. Τέτοιες καταστάσεις μπορεί να αναδειχθούν μόνο εάν δημιουργηθεί σοβαρό σφάλμα ή βλάβη.

5.2 Εξωτερικές απειλές

Οι εξωτερικές απειλές σε αντίθεση με τις εσωτερικές απειλές προέρχονται από το εξωτερικό περιβάλλον του οργανισμού. Υπεύθυνοι για την πραγματοποίηση τέτοιων απειλών μπορεί να είναι πρώην εργαζόμενοι, εξωτερικοί συνεργάτες ή ακόμη και εγκληματικές ομάδες. Οι κύριες κατηγορίες αυτών των ανθρώπων περιγράφονται παρακάτω:

Ο χάκερ

Στο μυαλό του κοινού, ο χάκερ είναι ένας κακοποιός του διαδικτύου ο οποίος επιτίθεται στα πληροφοριακά συστήματα και αποτελεί τη μεγαλύτερη απειλή για τους οργανισμούς. Ένα τέτοιο άτομο μπορεί να παραβιάσει ιστοσελίδες και εξυπηρετητές, να

υποκλέψει αριθμούς πιστωτικών καρτών ή να κλειδώσει σταθμούς εργασίας. Ο χάκερ σε γενικές γραμμές μπορεί να προκαλέσει σημαντικές καταστροφές στα πληροφοριακά συστήματα, να διαπράξει απάτες και να δημιουργήσει αρνητική δημοσιότητα στον οργανισμό.

Ο κλέφτης

Ο συγκεκριμένος τύπος επιτιθέμενου είναι καλά χρηματοδοτούμενος, ιδιαίτερα αφοσιωμένος και δεν αποθαρρύνεται εύκολα. Συνεχώς αναζητά ευάλωτα σημεία στα πληροφοριακά συστήματα του οργανισμού και λειτουργεί με επιμονή για να πετύχει τον στόχο του. Ως επί το πλείστων, ο κλέφτης δεν αφήνει αποδείξεις για την εισβολή και για τα στοιχεία που υποκλέπτει για να μην εντοπιστεί και συλληφθεί. Μια τέτοια συμπεριφορά έρχεται σε αντίθεση με τον χάκερ ο οποίος επιθυμεί να γίνεται αντιληπτός και να διαδίδονται τα κατορθώματά του.

Ο δημιουργός και ο διανομέας ιών

Οι ιοί και τα σκουλήκια των υπολογιστών τα οποία διαδίδονται μέσω του διαδικτύου σε λίγες ώρες ή λεπτά, είναι μη ελεγχόμενες και μη προσανατολισμένες μορφές επιθέσεων. Ο δημιουργός του ιού δεν μπορεί να είναι σίγουρος για το ποιος θα μολύνει και ποιος θα διαδώσει τον ιό σε άλλους. Τα άτομα αναπτύσσουν και διαδίδουν ιούς για διάφορους λόγους όπως, για να περηφανευθούν στους συνομήλικους τους ή για να προκαλέσουν ζημιές για δικό τους συμφέρον. Ο δημιουργός ιών ποτέ δεν ξέρει με βεβαιότητα ποιος είναι ο αντίκτυπος και, όταν εντοπίζεται, συχνά εκπλήσσεται από τα αποτελέσματα της επιτυχίας του. Υπάρχουν εκατοντάδες, ακόμη και χιλιάδες, νέων ιών που δημιουργούνται καθημερινά. Από αυτούς τους ιούς, πολύ λίγοι εξαπλώνονται σε παγκόσμιο επίπεδο και προκαλούν σημαντικές ζημίες.

Ο κατάσκοπος

Ο κατάσκοπος μπορεί να είναι επικίνδυνος για την αξιοπιστία και τη βιωσιμότητα ενός οργανισμού. Ένα τέτοιο άτομο ή ομάδα ατόμων επιχειρεί να κλέψει μυστικά για δίκτυα, συστήματα, λειτουργίες και δεδομένα. Οι πληροφορίες αυτές μπορούν να οδηγήσουν σε επακόλουθες πράξεις κλοπής ή, τρομοκρατίας ή, μπορούν να χρησιμοποιηθούν για άμεσο οικονομικό κέρδος, συχνά μέσω της πώλησης εταιρικών μυστικών σε άλλα ενδιαφερόμενα μέρη.

Ο κυβερνο-τρομοκράτης

Ο κυβερνο-τρομοκράτης μπορεί να είναι κατάσκοπος και κλέφτης. Σκοπός του είναι η καταστροφή και η πρόκληση μεγάλων ζημιών στον εχθρό ή ανταγωνιστή. Οι στόχοι του είναι πολύ συγκεκριμένοι και σαφώς καθορισμένοι. Μπορεί να ενεργεί μόνος του,

αλλά είναι πιθανότερο να είναι μέλος μιας ομάδας. Το έθνος ή, κράτος ή, η τρομοκρατική ομάδα για την οποία εργάζεται πληρώνει αδρά για τις δραστηριότητές του.

Περιπτώσεις τρομοκρατίας στον κυβερνοχώρο υπάρχουν πολλές. Ως παράδειγμα μπορούμε να αναφέρουμε τα αντίποινα κινέζων στην αμερικάνικη κυβέρνηση σε ένδειξη διαμαρτυρίας για το θάνατο μίας ομάδας μαθητών που επέβαινε σε βάρκα και ανατράπηκε από αμερικάνικο υποβρύχιο. Στη συγκεκριμένη περίπτωση οι κυβερνο-τρομοκράτες κατέστρεψαν διάφορες ιστοσελίδες της αμερικάνικης κυβέρνησης. Ένα άλλο παράδειγμα είναι η βομβιστική επίθεση της κινέζικης πρεσβείας στο Κοσσυφοπέδιο, η οποία προκάλεσε μια πληθώρα δικτυακών επιθέσεων στον κυβερνοχώρο ενάντια στην αμερικάνικη κυβέρνηση. Οι οργανισμοί που είναι δυνητικοί στόχοι πρέπει να κατανοήσουν την έκθεσή τους, η οποία μπορεί να οφείλεται στην υπεροχή τους, τη δημοτικότητά τους ή τη σημαντικότητά τους. Επιπλέον, πρέπει να λάβουν τα κατάλληλα αντίμετρα.

Μετά την επίθεση στο Παγκόσμιου Κέντρου Εμπορίου το 2001, έχει γίνει ολοένα και πιο προφανές ότι οι κρίσιμες υποδομές που υποστηρίζουν τις σύγχρονες οικονομίες όπως η ενέργεια, οι τηλεπικοινωνίες και οι μεταφορές είναι ιδιαίτερα αλληλεξαρτώμενες και ευάλωτες σε τρομοκρατικές επιθέσεις. Το γεγονός ότι η τρομοκρατία στον κυβερνοχώρο δεν έχει διαδοθεί αρκετά μέχρι σήμερα οφείλεται στο ότι, οι οργανισμοί δεν δημοσιοποιούν τις παραβιάσεις και τα περιστατικά ασφάλειας που αντιμετωπίζουν. Είναι προφανές ότι η τρομοκρατία στον κυβερνοχώρο με την πάροδο του χρόνου θα αυξηθεί. Αυτό οφείλεται κυρίως στο ότι οι επιθέσεις μπορούν διενεργηθούν από απόσταση με χρήση ενός απλού υπολογιστή ή φορητής συσκευής. Η εξωτερική ανάθεση, τόσο στο εσωτερικό όσο και στο εξωτερικό ενός οργανισμού, μπορεί να παρέχει στους εν δυνάμει τρομοκράτες πρόσβαση σε ευάλωτα πληροφοριακά συστήματα και δίκτυα υποδομών.

5.3 Κατηγορίες απειλών

Όπως περιγράψαμε παραπάνω, οι απειλές μπορούν να προέρχονται από εσωτερικά ή εξωτερικά άτομα του οργανισμού, από ερασιτέχνες ή επαγγελματίες, με προσωπικά ή πολιτικά κίνητρα. Από την άποψη της προστασίας, η πηγή μιας επίθεσης μπορεί να οδηγήσει σε διαφορετικούς τρόπους άμυνας. Στην ιδανική περίπτωση, ένας οργανισμός θα πρέπει να εφαρμόσει μέτρα προστασίας και άμυνες που μπορούν να αντιμετωπίσουν κάθε είδους επίθεση, αλλά αυτό δεν είναι εφικτό σε φυσικό και οικονομικό επίπεδο. Συνήθως υιοθετείται μια ενδιάμεση προσέγγιση, οι καθημερινές επιθέσεις χαμηλού επιπέδου αντιμετωπίζονται με βασικά μέτρα ασφάλειας ενώ οι πιο εξειδικευμένες και καταστροφικές επιθέσεις, με την εφαρμογή κατάλληλων διαδικασιών και πολιτικών. Όταν ένας οργανισμός έχει φτάσει σε ένα αποδεκτό επίπεδο ασφάλειας τότε, πρέπει να

εξασφαλίσει ότι οι συνεργάτες του και κυρίως οι εξωτερικοί πάροχοι υπηρεσιών βρίσκονται τουλάχιστον στο ίδιο επίπεδο. Οι κύριες απειλές που αντιμετωπίζουν σήμερα οι οργανισμοί περιγράφονται στην συνέχεια.

5.3.1 Ευπάθειες

Μια απειλή μπορεί να προκαλέσει ζημιές εκμεταλλευόμενη ευπάθειες σε συστήματα και διαδικασίες. Υπάρχουν πολλές μορφές ευπαθειών, από την τεχνική μέχρι την ανθρώπινη, οι οποίες θα πρέπει να εντοπιστούν, να αξιολογηθούν και να μετριαστούν.

5.3.2 Συστήματα και δίκτυα υπολογιστών

Τα σύγχρονα συστήματα και δίκτυα υπολογιστών, λόγω της πολυπλοκότητας και του εύρους των λειτουργιών που προσφέρουν, έχουν ευπάθειες. Τα συστήματα και τα δίκτυα υπολογιστών συνήθως υλοποιούνται για να προσφέρουν όλο και περισσότερα χαρακτηριστικά λειτουργίας στους πελάτες και όχι να τους προστατεύσουν από δικτυακές επιθέσεις. Για πολύ καιρό, η γνώση λειτουργίας των υπολογιστών και η πρόσβαση σε αυτούς ήταν στα χέρια μερικών ειδικών, πλέον αυτές οι γνώσεις είναι ευρέως διαδεδομένες. Εκατομμύρια άνθρωποι σε όλο τον κόσμο έχουν εκπαιδευτεί στην ανάπτυξη εφαρμογών, τον προγραμματισμό συστημάτων, την τεχνική υποστήριξη, την υποστήριξη πελατών και τη διαχείριση συστημάτων. Τέτοιες δεξιότητες αποκτώνται και μεταβιβάζονται εύκολα σε έναν μορφωμένο πληθυσμό. Αυτοί οι ειδικοί υπολογιστών μαζί με τους εκατοντάδες εκατομμυρίων καταρτισμένους χρήστες ηλεκτρονικών υπολογιστών, έχουν δημιουργήσει ένα τεράστιο σύνολο τεχνικών γνώσεων οι οποίες μπορούν χρησιμοποιηθούν παραγωγικά ή καταστροφικά. Σε αυτό, αν προσθέσουμε και την παγκόσμια πρόσβαση που προσφέρεται μέσα από το διαδίκτυο, τότε δημιουργείται μια φόρμουλα για κακόβουλες δραστηριότητες με εκτεταμένες συνέπειες. Η εξωτερική ανάθεση επιβαρύνει περαιτέρω το ήδη δύσκολο πρόβλημα της ασφάλειας. Οι οργανισμοί κατά την εξωτερική ανάθεση, εκτός από το εσωτερικό προσωπικό τους καλούνται να διαχειριστούν και να ελέγξουν το προσωπικό των εξωτερικών παρόχων. Με την εξωτερική ανάθεση, εκθέτουν αυτομάτως τα δίκτυα και τα συστήματά του σε ένα νέο σύνολο ατόμων, πολλοί από τους οποίους ενδέχεται να έχουν κακές προθέσεις.

5.3.3 Υλοποίηση λογισμικού

Οι προσδοκίες για τις δυνατότητες των πληροφοριακών συστημάτων πάντοτε ξεπερνούν την τεχνολογία που απαιτείται για τη διαχείριση και τον έλεγχο τους. Αυτό δημιούργησε μια κουλτούρα στην οποία, ως επί το πλείστων, η λειτουργικότητα εφαρμογών προηγείται των κινδύνων ασφάλειας και της ασφάλειας των πληροφοριών. Είναι γεγονός ότι οι εφαρμογές και το λογισμικό συστημάτων δεν έχουν κατασκευαστεί

για να είναι ασφαλείς. Ως εκ τούτου, συνήθως περιέχουν πολλά σφάλματα ή ευπάθειες που μπορεί να είναι εκμεταλλεύσιμα από κακόβουλους χρήστες.

Η πίεση από τους κριτικούς και τους πελάτες έχει οδηγήσει τις εταιρείες λογισμικού στο να δώσουν ιδιαίτερη έμφαση στα θέματα ασφάλειας. Σε πρόσφατη δήλωση του ο Bill Gates ανέφερε ότι, η ασφάλεια είναι η νούμερο ένα προτεραιότητα στην εταιρεία Microsoft. Μια άλλη ανησυχία όσον αφορά το λογισμικό είναι η πιθανότητα κάποιος να εισαγάγει σκόπιμα κακόβουλο ή εκμεταλλεύσιμο κώδικα σε ένα πρόγραμμα. Έχουν υπάρξει αρκετές περιπτώσεις ιών υπολογιστών που έχουν προσαρτηθεί σκόπιμα σε λογισμικό, χωρίς τη γνώση του κατασκευαστή. Όταν οι οργανισμοί συνάπτουν συμφωνία εξωτερικής ανάθεσης, η πιθανότητα να υπάρχουν σημαντικές διαφορές μεταξύ των πολιτισμών και της κουλτούρας των ανθρώπων είναι υψηλή, ιδιαίτερα όταν πρόκειται για απαιτήσεις ασφάλειας. Απαιτούνται αντικειμενικά κριτήρια, βάσει των οποίων μπορεί να μετρηθεί το επίπεδο της ποιότητας και της ασφάλειας του λογισμικού. Όπως θα αναλυθεί και στη συνέχεια, υπάρχουν ορισμένα πρότυπα αξιολόγησης ασφάλειας και ποιότητας, αλλά δεν είναι ευρέως αποδεκτά.

5.3.4 Συστημικός κίνδυνος

Ακόμη και αν το λογισμικό ή το σύστημα είναι προσεκτικά ελεγμένο και σαρωμένο για ευπάθειες, πάντα υπάρχει η πιθανότητα παραβίασής του. Τα εσωτερικά συστήματα των οργανισμών συνήθως είναι συνδεμένα και με εξωτερικά συστήματα συνεργατών γεγονός το οποίο αυξάνει την έκθεσή τους σε κινδύνους. Η εξωτερική ανάθεση προσθέτει μια άλλη διάσταση σε αυτό το πολύπλοκο σύνολο αλληλεπιδράσεων. Η εξάρτηση του οργανισμού από το επίπεδο ασφάλειας του εξωτερικού παρόχου είναι εξαιρετικά υψηλή και σε αυτό συντελεί αρνητικά η απομακρυσμένη λειτουργία των κρίσιμων συστημάτων. Η ανάγκη για ασφάλεια και αξιοπιστία είναι μεγάλη καθώς, οποιαδήποτε μη εξουσιοδοτημένη αλλαγή ή παραβίαση θα έχει άμεσες επιπτώσεις στη λειτουργία των συστημάτων. Τεχνολογίες όπως το υπολογιστικό σύννεφο, μπορούν να προκαλέσουν σημαντικά προβλήματα στη λειτουργία των οργανισμών. Οι διαχειριστές λογισμικού συνήθως δε γνωρίζουν καν το πού βρίσκονται οι εξυπηρετητές στους οποίους εκτελούν και αποθηκεύουν τα δεδομένα τους στο υπολογιστικό σύννεφο. Ζητήματα που αφορούν την ιδιωτικότητα και εμπιστευτικότητα γίνονται ακόμη πιο σημαντικά.

5.3.5 Λειτουργικός κίνδυνος

Ο λειτουργικός κίνδυνος οφείλεται σε ελλείψεις στα συστήματα πληροφοριών, διαχείρισης, υποστήριξης και ελέγχου των οργανισμών. Αυτές οι ελλείψεις αντιπροσωπεύουν έναν από τους μεγαλύτερους κινδύνους για τις σύγχρονες επιχειρήσεις. Με την εξωτερική ανάθεση, τα ζητήματα που αφορούν τη διαχείριση και

τον έλεγχο καθίστανται ακόμη πιο σημαντικά διότι, πολλές φορές οι λειτουργίες μοιράζονται μεταξύ διαφόρων οργανισμών με αυθαίρετο τρόπο. Το γεγονός ότι επιχειρησιακές διαδικασίες δίνονται σε εξωτερικούς παρόχους εγείρει πολλές ερωτήσεις σχετικά με το επίπεδο ασφάλειας και την ακεραιότητα των εξωτερικών παρόχων. Για τον λόγο αυτόν, οι οργανισμοί θα πρέπει να επιβάλουν ελέγχους ώστε να αξιολογούν συχνά τους εξωτερικούς παρόχους.

5.3.6 Κίνδυνος διαχείρισης

Πολλά προβλήματα που σχετίζονται με την ασφάλεια μπορούν να αποδοθούν στον ανθρώπινο παράγοντα. Οι οργανισμοί εξαρτώνται σε μεγάλο βαθμό από τους διαχειριστές των πληροφοριακών συστημάτων τους. Το διοικητικό προσωπικό θα πρέπει να εφαρμόζει ισχυρούς ελέγχους στα πληροφοριακά συστήματα για να εξασφαλίζει ότι λειτουργούν σύμφωνα με τις απαιτήσεις του οργανισμού. Οι διαχειριστές συστημάτων ενώ ανήκουν στην χαμηλότερη ιεραρχία προσωπικού των οργανισμών, έχουν τεράστια ευθύνη και εξουσία. Ένα σφάλμα διαχειριστή μπορεί να οδηγήσει σε δυσλειτουργίες ή και σε ολική καταστροφή των πληροφοριακών συστημάτων. Ένα απλό μήνυμα από έναν διαχειριστή, μπορεί να εκθέσει άκρως εμπιστευτικές πληροφορίες σε μη εξουσιοδοτημένα άτομα. Συνεπώς, θα πρέπει να καταβληθεί σημαντική προσπάθεια για την αυτοματοποίηση των διαχειριστικών εργασιών, έτσι ώστε να μειωθεί στο ελάχιστο η ανάγκη για ανθρώπινη παρέμβαση και ιδιαίτερα από διαχειριστές χαμηλού επιπέδου. Κατά την ανάθεση σε εξωτερικούς παρόχους, πολλές από αυτές τις διαχειριστικές εργασίες μεταφέρονται στον πάροχο υπηρεσιών. Ως αποτέλεσμα, δημιουργείται η ανάγκη για συνεχή έλεγχο και εποπτεία αυτών των εργασιών που εκτελούνται από τον εξωτερικό πάροχο. Η διενέργεια ελέγχου είναι δυνατή αλλά είναι δύσκολο να εφαρμοστεί. Συνήθως οι οργανισμοί επιβάλουν στους εξωτερικούς παρόχους να τους αποστέλλουν αναφορές διαχείρισης ανά τακτά χρονικά διαστήματα, για να ενημερώνονται σχετικά με την κατάσταση των υπηρεσιών που τους έχουν αναθέσει.

5.3.7 Κίνδυνος πολυπλοκότητας

Η μεταφορά υπηρεσιών και συστημάτων σε εξωτερικούς παρόχους, αυξάνει την πολυπλοκότητα λόγω της αλληλεπίδρασής τους με τα εσωτερικά συστήματα του οργανισμού. Όσο πιο πολύπλοκη είναι μια διάταξη αλληλοεπιδρώντων συστημάτων, τόσο μεγαλύτερη είναι η πιθανότητα σφάλματος ή βλάβης. Ως εκ τούτου, μπορεί κανείς να υποθέσει ότι η διαχείριση μιας εξωτερικής ανάθεσης είναι πιο δύσκολη και απαιτεί περισσότερη προσπάθεια από ότι οι εσωτερικές λειτουργίες. Αυτό δεν σημαίνει ότι ένας οργανισμός δεν θα πρέπει να αναθέτει σε τρίτους. Κατά την διαδικασία αξιολόγησης μια εξωτερικής ανάθεσης εκτός από τα οφέλη της θα πρέπει να τεθούν υπόψη και οι πρόσθετοι κίνδυνοι που μπορεί να προκύψουν λόγο αυξημένης πολυπλοκότητας.

5.3.8 Κίνδυνος κύκλου ζωής

Η διαδικασία με την οποία σχεδιάζεται, αναπτύσσεται, δοκιμάζεται και υλοποιείται ένα σύστημα ονομάζεται κύκλος ζωής συστήματος. Στον κόσμο της πληροφορικής, ο πιο διαδεδομένος είναι ο Κύκλος Ζωής του Συστήματος Ανάπτυξης (Systems Development Life Cycle – SDLC) (Radack, 2009). Κατά την ανάπτυξη συστημάτων, τα ζητήματα που αφορούν την ασφάλεια συχνά παραμελούνται. Στα συστήματα υψηλής ποιότητας, τα χαρακτηριστικά ασφάλειας θα πρέπει ορίζονται εξ' αρχής και να ενσωματώνονται σε κάθε στάδιο ανάπτυξης. Οι κίνδυνοι στον SDLC έχουν ιδιαίτερη σημασία όταν, οι εφαρμογές και η ανάπτυξη συστημάτων ανατίθενται σε εξωτερικούς παρόχους. Η ανάπτυξη εφαρμογών είναι η πιο διαδεδομένη λειτουργία ανάθεσης σε εξωτερικούς συνεργάτες. Με την εύκολη πρόσβαση σε καλά εκπαιδευμένους προγραμματιστές χαμηλού κόστους σε χώρες όπως η Ινδία, αυτή η μορφή εξωτερικής ανάθεσης επεκτείνεται ραγδαία. Άλλοι κύκλοι ζωής σχετίζονται με την νέα τεχνολογία. Η αξιοπιστία και η αποτελεσματικότητα του νέου υλικού και λογισμικού μπορεί να είναι χαμηλή, καθώς συχνά περιέχουν σφάλματα και κατασκευαστικά ελαττώματα που πρέπει να επιλυθούν με την πάροδο του χρόνου.

Στον εξοπλισμό, τα περισσότερα σφάλματα εμφανίζονται στην αρχή λειτουργίας του και στο τέλος της ζωής του. Στο λογισμικό η κατάσταση διαφέρει. Αρχικά υπάρχει μεγάλη βελτίωση καθώς εντοπίζονται και διορθώνονται τα πιο προφανή σφάλματα. Με την πάροδο του χρόνου, εντοπίζονται και επιλύονται νέα σφάλματα, μειώνοντας ακόμη περισσότερο το ποσοστό των σφαλμάτων. Όπως είναι προφανές, για το λογισμικό δεν υπάρχει περίοδος φθοράς. Ακόμη και στην περίπτωση που κάποιο λογισμικό σταματήσει να υποστηρίζεται από τον κατασκευαστή, θα συνεχίζει να λειτουργεί. Ωστόσο, όταν το λογισμικό αντικαθίσταται από νεότερες εκδόσεις, ο ρυθμός σφαλμάτων πάλι αυξάνεται. Ο υπολογισμός του συνδυαστικού ποσοστού σφαλμάτων νέου υλικού και λογισμικού είναι μια πολύπλοκη διαδικασία. Οι οργανισμοί μέσω των εξωτερικών αναθέσεων μπορούν να έχουν πρόσβαση σε νέες τεχνολογίες χωρίς να τους απασχολούν οι κίνδυνοι κύκλου ζωής που προαναφέραμε. Η ευθύνη μετακινείται στους εξωτερικούς παρόχους οι οποίοι καλούνται να αντιμετωπίσουν το πρόβλημα.

5.3.9 Κίνδυνος απαξίωσης

Ένας άλλος κίνδυνος ο οποίος σχετίζεται με την εισαγωγή νέων τεχνολογιών είναι αυτός της απαξίωσης. Ανταλλακτικά και εξειδικευμένοι μηχανικοί ενδέχεται να μην είναι πλέον διαθέσιμα για την υποστήριξη παλαιότερου εξοπλισμού. Πολλές φορές το κόστος συντήρησης των παλαιότερων συστημάτων υπερβαίνει το συνολικό κόστος αγοράς νέου εξοπλισμού. Αυτό ωθεί τους οργανισμούς στο να αντικαταστήσουν τον παλιό εξοπλισμό με καινούργιο για να έχουν χαμηλότερα κόστη συντήρησης. Το ίδιο σε γενικές γραμμές

συμβαίνει και στο λογισμικό. Το παλιό λογισμικό για να διατηρηθεί είναι πιο δαπανηρό από το καινούργιο και παράλληλα υστερεί σε χαρακτηριστικά και δυνατότητες.

Ενώ ορισμένοι εξωτερικοί πάροχοι υπηρεσιών χρησιμοποιούν τεχνολογίες αιχμής, άλλοι επιλέγουν να παρατείνουν τη διάρκεια ζωής των παλαιότερων τεχνολογιών. Στην τελευταία περίπτωση, οι εξωτερικοί πάροχοι αναγκάζονται να παραμείνουν σε ξεπερασμένες τεχνολογίες και πλατφόρμες λόγω του ότι, έχουν πελάτες που δεν επιθυμούν να μεταβούν σε νεότερες τεχνολογίες. Όποια και αν είναι η αιτία, τόσο οι πελάτες όσο και οι εξωτερικοί πάροχοι υπηρεσιών πρέπει να αξιολογούν περιοδικά την αποτελεσματικότητα των τρέχουσων τεχνολογιών για να καθορίσουν εάν είναι σκόπιμο να αναβαθμιστούν.

Εκτός από τα ζητήματα επιχειρησιακής λειτουργίας και υποστήριξης, υπάρχουν και τα ζητήματα που σχετίζονται με την ασφάλεια πληροφοριών. Οι παλιές εκδόσεις λογισμικού ενδέχεται να μην υποστηρίζονται από τον προμηθευτή και όπως προαναφέραμε, το μη υποστηριζόμενο λογισμικό αποτελεί κίνδυνο ασφάλειας. Σε αυτές τις περιπτώσεις, ο προμηθευτής λογισμικού δεν θα διορθώσει τις ευπάθειες που ανακαλύφθηκαν στα παλαιότερα μη υποστηριζόμενα λογισμικά ή συστήματα και, η πιθανότητα ένας κακόβουλος χρήστης να ανακαλύψει αυτές τις ευπάθειες και να τις εκμεταλλευτεί αυξάνεται.

5.3.10 Κίνδυνος βιωσιμότητας προμηθευτή

Οι προμηθευτές κατασκευάζουν υλικό και λογισμικό που μπορεί να χρησιμοποιηθεί από τους οργανισμούς ή από τους εξωτερικούς παρόχους υπηρεσιών. Όταν ένας προμηθευτής σταματήσει την επιχειρηματική του λειτουργία δεν είναι σε θέση να υποστηρίξει τους πελάτες του. Οι οργανισμοί που χρησιμοποιούν τα προϊόντα του, θα πρέπει να τα αντικαταστήσουν ή να αναζητήσουν νέο προμηθευτή για να τα υποστηρίξει. Αυτό το ζήτημα αφορά στον εξοπλισμό, στο λογισμικό, αλλά και στις υπηρεσίες. Η προσεκτική επιλογή των προμηθευτών μπορεί να μειώσει τον εν λόγω κίνδυνο. Για τον μετριασμό του ρίσκου βιωσιμότητας προμηθευτών, οι οργανισμοί θα πρέπει να επιλέγουν πολλούς διαφορετικούς προμηθευτές και να σχεδιάζουν τα πληροφοριακά τους συστήματα με τέτοιον τρόπο, ώστε να μπορούν να μεταφερθούν εύκολα σε άλλες πλατφόρμες και τεχνολογίες.

5.3.11 Κίνδυνος κακής ποιότητας υποστήριξης

Είναι γεγονός ότι, οι προμηθευτές και οι εξωτερικοί πάροχοι υπηρεσιών αναθέτουν το πιο ικανό προσωπικό τους στους μεγαλύτερους και πιο κερδοφόρους πελάτες τους. Οι μικρότεροι πελάτες συνήθως δεν βρίσκονται σε αυτήν την προνομιακή κατηγορία και ως αποτέλεσμα λαμβάνουν υπηρεσίες χαμηλότερης ποιότητας. Οποιαδήποτε

διαπραγμάτευση σχετικά με το επίπεδο εξυπηρέτησης πρέπει να διασφαλίζει το καλύτερο δυνατό επίπεδο υποστήριξης για τον οργανισμό. Ακόμη και οι μικρότεροι σε μέγεθος οργανισμοί, είναι σε θέση μέσα από σωστές συμφωνίες παροχής υπηρεσιών να λάβουν υπηρεσίες υψηλής ποιότητας από τους εξωτερικούς παρόχους.

5.3.12 Κίνδυνος μεταφοράς

Η μεταφορά μιας εσωτερικής λειτουργίας σε έναν εξωτερικό πάροχο καθώς και η δημιουργία μιας νέας λειτουργίας στην υποδομή ενός τρίτου, μπορεί να αντιμετωπίσει προβλήματα. Το προσωπικό που υποστηρίζει την εσωτερική λειτουργία που πρόκειται να μεταφερθεί, συνήθως δημιουργεί εμπόδια στη διαδικασία της μεταφοράς του. Αυτό οφείλεται κυρίως στο ότι αφαιρούνται αρμοδιότητες από τους εργαζομένους. Κάθε διαφωνία ή δυσαρέσκεια που σχετίζεται με το εσωτερικό προσωπικό του οργανισμού, θα πρέπει να παρακολουθείται στενά και να αντιμετωπίζεται έγκαιρα.

5.3.13 Κίνδυνος εξάρτησης από ανθρώπους «κλειδιά»

Συνήθως, οι ειδικοί στους οργανισμούς που γνωρίζουν σε λεπτομέρεια τις κρίσιμες εφαρμογές, τα δίκτυα και τα συστήματα είναι λίγοι. Η απώλεια αυτών των ατόμων, μπορεί να είναι εξαιρετικά επιζήμια για τη λειτουργία και την υποστήριξη αυτών των κρίσιμων πληροφοριακών συστημάτων. Όταν μια εσωτερική λειτουργία μεταφέρεται σε εξωτερικό πάροχο, αυτά τα άτομα πιθανών να αποφασίσουν να αποχωρήσουν από τον οργανισμό ακόμη και αν είναι σαφές ότι είναι απαραίτητα για τη λειτουργία αυτή. Είναι πολύ σημαντικό για την μελλοντική σταθερότητα της λειτουργίας ενός οργανισμού, να εντοπίζονται αυτά τα άτομα και να ενθαρρύνονται για να παραμείνουν. Τόσο οι οργανισμοί, όσο και οι εξωτερικοί πάροχοι μπορούν να διαθέτουν τέτοια άτομα. Κατά την εξωτερική ανάθεση θα πρέπει να διασφαλίζεται ότι αυτά τα ζητήματα αντιμετωπίζονται από τον οργανισμό και από τον εξωτερικό πάροχο με τον ίδιο βαθμό σημαντικότητας.

6. Κριτήρια Αξιολόγησης Εξωτερικών Αναθέσεων

Η ανάλυση κόστους και οφέλους που περιγράψαμε στο κεφάλαιο 3, αφορά κυρίως στον έλεγχο σκοπιμότητας της εξωτερικής ανάθεσης. Οι οργανισμοί, εφόσον κριθεί ωφέλιμο για αυτούς να προχωρήσουν σε ένα έργο εξωτερικής ανάθεσης, θα πρέπει να μπορούν να αξιολογήσουν τους εξωτερικούς παρόχους. Για την αξιολόγησή τους, θα πρέπει να βασιστούν σε συγκεκριμένα κριτήρια τα οποία προκύπτουν από την οικονομική ανάλυση, την ανάλυση των απαιτήσεων και έλεγχο των προσφερόμενων υπηρεσιών και δυνατοτήτων.

6.1 Κοστολόγηση

Πρόκειται για μια εκτενή και δαπανηρή διαδικασία η οποία είναι προτιμότερο να εκτελείται στην περίπτωση που η προκαταρκτική ανάλυση κόστους υποδείξει σημαντικές ωφέλειες για την εξωτερική ανάθεση. Ο αναλυτής, θα πρέπει να έχει θέσει εξ' αρχής τους στόχους της οικονομικής ανάλυσης και τον τρόπο με τον οποίο θα πραγματοποιηθεί. Μετά το πέρας της διαδικασίας, το αποτέλεσμα πολλές φορές μπορεί να είναι αρνητικό ως προς την εξωτερική ανάθεση. Αυτός όμως είναι ο κύριος λόγος εκτέλεσης της διαδικασίας, να αποτρέψει δηλαδή τον οργανισμό να προχωρήσει σε μια μη κερδοφόρα επένδυση. Στην κοστολόγηση, θα πρέπει να συμπεριλαμβάνεται και το κόστος της ίδιας της διαδικασίας κοστολόγησης, ώστε το τελικό αποτέλεσμα να είναι πιο πλήρες. Η διαδικασία συνήθως ξεκινά όταν η διοίκηση των οργανισμών αποφασίζει να αναθέσει μια συγκεκριμένη εσωτερική λειτουργία ή υπηρεσία σε εξωτερικό πάροχο. Σε αυτό το σημείο αξίζει να σημειωθεί ότι πολλές φορές οι αναλυτές θεωρούν ότι η απόφαση έχει ήδη παρθεί από την διοίκηση και θεωρούν λανθασμένα πως είναι καθήκον τους να παρέχουν τεκμηριωμένη αιτιολόγηση για να υποστηρίξουν αυτή την απόφαση (Halvey & Melby, 2007).

Οι πιο κοινές μέθοδοι αξιολόγησης επενδύσεων που μπορούν να χρησιμοποιηθούν στην φάση αυτή από τους οργανισμούς, είναι επιγραμματικά οι παρακάτω (Sparrow, 2003):

- Ανάλυση Κόστους Ωφέλειας (CBA-Cost Benefit Analysis)
- Καθαρή Παρούσα Αξία (NPV- Net Present Value)
- Απόδοση Επένδυσης (ROI- Return on Investment)
- Περίοδος Αποπληρωμής (PP- Payback Period)
- Νεκρού Σημείου (Breakeven)
- Εσωτερική Απόδοση Επένδυσης (IRR – Internal rate of Return)
- Οικονομική Προστιθέμενη Αξία (EVA - Economic value added)

6.2 Συλλογή των απαιτήσεων

Τα σημεία που θα πρέπει να διερευνηθούν προκειμένου να καταλήξει ένας οργανισμός στην απόφαση ανάθεσης υπηρεσιών σε εξωτερικό πάροχο, είναι πολλά. Σε πρώτη φάση, χρειάζεται να αναλογιστεί ο ίδιος ο οργανισμός αν είναι σε θέση να υποστηρίξει τις υπηρεσίες αυτές εσωτερικά. Στην συνέχεια, θα πρέπει να πραγματοποιήσει ανάλυση συνολικού κόστους για την εσωτερική υποστήριξη και την εξωτερική ανάθεση των υπηρεσιών και να συγκρίνει τα αποτελέσματα. Στο σημείο αυτό παίζει σημαντικό ρόλο για την λήψη τελικών αποφάσεων ο βαθμός ανάπτυξης της επιχείρησης τη δεδομένη στιγμή. Όπως και να έχει, μια ολοκληρωμένη διαδικασία ανάλυσης για την επιλογή του εξωτερικού παρόχου είναι προτιμότερη από το να γίνονται απλά προβλέψεις. Ανάλυση χρειάζεται να γίνει και στην περίπτωση επιλογής ενός παρόχου με δεσπόζουσα θέση στην αγορά ή, για την ανάθεση των υπηρεσιών σε περισσότερους από έναν παρόχους. Για την τελική επιλογή, συγκρίνονται οι τεχνολογίες και οι διαδικασίες στις οποίες βασίζεται η επιχειρησιακή λειτουργία του οργανισμού με τις αντίστοιχες του εξωτερικού παρόχου (Dhillon, Seyd, & Sa-Soares, 2017).

6.3 Επιχειρηματικές απαιτήσεις

Η απόφαση του οργανισμού σχετικά με το εάν θα επιλέξει ή όχι να προβεί σε εξωτερική ανάθεση υπηρεσιών, θεωρείται επιχειρησιακή απόφαση. Ωστόσο, η τεχνική συνιστώσα είναι επίσης μεγάλη, ειδικά για τους τομείς της ασφάλειας των πληροφοριών όπου, ένας από τους κρισιμότερους παράγοντες επιτυχίας είναι η ικανότητα υλοποίησης και διαχείρισης τεχνολογιών αιχμής. Σημαντικός λόγος για την εξωτερική ανάθεση, όπως περιγράφηκε προηγουμένως, είναι η αξιοποίηση προϊόντων, δεξιοτήτων και ικανοτήτων που δεν είναι άμεσα διαθέσιμα στην ανοικτή αγορά, αλλά έχουν αποκτηθεί και αναπτυχθεί εξωτερικά του οργανισμού από τρίτους. Εάν η υπηρεσία που αξιολογείται, εκτελείται ήδη για τον οργανισμό εσωτερικά, θα πρέπει να συνταχθεί ένα έγγραφο που να περιγράφει την ανάγκη για μια τέτοια υπηρεσία στο οποίο θα περιλαμβάνεται το εύρος, το μέγεθος και τα αναμενόμενα επίπεδα εξυπηρέτησης που θα παρέχει. Στην περίπτωση των νέο-ιδρυθέντων επιχειρήσεων, οι λεπτομέρειες αυτές ενδέχεται να έχουν δοθεί στους επενδυτές μέσω του επιχειρηματικού σχεδίου. Τα κύρια κίνητρα που μπορούν να οδηγήσουν έναν οργανισμό στην εξωτερική ανάθεση περιγράφονται παρακάτω:

- Τέλος της τρέχουσας σύμβασης για την υποστήριξη μιας εσωτερικής ή εξωτερικής λειτουργίας ή υπηρεσίας
- Εσωτερική ή εξωτερική, λειτουργία ή υπηρεσία που οδηγεί σε μειωμένα κέρδη για τον οργανισμό

- Μειωμένος βαθμός ικανοποίησης για το επίπεδο μιας υπηρεσίας ή λειτουργίας που εκτελείται εσωτερικά ή εξωτερικά του οργανισμού
- Απρόβλεπτες αυξήσεις κόστους
- Εξαγορά του παρόχου υπηρεσιών από άλλη εταιρεία
- Εξαγορά του οργανισμού από άλλη εταιρεία
- Διάλυση ή αλλιώς τερματισμός της λειτουργίας των παρεχόμενων υπηρεσιών από τον εξωτερικό πάροχο
- Καλύτερες οικονομικές προσφορές από άλλους εξωτερικούς παρόχους
- Καλύτερη τεχνολογία από άλλους εξωτερικούς παρόχους

Το αντικείμενο της άσκησης σε αυτό το στάδιο, είναι να καθοριστεί η επιχειρησιακή αιτιολόγηση της υπηρεσίας. Ορισμένες υπηρεσίες, είτε εκτελούνται εσωτερικά ή εξωτερικά, είναι υποχρεωτικές για κάθε οργανισμό (π.χ. μισθοδοσία, λογιστική, νομική). Άλλες υπηρεσίες ή λειτουργίες, όπως η εκπαίδευση, είναι προαιρετικές οπότε θα πρέπει να αποφασιστεί σε διοικητικό επίπεδο για το αν πραγματοποιηθούν ή όχι. Αν το κόστος αυτών των υπηρεσιών είναι χαμηλό, όπως συνήθως συμβαίνει στις εξωτερικές αναθέσεις, τότε αυξάνεται η πιθανότητα για θετική απόφαση της διοίκησης. Η εξωτερική ανάθεση των προαιρετικών ή αλλιώς μη κρίσιμων υπηρεσιών, παρουσιάζει τεράστια αύξηση διότι οι εξωτερικοί πάροχοι προσφέρουν υψηλό επίπεδο υπηρεσιών σε χαμηλότερο κόστος.

Εκτός από τις υποχρεωτικές και προαιρετικές λειτουργίες, υπάρχουν και οι απαραίτητες λειτουργίες οι οποίες χρειάζεται να εκτελούνται μακροπρόθεσμα για την μελλοντική υγεία και βιωσιμότητα του οργανισμού. Αυτές οι λειτουργίες μπορούν να αναβληθούν από τον οργανισμό για μια μελλοντική ημερομηνία χωρίς σημαντικές αρνητικές επιπτώσεις. Τέτοιες λειτουργίες είναι η έρευνα και η ανάπτυξη, η διαφήμιση, η τεκμηρίωση των εφαρμογών πληροφορικής κ.ά. Η μείωση δαπανών για αυτούς τους τύπους λειτουργιών μπορεί να οδηγήσει σε χαμένα μελλοντικά έσοδα από νέα προϊόντα, σε μείωση της αποδοτικότητας και σε αυξημένο κόστος συντήρησης που συνδέεται με ανεπαρκείς τεκμηριωμένες εφαρμογές υπολογιστών. Η επιδείνωση αυτών των λειτουργιών συνήθως οδηγεί τους οργανισμούς στην εξωτερική ανάθεση σε σχετικά σύντομο χρονικό διάστημα (Butler, 2000).

6.4 Βιωσιμότητα

Η ενδελεχής ανάλυση της βιωσιμότητας του εξωτερικού παρόχου, μπορεί να αποτρέψει τον οργανισμό να συνεργαστεί με μια εταιρία που δεν είναι οικονομικά υγιής, δεν είναι φερέγγυα και άρα μπορεί να διακόψει την συνεργασία χωρίς προειδοποίηση.

Οι κίνδυνοι είναι πολλοί. Για τον λόγο αυτόν, η ανάλυση πρέπει να διενεργείται από ειδικούς που εξειδικεύονται σε οικονομικά και νομικά ζητήματα (Power, 2006).

6.5 Οικονομική ανάλυση

Η οικονομική ανάλυση του εξωτερικού παρόχου θα πρέπει να πραγματοποιηθεί από έμπειρο και εξειδικευμένο εσωτερικό ή εξωτερικό προσωπικό. Εάν πρόκειται για δημόσια επιχείρηση, οι οικονομικές καταστάσεις και οι ετήσιες αναφορές του εξωτερικού παρόχου είναι εύκολο να βρεθούν. Αντίθετα, αν ο υποψήφιος πάροχος είναι ιδιώτης, οι διαθέσιμες οικονομικές πληροφορίες είναι γενικά λιγότερες και πιθανώς λιγότερο περιεκτικές. Οι πηγές χρηματοδότησης και τα ονόματα τον διαχειριστών του εξωτερικού παρόχου θα πρέπει να λαμβάνονται υπόψη. Για παράδειγμα, οι εταιρείες που εξαρτώνται σε μεγάλο βαθμό από επιχειρηματικά κεφάλαια, είναι πιθανό να είναι πολύ πιο ευμετάβλητες από τις εταιρείες που μπορούν να χρηματοδοτήσουν τις δραστηριότητές τους από έσοδα. Επίσης, αν είναι εφικτό, θα πρέπει να ληφθεί υπόψιν το μέγεθος, η ποιότητα και η διάρκεια δέσμευσης των υφιστάμενων και των δυνητικών συμβάσεων παροχής υπηρεσιών με άλλους πελάτες. Παρά την προσεκτική ανάλυση των οικονομικών στοιχείων, ένας οργανισμός δεν μπορεί να είναι απολύτως σίγουρος για το τί ακριβώς πραγματικά συμβαίνει σε έναν εξωτερικό πάροχο υπηρεσιών. Ωστόσο, στην συντριπτική πλειονότητα των περιπτώσεων, η διεξοδική οικονομική ανάλυση παρέχει μια λογικά καλή εικόνα της οικονομικής υγείας και της μελλοντικής βιωσιμότητας των δυνητικών επιχειρηματικών εταίρων (Power, 2006).

6.6 Αγορά και επιχειρηματικές προοπτικές

Κάθε οργανισμός δραστηριοποιείται συνήθως σε έναν συγκεκριμένο επιχειρηματικό κλάδο. Ο αναλυτής πρέπει να αντλήσει όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον κλάδο, για να αξιολογήσει τον αντίκτυπο μιας συγκεκριμένης απόφασης εξωτερικής ανάθεσης. Η αξιολόγηση του κλάδου είναι ένας άλλος τομέας όπου ο αναλυτής μπορεί να μην έχει τη δυνατότητα, τη γνώση ή την κατανόηση ώστε να καθορίσει ποιοί είναι οι κύριοι ανταγωνιστές, πώς επηρεάζει ο ένας τον άλλον, ποια συστήματα πληροφορικής και υπηρεσίες χρησιμοποιούν κ.ά. Η εγγραφή σε συμβουλευτικές υπηρεσίες, όπως είναι αυτές που παρέχονται από τον οργανισμό Gartner (Gartner, Inc, 2020), μπορεί να βοηθήσουν τον οργανισμό να αντλήσει πληροφορίες που αφορούν στην αγορά στην οποία δραστηριοποιείται ο εξωτερικός πάροχος. Η έρευνα στο διαδίκτυο, τα περιοδικά και τα φόρουμ συζητήσεων επίσης μπορούν να προσφέρουν σημαντική πληροφόρηση. Οι λιγότερο αξιόπιστες πηγές, είναι ανταγωνιστικές εταιρείες εξωτερικής ανάθεσης, οι οποίες προφανώς και θα υποβαθμίσουν τις δικές τους αδυναμίες και θα αναδείξουν τα προβλήματα άλλων (Power, 2006).

6.7 Οικονομία

Η υγεία της οικονομίας επηρεάζει τους οργανισμούς αλλά και τους εξωτερικούς παρόχους. Σε μια «φτωχή» οικονομία η αγορά συρρικνώνεται και οδηγεί σε μείωση των τιμών, σε χαμηλότερα κέρδη και σε αυξημένη πιθανότητα πτώχευσης ή εξαγοράς. Σε περιόδους οικονομικής ύφεσης, οι εξωτερικοί πάροχοι φαίνεται ότι αποδίδουν καλύτερα λόγω του χαμηλού κόστους υπηρεσιών που προσφέρουν. Φυσικά αυξάνεται η πιθανότητα ορισμένοι οργανισμοί να μην μπορούν να ανταποκριθούν στις πληρωμές τους. Σε αυτήν την περίπτωση, οι εξωτερικοί πάροχοι επιλέγουν το χαρτοφυλάκιο πελατών που επιθυμούν να στοχοποιήσουν, βασιζόμενοι σε οικονομικά στοιχεία κατατάσσοντάς τους σε κατηγορίες ανά βιομηχανία, εταιρεία, μέγεθος και περιοχή (Schniederjans, 2007).

6.8 Ζητήματα της αγοράς

Οι υπηρεσίες ασφάλειας πληροφοριών μπορούν να χωριστούν σε πολλές υποκατηγορίες υπηρεσιών, όπως συμβουλευτικές, αξιολόγησης, υποστήριξης, υλοποίησης και διαχείρισης. Υπάρχουν επιχειρήσεις που ειδικεύονται σε μια ή δύο από αυτές τις υπηρεσίες, ενώ άλλες συμμετέχουν σε περισσότερες. Ορισμένες, πωλούν προϊόντα λογισμικού ασφάλειας, ειδικεύονται στην ασφάλεια των πληροφοριών, παρέχουν γενικές υπηρεσίες ασφάλειας και άλλες, όπως οι μεγάλες εταιρείες λογιστικής, παρέχουν συμβουλευτικές υπηρεσίες ασφάλειας. Η αγορά ασφάλειας των πληροφοριών, η οποία είναι σχετικά νέα, έχει δει σε πολλούς νεοεισερχόμενους, αρκετές αποτυχίες και σημαντικό αριθμό συγχωνεύσεων και εξαγορών. Τα τελευταία χρόνια, η ανάπτυξη στην αγορά της ασφάλειας των πληροφοριών είναι μεγάλη. Τα διάφορα περιστατικά ασφάλειας που δημοσιεύονται κατά καιρούς αυξάνουν όλο και περισσότερο την ανησυχία των οργανισμών (Sparrow, 2003) (Halvey & Melby, 2007).

6.9 Ανταγωνιστικό περιβάλλον

Προχωρώντας στο επόμενο επίπεδο ανάλυσης, πρέπει να διαπιστωθεί εάν ο εξωτερικός πάροχος υπηρεσιών είναι υγιής και μπορεί να λειτουργήσει μακροπρόθεσμα σε ανταγωνιστικό περιβάλλον. Πώς τοποθετείται ο εξωτερικός πάροχος στον κλάδο του; Είναι ηγέτης ή ακόλουθος; Είναι μόνος του στην αγορά ή αντιμετωπίζει επιθετικό ανταγωνισμό από παρόμοιους εξωτερικούς παρόχους; Έχει διατηρήσει την αυτονομία του ή έχει ιστορικό με συγχωνεύσεις, εξαγορές, πτωχεύσεις και αποτυχίες; Όταν μια αγορά είναι σχετικά νέα και επηρεάζεται από κάθε είδους αναταραχές, όπως συμβαίνει στην περίπτωση της ασφάλειας των πληροφοριών, η επιλογή ενός εξωτερικού παρόχου υπηρεσιών είναι δύσκολη και επικίνδυνη. Για να παρθούν αποφάσεις σε ένα τέτοιο περιβάλλον, πρέπει να υπάρχει καλή γνώση της αγοράς. Η αποτυχία ενός εξωτερικού

παρόχου μπορεί να επηρεάσει άμεσα τους πελάτες του, θέτοντας σε κίνδυνο τις υπηρεσίες τους και την βιωσιμότητά τους (Schniederjans, 2007).

6.10 Ποικιλία υπηρεσιών

Οι εξωτερικοί πάροχοι μπορεί να προσφέρουν ένα ή περισσότερα προϊόντα και υπηρεσίες. Από επιχειρηματική άποψη, αυτοί που παρέχουν ένα προϊόν ή υπηρεσία, προσφέρουν και τις μεγαλύτερες αποδόσεις αλλά είναι πιο εκτεθειμένοι στις διακυμάνσεις της οικονομίας και στις αλλαγές τεχνολογίας και ζήτησης. Οι μεγάλοι οργανισμοί, για να μειώσουν τον κίνδυνο, συνήθως επιλέγουν τους πιο δημοφιλείς εξωτερικούς παρόχους οι οποίοι προσφέρουν και μεγάλη γκάμα υπηρεσιών. Σε αντίθεση, οι μικρότεροι οργανισμοί απευθύνονται σε μικρότερους και λιγότερο εδραιωμένους εξωτερικούς παρόχους ώστε να μειώσουν τα λειτουργικά κόστη και για να έχουν αυξημένη διαπραγματευτική δύναμη. Οι μικρότεροι εξωτερικοί πάροχοι, αναπτύσσονται σταδιακά όσο αυξάνεται το πελατολόγιό τους και μπορούν να επηρεαστούν αρνητικά σε περίπτωση που χάσουν πελάτες, εξαγοραστούν ή συγχωνευθούν (Amant, 2009).

6.11 Κλάδος δραστηριότητας

Οι οργανισμοί κατά την αξιολόγηση μιας εξωτερικής ανάθεσης εκτός από τον επιχειρηματικό κλάδο που δραστηριοποιούνται οι εξωτερικοί πάροχοι, απαιτείται να ελέγχουν και τα χαρακτηριστικά του ίδιου του επιχειρηματικού κλάδου. Θα πρέπει να εξετάζουν τους τύπους και το μέγεθος των πελατών του εξωτερικού παρόχου καθώς και τις τοποθεσίες όπου δραστηριοποιούνται. Στις μέρες μας, το ζήτημα της τοποθεσίας είναι λιγότερο σημαντικό για τους οργανισμούς. Αυτό οφείλεται στην ανάπτυξη των τηλεπικοινωνιών και των τεχνολογιών επικοινωνίας όπως είναι η τηλεδιάσκεψη, το ηλεκτρονικό ταχυδρομείο, η ανταλλαγή άμεσων μηνυμάτων, ή το πρωτόκολλο φωνής μέσω διαδικτύου. Υπάρχουν όμως και ορισμένες περιπτώσεις όπου οι συναντήσεις πρόσωπο με πρόσωπο είναι απολύτως απαραίτητες (Amant, 2009).

6.12 Μεγέθη οργανισμών

Το μέγεθος των οργανισμών και των εξωτερικών παρόχων μπορεί επίσης να επηρεάσει σε μεγάλο βαθμό τη βιωσιμότητά και τις σχέσεις τους (Schniederjans, 2007). Οι περιπτώσεις συνεργασίας που μπορεί να προκύψουν με βάση το μέγεθος των οργανισμών και των εξωτερικών παρόχων, περιγράφονται στην συνέχεια.

Μεγάλος οργανισμός και μικρός εξωτερικός πάροχος

Σε αυτήν την περίπτωση ο οργανισμός αποτελεί κύρια πηγή εσόδων για τον εξωτερικό πάροχο. Ο οργανισμός είναι σε θέση να διαπραγματεύεται επιθετικά τις τιμές και τα

παραδοτέα, με τον εξωτερικό πάροχο να συμφωνεί σε οτιδήποτε ζητηθεί. Από την άλλη πλευρά, η μεγάλη εξάρτηση από έναν μόνο πελάτη καθιστά τον εξωτερικό πάροχο υπηρεσιών ιδιαίτερα ευάλωτο. Αυτό είναι ιδιαίτερα επικίνδυνο για τους υπόλοιπους μικρότερους πελάτες του, οι οποίοι ενδέχεται να έχουν αναθέσει μικρές αλλά σημαντικές υπηρεσίες σε αυτόν. Οι πιθανοί πελάτες θα πρέπει να είναι πολύ προσεκτικοί σε αυτή την κατάσταση, ιδιαίτερα αν αντιπροσωπεύουν μόνο ένα μικρό μέρος της συνολικής δραστηριότητας εξωτερικού παρόχου. Όταν ο οργανισμός είναι πολύ μεγαλύτερος από τον εξωτερικό πάροχο, συνήθως ανησυχεί για την βιωσιμότητα του εξωτερικού παρόχου. Η οικονομική πίεση που δέχεται ο εξωτερικός πάροχος τον οδηγεί σε πρόσθετες χρεώσεις για να μπορέσει να ανταποκριθεί στο επίπεδο υπηρεσιών που έχουν συμφωνηθεί. Για τον πελάτη, τα έξοδα που θα προκύψουν εάν ο εξωτερικός πάροχος αποτύχει, πιθανότατα είναι πολύ μεγαλύτερα από τα οικονομικά οφέλη του μειωμένου κόστους υπηρεσιών.

Μικρός οργανισμός και μεγάλος εξωτερικός πάροχος

Ένας μικρός οργανισμός αποκτά πολλά οφέλη από την συνεργασία με έναν μεγάλο εξωτερικό πάροχο. Εκτός από τις οικονομίες κλίμακας που προσφέρει μια τέτοια σχέση, ο οργανισμός απολαμβάνει μεγαλύτερο επίπεδο ασφάλειας και υψηλότερο βαθμό διαθεσιμότητας συστημάτων και δικτύων. Παράλληλα, αποκτά πρόσβαση σε τεχνολογίες οι οποίες είναι πιο προχωρημένες από τις δικές του. Οι μεγάλοι εξωτερικοί πάροχοι διαθέτουν μεγαλύτερη οικονομική δύναμη και μπορούν εύκολα να θέσουν σε εφαρμογή νέες τεχνολογίες. Όσο μεγαλύτερος είναι ένας εξωτερικός πάροχος, τόσο αυξάνεται και η πιθανότητα της μακροπρόθεσμης βιωσιμότητάς του. Από την άλλη πλευρά, ο εξωτερικός πάροχος μπορεί να «ανησυχεί» για τη βιωσιμότητα του οργανισμού, αν και η απώλεια ενός μικρού πελάτη δεν έχει σημαντικές επιπτώσεις στην συνολική δραστηριότητά του.

Μεγάλος οργανισμός και μεγάλος εξωτερικός πάροχος

Στην περίπτωση που ο οργανισμός και ο εξωτερικός πάροχος είναι και οι δύο μεγάλοι, ο κίνδυνος της εξωτερικής ανάθεσης είναι μικρός αλλά υπαρκτός. Οι μεγάλες εταιρείες μπορεί να εξαγοραστούν ή να συγχωνευθούν με αποτέλεσμα να χάσουν την εμπιστοσύνη των πελατών τους, να μειώσουν το επίπεδο των προσφερόμενων υπηρεσιών ή και, να αποτύχουν γενικά. Και οι δύο τύποι εταιρειών μπορούν να διαπραγματευτούν από θέση ισχύος και να καταλήξουν από κοινού σε επικερδείς συμφωνίες. Είναι γεγονός ότι, οι μεγάλες εταιρείες προτιμούν να συνεργάζονται με εταιρείες αντίστοιχου μεγέθους για να μειώσουν τους κινδύνους που μπορεί να προκύψουν.

Μικρός οργανισμός και μικρός εξωτερικός πάροχος

Σε ορισμένες περιπτώσεις, το σενάριο αυτό είναι παρόμοιο με την κατάσταση των μεγάλων οργανισμών και εξωτερικών παρόχων. Και οι δύο πλευρές έχουν την ίδια διαπραγματευτική δύναμη και τον ίδιο βαθμό βιωσιμότητας. Αυτή είναι η πιο επικίνδυνη κατάσταση, αλλά η πιο συχνή στις σχέσεις μεταξύ των μικρότερων εταιρειών. Οι μικροί εξωτερικοί πάροχοι αντιμετωπίζουν δυσκολίες στην απόκτηση μεγάλων πελατών και οι μικροί οργανισμοί ενδέχεται να μην προτιμώνται από τους μεγαλύτερους εξωτερικούς παρόχους.

6.13 Απαιτήσεις των υπηρεσιών

Εκτός από τη διασφάλιση της επιχειρηματικής σχέσης, θα πρέπει να διασφαλιστεί και το επίπεδο των προσφερόμενων υπηρεσιών. Αυτό πραγματοποιείται με το συμφωνητικό SLA, αλλά είναι σαφές ότι δεν μπορεί να εγγυηθεί πως όλα θα λειτουργήσουν όπως έχουν συμφωνηθεί. Οι εξωτερικοί πάροχοι υπηρεσιών μπορούν να έχουν ίδιες δεσμεύσεις ως προς τα απτά και μετρήσιμα επίπεδα υπηρεσιών, όπως τον ρυθμό απόδοσης, την ικανότητα, τον χρόνο απόκρισης, τους χρόνους ολοκλήρωσης εργασιών, τη διαθεσιμότητα, την ακρίβεια, την ακεραιότητα των δεδομένων, τη διατήρηση της εμπιστευτικότητας, τις επικοινωνίες, τις αναφορές και την ανταπόκριση της τεχνικής υποστήριξης. Ωστόσο, ακόμη και αν πληρούνται με συνέπεια τα κριτήρια αυτά, ο πελάτης μπορεί να εξακολουθεί να είναι δυσαρεστημένος.

Η ικανοποίηση του πελάτη μπορεί να ποικίλλει σε μεγάλο βαθμό από έναν πάροχο σε έναν άλλο. Είναι σαφές ότι, ορισμένα χαρακτηριστικά της υπηρεσίας δεν μπορούν να μετρηθούν όπως η γνώση και η εξυπηρετικότητα του προσωπικού υποστήριξης. Οι οργανισμοί είναι φυσικό να αναρωτηθούν ποιά στοιχεία είναι αυτά που επηρεάζουν την ποιότητα των προσφερόμενων υπηρεσιών και πώς μπορούν να μετρηθούν οι άυλες υπηρεσίες. Κατά ειρωνικό τρόπο, τα τυπικά μέτρα μέτρησης επιδόσεων μπορεί να μην σχετίζονται με τις αντιλήψεις των τελικών χρηστών ή πελατών σχετικά με την καλή εξυπηρέτηση, ιδιαίτερα στον τομέα της πληροφορικής. Η διαχείριση της ικανοποίησης των πελατών απαιτεί την σύγκλιση των προσδοκιών και των αντιλήψεων τόσο του πελάτη όσο και του παρόχου υπηρεσιών. Ο στόχος είναι να μειωθεί ή κατά προτίμηση να εξαλειφθεί το κενό στην κατανόηση του τί αναμένει ο πελάτης όσον αφορά στο επίπεδο εξυπηρέτησης και τι σκέφτεται ο πάροχος ότι χρειάζεται ο πελάτης. Αυτό το κενό πρέπει να τεθεί με συγκεκριμένους όρους και στην συνέχεια να διοχετευθεί στον πελάτη και τον πάροχο, προκειμένου να αλλάξει τις αντιλήψεις τους σχετικά με το αποδεκτό επίπεδο απόδοσης. Χωρίς την ανατροφοδότηση και την προθυμία αλλαγής, τα επίπεδα υπηρεσιών δεν θα βελτιωθούν (Halvey & Melby, 2007).

Ο οργανισμοί δεν ενδιαφέρονται για την αιτία μιας διακοπής σε μια εξωτερικά ανατιθέμενη υπηρεσία. Σημαντικά για αυτούς είναι, οι επιπτώσεις της διακοπής, ο χρόνος αποκατάστασης και η ανάκτηση των δεδομένων τους. Η υπηρεσία ενδέχεται για διάφορους λόγους, τυχαίους ή σκόπιμους, να μην είναι διαθέσιμη ή να υπολειτουργεί. Κατά τη διαπραγμάτευση συμφωνίας SLA με έναν εξωτερικό πάροχο υπηρεσιών, τα θέματα αυτά πρέπει να διερευνηθούν και να αντιμετωπιστούν. Η αντιμετώπιση αυτών των περιστατικών, περιλαμβάνει τον χρόνο να συνειδητοποιήσουμε ότι το σύστημα δεν λειτουργεί, τον χρόνο που χρειάζονται οι μηχανικοί των υπηρεσιών για να φτάσουν στον χώρο ή για να συνδεθούν από απόσταση, τον χρόνο για τον προσδιορισμό της αιτίας του προβλήματος και τον χρόνο επισκευής και τελικής αποκατάστασης. Οι πιο σημαντικοί δείκτες για την μέτρηση αυτών των διαστημάτων είναι ο μέσος χρόνος μεταξύ βλαβών (Mean Time Between Failures - MTBF), ο χρόνος μέχρι να συμβεί μια αστοχία (Mean Time To Failure - MTTF) και ο μέσος χρόνος επιδιόρθωσης (Mean Time To Repair - MTTR). Αυτοί οι χρόνοι δίνουν στον υπεύθυνο λήψης αποφάσεων τη δυνατότητα μέτρησης των επιδόσεων των εξωτερικών παρόχων και βοηθάνε στον υπολογισμό του αντίκτυπου που θα έχει στον οργανισμό η διακοπή μιας υπηρεσίας. Είναι πολύ σημαντικό, οι οργανισμοί να συγκρίνουν τις επιδόσεις MTBF, MTTF και MTTR των υποψήφιων εξωτερικών παρόχων πριν πάρουν οποιεσδήποτε αποφάσεις (Butler, 2000).

Ένας από τους βασικούς λόγους για τους οποίους οι οργανισμοί επιδιώκουν να αναθέσουν σε εξωτερικούς συνεργάτες συγκεκριμένες λειτουργίες είναι ότι αναζητούν έναν αξιόπιστο και φθηνό τρόπο να υιοθετήσουν νέες τεχνολογίες και να αποκτήσουν νέες δυνατότητες. Με την τεχνολογία να προχωράει τόσο γρήγορα, οι επιχειρήσεις συνήθως καθίστανται μη ανταγωνιστικές χρησιμοποιώντας παρωχημένες και δαπανηρές τεχνολογίες που δεν ανταποκρίνονται στις ανάγκες τους. Σε ορισμένους κλάδους, τα νομικά και ρυθμιστικά ζητήματα μπορεί να είναι τόσο σημαντικά που δεν επιτρέπουν στις μικρότερες επιχειρήσεις να διατηρούν τις εφαρμογές και τα συστήματά τους ενημερωμένα, με αποτέλεσμα να αναζητούν λύσεις σε εξωτερικούς παρόχους. Υπάρχει μια λεπτή ισορροπία μεταξύ της χρήσης των τελευταίων τεχνολογιών και της αναμονής μέχρι να δοκιμαστούν από άλλους πριν υιοθετηθούν ευρέως. Επειδή πολλά καινοτόμα συστήματα αντιμετωπίζουν προβλήματα στα αρχικά στάδια λειτουργίας τους, πρέπει να διερωτηθεί κανείς κατά πόσο αξίζει ο κίνδυνος να τα χρησιμοποιήσει.

Κατά την επιλογή ενός εξωτερικού παρόχου υπηρεσιών, η τεχνολογία διαδραματίζει σημαντικό ρόλο, ιδίως για την εξωτερική ανάθεση υπηρεσιών πληροφορικής και ακόμη περισσότερο για την εξωτερική ανάθεση της ασφάλειας των πληροφοριών. Είναι γενικά ασφαλέστερο οι οργανισμοί να επιλέγουν έναν εξωτερικό πάροχο με αποδεδειγμένη

εμπειρία και σταθερή τεχνολογία, από το να πειραματίζονται με νέες «γοητευτικές» τεχνολογίες. Η χρήση των πιο σύγχρονων συστημάτων και αρχιτεκτονικών, συνήθως οδηγεί σε σημαντικά λειτουργικά και οικονομικά προβλήματα. Οι οργανισμοί δεν θα πρέπει να αποφεύγουν τις νέες τεχνολογίες, θα πρέπει όμως να τις προσεγγίζουν με ιδιαίτερη προσοχή και να τις δοκιμάζουν σε εξαντλητικό βαθμό πριν τις υιοθετήσουν. Κύριος στόχος τους θα πρέπει να είναι η επιλογή αποτελεσματικών, λιγότερο δαπανηρών και εύκολων στην χρήση συστημάτων. Για τις ταχέως μεταβαλλόμενες τεχνολογίες, ιδίως εκείνες που αφορούν στην ασφάλεια των πληροφοριών, συχνά η επιλογή της άμεσης εφαρμογής είναι μονόδρομος. Ο κίνδυνος μη επαρκούς προστασίας και καθυστερημένης απόκρισης είναι πολύ υψηλός (Amant, 2009).

7. Εξωτερική Ανάθεση Λειτουργιών Ασφάλειας

Στο αυτό το κεφάλαιο, θα εξετάσουμε την ανάθεση των υπηρεσιών ασφάλειας σε εξωτερικούς παρόχους επικεντρώνοντας στα ζητήματα που μπορεί να προκύψουν κατά την εφαρμογή της. Η λειτουργία της ασφάλειας, αποτελεί κρίσιμη παράμετρο σε κάθε εξωτερική ανάθεση. Αφορά κυρίως στην προστασία των πληροφοριών, των υποδομών και του προσωπικού του οργανισμού αλλά, μπορεί να ανατεθεί και ως πρωταρχική λειτουργία σε εξωτερικούς παρόχους. Στη συνέχεια, βασιζόμενοι στις γνωστικές περιοχές του Βρετανικού προτύπου ασφάλειας πληροφοριών ISO 17799:2005 (ISO/IEC 17799:2005, 2020) και στο Κοινό Σώμα Γνώσης (Common Body of Knowledge - CBK) του οργανισμού (ISC)² ((ISC)²: The World's Leading Cybersecurity Professional Organization, 2020), θα προσπαθήσουμε να ορίσουμε τα μέτρα ασφάλειας πληροφοριών τα οποία μπορούν να εφαρμοστούν και στις εξωτερικές αναθέσεις.

Γνωστικές περιοχές (ISC)² CBK:

1. Πρακτικές Διαχείρισης Ασφάλειας ΠΣ
2. Έλεγχος Προσβάσεων
3. Μοντέλα Ασφάλειας και Αρχιτεκτονική
4. Φυσική Ασφάλεια
5. Τηλεπικοινωνίες και Ασφάλεια Δικτύων
6. Κρυπτογραφία
7. Επαναφορά από Καταστροφές και Επιχειρηματική Συνέχεια
8. Νόμοι, Έρευνες και Ηθική
9. Εφαρμογές και Υλοποίηση Συστημάτων
10. Ασφάλεια Λειτουργιών

Γνωστικές περιοχές ISO 17799:2005:

1. Σχεδιασμός Επιχειρηματικής Συνέχειας
2. Έλεγχος Προσβάσεων Συστημάτων
3. Υλοποίηση Συστημάτων και Συντήρηση
4. Φυσική και Περιβαλλοντική Ασφάλεια
5. Εναρμόνιση
6. Ασφάλεια Προσωπικού
7. Ασφάλεια Οργανισμού
8. Διαχείριση Υπολογιστών και Λειτουργιών
9. Διαβάθμιση και Έλεγχος Περιουσιακών Στοιχείων
10. Πολιτική Ασφάλειας

Στον Πίνακας 8 αντιστοιχίζονται οι γνωστικές περιοχές του (ISC)² CBK με τις γνωστικές περιοχές του ISO 17799:2005 και, αξιολογείται αν η εκάστοτε γνωστική περιοχή μπορεί να ανατεθεί σε εξωτερικό πάροχο ως συμβουλευτική υπηρεσία ή ως υπηρεσία εξωτερικής ανάθεσης.

Πίνακας 8*:Αντιστοίχιση γνωστικών περιοχών (ISC)² CBK και ISO 17799:2005*

(ISC)² CBK	**ISO 17799**	**Καταλληλότητα για Συμβουλευτικές υπηρεσίες / Εξωτερική ανάθεση**
Πρακτικές Διαχείρισης Ασφάλειας ΠΣ	Ασφάλεια Οργανισμού	Αναλαμβάνεται συνήθως από εξωτερικούς συμβούλους.
	Ασφάλεια Προσωπικού	Επειδή απαιτείται συγκεκριμένη τεχνογνωσία, μέρος ή ολόκληρη η ασφάλεια του προσωπικού ανατίθεται σε εξωτερικούς παρόχους
	Διαβάθμιση και Έλεγχος Περιουσιακών Στοιχείων	Κυρίως αναπτύσσεται εσωτερικά στους οργανισμούς. Σε άλλες περιπτώσεις υλοποιείται σε συνεργασία με εξειδικευμένο προσωπικό εξωτερικού παρόχου.
	Πολιτική Ασφάλειας	Μπορεί εύκολα να δημιουργηθεί εσωτερικά αλλά πολλοί οργανισμοί επιλέγουν να προσλάβουν εξωτερικούς συμβούλους για την συγγραφή της.
Έλεγχος Προσβάσεων	Έλεγχος Προσβάσεων Συστημάτων	Αφορά συνήθως εσωτερική λειτουργία αλλά μπορεί να ανατεθεί εύκολα και σε εξωτερικούς παρόχους.
Μοντέλα Ασφάλειας και Αρχιτεκτονική		Μπορεί να υλοποιηθούν με χρήση κατάλληλου λογισμικού εσωτερικά στους οργανισμούς ή να ανατεθεί σε εξειδικευμένο προσωπικό εξωτερικού παρόχου.
Φυσική Ασφάλεια	Φυσική και Περιβαλλοντική Ασφάλεια	Αποτελεί συνήθη πρακτική των οργανισμών να προσλαμβάνουν εξωτερικές εταιρείες για την φυσική ασφάλεια.
Τηλεπικοινωνίες και Ασφάλεια Δικτύων		Η υλοποίηση ασφαλών δικτύων, συστημάτων και αρχιτεκτονικών απαιτεί συνήθως την βοήθεια εξωτερικών συμβούλων.
Κρυπτογραφία		Γενικά δεν προσφέρεται ως ξεχωριστή υπηρεσία και αλλά ενσωματώνεται ως

		λειτουργία σε άλλες οι οποίες μπορούν να ανατεθούν σε εξωτερικούς παρόχους.
Επαναφορά από Καταστροφές και Επιχειρηματική Συνέχεια	Σχεδιασμός Επιχειρηματικής Συνέχειας	Πολύ συνήθης υπηρεσία η οποία ανατίθεται σε εξωτερικούς παρόχους. Εξειδικευμένοι σύμβουλοι χρησιμοποιούνται συχνά για την ανάπτυξη αυτών των υπηρεσιών.
Νόμοι, Έρευνες και Ηθική	Εναρμόνιση	Χρησιμοποιούνται συνήθως εξωτερικοί εμπειρογνώμονες και νομικοί.
Εφαρμογές και Υλοποίηση Συστημάτων	Υλοποίηση Συστημάτων και Συντήρηση	Η ανάπτυξη εφαρμογών και η υποστήριξή τους συχνά ανατίθεται σε εξωτερικούς παρόχους. Η εκπαίδευση για ασφαλή συγγραφή κώδικα προγραμματισμού συνήθως ανατίθεται σε εξωτερικούς συμβούλους. Η αξιολόγηση του επιπέδου ασφάλειας των συστημάτων πραγματοποιείται κυρίως από εξωτερικούς συμβούλους ασφάλειας.
Ασφάλεια Λειτουργιών	Διαχείριση Υπολογιστών και Λειτουργιών	Η ασφάλεια των λειτουργιών και των επικοινωνιών των ανατεθέντων υπηρεσιών και λειτουργιών καλύπτεται από τον εξωτερικό πάροχο. Εναλλακτικά, μπορεί να ανατεθεί ως κύρια υπηρεσία σε εξωτερικό πάροχο όπου την διαχείριση μπορεί να έχει εξ' ολοκλήρου ο ίδιος ή το προσωπικό του οργανισμού.

7.1 Πρακτικές διαχείρισης ασφάλειας

Ο τρόπος διαχείρισης των λειτουργιών ασφάλειας καθώς και ο βαθμός στον οποίο αντιμετωπίζονται, διαφέρει σημαντικά μεταξύ των οργανισμών. Η πολιτική ασφάλειας, η προστασία των πληροφοριών, η ασφάλεια του προσωπικού καθώς και η διαβάθμιση και ο έλεγχος των πληροφοριακών περιουσιακών στοιχείων, ως κύριες πρακτικές διαχείρισης ασφάλειας, θα πρέπει να ακολουθούνται από όλους τους οργανισμούς στα πλαίσια των εξωτερικών αναθέσεων (Harold & Krause, 2008) (Allen, Gabbard, May, Hayes, & Sledge, 2003).

7.1.1 Προστασία πληροφοριών

Ή προστασία των εμπιστευτικών πληροφοριών είναι ένα πιο σημαντικά προβλήματα που καλούνται να λύσουν οι οργανισμοί. Όλο και περισσότεροι κανονισμοί και νόμοι

επιβάλλουν μέτρα ασφάλειας για την προστασία των πληροφοριών ιδίως όταν αφορά στα προσωπικά δεδομένα. Οι ρόλοι, οι ευθύνες, οι στόχοι, οι λειτουργίες και η δομή της ασφάλειας των οργανισμών προσεγγίζονται με διάφορους τρόπους. Τα ζητήματα ασφάλειας στους οργανισμούς, συνήθως αντιμετωπίζονται από εξειδικευμένο προσωπικό το οποίο βρίσκεται υψηλά στην διοικητική ιεραρχία. Στις αρμοδιότητές τους ανήκουν εργασίες όπως η εφαρμογή πολιτικών, η εφαρμογή προτύπων ασφάλειας και η διαχείριση συστημάτων ασφάλειας, η διαχείριση του ελέγχου πρόσβασης, τα συστήματα ανίχνευσης και παρεμπόδισης εισβολών.

Σε ορισμένους οργανισμούς, η φυσική ασφάλεια, η ασφάλεια του προσωπικού, οι λειτουργίες επιχειρηματικής συνέχειας, ο σχεδιασμός και η αποκατάσταση από καταστροφή αποτελούν ευθύνη του υπεύθυνου ασφάλειας. Η θέση του υπευθύνου ασφάλειας στο οργανοδιάγραμμα του εκάστοτε οργανισμού ποικίλει. Ο υπεύθυνος ασφάλειας (Chief Information Security Officer - CISO) ή ο επικεφαλής ασφάλειας (Chief Security Officer - CSO) πολλές φορές αναφέρεται στον υπεύθυνο πληροφοριών (Chief Information Officer - CIO). Σε άλλες περιπτώσεις, ο CISO μπορεί να αναφέρεται στον επικεφαλή λειτουργιών (Chief Operations Officer - COO) ή απευθείας στον γενικό διευθυντή (Chief Executive Officer - CEO).

Οι μεγάλες συμβουλευτικές εταιρείες, οι οποίες διαθέτουν μεγάλη εμπειρία σε πρακτικές ασφάλειας και σε συμβουλευτικές υπηρεσίες ασφάλειας μπορούν να αξιολογήσουν την γενική εσωτερική διάρθρωση των οργανισμών και να προτείνουν αποτελεσματικές λειτουργίες ασφάλειας πληροφοριακών συστημάτων. Συνήθως, οι προτάσεις αυτών των συμβουλευτικών εταιρειών, είναι καλοδεχούμενες από το εσωτερικό προσωπικό διότι αναδεικνύουν ζητήματα ασφάλειας τα οποία δύσκολα θα μπορούσαν να εγκριθούν σε άλλη περίπτωση από την διοίκηση. Ένας άλλος καθοριστικός παράγοντας που ορίζει τη δομή ασφάλειας των οργανισμών είναι ο τρόπος λειτουργίας των άλλων οργανισμών που ανήκουν στον ίδιο επιχειρηματικό κλάδο. Οι δημοσιεύσεις σε άρθρα, περιοδικά, οι συζητήσεις με συναδέλφους, οι παρουσιάσεις σε συνέδρια έχουν την μεγαλύτερη επιρροή.

Η εσωτερική δομή της ασφάλειας ενός οργανισμού ορίζει και τις λειτουργίες που θα μπορούσαν να ανατεθούν σε εξωτερικούς παρόχους. Οι συμβουλευτικές εταιρείες που προαναφέραμε, συνήθως παρέχουν και οι ίδιες λύσεις εξωτερικής ανάθεσης ασφάλειας ή τις παρέχουν μέσω συνεργαζόμενων εξωτερικών παρόχων. Αυτές οι εταιρείες, στα πλαίσια της συνεργασίας, ενδέχεται να προτείνουν συνεργασίες τέτοιου είδους εκμεταλλευόμενοι την σχέση που ήδη έχουν με τον οργανισμό. Οι οργανισμοί, θα πρέπει

να αποφεύγουν την ανάθεση διαφορετικών λειτουργιών στις ίδιες εταιρείες για να μειώσουν τον βαθμό εξάρτησης από μεμονωμένους συνεργάτες.

Η δομή της ασφάλειας πληροφοριών, σε γενικές γραμμές επηρεάζεται από την γενική δομή και την κουλτούρα των οργανισμών. Οι συμβουλές ενός εξωτερικού συμβούλου για τον τρόπο οργάνωσης και τη δομή ασφάλειας πληροφοριών, είναι χρήσιμες όταν οι σύμβουλοι γνωρίζουν καλά τον τρόπο λειτουργίας ενός οργανισμού. Στην περίπτωση που δεν ισχύει αυτό, υπάρχει μεγάλη πιθανότητα οι συμβουλές να είναι επιζήμιες, ιδιαίτερα όταν η εφαρμογή της ασφάλειας πληροφοριών δεν ευθυγραμμίζεται με κρίσιμες επιχειρηματικές λειτουργίες.

7.1.2 Ασφάλεια προσωπικού

Η ασφάλεια του προσωπικού μπορεί να ερμηνευτεί με δύο τρόπους. Πρώτον, στόχος της είναι να προστατεύσει τα άτομα που εργάζονται στον οργανισμό από φυσικούς τραυματισμούς, οικονομικές απώλειες και οτιδήποτε άλλο μπορεί να τους βλάψει. Δεύτερον, σχετίζεται με την αντιμετώπιση των προσωπικών προβλημάτων (ανησυχίες), οι οποίες αν δεν αντιμετωπιστούν έγκαιρα, μπορεί να αποτελέσουν κίνδυνο για την ασφάλεια του οργανισμού (Harold & Krause, 2008).

Φυσική ασφάλεια

Η φυσική ασφάλεια του προσωπικού είναι σχετικά εύκολα εφαρμόσιμη και μεταξύ άλλων μπορεί να περιλαμβάνει τις παρακάτω λειτουργίες:

- Έλεγχος ιστορικού σε συμβούλους, εργολάβους και νέο προσωπικό
- Χρήση προσωπικού ασφάλειας
- Σύστημα ελέγχου φυσικής πρόσβασης
- Σύστημα καταγραφής στοιχείων επισκεπτών
- Χρήση συστημάτων βίντεο-επιτήρησης

Η εκτέλεση αυτών των λειτουργιών ασφάλειας μπορεί να ανατεθεί σε εξωτερικό πάροχο.

Προσωπικές ανησυχίες

Οι οργανισμοί στις μέρες μας, επικεντρώνουν όλο και περισσότερο στην προστασία της ψυχολογίας και των συναισθημάτων του προσωπικού τους. Με τα σεμινάρια χρηματοοικονομικού σχεδιασμού, τα εταιρικά προγράμματα αποταμιεύσεων, τα οικονομικά κίνητρα για την επίτευξη στόχων, τις αυξήσεις, την εργασιακή αξιοκρατία και άλλα, οι εργαζόμενοι αισθάνονται πιο ασφαλείς και επομένως είναι λιγότερο πιθανό να εξαπατήσουν τον οργανισμό στον οποίο εργάζονται. Η προστασία της ψυχολογίας των εργαζομένων είναι το ίδιο σημαντική με την φυσική ασφάλεια και απαιτεί πρόσθετα οικονομικά κεφάλαια.

Λοιπά ζητήματα ασφάλειας προσωπικού

Η ανασφάλεια για τις μακροχρόνιες προοπτικές της θέσης των εργαζομένων δημιουργεί δυσαρέσκεια η οποία μπορεί να μετατραπεί σε απειλή για τον οργανισμό. Οι δυσαρεστημένοι υπάλληλοι, οι οποίοι γνωρίζουν τις εσωτερικές λειτουργίες και τα πληροφοριακά συστήματα, θα μπορούσαν να προκαλέσουν σημαντικά προβλήματα στις λειτουργίες του οργανισμού. Η αίσθηση της ασφάλειας των εργαζομένων επηρεάζεται σε μεγάλο βαθμό και από την ανάθεση εσωτερικών λειτουργιών σε εξωτερικό πάροχο. Αυτό συμβαίνει γιατί, αφαιρούνται αρμοδιότητες από τους εσωτερικούς υπαλλήλους και μεταφέρονται στο προσωπικό των εξωτερικών παρόχων. Σε άλλες περιπτώσεις, το εσωτερικό προσωπικό των οργανισμών μεταφέρεται στον εξωτερικό πάροχο ως μέρος της συμφωνίας. Ορισμένοι εργαζόμενοι μπορεί να θεωρήσουν ότι θα έχουν ένα καλύτερο και πιο σίγουρο μέλλον στον εξωτερικό πάροχο ενώ άλλοι μπορεί να το αντιμετωπίσουν αρνητικά.

Από άποψη ασφάλειας, μια τέτοια μεταφορά μπορεί να είναι η προτιμότερη δεδομένου ότι μπορεί να μειώσει τον αριθμό των δυσαρεστημένων εργαζομένων που θα μπορούσαν να αποτελέσουν απειλή για τη λειτουργία του οργανισμού. Στις περιπτώσεις όπου χάνονται θέσεις εργασίας, η δυσαρέσκεια των εργαζομένων είναι πολύ υψηλή και υπάρχει μεγάλος κίνδυνος από ενδεχόμενες κακόβουλες ενέργειες «θυμωμένων» και απολυμένων εργαζομένων. Η υπεξαίρεση, η προσπάθεια πώλησης πολύτιμων επιχειρηματικών πληροφοριών, η υποκλοπή και η καταστροφή δεδομένων είναι κάποιες από τις πιο συνηθισμένες κακόβουλες ενέργειες.

Σε άλλες περιπτώσεις εξωτερικών αναθέσεων, μπορεί να απαιτηθεί από τους εσωτερικούς εργαζομένους να αναλάβουν την εκπαίδευση του προσωπικού των εξωτερικών παρόχων, μέχρις ότου ολοκληρωθεί το έργο της μετάπτωσης. Συχνά το μέγεθος της αποζημίωσης κατά την αποχώρησή τους, εξαρτάται από το επίπεδο επιτυχίας της εκπαίδευσης των αντικαταστατών. Σε αυτές τις περιπτώσεις, ο εκπαιδευτής πιθανών να παραλείψει εσκεμμένα να μεταφέρει στον εκπαιδευόμενο κρίσιμα στοιχεία θέτοντας με αυτόν τον τρόπο το νέο περιβάλλον λειτουργίας σε κίνδυνο.

Οι οργανισμοί γνωρίζοντας αυτούς τους κινδύνους, θα πρέπει να εφαρμόσουν κατάλληλα μέτρα ασφάλειας για να τους μετριάσουν ή να τους εξαλείψουν. Το πιο απλό μέτρο, είναι να είναι ειλικρινείς με τους εργαζομένους τους. Αυτό δεν σημαίνει ότι θα πρέπει να τους ενημερώνουν για όλα τα θέματα, αλλά σίγουρα θα πρέπει να τους λένε αλήθειες. Η συμμετοχή των εργαζομένων σε κρίσιμες αποφάσεις των οργανισμών όπως οι εξωτερικές αναθέσεις θα μπορούσε επίσης να μετριάσει τον κίνδυνο. Αν ο οργανισμός είναι αρκετά ευέλικτος θα μπορούσε να αναθέσει στο προσωπικό άλλες λειτουργίες ή να

το μεταφέρει σε άλλες εγκαταστάσεις. Η καταβολή μέρους των αποζημιώσεων, κατόπιν συμφωνίας με τους εργαζομένους, αποτελεί ένα άλλο μέτρο για να αποφύγει ο οργανισμός νομικές διαμάχες και να διασφαλίσει την συνεργασία κατά το στάδιο μετάπτωσης στον εξωτερικό πάροχο. Όλα τα παραπάνω έχουν την ίδια ισχύ ανεξάρτητα από το αν προκύπτουν από εξωτερικές αναθέσεις, οικονομικά προβλήματα, νέες τεχνολογίες ή άλλους παράγοντες.

7.1.3 Διαβάθμιση και έλεγχος πληροφοριακών περιουσιακών στοιχείων

Η διαβάθμιση και η προστασία των πληροφοριακών περιουσιακών στοιχείων αποτελεί κατά κανόνα αρμοδιότητα του οργανισμού που κατέχει τις πληροφορίες. Στις μέρες μας, επιβάλλονται όλο και περισσότεροι κανόνες από ρυθμιστικές αρχές για την προστασία των δεδομένων είτε αυτά είναι προσωπικά είτε είναι επιχειρηματικά. Οι νομοθέτες και οι ρυθμιστικές αρχές θέτουν υπεύθυνους για την προστασία αυτών των δεδομένων τους ίδιους τους οργανισμούς, ανεξάρτητα από το αν τις μεταφέρουν ή τις επεξεργάζονται σε εξωτερικούς παρόχους. Οι ρυθμιστικές αρχές στην Ευρώπη, το Ηνωμένο Βασίλειο, τις Ηνωμένες Πολιτείες και σε άλλες χώρες, απαιτούν ολοένα και περισσότερο από τα χρηματοπιστωτικά ιδρύματα και τα ιδρύματα παροχής υπηρεσιών υγείας, να διευρύνουν την εποπτεία και την προστασία τέτοιων δεδομένων κατά την παραλαβή, επεξεργασία, αποθήκευση και διανομή τους σε τρίτους. Απαιτούν επίσης, να έχουν άμεση πρόσβαση στα πληροφοριακά συστήματα των οργανισμών, εφόσον κριθεί απαραίτητο για τη διενέργεια ελέγχου.

Η διαβάθμιση των δεδομένων μπορεί να πραγματοποιηθεί με διάφορους τρόπους. Η πιο συχνή μέθοδος βασίζεται στην εκτίμηση της ζημιάς που μπορεί να προκληθεί στον οργανισμό, στους πελάτες ή στους συνεργάτες του αν αυτά τα δεδομένα προσπελαστούν, αλλοιωθούν ή διαγραφούν μέσω μη εξουσιοδοτημένης πρόσβασης. Οι εκτιμήσεις των οργανισμών ως προς το ποιά ζημιά μπορεί να προκύψει και ποιές είναι οι πιθανότητες να πραγματοποιηθεί, είναι εξαιρετικά υποκειμενικές. Επιπλέον, είναι πολύ δύσκολο να υπολογιστεί η έκτασης της ζημίας, ειδικά αν αφορά στην φήμη του οργανισμού, η οποία είναι ιδιαίτερα δύσκολο να προσδιοριστεί ποσοτικά. Κατά συνέπεια, οι οργανισμοί παρέχουν συνήθως παραδείγματα διαβάθμισης πληροφοριών. Στον Πίνακας 9, απεικονίζονται οι κύριες διαβαθμίσεις πληροφοριών και αναφέρονται παραδείγματα για κάθε μια από αυτές.

Πίνακας 9:*Κατηγορίες διαβάθμισης πληροφοριών και παραδείγματα*

Διαβάθμιση	**Ορισμός**	**Παράδειγμα**
Δημόσιο	Πληροφορίες που είναι γενικά διαθέσιμες και η διάδοσή τους δεν επηρεάζει τον	Τιμές μετοχών, εφημερίδες, άρθρα στο διαδίκτυο,

	οργανισμό, τους πελάτες ή τους συνεργάτες.	ανακοινώσεις μέσω τηλεόρασης ή ραδιοφώνου.
Εσωτερικό	Πληροφορίες οι οποίες είναι εύκολα προσβάσιμες εσωτερικά στον οργανισμό και στους συνεργάτες αλλά δεν είναι δημόσιες. Η πιθανή διαρροή τους, δεν προκαλεί κάποια ζημιά στον οργανισμό, στους πελάτες ή στους συνεργάτες	Περιγραφές εσωτερικών λειτουργιών και διαδικασιών.
Εμπιστευτικό	Πληροφορίες που αν διαρρεύσουν θα μπορούσαν να προκαλέσουν σημαντική ζημιά στον οργανισμό, τους πελάτες και τους συνεργάτες. Ο οργανισμός θα πρέπει να υπογράφει σύμφωνο εμπιστευτικότητας με οποιονδήποτε ανταλλάσσει τέτοιου είδους πληροφορίες.	Εσωτερικές και εξωτερικές επιχειρηματικές επικοινωνίες. Οικονομικές πληροφορίες σχετικά με την εταιρεία, τους συνεργάτες και τους πελάτες.
Μη δημόσιο προσωπικό	Πληροφορίες που σχετίζονται με άτομα. Τυχόν διαρροή τους, μπορεί οδηγήσει σε ατομικά προβλήματα και να προκαλέσει ζημιά στην φήμη του οργανισμού.	Συνδυασμός προσωπικών πληροφοριών όπως όνομα, επίθετο, διεύθυνση, αριθμός κοινωνικής ασφάλισης κ.τ.λ.
Ευαίσθητο προσωπικό	Πολύ προσωπικές πληροφορίες που δεν πρέπει να συλλέγονται χωρίς συγκεκριμένο ή βάσιμο λόγο, και για τις οποίες έχει δώσει συγκατάθεση το άτομο. Η λανθασμένη αποκάλυψή τους μπορεί να προκαλέσει σημαντικά προβλήματα στο οργανισμούς.	Θρησκεία, σεξουαλικές προτιμήσεις.
Απόρρητο	Πολύ περιορισμένες πληροφορίες που η αποκάλυψή τους σε μη εξουσιοδοτημένα άτομα μπορεί να προκαλέσει σοβαρές ζημιές στον οργανισμό, τους πελάτες και τους συνεργάτες.	Πληροφορίες οι οποίες σχετίζονται με επερχόμενες συγχωνεύσεις ή εξαγορές, επιχειρηματικές δραστηριότητες, μισθοί εργαζομένων κ.ά.
Άκρως απόρρητο	Πληροφορίες υψηλής κρισιμότητας που διατίθενται σε πολύ μικρό αριθμό ατόμων οι οποίες αν χρησιμοποιηθούν με λάθος τρόπο μπορούν να προκαλέσουν τεράστιες καταστροφές.	Πληροφορίες που αφορούν στην εθνική άμυνα ή πατέντες προϊόντων.

Εφόσον διαβαθμιστούν οι πληροφορίες, είναι απαραίτητο να καθοριστεί ο τρόπος διάθεσης των δεδομένων αυτών κατά τη δημιουργία, επεξεργασία, αποθήκευση και μετάδοση, δεδομένου ότι κάθε κατηγορία αντιμετωπίζεται διαφορετικά. Στον Πίνακας 10 απεικονίζεται ο τρόπος με τον οποίο ορίζεται η διάθεση των δεδομένων.

Πίνακας 10:*Διάθεση πληροφοριών βάση κατηγορίας διαβάθμισης*

Διαβάθμιση	Δημιουργία	Επεξεργασία	Μεταφορά	Αποθήκευση	Διάθεση
Δημόσιο	Δημιουργούνται από οποιονδήποτε.	Δεν απαιτείται κάποια προστασία.	Δεν απαιτείται κάποια προστασία.	Δεν απαιτείται κάποια προστασία.	Δεν απαιτούνται ειδικές διαδικασίες.
Εσωτερικό	Από το εσωτερικό προσωπικό στα πλαίσια της λειτουργίας του οργανισμού.	Θα πρέπει να ορίζεται ότι είναι μόνο για εσωτερική χρήση.	Δεν απαιτείται κάποια προστασία.	Δεν απαιτείται κάποια προστασία.	Δεν απαιτούνται ειδικές διαδικασίες.
Εμπιστευτικό	Δημιουργούνται κατά την κανονική λειτουργία του οργανισμού.	Θα πρέπει να ορίζεται ότι είναι εμπιστευτικά. Στις περιπτώσεις απομακρυσμένης πρόσβασης σε αυτά θα πρέπει να εφαρμόζονται ισχυροί μηχανισμοί αυθεντικοποίησης.	Θα πρέπει να κρυπτογραφούνται όταν μεταφέρονται από δημόσια δίκτυα.	Θα πρέπει να αποθηκεύονται με κρυπτογραφημένη μορφή.	Απαιτούνται ειδικά μέτρα προστασίας όπως η ασφαλή καταστροφή εγγράφων και μέσων αποθήκευσης.
Μη δημόσιο προσωπικό	Δημιουργούνται κατά την κανονική λειτουργία του οργανισμού.	Θα πρέπει να ορίζεται ότι είναι εμπιστευτικά. Στις περιπτώσεις απομακρυσμένης πρόσβασης σε αυτά θα πρέπει να εφαρμόζονται ισχυροί μηχανισμοί αυθεντικοποίησης.	Θα πρέπει να κρυπτογραφούνται όταν μεταφέρονται από δημόσια δίκτυα.	Θα πρέπει να αποθηκεύονται με κρυπτογραφημένη μορφή.	Απαιτούνται ειδικά μέτρα ασφάλειας για την προστασία από αποκάλυψη.
Ευαίσθητο προσωπικό	Δημιουργούνται μόνο σε περιπτώσεις που κρίνεται απαραίτητο.	Θα πρέπει να ορίζεται ότι είναι απόρρητα. Στις περιπτώσεις απομακρυσμένης πρόσβασης σε αυτά θα πρέπει να εφαρμόζονται ισχυροί μηχανισμοί αυθεντικοποίησης. Η πρόσβαση θα πρέπει να είναι πολύ περιορισμένη.	Θα πρέπει να κρυπτογραφούνται όταν μεταφέρονται από δημόσια δίκτυα.	Θα πρέπει να αποθηκεύονται με κρυπτογραφημένη μορφή.	Απαιτούνται ειδικά μέτρα ασφάλειας για την προστασία από αποκάλυψη.
Απόρρητό	Δημιουργούνται κατά την κανονική λειτουργία του οργανισμού.	Θα πρέπει να ορίζεται ότι είναι απόρρητα. Στις περιπτώσεις απομακρυσμένης πρόσβασης σε αυτά θα πρέπει να εφαρμόζονται ισχυροί μηχανισμοί αυθεντικοποίησης. Η πρόσβαση θα πρέπει να είναι περιορισμένη.	Θα πρέπει να κρυπτογραφούνται όταν μεταφέρονται από δημόσια δίκτυα.	Θα πρέπει να αποθηκεύονται με κρυπτογραφημένη μορφή.	Απαιτούνται ειδικά μέτρα ασφάλειας για την προστασία από αποκάλυψη.
Άκρως απόρρητο	Δημιουργούνται κατά την κανονική λειτουργία του οργανισμού.	Θα πρέπει να ορίζεται ότι είναι άκρως απόρρητα. Στις περιπτώσεις απομακρυσμένης πρόσβασης σε αυτά θα πρέπει να εφαρμόζονται ισχυροί μηχανισμοί	Δεν θα πρέπει να μεταφέρονται από δημόσια δίκτυα	Θα πρέπει να αποθηκεύονται κρυπτογραφημένα πάντα.	Απαιτούνται ειδικά μέτρα ασφάλειας για την προστασία από αποκάλυψη.

		αυθεντικοποίησης. Η πρόσβαση θα πρέπει να είναι απολύτως περιορισμένη.			

Ο κάτοχος δεδομένων ή, κατά πάσα πιθανότητα, ο κάτοχος της εφαρμογής που δημιουργεί και διατηρεί τα δεδομένα, καθορίζει και τη διαβάθμιση των συγκεκριμένων δεδομένων. Η διαβάθμιση των δεδομένων, ουσιαστικά ορίζει την πολιτική και τις διαδικασίες που θα πρέπει να εφαρμοστούν για την προστασία των δεδομένων ανεξάρτητα αν αυτά παραμένουν εντός του οργανισμού ή μεταβιβάζονται σε εξωτερικό πάροχο. Οι εξωτερικοί πάροχοι, για να ικανοποιήσουν αυτές τις απαιτήσεις, θα πρέπει να υιοθετήσουν την ίδια πολιτική και τις διαδικασίες διαβάθμισης δεδομένων με τους οργανισμούς που εξυπηρετούν (Harold & Krause, 2008) .

7.1.4 Πολιτική ασφάλειας

Όπως και στη διαβάθμιση των πληροφοριών, ένας οργανισμός θα μπορούσε να προσλάβει έναν εξωτερικό συνεργάτη για να αναπτύξει την πολιτική ασφάλειας των πληροφοριών μαζί με τα συνοδευτικά πρότυπα, τις βασικές γραμμές, τις κατευθυντήριες γραμμές και τις διαδικασίες. Οι εξωτερικοί συνεργάτες θα μπορούσαν επίσης να χρησιμοποιηθούν για να υλοποιήσουν και τα εσωτερικά συστήματα ενημέρωσης μέσω των οποίων θα ενημερώνεται το προσωπικό του οργανισμού για τις πολιτικές και τα πρότυπα ασφάλειας που εφαρμόζονται. Οι εξωτερικοί σύμβουλοι είναι ένα αναγνωρισμένο μέσο για την καθιέρωση βέλτιστων πρακτικών στον οργανισμό, γρήγορα και αποτελεσματικά.

Αρχικά, είναι πολύ σημαντικό για διαχωριστούν οι οδηγίες και οι εντολές που αφορούν στην ασφάλεια των πληροφοριών του οργανισμού. Με αυτόν τον τρόπο αποφεύγεται η σύγχυση στο προσωπικού του οργανισμού, για τα «πρέπει» και «δεν πρέπει» της ασφάλειας των πληροφοριών. Σε γενικές γραμμές, η πολιτική ασφάλειας είναι μια οδηγία υψηλού επιπέδου που ορίζει την κατάλληλη και απαιτούμενη συμπεριφορά του προσωπικού σε ορισμένες συνθήκες. Η πολιτική ασφάλειας δεν αλλάζει πολύ με την πάροδο του χρόνου, ειδικά στις περιπτώσεις που περιλαμβάνει γενικούς όρους. Αλλά ακόμη και σε αυτές τις περιπτώσεις, η χρήση νέων τεχνολογιών εντός και εκτός του οργανισμού θα μπορούσε να οδηγήσει στην αναθεώρησή της.

Η πολιτική ασφάλειας είναι πιο ανθεκτική στις αλλαγές από τα πρότυπα ασφάλειας. Η εφαρμογή της πολιτικής ασφάλειας σε εφαρμογές και πληροφοριακά συστήματα με συγκεκριμένη αρχιτεκτονική και ρυθμίσεις υλικού και λογισμικού, μπορεί να εκφραστεί μόνο μέσα από συγκεκριμένα πρότυπα, βασικές γραμμές και διαδικασίες. Κατά την

συνεργασία με κάποιον εξωτερικό πάροχο υπηρεσιών, ο οργανισμός θα πρέπει να διασφαλίσει ότι και ο πάροχος συμμορφώνεται με τις πολιτικές ασφαλείας του. Η συμμόρφωση μπορεί να επιτευχθεί με διάφορους τρόπους, οι οποίοι περιγράφονται παρακάτω (Purser, 2004) (Harold & Krause, 2008).

Υιοθέτηση πολιτικής πελατών

Ο εξωτερικός πάροχος θα πρέπει να συμφωνήσει και να τηρήσει την πολιτική ασφάλειας του οργανισμού. Κάτι τέτοιο όμως μπορεί να απαιτεί σημαντική προσπάθεια και κεφάλαια από τον εξωτερικό πάροχο. Μπορεί επίσης να υπάρχουν εθνικοί, περιφερειακοί και τοπικοί κανονισμοί που περιορίζουν τον εξωτερικό πάροχο στο να εφαρμόσει ορισμένους όρους της πολιτικής.

Υιοθέτηση της πολιτικής του εξωτερικού παρόχου

Ο οργανισμός μπορεί να συμφωνήσει να υιοθετήσει την πολιτική ασφάλειας του εξωτερικού παρόχου υπηρεσιών, όταν ο εξωτερικός πάροχος εφαρμόζει τα ίδια ή ισχυρότερα πρότυπα ασφάλειας. Στην περίπτωση αυτή, η πολιτική του εξωτερικού παρόχου υπερισχύει της πολιτικής του οργανισμού. Συνήθως ο εξωτερικός πάροχος, επειδή υποστηρίζει πολλούς πελάτες, διαθέτει καλύτερη πολιτική, πρότυπα, και διαδικασίες.

Ανταπόκριση και αξιολόγηση

Όταν ο οργανισμός και ο εξωτερικός πάροχος υπηρεσιών δεν είναι πρόθυμοι να μοιραστούν την ίδια πολιτική, πρότυπα και διαδικασίες, θα πρέπει ο οργανισμός να καθορίσει τον βαθμό που αυτά ικανοποιούν τις απαιτήσεις του, θέτοντας μια σειρά ερωτήσεων σχετικά με τον χειρισμό διαφόρων καταστάσεων. Στον Πίνακας 11 δίνονται παραδείγματα πολιτικών, προτύπων και διαδικασιών αλλά περιλαμβάνονται και σχόλια σχετικά με την εφαρμογή τους.

Πίνακας 11:*Παραδείγματα πολιτικών, προτύπων και διαδικασιών*

Τύπος οδηγίας	**Παράδειγμα**	**Σχόλια**
Πολιτικές	Ηλεκτρονικό ταχυδρομείο, απομακρυσμένη πρόσβαση, χρήση διαδικτύου.	Σε γενικές γραμμές εφαρμόζεται στους χρήστες του οργανισμού. Απαιτούνται ελάχιστες αλλαγές κατά την πάροδο του χρόνου.

Πρότυπα	Λειτουργικά συστήματα, προσωπικοί υπολογιστές, δρομολογητές, διακλαδωτές, τείχη προστασίας κ.ά. Διασφαλίζεται ο έλεγχος και ο τρόπος παραμετροποίησης του λογισμικού και των συστημάτων. Διευκολύνεται η διενέργεια αναβαθμίσεων και παραμετροποιήσεων.	Περιλαμβάνονται συνήθως τεχνικά θέματα όπως για παράδειγμα οι τεχνικές προδιαγραφές των συστημάτων και του λογισμικού. Αλλάζει μόνο αν υπάρξει σημαντική αλλαγή που αφορά στο λογισμικό ή στα συστήματα.
Βασικές γραμμές	Περιλαμβάνουν συγκεκριμένες εφαρμογές προτύπων λειτουργίας. Ως παράδειγμα μπορούμε να αναφέρουμε τις εκδόσεις λειτουργικών συστημάτων.	Πιο τεχνικές από τα πρότυπα. Ενημερώνονται κάθε λίγους μήνες διότι το λογισμικό και τα συστήματα αλλάζουν συχνά.
Κατευθυντήριες γραμμές	Αφορούν στους προτεινόμενους αλλά όχι υποχρεωτικούς τρόπους εφαρμογής ενός προτύπου.	Προορίζεται συνήθως για περιβάλλοντα που απαιτούν κάποιο επίπεδο ευελιξίας και μεταβλητότητας.
Διεργασία	Αφορά στην υψηλού επιπέδου σειρά εργασιών που είναι σχεδιασμένες να επιτρέπουν σε όσους βρίσκονται εσωτερικά στον οργανισμό, να συμμορφωθούν με την πολιτική.	Αποτελεί τον τρόπο διαχείρισης των εσωτερικών δραστηριοτήτων του οργανισμού.
Διαδικασία	Αφορά στις εργασίες χαμηλού επιπέδου οι οποίες περιλαμβάνουν τις διεργασίες.	Ακολουθούνται με λεπτομέρεια και ορίζουν συγκεκριμένες σειριακές ή παράλληλες ενέργειες.

Εφαρμογή και συμμόρφωση

Οι οργανισμοί κατά την αξιολόγηση των πολιτικών, των προτύπων και των διαδικασιών των εξωτερικών παρόχων, θα πρέπει να δίνουν ιδιαίτερη έμφαση και στον βαθμό τεκμηρίωσης και εφαρμογής τους. Η υλοποίηση αυτών είναι εύκολη, δεν ισχύει όμως το ίδιο και για την εφαρμογή τους. Ο προσδιορισμός του επιπέδου ποιότητας και του βαθμού τήρησης των πολιτικών, των προτύπων και των διαδικασιών είναι εργασίες που καλύτερα να ανατίθεται σε εξειδικευμένους εξωτερικούς συμβούλους. Αυτοί, διαθέτουν

την απαραίτητη τεχνογνωσία για να εξετάσουν και να διαπιστώσουν αν εφαρμόζονται όλες οι απαραίτητες διαδικασίες συμμόρφωσης από τον εξωτερικό πάροχο.

7.2 Έλεγχος προσβάσεων

Ένα από τα σημαντικότερα ζητήματα που σχετίζεται με την ασφάλεια πληροφοριακών συστημάτων, είναι ο έλεγχος προσβάσεων στα πληροφοριακά περιουσιακά στοιχεία ενός οργανισμού. Ο έλεγχος προσβάσεων, «ανησυχεί» σε μεγάλο βαθμό τους οργανισμούς, τους νομοθέτες και τις ρυθμιστικές αρχές. Η απάτη της κλοπής ταυτότητας, έχει λάβει μεγάλες διαστάσεις στους οργανισμούς και προκαλεί σημαντικά οικονομικά προβλήματα. Οι πληροφορίες που σχετίζονται με το προσωπικό του οργανισμού ή των εξωτερικών παρόχων και διαβιβάζονται από το ένα μέρος στο άλλο στα πλαίσια μιας εξωτερικής ανάθεσης, πρέπει να διασφαλιστούν. Τα μέτρα ασφάλειας που μπορούν να προστατεύσουν τους οργανισμούς από την υποκλοπή ταυτοτήτων είναι η πιστοποίηση ταυτότητας, η εξουσιοδότηση, η διαχείριση και ο έλεγχος της πρόσβασης. Οι μηχανισμοί που μπορούν να εφαρμοστούν για την εξακρίβωση της γνησιότητας της ταυτότητας μπορεί να είναι:

- Κωδικοί, μαγνητικές κάρτες
- Κωδικοί μιας χρήσης
- Ψηφιακά πιστοποιητικά
- Αυθεντικοποίηση με χρήση βιομετρικών
- Πολλαπλοί τρόποι αυθεντικοποίησης

Στον Πίνακας 12 απεικονίζεται το επίπεδο ασφάλειας και το κόστος του κάθε μηχανισμού ταυτοποίησης.

Πίνακας 12:*Μηχανισμοί ταυτοποίησης ανά επίπεδο ασφάλειας.*

Επίπεδο ασφάλειας	**Τεχνολογία**	**Κόστος**	**Παραδείγματα εφαρμογής**
Χαμηλό	Κωδικοί πρόσβασης.	Χαμηλό κόστος υλοποίησης και υποστήριξης.	Ιστοσελίδες και απλές εφαρμογές.
Μεσαίο	Κωδικοί μιας χρήσης & Ψηφιακά πιστοποιητικά.	Σχετικά χαμηλό κόστος υλοποίησης και υποστήριξης.	Τραπεζικά συστήματα και συστήματα μεσαίου επιπέδου ασφάλειας.
Υψηλό	Αυθεντικοποίηση με χρήση βιομετρικών &	Υψηλό κόστος υλοποίησης και υποστήριξης.	Πρόσβαση σε εφαρμογές και

	Αυθεντικοποίηση με πολλαπλούς τρόπους.		περιοχές υψηλής ασφάλειας.

Ο έλεγχος των δικαιωμάτων πρόσβασης αποτελεί μια από τις πιο δύσκολες και απαιτητικές διαδικασίες διαχείρισης ασφάλειας των πληροφοριακών συστημάτων. Στις περιπτώσεις που εμπλέκονται πολλά μέρη όπως οι εξωτερικοί πάροχοι, ο έλεγχος αυτός γίνεται ακόμη πιο πολύπλοκος και δύσκολος διότι, πρόσβαση σε σημαντικές πληροφορίες του οργανισμού εκτός από τους εσωτερικούς υπαλλήλους, έχουν και οι υπάλληλοι του εξωτερικών παρόχων. Οι οργανισμοί θα πρέπει να διασφαλίζουν ότι οι έλεγχοι ιστορικού των υπαλλήλων είναι ακριβείς και πλήρεις. Αυτό είναι αρκετά δύσκολο να πραγματοποιηθεί για τους εσωτερικούς υπαλλήλους και ακόμη δυσκολότερο για το προσωπικό των εξωτερικών παρόχων, ιδίως εκείνων που δραστηριοποιούνται σε ξένη χώρα.

Όσο οι νομοθέτες και οι ρυθμιστικές αρχές επικεντρώνουν σε θέματα που αφορούν στην μη εξουσιοδοτημένη πρόσβαση και κατάχρηση προσωπικών δεδομένων, η ανάγκη να διασφαλιστεί ότι οι πάροχοι υπηρεσιών λαμβάνουν τα απαραίτητα μέτρα ασφάλειας γίνεται όλο και πιο σημαντική καθώς τα πρόστιμα και ο αντίκτυπος στην φήμη των οργανισμών, συνεχώς αυξάνονται (Harold & Krause, 2008).

7.3 Μοντέλα ασφάλειας και αρχιτεκτονική

Οι οργανισμοί, πλέον κατανοούν ότι για την προστασία των πληροφοριακών συστημάτων απαιτούνται συγκεκριμένες αρχιτεκτονικές ασφάλειας οι οποίες επιτρέπουν την ορθή εφαρμογή μηχανισμών πιστοποίησης, εξουσιοδότησης, ελέγχου και διαχείρισης. Για την υλοποίηση των αρχιτεκτονικών ασφάλειας, θα πρέπει να χρησιμοποιούνται διάφορα εργαλεία ασφάλειας όπως τα τείχη προστασίας, τα συστήματα εντοπισμού και παρεμπόδισης εισβολών, τα λογισμικά προστασίας από ιούς ή λογισμικά εντοπισμού ευπαθειών. Κατά την εξωτερική ανάθεση, οι απαιτήσεις των οργανισμών από τους εξωτερικούς παρόχους για την ασφάλεια των ανατεθέντων υπηρεσιών θα πρέπει να βασίζονται κυρίως στα ακόλουθα (Harold & Krause, 2008).

Πλαίσιο υπηρεσιών ασφάλειας

Το πλαίσιο ασφάλειας περιλαμβάνει τις διαδικασίες μέσω των οποίων οι εξωτερικοί πάροχοι ενσωματώνουν τις υπηρεσίες ασφάλειας στο συνολικό σύστημα εφαρμογών και στις αρχιτεκτονικές δικτύου ενός οργανισμού. Στο ίδιο πλαίσιο εντάσσονται και οι προδιαγραφές ασφάλειας, τις οποίες θα πρέπει να καλύπτουν τα λογισμικά και οι συσκευές που χρησιμοποιούνται από τους εξωτερικούς παρόχους για την προστασία

των πελατών τους. Η ανάπτυξη ενός ισχυρού πλαισίου ασφάλειας αυξάνει τον έλεγχο των λειτουργιών ασφάλειας και μειώνει το κόστος και τον χρόνο διάθεσης των εφαρμογών. Οι υπηρεσίες ασφάλειας δεν θα πρέπει να ενσωματώνονται στις ίδιες τις εφαρμογές αλλά οι εφαρμογές θα πρέπει να τις καλούν ανάλογα με τις ανάγκες τους. Με αυτόν τον τρόπο υπάρχει μεγαλύτερη ευελιξία κατά την υλοποίηση εφαρμογών και πολύ καλύτερο επίπεδο ελέγχου ασφάλειας.

Υποδομή Ασφάλειας

Ως υποδομή ασφάλειας ορίζεται ο συνδυασμός πολιτικών ασφάλειας, προτύπων, διαδικασιών, συσκευών και λογισμικού που συντελούν στην αποτροπή, αποφυγή, πρόληψη, προστασία και παρακολούθηση των λειτουργιών ενός οργανισμού. Για παράδειγμα, ο συνδυασμός συστημάτων ανίχνευσης και προστασίας εισβολών, τα τείχη προστασίας, το λογισμικό προστασίας από ιούς, οι υπηρεσίες ελέγχου ασφάλειας ηλεκτρονικού ταχυδρομείου και πρόσβασης σε ιστοσελίδες αποτελούν παραδοσιακά τεχνικά μέτρα ασφάλειας. Αντιθέτως, η καθιέρωση, η ευαισθητοποίηση και η επιβολή πολιτικών, προτύπων και διαδικασιών έχουν να κάνουν με την ανθρώπινη και λογική ασφάλεια.

Διαχείριση ασφάλειας και έλεγχος

Οι λειτουργίες διαχείρισης ασφάλειας αφορούν στη διαχείριση όλων των συστημάτων ασφάλειας που περιλαμβάνονται στην υποδομή ενός οργανισμού. Επιπλέον, οι λειτουργίες επιβολής πολιτικών ασφάλειας αποσκοπούν στην ευαισθητοποίηση, την κατάρτιση, την επίσημη αποδοχή της πολιτικής, των προτύπων και των διαδικασιών από τα υποκείμενα (υπαλλήλους, εργολάβους και φορείς παροχής υπηρεσιών) καθώς και στην παρακολούθηση, στον έλεγχο και στην αναφορά συμμόρφωσης.

Εφαρμογή των μοντέλων ασφάλειας από τους εξωτερικούς παρόχους

Προκειμένου να μπορέσουν οι εξωτερικοί πάροχοι να εφαρμόσουν αυτά τα μοντέλα ασφάλειας, θα πρέπει να συμμορφώνονται με την πολιτική και τα πρότυπα ασφάλειας των οργανισμών που υποστηρίζουν και αντίστοιχα, η αρχιτεκτονική ασφάλειάς τους θα πρέπει να είναι συμβατή με αυτή των οργανισμών. Στις περιπτώσεις που κάτι τέτοιο δεν είναι εφικτό, όπως για παράδειγμα λόγω περιορισμών τεχνολογίας, κόστους ή νομικών και κανονιστικών απαιτήσεων, οι οργανισμοί θα πρέπει να συμφωνήσουν από κοινού με τους εξωτερικούς παρόχους πριν προχωρήσουν σε οποιαδήποτε ενέργεια.

Η βασική προσέγγιση σε αυτό το σημείο, είναι να εξεταστεί ο τρόπος με τον οποίο οι προσφερόμενες υπηρεσίες και προϊόντα που σχετίζονται με την ασφάλεια μπορούν να ακολουθήσουν το πλαίσιο ασφάλειας ή μπορούν να ενταχθούν στη γενική αρχιτεκτονική

ασφάλειας και στα συστήματα διαχείρισης και ελέγχου. Θα πρέπει να εξεταστεί επίσης, κατά πόσον οι προσφερόμενες λειτουργίες ταιριάζουν στην υπάρχουσα υποδομή και αν μπορούν να διασυνδέονται αποτελεσματικά με τις εγκατεστημένες εφαρμογές τελικών χρηστών και συστημάτων. Η συμβατότητα με την υποδομή των οργανισμών μπορεί να ελεγχθεί εξετάζοντας τις τεχνικές προδιαγραφές των λογισμικών και των συστημάτων αλλά με την υλοποίηση πιλοτικών εγκαταστάσεων.

Τα ίδια κριτήρια ισχύουν και στην απόκτηση προϊόντων διαχείρισης και ελέγχου που πρέπει να χρησιμοποιούνται είτε στις τοποθεσίες των οργανισμών ή, των εξωτερικών παρόχων. Παραδείγματος χάριν, ο εξωτερικός πάροχος θα μπορούσε να παρακολουθεί τα συστήματα ανίχνευσης εισβολών και τα τείχη προστασίας που είναι εγκατεστημένα στις εγκαταστάσεις του οργανισμού ή, να φροντίζει για την εγκατάσταση εργαλείων παρακολούθησης τόσο στην τοποθεσία του οργανισμού όσο και στη δική του. Η επιλογή της αρχιτεκτονικής ασφάλειας εξαρτάται κυρίως από την τεχνογνωσία του εξωτερικού παρόχου καθώς και από τους οικονομικούς πόρους των οργανισμών.

Σε όλες αυτές τις περιπτώσεις, το πιο σημαντικό για τους εξωτερικούς παρόχους, είναι η συμμόρφωση με την πολιτική και τα πρότυπα ασφάλειας των οργανισμών καθώς και η συμβατότητα με την υποδομή τους. Εάν υπάρχουν λόγοι για τους οποίους δεν μπορεί να επιτευχθεί συμμόρφωση, πρέπει να σημειωθούν οι εξαιρέσεις και να εφαρμοστούν διαδικασίες και συστήματα περιορισμού του κινδύνου.

7.4 Φυσική ασφάλεια

Όπως αναφέρθηκε προηγουμένως, είναι σύνηθες να ανατίθεται σε εξωτερικούς παρόχους η φυσική ασφάλεια για την προστασία των φυσικών περιουσιακών στοιχείων ενός οργανισμού, ανεξάρτητα από το εάν τα συγκεκριμένα περιουσιακά στοιχεία διαθέτουν ή όχι πληροφορίες. Ακόμη και σήμερα, πολλά από τα συστήματα φυσικής ασφάλειας είναι χαμηλής τεχνολογίας. Ωστόσο, υπάρχει η τάση προς την απομακρυσμένη κεντρική διαχείριση και τον έλεγχο. Η τεχνολογία και το κόστος έχουν αρχίσει να οδηγούν όλο και περισσοτέρους οργανισμούς στην υλοποίηση απομακρυσμένων σταθμών εποπτείας, οι οποίοι διαχειρίζονται εξ' αποστάσεως τα συστήματα φυσικής ασφάλειας. Επιπλέον, καθώς ο έλεγχος της φυσικής πρόσβασης συγκλίνει με τον έλεγχο πρόσβασης σε πληροφοριακά συστήματα, δημιουργείται η ανάγκη για ολοκληρωμένη φυσική και λογική ασφάλεια. Όσο εξελίσσονται τα συστήματα ασφάλειας τόσο αυξάνεται και η απαίτηση για εξειδικευμένο προσωπικό στους οργανισμούς. Για να αντιμετωπιστεί αυτό το πρόβλημα, οι οργανισμοί συνήθως στρέφονται σε εξωτερικούς παρόχους οι οποίοι διαθέτουν την απαιτούμενη τεχνογνωσία και τους απαραίτητους ανθρώπινους πόρους. Από την άλλη πλευρά, υπάρχουν και

οργανισμοί οι οποίοι δε ρισκάρουν να αναθέσουν σημαντικές λειτουργίες, όπως είναι η φυσική ή λογική ασφάλεια σε εξωτερικούς παρόχους.

Μια άλλη πτυχή που πρέπει να εξεταστεί, η οποία θα μπορούσε να ευνοηθεί από την χρήση ενός εξωτερικού παρόχου, είναι η αντιμετώπιση καταστάσεων έκτακτης ανάγκης στις οποίες θα πρέπει να εφαρμοστούν σχέδια αποκατάστασης καταστροφών. Σε αυτές τις περιπτώσεις, ο εξωτερικός πάροχος θα μπορούσε να καλύψει διάφορες λειτουργίες του οργανισμού μέχρι ο οργανισμός να επανέλθει σε καθεστώς κανονικής λειτουργίας. Αυτό είναι προτιμότερο για τον οργανισμό από το να βασίζεται εξ' ολοκλήρου στις δικές του εσωτερικές λειτουργίες αποκατάστασης (Harold & Krause, 2008).

7.5 Τηλεπικοινωνίες και ασφάλεια δικτύων

Οι τηλεπικοινωνίες συγκαταλέγονται στις πρώτες τεχνολογικές περιοχές που ανατίθενται σε εξωτερικούς παρόχους και μάλιστα σε μεγάλη κλίμακα. Τα κόστη και οι δυσκολίες εγκατάστασης και συντήρησης των τηλεπικοινωνιών από το εσωτερικό προσωπικό, οδήγησαν όλο και περισσότερους οργανισμούς προς αυτήν την κατεύθυνση. Πριν από το διαδίκτυο, τα δίκτυα μεγάλης ταχύτητας υποστηρίζονταν από μισθωμένες γραμμές. Η ασφάλεια αυτών των γραμμών δεν αποτελούσε σημαντικό ζήτημα, καθώς η πρόσβαση περιοριζόταν σε κάθε της άκρο. Σημαντικότερα ζητήματα εκείνη την εποχή ήταν η υψηλή διαθεσιμότητα, η ταχεία ανάπτυξη και η άμεση επιδιόρθωση των γραμμών. Στις μέρες μας, η αυξανόμενη χρήση του διαδικτύου για την μείωση του κόστους επικοινωνίας δημιούργησε άλλες ανάγκες όπως, η διασφάλιση της χωρητικότητας και η προστασία των δεδομένων.

Για να ανταποκριθούν πολλοί οργανισμοί σε αυτές τις ανάγκες, δημιούργησαν τα δικά τους κέντρα διαχείρισης ασφάλειας στα οποία απασχολούνται εξειδικευμένα άτομα με ειδικές γνώσεις ασφάλειας. Παράλληλα, το ίδιο έπραξαν και πολλές εταιρείες παροχής υπηρεσιών ασφάλειας για να μπορέσουν να προσφέρουν υπηρεσίες ασφάλειας σε πελάτες τους, όπως η διαχείριση των τειχών προστασίας, η προστασία από κακόβουλο λογισμικό, ο εντοπισμός και η πρόληψη εισβολών κ.ά. Οι διαμορφώσεις παραμετροποίησης των συστημάτων ασφάλειας ποικίλλουν ανάλογα με τα κόστη και τις απαιτήσεις των οργανισμών που υποστηρίζουν. Συνήθως, οι υπηρεσίες ασφάλειας ανατίθενται εξ' ολοκλήρου στους εξωτερικούς παρόχους. Σε άλλες περιπτώσεις, οι οργανισμοί μοιράζονται τις υπηρεσίες ασφάλειας με τους εξωτερικούς παρόχους έχοντας από κοινού πρόσβαση στα συστήματα ασφάλειας. Ορισμένοι οργανισμοί επιλέγουν να έχουν οι ίδιοι τον έλεγχο στις εργάσιμες ώρες και να αναλαμβάνουν οι εξωτερικοί πάροχοι τη νύχτα, τα σαββατοκύριακα και τις αργίες. Με αυτόν τον τρόπο

διατηρείται ένα καλό επίπεδο εσωτερικής τεχνογνωσίας στους οργανισμούς μειώνοντας τον βαθμό εξάρτησης από τους εξωτερικούς παρόχους.

Στις μέρες μας, υπάρχει η τάση για σύνδεση των κέντρων διαχείρισης δικτύου με τα κέντρα διαχείρισης ασφάλειας. Αυτό συμβαίνει γιατί τα εργαλεία ασφάλειας όλο και περισσότερο χρειάζεται να επικοινωνήσουν με τα λογισμικά διαχείρισης δικτύων. Επίσης, οι μηχανικοί δικτύων εξοικειώνονται περισσότερο με τη διαχείριση και τη χρήση εργαλείων παρακολούθησης, ανάλυσης και αναφορών ασφάλειας. Πολλές συσκευές ασφάλειας υλοποιούνται και ελέγχονται από το προσωπικό του τμήματος τηλεπικοινωνιών. Συχνά, οι διαχειριστές δικτύου είναι αυτοί που εντοπίζουν πρώτοι τα περιστατικά ασφάλειας και καλούν την εξειδικευμένη ομάδα ασφάλειας για βοήθεια.

Οι ομάδες ασφάλειας, είναι υπεύθυνες κυρίως για την παρακολούθηση και τη διαχείριση των εσωτερικών και εξωτερικών συμβάντων ασφάλειας και για τον προσδιορισμό των πιθανών επιπτώσεων στον οργανισμό από επιθέσεις σε τρωτά σημεία. Οι περισσότεροι εξωτερικοί πάροχοι όπως οι οργανισμοί, ακολουθούν τον ίδιο τρόπο οργάνωσης αντιμετωπίζοντας την ασφάλεια και τα δίκτυα με διαφορετικές ομάδες. Με την συγχώνευση των λειτουργικών πτυχών της ασφάλειας στο περιβάλλον του δικτύου και των συστημάτων, η σχέση μεταξύ ασφάλειας και δικτύων καθίσταται ολοένα και περισσότερο ασαφής. Οι κύριοι παράγοντες για την εξωτερική ανάθεση της ασφάλειας του δικτύου είναι η έλλειψη τεχνογνωσίας και το χαμηλότερο κόστος για 24ωρη εβδομαδιαία κάλυψη (Harold & Krause, 2008).

7.6 Κρυπτογραφία

Όταν άρχισε να αναπτύσσεται η κρυπτογραφία, θεωρήθηκε ως προϊόν το οποίο θα έπρεπε να αγοραστεί και να εφαρμοστεί μόνο σε συγκεκριμένες περιπτώσεις. Αυτό άρχισε να αλλάζει με την υλοποίηση υποδομών δημόσιου κλειδιού (Public Key Infrastructure - PKI) από τους οργανισμούς, με την ευρεία χρήση του διαδικτύου για την μεταφορά ευαίσθητων δεδομένων και, με την απαίτηση των οργανισμών για προστασία των αποθηκευμένων δεδομένων. Πολλές εταιρείες άρχισαν να προσφέρουν υπηρεσίες διαχείρισης υποδομών δημόσιου κλειδιού και λογισμικά κρυπτογράφησης δεδομένων και επικοινωνιών. Ωστόσο, η εξωτερική ανάθεση των υπηρεσιών που σχετίζονται με την κρυπτογραφία δεν κέντρισε το ενδιαφέρον των οργανισμών κυρίως, λόγω της απαίτησης υψηλού επιπέδου εμπιστοσύνης με τους εξωτερικούς παρόχους. (Harold & Krause, 2008).

7.7 Επαναφορά από καταστροφές και επιχειρησιακή συνέχεια

Καταστροφές συμβαίνουν και θα συνεχίσουν να συμβαίνουν στους οργανισμούς παρά τις προσπάθειες που καταβάλλουν για να τις αποφύγουν. Αυτές οι καταστροφές

συνήθως έχουν επιπτώσεις και στην ασφάλεια. Για την αντιμετώπισή τους, οι οργανισμοί θα πρέπει να διαθέτουν προγράμματα επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές τα οποία συλλογικά ονομάζονται και, σχέδια έκτακτης ανάγκης. Η ανάκαμψη από καταστροφές αφορά στην αντίδραση του οργανισμού ως προς την απώλεια σημαντικών επιχειρησιακών λειτουργιών ενώ, η επιχειρησιακή συνέχεια σχετίζεται με τη διατήρηση των επιχειρηματικών λειτουργιών στην περίπτωση που οι πρωτεύουσες τοποθεσίες ή λειτουργίες, διαταράσσονται ή καθίστανται μη λειτουργικές (Harold & Krause, 2008) (Butler, 2000).

Ανάλυση επιχειρησιακών επιπτώσεων

Τα σχέδια επιχειρησιακής συνέχειας και αποκατάστασης καταστροφών θα πρέπει να βασίζονται σε αναλύσεις κινδύνου που συγκρίνουν τις πιθανές απώλειες που προκύπτουν από ένα περιστατικό, όπως πυρκαγιά ή πλημμύρα, με το κόστος παροχής εφεδρικών εγκαταστάσεων. Μια τέτοια ανάλυση επιχειρησιακών επιπτώσεων μπορεί να ανατεθεί σε εξειδικευμένους εξωτερικούς συνεργάτες ή να πραγματοποιηθεί από το προσωπικό του οργανισμού χρησιμοποιώντας εργαλεία που διατίθενται στην αγορά.

Σχεδίαση

Η δημιουργία ενός σχεδίου επιχειρησιακής συνέχειας και αποκατάστασης καταστροφών μπορεί να πραγματοποιηθεί εσωτερικά στον οργανισμό, αλλά συνήθως είναι πολύ πιο εύκολο και πιο οικονομικό να ανατεθεί σε εξωτερικό συνεργάτη. Η συντήρηση του σχεδίου, αποτελεί τον πιο σημαντικό παράγοντα διότι, συχνά τέτοια σχέδια παραμελούνται ή δεν ενημερώνονται ανά τακτά χρονικά διαστήματα. Η ανάθεση αυτής της εργασίας σε εξωτερικούς παρόχους διασφαλίζει την επικαιροποίηση και αυξάνει τον βαθμό αξιοπιστίας των συγκεκριμένων σχεδίων.

Υλοποίηση και δοκιμή

Οι οργανισμοί οφείλουν να δοκιμάζουν το κάθε σχέδιο περιοδικά για να διασφαλίζουν ότι θα λειτουργήσει σωστά όταν υπάρχει ανάγκη. Οι δοκιμές και οι επακόλουθες αναθεωρήσεις διατηρούν τα σχέδια βιώσιμα. Η περιοδική επανεξέταση των σχεδίων είναι απαραίτητη για να διασφαλιστεί η προσαρμογή τους στις αλλαγές του περιβάλλοντος των οργανισμών. Οι εξωτερικοί πάροχοι, μπορούν επίσης να βοηθήσουν τους οργανισμούς στη διαδικασία των δοκιμών, ειδικά όταν οι δοκιμές ξεπερνούν τα όρια του οργανισμού και εμπλέκουν επιχειρηματικούς εταίρους, προμηθευτές και άλλους. Η δημιουργία εφεδρικών εγκαταστάσεων, είναι εξαιρετικά δαπανηρή για τους οργανισμούς σε αντίθεση με τους εξωτερικούς παρόχους οι οποίοι μπορούν να τις προσφέρουν σε πολύ χαμηλότερο κόστος. Το υψηλό κόστος κατασκευής και συντήρησης των εφεδρικών

εγκαταστάσεων, συστημάτων και δικτύων, μοιράζεται σε πολλούς πελάτες και με αυτόν τον τρόπο οι εξωτερικοί πάροχοι με την ίδια υποδομή, μπορούν να υποστηρίξουν μεγάλο αριθμό πελατών. Οι εξωτερικοί πάροχοι, στη δημιουργία εφεδρικών αντιγράφων ασφάλειας και στις λειτουργίες αποκατάστασης καταστροφών και επιχειρησιακής συνέχειας, θα πρέπει να διασφαλίζουν και το απόρρητο των πληροφοριών. Η καθιέρωση μιας τέτοιας σχέσης εμπιστοσύνης με τον εξωτερικό πάροχο δεν είναι εύκολη υπόθεση. Οι οργανισμοί θα πρέπει να αξιολογούν τον εξωτερικό πάροχο και να κατανοούν πλήρως τις πολιτικές ασφάλειας, τις διαδικασίες και τους μηχανισμούς ασφάλειας που διαθέτει.

7.8 Νόμοι, έρευνες και ηθική

Από όλους τους τομείς που προαναφέραμε, αυτός που απαιτεί την περισσότερη εμπειρογνωμοσύνη, είναι η νομική κάλυψη σε περίπτωση περιστατικού ασφάλειας που σχετίζεται με τον εξωτερικό πάροχο. Οι οργανισμοί θα πρέπει να ζητούν νομικές συμβουλές κατά την έναρξη συνεργασίας με τους εξωτερικούς παρόχους, κυρίως στην φάση της διαπραγμάτευσης της αρχικής σύμβασης συνεργασίας. Αν διαθέτουν εσωτερικό νομικό σύμβουλο, τότε αυτός ίσως να μπορεί να χειριστεί αυτά τα ζητήματα σε νομικό επίπεδο. Διαφορετικά, ο οργανισμός θα πρέπει να απευθυνθεί σε εξειδικευμένο εξωτερικό νομικό σύμβουλο. Εφόσον συμβεί κάποιο περιστατικό ασφάλειας στις υπηρεσίες που έχουν ανατεθεί στον εξωτερικό πάροχο, τότε ο οργανισμός οφείλει να πραγματοποιήσει έρευνα συλλέγοντας όλα τα απαραίτητα αποδεικτικά στοιχεία. Και σε αυτήν την περίπτωση, είναι προτιμότερο να απευθυνθεί σε εξειδικευμένους εξωτερικούς νομικούς συμβούλους διότι, ο βαθμός δυσκολίας μιας τέτοιας έρευνας είναι πολύ μεγάλος, ιδιαίτερα όταν ο εξωτερικός πάροχος υπάγεται στη δικαιοδοσία άλλης χώρας (Sparrow, 2003).

7.9 Εφαρμογές και υλοποίηση συστημάτων

Οι οργανισμοί συχνά αναθέτουν σε εξωτερικούς παρόχους την ανάπτυξη, τον έλεγχο και την συντήρηση των εφαρμογών και συστημάτων τους. Με την εξωτερική ανάθεση, αποκτούν τεχνογνωσία την οποία δε διαθέτουν και προκειμένου να μειώσουν το κόστος, επιλέγουν εταιρείες οι οποίες δραστηριοποιούνται σε χώρες οι οποίες προσφέρουν φθηνό εργατικό προσωπικό με ισχυρές τεχνικές γνώσεις. Κατά την εξωτερική ανάθεση ανάπτυξης εφαρμογών μπορεί να προκύψουν διάφορα προβλήματα τα οποία σχετίζονται με την ασφάλεια πληροφοριών. Η υποκλοπή πηγαίου κώδικα, η ενσωμάτωση κακόβουλου λογισμικού και η κλοπή πνευματικής ιδιοκτησίας είναι οι πιο σημαντικοί κίνδυνοι που καλούνται να αντιμετωπίσουν οι οργανισμοί. Όσο οι εξωτερικοί πάροχοι αυξάνουν το επίπεδο τεχνογνωσίας του προσωπικού τους, τόσο περισσότερο εμπλέκονται στις κρίσιμες εφαρμογές και στα συστήματα των οργανισμών που υποστηρίζουν. Κατά συνέπεια, οι λεπτομερείς γνώσεις που αποκτούν για τα συστήματα

και τις εφαρμογές των οργανισμών, αυξάνει δραματικά τον βαθμό εξάρτησης των οργανισμών και αλλάζει την ισορροπία εξουσίας μεταξύ τους προς όφελος των εξωτερικών παρόχων (Harold & Krause, 2008).

7.10 Ασφάλεια λειτουργιών

Κάθε υπηρεσία που ανατίθεται σε εξωτερικούς παρόχους περιλαμβάνει συστήματα και λογισμικά διαχείρισης όπως συσκευές για την παρακολούθηση της ασφάλειας, εφαρμογές δημιουργίας αναφορών, εφαρμογές εισαγωγής δεδομένων, εφαρμογές επεξεργασίας δεδομένων κ.ά. Κάθε φορά που υπάρχει ανθρώπινη συμμετοχή σε μια λειτουργία, υπάρχει και κίνδυνος. Η συμμετοχή του ανθρώπου αυξάνει τα σφάλματα, δημιουργεί μεγάλες διακυμάνσεις στην ποιότητα και επηρεάζει αρνητικά τον χρόνο ολοκλήρωσης των λειτουργιών. Επίσης, μπορεί να οδηγήσει σε σημαντικά προβλήματα ασφάλειας όπως είναι η απάτη, η κλοπή, η καταστροφή, η κακή χρήση, η παραποίηση, η μή εξουσιοδοτημένη πρόσβαση και η μή εξουσιοδοτημένη γνωστοποίηση. Στις εξωτερικές αναθέσεις, οι οργανισμοί συνήθως αδυνατούν να ελέγξουν τις ενέργειες του προσωπικού των εξωτερικών παρόχων. Το πρόβλημα αυτό είναι ακόμη μεγαλύτερο, όταν οι εργαζόμενοι των εξωτερικών παρόχων, βρίσκονται χιλιάδες χιλιόμετρα μακριά, έχουν διαφορετικές αξίες, νόμους και κουλτούρα. Οι οργανισμοί για να μετριάσουν αυτόν τον κίνδυνο, θα πρέπει να εκπαιδεύουν το προσωπικό τους και να ελέγχουν τους εξωτερικούς παρόχους εφαρμόζοντας κατάλληλους μηχανισμούς εποπτείας ασφάλειας λειτουργιών. Επίσης, θα πρέπει να γνωρίζουν τις πολιτικές και τις διαδικασίες ασφάλειας που εφαρμόζουν οι εξωτερικοί πάροχοι αλλά και να εξασφαλίζουν την τήρηση των απαιτούμενων προτύπων και μέτρων ασφάλειας (Harold & Krause, 2008).

8. Προτεινομένη Μεθοδολογία Προσέγγισης Εξωτερικών Αναθέσεων

Στα προηγούμενα κεφάλαια περιγράψαμε εκτενώς όλα τα θέματα που αφορούν στις εξωτερικές αναθέσεις όπως η χρησιμότητα, τα κόστη, τα οφέλη, οι κίνδυνοι, οι απειλές της ασφάλειας πληροφοριών, τα κριτήρια επιλογής και οι λειτουργίες ασφάλειας των εξωτερικών παρόχων. Στο κεφάλαιο αυτό, θα συγκεντρώσουμε όλα τα παραπάνω σε ένα κοινό πλαίσιο και θα προτείνουμε μια συνολική διαδικασία που περιλαμβάνει δεκαοχτώ στάδια, η οποία προτείνεται να ακολουθείται από τους οργανισμούς, από την έναρξη μέχρι την ολοκλήρωση και τη λειτουργία μιας ασφαλούς εξωτερικής ανάθεσης.

1.Εκκίνηση της διαδικασίας αξιολόγησης εξωτερικής ανάθεσης: Η έναρξη μιας νέας επιχείρησης ή μιας καινούργιας επιχειρηματικής δραστηριότητας μπορεί να οδηγήσει στην ανάγκη να εξεταστεί εκ των προτέρων η εξωτερική ανάθεση. Σε άλλες περιπτώσεις, η είδηση ότι μια μεγάλη επιχείρηση έχει αναθέσει σε τρίτους μια σημαντική λειτουργία, μπορεί να οδηγήσει τα στελέχη και άλλων εταιρειών στον ίδιο δρόμο.

2.Έλεγχος σκοπιμότητας: Οι οργανισμοί θα πρέπει να προσδιορίζουν την πραγματική επιχειρησιακή ή επιχειρηματική ανάγκη πριν αποφασίσουν να επιλέξουν την εξωτερική ανάθεση. Η απόφαση αυτή, θα πρέπει να δικαιολογείται μέσω ενός συγκεκριμένου επιχειρηματικού σχεδίου.

3.Έρευνα βαθμού ανάθεσης: Στο στάδιο αυτό, οι οργανισμοί θα πρέπει να εκτελέσουν έρευνα, για να προσδιορίσουν τον βαθμό στον οποίο ανατίθενται σε εξωτερικούς παρόχους από άλλους οργανισμούς, οι υπηρεσίες ή λειτουργίες που τους ενδιαφέρουν να αναθέσουν σε εξωτερικό πάροχο. Για να αντλήσουν πληροφορίες μπορούν να χρησιμοποιήσουν διάφορες πηγές όπως το διαδίκτυο, τα συνέδρια, τα ερευνητικά έγγραφα κ.ά. Επίσης, μπορούν να απευθυνθούν σε εξωτερικούς συνεργάτες και προμηθευτές που έχουν υλοποιήσει αντίστοιχα έργα εξωτερικής ανάθεσης.

4.Εφικτότητα εξωτερικής ανάθεσης: Σε αυτό το στάδιο, ο οργανισμός θα πρέπει προσδιορίσει βασιζόμενος στα στοιχεία της έρευνας, κατά πόσο η εξωτερική ανάθεση είναι εφικτή ως εναλλακτική λύση. Εφόσον αναδειχθεί η σκοπιμότητα και το ενδεχόμενο όφελος της εξωτερικής ανάθεσης, μπορεί να προχωρήσει στα επόμενα στάδια.

5.Προσδιορισμός πεδίου εφαρμογής και απαιτήσεων: Εφόσον το επιχειρηματικό σχέδιο εγκριθεί και κριθεί ως εφικτή η εξωτερική ανάθεση, θα πρέπει να οριστούν με λεπτομέρεια οι απαιτήσεις της λειτουργίας και της ασφάλειας του οργανισμού στα πλαίσια της εξωτερικής ανάθεσης. Με βάση αυτές τις απαιτήσεις, ο οργανισμός θα πρέπει στη συνέχεια να καθορίσει τα κύρια κριτήρια επιλογής εξωτερικού παρόχου.

6.Δημιουργία και αποστολή RFI στους εξωτερικούς παρόχους: Η καλή έρευνα μπορεί να παράσχει ουσιαστικές πληροφορίες στους οργανισμούς, ιδίως ως προς το ποιοί είναι οι κύριοι υποψήφιοι εξωτερικοί πάροχοι για την ανάθεση του έργου. Για την άντληση λεπτομερών πληροφοριών που αφορούν την προς εξωτερική ανάθεση λειτουργία, οι οργανισμοί θα πρέπει να δημιουργήσουν και να στείλουν στους εξωτερικούς παρόχους RFI. Στο RFI, εκτός από τα ερωτήματα που αφορούν τη λειτουργία της εξωτερικής ανάθεσης, θα πρέπει να περιλαμβάνονται και πληροφορίες που σχετίζονται με το επίπεδο ασφάλειας των παρεχόμενων υπηρεσιών ή λειτουργιών.

7.Συλλογή πληροφοριών και διενέργεια προκαταρκτικής ανάλυσης: Τα αποτελέσματα από την ανάλυση των δεδομένων που λαμβάνονται από το RFI πιθανόν να υποστηρίξουν ή να αντικρούσουν την αρχική ιδέα εξέτασης εξωτερικής ανάθεσης. Είναι προτιμότερο οι οργανισμοί να εγκαταλείψουν την ιδέα της εξωτερικής ανάθεσης σε αυτό το σημείο, όπου ο χρόνος και η προσπάθεια που καταβλήθηκε είναι σχετικά μικρή, παρά να επενδύσουν περαιτέρω πόρους στην αξιολόγηση. Αν η προσέγγιση της εξωτερικής ανάθεσης κρίνεται εφικτή και αποδοτική ως προς το κόστος, οι οργανισμοί μπορούν να προχωρήσουν στο επόμενο βήμα του RFP.

8.Προετοιμασία και αποστολή RFP: Σε αυτήν την φάση οι οργανισμοί θα πρέπει να ετοιμάσουν το RFP και να το στείλουν στους εξωτερικούς παρόχους. Το RFP θα πρέπει να περιλαμβάνει τις προϋποθέσεις, τους όρους, τα χαρακτηριστικά και τις απαιτήσεις λειτουργίας και ασφάλειας της εξωτερικής ανάθεσης. Επίσης, είναι σημαντικό να ορίζεται σε αυτό και η καταληκτική ημερομηνία και ώρα παραλαβής τον προτάσεων από τους εξωτερικούς παρόχους.

9.Λήψη προσφορών: Δεδομένου ότι η διαδικασία λήψης προτάσεων μπορεί να αντιμετωπίσει διάφορα προβλήματα, πρέπει να διενεργηθεί με επίσημο τρόπο. Η ημερομηνία και η ώρα παραλαβής των προτάσεων, είτε σε εκτυπώσιμη μορφή, είτε σε άλλα μέσα ή σε ηλεκτρονική μορφή, θα πρέπει να καταγράφονται προσεκτικά, ιδίως για τις προτάσεις που υποβάλλονται σε χρονικές στιγμές κοντά στην προτεινόμενη προθεσμία. Εφόσον ληφθούν οι προσφορές από τους υποψήφιους εξωτερικούς παρόχους, ο οργανισμός μπορεί να προχωρήσει στην επόμενη φάση της ανάλυσης και αξιολόγησης.

10.Προκαταρκτική αξιολόγηση προτάσεων: Μια αρχική αξιολόγηση των προτάσεων η οποία βασίζεται στον έλεγχο των βασικών κριτηρίων επιλογής, μπορεί να αποκλείσει εύκολα ένα μεγάλο σύνολο υποψήφιων εξωτερικών παρόχων. Στις περιπτώσεις που κάποιος υποψήφιος δεν έχει ακολουθήσει τις οδηγίες μορφοποίησης, περιεχομένου ή έχει παραλείψει να συμπεριλάβει βοηθητικά έγγραφα, ο οργανισμός θα πρέπει να τον

ενημερώσει ώστε να προβεί στις κατάλληλες διορθώσεις ή προσθήκες εντός συγκεκριμένου χρονικού πλαισίου. Υπάρχει επίσης το ενδεχόμενο, ένας από τους εξωτερικούς παρόχους να θέσει ένα σημαντικό θέμα που δεν συμπεριλαμβάνεται στο RFP και να κριθεί απαραίτητο να ζητηθούν πρόσθετες πληροφορίες από όλους τους υποψηφίους. Όλα τα παραπάνω ζητήματα, θα πρέπει να αντιμετωπιστούν με σωστή διαχείριση από τους οργανισμούς ώστε να εξελιχθεί ομαλά η όλη διαδικασία προς όφελός τους.

11.Επιλογή των κύριων υποψηφίων εξωτερικών παρόχων: Οι οργανισμοί μετά την προκαταρκτική αξιολόγηση των προτάσεων συνήθως καταλήγουν σε τρεις ή τέσσερις κύριους υποψήφιους εξωτερικούς παρόχους. Οι υποψήφιοι που έχουν αποκλειστεί από το έργο εξωτερικής ανάθεσης, απαιτείται να ενημερωθούν επίσημα από τον οργανισμό. Κατά την ενημέρωσή τους, ο οργανισμός θα πρέπει να τους ευχαριστήσει για την προσπάθεια και την συμμετοχή τους και να τους βεβαιώσει ότι θα τους λάβει υπόψιν σε μελλοντικά έργα. Με αυτήν τη διαβεβαίωση, ο οργανισμός έχει τη δυνατότητα να απευθυνθεί ξανά σε αυτούς, ακόμη και για το ίδιο έργο, σε περίπτωση που αποκλειστούν οι κύριοι υποψήφιοι στο επόμενο στάδιο της διαδικασίας αξιολόγησης.

12.Λεπτομερή ανάλυση των προτάσεων: Σε αυτό το στάδιο, οι οργανισμοί θα πρέπει να αξιολογήσουν τις προτάσεις βασιζόμενοι σε συγκεκριμένα κριτήρια και να διενεργήσουν πιστωτικούς ελέγχους και οικονομικές αναλύσεις. Στην συνέχεια, θα πρέπει να καλέσουν τους υποψήφιους για να παρουσιάσουν τις προτάσεις τους και να απαντήσουν στα ερωτήματα που πιθανών να έχουν προκύψει. Στην περίπτωση ανάθεσης κρίσιμων λειτουργιών, θα ήταν ωφέλιμο για τους οργανισμούς, να επισκεφθούν τις εγκαταστάσεις των εξωτερικών παρόχων για να παρακολουθήσουν τον τρόπο με τον οποίο υποστηρίζουν άλλους πελάτες σε αντίστοιχα έργα εξωτερικής ανάθεσης.

13.Τελική επιλογή εξωτερικού παρόχου: Εφόσον ολοκληρωθεί η λεπτομερή ανάλυση των προτάσεων, επιλέγεται ο τελικός εξωτερικός πάροχος που θα αναλάβει την εξωτερική ανάθεση. Ο οργανισμός σε αυτό το στάδιο, οφείλει να ενημερώσει τους υπόλοιπους υποψήφιους που δεν έχουν επιλεγεί. Αυτό μπορεί να πραγματοποιηθεί μέσω μιας προσωπικής κλήσης και στην συνέχεια με την αποστολή μιας επίσημης ευχαριστήριας επιστολής.

14.Δημιουργία σύμβασης παροχής υπηρεσιών: Μέχρι την τελική επιλογή, θα πρέπει να έχουν οριστεί πολλοί από τους όρους και τις προϋποθέσεις της σύμβασης παροχής υπηρεσιών. Ωστόσο, μέχρι να πραγματοποιηθεί η τελική επιλογή, δεν μπορεί κανείς να ξεκινήσει επίσημα σοβαρή διαπραγμάτευση της σύμβασης και ιδιαίτερα του SLA. Στο στάδιο αυτό, ο οργανισμός σε συνεργασία με τον εξωτερικό πάροχο θα πρέπει να

καταλήξουν από κοινού, στους όρους και στις προϋποθέσεις της σύμβασης παροχής υπηρεσιών και του SLA. Στο SLA, εκτός από τις απαιτήσεις που αφορούν τη λειτουργία της εξωτερικής ανάθεσης, θα πρέπει να ορίζονται σαφώς και οι απαιτήσεις του οργανισμού ως προς την ασφάλεια.

15.Συμφωνία έναρξης έργου εξωτερικής ανάθεσης: Εφόσον ολοκληρωθούν όλα τα παραπάνω στάδια με τον προτιμώμενο εξωτερικό πάροχο, η υλοποίηση του έργου μπορεί να αρχίσει με την σύναψη συμφωνίας έναρξης έργου.

16.Μετάβαση στον εξωτερικό πάροχο: Η μετάβαση στον εξωτερικό πάροχο θα πρέπει να σχεδιαστεί και να εκτελεστεί προσεκτικά για να διασφαλιστεί ότι το έργο θα προχωρήσει ομαλά και θα ανταποκρίνεται στις προσδοκίες όλων. Ο οργανισμός και ο εξωτερικός πάροχος θα πρέπει να περιφρουρήσουν την όλη διαδικασία επιλύοντας άμεσα οποιοδήποτε πρόβλημα εμφανιστεί.

17.Συνεργασία με τον εξωτερικό πάροχο: Μόλις ολοκληρωθεί το στάδιο της μετάπτωσης, ο οργανισμός θα πρέπει να είναι σε θέση να ελέγξει τον εξωτερικό πάροχο και να συνεργαστεί μαζί του αποδοτικά. Αυτό επιτυγχάνεται με την συνεχή παρακολούθηση της τήρησης των όρων του SLA, με την τακτική επαφή μέσω συναντήσεων και με την υλοποίηση συγκεκριμένης «ατζέντας» θεμάτων προς επίλυση ανά τακτά χρονικά διαστήματα. Επίσης, είναι πολύ σημαντικό να αναφέρονται τυχόν ουσιώδεις αλλαγές στην κατάσταση των δύο μερών, όπως είναι η απώλεια βασικού προσωπικού, συγχωνεύσεις, εξαγορές κ.ά.

18.Ανανέωση και τερματισμός σύμβασης παροχής υπηρεσιών: Σε κανονικές συνθήκες, η σύμβαση παροχής υπηρεσιών που συνάπτει ο οργανισμός με τον εξωτερικό πάροχο έχει διάρκεια από ένα έως τρία έτη. Συχνά, αυτή η σύμβαση ανανεώνεται αυτόματα για μια καθορισμένη περίοδο, εκτός εάν ένα από τα δύο μέρη διαφωνεί. Σε περίπτωση αδυναμίας ανταπόκρισης του εξωτερικού παρόχου στις ανάγκες του οργανισμού, είναι προτιμότερη η πρώιμη καταγγελία της σύμβασης και η καταβολή χρηματικής ποινής.

Η αξιολόγηση των ευκαιριών εξωτερικής ανάθεσης υπηρεσιών έχει καταστεί ως μια συνεχής διαδικασία διότι προσφέρονται συνεχώς νέες υπηρεσίες και τεχνολογίες. Ενώ οι παράμετροι και οι συνθήκες αλλάζουν, η διαδικασία που προαναφέραμε παραμένει η ίδια. Οι οργανισμοί θα πρέπει να είναι ευέλικτοι και σε θέση να μπορούν να αξιολογούν με σωστό τρόπο τις επιλογές που τους παρέχονται, ώστε να επιβιώσουν σε μια τόσο ανταγωνιστική παγκόσμια αγορά.

Επίλογος - Συμπεράσματα

Ο όρος εξωτερική ανάθεση χρησιμοποιείται όλο και περισσότερο στους οργανισμούς και, η έννοια χρήσης εξωτερικού παρόχου για κρίσιμες λειτουργίες και τεχνολογίες πληροφορίας είναι πλέον συνήθης. Η εξωτερική ανάθεση υπηρεσιών έφερε σημαντικά κέρδη σε πολλούς οργανισμούς. Η δυνατότητα της ανάθεσης σημαντικών δραστηριοτήτων σε τρίτους, τους επέτρεψε να αναπτυχθούν και να επιβιώσουν. Οι διοικήσεις των οργανισμών, έχουν αρχίσει να ζητούν από τα στελέχη τους να αξιολογήσουν και την εξωτερική ανάθεση ως επιλογή κατά την υλοποίηση νέων ή την αναδιάρθρωση υφιστάμενων υπηρεσιών. Συχνά, η προθυμία για εξωτερική ανάθεση εκφράζεται σε υψηλό εκτελεστικό επίπεδο. Όλο και περισσότερες επιχειρήσεις σήμερα επιλέγουν να αναθέσουν σε τρίτους, σημαντικές εσωτερικές λειτουργίες όπως την διαχείριση του δικτύου, των υπολογιστών, του λογισμικού αλλά και των συστημάτων ασφάλειας. Αναζητούν εξωτερικούς συνεργάτες που διαθέτουν την τεχνογνωσία με σκοπό να μεταφέρουν την ευθύνη εκτός του οργανισμού, να μειώσουν τα λειτουργικά έξοδα και παράλληλα να αυξήσουν την παραγωγικότητα.

Πριν εξεταστεί οποιοδήποτε σενάριο εξωτερικής ανάθεσης θα πρέπει να έχουν συγκεντρωθεί και καταγραφεί οι κύριοι λόγοι για τους οποίους κρίνεται η εξωτερική ανάθεση ως η καλύτερη επιλογή. Η εξωτερική ανάθεση είναι μια επιλογή που πρέπει να βασίζεται σε τεκμηριωμένη ανάλυση. Ο οργανισμός που προτίθεται να προβεί σε χρήση εξωτερικών υπηρεσιών, πρέπει να απαντήσει σε σημαντικά ερωτήματα που αφορούν στην επιλογή παρόχου και να ακολουθήσει συγκεκριμένη διαδικασία από την έναρξη μέχρι την ολοκλήρωση και τη λειτουργία μιας εξωτερικής ανάθεσης. Κύριος στόχος του θα πρέπει να είναι η επιλογή ασφαλών, αποτελεσματικών, λιγότερο δαπανηρών και εύκολων στην χρήση υπηρεσιών.

Η εξωτερική ανάθεση έχει ρίσκο αναφορικά με τη διαρροή πληροφοριών, τη βιωσιμότητα και την φήμη ενός οργανισμού. Η ασφάλεια, αποτελεί κρίσιμη παράμετρο σε κάθε εξωτερική ανάθεση υπηρεσιών. Η προστασία των εμπιστευτικών πληροφοριών που ανήκουν σε οργανισμούς ή σε ιδιώτες, είναι ένα ζήτημα κρίσιμης σημασίας για τους οργανισμούς και ένα από τα δυσκολότερα ζητήματα στις εξωτερικές αναθέσεις. Το γεγονός ότι επιχειρησιακές διαδικασίες δίνονται σε εξωτερικούς παρόχους, εγείρει πολλές ερωτήσεις σχετικά με το επίπεδο ασφάλειας και την ακεραιότητα των εξωτερικών παρόχων. Το κύριο ερώτημα είναι, πόσο ασφαλής μπορεί είναι μια εξωτερική ανάθεση για τον οργανισμό. Η διασφάλιση της ασφάλειας, αποτελεί τον μεγαλύτερο από όλους τους κινδύνους δεδομένου του υψηλού βαθμού εμπιστοσύνης προς τους εξωτερικούς παρόχους, οι οποίοι είναι υπεύθυνοι για τη διαχείριση των υπηρεσιών ασφάλειας. Με την εξωτερική ανάθεση ο οργανισμός εκθέτει αυτομάτως τις λειτουργίες του, τα δίκτυα

και τα συστήματά του σε ένα νέο σύνολο κινδύνων. Η εξάρτηση του οργανισμού από το επίπεδο ασφάλειας του εξωτερικού παρόχου είναι εξαιρετικά υψηλή και, η ανάγκη για ασφάλεια και αξιοπιστία είναι μεγάλη. Στην περίπτωση που συμβεί κάποιο περιστατικό ασφάλειας και διαπιστωθεί ότι δεν τηρούνταν οι απαιτούμενες δικλείδες ασφάλειας από τον εξωτερικό πάροχο, υπεύθυνος είναι ο ίδιος ο οργανισμός. Οι κανονισμοί και οι νόμοι, έχουν ισχύ για τους οργανισμούς ανεξάρτητα από το αν επεξεργάζονται εσωτερικά ή σε εξωτερικό πάροχο τα δεδομένα των πελατών τους.

Για να διασφαλιστεί η ασφάλεια των πληροφοριών και των δεδομένων του οργανισμού, ο εξωτερικός πάροχος υποχρεούται να αντιμετωπίσει σοβαρά και υπεύθυνα τους ενδεχόμενους κινδύνους γνωρίζοντας τον τρόπο αντιμετώπισής τους. Υπάρχουν πολλαπλά επίπεδα ασφάλειας από άποψη διαδικασιών και τεχνολογιών, που μπορούν να εφαρμοστούν σε έναν οργανισμό ή σε έναν εξωτερικό πάροχο ώστε να διασφαλιστούν οι επιχειρηματικές σχέσεις, τα δεδομένα και η πνευματική ιδιοκτησία. Όσο ισχυρότερη είναι η προστασία ασφάλειας, τόσο μικρότερη είναι η πιθανή επίπτωση μιας απειλής.

Οι οργανισμοί κατά την επιλογή του εξωτερικού παρόχου θα πρέπει να αξιολογούν και να κατανοούν πλήρως τις πολιτικές ασφάλειας, τις διαδικασίες και τους μηχανισμούς ασφάλειας που διαθέτουν οι ίδιοι αλλά και ο εξωτερικός πάροχος. Χρειάζεται να ελέγχουν ανά τακτά χρονικά διαστήματα αν η πολιτική, τα πρότυπα και οι διαδικασίες ασφάλειας πληροφοριών εφαρμόζονται από τους εξωτερικούς παρόχους. Θα πρέπει να λαμβάνουν υπόψη, τους πρόσθετους κινδύνους που μπορεί να προκύψουν λόγω της αυξημένης πολυπλοκότητας. Ακόμη, απαιτείται να καταβάλουν σημαντικές προσπάθειες για την αυτοματοποίηση των διαχειριστικών εργασιών έτσι ώστε να μειωθεί στο ελάχιστο η ανάγκη για ανθρώπινη παρέμβαση. Κάθε διαφωνία ή δυσαρέσκεια που σχετίζεται με το εσωτερικό προσωπικό του οργανισμού και εξωτερικό προσωπικό του παρόχου, θα πρέπει να παρακολουθείται στενά και να αντιμετωπίζεται έγκαιρα. Για να διατηρηθεί υψηλός ο βαθμός ασφάλειας, ο εξωτερικός πάροχος υπηρεσιών πρέπει να αναπτύξει, να υιοθετήσει, να ακολουθήσει και να επιβάλει πολιτικές και διαδικασίες, αλλά και να εφαρμόσει κατάλληλα προστατευτικά μέτρα. Επιπροσθέτως, θα πρέπει να διαθέτει συγκεκριμένα σχέδια απόκρισης στις περιπτώσεις τυχόν ασυνήθιστων δραστηριοτήτων ή εισβολών, προκειμένου να αποφευχθεί η κατάχρηση, να αποκατασταθεί οποιαδήποτε ζημία έχει γίνει και να μπορεί να διώξει ποινικά τους δράστες. Εξίσου σημαντικό είναι οι οργανισμοί και οι εξωτερικοί πάροχοι να λαμβάνουν τα απαιτούμενα μέτρα προστασίας σε περίπτωση παραβίασης της ασφάλειας εφόσον, έχουν αξιολογήσει το επίπεδο ελέγχου κινδύνων των πληροφοριών και της φύσης των επιχειρηματικών σχέσεων. Οι εξωτερικοί πάροχοι, θα πρέπει να διαθέτουν κατάλληλα πλάνα έκτακτης ανάγκης,

επιχειρηματικής συνέχειας και ανάκαμψης σε περιπτώσεις καταστροφών αλλά και να διαθέτουν τις απαραίτητες εγκαταστάσεις και δυνατότητες προκειμένου να αντιμετωπίσουν τέτοια γεγονότα. Η εξωτερική ανάθεση των επιχειρηματικών λειτουργιών και υπηρεσιών σε εξωτερικό πάροχο, χρειάζεται να συνοδεύεται από εσωτερική υποστήριξη για την αποφυγή ή μείωση των κινδύνων.

Για τον μετριασμό του ρίσκου βιωσιμότητας των εξωτερικών παρόχων, οι οργανισμοί θα οφείλουν να επιλέγουν πολλούς διαφορετικούς παρόχους και να σχεδιάζουν τα πληροφοριακά τους συστήματα με τέτοιον τρόπο, ώστε να μπορούν να μεταφερθούν εύκολα σε άλλες πλατφόρμες και τεχνολογίες. Κατά τη διαδικασία αξιολόγησης, θα πρέπει επίσης να ελέγχουν και την οικονομική βιωσιμότητα των εξωτερικών παρόχων. Η επιλογή των εξωτερικών συμβούλων στα πλαίσια της διαδικασίας αξιολόγησης χρειάζεται να διενεργείται με ιδιαίτερη προσοχή. Οι οργανισμοί θα πρέπει να είναι καλά προετοιμασμένοι και κατά τη διαδικασία μεταφοράς στον εξωτερικό πάροχο και επιπροσθέτως, θα πρέπει να αναλύσουν με βάση τις πιθανότητες κάθε πιθανή έκβαση, υπολογίζοντας παράλληλα το κόστος και τις απώλειες που μπορεί να προκύψουν. Για να διατηρήσει ο οργανισμός τη διαπραγματευτική του δύναμη, θα πρέπει να φροντίζει το προσωπικό του και να ενημερώνεται ανά τακτά χρονικά διαστήματα από τον εξωτερικό πάροχο, για τα τεχνικά θέματα και τις λειτουργίες των ανατεθέντων υπηρεσιών. Οποιαδήποτε διαπραγμάτευση σχετικά με το επίπεδο εξυπηρέτησης πρέπει να διασφαλίζει το καλύτερο δυνατό επίπεδο υποστήριξης για τον οργανισμό, μέσα από ισχυρές συμφωνίες παροχής υπηρεσιών. Για την ποιότητα των προσφερόμενων υπηρεσιών, οι οργανισμοί χρειάζεται να αξιολογούν συνεχώς τους εξωτερικού παρόχους ορίζοντας και εφαρμόζοντας εξ' αρχής συγκεκριμένα κριτήρια αξιολόγησης. Η γρήγορη ενσωμάτωση συστημάτων και λειτουργιών επίσης, αποτελούν καθοριστικό παράγοντα επιλογής ενός εξωτερικού παρόχου. Η δυνατότητα πληρωμής σε μηνιαία βάση, χωρίς μεγάλη αρχική δαπάνη κεφαλαίου, αποτελεί σημαντικό παράγοντα για τις εξωτερικές αναθέσεις, ιδιαίτερα για τους νεοσυσταθέντες οργανισμούς.

Εν κατακλείδι, οι οργανισμοί στα πλαίσια μιας εξωτερικής ανάθεσης υπηρεσιών, υποχρεούνται να δίνουνε ιδιαίτερη προσοχή στα ζητήματα που αφορούν στην ασφάλεια των πληροφοριών. Ακολουθώντας τη συγκεκριμένη μεθοδολογία (βλ. κεφ. 8) από τον έλεγχο σκοπιμότητας, την επιλογή κατάλληλου παρόχου ως και τη λειτουργία της ανάθεσης, διασφαλίζουν την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των πληροφοριακών περιουσιακών στοιχείων τους θωρακίζοντας με αυτόν τον τρόπο την λειτουργία της εξωτερικής ανάθεσης.

Βιβλιογραφία

(ISC)²: The World's Leading Cybersecurity Professional Organization. (2020). *(ISC)² CBK*. Ανάκτηση από https://www.isc2.org/Certifications/CBK#

Allen, J., Gabbard, D., May, C., Hayes, E., & Sledge, C. (2003). *Outsourcing managed security services.* CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Amant, K. S. (2009). *IT Outsourcing: Concepts, Methodologies, Tools, and Applications.* Business Science Reference.

Axelrod, C. W. (2004). *Outsourcing information security.* Artech house.

BPI BITS. (2020). *Technology policy division of the Bank Policy Institute.* Ανάκτηση από https://bpi.com/category/bits/

Buck-Lew, M. (1992). To Outsource or Not? *International Journal of Information Management, Vol 12*, 3–20.

Butler, J. (2000). *Winning the Outsourcing Game: making the best deals and making them work.* CRC Press.

Chorafas, D. N. (2003). *Outsourcing, Insourcing and IT for Enterprise Management.* Palgrave Macmillan.

Cross, J. (1995). IT outsourcing: British Petroleum's competitive approach. *Harvard Business Review*, 95–102.

Currie, W. (1996). Outsourcing in the private and public sectors:An unpredictable IT strategy. *European Journal of Information Systems, Vol 4*, 226–236.

De Looff, L. (1995). Information systems outsourcing decision making:A framework, organisational theories and case studies. *Journal of Information Technology, Vol 10*, 281–297.

Dhillon, G., Seyd, R., & Sa-Soares, F. (2017). Information security concerns in IT outsourcing. dentifying (in) congruence between clients and vendors. *Information & Management*, 452-464.

Earl, M. (1996). he risks of outsourcing IT. *SloanManagement Review*, 26–32.

Fink, D. (1994). A security framework for information systems outsourcing. *Information Management & Computer Security, Vol 2, No 2*, 3-8.

Gartner, Inc. (2020). *Gartner is the world's leading research and advisory company*. Ανάκτηση από https://www.gartner.com

Greenemeier, L. (2001). Companies reconsider offshoreoutsourcing. *InformationWeek, Vol 12*, 114–15.

Grover, V., Cheon, M., & Teng, J. (1994). An evaluation of the impact of corporate strategy and the role of information technology. *European Journal of Information Systems, Vol 3, No 3*, 179–190.

Halvey, J. K., & Melby, B. M. (2005). *Information Technology Outsourcing Transactions: Process, Strategies, and Contracts.* John Wiley & Sons, INC.

Halvey, J. K., & Melby, B. M. (2007). *Business Process Outsourcing. Process, Strategies, and Contracts.* John Wiley & Sons, Inc.

Harold, T. F., & Krause, M. (2008). *Information Security Management Handbook, Sixth Edition, Volume 2 6th.* Auerbach Publications.

ISO/IEC 17799:2005. (2020, April). *ISO/IEC 17799:2005 Information technology — Security techniques — Code of practice for information security management*. Ανάκτηση από ISO - International Organization for Standardization: https://www.iso.org/standard/39612.html

ISO/IEC 27001:2013. (2020, April). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Ανάκτηση από International Organization for Standardization: https://www.iso.org/standard/54534.html

Jack, G. (1992). Successful outsourcing depends on a successful contract. *Corporate Controller, Vol 4, No 5*, 17-20Corporate Controller, 4(5).

Jouini, M. R. (2014). Classification of security threats in information systems. *Procedia Computer Science, 32*, 489-496.

Karabulut, Y. K. (2007). Security and trust in it business outsourcing: a manifesto. *Electronic Notes in Theoretical Computer Science*, 179, 47-58.

Lacity, .., & Hirschheim, R. (1993). *Information Systems Outsourcing.* New York: John Wiley & Sons.

Lee, M. (1995). *IT Outsourcing Contracts:Practical Issues for Management.* Hong Kong: Information Systems Department, City University of Hong Kong.

Loh, L., & Venkatraman, N. (1992b). Diffusion of information technology outsourcing:Influence sources and kodak effect. *Information Systems Research, Vol. 3, No. 4*, 334–358.

Loh, L.; Venkatraman, N. (1992a). Determinants of information technology outsourcing: A cross-sectional analysis. *Management Information Systems, Vol 9, No 1*, 265–275.

McCarthy, L. (2002). *IT Security: Risking the Corporation.* Upper Saddle River,NJ: Prentice Hall.

O'Leary, M. (1990). The mainframe doesn't work here anymore. *CIO, Vol 6, No 6*, 77–79.

Peterson, B. B., & Maw, R. (2002). *Information security in outsourcing agreements*. Ανάκτηση από Mayer Brown: https://www.mayerbrown.com/en/perspectives-events/publications/2002/03/information-security-in-outsourcing-agreements

Power, M. (2006). *The outsourcing handbook: how to implement a successful outsourcing process.* Kogan Page Publishers.

Purser, S. (2004). *A Practical Guide to Managing Information Security.* Norwood,MA: Artech House.

Radack, S. (2009). The system development life cycle (sdlc) . *National Institute of Standards and Technology*.

Radcliff, D. (2000). Thinking ASP? Don’t forget security! *Computerworld, Vol 34, No 44*, 58.

Robinson, M., & Kalakota, R. (2004). *Offshore Outsourcing: Business Models, ROI and Best Practices.* Alpharetta, GA: Mivar Press, Inc.

Saunders, C., Gebelt, M., & Hu, Q. (1997). Achieving success in information systems outsourcing. *California Management Review, Vol 39, No 2*, 63–97.

Schniederjans, M. A. (2007). *Outsourcing Management Information Systems.* Idea Group Pub.

Sherwood, J. . (1997). Managing Security for Outsourcing Contracts. *Computers & Security, Vol 2*, 603–609.

Slaughter, S., & Ang, S. (1996). Employment Outsourcing in Information Systems. *Communications of the ACM, Vol 39, No 7*, 47–54.

Solli-Saether, H. (2010). *Managing It Outsourcing Performance .* Business Science Reference.

Solli-Saether, H., & Gottschalk, P. (2006). *Managing Successful It Outsourcing Relationships.* IRM Press.

Sparrow, E. (2003). *Successful IT Outsourcing: From Choosing a Provider to Managing the Project.* Springer.

Statista. (2020, April). *Global outsourcing market size 2000-2019*. Ανάκτηση από Statista: https://www.statista.com/statistics/189788/global-outsourcing-market-size/

Surja Datta, N. O.-M. (2015). *Understanding and Managing IT Outsourcing: A Partnership Approach.* Palgrave Macmillan.

T.D. Clark Jr. (1992). Corporate systems management: an overviewand research perspective. *Communications of the ACM, Vol 35, No 2*, 61–75.

Technavio. (2020). *Technavio*. Ανάκτηση από Market Research Reports - Industry Analysis Size & Trends - Technavio: https://www.technavio.com/

Tho, I. (2005). *Managing the risks of IT outsourcing .* Computer Weekly Professional.

Vijayan, J. (2001). Outsourcers rush to meet security demand. *Computerworld, Vol 35, No 9*, 34.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ

ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΤΗ ΔΙΟΙΚΗΣΗ

ΕΠΙΧΕΙΡΗΣΕΩΝ ΓΙΑ ΣΤΕΛΕΧΗ (Ε-ΜΒΑ)