Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Συστημάτων Πληροφόρησης

Σχολή Διοικητικών, Οικονομικών και Κοινωνικών Επιστημών

Department of Archival, Library and Information Studies
School of Management, Economics and Social Sciences

Πτυχιακή Εργασία

Πλάνα διαχείρισης εκτάκτων αναγκών και καταστροφών σε αρχειακούς φορείς : Ανάλυση και σύγκριση πλάνων από πέντε αρχειακούς φορείς

Όνομα Επώνυμο Φωκάς Ιωάννης (ΑΜ: 17074)

Επιβλέπων:
Νικόλαος Καρεκλάς

Αθήνα, Δεκέμβριος 2021

Επιτροπή Εξέτασης

1. Ονοματεπώνυμο

Ιωάννης Τριανταφύλλου

Ioannis Triantafyllou
Digitally signed by Ioannis Triantafyllou
Date: 2022.03.15 09:52:58 +02'00'

2. Ονοματεπώνυμο

Γιώργος Γιαννακόπουλος

Georgios Giannakopoulos
Digitally signed by Georgios Giannakopoulos
Date: 2022.03.18 10:47:35 +02'00'

3. Ονοματεπώνυμο

Ιωάννης Στογιαννίδης

Ioannis Stogiannidis
Digitally signed by Ioannis Stogiannidis
Date: 2022.03.15 21:20:05 +02'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ/ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Φωκάς Ιωάννης, με αριθμό μητρώου 17074 Φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής Διοικητικών, Οικονομικών και Κοινωνικών Επιστημών του Τμήματος Αρχειονομίας, Βιβλιοθηκονομίας και Συστημάτων Πληροφόρησης, δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της πτυχιακής/διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο/Η Δηλών/ούσα

Περίληψη στα ελληνικά

Στη παρακάτω εργασία γίνεται ανάλυση της έννοιας των πλάνων εκτάκτων αναγκών και της εφαρμογής τους στο πλαίσιο της λειτουργείας ενός αρχειακού φορέα. Γίνεται αναφορά στους παράγοντες που ενδέχεται να επηρεάσουν τη λειτουργεία ενός αρχειακού φορέα τόσο των ανθρωπογενών όσο και των φυσικών καταστροφών. Υπογραμμίζεται η σημασία εκπόνησης μελετών εκτίμησης κινδύνου καθώς και η σημασία της εκπαίδευσης του προσωπικού. Έπειτα γίνεται αναφορά στις μεθόδους προστασίας του φορέα από τις διάφορες μορφές κυβερνοεπιθέσεων. Τέλος παρουσιάζεται του σύστημα διαχείρισης πρόσβασης βάσει ρόλων στο ηλεκτρονικό σύστημα του φορέα σε συνάρτηση με την πρόσβαση στο φυσικό χώρο του κτιρίου.

Λέξεις Κλειδιά: Πλάνο εκτάκτων αναγκών, εκτίμηση κινδύνων, πλάνο επιχειρησιακής συνέχειας, πλάνο εκτάκτων αναγκών για τα πληροφοριακά συστήματα, διαχείριση εμπειρικών δεδομένων, κυβερνοεπίθεση, αντίγραφα ασφαλείας

Περίληψη στα αγγλικά

In this thesis is discussed the concept of disaster plans management and their application in record management. We discuss the factors that could affect physical or digital data, either coming from human error or from a natural disaster. We also mention that risk assessment and employee training is in high priority for every sector. Afterwards we project methods of protection for the digital data from hacking. Finally, we present the role base access control not only for the IT but also for the access to the site.

Keywords: Disaster recovery plan, risk assessment, business continuity, disaster recovery plan for IT, knowledge management, hacking, backup

Πίνακας Περιεχομένων

1 Κεφάλαιο 1ο

1.1 Εισαγωγή – Σύντομη ιστορική αναδρομή

Το αρχείο δημιουργήθηκε από την περίοδο που η ανθρώπινη κοινωνία χρειάστηκε να οργανώσει τις πληροφορίες που σχετίζονται με τις ανθρώπινες δραστηριότητες με σκοπό να διατηρηθούν για μετέπειτα χρήση. Η εμφάνιση των αρχείων και η γραφή συμβαίνουν ταυτόχρονα, καθώς η καταγραφή εντοπίζεται ήδη από πολλούς αρχαίους πολιτισμούς (Γιαννακόπουλος Γ. , 2016).

Πιο συγκεκριμένα, στον ελληνικό χώρο η ιστορία της καταγραφής δεδομένων ξεκινά ήδη από τη δεύτερη χιλιετία σε σημαντικά διοικητικά ανακτορικά κέντρα. Η Πύλος και οι Μυκήνες διασώζουν τα πρώτα τεκμήρια σε μορφή γραπτού καταλόγου πάνω σε πινακίδες από ωμό πηλό, στις οποίες καταγράφονταν τα εξαγόμενα προϊόντα και οι ανάγκες του παλατιού. Τα κείμενα αυτά είχαν ένα πολύ συγκεκριμένο σύστημα ταξινόμησης σε συγκεκριμένα δωμάτια των ανακτόρων όπου φυλάσσονταν. Μετά την περίοδο της παρακμής των μεγάλων ανακτορικών κέντρων η γραφή ξεχάστηκε μέχρι την επιδρομή των Δωριέων και την ανακατανομή των προηγούμενων φυλών κεντρικά του Αιγαίου και στα Μικρασιατικά παράλια. Η ανάγκη για την ύπαρξη κοινής γλώσσας επέφερε τη γένεση του ελληνικού αλφαβήτου και μακροχρόνια και τη δημιουργία κοινών όρων και συστηματικής αρχειοθέτησης (MOSSE CLAUDE, 2015).

Μετά την εδραίωση του πολιτικού συστήματος της πόλης-κράτους στον ελληνικό χώρο η συστηματική αρχειοθέτηση των εγγράφων εξελίχθηκε σημαντικά. Τον 6ο αι. Π.Χ καταγράφονται για πρώτη φορά οι άγραφοι νόμοι του Δράκοντα και του Σόλωνα και μετά τις μεταρρυθμίσεις του Κλεισθένη, διαμορφώνεται ένα σύστημα αρχειοθέτησης στις νέες περιφερειακές ενότητες «δήμοι» που αντιστοιχούσαν σε ανάλογους καταλόγους. Τα υλικά τεκμήρια που μας έχουν διασωθεί είναι λίγα λόγω της φθαρτότητας των υλικών (ξύλο περγαμηνή, πάπυρος) ενώ οι γνώσεις μας προέρχονται κυρίως από τα αρχεία που βρέθηκαν κατά τις ανασκαφές του Μετρό των Αθηνών και από μεταγενέστερες πηγές των ελληνιστικών χρόνων. Κατά τον ώριμο 5ο αι. Π.Χ. πολλά

δημόσια έγγραφα καταγράφονται σε ενεπίγραφες λίθους και φυλάσσονται σε κτίρια κρατικών αρχείων όπως η Βουλή των Πεντακοσίων και μετέπειτα το «Μητρώον» στην Αθηναϊκή Αγορά (Brosius M. , 2004) . Γνωρίζουμε όμως μέσω αναφορών του Αριστοτέλη για δημόσια κτίρια που φύλασσαν κρατικά έγραφα και έφεραν μάλιστα τον όρο «αρχείον» καθώς και «γραμματείον» «γραμματοφυλάκειον» και «συγγραφοφυλάκειον» (Dareste, 1882). Άλλοι χώροι φύλαξης αρχείων βρίσκονταν στον περίβολο ιερών σε ειδικά κτίρια (ή στους λεγόμενους «Θησαυρούς») όπου υπήρχαν ειδικοί κατάλογοι με τις δαπάνες και τις εισπράξεις των ιερών (Posner, Archives in the Ancient World, 1972).

Ο συνδυασμός των αρχειακών και των συμβολαιογραφικών αρμοδιοτήτων έγινε χαρακτηριστικός και η αποτελεσματικότητά της γραφειοκρατίας επηρέασε τη γένεση του Ρωμαϊκού δικαίου (gestorum). Η Ρωμαϊκή γραφειοκρατία πέρασε από πολλές φάσεις και καθώς τα ρωμαϊκά αρχεία αναγράφονταν σε ξύλινες πλάκες (ή κέρινες πινακίδες) μας έχουν διασωθεί μόνο αποσπασματικά κυρίως από την περιοχή της Πομπηίας. Κατά την πρώτη περίοδο της Δημοκρατικής Ρώμης υπήρχε το κρατικό ταμείο που ονομαζόταν Aerarium, και λειτουργούσε ως κτίριο που προστάτευε και διατηρούσε τα δημόσια και ιδιωτικά αρχεία, αφιερωμένο στον θεό Κρόνο, στον οποίο η παράδοση απέδιδε την προέλευση της τέχνης της λογιστικής και της τάξης, σύμφωνα με τα λεγόμενα του Πλουτάρχου (Millar, 1964). Οι αρμοδιότητες της αρχειοθέτησης μετατέθηκαν έπειτα στο Tabularium, το κεντρικό αρχείο της Δημοκρατίας στο οποίο συγκεντρώθηκαν τα περισσότερα, αν και όχι όλα, από τα αρχεία εκείνης της περιόδου, αλλά η πιο σημαντική τεκμηρίωση βρισκόταν στο Παλατίνο, την έδρα των αυτοκρατόρων (Posner, Rome Archives in the ancient world, 1972).

Τα βυζαντινά κρατικά αρχεία βρίσκονταν στην Κωνσταντινούπολη μετά την παντοκρατορία του Μέγα Κωνσταντίνου και τη μεταφορά της πρωτεύουσας στην Ανατολικό τμήμα της Ρωμαϊκή Αυτοκρατορίας. Φαίνεται ότι δεν ήταν οργανωμένα με κάποιο τρόπο, αλλά ακολουθούσαν το σύστημα της συγγραφής καταλόγων από διάφορους χρονικογράφους. Αυτό τα καθιστούσε δύσκολα στη διαχείριση και την εύρεση συγκεκριμένων πληροφοριών καθώς δε συνεχίστηκε το παράδειγμα της ρωμαϊκής συστηματικής αρχειακής έρευνας (Treadgold, 2013). Τα αρχεία που μας διασώθηκαν προέρχονται από μονές και μεγάλα μοναστήρια που έχαιραν της κρατικής εύνοιας. Σε αυτές τις μονές υπήρχε ένας αρχειοφύλακας ο οποίος ήταν υπεύθυνος για τον διαχωρισμό των εγγράφων σε χρηστικά και μη. Μετά τον 11ο αι, χρησιμοποιείται

ευρύτατα και συστηματικότερα η χρήση του χαρτιού, καθιστώντας την ταξινόμηση πολύ πιο ευέλικτη (Γεώργιος Γιαννακόπουλος, 2016).

Η Δυτική Ρωμαϊκή Αυτοκρατορία με κέντρο της την Βενετία μετά την επιτυχημένη της επίθεση κατέλυσε την Ανατολική το 1204. Αυτό είχε σαν αποτέλεσμα μια διαφορετική διακυβέρνηση που στηρίχθηκε σε ένα ισχυρό αρχειακό σύστημα. Οι διαφορετικές διοικητικές περιφέρειες, τα γνωστά «πριγκιπάτα» φύλασσαν τα αρχεία τους με μεγάλη προσοχή στα κάστρα των εκάστοτε ελληνικών πόλεων (Duran, 2013). Μετά την άλωση της Κωνσταντινούπολης από τους Οθωμανούς Τούρκους και έγινε μεταβίβαση της κρατικής διακυβέρνησης στο ανατολικό πρότυπο, με τη χαρακτηριστική ισχυρή γραφειοκρατική πολιτική. Τα αρχεία αυτά φυλάσσονταν δίπλα στα διοικητικά κτίρια, στο σαράι (παλάτι του Σουλτάνου) και την μεγάλη πύλη (κατοικία του μεγάλου βεζίρη) και τα διαχειρίζονταν ουλεμάδες ή όπως αλλιώς αναφέρονται ως «άνθρωποι της πένας». Κατά την περίοδο παρακμής του Οθωμανικού κράτους στα τελευταία χρόνια του 16ου αι. Η οθωμανική γραφειοκρατία υπέστη μεγάλη ρήξη (Μπαλτά, 1989). Στον ελλαδικό χώρο τα αρχεία αφορούσαν μικρές επαρχιακές ενότητες τα οποία δεν διασώθηκαν πλήρως μετά το 1821.

Τον 19ο αιώνα τα αρχεία αρχίζουν να αντιμετωπίζονται διαφορετικά. Οι αρχές της Γαλλικής επανάστασης, η απελευθέρωση και αυτοδιάθεση των εθνών και τα νέα απολιτικά δεδομένα με υπερίσχυση των δημοκρατικών καθεστώτων, αποσύνδεσαν την μοναρχική και εκκλησιαστική εξουσία με την αποκλειστική διαχείριση των αρχείων και τα ενέταξαν επίσης και στην διαθεσιμότητα του ευρύτερου κοινού. Παράλληλα, θεωρούνται πλέον και πρώτη ύλη για την ιστορική έρευνα. Στον ελληνικό χώρο μετά τον απελευθερωτικό αγώνα του 1821, το νεοσύστατο ελληνικό κράτος κλήθηκε να οργανώσει ένα νέο αρχειακό σύστημα. Τα εθνικά αρχεία της Ελλάδας θα ιδρυθούν μόλις το Ι914 με την ονομασία Γενικά Αρχεία του Κράτους και αποστολή τη «συναγωγήν και εποπτεία πάντων των δημοσίων αρχείων» (Νόμος 380/1914) (Γιαννακόπουλος Γ. , 2015).

2 Κεφάλαιο 2ο

2.1 Μεθοδολογία έρευνας

Στο πλαίσιο της πτυχιακής έγινε έρευνα στη βιβλιογραφία μαθημάτων του προπτυχιακού προγράμματος της σχολής. Αρχικά εντοπίστηκε το θέμα και έπειτα έγινε μια αρχική αναζήτηση σε Google και Wikipedia για να γίνει κατανοητό κατά πόσον υπάρχει κενό στην ελληνική βιβλιογραφία στο συγκεκριμένο ζήτημα. Σύντομα φάνηκε από τα ιδρυματικά αποθετήρια των ελληνικών πανεπιστημίων ότι ακόμα και η γκρίζα βιβλιογραφία είναι ιδιαίτερα περιορισμένη σε ό,τι αφορά τα θέματα των πλάνων εκτάκτων αναγκών και σχεδόν ανύπαρκτη σε θέματα σχετικά με τα πλάνα που προαναφέρθηκαν και την εφαρμογή τους σε αρχειακούς φορείς.

Έπειτα χρησιμοποιήθηκαν εργαλεία για την αναζήτηση ξενόγλωσση βιβλιογραφίας όπως Scopus, Google Scholar και Science Direct. Από την εν λόγω έρευνα φάνηκε η πολυπλοκότητα του ζητήματος καθώς και το εκτεταμένο επίπεδο οργάνωσης που πρέπει να φέρει ένας φορέας από την αρχή της σύστασής του για την ορθή εκπόνηση των πλάνων. Επίσης έγινε αντιληπτή η έλλειψη βιβλιογραφίας που να συνδυάζει το σύνολο τόσο των φυσικών - ανθρωπογενών όσο και των ψηφιακών παραγόντων. Για το πεδίο των αρχείων που μας αφορά οι πηγές ήταν ιδιαίτερα περιορισμένες ακόμα και στην ξενόγλωσση βιβλιογραφία. Στο κομμάτι των μέτρων προστασίας που πρέπει να εφαρμόζονται και στους αρχειακούς φορείς πληροφορίες αντλήθηκαν από την οργάνωση που ακολουθούν τραπεζικοί φορείς.

Τέλος για να διαπιστωθεί η κατάσταση που επικρατεί στην Ελλάδα αναφορικά με τα πλάνα εκτάκτων αναγκών δημιουργήθηκε και ένα ερωτηματολόγιο που απεστάλη σε διάφορους αρχειακούς φορείς καθώς και βιβλιοθήκες. Η μορφή του ερωτηματολογίου επιλέχθηκε εσκεμμένα. Οι ερωτήσεις εστιάζουν στις αποφάσεις και στα μέτρα που έχουν ληφθεί από τους φορείς για την εκπόνηση των πλάνων εκτάκτων αναγκών. Θεωρήθηκε ότι ερωτήσεις κλειστού τύπου (ΝΑΙ/ ΟΧΙ ή κλίμακας Likert) δεν θα αποτύπωναν επακριβώς όλες τις πτυχές των πλάνων σε συνάρτηση με τις αιτίες που επιλέχθηκαν οι εκάστοτε αποφάσεις. Το ερωτηματολόγιο αποτελείται από 8 ενότητες και 38 ερωτήσεις. Στόχος ήταν μια πιο αναλυτική προσέγγιση ώστε έπειτα να γίνει μια σύντομη σύγκριση μεταξύ των πλάνων.

2.2 Περιορισμοί

Στην περίοδο που εκπονήθηκε η πτυχιακή ήταν δύσκολη η πρόσβαση σε όλους τους φορείς που μας αφορούσαν διότι λόγω της νόσου Covid-19. Η αδυναμία επίσκεψης αρχειακών φορέων, αρχείων επιχειρήσεων και βιβλιοθηκών περιόρισε την εμπειρία από την πραγματική κατάσταση που επικρατεί ενώ ταυτόχρονα δεν άφησε το περιθώριο για την παρουσίαση πρωτότυπου φωτογραφικού υλικού από αυτοψίες.

Επίσης στο πλαίσιο των δυσκολιών αξίζει να σημειωθεί ότι σε πολλούς φορείς δεν υπήρχαν υπεύθυνοι που να μπορούν να απαντήσουν στο ερωτηματολόγιο. Στις περισσότερες περιπτώσεις την εκπόνηση των ερευνών σχετικά με τις προδιαγραφές και τα πλάνα, όπου υπάρχουν, έχουν εκτελεστεί από διαφορετικά άτομα και η παρούσα ευθύνη για την εκπόνηση των πλάνων επιβαρύνει υπαλλήλους με άλλες κύριες αρμοδιότητες με αποτέλεσμα να μην έχουν αρκετό χρόνο για να απαντήσουν στο ερωτηματολόγιο.

Τέλος αξίζει να σημειωθεί ότι υπήρχαν αρκετές βιβλιογραφικές πηγές στις οποίες η πρόσβαση ήταν μόνο επί πληρωμή. Επιπλέον σε κάποιες περιπτώσεις δημοσιεύσεων και βιβλίων επί πληρωμή δεν ήταν ξεκάθαρο αν αφορούσαν τη θεματολογία της πτυχιακής.

2.3 Βιβλιογραφική επισκόπηση

Το σύνολο της βιβλιογραφίας που συγκεντρώθηκε αποτελείται κυρίως από επιστημονικές δημοσιεύσεις σε άρθρα, από κεφάλαια βιβλίων καθώς και από πρακτικά συνεδρίων.

Ένα από τα περιοδικά που κατατόπισαν στο μεγάλο βαθμό και βοήθησαν στην κατανόηση του θέματος ήταν το International Journal of Disaster Risk Reduction. Στο περιοδικό αυτό μελετητές, όπως μηχανικοί, περιβαλλοντολόγοι, γεωπολιτικοί, κοινωνιολόγοι, διεξάγουν έρευνες, ο καθένας από τη δική του επιστημονική σκοπιά, σχετικές με τη θεματολογία με σκοπό να προβάλλονται παγκοσμίως και να βελτιώνουν τις επικρατούσες πρακτικές. Εξίσου σημαντικές ήταν και οι πληροφορίες που αντλήθηκαν από τα πρακτικά του συνεδρίου Mid-Atlantic Regional Archives Conference. Στο συνέδριο αυτό συμμετέχουν αρχειονόμοι από διάφορες πολιτείες των Η.Π.Α. και στοχεύουν στη σύγκριση των γνώσεων τους με τα εμπειρικά προβλήματα που έχουν κληθεί να αντιμετωπίσουν. Στις δημοσιεύσεις τους προσφέρουν χρήσιμες και κατατοπιστικές συμβουλές για αρχειακούς φορείς με θεματολογία την αρχειονομία. Επίσης σχετικές πληροφορίες με τις μεθόδους αντιμετώπισης εκτάκτων αναγκών και κινδύνων περιέχονται και στο βιβλίο που έχει εκδοθεί από το Getty Conservation

Institute του Λος Άντζελες. Το παραπάνω ινστιτούτο εκπονεί έρευνες σχετικές με το χώρο των πολιτισμικών φορέων και αποβλέπει στη βελτίωση των πρακτικών συντήρησης πολιτισμικών στοιχείων.

Έπειτα μια από τις σημαντικότερες προσωπικότητες που αποτελεί αυθεντία στο χώρο του και βοήθησε σημαντικά στην κατανόηση των πιθανών κινδύνων του διαδικτύου είναι ο Marc Rogers. Ευρέως γνωστός hacker που ξεκίνησε από τα εφηβικά του χρόνια να ανακαλύπτει τις δυνατότητες των ηλεκτρονικών υπολογιστών. Έπειτα συνέχισε μια καριέρα συνασπισμένος στην θεωρητική προσέγγιση των «white hats» βελτιώνοντας τις τακτικές κυβερνοασφάλειας και έπειτα δημιουργώντας της δική του εταιρεία που δραστηριοποιείται σε αυτόν τον τομέα. Επίσης έχει συνεργαστεί με εταιρείες «κολοσσούς» στο χώρο της πληροφορικής και διαθέτει ένα «πλούσιο» βιογραφικό που επιβεβαιώνει την δεινότητά του στον τομέα.

Επιπλέον πληροφορίες αντλήθηκαν από δημοσιεύσεις του USENIX: The Advanced Computing Systems Association, ενός μη κερδοσκοπικού οργανισμού με βάση το Μπέρκλεϊ στην Καλιφόρνια. Στόχος του οργανισμού είναι η υποστήριξη προηγμένων υπολογιστικών συστημάτων με τεχνολογικές καινοτομίες, πρακτικές και έρευνες σε τρέχοντα τεχνολογικά θέματα. Επιπλέον πληροφορίες για τη δομή και τη λειτουργία των υπολογιστικών συστημάτων προέκυψαν από δημοσιεύσεις του European Institute for Computer Antivirus Research το οποίο αποσκοπεί στη βελτιστοποίηση των λογισμικών προστασίας των υπολογιστών των τοπικών δικτύων (LAN) καθώς και τη βελτίωση των RFID, συστημάτων για την αναγνώριση αντικειμένων.

Για την κατανόηση του hacking και των κατηγοριών του, σημαντική επίδραση είχε και το βιβλίο του Jon Erickson, έμπειρου γνώστη του τομέα της πληροφορικής που εργάζεται στον τομέα της κυβενροασφάλειας και της προστασίας των υπολογιστικών νεφών. Επιπλέον σε ό,τι αφορά τον τομέα της επιχειρησιακής συνέχειας οι συμβουλές της εταιρείας IBM (International Business Machines Corporation) ήταν πολύ κατατοπιστικές καθώς, μέσα από αυτές, έγινε κατανοητή η αξία των πλάνων επιχειρησιακής συνέχειας καθώς και η ειδοποιός διαφορά τους από τα πλάνα εκτάκτων αναγκών.

Τέλος σε ό,τι αφορά τα πρότυπα και τις καθιερωμένες πρακτικές λειτουργείες, πληροφορίες αντλήθηκαν από το Διεθνή Οργανισμό Τυποποίησης (ISO) όπου υπάρχουν πληροφορίες για πρακτικά ζητήματα καθώς και λύσεις σε τεχνικά προβλήματα που προκύπτουν στους φορείς.

2.4 Περιγραφή κεφαλαίων

Κεφάλαιο 1ο : Γίνεται αναφορά στις μεθόδους που χρησιμοποιήθηκαν για την κατανόηση του θέματος και για τη συγγραφή της πτυχιακής. Επίσης θα αναφερθούν οι περιορισμοί και οι δυσκολίες που έπρεπε να αντιμετωπιστούν καθώς και μια επισκόπηση της κατάστασης που επικρατεί σήμερα στον ερευνητικό χώρο του θέματος.

Κεφάλαιο 2ο : Στο δεύτερο κεφάλαιο θα γίνει μια σύντομη ιστορική αναδρομή όπου θα γίνει αναφορά σε κάποια ορόσημα της ιστορικής εξέλιξης του αρχείου σαν έννοια. Ξεκινώντας από τις πρώτες μορφές αρχειακών τεκμηρίων μέχρι την αναγνώριση της αξίας τους ως φορείς σημαντικών πληροφοριών και μέσα τεκμηρίωσης ιστορικών γεγονότων από τη Γαλλική Επανάσταση και έπειτα.

Κεφάλαιο 3ο : Συνεχίζοντας από την ιστορική αναδρομή, σε αυτό το κεφάλαιο παρατίθενται οι βασικότερες έννοιες που αφορούν τους διαχειριστές των αρχειακών φορέων καθώς και οι παράγοντες που έχουν αντίκτυπο στις κτιριακές εγκαταστάσεις, τους χώρους φύλαξης (φυσικούς ή ψηφιακούς) καθώς και στα τεκμήρια φυσικών υποστρωμάτων. Τα αρχεία ηλεκτρονικών υποστρωμάτων αποτελούν μια πηγή πληροφοριών που όλοι οι αρχειακοί φορείς διαθέτουν τουλάχιστον τις τελευταίες δυο δεκαετίες. Πέραν λοιπόν από τα πλάνα που αναφέρονται προηγουμένως στις μεθόδους προστασίας των φυσικών αρχείων δεν πρέπει να παραβλέπονται και οι παράγοντες πιθανών καταστροφών των ηλεκτρονικών αρχείων.

Κεφάλαιο 4ο : Έχοντας πλήρη γνώση των παραγόντων που ενδέχεται να έχουν επιπτώσεις στους αρχειακούς φορείς, σε αυτό το κεφάλαιο προβαίνουμε στη διατύπωση πλάνων αντιμετώπισης καταστροφών. Παρακάτω λοιπόν αποτυπώνονται οι πληροφορίες που συγκεντρώθηκαν από τη μελέτη της σχετικής βιβλιογραφίας, αναφορικά με τα πλάνα αντιμετώπισης καταστροφών και εκτάκτων αναγκών.

Κεφάλαιο 5ο : Παρόλο που η διατύπωση των παραπάνω πλάνων μετά από σχετικές μελέτες αποτελεί παράγοντα που ενισχύει την ανθεκτικότητα του φορέα στις δύσκολες συνθήκες, είναι αναγκαίο να υπάρχουν και πλάνα που εξασφαλίζουν τη συνέχιση των εργασιών για την αδιάκοπη παροχή των υπηρεσιών του φορέα. Στο παρακάτω κεφάλαιο θα γίνει ανάλυση της έννοιας των πλάνων επιχειρησιακής συνέχειας και της σημασίας της ένταξής τους στις προδιαγραφές λειτουργείας ενός αρχειακού φορέα.

Κεφάλαιο 6ο : Δεν χρειάζεται να προλογίσουμε τη σημασία των αρχείων ηλεκτρονικού υποστρώματος στη σημερινή εποχή. Όπως όμως υποδεικνύει η διεθνής βιβλιογραφία η προστασία των ηλεκτρονικών αρχείων είναι μια κοπιώδης διαδικασία

που χρήζει συνεχούς εκσυγχρονισμού που είναι αδύνατον να παραληφθεί από έναν αρχειακό φορέα και δη απ' όσους διαχειρίζονται ενεργά αρχεία επιχειρήσεων. Στο παρακάτω κεφάλαιο θα παρατεθούν πληροφορίες που σχετικά με τα πλάνα διαχείρισης ψηφιακών καταστροφών.

Κεφάλαιο 7ο : Στο παρόν κεφάλαιο παρατίθενται κάποιες από τις βασικότερες πληροφορίες που εμπεριέχονται στα πλάνα εκτάκτων αναγκών διαφόρων φορέων, οι οποίες μάλιστα σκιαγραφούν και κατά πόσον έχουν ευοδωθεί στη μελέτη των πιθανών κινδύνων και έπειτα στη λήψη αποφάσεων για την πρόληψη και την προστασία. Στο πρώτο μέρος αποδίδεται ένα παράδειγμα από κρατικό φορέα των Η.Π.Α. Στα δυο επόμενα μέρη δυο παραδείγματα με ελληνικά δεδομένα, από το δημόσιο και τον ιδιωτικό φορέα, εδώ χρησιμοποιούνται πληροφορίες που προέκυψαν από το ερωτηματολόγιο. Τέλος αναφέρονται κάποια συμπεράσματα.

3 Κεφάλαιο 3ο

3.1 Αρχεία ζωτικής σημασίας

Στην ενεργή τους φάση τα αρχεία (records) χρησιμοποιούνται σε καθημερινή βάση διότι εξυπηρετούν τη δραστηριότητα μιας επιχείρησης ή ενός φορέα ή ενός οργανισμού. Για την ταχύτερη πρόσβαση σε αυτό, το ενεργό αρχειακό υλικό προβλέπεται να διατηρείται στον χώρο που δημιουργήθηκε, δηλαδή στα γραφεία των υπαλλήλων που το δημιούργησαν.

Τα αρχεία τα οποία διατηρούνται στο διηνεκές λόγω της αξίας που φέρουν για τον φορέα ονομάζονται αρχεία ζωτικής σημασίας. Πρόκειται για τεκμήρια αναγκαία για την επαναλειτουργία του οργανισμού μετά από κάποια καταστροφή. Μέσα από αυτά διαφαίνονται τα περιουσιακά στοιχεία, οι πόροι, οι υποχρεώσεις και τα δικαιώματα του φορέα. Τέτοια τεκμήρια είναι:

- το ιδρυτικό
- τα πρακτικά του διοικητικού συμβουλίου
- οι τίτλοι ιδιοκτησίας
- οι δανειακές συμβάσεις

Επίσης συναντάται συχνά στους αρχειακούς φορείς και η έννοια των σημαντικών αρχείων. Συνήθως σε αυτά τα τεκμήρια αναγράφονται πληροφορίες που αφορούν το προσωπικό, την πολιτική και τους στόχους του φορέα ή στοιχεία πελατών. Τα σημαντικά αρχεία προστατεύονται κατά προτεραιότητα έπειτα από τα αρχεία ζωτικής σημασίας. Τα πλάνα που περιγράφουν τις διαδικασίες εκτάκτων αναγκών, τις περισσότερες φορές, περιέχουν μια κατάτμηση του υλικού ανάλογα με τη σημασία που φέρουν οι πληροφορίες που περιέχει.

3.2 Είδη Καταστροφής Αρχείων

Οι φυσικές καταστροφές ποικίλουν και όλες τους κυμαίνονται στον ίδιο περίπου βαθμό καταστροφικότητας για τα αρχεία. Στις φυσικές καταστροφές τοποθετούνται οι πλημύρες, οι πυρκαγιές, τα ηφαίστεια, οι σεισμοί, επίσης στους τρόπους φυσικής καταστροφής των αρχείων συμπεριλαμβάνονται ο ήλιος, η θερμοκρασία καθώς και η υγρασία (μύκητες).

Καταστροφή ορίζεται το σύνολο των παραγόντων που προκαλούνται είτε από τον άνθρωπο είτε από τη φύση και διαταράσσουν την ομαλή λειτουργεία της κοινωνίας,

καταστρέφοντας περιουσιακά στοιχεία ατόμων, φορέων ή της πολιτείας. Ο βαθμός ετοιμότητας στον οποίο μπορεί να βρίσκεται ένα άτομο, ένας φορέας ή η πολιτεία για κάποια πιθανή καταστροφή, η οποία έχει οριστεί σε μεγάλο μέρος της από διάφορους περιβαλλοντικούς ή κοινωνικούς παράγοντες, ορίζει και την ανθεκτικότητά τους στις επιφερόμενες ζημίες (Jaffer Kabir Najar, 2021).

3.3 Ανθρώπινος παράγοντας και τεχνολογία

Ο ανθρώπινος παράγοντας σχετίζεται με τις κλοπές είτε φυσικές είτε και με τους βανδαλισμούς σε όλα τα είδη των τεκμηρίων (ενεργά - ιστορικά). Ο τελευταίος παράγοντας σχετίζεται περισσότερο με τα ιστορικά αρχεία, είτε πρόκειται για κρατικά είτε για φορέα. Δεν είναι λίγες οι φορές που τα κτίρια των αρχείων έχουν αντιμετωπιστεί ως ταυτόσημα με τους κρατικούς ή εταιρικούς φορείς που με τις αποφάσεις τους όρισαν το μέλλον μιας ομάδας ανθρώπων εγείροντας αντιδράσεις. Γίνεται κατανοητό λοιπόν ότι δεν απουσιάζουν από τον ρού της ιστορίας οι φορές που συμβάντα μαζικών αντιδράσεων κατέληξαν να ζημιώνουν αρχειακούς φορείς (Jaffer Kabir Najar, 2021).

Όσον αφορά τις τεχνολογικές καταστροφές, οι οποίες δημιουργούνται αποκλειστικά από τον ανθρώπινο παράγοντα, προκαλούνται σχεδόν πάντα από λανθασμένες πρακτικές. Τα αίτια που οδηγούν σε τεχνολογικές καταστροφές είναι κυρίως ο ελλιπής σχεδιασμός και η κατασκευή, η ανεπαρκής διαχείριση και η άγνοια του προσωπικού. (Μπάγιας, 1999)

Συγκεκριμένα:

- Μεγάλης κλίμακας κοινωνικές εντάσεις
- Μαζικές μεταφορές αρχειακού υλικού
- Βιομηχανίες

3.3.1 Καταστροφή ηλεκτρονικών δίσκων

Χάρη στην εξέλιξη της τεχνολογίας καθώς και της μεγάλης πλέον ύπαρξης των τεκμηρίων που δημιουργούνται καθημερινά, προέκυψε η ανάγκη για επιπλέον χώρο αποθήκευσης. Επειδή όμως αυτός ο χώρος δεν ήταν εφικτό να υπάρξει για κάθε επιχείρηση και οργανισμό, άρχισε να αναπτύσσεται η χρήση ψηφιοποιημένων ή ψηφιακών τεκμήριων ώστε να εξασφαλισθεί χώρος αποθήκευσης. Το πρόβλημα που προκύπτει βέβαια απ' την ψηφιοποίηση των αρχείων, είναι ότι σε περίπτωση απώλειας ενός ηλεκτρονικού δίσκου είναι δύσκολο, και σε πολλές περιπτώσεις, αδύνατον να

ανακτηθούν τα αρχεία, έστω και μερικώς κατεστραμμένα όπως θα γινόταν σε περίπτωση φυσικής καταστροφής.

3.3.2 Τάσεις Ρεύματος

Οι αυξομειώσεις των τάσεων ρεύματος ή η πλήρης διακοπή αυτών είναι πιθανόν να προκαλέσουν ανεπανόρθωτες υλικές ζημιές στις ηλεκτρονικές συσκευές, αλλά και απώλεια ψηφιακών δεδομένων εξαιτίας της απότομης διακοπής λειτουργίας τους. Γεγονός που δημιουργεί σοβαρό πρόβλημα, ειδικά σε επιχειρήσεις και οργανισμούς διότι η απώλεια των ψηφιακών τους δεδομένων εάν δεν έχουν αποθηκευτεί οδηγεί στην μη εύρεσή τους ξανά και επαναδημιουργία τους.

3.4 Καταστροφή Αρχείων Ηλεκτρονικού υποστρώματος

Το ηλεκτρονικό έγκλημα ήρθε για πρώτη φορά στην επιφάνεια στις αρχές της δεκαετίας του 1970 όταν κάποια άτομα που ασχολούνταν με την τεχνολογία της εποχής προσπαθούσαν να ανακαλύψουν τις δυνατότητες των συστημάτων. Στη σύγχρονη εποχή το ηλεκτρονικό έγκλημα είναι αδύνατον να εκτελεστεί από απλούς χρήστες των ηλεκτρονικών υπολογιστών. Τα μέσα προστασίας τόσο των οικιακών υπολογιστών όσο και των μεγάλων βάσεων δεδομένων μεγάλων φορέων είναι πολλαπλά και πολυδαίδαλα. Ως εκ τούτου η απόκτηση μη εξουσιοδοτημένης πρόσβασης απαιτεί υψηλό γνωστικό επίπεδο στον τομέα των υπολογιστών (Rogers, 2000).

Οι hackers σύμφωνα με τη Sukhai είναι άτομα με ταλέντο στην πληροφορική και πολλές δυνατότητες. Είναι τα άτομα που εφηύραν πολλές τεχνολογίες που πλέον χρησιμοποιούνται στην καθημερινότητα όπως το διαδίκτυο και το λειτουργικό σύστημα UNIX. Οι crackers, όπως ονομάζονται από την ερευνήτρια, είναι τα άτομα με την παραβατική συμπεριφορά που συνήθως προσπαθούν να αποκτήσουν ηλεκτρονικά αγαθά, όπως μουσική, ταινίες, λογισμικό κ.α., χωρίς να πληρώσουν την αξία τους στον δημιουργό ή τον κάτοχο των πνευματικών δικαιωμάτων (Sukhai, 2005). Με άλλα λόγια η κυβερνοεπίθεση (hacking) είναι η διαδικασία που ένα άτομο αποκτά πρόσβαση σε έναν υπολογιστή χωρίς την άδεια του χρήστη που το διαχειρίζεται. Το άτομο αυτό πρέπει να διαθέτει γνώσεις για να καταφέρει να υπερνικήσει τα υπολογιστικά συστήματα που πάντα φέρουν προγράμματα προστασίας και να μην αφήσει ενοχοποιητικά στοιχεία της ταυτότητάς του. Άπαξ και το άτομο αυτό (hacker) αποκτήσει πρόσβαση σε ένα υπολογιστικό σύστημα, μπορεί να τροποποιήσει, να υποκλέψει αρχεία ή και να εγκαταστήσεις κακόβουλο λογισμικό αποσκοπώντας σε χρηματικά κέρδη. (Patricia Y. Logan, 2005)

Στο πλαίσιο της εξέτασης του ζητήματος από κοινωνιολογική άποψη, έχουν διατυπωθεί από τους ερευνητές τέσσερεις κατηγορίες hackers ανάλογα με τη δράση που είχαν. Η πρώτη γενιά των hackers περιλαμβάνει προγραμματιστές του πανεπιστημίου MIT της εποχής μεταξύ του 1950 και 1960. Τα άτομα αυτά διαμόρφωσαν τη μορφή λειτουργείας των υπολογιστών καθώς κατανόησαν σε βάθος και έπειτα έλυσαν τα σύνθετα υπολογιστικά προβλήματα. Έφεραν υψηλή κατάρτιση στο χώρο τους και μέσω της εφευρετικότητάς τους συνετέλεσαν στη δημιουργία του διαδικτύου και διαφόρων άλλων εφαρμογών των πρώτων υπολογιστών. Έπειτα συναντάμε hackers όπως ο Steve Jobs, και ο συνεργάτης του στην ίδρυση της εταιρείας Apple, Stephen Wozniak οι οποίοι έφεραν τους υπολογιστές πιο κοντά στις μάζες των απλών χρηστών. Δημιουργώντας ένα σημείο διεπαφής (interface) το οποίο ήταν φιλικό για άτομα που δεν ήταν εξειδικευμένα στον προγραμματισμό, μετέφεραν την τεχνολογία των υπολογιστών από την αποκλειστική χρήση σε εταιρείες και πολυεθνικές, στη ζωή του μέσου ανθρώπου. Προχωρώντας συναντάμε τους Hackers που έδωσαν τα φώτα τους στην πρώιμη μορφή των παιχνιδιών ηλεκτρονικού υπολογιστή. Σε αυτό το σημείο παρατηρείται και ο διαχωρισμός της θετικής έννοιας των hackers καθώς πλέον εμφανίζεται και μια πληθυσμιακή ομάδα από βιρτουόζους της πληροφορικής που προσπαθεί να επωφεληθεί από την «πειρατεία». Με την έννοια «πειρατεία» (piracy) εννοούμε την παράβλεψη των πνευματικών δικαιωμάτων ενός δημιουργού καθώς και την έκδοση λογισμικού και αρχείων ιδιωτικού και απόρρητου χαρακτήρα. Τέλος αναφέρεται η τέταρτη γενιά των hackers η οποία φέρει αποκλειστικά τον παραβατικό χαρακτήρα και την παράνομη συμπεριφορά καθώς συνεχίζει την «πειρατεία» και πλέον σχεδιάζει σύνθετα υπολογιστικά προγράμματα που λειτουργούν ως κακόβουλο λογισμικό και μπορούν να εισβάλλουν σε οικιακούς υπολογιστές από διάφορες πηγές του διαδικτύου (KLEINKNECHT, 2003).

Σύμφωνα με τους Logan και Clarkson για να μπορέσει κάποιος να μάθει επαρκώς πληροφορική καθώς και τους ελιγμούς και τα τεχνάσματα που χρησιμοποιούν οι hackers πρέπει και ο ίδιος ο μαθητής να γίνει πραγματοποιήσει hacking. Με αυτό το σκεπτικό μπορεί να γίνει κατανοητός και ένας ακόμα διαχωρισμός των hackers ανάλογα με τους σκοπούς που εξυπηρετούν. Πιο αναλυτικά διακρίνονται οι εξής κατηγορίες:

- «White Hats» αποκαλούνται οι hackers που λειτουργούν με βάση τη ηθική (ethics) και δεν προσπαθούν να αποκτήσουν πρόσβαση σε υπολογιστές αθώων χρηστών, αλλά εξετάζουν τις μεθόδους προστασίας ενός

υπολογιστικού συστήματος για να ενδυναμώσουν τα τρωτά του σημεία ή καταπολεμούν το ηλεκτρονικό έγκλημα.

- «Black Hats» αποκαλούνται οι hackers με παραβατική συμπεριφορά που προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα με σκοπό να διαπράξουν απάτες ή/και να υποστηρίξουν μια εγκληματική πράξη.
- «Gray Hats» στην τελευταία κατηγορία εντάσσονται οι hackers που λειτουργούν στις παρυφές των κανόνων ηθικής (ethics) και υποστηρίζουν είτε ως εξωτερικοί συνεργάτες την ανάπτυξη των συστημάτων προστασίας είτε χρησιμοποιούν το hacking σαν μέσω για την επιβολή της διαφάνειας των πολιτικών πράξεων (hactivists) (Patricia Y. Logan, 2005) ; (Pashel, 2006).

Αξιοσημείωτο είναι το ορόσημο ενός hacker που καθόρισε τον τρόπο που βλέπουμε σήμερα αυτά τα άτομα καθώς και όρισε τις μεθόδους που τους αντιμετωπίζει η κοινωνία σαν σύνολο. Όπως έγινε αντιληπτό δεν είναι παραβάτες όλοι οι hackers. Κάποιοι μπορούν να εργάζονται για την ευημερία της κοινωνίας. Ο Kevin D. Mitnick είναι μια εξέχουσα προσωπικότητα του χώρου καθώς από την ηλικία των δώδεκα ετών ξεκίνησε να παραποιεί τη λειτουργεία συστημάτων προς όφελός του. Από τα πλαστά εισιτήρια λεωφορείων μέχρι την κυβερνοεπίθεση σε μεγάλες εταιρείες τηλεπικοινωνίων και το γραφείο ερευνών των Η.Π.Α. (FBI) ο Mitnick καταδικάστηκε πολλές φορές για τα ηλεκτρονικά του εγκλήματα. Αφού λοιπόν εξέτισε τις ποινές του, ίδρυσε την εταιρεία «Mitnick Security Consulting» στο Las Vegas της Νεβάδα το 2003 και έκτοτε παρέχει συμβουλευτικές υπηρεσίες σε επιχειρήσεις. Επίσης μέσα από τα βιβλία του και τις ομιλίες του προωθεί τα ethics στο πλαίσιο του hacking και την φιλοσοφία των white hats hackers (Editors, TheFamousPeople.com, n.d.).

3.5 Ethics

Είναι σαφές ότι μια πράξη που αποσκοπεί στην παραβίαση προσωπικών αρχείων ενός ατόμου ή ενός φορέα, είναι παράνομη και αντισυνταγματική. Σε περιπτώσεις όπου υπάρχουν σαφή πνευματικά δικαιώματα για ένα προϊόν τέχνης ή επιστήμης η υποκλοπή αποτελεί σοβαρό παράπτωμα.

Από την άλλη πλευρά υπάρχει ενδιαφέροντας αντίλογος που αναφέρει ότι το hacking δεν προωθεί αποκλειστικά την παραβατική συμπεριφορά με κακόβουλη πρόθεση. Στις περιπτώσεις που το αποτέλεσμά του στοχεύει στη δημοσίευση αγαθών που σχετίζονται

με την παιδεία όπως επιστημονικά άρθρα και μελέτες τα οποία βρίσκονται πίσω από ιστοσελίδες επιστημονικών περιοδικών που απαιτούν αδρή πληρωμή για την εμφάνισή τους αποβλέπει στην προώθηση της γνώσης σε σπουδαστές ή σε ομάδες που δεν έχουν οικονομική δυνατότητα να τα αγοράσουν (Lawson, 2017).

Επιπροσθέτως στον ρούν της ιστορίας έχουν έρθει στην επιφάνεια γεγονότα κυβερνοεπίθεσης που αποσκοπούσαν στη δημοσίευση κρατικών εγγράφων απόρρητου χαρακτήρα που αποκρύπτονταν από το φως της δημοσιότητας για να αποφευχθούν οι κυρώσεις στα αρμόδια άτομα που αποφάσισαν εναντίον της δημόσιας ευδαιμονίας εποφθαλμιώντας το προσωπικό όφελος. Τα λεγόμενα wikileaks απασχόλησαν τους σύγχρονους φιλοσόφους καθώς η κατά παράδοση «παραβατική συμπεριφορά» προστάτευσε ομάδες και άτομα από την πιθανή απόφανση συγκεκαλυμένων αποφάσεων εναντίον τους. Επίσης δεν πρέπει να ξεχνάμε ότι προωθείται η ελευθερία των ατόμων από πρακτικές hacking αντίστοιχές με την παραπάνω (Pashel, 2006).

Παρόλα αυτά η προστασία των προσωπικών δεδομένων ατόμων και εταιρειών που υπάρχουν σε αρχειακούς φορείς δεν παύει να αποτελεί απαραίτητη προϋπόθεση και αναπόσπαστη υποχρέωση των αρχειονόμων απέναντι στους πελάτες τους.

3.6 Τύποι κυβερνοεπίθεσης «hacking»

Παρακάτω παρουσιάζονται κάποιες συνοπτικές πληροφορίες αναφορικά με τους τύπους επίθεσης που μπορεί να δεχτεί ένας χρήστης στον ηλεκτρονικό του υπολογιστή ή ένα υπολογιστικό σύστημα. Οι social engineers είναι μια γνωστή και σύγχρονη κατηγορία τεχνικής hacking όπου οι hackers προσπαθούν να παραπλανήσουν τους χρήστες σε ένα περιβάλλον που φαίνεται έγκυρο και ασφαλές για να αποσπάσουν προσωπικά στοιχεία (usernames, passwords, αριθμούς τηλεφώνων, αριθμούς λογαριασμών τραπέζης). Χρησιμοποιούν το συναίσθημα της ασφαλούς περιήγησης που περιφέρεται στο χώρο του surface web και παραπλανούν τους χρήστες που δεν είναι κατάλληλα ενημερωμένοι (Workman, 2007). Είναι λοιπόν πολύ σημαντικό να είναι γνωστοί οι τύποι επιθέσεων, ηλεκτρονικών και μη, σε όλους τους υπαλλήλους του φορέα καθώς καθίσταται πιο δύσκολο να εξαπατηθούν και να υποπέσουν σε κάποια παγίδα φέρνοντας σε κίνδυνο την ακεραιότητα του υπολογιστικού συστήματος.

3.6.1 Ransomware

Στο παρόν ζήτημα που εξετάζεται οι hackers και η πειρατεία γενικότερα είναι ένα φαινόμενο που αφορά και τους αρχειακούς φορείς καθώς έχουν στα αποθετήριά τους

ψηφιακό υλικό μεγάλη αξίας ενώ ταυτόχρονα μπορεί να αποτελέσουν το θύμα σε μια επίθεση ransomware. Πιο αναλυτικά το ηλεκτρονικό έγκλημα υπάρχει περίπτωση είτε να αποσκοπεί σε απόκτηση απόρρητων αρχειακών τεκμηρίων που περιέχουν ευαίσθητα προσωπικά δεδομένα, καθώς και εταιρικά αρχεία είτε στην απόσπαση χρηματικού ποσού. Το δεύτερο σενάριο αποτελεί την ευρέως γνωστή επίθεση ransomware, όπου έμπειροι hackers εισβάλουν σε ένα σύστημα αποσκοπώντας είτε στην κρυπτογράφηση των αρχείων ενός υπολογιστή ή μια βάσης δεδομένων είτε στον αποκλεισμό της πρόσβαση από τους χρήστες. Οι εγκληματίες αυτής της κατηγορίας διαθέτουν πολλές γνώσεις προγραμματισμού, πληροφορικής και μαθηματικών και στοχεύουν στην απολαβή κρυπτονομισμάτων. Αρχικά δημιουργούν ένα πρόγραμμα τύπου malware, trojan ή ενός κακόβουλου αρχείου που μπορεί να σταλεί και μέσω ηλεκτρονικού ταχυδρομείου, έπειτα αυτό κρυπτογραφεί τα όλα αρχεία του υπολογιστή εκτός από κάποια λειτουργικά, ή σε πιο απλές περιπτώσεις κλειδώνει τον υπολογιστή με αποτέλεσμα να μην έχουν πρόσβαση οι χρήστες. Το κλειδί της αποκρυπτογράφησης είναι γνωστό μόνο στον εισβολέα ο οποίος μετά την επίθεση απαιτεί από το θύμα χρηματική πληρωμή με κρυπτονομίσματα, τα οποία είναι πολύ δύσκολο να εντοπιστούν. Έπειτα από την χρηματική συναλλαγή μεταξύ του θύτη και του θύματος, ο hacker αποστέλλει στον υπολογιστή το κλειδί της αποκρυπτογράφησης και «ξεκλειδώνει» είτε τα αρχεία είτε τον υπολογιστή.

Σύμφωνα με στατιστική μελέτη από τον Ιούνιο του2015 έως τον Ιούνιο του 2016 το 79% των εμπορικών επιχειρήσεων της Αμερικής δέχτηκε τουλάχιστον μια επίθεση τύπου ransomware ενώ το 22% περισσότερες από είκοσι (Ronny Richardson, 2017)

Γίνεται λοιπόν κατανοητό ότι στο πλαίσιο του DRP για τα ηλεκτρονικά συστήματα είναι αναγκαίος ο συνυπολογισμός και του παραπάνω πιθανού παράγοντα καταστροφής.

3.6.2 Phishing

Το phishing είναι ένας τύπος κυβερνοεπίθεσης που αποσκοπεί στην αποκόμιση προσωπικών δεδομένων, όπως αναφέρθηκαν και παραπάνω στο πλαίσιο του social engineering. Αναφορικά με τη μέθοδο του hacking ο χρήστης έρχεται σε επαφή με μια ιστοσελίδα που παρουσιάζεται έγκυρη και φέρει τα χαρακτηριστικά όμοια με αυτά αξιόπιστων ιστοσελίδων. Έπειτα καλείται να δώσει κάποια από τα στοιχεία του, τα οποία γίνονται ταυτόχρονα διαθέσιμα σε έναν hacker.

Σχετικές μελέτες αναφέρουν ότι με αυτά τα τεχνάσματα έχουν συνεχή πρόοδο και δέχονται συνεχείς αναβαθμίσεις αφού πλέον υπάρχουν plugins στους φυλλομετρητές που εντοπίζουν την πιθανότητα phishing.

Με το παραπάνω τέχνασμα δεν γίνεται χρήση κάποιου λογισμικού. Όλες οι ενέργειες λαμβάνουν χώρα στο χώρο του διαδικτύου μέσω μιας ψευδούς ιστοσελίδας. Σε αυτή την ιστοσελίδα μπορεί να έχει γίνει ανακατεύθυνση μετά από κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου που δέχτηκε ο χρήστης από μια εταιρεία που φαίνεται σαν να τη χρησιμοποιεί. Για παράδειγμα μπορεί να αναφέρεται ότι είναι από την «Google Enterprises» εταιρεία που δεν υπάρχει αλλά μοιάζει με αυτή που χρησιμοποιούν όλοι οι χρήστες καθημερινά (Nalin Asanka Gamagedara Arachchilage, 2014).

3.6.3 Impersonation on help desk calls

Στις κατηγορίες των επιθέσεων social engineering η πλαστοπροσωπία (impersonation) ενός υπαλλήλου που εξυπηρετεί από σύστημα τηλεφωνικής υποστήριξης αποτελεί διαφορετική κατηγορία. Γενικότερα στο πλαίσιο του hacking ενός φορέα συναντάμε τις πιθανές επιθέσεις συνδυαστικά και πολλώ μάλλον στην κατηγορία του impersonation όπου ένα άτομο προσποιείται ότι εργάζεται σε μια νόμιμη εταιρεία που έχει σκοπό την εξυπηρέτηση ή την παρουσίαση μια υπηρεσίας. Οι αληθοφανείς ταυτότητες μπορεί εύκολα να φανούν έγκυρες και όχι ψευδείς σε άτομα που δεν είναι προϊδεασμένα με αυτή την απάτη, με αποτέλεσμα να ακολουθήσουν βήματα εγκατάστασης λογισμικού, trojan-ransomware κ.α., ή να παραθέσουν τα στοιχεία τους, ή του φορέα, σε ιστοσελίδες που πραγματοποιούν phishing ή ακόμα και να αναφέρουν απόρρητα στοιχεία τηλεφωνικώς (Hussain Aldawood, 2020).

Γενικότερα η παραπάνω μέθοδος φαίνεται να είναι αρκετά αποτελεσματική καθώς οι μελέτες αναφέρουν πως σαν άνθρωποι έχουμε περισσότερη εμπιστοσύνη σε έναν άλλο άνθρωπο που μας μιλά φιλικά και είναι πρόθυμος να μας εξυπηρετήσει. Κάθε μορφή απάτης χρησιμοποιεί ένα μέσω για να φτάσει στο χρήστη-θύμα, στην προκυμμένη περίπτωση είναι το τηλέφωνο, και όχι μια σελίδα στο διαδίκτυο (phishing). Τεχνάσματα όπως η επίκληση στο συναίσθημα, η κίβδηλη ευγένεια, άσχετα θέματα συζήτησης και σύμφωνη προσωπική γνώμη του υπαλλήλου του τηλεφωνείου, ιδιαίτερη προφορά αποσκοπούν στην απόσπαση της εμπιστοσύνης του θύματος για την πραγματοποίηση της απάτης (Huahong Tu, 2019).

3.6.4 Trojans

Τα λογισμικά τύπου trojan ή trojan horse είναι προγράμματα που φαίνονται έγκυρα και έμπιστα στους χρήστες που δεν έχουν εμπειρία. Μπορεί να περιέχονται σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου ως συνημμένα, σε αρχεία που αποστέλλονται μέσω Skype, Yahoo chat ή σε εφαρμογές διαμοιρασμού αρχείων μέσω χρηστών (peer-to-peer) (Al-Saadoon, 2011).

Αφού λοιπόν τα αρχεία trojans αποθηκευτούν στον υπολογιστή, με ονομασίες και σε μέρη που είναι δύσκολο να εντοπιστούν από τους χρήστες καθώς φαίνονται ως χρήσιμα αρχεία για τη λειτουργεία του υπολογιστή, παρακωλύουν την λειτουργεία του υπολογιστή και μπορεί να διαγράφουν ή να τα καταστρέφουν αρχεία, να εγκαθιστούν ιούς, να υποκλέπτουν πληροφορίες και να διαδίδονται στους υπολογιστές του ίδιου δικτύου. Τέλος η λειτουργεία των trojan μπορεί να γίνει αντιληπτή και από ανεπιθύμητα και αλλεπάλληλα μηνύματα τύπου pop up που εμφανίζονται στα windows (Hussain Aldawood, 2020).

3.6.5 Fake software

Τα ψευδή λογισμικά είναι μια ακόμη κατηγορία που αποτελεί κίνδυνο για τους χρήστες. Πιο συγκεκριμένα με την παραπάνω έννοια αναφερόμαστε σε εφαρμογές του ηλεκτρονικού υπολογιστή (ή και άλλων πλατφορμών) που δεν έχουν περάσει από έλεγχο και δεν είναι διαθέσιμες από κάποια εταιρεία πληροφορικής. Δεν αποτελούν πάντα το σύνηθες κακόβουλο λογισμικό που στοχεύει στην καταστροφή ενός υπολογιστή. Σύμφωνα με μελέτες τα περισσότερα fake software που μπορεί κάποιος να συναντήσει είναι προγράμματα που δίνουν την εντύπωση ότι λειτουργούν σαν τα antiviruses (AV). Στις περισσότερες όμως περιπτώσεις αποτελούν το μέσο κάποιων προγραμματιστών να αποσπάσουν χρηματικά ποσά από ανυποψίαστους χρήστες αφού τους εμφανίζουν μηνύματα, κατά τη διάρκεια της ψευδούς σάρωσης των αρχείων που πραγματοποιούν για να «εντοπίσουν» τους ιούς, τα οποία διαφημίζουν την αγορά ολόκληρων των προϊόντων και όχι μόνο του δοκιμαστικού πακέτου (Free Trial) για να διαγράψουν τους ιούς ή να απελευθερώσουν την λειτουργεία προγραμμάτων που έχουν αποκλειστεί (Douglas Steigerwald, 2011).

Συχνά τα ψευδή λογισμικά παρουσιάζονται με παρεμφερή ονόματα με τα αυθεντικά και προσπαθούν να εξαπατήσουν τους χρήστες ότι είναι τα ίδια. Στο ίδιο πλαίσιο κινείται και η διεπαφή (interface) των fake software καθώς και λογοτύπων που χρησιμοποιούν (Chongbin Tang, 2019).

3.6.6 Dumpster diving

Η αναζήτηση θραυσμάτων πληροφοριών στα απορρίμματα ενός φορέα είναι επίσης μια τακτική η οποία μας αφορά περισσότερο από τις επιθέσεις λογισμικού. Στο πλαίσιο της προστασίας ενός δικτύου, όπως θα γίνει αναφορά παρακάτω, τα κακόβουλα λογισμικά και οι παραπλανητικές ιστοσελίδες δεν θα φτάσουν ποτέ στους χρήστες ακόμα και αν το ζητήσουν στους φυλλομετρητές τους. Όμως οι υπάλληλοι πρέπει να γνωρίζουν ότι πετώντας στα σκουπίδια χαρτιά με πληροφορίες όπως προσωπικά στοιχεία πελατών, επιχειρησιακά πλάνα, αποφάσεις διευθυντών, πληροφορίες λογιστηρίου, ιατροφαρμακευτική περίθαλψη εργαζομένων, memos μπορεί να φανερωθούν σε άτομα εκτός του φορέα. Για να αποφευχθεί μια απώλεια δεδομένων αυτής της μορφής, πρέπει να υπάρχουν αυστηρά πλάνα καταστροφής αρχείων, τόσο αναλογικού όσο και ψηφιακού υποστρώματος (Long, 2007)

3.6.7 Physical access

Ένα ακόμα σημαντικό ζήτημα πρόσβασης σε στοιχεία του φορέα είναι και η ανεξέλεγκτη πρόσβαση ατόμων στους χώρους. Όπως έχει προαναφερθεί οι χώροι του αρχειοστασίου, του αναγνωστηρίου, των υπαλλήλων και οι εφεδρικές εγκαταστάσεις πρέπει να είναι κατάλληλα σχεδιασμένοι και να προστατεύονται από στάδια ελέγχου. Το κομμάτι της ηλεκτρονικής πρόσβασης με βάση ιεραρχικά μοντέλα θα εξεταστεί παρακάτω. Το κομμάτι όμως της πρόσβασης ατόμων σε χώρους που δεν έχουν τη δικαιοδοσία να βρίσκονται αφορά την κλοπή πληροφοριών.

Η πρόσβαση μπορεί να περιοριστεί με σταδιακούς ελέγχους που υπάρχουν σε πύλες που εισέρχονται μόνο άτομα με εξουσιοδότηση. Ο έλεγχος μπορεί να γίνεται από κάρτες που φέρουν μόνιμα μαζί τους οι εργαζόμενοι για να κυκλοφορούν στους χώρους. Οι κάρτες αυτές μπορεί να έχουν barcode, QR code ή να χρησιμοποιούν άλλες τεχνολογίες. Αντί για κάρτες υπάρχει και η εναλλακτική του κινητού με τη χρήση της τεχνολογίας NFC.

Συνήθως με την εφαρμογή σύγχρονων μεθόδων R.B.A.C. σε συνδυασμό με την πληροφόρηση του προσωπικού και την επιβολή κανόνων και κυρώσεων σε περίπτωση μη τήρησης περιορίζεται η πιθανότητα πρόσβασης ανεπιθύμητων στις εγκαταστάσεις του φορέα (Sara Rouhani, 2019)

3.6.8 Shoulder surfing

Μια ματιά ασκαρδαμυκτί και ακροποδητί αρκεί για κάποια άτομα ώστε να καταφέρουν να αποσπάσουν πληροφορίες από κάποιον χρήστη τη στιγμή που εργάζεται. Γίνεται κατανοητό ότι πρόκειται για μια ακόμη τεχνική hacking χωρίς τη

χρήση τεχνολογίας. Η πρακτική shoulder surfing πραγματοποιείται όταν ένα άτομο κοιτά «από τον ώμο» του χρήστη την οθόνη εργασίας του υπολογιστή του με αποτέλεσμα να του φανερώνονται πληροφορίες όπως ονόματα χρηστών (usernames),κωδικοί (passwords), διευθύνσεις ηλεκτρονικού ταχυδρομείου (emails), τηλέφωνα κ.α. Εδώ αξίζει να σημειωθεί ότι η παραπάνω τεχνική μπορεί να εφαρμοστεί πιο εύκολα όταν το θύμα χρησιμοποιεί ακουστικά ή βρίσκεται σε δημόσιο χώρο που δεν ελέγχει αν υπάρχουν άτομα που στέκονται πίσω του παρατεταμένα. Τα παραπάνω στοιχεία μπορούν να χρησιμοποιηθούν όπως προαναφέρετε συνδυαστικά με έμπειρες τακτικές hacking και να έχουν μεγαλύτερη αποτελεσματικότητα, για τους hackers φυσικά (Long, 2007).

3.6.9 Stealing important documents

Η κλοπή δεδομένων από τα γραφεία των υπαλλήλων είναι κάτι που συνήθως συνδυάζεται με την τακτική tailgating, όταν δηλαδή άτομα εκτός του φορέα ακολουθούν τους εργαζόμενους μέχρι τα γραφεία τους χωρίς να γίνουν αντιληπτοί από άλλους. Προφανώς αναφερόμαστε σε σενάρια που δεν υπάρχουν ούτε συστήματα R.B.A.C. ούτε προσωπικό προστασίας του κτιρίου.

Σε περίπτωση λοιπόν που εντός των εγκαταστάσεων δεν υπάρχουν οι κατάλληλες υποδομές και ο αντίστοιχος σχεδιασμός, είναι πιθανό κάποιος να εισβάλλει στο χώρο και να κλέψει έγγραφα ή σκληρούς δίσκους. Αν λοιπόν είναι αδύνατον να τοποθετηθούν τα αρχεία σε ασφαλές σημείο ή υπάρχει πιθανότητα κλοπής από κάποιον συνάδελφο (σκευωρία, προσωπικό κέρδος), καλά είναι να κλειδώνονται τα γραφεία κάθε φορά που αποχωρούν οι υπάλληλοι (Long, 2007).

4 Κεφάλαιο 4ο

4.1 Πλάνο Αντιμετώπισης Καταστροφών – Disaster Recovery Plan

Οι καταστροφές είτε φυσικές είναι είτε τεχνολογικές είναι σχεδόν απίθανο να αποφευχθούν ή να μην προκύψουν ποτέ, βέβαια σε περίπτωση που συμβεί, είναι δυνατόν να υπάρξει μείωση της δράσης τους κατά έναν μεγάλο βαθμό. Αυτός ακριβώς είναι και ο στόχος των πλάνων αντιμετώπισης καταστροφών (disaster recovery plans). Τα πλάνα DRP στοχεύουν, μέσω της έρευνας των ιδιαίτερων συνθηκών, που υπάρχουν πιθανότητες να επηρεάσουν τον φορέα, και της πειθαρχημένης οργάνωσης του προσωπικού, στην άμεση αντίδραση την στιγμή που εκδηλώνεται ένα συμβάν και την μέγιστη δυνατή καταστολή των συνεπειών του.

Συνοψίζοντας το πλάνο πρέπει να διαθέτει τους εξής στόχους:

- Πρόληψη για τους πιθανούς κινδύνους και λήψη μέτρων για την αντιμετώπισή τους
- Ενημέρωση του προσωπικού για τις σχετικές διεργασίες
- Ορισμός συχνότητας ελέγχων του κτιρίου
- Ορισμός απαραίτητων εργαλείων, αποθεμάτων και υλικών που χρειάζονται καθώς και έλεγχος της ετοιμότητάς τους
- Επικοινωνία με σώματα πυροσβεστικής, αστυνομίας για την ενημέρωση και την εξοικείωση με τις εγκαταστάσεις του φορέα
- Ορισμός βασικών παραγόντων που πρέπει να αποκατασταθούν πρωτίστως για την άμεση επαναλειτουργία του φορέα με ομαλούς ρυθμούς
- Ορισμός ομάδας δράσης και υπεύθυνων για την πραγμάτωση του σχεδίου καθώς και τη βελτίωσή του (G. Morgan, 1997).

4.1.1 Εκτίμηση Κινδύνου / Risk Assessment

Η εκτίμηση του κινδύνου θεωρείται η πρώτη κίνηση που πρέπει να υπάρξει προκειμένου να αναπτυχθεί ένα πλάνο αντιμετώπισης καταστροφών. Εκτιμώντας τον κίνδυνο επιτυγχάνεται η συγκέντρωση πληροφοριών σχετικά με τους πιθανούς τρόπους εκδήλωσης των κινδύνων, καθώς και των τρόπων μέσω των οποίων αυτός μπορεί να ελαχιστοποιηθεί. Όλα τα σχέδια καταστροφών περιέχουν πληροφορίες σχετικά με την ετοιμότητα και την πρόληψη, την αντίδραση, την διάσωση και την ανάρρωση.

Το σχέδιο θα πρέπει να ξεκινήσει με μια σύντομη εισαγωγή που θα εξετάζει τους εξής καθοριστικούς παράγοντες:

- Γιατί είναι σημαντικό να έχουμε ένα σχέδιο;
- Ποιους στόχους ελπίζει να επιτύχει το σχέδιο;
- Ποιες βασικές αρμοδιότητες περιγράφει το σχέδιο;
- Ποιες πιθανές καταστάσεις έκτακτης ανάγκης και καταστροφές περιγράφει το σχέδιο;

Αν και δεν μπορούν να προληφθούν όλες οι καταστροφές, το προσωπικό μπορεί να μετριάσει τη ζημία στις συλλογές διενεργώντας εκτιμήσεις κινδύνου για πιθανές καταστροφές ή ζητήματα διατήρησης που μπορούν να βλάψουν τις συλλογές.

Αρχικά κάθε μέλος του προσωπικού πρέπει να γνωρίζει τον οδηγό σχεδίου έκτακτης ανάγκης με τις βασικές πληροφορίες. Επίσης, ο οδηγός θα πρέπει να βρίσκεται σε κάποιο προσβάσιμο μέρος για άμεση πρόσβαση σε περίπτωση έκτακτης ανάγκης. Επιπλέον μέσα στον οδηγό θα πρέπει να αναφέρονται όλα τα παρακάτω:

- Κίνδυνοι έκτακτης ανάγκης (με βαθμούς πιθανότητας εκδήλωσης)
- Διαδικασίες που πραγματοποιούνται σε περιπτώσεις εκτάκτων αναγκών
- Έξοδοι κινδύνου
- Πρώτοι ανταποκριτές έκτακτης ανάγκης (Πυροσβεστική, Αστυνομία, Ασθενοφόρο)

Όπως επίσης θα πρέπει να αναφέρονται και τα κινητά τηλέφωνα των αρμόδιων μελών της ομάδας αντιμετώπισης καταστροφών, δηλαδή:

- Διαχειριστής ομάδας αντιμετώπισης καταστροφών
- Συντονιστής Αποκατάστασης Καταστροφών
- Συντονιστής Συλλογής
- Συντονιστής Εγκαταστάσεων
- Συντονιστής Δημόσιας Ασφάλειας
- Ειδικός αποκατάστασης πληροφορικής
- Συντονιστής Επικοινωνίας
- Εξωτερικοί Σύμβουλοι Καταστροφών

Συμπεραίνουμε λοιπόν με βάση όσα προαναφέρθηκαν, ότι το σχέδιο εκτίμησης κινδύνου (Risk assessments) είναι ζωτικής σημασίας και πως κρίνεται απαραίτητο να δημιουργηθούν καλές σχέσεις εργασίας με τις εγκαταστάσεις, την ασφάλεια και το προσωπικό πυρασφάλειας. Το προσωπικό εγκαταστάσεων πρέπει να είναι πάντοτε σε

ετοιμότητα ώστε σε περίπτωση καταστροφής να βοηθήσει το προσωπικό των αρχείων στην επίλυση αυτών των ζητημάτων διατήρησης.

Η εκτίμηση κινδύνου αποτελεί κεντρική συνιστώσα κάθε σχεδίου καταστροφής. Το προσωπικό θα πρέπει να διεξάγει έρευνες για το κτιριακό περιβάλλον, την αποθήκευση και τις διαδικασίες πυρασφάλειας και του εξοπλισμού. Επιπλέον, όλες οι πιθανές ανθρωπογενείς και φυσικές καταστροφές θα πρέπει να συμπεριληφθούν σε αυτό το τμήμα. (Shepard, 2018)

Η έρευνα εκτίμησης κινδύνου ενδεικτικά πρέπει να περιέχει πληροφορίες σχετικές με τα παρακάτω:

- Εξέταση πιθανών κινδύνων από φυσικές αιτίες
- Εξέταση του σχεδίου του κτηρίου
- Εντοπισμός εστιών μούχλας ή άλλων παρασίτων
- Ανάλυση προηγούμενων περιστατικών
- Δημιουργία τακτικών χρονοδιαγραμμάτων συντήρησης των συστημάτων ψύξης, θέρμανσης και εξαερισμού
- Χρονοδιάγραμμα αναβάθμισης συστημάτων

Προσδιορισμός προληπτικών μέτρων για τον περιορισμό εκδήλωσης των πιθανών ζημιών από καταστροφές:

- Αποθήκευση όλων των κουτιών σε ράφια (dexion) ή παλέτες που δεν είναι απευθείας στο πάτωμα αλλά σε ύψος τουλάχιστον 15 εκατοστών.
- Τα ράφια (dexion) να είναι βιδωμένα στους τοίχους ή στην οροφή.
- Επιλογή κατάλληλου συστήματος καταιονισμού (Σκόνης, Co2, νερού).
- Διατήρηση διαδρόμων ακόμα και σε περίπτωση πτώσης αντικειμένων.
- Τοποθέτηση του αρχειακού υλικού σε αντιόξινα κυτία.
- Πρόβλεψη για τη στατικότητα των ραφιών dexion σε περίπτωση επιπρόσθετου βάρους από χαρτιά που έχουν βραχεί (Artim, 1999)

Για παράδειγμα όταν αναφερόμαστε σε φυσικές καταστροφές (σεισμούς, πλημύρες) η ορθή εκτίμηση μπορεί να αναδείξει και όλα τα πιθανά είδη κινδύνων που μπορεί να συμβούν στη συγκεκριμένη γεωγραφική περιοχή. Είναι εύκολα αντιληπτό πως αν στοχεύουμε στην ορθότερη εκτίμηση κινδύνου θα πρέπει να υπάρχουν συστήματα και μηχανήματα τα οποία θα είναι υπεύθυνα για την πρόβλεψη των πιθανών κινδύνων που μπορεί να συμβούν. (Πανεπιστήμιο Πατρών, 2005)

4.1.2 Σύστημα παρακολούθησης & Ελέγχου

Το αμέσως επόμενο και εξίσου σημαντικό στάδιο για την επίτευξη δημιουργίας ενός ορθού πλάνου πρόληψης καταστροφών, είναι η δημιουργία ενός συνεχούς συστήματος παρακολούθησης και ελέγχου. Αφού εκτιμηθεί ο κίνδυνος και κριθούν οι απαραίτητες αποφάσεις για τη σύστασή του κτιρίου και κατ' επέκτασίν των συστημάτων συναγερμού που θα υπάρχουν μέσα σε αυτό, ώστε να επιτευχθεί το καλύτερο δυνατό αποτέλεσμα. Επιπλέον πρέπει να τονιστεί ότι το κτήριο θα πρέπει να συντηρείται σε τακτά χρονικά διαστήματα και άμεσα κάθε φορά που προκύπτει κάποια βλάβη ώστε όλα τα συστήματα να είναι απολύτως λειτουργικά. (Γιαννακόπουλος Γ. , 2015)

Η Επανεξέταση του εξοπλισμού πυρασφάλειας όσον αφορά την ανθρώπινη ασφάλεια. Το κτίριο θα πρέπει να έχει όλα αυτά τα συστήματα πυροπροστασίας. εξόδους κινδύνου, κουμπιά έλξης, ανιχνευτές καπνού, ψεκαστήρες, πυροσβεστήρες και ηχητικούς συναγερμούς. Είναι ιδιαίτερα σημαντικό να συνδεθεί το σύστημα συναγερμού πυρκαγιάς με την τοπική πυροσβεστική υπηρεσία. (Shepard, 2018)

Έπειτα από μια καταστροφική απώλεια οι αρχειονόμοι πρέπει να είναι απόλυτα ενημερωμένοι αναφορικά με τα μέσα πρόληψης που διαθέτουν καθώς και τις πιθανές παρενέργειες που ενδεχομένως να επιφέρουν. Για παράδειγμα σε περίπτωση φωτιάς η χρήση συστήματος καταιονισμού (sprinklers) για κατάσβεση ενδέχεται να βρέξει τα χαρτιά ή τα υπολογιστικά μέσα προκαλώντας ζημιές, ίσως και ανεπανόρθωτες. Αντίστοιχα η διαδικασία ανάκτησης αρχειακού υλικού που έχει βραχεί με τη μέθοδο της ψύχρανσης ενδέχεται να μετατρέψει τα φύλλα χαρτί σε μια ενιαία μάζα, αν δεν υπάρχει σε ταυτόχρονη λειτουργεία σύστημα αφύγρανσης (Echezona, 2012).

Παρακάτω αναφέρονται μερικά αναγκαία συστήματα εξοπλισμού για τους χώρους φύλαξης των αρχείων:

- συστήματα ανίχνευσης πυρκαγιάς
- συστήματα ανίχνευσης καπνού
- συστήματα καταιονισμού (sprinklers)
- πυροσβεστήρες (και εκπαίδευση του προσωπικού στον τρόπο χρήσης τους)
- συσκευές ανίχνευσης νερού
- γεννήτρια έκτακτης ανάγκης και καύσιμα
- αφυγραντήρες

Έκτακτη ανάγκη αποθεμάτων προμήθειες και εξοπλισμός:

- δοχεία και υλικό συσκευασίας για τη μετεγκατάσταση αντικειμένων

- εφεδρική γεννήτρια και επιπλέον καύσιμα
- υγρές/ξηρές σκούπες
- πυροσβεστήρες
- ανεμιστήρες δαπέδου
- καρότσια
- καταψύκτες
- φακοί και μπαταρίες
- νερό και ξηρά τροφή για το προσωπικό
- κάμερες, φιλμ, στυλό, χαρτί και άλλα στοιχεία για τεκμηρίωση (Dorge, 1999)
- μπότες και ποδιές από υλικά που δεν αποτελούν αγωγούς ηλεκτρισμού
- πλαστικές στολές
- γάντια
- σακίδια πρώτων βοηθειών
- πλαστικά γυαλιά και μάσκες (τύπου N,R, P-95)
- εργαλεία (πένσες, κατσαβίδια, σφυριά, πριόνια) (Minnesota Historical Society, 2007)

Από μελέτες έχει φανεί ότι αντίστοιχοι φορείς διαθέτουν μέσα προστασίας από τον παράγοντα της πυρκαγιάς όπως πυροσβεστήρες (94,1%), ανιχνευτές καπνού (70,6%), ηχητικοί συναγερμοί (91,2%), συναγερμοί με διακόπτες γυαλιού (82,4%), συστήματα καταιονισμού (73,5%), φώτα ασφαλείας και σηματοδότες εξόδου (61,8%), τακτική συντήρηση κτιρίου (76,5%). Μέσα από τα ποσοστά αποκαλύπτεται ότι δεν υπάρχει πάντα πληρότητα και συνέπεια στα μέσα προστασίας κάτι που σημαίνει ότι σε μια κατάσταση ανάγκης η ετοιμότητα του φορέα μπορεί να φανεί ανεπαρκής. Επίσης από το παραπάνω παράδειγμα φαίνεται ότι η πρόληψη για πιθανή πλημμύρα είναι ανύπαρκτη. Συμπερασματικά δεν είναι λίγοι οι φορείς που δεν πραγματοποιούν έρευνα για εκτίμηση κινδύνου ενώ ταυτόχρονα δεν συγκροτούν ομάδες αντιμετώπισης. Υπάρχει ακόμα σε κάποιον βαθμό αμφισβήτηση στο κατά πόσον είναι αναγκαίο να πραγματοποιηθούν ποσοτικοποιημένες εκτιμήσεις κινδύνου και να ληφθούν μέσα προστασίας κυρίως λόγο του κόστους που επιφέρει η διαδικασία, του χρόνου που είναι αναγκαίο να διοχετευθεί καθώς και του επιπλέον χώρου για τη διατήρηση υλικών και μέσων προστασίας (Khalid, 2015).

Επιπλέον άλλα προτεινόμενα μέσα προστασίας είναι οι κουβάδες άμμου, πλαστικά καλύμματα για προστασία υλικών από τον ψεκασμό νερού ή κατάλληλα καλύμματα για τον περιορισμό παροχής οξυγόνου και ο εξοπλισμός αντιμετώπισης πυρκαγιάς όπως

σκάλες, πριόνια και εργαλεία διάνοιξης. Επίσης πρέπει να σημειωθεί ότι μια φωτιά μπορεί να γίνει αντιληπτή και από το κλειστό κύκλωμα παρακολούθησης (CCTV).

Αξιοσημείωτο είναι το γεγονός ότι μικρά περιστατικά όπως διαρροή σωλήνων και ελαττωματικές ηλεκτρικές συνδέσεις μπορεί να προκαλέσουν σοβαρές ζημιές στο φορέα και να οδηγήσουν ακόμα και στη διακοπή της λειτουργείας του. Ως εκ τούτου, η ομάδα που είναι υπεύθυνη για τις καταστροφές του αρχείου θα πρέπει πάντα να διενεργεί με μέριμνα τον έλεγχο των εγκαταστάσεων, να εξασφαλίζει ότι επισκευάζονται σύντομα οι βλάβες και ότι υπάρχει πρόσβαση στα απαραίτητα εργαλεία που απαιτούνται για την πραγματοποίηση των πρώτων βημάτων του σχεδίου εκτάκτων αναγκών και ανάκλησης, ακόμα και πριν φτάσουν στο χώρο οι κατάλληλες αρχές. (Ilo, 2018)

4.1.3 Εκπαίδευση υπαλλήλων

Για την ύπαρξη ενός πραγματικά ορθού πλάνου διαχείρισης καταστροφών στους αρχειακούς χώρους, θα πρέπει και οι υπάλληλοι να γνωρίζουν τι ακριβώς πρέπει να συμβεί σε τέτοιες περιπτώσεις. Σε ορισμένους μάλιστα φορείς, υπάρχουν ομάδες υπαλλήλων οι οποίες εκπαιδεύονται στην διαχείριση τέτοιων περιστάσεων. Μέσω της ορθής εκπαίδευσης και ενημέρωσης των υπαλλήλων οι υπεύθυνοι των σχεδίων εκτάκτων αναγκών προλαμβάνουν τους κινδύνους με αποτέλεσμα να μειώνεται η επίδρασή τους και να περιορίζονται οι εργασίες διάσωσης που πρέπει να λάβουν χώρα. Οι υπάλληλοι δηλαδή θα πρέπει να γνωρίζουν κάποιους κανόνες πρόληψης προστασίας αρχικά των ίδιων, αλλά και των τεκμηρίων. Χρειάζεται χρόνος και χρηματικό κεφάλαιο για την εκπαίδευση του προσωπικού. Τα πλεονεκτήματα όμως είναι πολλά καθώς σε μια περίπτωση ανάγκης οι γνώσεις του προσωπικού θα αποβούν χρήσιμες και θα περισώσουν μέρος της ζημίας που αφήνει ανοιχτό το ενδεχόμενο της κατάρρευσης του φορέα (Kostagiolas, 2011). Παρακάτω παρατίθενται κάποια συγκεκριμένα παραδείγματα για την ανάγκη εκπαίδευσης του προσωπικού:

Στην περίπτωση των τεκμηρίων χάρτινου υποστρώματος οι υπάλληλοι θα πρέπει να φοράνε γάντια και στολές όσοι ασχολούνται με τα ίδια τα τεκμήρια ώστε να μην υπάρξει κίνδυνος και για την υγεία των ίδιων αλλά και για την ευαισθησία των τεκμηρίων. (Albright, 1999)

Επίσης στην περίπτωση των ηλεκτρολογικών συστημάτων, τα μέτρα προστασίας είναι διαφορετικά. Οι υπάλληλοι θα πρέπει μην έχουν σε κοντινή απόσταση εκτεθειμένα υγρά καθώς η επαφή τους με ηλεκτρονικά και ηλεκτρολογικά συστήματα μπορεί να

προκαλέσει ηλεκτροπηξία, βραχυκυκλώματα ή ακόμη και πυρκαγιά (Graham Matthews, 1996).

Οι υπάλληλοι που βρίσκονται στο κομμάτι της συσκευασίας και της μεταφοράς των αρχείων θα πρέπει επίσης να χρησιμοποιούν στολές και γάντια με στόχο την προστασία των τεκμήριών . Θα πρέπει να χρησιμοποιούν συσκευασίες με κατάλληλες προδιαγραφές, από άποψη χημικής σύνθεσης, αλλά και να τοποθετούν θήκες γύρω από τα αντικείμενα με σκοπό την μέγιστη προστασία τους. Εδώ να σημειωθεί ότι υπάρχουν δύο κατηγορίες υπαλλήλων που εργάζονται σε αυτό το κομμάτι της επιχείρησης. Οι πρώτοι είναι οι αρχειονόμοι που μεταφέρουν τα αρχεία εντός του φορέα για π.χ. από το αρχειοστάσιο στο αναγνωστήριο. Ενώ οι δεύτεροι είναι εκείνοι που μεταφέρουν το αρχείο από το αρχειοστάσιο στην εταιρεία, επειδή δεν βρίσκονται στο ίδιο κτήριο τα γραφεία. Η μεταφορά αυτή συνήθως γίνεται με οχήματα, αφού τα αρχεία έχουν τοποθετηθεί σε κατάλληλες κούτες οι οποίες είναι καλά να είναι επαναχρησιμοποιήσιμες.

Σε κάθε περίπτωση όμως θα πρέπει να δημιουργηθεί μία ομάδα διαχείρισης κρίσεων, η οποία θα είναι έτοιμη να παρέμβει όταν παρουσιαστεί ανάγκη. Επιπλέον θα πρέπει να υπάρξει μία στρατηγική η οποία θα κατευθύνει και τους υπόλοιπους εργαζομένους. Αυτή η ομάδα θα πρέπει να απαρτίζεται από άτομα που βρίσκονται σε διαφορετικούς τομείς της επιχείρησης και διαθέτουν διαφορετικές αρμοδιότητες. (Μπάγιας, 1999)

Η ομάδα αντιμετώπισης των καταστροφών είναι υπεύθυνη για τα περισσότερα αρχεία, τα οποία είναι μέρος ενός μεγαλύτερου οργανισμού. Ο μητρικός οργανισμός μπορεί να είναι μια εταιρεία, κυβερνητική υπηρεσία, κολέγιο ή πανεπιστήμιο, μη κερδοσκοπικός οργανισμός, μουσείο ή βιβλιοθήκη. Κάθε σχέδιο διαχείρισης καταστροφών θα πρέπει να προσαρμόζεται στις ανάγκες αυτού του οργανισμού. Όταν η ομάδα οργανώνει το δικό της σχέδιο, το προσωπικό των αρχείων μπορεί να χρειαστεί να εξετάσει τη θεσμική του ιεραρχία. Σε ένα μικρό αρχειακό ίδρυμα, το σχέδιο καταστροφής μπορεί να συνταχθεί από ένα άτομο, ενώ σε μεγαλύτερο οργανισμό, μπορεί να συνταχθεί από μια επιτροπή.

Τέλος ας μην ξεχνάμε την ανάγκη εκπαίδευσης του προσωπικού στους πιθανούς κινδύνους που εγκυμονεί το διαδίκτυο καθώς και στις πιθανές μεθόδους εισβολής στο υπολογιστικό σύστημα που περιέχει τα ψηφιακά αρχεία του φορέα. Οι «παγίδες» που υπάρχουν στο χώρο του διαδικτύου μπορεί να μην είναι εμφανείς και να πείθουν με την αληθοφανή γνησιότητάς τους. Όμως όπως θα δούμε και σε επόμενο κεφάλαιο το προσωπικό πρέπει να γνωρίζει τους παράγοντες από τους οποίους κινδυνεύει.

4.1.3.1 Ομάδα Διαχείρισης Εκτάκτων αναγκών

Όλα τα σχέδια αντιμετώπισης καταστροφών περιέχουν πληροφορίες σχετικά με την ετοιμότητα, την πρόληψη, την αντίδραση, τη διάσωση και την ανάκτηση (Shepard, 2018) . Από τη βιβλιογραφία είναι προτεινόμενο να υπάρχει ένα άτομο επιφορτισμένο με τη διεκπεραίωση του σχεδίου DRP. Με αυτό τον τρόπο θα μοιράζονται και θα εκτελούνται με συνέπεια και αξιοπιστία οι επιμέρους εργασίες στα άτομα που συναποτελούν την ειδική επιτροπή. Είναι λοιπόν απαραίτητο να γίνει μια ανάλυση σχετικά με τον ρόλο του διαχειριστή ετοιμότητας έκτακτης ανάγκης.

- Ο διαχειριστής θα πρέπει να συμβάλει στη δημιουργία ενός περιβάλλοντος στο οποίο η ετοιμότητα και η αντιμετώπιση καταστάσεων έκτακτης ανάγκης θα λαμβάνονται σοβαρά υπόψη
- Να ηγηθεί μέσω της διαδικασίας συλλογής των πληροφοριών που απαιτούνται ώστε να συντάξει ένα σχέδιο έκτακτης ανάγκης
- Να συνεργασθεί με την υπόλοιπη ομάδα για τον ορισμό συντονιστή αντιμετώπισης καταστάσεων έκτακτης ανάγκης
- Να συνεργαστεί με την υπόλοιπη ομάδα για να ξεκινήσει ένα εκπαιδευτικό πρόγραμμα που βοηθά το προσωπικό
- Να ενημερώνει το διοικητικό προσωπικό για τα σχετικά θέματα

Στο πλαίσιο της διατύπωσης ενός σχεδίου DRP από το διαχειριστή πρέπει να λαμβάνονται υπόψιν δεδομένα που θα συλλεχθούν από διάφορους φορείς και επιστημονικούς κλάδους. Ξεκινώντας από τις απαιτούμενες προδιαγραφές, που θα αναφερθούν και παρακάτω, μέχρι και τις μετρήσεις από γεωλόγους και μετεωρολόγους για την κατανόηση των πιθανών καταστροφών που μπορεί ανακύψουν ο διαχειριστής (Emergency Preparedness Manager) είναι αναγκαίο να συνδυάσει όσο το δυνατόν περισσότερους παράγοντες. Επίσης συμβουλές μπορεί να παράσχουν και οι εμπειρογνώμονες από τοπικά σώματα όπως αστυνομία, πυροσβεστική και νοσοκομεία.

Ο διαχειριστής (EPM) έπειτα από την αρχική διαμόρφωση του σχεδίου εκτάκτων αναγκών και ανάκτησης κρίνεται αναγκαίο να ορίσει επιτροπή για τις επιμέρους εργασίες (συντήρησης-επίβλεψης, εφαρμογής, επικοινωνίας με το κοινό, ασφάλειας). Η επιτροπή (Emergency Preparedness Committee) είναι καλά να ξεκινάει με την εκπόνηση απλών εργασιών για να επιτευχθεί το πνεύμα συνεργασίας μεταξύ των ατόμων.

Το άτομα που τελεί χρέη διαχειριστή, είναι καλό να διαθέτει εμπειρία σε θέματα σχετικά με DRP καθώς και ικανότητες ηγεσίας και οργάνωσης. Από την πλευρά του ο διαχειριστής (EPM) πρέπει να οργανώνει εβδομαδιαίες συναντήσεις με την επιτροπή και

να αναθέτει εργασίες στα μέλη. Στο πλαίσιο της άρτιας λειτουργείας της επιτροπής πρέπει να υπάρχουν κανόνες, χρονικά περιθώρια παράδοσης των διαφόρων εργασιών, ενώ σε κάποιες περιπτώσεις κρίνεται αναγκαίο να ξεκαθαρίζεται και το περιθώριο απουσιών από τις συνελεύσεις αυτές.

Μια επιτροπή με μέλη που σέβονται τον φορέα και ενδιαφέρονται για την άρτια λειτουργεία του παρατηρούν σε πρακτικό και καθημερινό επίπεδο τη λειτουργεία του DRP συλλέγοντας χρήσιμες πληροφορίες που όταν έρχονται στην επιφάνεια μπορούν να βελτιώσουν το σχέδιο. Εποικοδομητικά σχόλια προς τα μην ΕΡΟ έχουν πάντα θετικό αντίκτυπο και μπορούν να διατυπωθούν από την επίτευξη μηνιαίων στόχων (Dorge, 1999).

4.1.4 Σχέδιο έκτακτης ανάγκης – Εκκένωση χώρων εργασίας

Για την προστασία εργαζομένων και κοινού είναι αναγκαίο να υπάρχει ένα σχέδιο με τις αναγκαίες δράσεις για την αντιμετώπιση μιας πυρκαγιάς και την εκκένωση των χώρων εργασίας. Ιδιαίτερη μέριμνα πρέπει να υπάρχει για την προστασία ΑμεΑ και ευαίσθητων ομάδων πληθυσμού όπως:

- Ηλικιωμένων ατόμων που αντιμετωπίζουν προβλήματα υγείας και για άτομα που δεν γνωρίζουν τη γλώσσα και τα σήματα κινδύνου που χρησιμοποιούνται (μετανάστες, πρόσφυγες) και μπορεί να βρίσκονται στον χώρο.

- Οι εργαζόμενοι πρέπει να είναι ενημερωμένοι και να εκπαιδεύονται κατάλληλα, ανάλογα με τη φύση των κινδύνων και το σχέδιο έκτακτης ανάγκης, στη χρήση πυροσβεστικών μέσων και, γενικότερα, στις ενέργειες αντιμετώπισης εκτάκτων περιστατικών.

Το σχέδιο διαφυγής και διάσωσης από τους χώρους εργασίας, εφόσον απαιτείται από τη θέση, την έκταση και το είδος της εκμετάλλευσης. Το σχέδιο διαφυγής και διάσωσης πρέπει να αναρτάται σε κατάλληλες θέσεις στους χώρους εργασίας. Το σχέδιο πρέπει να δοκιμάζεται τακτικά, με ασκήσεις ή άλλο πρόσφορο τρόπο, ώστε σε περίπτωση κινδύνου ή καταστροφής να μπορούν οι εργαζόμενοι να διασωθούν. Γενικά, επιβάλλεται η **ανάρτηση σχεδιαγραμμάτων διαφυγής και διάσωσης** στα κτήρια που η κύρια χρήση τους αναπτύσσεται σε τρεις (3) ή περισσότερους ορόφους και τα οποία έχουν συνολικό πληθυσμό πάνω από διακόσια (200) άτομα, καθώς και όπου προβλέπεται από τις ιδιαίτερες ανάγκες τις γεωγραφικής περιοχής, ανά χρήση κτηρίου. Σε κάθε περίπτωση η ύπαρξη και ανάρτηση σχεδιαγράμματος διαφυγής και διάσωσης

αποτελεί μια καλή πρακτική για τον χώρο εργασίας. Για την ασφαλή και αποτελεσματική εκκένωση των χώρων εργασίας:

- Διατηρούνται συνεχώς ελεύθερες οι οδοί διαφυγής και η έξοδος/οι έξοδοι κινδύνου.
- Οι θύρες/η θύρα κινδύνου πρέπει να ανοίγουν/-ει προς τα έξω, περιορίζοντας έτσι τον κίνδυνο εγκλωβισμού και τραυματισμού κατά τη φάση της εκκένωσης.
- Οι θύρες/η θύρα κινδύνου δεν πρέπει να είναι κλειδωμένες.
- Πρέπει να υπάρχει κατάλληλος φωτισμός ασφαλείας (είτε με μπαταρίες είτε με ρεύμα γεννήτριας για τις περιπτώσεις διακοπής ρεύματος).
- Οι οδεύσεις διαφυγής και οι έξοδοι κινδύνου θα πρέπει να φέρουν την κατάλληλη σήμανση για να μπορούν να εντοπίζονται άμεσα σε έκτακτες καταστάσεις.

4.1.5 Στάδιο Αντίδρασης & Ανάκτησης

Το στάδιο αντίδρασης αναφέρεται στην περίπτωση που ο φορέας έχει ήδη προετοιμαστεί για τα σενάρια μιας πιθανής της καταστροφής, φυσικής ή ηλεκτρονικής και πρέπει να αντιδράσει σε αυτό. Αφού ο φορέας υποστεί κάποια καταστροφή, οι υπεύθυνοι υπάλληλοι θα πρέπει να δράσουν έτσι ώστε η καταστροφή να περιοριστεί στο μικρότερο δυνατό επίπεδο. Σε αυτό το στάδιο η επιτροπή διαχείρισης κρίσης αναλαμβάνει να εκτελέσει το DRP.

Αρχικά πρέπει να υπάρχει μία σειρά από διεργασίες που θα βοηθούν στη διαχείριση της κρίσης. Το βασικότερο είναι η επικοινωνία μεταξύ των στελεχών της επιχείρησης, αλλά και ο διαμερισμός των αρμοδιοτήτων για τον κάθε υπάλληλο ώστε να αντιμετωπιστεί πλήρως η καταστροφή. Επιπλέον, πρέπει να γίνει μια εκτίμηση του πλήγματος με βάση τον οικονομικό παράγοντα (cost-evaluation). Επίσης είναι φανερό πως σε τέτοιου είδους περιπτώσεις τα μέλη ολόκληρης της επιχείρησης πρέπει να βρίσκονται σε ασυνεχή επικοινωνία έτσι ώστε όλες οι νέες πληροφορίες να ανταλλάσσονται.

Επιπροσθέτως στο πλαίσιο της αντίδρασης εντάσσεται η πρακτική εφαρμογή που έχει δεχτεί το προσωπικό στις διάφορες εκπαιδεύσεις που δέχονται ανά διαστήματα στο πλαίσιο του DRP. Με άλλα λόγια το προσωπικό πρέπει να γνωρίζει που βρίσκονται τα υλικά και τα εργαλεία για τα πρώτα στάδια της αντιμετώπισης μιας κρίσης. Για παράδειγμα όταν ξεσπάσει μια φωτιά τα μέλη της επιτροπής (EPC) πρέπει να γνωρίζουν που ακριβώς βρίσκονται οι πυροσβεστήρες, οι κάδοι με την άμμο, τα πριόνια, καρότσια και τα υπόλοιπα εργαλεία. Παρομοίως σε μια πλημμύρα χρειάζεται να είναι σε ετοιμότητα για να χρησιμοποιήσουν φτυάρια, πλαστικές ποδιές και προστατευτική

ενδυμασία, καλύμματα για τον περιορισμό της καταστροφής ευάλωτων υλικών, ηλεκτρομονωτικά γάντια για την αποφυγή ηλεκτροπληξίας κ.ο.κ. (Graham Matthews, 1996).

Τέλος, η επικοινωνία δεν θα πρέπει να αφορά μονάχα την ανταλλαγή των πληροφοριών αλλά και την ψυχολογική καθησύχαση των εργαζομένων της επιχείρησης καθώς σε τέτοιες καταστάσεις προκύπτουν διάφορα συναισθήματα όπως είναι ο φόβος και το άγχος, λόγω των διαφορετικών συνθηκών που καλούνται να αντιμετωπίσουν, καθώς και σε κάποιες περιπτώσεις η αβεβαιότητα για το τι θα συμβεί τη δεδομένη στιγμή ή στην πορεία της αντιμετώπισης. (ΣΒ. Καρουμπάκου, 2017)

Το στάδιο ανάκτησης θεωρείται ένα δύσκολο στάδιο για τους φορείς. Αυτό προκύπτει εξαιτίας του πλήγματος που δέχεται η επιχείρηση σε όλα της τα μέρη. Ο φορέας θα πρέπει να έχει προνοήσει για τέτοιες καταστάσεις ώστε να υπάρχουν πρακτικά σχέδια τα οποία θα φροντίσουν η επιχείρηση να επανέλθει. Αυτό όμως είναι κάτι που θα χρειαστεί χρόνο εξαιτίας του όγκου των τεκμηρίων που πρέπει να ανακτηθούν. Το στάδιο αυτό ολοκληρώνεται μόνο όταν η φορέας αποκατασταθεί πλήρως και λειτουργεί όπως πρώτα. (Γιαννακόπουλος Γ. , 2015) Είναι επίσης σημαντικό στο πλαίσιο της ανάκτησης να γίνεται καταγραφή των ζημιών και των αιτιών που τις προκάλεσαν διότι σε μεταγενέστερο χρονικό διάστημα μπορούν να χρησιμοποιηθούν για έρευνα βελτίωσης του DRP (DURHAM CIVIL CONTINGENCIES UNIT, 2002).

Έχει παρατηρηθεί ότι στο πλαίσιο μιας καταστροφής μεγάλου μεγέθους οι αρχές και τα σώματα ασφαλείας αδυνατούν να εξυπηρετήσουν τους μεγάλους φορείς καθώς σε προτεραιότητα βρίσκονται τα άτομα που έχουν πληγεί. Για τον παραπάνω λόγο στο στάδιο της ανάκτησης είναι αναγκαίο να υπάρχει πρόβλεψη για καταστολή των παραγόντων που επηρεάζουν τη λειτουργεία του φορέα από τα μέλη του προσωπικού. Υπό την προϋπόθεση ότι οι εργαζόμενοι έχουν τη δυνατότητα να εργαστούν, στο πλαίσιο μιας μεγάλης καταστροφής, πρωταρχική ανάγκη που θα προκύψει για την οργάνωση των εργασιών είναι η επικοινωνία. Επίσης η επικοινωνία με τον τύπο και τα τηλεοπτικά κανάλια που προβάλλουν το πρόσωπο του φορέα δημόσια, διαδραματίζει σημαντικό ρόλο στο πλαίσιο της ανάκτησης (Adrienne Muir, 2002).

Ένα αποτελεσματικό σύστημα επικοινωνιών αποτελεί σημαντικό και δυσεπίλυτο ζήτημα κατά την προετοιμασία για καταστάσεις έκτακτης ανάγκης ή καταστροφές. Μια ομάδα επικοινωνίας πρέπει να είναι προετοιμασμένη ώστε:

- να επιβλέπει όλες τις εξωτερικές επικοινωνίες κατά τη διάρκεια έκτακτης ανάγκης
- να διασφαλίζει τη δημιουργία σαφούς εσωτερικού συστήματος επικοινωνιών

- να συγκεντρώσει και να συντονίσει τις πληροφορίες για τη διάδοση μέσω των μέσων ενημέρωσης
- να συγκεντρώσει και να διαδώσει τις εισερχόμενες πληροφορίες σχετικά με την κατάσταση έκτακτης ανάγκης στην περιοχή
- να λειτουργεί ως σύνδεσμος με εξωτερικούς οργανισμούς και την κοινότητα
- να λειτουργεί ως σύνδεσμος με τις οικογένειες των εργαζομένων και των επισκεπτών
- να ενημερώσει τους χορηγούς ή/και άλλα ιδρύματα σχετικά με την κατάσταση των ζημιών και την εξέλιξη του σχεδίου της ανάκτησης
- να επικοινωνήσει με τους ασφαλιστικούς πράκτορες, τους δικηγόρους, διαχειριστές, αστυνομικά τμήματα, υπηρεσίες έκτακτης ανάγκης και μέσα ενημέρωσης
- να ενημερώσει το προσωπικό και τους διαχειριστές σχετικά με τη διαδικασία ετοιμότητας
- να ενημερώσει τα μέλη του προσωπικού σχετικά με τους ρόλους τους κατά τη διάρκεια έκτακτης ανάγκης

Ένα αποτελεσματικό σχέδιο επωφελείται σε μεγάλο βαθμό από την ευρεία και αποτελεσματική επικοινωνία κατά τη διάρκεια της διαδικασίας σχεδιασμού – τόσο εσωτερικά όσο και με εξωτερικά ιδρύματα, όπως οι υπηρεσίες έκτακτης ανάγκης και τα μέσα ενημέρωσης. Ομοίως, μια αποτελεσματική απάντηση στην καταστροφή απαιτεί από όλα τα πρόσωπα να γνωρίζουν το σχέδιο του ιδρύματος και τον ρόλο τους σε αυτό.

Πώς δίνονται οι πληροφορίες που χρειάζονται οι ομάδες:

- Προγραμματισμός παρουσιάσεων από εξωτερικούς εμπειρογνώμονες
- Ανακοίνωση και ανάρτηση στον χώρο της επιχείρησης
- Προβολή βίντεο με προσομοίωση πραγματικών καταστροφών
- Εργαστήρια με πρακτική εφαρμογή μεθόδων ανάκτησης
- Δοκιμαστικά σενάρια καταστροφών για εξομοίωση(πρακτική εφαρμογή και αντιμετώπιση πιο ρεαλιστικών προβλημάτων π.χ. σε κατάσταση πλημμύρας δεν μετακινούμε βαριά πράγματα σε περίπτωση που δεν μπορούμε να τα σηκώσουμε με ευκολία)

Οι περισσότεροι φορείς δημόσιοι αλλά και ιδιωτικοί ορίζουν κάποιον συντονιστή επικοινωνίας ώστε να είναι υπεύθυνός για όλες τις ερωτήσεις και απαντήσεις σχετικά με τα θέματα που οι υπάλληλοι καλούνται να αντιμετωπιστούν σε περίπτωση κινδύνου. Να

παρέχει δηλαδή πληροφορίες αναφορικά με την λήψη εξωτερικών πληροφοριών ανάλογα με τις ανάγκες κατά τη διάρκεια έκτακτης ανάγκης.

Σε κατάσταση έκτακτης ανάγκης, οι βασικές αρμοδιότητες του συντονιστή επικοινωνιών είναι να εκτελεί ή να εποπτεύει τα ακόλουθα:

- Συγκέντρωση και συντονισμός πληροφοριών για τη διάδοση μέσω των ΜΜΕ
- Συγκέντρωση και διάδοση πληροφοριών από εξωτερικές πηγές, αναφορικά με την έκταση της έκτακτης ανάγκης της ευρύτερης περιοχής του φορέα
- Αξιολόγηση της ακρίβειας των πληροφοριών
- Συντονισμός δελτίων τύπου από τις δημόσιες αρχές, όπως πυροσβεστικές αστυνομικά τμήματα και πολιτική προστασία
- Να κρατά το προσωπικό, τους επισκέπτες και την κοινότητα ενημερωμένα
- Να ενημερώνει τα μέσα ενημέρωσης και να διατηρεί τον έλεγχο των δημοσιεύσεών τους
- Να κρατά αρχείο καταγραφής όλων των πληροφοριών πολυμέσων που έχουν κυκλοφορήσει
- Να προσελκύσει χορηγούς καθώς και τη δημόσια στήριξη (Dorge, 1999).

4.2 Γεωγραφική τοποθεσία

Η τοποθεσία του αρχειακού φορέα διαδραματίζει καθοριστικό ρόλο στο πλαίσιο του πλάνου εκτάκτων αναγκών. Μέσα από μια ανάλυση του τόπου και του χώρου μπορεί να αποφευχθεί ένα σημαντικό μέρος των ενδεχόμενων κινδύνων. Τα βασικά κριτήρια που πρέπει να ελέγχονται πριν την επιλογή της τοποθεσίας είναι τα εξής:

- Αν βρίσκεται κοντά σε ποτάμια υπάρχει πιθανότητα πλημμύρας
- Αν βρίσκεται κοντά σε δάσος υπάρχει πιθανότητα πυρκαγιάς από φωτιά που μπορεί να ξεσπάσει στα δέντρα
- Αποφυγή ανέγερσης κτιρίου σε πολυκατοικημένη περιοχή, καθιστά πιο δύσκολη την μεταφορά των αρχείων στην μητρική εταιρεία ενώ εντείνονται οι πιθανότητες να βρίσκεται ευάλωτο σε εξεγέρσεις και εμπρησμούς
- Εξασφάλιση τοποθεσία που τηρούνται οι φυσικές προδιαγραφές, π.χ. αποφυγή τοποθέτησης σε παραθαλάσσια περιοχή που έχει επιχωματωθεί ή σε περιοχή που έχουν πραγματοποιηθεί αντίστοιχα έργα πάνω σε χείμαρρους και ρυάκια (Dorge, 1999)
- Αποφυγή βιομηχανικών ζωνών

- Αποφυγή περιοχών με διυλιστήρια και σταθμού παραγωγή ηλεκτρισμού (Καρεκλάς, 2016)
- Αποφυγή τοποθέτησης κοντά σε πολυσύχναστους δρόμους. Αξίζει να σημειωθεί ότι ένας αρχειακός φορέας πρέπει να βρίσκεται αφενός σε επαρκή απόσταση από αυτοκινητοδρόμους αλλά αφετέρου να είναι εύκολα προσβάσιμος τόσο από τους επισκέπτες όσο και από φορτηγά μεταφοράς (Jaffer Kabir Najar, 2021)
- Αποφυγή περιοχών κοντά σε αεροδρόμια, σιδηροδρομικούς σταθμούς και εμπορικά κέντρα (Varlamoff, 2005)

Για να εξασφαλιστεί ο υγιής χώρος εργασίας και ταυτοχρόνως οι κατάλληλες προδιαγραφές για την ύπαρξη αρχείων είναι αναγκαίο να υπάρξει σχετική μελέτη και για την τοποθέτηση του κτιρίου. Με άλλα λόγια η συνήθης πρακτική που ακολουθείται είναι να αποφεύγονται σημεία που βρίσκονται κοντά σε ποτάμια και χείμαρρους για να περιορίζονται τα σενάρια εκδήλωσης πλημμυρών μετά από έντονες βροχές. Αντίστοιχα αρχειακοί φορείς δεν βρίσκονται κοντά σε βιομηχανικές ζώνες ή σταθμούς παραγωγής ηλεκτρικής ενέργειας ή καυσίμων (διυλιστήρια) για να αποφεύγονται οι ρύποι και η σκόνη που επηρεάζουν το χαρτί και τα υπόλοιπα αναλογικά υποστρώματα, καθώς και η πιθανότητες έντονης πυρκαγιάς. Για τον ίδιο λόγο τα αρχεία δεν βρίσκονται κοντά σε αυτοκινητοδρόμους (παράγοντας ηχορύπανσης) και δασικές εκτάσεις (Jaffer Kabir Najar, 2021).

Είναι προφανές ότι με την σωστή επιλογή της περιοχής για την ανέγερση του κτιρίου μπορούμε να περιορίσουμε σημαντικά τις πιθανότητες εκδήλωσης κάποιων καταστροφών.

4.2.1 Κτιριακός Σχεδιασμός

Το σχέδιο του κτιρίου που προορίζεται για να στεγάσει τον αρχειακό φορέα πρέπει να φέρει προδιαγραφές που να καλύπτουν όσο το δυνατόν περισσότερα κριτήρια προστασίας του αρχειακού υλικού ανεξαρτήτου υποστρώματος και αποφυγής ενδογενών παραγόντων καταστροφών (ηλεκτρολογικές βλάβες, κατάρρευση χώρων του κτιρίου κ.α.). Τα κρισιμότερα κριτήρια που πρέπει να πληροί ένα κτίριο είναι τα εξής:

- Επάρκεια αποθηκευτικών χώρων
- Στατική επάρκεια
- Αντισεισμική κατασκευή

- Στεγανότητα και μόνωση για τη διατήρηση της θερμοκρασίας στους εσωτερικούς χώρους
- Επαρκής φωτισμός με παράθυρα στους χώρους του αναγνωστηρίου και των επισκεπτών, τα οποία να διαθέτουν φίλτρα UV
- Σωστή διαρρύθμιση
- Κατάλληλα υλικά κατασκευής (τούβλα ή οπλισμένο σκυρόδεμα)
- Θύρες εξόδων σε περίπτωση ανάγκης
- Σύστημα ελέγχου επισκεπτών και προσωπικού

Τα υλικά κατασκευής πρέπει να είναι ανθεκτικά στη φωτιά και να διατηρούν σταθερή θερμοκρασία μεταξύ των διαφορετικών δωματίων για την παρακώληση της επέκτασης της φωτιάς καθώς και να μην επιτρέπουν τη διάδοση της πλημμύρας. Επίσης τα παράθυρα καλό είναι να κλείνουν αεροστεγώς ώστε να διατηρείται η εσωτερική θερμοκρασία σε σταθερό επίπεδο. Επίσης σε αυτό το κομμάτι πρέπει να ληφθεί η απόφαση για την επιλογή των συστημάτων ψύξης-θέρμανσης, ανιχνευτών φωτιάς και συστημάτων κατάσβεσης. Τα συστήματα αυτά πρέπει να επιλεχθούν με συνάρτηση την προστασία του αρχειακού υλικού, του κοινού και των εργαζομένων καθώς και των περιβαλλοντικών συνεπειών. Για παράδειγμα ένα σύστημα fan-coil, στο οποίο κυκλοφορεί νερό, δεν ενδείκνυται για το αρχειοστάσιο διότι υπάρχει ενδεχόμενο διαρροής (Ζερβός, 2002). Επίσης σε περίπτωση που επιλεγεί σαν μέθοδος κατάσβεσης το διοξείδιο του άνθρακα (Co2) στους χώρους των αρχείων, καθότι είναι επικίνδυνο για τους ανθρώπους, πρέπει να υπάρχει πρόβλεψη για αεροστεγείς πόρτες (Artim, 1999).

Η διαρρύθμιση των χώρων φέρει μεγάλη σημασία. Ο χώρος του αρχειοστασίου πρέπει να βρίσκεται σε επαρκή απόσταση από τις εφεδρικές μονάδες ηλεκτρισμού, υδραυλικά συστήματα και σωληνώσεις, μονάδες κλιματισμούς και θέρμανσης (HVAC), κουζίνες, εργαστήρια συντηρητών και servers για να περιοριστούν τα σενάρια οπού μια φωτιά ή πλημμύρα που μπορεί να προκύψει θα επεκταθεί και στα αναλογικά αρχεία. Επίσης στο χώρο του αρχειοστασίου δεν πρέπει να τοποθετούνται ηλεκτρονικοί υπολογιστές και φωτοτυπικά μηχανήματα για παρόμοιους λόγους. Επιπροσθέτως καφετέριες και αναψυκτήρια και χώροι διαλείμματος των υπαλλήλων πρέπει να βρίσκονται σε απομακρυσμένη τοποθεσία από τα αρχεία (Varlamoff, 2005).

Επιπλέον, θα πρέπει να αναφερθεί ότι τα κτήρια πρέπει να διαθέτουν ένα σύστημα ελέγχου επισκεπτών. Δηλαδή, ένα αρχείο επισκεπτών στο οποίο θα σημειώνονται τα ονόματα αυτών για λόγους ασφαλείας. Σημαντικό ρόλο κατέχει και η κατανομή του χώρου με κατάλληλο τρόπο, ώστε ο χώρος του αρχειοστασίου και ο χώρος των

υπολογιστών στους οποίους υπάρχει πρόσβαση στο ηλεκτρονικό σύστημα, να είναι ξεχωριστός και με αυξημένους κανόνες ασφαλείας με στόχο να αποφευχθούν κλοπές και υποκλοπές. Στο πλαίσιο της προστασίας του υλικού ενός αρχειακού φορέα η πρόσβαση του κοινού πρέπει να γίνεται με ελεγχόμενο τρόπο. Είναι αναγκαίο να εργάζονται άτομα που προστατεύουν το κτίριο σε περίπτωση ανεπιθύμητης εισβολής ενώ ταυτόχρονα γνωρίζουν και επικοινωνούν αμέσως με τις αρχές οποιοδήποτε περιστατικό που μπορεί να προκαλέσει πρόβλημα στο φορέα.

4.2.2 Περιβάλλον φύλαξης

Το περιβάλλον φύλαξης των αρχείων φέρει μεγάλη σημασία για την μακροχρόνια διατήρηση του υλικού. Στο αρχειοστάσιο πρέπει να είναι ελεγχόμενη η ποιότητα του αέρα (για να μη φέρει σκόνη και ρύπους) καθώς και τα ποσοστά υγρασίας (35-45%) σε συνάρτηση με τη θερμοκρασία (εξαρτάτε ανάλογα με το είδος των αρχείων). Οι χώροι φύλαξης πρέπει να είναι σκοτεινοί ή τουλάχιστον να μην έρχονται σε επαφή με το φως του ηλίου καθώς το χαρτί επηρεάζεται από την υπεριώδη ακτινοβολία (Καρεκλάς, 2016).

Παρακάτω παρουσιάζονται κάποιοι από τους συνήθεις παράγοντες που αποτελούν κίνδυνο για τα τεκμήρια:

- Κακές πρακτικές φύλαξης και χειρισμού
- Χημική αστάθεια των υλικών
- Αμέλεια των υπευθύνων ή των εργαζομένων (αδιαφορία για τη διόρθωση βλαβών, συνωστισμός στο χώρο των αρχείων, κάπνισμα)
- Έλλειψη γνώσεων των εργαζομένων
- Ελλιπής πόροι (Πανεπιστήμιο Πατρών, 2005)

Δεν πρέπει να ξεχνάμε ότι όλοι οι χώροι του αρχείου πρέπει να καθαρίζονται συχνά στο πλαίσιο της λειτουργείας του φορέα και να υπάρχει ειδική μέριμνα για τον καθαρισμό του αρχειοστασίου από ειδικά εκπαιδευμένη ομάδα καθαριστών. Στο πλαίσιο της καθαριότητας πρέπει να είναι προγραμματισμένες οι απεντομώσεις και οι μυοκτονίες. Επιπλέον είναι υποχρεωτικό να υπάρχουν μηχανισμοί προσέλκυσης ζωυφίων, εντόμων και τρωκτικών για να γίνει σύντομα αντιληπτή η παρουσία τους ώστε να ληφθούν τα αντίστοιχα μέτρα (Ζερβός, 2002).

4.3 Εντοπισμός και ανάκτηση αρχείων μετά από καταστροφή

Οι υλικές ζημίες σε φυσικά τεκμήρια είναι δύσκολο να ανακτηθούν και διαφέρουν ανάλογα με την μορφή της καταστροφής που τις προξένησε. Ανάλογα με την έκταση και τη μορφή της ζημιάς του αναλογικού υποστρώματος, οι πρακτικές μπορεί να διαφέρουν, παρόλο που συνήθως χρησιμοποιούνται συνδικάστηκα. Σε μια προσπάθεια ανάκτησης υλικού κρίνεται πάντα απαραίτητη η γνώμη και η καθοδήγηση από εξειδικευμένο χημικό - συντηρητή. Κάποια από τα μέτρα που εφαρμόζονται συνήθως αναφέρονται παρακάτω.

Σε περίπτωση πλημύρας τα τεκμήρια χρειάζονται μια ολόκληρη διαδικασία ώστε να ανακτηθούν, η συνήθης πρακτική αποτελείται από τα παρακάτω βήματα:

- Τοποθέτηση του αρχείου σε ψυγεία με χαμηλή θερμοκρασία ώστε να σταματήσει η ανάπτυξη της μούχλας
- Ταυτόχρονη φύγρανση του αρχείου
- Σταδιακό καθάρισμα του αρχείου
- Απολύμανση- αποστείρωση σε ειδικούς θαλάμους
- Χημική επεξεργασία δηλαδή αποξίνιση και ουδετεροποίηση
- Στερεοποίηση και αποκατάσταση του χαρτιού
- Τοποθέτηση του υλικού σε δοχεία με αντιόξινη και αντιμυκητιακή προστασία

Σε περίπτωση σεισμού και ειδικά σε περίπτωση κατάρρευσης του κτηρίου πρέπει να επέμβουν οι ειδικοί αποκατάστασης για να ανακτήσουν τα τεκμήρια. Κάποιες ενέργειες που μπορούν να γίνουν είναι:

- Είναι καθαρισμός από την σκόνη
- Αποκατάσταση σκισμένου χαρτιού από συντηρητή
- Χρήση ιαπωνικών χαρτιών

Σε περίπτωση πυρκαγιάς, οποιοδήποτε υλικό που έχει γίνει μαύρο από τη φωτιά είναι γενικά δύσκολο να ανακτηθεί. Οι δύο σημαντικές μέθοδοι ανάκτησης είναι:

- Η απολύμανση με σκοπό την απολύμανση και την συντήρησης του χαρτιού.
- Η μέθοδος ξήρανσης η οποία τα τεκμήρια έχουν υποστεί (Ζερβός, 2002)

5 Κεφάλαιο 5ο

5.1 Πλάνο Επιχειρησιακής Συνέχειας - Business Continuity Plan

Η έννοια της επιχειρησιακής συνέχειας αναδύθηκε από το χώρο του χρηματοοικονομικού συστήματος στις αρχές της δεκαετίας του ’70. Στο πλαίσιο της λειτουργείας των τραπεζών είχε φανεί από νωρίς το μεγάλο μέγεθος της καταστροφής που μπορούσε να προκύψει έπειτα ακραία καιρικά φαινόμενα και περιπτώσεις πυρκαγιάς. Η επιχειρησιακή συνέχεια λοιπόν έρχεται για να προνοήσει τους πιθανούς κινδύνους και να ορίσει μεθόδους για τη συνέχιση της ομαλής λειτουργείας ενός φορέα.

Το πλάνο επιχειρησιακής συνέχειας θα μπορούσε να οριστεί ως μια ολιστική συγκέντρωση των κινδύνων που ενδεχομένως να προξενήσουν βλάβες στο φορέα και η δημιουργία ενός σχεδίου το οποίο μπορεί να εφαρμοστεί εξασφαλίζοντας την ανθεκτικότητα του φορέα και τη διασφάλιση των συμφερόντων των μετόχων και της φήμης του (Kasim Randeree, 2012).

Τα πλάνα της επιχειρησιακής συνέχειας (BCP) αποσκοπούν στην εξασφάλιση της αδιάλειπτης λειτουργίας ενός φορέα και εφαρμόζονται στις περιπτώσεις που συμβάντα που επηρεάζουν την ομαλή λειτουργεία ανακύπτουν χωρίς κανένα προειδοποιητικό στοιχείο. Στα πλάνα αυτά είναι αναγκαίο να προβλέπονται εναλλακτικές λύσεις ολιστικά για κάθε λειτουργικό μέλος του φορέα (IBM Services, 2020). Με άλλα λόγια στο BCP διατυπώνεται ένα σύνολο από παράγοντες που προκαλούν αναστάτωση στις καθημερινές διεργασίες. Οι παράγοντες μπορεί να προέρχονται από όλα τα τμήματα, όπως οι υπάλληλοι (πανδημία), κάποια δυσλειτουργία στις αποφάσεις του τμήματος του ανθρώπινου δυναμικού (απεργία), στους εξωτερικούς συνεργάτες και στους προμηθευτές, στην κτηριακή εγκατάσταση, καθώς και στο κομμάτι των πληροφοριακών συστημάτων (IT) (Brahim Herbane, 2004). Είτε είναι ενδογενείς είτε εξωγενείς (κοινωνικοί) οι παράγοντες που προκαλούν αναστάτωση πρέπει να αναλύονται και να τοποθετούνται σε κλίμακα πιθανής εκδήλωσης σε συνάρτηση με τις πιθανές εναλλακτικές λύσεις που είναι διαθέσιμες για χρήση ώστε να μη σταματήσει τη λειτουργεία του ο φορέας. Παρακάτω παρατίθενται συνοπτικά οι παράγοντες που αφορούν και την διατύπωση του BCP:

- Κυβερνητικές αποφάσεις (αυξήσεις στου φόρους, πρόκληση κοινωνικών αναταραχών)

- Μεταβολές του βασικού αγοραστικού κοινού (π.χ. μιας εταιρείας που διαχειριζόμαστε το αρχείο δημιουργεί παράρτημα για να διαχειρίζεται το αρχείο της)
- Ανταγωνιστές και πολιτικές που ακολουθούν
- Τεχνολογικά μέσα (υπάρχει περίπτωση ένας φορέας να διαθέτει παρωχημένο τεχνολογικό εξοπλισμό)
- Υποκατάστατα των υπηρεσιών ενός φορέα
- Λάθη που προέρχονται από την τακτική διαφήμισης ή από το τμήμα του ανθρώπινου δυναμικού
- Ανεπάρκεια υλικών (αναξιόπιστοι προμηθευτές)
- Χαμηλής ποιότητας προμήθειες
- Φυσικές καταστροφές (όσες έχουν αναφερθεί και στο DRP)
- Εργατικά ατυχήματα
- Απώλεια βασικών πελατών (Gallagher, 2003).

Το πλάνο επιχειρησιακής συνέχειας πρέπει να διατυπώνεται από έναν διαχειριστή που έχει λάβει υπόψιν του τις παρεχόμενες υπηρεσίες, τις απαιτήσεις των πελατών ή των υπεύθυνων του φορέα, το κόστος που μπορεί να καλύψει ο φορέας στο πλαίσιο της προετοιμασίας και πως να ποσοτικοποιήσει την αποδοτικότητα του σχεδίου. Έπειτα όπως έχει αναφερθεί πρέπει να γίνονται συνεχείς ανανεώσεις και προσθήκες στο πλάνο καθώς και να παραδίδεται στο προσωπικό του φορέα. Σημαντικοί παράγοντες που ορίζουν την αποδοτικότητα του πλάνου είναι οι εξής:

- Υποστήριξη δικτύου IT: Πρέπει να υπάρχει πρόσβαση σε backup για να συνεχίσουν οι υπηρεσίες να παρέχονται στο κοινό.
- Σύνδεση στο διαδίκτυο: Εξασφάλιση πρόσβαση στην ιστοσελίδα
- Επικοινωνία με προμηθευτές και τεχνικούς για σύντομη επισκευή βλαβών

Επίσης αξίζει να σημειωθεί ότι παρόλο που όλοι οι φορείς έχουν μια ασφάλεια που τους καλύπτει σε περιπτώσεις καταστροφών δεν σημαίνει ότι δεν πρέπει να διαθέτουν επαρκώς επιμελημένα πλάνα εκτάκτων αναγκών, ανάκτησης και επιχειρησιακής συνέχειας. Τα πλεονεκτήματα που επιφέρουν τα εξατομικευμένα σε κάθε οργανισμό (καλή εικόνα στο κοινό, μικρότερες δαπάνες σε περιπτώσεις καταστροφών, συνέχιση της λειτουργείας κτλ.) είναι ανεξάρτητα από τα χρήματα που μπορεί να καλύψουν τις

υλικές βλάβες. Επιπλέον, όπως είναι προφανές, με τη σύνταξη αυτών των πλάνων οι ασφαλιστικές υπάρχει περίπτωση να παρέχουν προγράμματα σε καλύτερες τιμές ή επαυξημένες υπηρεσίες (Gallagher, 2003).

5.2 Διαφορές και ομοιότητες μεταξύ DMP - BCP

Υπάρχει διαφορά μεταξύ των στόχων που μπορούν να επιτευχθούν μεταξύ των πλάνων διαχείρισης εκτάκτων αναγκών και ανάκτησης (DMP - DRP) και του πλάνου επιχειρησιακής συνέπειας καθώς **δεν εξετάζει πως μπορούμε να αποφύγουμε τους κινδύνους περιορίζοντας την επίδρασή τους στο φορέα και έπειτα την ανάκληση των κατεστραμμένων πόρων, αλλά αποβλέπει στην συνέχιση της λειτουργείας του φορέα κατά τη διάρκεια της εξέλιξης των καταστροφών και των μέτρων ανάκλησης**. Στις περιπτώσεις που τα σχέδια BCP φάνηκαν αποτελεσματικά σε κρίσιμες στιγμές, δεν πρέπει να ξεχνάμε ότι η φήμη των φορέων διατηρείται και ενισχύεται (Brahim Herbane, 2004).

Κάθε πλάνο επιχειρησιακής συνέχειας πρέπει να ορίζει την μέθοδο χρήσης και διαχείρισης των παρακάτω προϋποθέσεων:

- Δημιουργία αντιγράφων ασφαλείας (ψηφιακά και σε κάποιες περιπτώσεις και αναλογικά)
- Εξασφάλιση ομαλής λειτουργείας συστημάτων παρακολούθησης αρχειοστασίου
- Ομαλή λειτουργεία συστημάτων IT (γίνεται εκτενέστερη αναφορά παρακάτω)
- Εναλλακτικά μέσα επικοινωνίας μεταξύ των πελατών ή της μητρικής εταιρείας, στην οποία ανήκει ο φορέας, με τον φορέα
- Εναλλακτικά μέσα επικοινωνίας μεταξύ των υπαλλήλων του φορέα

Ο αντίκτυπος στην εικόνα που έχει διαμορφώσει ένας φορέας στην κοινωνία αν παραμείνει αλώβητη έπειτα από μια καταστροφή (είτε ενδογενής είτε εξωγενής) διαδραματίζει σημαντικό ρόλο στην άποψη τόσο του κοινού, του διοικητικού συμβουλίου το οποίο παρέχει το μεγαλύτερο μέρος της χρηματοδότησης, των μετόχων και των επενδυτών (στις περιπτώσεις που υπάρχουν). Επίσης η διατήρηση ενός ασφαλούς και ήρεμου εργατικού περιβάλλοντος αποτελεί πόλο έλξης καλού εργατικού δυναμικού καθώς και λόγο για τη διατήρηση του υπάρχοντος (Gallagher, 2003).

Για ακόμη μια φορά το πλάνο της επιχειρησιακής συνέχειας πρέπει να ανανεώνεται συνεχώς. Οι ενημερώσεις του BCP εξαρτώνται από περισσότερους παράγοντες σε σχέση

με το DRP. Πιο συγκεκριμένα το BCP περιλαμβάνει και κοινωνικούς παράγοντες που μπορεί να βλάψουν ένα φορά (Brahim Herbane, 2004). Για παράδειγμα με την εμφάνιση της πανδημίας του SARS-CoV-2 το 2019 οι υπεύθυνοι της διαχείρισης του πλάνου έπρεπε να προβλέψουν την πιθανότητα επιβολής καραντίνας και μέτρων εργασίας (π.χ. δια ζώσης εργασία μόνο του ήμισυ του δυναμικού ενός φορέα). Συνεχίζοντας, ένα καλό BCP θα περιείχε την αγορά φορητών υπολογιστών και εταιρικών κινητών τηλεφώνων ώστε να παραμένουν οι υπάλληλοι σε συνεχή επικοινωνία με τους συναδέλφους τους και να πραγματοποιούν το εργασιακό τους πρόγραμμα από το σπίτι τους. Κατ' αυτόν τον τρόπο ο φορέας θα συνέχιζε τη λειτουργεία του με αναστάτωση.

Γίνεται λοιπόν κατανοητό ότι πέραν της συνεχούς ανασκόπησης του πλάνου χρειάζεται και η εκπαίδευση του προσωπικού για να μην υπάρχει μεγάλη κωλυσιεργία στην περίοδο προσαρμογής στον προσωρινό τρόπο λειτουργείας. Σε ό,τι αφορά την εκπαίδευση του προσωπικού και τα απαραίτητα υλικά (κτιριακές εγκαταστάσεις, εξοπλισμός, υλισμικό, λογισμικό, εναλλακτικούς προμηθευτές κ.α.) το BCP δεν διαφέρει παρασάγγας από το DRP. Ειδοποιός διαφορά είναι η μέθοδος με την οποία χρησιμοποιούνται καθώς και το πότε γίνεται χρήση των εναλλακτικών επιλογών. Από τη στιγμή δηλαδή που θα εκδηλωθεί μια κρίση ενεργοποιείται το DRP ενώ το BCP ενεργοποιείται με σκοπό να χρησιμοποιήσει τα υλικά για να συνεχίσει ο φορέας να παρέχει τις υπηρεσίες του.

Σύμφωνα με τη βιβλιογραφία σε παλαιότερες εποχές ήταν αποδεκτή η «απώλεια δεδομένων» ενός εικοσιτετράωρου, δηλαδή η παύση της λειτουργείας ενός φορέα για μια μέρα δεν είχε σημαντική επίδραση στις εργασίες του και στην υπόληψή του. Παρ' όλα αυτά το DRP που εφαρμοζόταν δεν επαρκεί στους σύγχρονους ρυθμούς του εμπορείου καθώς υπάρχει ανάγκη εξυπηρέτησης σε εικοσιτετράωρη βάση όλες τις ημέρες τις εβδομάδας. Οπότε η δημιουργία ενός BCP είναι αναγκαία για κάθε φορέα (Hecht, 2002).

6 Κεφάλαιο 6ο

6.1 Πλάνο διαχείρισης ψηφιακών καταστροφών - Disaster Recovery Plan for IT

Το πλάνο διαχείρισης ψηφιακών καταστροφών αποσκοπεί στην ομαλή λειτουργεία των ηλεκτρονικών συστημάτων ενός αρχειακού φορέα. Είναι μια συνεχώς αναπτυσσόμενη διαδικασία καθώς η στασιμότητα του σχεδίου σε αυτόν τον τομέα εγκυμονεί τον κίνδυνο να γίνει αναχρονιστικό με αποτέλεσμα οι «πειρατές» να φτάνουν όλο και πιο κοντά στην απόκτηση της πρόσβασης στα αρχεία του φορέα. Επιπλέον στο παραπάνω πλάνο εντάσσονται και όλα τα μετρά που θα εξασφαλίσουν την αποτελεσματική και αποδοτική λειτουργεία των συστημάτων, τόσο σε περιπτώσεις ενδογενών παραγόντων κατάρρευσης όσο και σε εξωγενείς παράγοντες που φέρουν επίδραση στα ηλεκτρονικά συστήματα.

Οι τύποι τον καταστροφών που έχουν επίδραση στα ηλεκτρονικά μέσα χωρίζονται στις παρακάτω κατηγορίες:

I. Κατάρρευση λόγω βλάβης, κατεστραμμένα αρχεία λειτουργικού συστήματος, λάθη χρηστών, απώλεια σύνδεσης στο διαδίκτυο, σφάλματα λογισμικού, κακόβουλο λογισμικό, λογισμικό κατασκοπίας, κυβερνοεπίθεση (hacking)
II. Διακοπή ρεύματος, πυρκαγιά στο σύστημα του ηλεκτρονικού υπολογιστή, πυρκαγιά στο ηλεκτρολογικό κύκλωμα του κτιρίου, κατάρρευση του συστήματος εξαερισμού – θέρμανσης – ψύξης, λανθάνουσα τακτική κατάσβεσης με ψεκασμό νερού (Sprinkler)
III. Κλοπή, εμπρησμός, επίθεση στο κτίριο, έκρηξη βόμβας, ρύπανση αέρα
IV. Σεισμοί, ανεμοστρόβιλοι, ισχυρές καταιγίδες, χιονοπτώσεις, εκρήξεις ηφαίστειων, πτώση κεραυνού, παλιρροιακό κύμα, φωτιά στο περιβάλλον που βρίσκεται αρχειακό φορέας. (Hossam Abdel Rahman Mohamed, 2014)

Οι παραπάνω παράγοντες είναι κρίσιμοι στην διαδικασία δημιουργίας και προετοιμασίας ενός πλάνου ανάκαμψης των συστημάτων πληροφορικής. Ένα εύστοχο πλάνο ανάκαμψης είναι αναγκαίο να έχει συνυπολογίσει τις πιθανότητες να εκδηλωθούν ένας ή παραπάνω παράγοντες καθώς και να προβλέπει τις διαδικασίες σύντομης αποκατάστασης (business impact analysis) (Hanung Nindito Prasetyo, 2020). Για την

κατάλληλη προετοιμασία απαιτείται τόσο λογισμικό όσο και υλισμικό (software-hardware). Αυτά μπορεί να παρέχονται από μια εταιρεία πληροφορικής ή από τον ίδιο το φορέα, παρ' όλα αυτά είναι απαραίτητο να υπάρχουν εναλλακτικές λύσεις. Για παράδειγμα αν υπάρχει πρόβλημα στην εταιρεία πληροφορικής πρέπει να υπάρχουν αντίγραφα ασφαλείας των αρχείων του φορέα, και τοπικά σε διαφορετική τοποθεσία (backup). Μια ακόμη τακτική είναι η διατήρηση αντιγράφων ασφαλείας σε υπολογιστικό νέφος (cloud).

Στο πλαίσιο της σχεδίασης των πλάνων εκτάκτων αναγκών υπάρχει ανάγκη για την πρόβλεψη καλής επικοινωνίας και συνεργασίας με προμηθευτές υλισμικού και λογισμικού. Όλα τα συστήματα που λειτουργούν τόσο στο βασικό κτίριο του φορέα όσο και του εφεδρικού κτιρίου πρέπει να περιέχονται σε κατάλογο με αναλυτικές πληροφορίες για τα ανταλλακτικά και τα εξαρτήματά τους. Με την παραπάνω τακτική εξασφαλίζεται ο άμεσος εντοπισμός των υλικών που χρειάζονται είτε στο σενάριο μιας απλής βλάβης είτε σε μια καταστροφή μεγάλου μεγέθους (Hanung Nindito Prasetyo, 2020).

Ένας επιπλέον πολύ σημαντικός παράγοντας που μπορεί να προκαλέσει δυσλειτουργία στα ηλεκτρονικά συστήματα, είναι οι πάροχοι ηλεκτρισμού και τηλεπικοινωνιών. Είναι πιθανό να προκύψει κάποια βλάβη στα συστήματα του εκάστοτε παρόχου, ένα επαρκές σύστημα εκτάκτων αναγκών πρέπει να ορίζει κάποιες εναλλακτικές επιλογές.

Στην εκδοχή της διακοπής ρεύματος υπάρχει δυνατότητα το κτίριο να ηλεκτροδοτείται από δυο παρόχους ταυτόχρονα με αποτέλεσμα να περιορίζονται οι πιθανότητες να προκύψουν ταυτόχρονες βλάβες στα δίκτυα ηλεκτροδότησης. Βέβαια σε κάποια πιθανή καταστροφή, όπως η πλημμύρα, υπάρχει το ενδεχόμενο η βλάβη στο δίκτυο να είναι πολυήμερη. Λύσεις υπό αυτές τις συνθήκες δίνουν οι γεννήτριες ηλεκτρικούς ρεύματος που μπορούν να εξασφαλίσουν την ηλεκτροδότηση των εγκαταστάσεων και κυρίως των λειτουργικών μηχανημάτων που εξασφαλίζουν τη λειτουργεία του οργανισμού.

Αντίστοιχες μπορούν να είναι και οι λύσεις για το κομμάτι των τηλεπικοινωνιών. Περιορίζονται οι πιθανότητες απώλειας της σύνδεσης στον παγκόσμιο ιστό καθώς και στο τοπικό δίκτυο όταν δυο πάροχοι εξασφαλίζουν τη δικτυακή κάλυψη. Επίσης τουλάχιστον για τη σταθερότητα της πρόσβασης στον ιστό, ο οργανισμός, καλά είναι να διαθέτει και ασύρματη πρόσβαση στο δίκτυο μέσα από τη χρήση καρτών SIM, παρόλο που αποτελεί έσχατη λύση διότι αυτής της μορφής οι συνδέσεις δεν ενδείκνυνται για

μεταφορά μεγάλου όγκου δεδομένων (National Institute of Standards and Technology, 2010).

Επίσης δεν πρέπει να ξεχνάμε ότι στο πλαίσιο των παραπάνω ειδών κυβερνοεπίθεσης υπάρχουν και νομικές κυρώσεις σε περιπτώσεις δημοσίευσης προσωπικών δεδομένων. Σύμφωνα με την νομοθεσία Data Protection Directive 95/46/EC πρέπει να τηρούνται οι εξής επτά κανόνες από κάθε φορά που διατηρεί προσωπικά δεδομένα άλλων προσώπων:

1. Προειδοποίηση, σε περίπτωση που διατηρούνται δεδομένα χρηστών
2. Σκοπός που διατηρούνται τα δεδομένα
3. Συγκατάθεση του χρήστη
4. Ασφάλεια των δεδομένων
5. Ξεκάθαρη δημοσίευση των φορέων που διατηρούν τα προσωπικά δεδομένα
6. Πρόσβαση ατόμων στα προσωπικά τους δεδομένα
7. Ανάληψη της ευθύνης από το φορέα που διατηρεί τα προσωπικά δεδομένα (Official Journal of the European Union, 2016)

Συμπερασματικά η μεθοδευμένη καταστροφή των αρχείων φέρει μεγάλης σημασίας και δεν πρέπει να παραβλέπεται από τους φορείς. Είτε ψηφιακά είτε αναλογικά αρχεία οι φορείς είναι υποχρεωμένοι να τα καταστρέφουν και να τα διαχειρίζονται με βάση κανονισμούς όπως το ISO 17799 (Gallagher, 2003). Το πλαίσιο της προστασίας των προσωπικών δεδομένων είναι πολυδαίδαλο και τα λογισμικά που χρησιμοποιούνται πρέπει να έχουν σχεδιαστεί από έμπειρα άτομα με γνώσεις στον τομέα της πληροφορικής (Ma, 2005)

6.1.1 Knowledge management in DRPIT

Σύμφωνα με τη βιβλιογραφία και την εμπειρία που έχει εκπορευθεί μέσα από την οργάνωση των φορέων για την ελαχιστοποίηση των επιπτώσεων μιας καταστροφής, η διατύπωση του πλάνου εκτάκτων αναγκών και ανάκαμψης πρέπει να γίνεται πριν το σχεδιασμό της κτιριακής υποδομής και έπειτα να συνοδεύει τον φορέα στα χρόνια λειτουργείας του. Ενημερώσεις και αναθεωρήσεις των πλάνων αυτών πρέπει να γίνονται ανά τακτά διαστήματα. Παρόλα αυτά ένα πολύ σημαντικό πόρος γνώσεων για τη βελτίωση των πλάνων είναι η ίδια η καταστροφή.

Ανεξάρτητα από τις γνώσεις που προκύπτουν από τις εικονικές εφαρμογές του πλάνου για τον έλεγχο της ομαλής εφαρμογής του από τα μέλη του προσωπικού, μια κρίσιμη στιγμή που λαμβάνει χώρα ένα γεγονός που διαταράσσει τη λειτουργεία του οργανισμού είναι απαραίτητο να διατηρούνται από τους υπευθύνους αρχεία καταγραφής των συνθηκών και των τακτικών αντίδρασης. Σε μεταγενέστερο χρόνο όλα αυτά τα στοιχεία χρήζουν ανάλυσης διότι βρίθουν χρήσιμων πληροφοριών οι οποίες θα αποτελέσουν άξονες για την αύξησης της αποτελεσματικότητας των μέτρων πρόληψης (Dinesh Alawanthan, 2017).

6.2 Γεννήτριες Ηλεκτρισμού

Οι γεννήτριες ηλεκτρικού ρεύματος μπορούν να φανούν χρήσιμες όχι μόνο στα σενάρια DRP-IT αλλά και στα πλάνα επιχειρησιακής συνέχειας καθώς εξασφαλίζουν την παροχή ρεύματος είτε στη βασική κτιριακή μονάδα είτε στην εφεδρική. Μέσω της αδιάληπτης παροχής ηλεκτρισμού, οι servers, οι υπολογιστές των υπαλλήλων και των χρηστών και όλα τα συστήματα τηλεπικοινωνίας μπορούν να συνεχίσουν να λειτουργούν. Ως εκ τούτου υπάρχει πρόσβαση στα αντίγραφα ασφαλείας, σε περίπτωση που δεν είναι δυνατή η πρόσβαση στα αναλογικά (π.χ. λόγω καταστροφής), και επίσης εξασφαλίζεται η συνέχιση της παροχής των υπηρεσιών του φορέα.

Οι σταθμοί παραγωγής ηλεκτρισμού που λειτουργούν σαν εφεδρικές μονάδες συνήθως λειτουργούν με πετρέλαιο, φυσικό αέριο ή μπαταρίες. Πιο αναλυτικά είναι ένα σύστημα που βρίσκεται μεταξύ του βασικού παρόχου ηλεκτρισμού και του κτιρίου το οποίο τίθεται σε λειτουργεία κάθε φορά που υπάρχει διακοπή. Σημαντικός παράγωγοντας που μας αφορά είναι το μέσο παραγωγής ηλεκτρισμού της τοπική μονάδας καθώς σε περίπτωση φυσικής καταστροφής υπάρχει ανοιχτό το ενδεχόμενο η πρόσβαση οχημάτων μεταφοράς υγρών καυσίμων να είναι αδύνατη ή λόγω της αυξημένης ζήτησης να υπάρχει έλλειψη. Στην εκδοχή του φυσικού αερίου είναι λιγότερο πιθανό να υπάρχει βλάβη στο δίκτυο παροχής, αλλά δεν αποκλείεται. Με άλλα λόγια οι γεννήτριες που λειτουργούν και με μπαταρίες αποτελούν μια πιο αξιόπιστη λύση (Kwasinski, 2010).

Παρόλα αυτά πρέπει να σημειωθεί το μέγεθος του κόστους ων γεννητριών ηλεκτρισμού. Είναι δύσκολο να καθοριστούν συγκεκριμένα ποσά διότι είναι ένας τομέας που δεν παύει να εξελίσσεται όμως τα ποσά της συντήρησης της μονάδας είναι πολύ μεγάλα. Γενικότερα στην λήψη των αποφάσεων αναφορικά με τις εφεδρικές επιλογές σε

σενάρια καταστροφών είναι αναγκαίο να γίνεται ένας υπολογισμός της αποδοτικότητας και της αποτελεσματικότητας (cost-effective vs cost-efficient) (Musiliu O. Oseni, 2013).

6.3 Uninterruptible Power Supply – UPS

Οι συσκευές αδιάλειπτης παροχής ενέργειας αποτελούν μια επαρκή αλλά προσωρινή λύση για την εξασφάλιση της λειτουργείας των υπολογιστών των χρηστών του φορέα καθώς και των βάσεων δεδομένων. Μέσω αυτών των συσκευών εξασφαλίζεται η τροφοδοσία ηλεκτρικού ρεύματος στις ηλεκτρονικές συσκευές για το διάστημα που χρειάζεται, μεταξύ 30 λεπτών και μιας ώρας, μέχρι να σωθούν οι εργασίες των χρηστών και να απενεργοποιηθούν με ασφάλεια οι συσκευές. Επίσης προστατεύει όλα τα συστήματα από τις μεταβολές της τάσης του ηλεκτρικού ρεύματος (National Institute of Standards and Technology, 2010).

Η χρήση των UPS είναι αναγκαία για την αποφυγή κατάρρευσης του συστήματος μετά από στιγμιαία διακοπή ρεύματος καθώς και για την αποφυγή βλαβών που προκύπτουν από μεταβολές της τάσης του ρεύματος. Όπως είναι όμως λογικό δεν μπορούν να αντικαταστήσουν τις γεννήτριες ηλεκτρισμού που εξασφαλίζουν την παροχή ρεύματος για μεγάλα χρονικά διαστήματα διατηρώντας τη σταθερή και ομαλή λειτουργεία των βάσεων δεδομένων και των συστημάτων του φορέα ακόμα και σε περιπτώσεις πολύωρης διακοπής ηλεκτρισμού (Langan Engineering, 2013).

6.4 Backup

Τα αντίγραφα ασφαλείας είναι μια τεχνική ευρέως διαδεδομένη την τελευταία δεκαετία καθώς είναι πολύ αποτελεσματική και οικονομική λύση. Παρόλα αυτά είναι αναγκαίο να προβλέπεται ο τρόπος λειτουργείας συσκευών που διατηρούν τα αντίγραφα ασφαλείας και στο πλαίσιο της επιχειρησιακής συνέχειας. Σύμφωνα με τον Budiman η μέθοδος Distributed Replicated Block Device (DRBD) είναι επαρκώς ασφαλής καθώς αποτελείται από μονάδες αντιγραφής των αρχείων οι οποίες βρίσκονται σε διαφορετική τοποθεσία από τους υπολογιστές στους οποίους δημιουργούνται και είναι αποθηκευμένα τα αρχεία για πρόσβαση. Πιο αναλυτικά με τη χρήση του διαδικτύου είναι δυνατόν να γίνεται κάποια προγραμματισμένη ώρα μέσα στην ημέρα, ή κάποια ημέρα της εβδομάδας αντιγραφή όλων των αρχείων που βρίσκονται στη βάση δεδομένων. Οι δυο βάσεις θα λειτουργούν παράλληλα, όμως μόνο η μια που βρίσκεται εντός του κτιρίου όπου στεγάζεται το αρχείο θα είναι προσβάσιμη στους χρήστες. Γίνεται λοιπόν κατανοητό πως αν προκύψει κάποιο σφάλμα στη βάση δεδομένων ή κάποια

καταστροφή στο χώρο του φορέα, τα αντίγραφα θα μείνουν ανεπηρέαστα (K Budiman, 2020).

Το κτίριο που θα διατηρούνται τα αντίγραφα ασφαλείας είναι καλό να βρίσκεται σε μακρινή τοποθεσία ώστε να περιορίζονται όσο το δυνατόν περισσότερο οι πιθανότητες να πληγεί από τους ίδιους παράγοντες καταστροφής με το βασικό κτίριο του φορέα. Σύμφωνα μάλιστα με το ISO 27001 ιδανική απόσταση από το βασικό κτίριο είναι από 30 χιλιόμετρα και πάνω. Επίσης η επιλογή της τοποθεσίας είναι σημαντική γιατί πρέπει να βρίσκεται σε σημείο που υπάρχει γρήγορη πρόσβαση σε περίπτωση ανάγκης, ενώ ταυτόχρονα να διατηρείται προσωπικό υπεύθυνο για τη συντήρηση και την προστασία του χώρου αυτού. Καθώς και το δεύτερο κτίριο όπου υπάρχουν τα backups αποτελεί μέρος του φορέα, δεν πρέπει σε καμία περίπτωση να εξαιρείται από τα σχέδια εκτάκτων αναγκών και των πλάνων ανάκτησης (Hanung Nindito Prasetyo, 2020).

Επιπροσθέτως, για την αποφυγή εισβολών από μη εξουσιοδοτημένους χρήστες που προέρχονται από το χώρο του διαδικτύου, αποτελεί καλή τακτική η τοποθέτηση ενός δικτύου Local Area Network (LAN) στο οποίο να περιλαμβάνεται και η εφεδρική βάση δεδομένων (Steve M. Hawkins, 2020). Μια εναλλακτική είναι η κρυπτογράφηση των δεδομένων που βρίσκονται στην εφεδρική τοποθεσία. Με αυτή την επιλογή πρέπει να υπάρχουν άτομα του προσωπικού που να γνωρίζουν το κλειδί αποκρυπτογράφησης σε περίπτωση ανάγκης ώστε να υπάρχει πρόσβαση στα αντίγραφα ασφαλείας.

Επίσης στην περίπτωση που υπάρχει ανάγκη για αντίγραφα ασφαλείας σε προσωπικούς υπολογιστές, μια καλή επιλογή είναι και οι δίσκοι NAS (network attached storage) καθώς και τα δίκτυα SAN (storage area network). Οι δίσκοι NAS λειτουργούν εντός του δικτύου και είναι άμεσα συνδεδεμένοι είτε μέσω καλωδίου είτε μέσω της τοπικής σύνδεσης LAN στους υπολογιστές. Τα δίκτυα SAN αποτελούν τη λύση για τις περιπτώσεις που δεν υπάρχει πρόσβαση σε LAN καθώς από μόνα τους αποτελούν ένα δίκτυο αποκλειστικά για τη διατήρηση των αντιγράφων ασφαλείας.

Παρακάτω παρατίθενται κάποιες από τις βασικότερες μεθόδους για τη διατήρηση αντιγράφων ασφαλείας με τα πλεονεκτήματα και τα μειονεκτήματά τους:

- Πλήρης Αντιγραφή: με αυτή τη μέθοδο αντιγράφονται όλα τα αρχεία από τους υπολογιστές - χρήστες ή τα αρχεία που βρίσκονται μέσα στο φάκελο που έχει επιλεχθεί από το διαχειριστή. Το πλεονέκτημα είναι ότι όλα τα αρχεία ανά πάσα στιγμή που έχει πραγματοποιηθεί η αντιγραφή τους είναι διαθέσιμα. Το μειονέκτημα είναι ότι υπάρχει ανάγκη μεγάλων ταχυτήτων μεταφοράς των αρχείων μεταξύ των υπολογιστών και των

μονάδων στις οποίες διατηρούνται τα αντίγραφα. Επιπλέον δεν τηρείται μια οικονομική διαχείριση της χωρητικότητα των σκληρών δίσκων καθώς καθημερινά μπορεί να αντιγράφονται λειτουργικά αρχεία των υπολογιστών ή αρχεία που δεν έχουν υποστεί αλλαγές από το προηγούμενο backup.

- Σταδιακή Αντιγραφή: με αυτή τη μέθοδο αντιγράφονται αρχεία που έχουν υποστεί αλλαγές από τους χρήστες με αποτέλεσμα να καταλαμβάνουν μικρότερο αποθηκευτικό χώρο και να απαιτούν μικρότερες ταχύτητες μετάδοσης των δεδομένων. Παρόλα αυτά η παραπάνω μέθοδος εγκυμονεί τον κίνδυνο της απώλειας δεδομένων μεταξύ των χρονικών διαστημάτων που είναι προγραμματισμένες οι αντιγραφές.
- Διαφορική Αντιγραφή: αυτή η μέθοδος αποτελεί ένα υβριδικό σύστημα και συνυπάρχει με την μέθοδο της πλήρους αντιγραφής. Στην παρούσα περίπτωση αντιγράφονται μόνο τα νέα αρχεία ή τα αρχεία που έχουν μορφοποιηθεί στο χρονικό διάστημα μεταξύ της προηγούμενης Πλήρους Αντιγραφής. Αφενός λόγω της παραπάνω λειτουργεία απαιτείται μικρότερη ταχύτητα διότι ο όγκος των δεδομένων είναι μικρότερος. Αφετέρου χρειάζεται περισσότερο χρόνο από τη σταδιακή αντιγραφή (National Institute of Standards and Technology, 2010).

6.4.1 Hardware Failure

Σε αυτό το κομμάτι αξίζει να αναφερθεί ότι στο πλαίσιο του Business Continuity πρέπει να υπάρχει πρόβλεψη για την πιθανότητα αστοχίας των συστημάτων του υλισμικού. Είτε αναφερόμαστε στους υπολογιστές των υπαλλήλων είτε στον server, είναι αναγκαίο να υπάρχουν ανά πάσα στιγμή εφεδρικά εξαρτήματα του server ή των υπολογιστών που χρησιμοποιούν οι υπάλληλοι.

Στην περίπτωση των servers υπάρχουν προγράμματα που συγκεντρώνοντας πληροφορίες τόσο από τις εταιρείες κατασκευής των εξαρτημάτων όσο και από τις ώρες λειτουργείας τους προβλέπουν περίπου την χρονική περίοδο που αναμένετε η αστοχία τους. Η χρήση αυτού του λογισμικού είναι σίγουρα αναγκαία καθώς και ο συχνός έλεγχος του hardware από τους μηχανικούς πληροφορικής.

Στο πλαίσιο της καταστροφής ενός υπολογιστή που χρησιμοποιείται από κάποιον εργαζόμενο μπορούμε να εξασφαλίσουμε είτε ανταλλακτικά για την άμεση επαναλειτουργία του είτε φορητούς υπολογιστές (laptops) που να έχουν εφεδρικό ρόλο σε περίπτωση αστοχίας (Xiaoyi Sun, 2019).

6.5 Cloud

Η τακτική του υπολογιστικού νέφους αποτελεί μια ακόμη υπό εξέταση τακτική για εξασφάλιση αντιγράφων ασφαλείας. Το υπολογιστικό νέφος είναι μια μορφή υπηρεσία που παρέχεται από πολλές εταιρείες που δραστηριοποιούνται στο χώρο της πληροφορικής και της ανάπτυξης λογισμικών ως υπηρεσία όπως η Google, η Amazon,η Dropbox, η Scaleway και άλλες.

Τα πλεονέκτημα αυτής της τακτικής είναι ότι δεν χρειάζεται να υπάρχει επιπλέον κτιριακή εγκατάσταση με εξατομικευμένα πλάνα διαχείρισης εκτάκτων αναγκών και ανάκτησης. Παρόλο βέβαια που μπορεί να φαίνεται σαν μια πιο οικονομική λύση μακροπρόθεσμα δεν συνεχίζει να είναι. Επίσης δεν απαιτείται εκπαίδευση του προσωπικού για την χρήση ενός cloud, καθώς και επιπλέον προσωπικό για να διαχειρίζεται και να διατηρεί την εφεδρική βάση δεδομένων (Wenjin Hu, 2020).

Αντιθέτως υπάρχουν και κάποια σοβαρά μειονεκτήματα που πρέπει να ληφθούν υπόψιν πριν τη διαμόρφωση της τακτικής αξιοποίησης του υπολογιστικού νέφους. Το βασικότερο από αυτά είναι ότι δεν υπάρχει επαρκής προστασία των δεδομένων από τυχόν κυβερνοεπιθέσεις. Παρόλο που οι μεγάλες εταιρείες πρωτοπορούν στην ανάπτυξη αλγορίθμων για την προστασία των δεδομένων, δεν παύει να είναι μια τεχνολογία που απευθύνεται σε κοινό για οικιακή χρήση και όχι για επαγγελματικού επιπέδου. Επίσης οι ταχύτητες του διαδικτύου στις περισσότερες περιοχές δεν εξασφαλίζει την συνέπεια αυτού του συστήματος, καθώς είναι χαμηλές σε σχέση με αυτές που μπορούν να επιτευχθούν με τις ενσύρματες συνδέσεις και ακόμα και το LAN. Επίσης ο μεγάλος όγκος των δεδομένων που μπορεί να στέλνει ταυτόχρονα ένας φορέας στο cloud μπορεί να προκαλέσει σφάλματα στο δίκτυο (Muthu Ramachandran, 2016).

Συμπερασματικά η διατήρηση αντιγράφων ασφαλείας σε υπολογιστικό νέφος δεν ενδείκνυται ακόμα για χρήση από φορείς μεγάλου μεγέθους. Σημειώνεται βέβαια ότι με την κατάλληλη πολιτική διαχείρισης δυνητικά υπάρχει περιθώριο απόθεσης μέρους των ενεργών - λειτουργικών αρχείων στο νέφος. Για παράδειγμα αρχεία που χρησιμοποιούν πολλά άτομα σε μια υπηρεσία καθημερινά είναι δυνατόν να διατηρούνται σε cloud με κοινή πρόσβαση και να αποθέτονται αν συγκεκριμένα χρονικά διαστήματα που έχουν οριστεί στη βάση δεδομένων.

6.6 Firewall – LAN

Το firewall είναι μια τεχνολογία υλισμικού (software) που αποσκοπεί στην προστασία ενός υπολογιστή ή ενός δικτύου από την πρόσβαση των μη

εξουσιοδοτημένων χρηστών ή και πειρατών (hackers) σε αυτό (V. Selvi, 2014). Για να επιτευχθεί αυτός ο σκοπός, το τοίχος προστασίας ελέγχει την επικοινωνία, δηλαδή την ανταλλαγή των πακέτων δεδομένων, του υπολογιστή ή του δικτύου με τον παγκόσμιο ιστό (Ogbulezie, 2016). Η λειτουργεία του τοίχους προστασίας εξασφαλίζει ότι τα πακέτα δεδομένων που ανταλλάσσονται μεταξύ του υπολογιστή – δικτύου και του παγκόσμιου ιστού, τηρούν τα κριτήρια που έχουν οριστεί από τους διαχειριστές. Επομένως περιορίζονται σε μεγάλο βαθμό οι πιθανότητες κυβερνοεπίθεσης, ανεξαρτήτως της μεθόδου (hacking, καταγραφή κωδικών, trojan, malware) αφού τα πακέτα δεδομένων φέρουν αναγνωριστικά καθ' όλη τη διάρκεια της ανταλλαγής.

Το firewall βρίσκεται συνήθως προεγκατεστημένο στη συσκευή του δρομολογητή (router) της σύνδεσης του δικτύου τηλεπικοινωνιών. Σε περιπτώσεις όπως οι αρχειακοί φορείς ενδείκνυται η χρήση συσκευών (hardware) firewall οι οποίες τοποθετούνται στο δίκτυο μετά τον δρομολογητή, προσφέρονται ένα ακόμα επίπεδο προστασίας στο οποίο μπορούν να οριστούν εξ' ολοκλήρου νέοι κανόνες ελέγχου των πακέτων δεδομένων. Οι βασικές δυνατότητες ενός firewall είναι οι εξής:

- Ορίζει ένα μοναδικό σημείο πρόσβασης για την πρόσβαση των εξουσιοδοτημένων χρηστών και τον αποκλεισμό των μη εξουσιοδοτημένων.
- Αποτελεί ένα σημείο αναφορά στο οποίο διατηρείται αρχείο καταγραφή των κινήσεων μεταξύ του δικτύου και του παγκόσμιου ιστού. Επίσης σημαίνει συναγερμό σε περιπτώσεις παραβιάσεων και σφαλμάτων.
- Προστατεύει την ταυτότητα IP του δικτύου ενώ δύναται να δημιουργήσει και εικονικές IP (Virtual Private Network) (V. Selvi, 2014).

Επιπλέον μπορεί να εγκατασταθεί και σε κάθε υπολογιστή ξεχωριστά παρέχοντας επιπλέον προστασία καθώς απομονώνει τις διόδους επικοινωνίας του υπολογιστή που δεν χρησιμοποιούνται από πιθανές επιθέσεις.

Για να επιτευχθεί η μέγιστη δυνατή προστασία του αρχειακού φορέα στο κομμάτι της πληροφορικής και των δικτύων, είναι σαφές ότι πρέπει να χρησιμοποιούνται πολλές τεχνολογίες, τόσο σε επίπεδο software όσο και hardware, συνδυαστικά. Το τοπικό δίκτυο υπολογιστών (Local Area Network) είναι ένα σύνολο υπολογιστών που λειτουργεί σε τοπικό δίκτυο χωρίς να αφήνει το περιθώριο αλληλεπίδρασης, σε κάθε υπολογιστή ξεχωριστά, με τον παγκόσμιο ιστό. Όλα τα αρχεία βρίσκονται σε μια κοινή βάση δεδομένων στην οποία έχει πρόσβαση κάποιος χρήστης μόνο αν χρησιμοποιεί κάποιο υπολογιστή που είναι συνδεδεμένος, ενσύρματα ή ασύρματα, με το δίκτυο. Η

αλληλεπίδραση με τον παγκόσμιο ιστό γίνεται μόνο από έξοδο, όπερ σημαίνει ότι σε αυτή την έξοδο μπορούν τοποθετηθούν πολλαπλές δικλείδες ασφαλείας που λειτουργούν αρμονικά.

Σύμφωνα με τον Michael R. Lyu το τοίχος προστασίας μπορεί να έχει επιπτώσεις στην ταχύτητα του δικτύου. Παρόλα αυτά δεν είναι επαρκώς αξιοσημείωτες για να επηρεάσουν την γενικότερη εικόνα των πλεονεκτημάτων του firewall. Όπως αναφέρθηκε μέσω του τοίχους προστασίας ελέγχονται τα πακέτα δεδομένων ενδελεχώς. Μέσω της τεχνολογίας των proxy servers αλλάζει η ταυτότητα IP, ανά τακτά χρονικά διαστήματα, ώστε να μην είναι ευάλωτη σε επιθέσεις. Επιπλέον διαθέτει μνήμη cache καθώς επίσης διατηρεί logs με όλες τις ιστοσελίδες που έχουν επισκεφτεί οι χρήστες ώστε την επόμενη φορά η πρόσβαση να είναι ταχύτερη. Μια ακόμα τεχνολογία που έχει διαδεδομένη χρήση είναι η μετάφραση της διεύθυνσης του δικτύου (Network Address Translation) η οποία αποκρύπτει την ταυτότητα IP από τις ιστοσελίδες που βρίσκονται στον παγκόσμιο ιστό. Διατηρούνται και με αυτή την τεχνολογία πίνακες με πακέτα δεδομένων ώστε να υπάρχει η δυνατότητα ανακατεύθυνσης των χρηστών στις ιστοσελίδες που ζητούν (Lyu, 2001).

Συμπερασματικά, οι παραπάνω τεχνολογίες λειτουργούν αποδοτικά και έχουν εφαρμοστεί σε πολλούς φορείς τα τελευταία χρόνια. Το τοίχος προστασίας συνδυαστικά με τις υπόλοιπες τεχνολογίες, ελέγχουν τις κινήσεις στο χώρο του δικτύου και ειδοποιούν σε περίπτωση που υπάρχει κάποια πιθανή εισβολή στο σύστημα. Μέσω των αρχείων που διατηρούν κατά τη διάρκεια των συνόδων εξετάζουν αν οι απαντήσεις έρχονται αποκλειστικά από τους ιστοτόπους (HTTP) που έχουν ζητηθεί ενώ τα αρχεία που μεταφέρονται μέσω File Transfer Protocol δεν περιέχουν κακόβουλο λογισμικό. Τέλος αρχεία Simple Mail Transfer Protocol και Post Office Protocol, τα οποία σχετίζονται με το ηλεκτρονικό ταχυδρομείο, τίθενται επίσης υπό εξέταση ελαχιστοποιώντας με αυτή τη μέθοδο και την πιθανότητα εισβολής Tojan και επίθεσης Ransomware (Ogbulezie, 2016).

6.7 R.B.A.C.– Διαχείριση Πρόσβασης βάσει Ρόλων

Μια ακόμη πρακτική που συνεπικουρεί στη χαλύβδωση ενός αρχειακού φορέα από τυχόν επιθέσεις είναι η Διαχείριση Πρόσβασης βάσει ρόλων (Role Base Access Control). Λειτουργεί παράλληλα με τα προηγούμενα μέσα προστασίας και αποσκοπεί στην καταγραφή των κινήσεων των ατόμων που έχουν εξουσιοδοτημένη πρόσβαση στο σύστημα ενός φορέα. Παράλληλα περιορίζει την πρόσβαση μη εξουσιοδοτημένων χρηστών καθώς επίσης καταγράφει τις κινήσεις και τις προσπάθειες πρόσβασης.

Ταυτόχρονα αποτελεί το σύστημα στο οποίο αφού καθοριστούν κάποιοι συγκεκριμένοι «ρόλοι», ανάλογα με τον τίτλο εργασίας των υπαλλήλων, τις υποχρεώσεις και τις δικαιοδοσίες τους, παρέχει επιμερισμένη πρόσβαση στο σύστημα του φορέα αντίστοιχη με τις εργασίες του κάθε υπαλλήλου (Andreas Schaad, 2001).

Στο πλαίσιο της λειτουργίας του R.B.A.C. πρότερος στόχος είναι η κατάλληλη επιλογή ενός συστήματος επιβεβαίωσης της γνησιότητας των χρηστών (authentication). Η πιο γνωστή μέθοδος επαλήθευσης της γνησιότητας είναι η χρήση ονόματος και κωδικού πρόσβασης χρήστη (username / password). Παρόλα αυτά κρίνεται ανεπαρκής καθώς αυτά τα στοιχεία είναι ευάλωτα για υποκλοπή. Γι' αυτόν τον λόγο χρησιμοποιούνται κι άλλες μέθοδοι όπως η χρήση κάρτας, επιβεβαίωση με κωδικό μικρής διάρκειας ζωής που αποστέλλεται στο κινητό, δακτυλικό αποτύπωμα κ.α. (R. S. Sandhu, 1994).

Συνήθως στο πλαίσιο της λειτουργείας ενός φορέα, οι πληροφορίες που σχετίζονται με τις ευθύνες και τις δυνατότητες των εργαζομένων ορίζονται από το τμήμα του Ανθρώπινου Δυναμικού (Human Resources). Ο ρόλος που του αποδίδεται λοιπόν και στο πληροφοριακό σύστημα φέρει τα χαρακτηριστικά που αναλογούν.

Ένα σημαντικό πλεονέκτημα που απορρέει από το σύστημα R.B.A.C. είναι η διατήρηση αρχείου που καταγράφει τις κινήσεις των χρηστών (evidence generation) που εργάζονται στον φορέα και χρησιμοποιούν το πληροφοριακό σύστημα. Το σύνολο των κινήσεων μπορεί να προστεθεί στο αρχείο των υπαλλήλων, είτε είναι ενεργοί είτε είναι ανενεργοί, και να λειτουργεί σαν τεκμήριο σε περιπτώσεις που είναι αναγκαία η απόδειξη πράξεων και αποφάσεων.

Το σύστημα Διαχείρισης Πρόσβασης βάσει Ρόλων προαπαιτείτε να είναι ανοιχτό στις παραμετροποιήσεις και «ελαστικό» - ευέλικτο στον καθορισμό των ρόλων. Πολλά συστήματα παλαιότερων γενεών δεν αναγνώριζαν τους πολλαπλούς ρόλους που ενδέχεται να φέρει ένα μόνο άτομο (single entity -> 2+ functions). Σε περιπτώσεις που άτομα από το προσωπικό βρίσκονται σε άδεια ή είναι εκτός εργασίας λόγω ασθενείας, κρίνεται αναγκαίο να υπάρχουν άτομα που θα αναπληρώσουν τις κενές θέσεις. Αυτό σημαίνει ότι άτομα με συγκεκριμένα functions θα λειτουργούν για συγκεκριμένο χρονικό διάστημα με κάποια διαφορετικά ή με κάποια επιπλέον. Αντίστοιχα σφάλματα διαπιστώνονται στα σενάριο, όπου υπάρχει αδυναμία καταγραφής των κινήσεων και αποφάσεων εντός του συστήματος οι οποίες μάλιστα να συνδυάζονται και διατηρούνται από κοινού με το άτομο που διαχειρίζεται υπό κανονικές συνθήκες την υπόθεση. Ατοπήματα παρόμοια με τα προαναφερθέντα είναι αναγκαίο να διευθετούνται από την

αρχή του σχεδιασμού του συστήματος ώστε να περιορίζονται οι πιθανότητες να προκύψουν στη λειτουργεία του (Andreas Schaad, 2001).

6.7.1 Ιεραρχικά επίπεδα πρόσβασης

Η ιεραρχία των χρηστών προκύπτει από τον σχεδιασμό των ρόλων του συστήματος και δεν διαφέρουν σε μεγάλο βαθμό από την πραγματική μηχανοργάνωση του φορέα. Παραδείγματος χάρη μέσα σε ένα σύστημα οι χρήστες που προβλέπονται μπορεί να είναι οι εξής: i: χρήστες αναγνωστηρίου, ii: υπάλληλοι αναγνωστηρίου, iii: συντηρητές, iv: εξουσιοδοτημένοι ερευνητές - αρχειονόμοι, v: διευθυντές. Στα περισσότερα λοιπόν συστήματα προβλέπεται η κληρονομικότητα των δικαιωμάτων, δηλαδή οι ερευνητές - αρχειονόμοι έχουν πρόσβαση σε ένα σύνολο αρχείων και δυνατοτήτων που δεν έχουν οι συντηρητές και οι υπόλοιπες κατώτερες θέσεις, χωρίς όμως να σημαίνει ότι χρήστες κατώτερων θέσεων έχουν πρόσβαση σε υλικό και δυνατότητες στις οποίες δεν έχουν οι ανώτεροί τους.

Επιπροσθέτως στο πλαίσιο της προσαρμογής ενός συστήματος για έναν φορέα με συγκεκριμένες λειτουργείες, η λειτουργεία του ιεραρχικού μοντέλου μπορεί να περιοριστεί. Με άλλα λόγια υπάρχει δυνατότητα παραμετροποίησης του περιβάλλοντος του συστήματος για να προβάλλει αποκλειστικά οτιδήποτε είναι χρήσιμο και εντός του πλαισίου των εργασιών ενός υπαλλήλου (C.A. Ardagna, 2006).

6.7.2 Κατάτμηση εξουσιών – Separation Duties

Σημαντική στο πλαίσιο της λειτουργείας του R.B.A.C. είναι και η έννοια της κατάτμησης των εξουσιών. Πιο αναλυτικά, μια πιθανή αδυναμία που προκύπτει από το διαχωρισμό ιεραρχικών επιπέδων πρόσβασης είναι ότι ο ανώτερος ρόλος του συστήματος θα συσσωρεύσει όλη την εξουσία. Για να αποκλειστεί λοιπόν το σενάριο λανθάνουσας χρήσης των εξουσιών του υπαλλήλου που φέρει τον ανώτερο ρόλο, ή και κάποιον ανώτερο ρόλο γενικότερα, προβλέπεται σαν καλή πρακτική η κατάτμηση της εξουσίας. Πρέπει δηλαδή να υπάρχει και ένα δεύτερο στάδιο επιβεβαίωσης μιας απόφασης. Για παράδειγμα μια απόφαση για καταστροφή ανενεργού ψηφιακού αρχείου από τη βάση δεδομένων πρέπει να επιβεβαιώνεται τουλάχιστον από έναν ακόμη χρήστη που φέρει ισάξιο ρόλο με τον πρώτο. Κατ' αυτόν τον τρόπο αποφεύγεται η κατάχρηση εξουσιών και σημαντικά λάθη που ενδέχεται να συμβούν και εκ παραδρομής στο πλαίσιο των καθημερινών εργασιών (R. S. Sandhu, 1994).

7 Κεφάλαιο 7ο

7.1 Παράδειγμα οργάνωσης πλάνων από φορείς του εξωτερικού

Τα παρακάτω πλάνα προκύπτουν από έρευνα που έχει εκπονηθεί από τους εμπειρογνώμονες του Παγκόσμιου δικτύου ανάπτυξης Ηνωμένων Εθνών (UNDP). Τα προτεινόμενα πλάνα εκτάκτων αναγκών και επιχειρησιακής συνέχειας αναφέρονται κατά κύριο λόγο στους υπεύθυνους, για την εκπόνηση αυτών, που εργάζονται σε διάφορους φορείς παγκοσμίως. Στην έκδοση λοιπόν που αναφέρεται στους υπευθύνους καθώς και τους εργαζομένους ενός φορέα, προτείνονται οι εξής βασικές διαδικασίες.

Προβλέπεται λοιπόν η οργάνωση και διατήρηση μια ομάδας που θα επωμιστεί την επίβλεψη και έπειτα την εφαρμογή των πλάνων. Τα πλάνα αυτά εκπονούνται από έναν, ή και περισσότερους υπευθύνους, οι οποίοι πρέπει να επιβλέπουν και να καθοδηγούν την έναρξη της κατασκευής των κτιριακών εγκαταστάσεων, προτείνοντας υλικά και μεθόδους διαρρύθμισης. Έπειτα επιλέγουν μεθόδους προστασίας των φυσικών εγκαταστάσεων και επανδρώνουν το τμήμα πληροφορικής για τη δημιουργία ενός συστήματος IT με βάση τα πρότυπα που ορίζονται από τα πλάνα.

Στο πλαίσιο των Πλάνων Ανάπτυξης των Η.Π.Α. προβλέπεται και η ύπαρξη συμβουλευτικών τμημάτων για διευκρινήσεις και συμβουλές αναφορικά με αποφάσεις και παραμετροποιήσεις των πλάνων. Στα παραπάνω τμήματα μπορούν να αποταθούν οι υπεύθυνοι που διαχειρίζονται τα πλάνα διαχείρισης κρίσεων και καταστροφών, ανάκλησης του IT, συνέχισης των σημαντικών υπηρεσιών και επιστροφής στην κανονικότητα.

Προβλέπονται σχέδια αντίδρασης σε καταστάσεις ανάγκης εντός δώδεκα ωρών, 48 ωρών, για τις επόμενες 72 ώρες καθώς και για το μετέπειτα διάστημα έως τους τρεις μήνες. Στο πρώτο στάδιο γίνεται εκτίμηση των επιπτώσεων (στις κτιριακές εγκαταστάσεις, στα συστήματα πληροφορικής, στα αρχεία των φυσικών υποστρωμάτων καθώς και στους συνεργάτες και προμηθευτές, ειδικά σε περιπτώσεις που δεν δύνανται τη συνέχεια των εργασιών τους) από τα μέλη του προσωπικού που τις αντιμετωπίζουν.

Οι υπεύθυνοι των πλάνων πρέπει να διατηρούν συνεχή επικοινωνία με τις συμβουλευτικές υπηρεσίες και να αποστέλλουν αναφορές σχετικά με την πρόοδο των εργασιών και των πιθανών αδυναμιών και δυσκολιών που καλούνται να

αντιμετωπίσουν. Επίσης πρέπει να καθοδηγούν το προσωπικό ώστε να αποφευχθεί ο κίνδυνος και έπειτα να εφαρμοστούν σωστά τα πλάνα. Αξίζει να σημειωθεί ότι στο Πρόγραμμα των Η.Π.Α. για την ανάπτυξη δίνεται βαρύτητα στη διάσωση ή τουλάχιστον τη βοήθεια των οικογενειών των εργαζομένων ενός φορέα.

Εντός του διαστήματος μεταξύ των 12 και 48 ωρών καθώς και στο πλαίσιο των τριών μηνών που έπονται προβλέπεται και η αναθεώρηση του Risk Assessment. Η σειρά των προτεραιοτήτων στο πλαίσιο της εκτίμησης των κινδύνων που υπάρχει μεγάλη πιθανότητα να επηρεαστούν είναι η εξής: ασφάλεια προσωπικού, ασφάλεια κτιριακών εγκαταστάσεων, εξασφάλιση ομαλής λειτουργείας IT, εξασφάλιση παροχής υπηρεσιών από συνεργάτες και προμηθευτές.

Αναφέρεται ότι το προσωπικό των φορέων έχει πρόσβαση σε προμήθειες και υλικά. Για παράδειγμα υπάρχον μπαταρίες και ηλιακοί συλλέκτες ή άλλοι φορτιστές που να είναι κατάλληλοι για σύνδεση σε αυτοκίνητο σε περίπτωση απώλειας ρεύματος. Επίσης αναφέρεται ότι υπάρχουν συσκευές με ασύρματη πρόσβαση στο διαδίκτυο ώστε να συνεχίσουν οι εργασίες σε περίπτωση διακοπή από τον πάροχο τηλεπικοινωνίων.

Στο πλαίσιο των πλάνων αναφέρεται ότι γίνεται και business impact analysis. Πρόκειται για αντιπαραβολή των πιθανών κινδύνων με τις καταστροφές που πράγματι εκδηλώθηκαν καθώς και τις βλάβες που προκλήθηκαν. Έπειτα γίνεται κατανοητός ο αντίκτυπος στις καθημερινές εργασίες του φορέα. Επίσης αναφέρεται ότι τα αντίγραφα ασφαλείας προβλέπεται να διατηρούνται εκτός του βασικού κτιρίου. Στο πλαίσιο της εκπόνησης των πλάνων διατηρείται και αρχείο δραστηριοτήτων και επιπτώσεων για τη βελτίωση των πλάνων.

Τέλος προβλέπεται η εφαρμογή των πλάνων σε μια προσομοίωση που εκτελείται κάθε χρόνο από μια τουλάχιστον φορά για να εξοικειώνεται το προσωπικό και να εντοπίζονται τυχόν αδυναμίες.

7.2 Δημόσια Βιβλιοθήκη της Βέροιας

Παρακάτω παρατίθενται οι απαντήσεις που συγκεντρώθηκαν από την υπεύθυνη της βιβλιοθήκης της Βέροιας, σε συνεργασία με τον υπεύθυνο των υπολογιστικών συστημάτων.

Στο πρώτο σκέλος των ερωτήσεων διατυπώθηκε ότι δεν υπάρχει κάποιος υπεύθυνος για την εκτέλεση των μελετών καθώς και την διατύπωση των πλάνων εκτάκτων αναγκών. Όσον αφορά το δεύτερο σκέλος, αναφέρθηκε ότι το σύνολο του υλικού της βιβλιοθήκης βρίσκεται σε ένα κτίριο. Επίσης αναφέρθηκε ότι το γραφείο πολιτικής

προστασίας της περιφέρειας Ημαθίας ήταν υπεύθυνο για την καταγραφή των σπάνιων κειμηλίων καθώς επίσης κατατόπιζε τους υπευθύνους της βιβλιοθήκης αναφορικά με τις κινήσεις που πρέπει να κάνουν σε περίπτωση ανάγκης. Πιο αναλυτικά αναφέρθηκε ότι υπάρχει πρόβλεψη σε περίπτωση κινδύνου τα σπάνια κειμήλια να μεταφέρονται σε συγκεκριμένο χώρο, ο οποίος όμως δεν ανήκει στη βιβλιοθήκη. Βέβαια αναφέρεται ότι ενημερώσεις αναφορικά με αυτές τις διαδικασίες είναι παρωχημένες καθώς δεν έχουν ανανεωθεί τα τελευταία δέκα χρόνια. Τα τεκμήρια που έχει στην κατοχή της η βιβλιοθήκη βρίσκονται σε ένα κτήριο στο σύνολό τους και τα μορφότυπα στα οποία εκτείνονται είναι τα εξής: ~160.000 βιβλία, ~ 10.000 δίσκοι LP, χαρακτικά, σπάνια βιβλία από το 1700-1800, παραδοσιακές κούκλες κ.α. Στο σύνολό του το υλικό είναι ψηφιοποιημένο, ακόμα και οι κούκλες είναι φωνογραφημένες, στην ιστοσελίδα (http://medusa.libver.gr/jspui/). Στον OPAC υπάρχουν 10.000 εγγραφές, ψηφιοποιημένα βιβλία και εφημερίδες καθώς και φωτογραφίες της περιοχής. Αξίζει να αναφέρουμε ότι η βιβλιοθήκη της Βέροιας έλαβε την πρωτοποριακή απόφαση να φωτογραφήσει την περίοδο της πανδημίας την πόλη το διάστημα των απαγορεύσεων της κυκλοφορίας, δημιουργώντας ένα ξεχωριστό φωτογραφικό αρχείο 500 φωτογραφιών με περιγραφές.

Τα σχέδια της κτιριακής εγκατάστασης εκπονήθηκαν από αρχιτέκτονα με αποκλειστικό σκοπό τη στέγαση βιβλιοθήκης. Το 1999 ολοκληρώθηκαν οι εργασίες κατασκευής του κτιρίου. Έκτοτε υπάρχει διαρκής επίβλεψη από το διευθυντή της βιβλιοθήκης καθώς και από τους εργαζόμενους οι οποίοι βρίσκονται σε μόνιμη επαγρύπνηση και αναφέρουν αμέσως κάθε πιθανή βλάβη. Κατά κύριο λόγο τα υλικά κατασκευής είναι οπλισμένο σκυρόδεμα και τούβλα. Υπάρχουν αισθητήρες πυρασφάλειας και πυρανίχνευσης ενώ δεν υπάρχουν αισθητήρες υγρασίας. Η συντήρηση τους γίνεται ανά 6 μήνες καθώς και κάθε φορά που ενεργοποιείτε ο συναγερμός εσφαλμένα. Τα πατώματα έχουν κατάλληλη αντοχή για το βάρος. Οι διαχωριστικοί τοίχοι δεν υπάρχει πρόβλεψη να είναι πυράντοχοι, παρόλα αυτά υπάρχουν πόρτες τέτοιων προδιαγραφών στο ήμισυ των χώρων της βιβλιοθήκης. Τα συστήματα πυρασφάλειας που χρησιμοποιούνται είναι νερού καθώς και σκόνης στους χώρους όπου φυλάσσονται τα σπάνια βιβλία και τα κειμήλια. Αναφορικά με τα συστήματα εξαερισμού δεν υπάρχει ειδική πρόβλεψη για ιονιστές και απομάκρυνση καπνού. Παρόλα αυτά αναφέρεται ότι υπάρχουν αφυγραντήρες στα υπόγεια της βιβλιοθήκης για να διατηρούνται χαμηλά ποσοστά υγρασίας.

Η βιβλιοθήκη βρίσκεται στο κέντρο της πόλης η οποία δεν είναι πυκνοκατοικημένη ενώ στο μπροστινό μέρος υπάρχει πλατεία. Δεν βρίσκεται κοντά σε διυλιστήρια και

βιομηχανικές περιοχές, αποφεύγοντας τους ατμοσφαιρικούς ρύπους. Οι καθαρισμοί του κτιρίου γίνονται σε εβδομαδιαία βάση και οι απεντομώσεις μια φορά το χρόνο. Για άλλη μια φορά αναφέρεται ότι το προσωπικό μεριμνά για τους χώρους ενώ κάθε φορά που παρατηρείται κάποιας μορφής μόλυνση διενεργούνται οι κατάλληλες ενέργειες.

Δεν υπάρχει risk assessment, και δεν υπάρχουν μέλη του προσωπικού επιφορτισμένα με την εκτέλεση πρώτων βοηθειών ή κατάσβεσης. Αναφέρεται όμως ότι όλο το προσωπικό καλεί τις αρμόδιες αρχές σε περίπτωση ανάγκης. Δεν υπάρχει γραπτός κατάλογος με τεκμήρια που πρέπει να διασωθούν κατά προτεραιότητα σε περίπτωση κινδύνου. Υπάρχει ειδικός εξοπλισμός όπως μάσκες, γάντια και γυαλιά για να προφυλάσσουν από τη σκόνη και τα ακάρεα που υπάρχουν πάνω σε παλιά βιβλία. Επίσης υπάρχουν πυροσβεστήρες σε διάφορα μέρη της βιβλιοθήκης.

Αναφορικά με τα συστήματα πληροφόρησης της βιβλιοθήκης, υπάρχει LAN με παραμετροποιήσεις για την εξασφάλιση της μέγιστης ασφάλειας του φορέα. Υπάρχουν UPS σε κάθε υπολογιστή που λειτουργεί ως server καθώς και στο κτίριο για τη διατήρηση λυχνιών κινδύνου. Τα αντίγραφα ασφαλείας δημιουργούνται σε πραγματικό χρόνο ενώ ορίζονται και εκδόσεις στα αρχεία των αντιγράφων. Επίσης όλα τα backups μεταφορτώνονται και στο cloud «One Drive for business». Υπάρχει διαφορετικό δίκτυο για τους υπολογιστές και το δίκτυο του κοινού από το δίκτυο των υπαλλήλων της βιβλιοθήκης. Επίσης χρησιμοποιείται firewall για τον αποκλεισμό της πρόσβασης σε διάφορες σελίδες του παγκόσμιου ιστού. Επιπροσθέτως αναφέρεται ότι το προσωπικό είναι εξοικειωμένο με τους κινδύνους που υπάρχουν στο διαδίκτυο.

Αναφορικά με την επιχειρησιακή συνέχεια υπάρχουν γεννήτριες ηλεκτρισμού με τη καύση πετρελαίου καθώς και εφεδρικοί φορητοί υπολογιστές για χρήση σε περίπτωση αστοχίας του συστήματος. Ο server σε περίπτωση αστοχίας του υλισμικού μπορεί να μεταφερθεί σε άλλο υπολογιστή, διότι είναι εικονικός, ο οποίος όμως να έχει τις ίδιες προδιάγραφες. Υπάρχουν τρεις υπολογιστές με κατάλληλες προδιαγραφές για να δεχτούν τον server. Τέλος η βιβλιοθήκη διαθέτει δυο γραμμές για παροχή διαδικτύου για τις περιπτώσεις που υπάρχουν βλάβες στο σύστημα του παρόχου ή για τις περιπτώσεις που οι ταχύτητες σύνδεσης είναι πολύ χαμηλές.

Τέλος δεν υπάρχει πλάνο διαχείρισης πρόσβασης βάσει ρόλων στους φυσικούς χώρους της βιβλιοθήκης.

Συμπερασματικά η βιβλιοθήκη της Βέροιας βασίζεται στο επαρκώς ενημερωμένο προσωπικό για τον εντοπισμό βλαβών στις εγκαταστάσεις καθώς και για την αποφυγή κακόβουλου λογισμικού. Το σύστημα πληροφόρησης όλα τα βασικά μέσα προστασίας,

διαθέτει διαφορετικά δικτυακά περιβάλλοντα ανάλογα με τον τύπο του χρήστη, ενώ υπάρχουν προβλέψεις για την επιχειρησιακή συνέχεια. Με άλλα λόγια, παρόλο που δεν υπάρχουν αναλυτικά πλάνα εκτάκτων αναγκών, εκτίμησης κινδύνου και επιχειρησιακής συνέχειας όπως ορίζει η βιβλιογραφία, η βιβλιοθήκη φέρει της όσο το δυνατόν επαρκέστερες, με βάση τους περιορισμούς της χρηματοδότησης, προδιαγραφές για τις καταστάσεις κινδύνων.

7.3 Αρχείο τράπεζας Eurobank

Η τράπεζα Eurobank αποτελεί ένα πολύ καλό παράδειγμα εφαρμογής των πλάνων που έχουν αναφερθεί παραπάνω. Ο υπεύθυνος της εκπόνησής τους κύριος Πριναράκης Ελευθέριος ήταν προθυμότατος να απαντήσεις στο ερωτηματολόγιο και οι απαντήσεις του ήταν πολύ κατατοπιστικές.

Αρχικά, από το πρώτο σκέλος των ερωτήσεων φάνηκε ότι υπάρχει υπεύθυνος για την εκπόνηση των πλάνων στον αρχειακό φορέα ο οποίος μάλιστα είναι σε ώριμη ηλικία, είναι κατάλληλα καταρτισμένος, καθώς το επίπεδο σπουδών του είναι μεταπτυχιακό, και διαθέτει δεκαπενταετή προϋπηρεσία. Γίνεται λοιπόν κατανοητό ότι γνωρίζει με πρακτικές εφαρμογές αλλά και με θεωρητικές λεπτομέρειες τα καθήκοντα που του έχουν ανατεθεί.

Στο δεύτερο σκέλος των απαντήσεων αναφέρεται ότι το αρχείο της Eurobank βρίσκεται σε τέσσερα διαφορετικά κτίρια ανάλογα με το είδος του υλικού. Το ενεργό και το ημιενεργό αρχείο δεν βρίσκονται σε χώρο από κοινού με το ανενεργό αλλά στεγάζεται σε μισθωμένες αποθήκες συνεργατών. Γενικότερα στα αρχεία δεν έχει δοθεί ακόμη πρόσβαση σε ερευνητικό κοινό ενώ δεν έχει σημειωθεί ποτέ κάποια βλάβη κατά τη μεταφορά του. Πιο συγκεκριμένα τα υποστρώματα του αρχείου είναι χαρτώα, ηλεκτρονικά και ψηφιακά, με μορφότυπα doc, xls, pdf, ppt, tif, png, jpeg, παρόλα αυτά αναφέρεται ότι δεν διατηρούνται ξεχωριστά οι σκληροί δίσκοι. Τέλος τα αντίγραφα ασφαλείας των ψηφιακών αρχείων καθώς και τα ανενεργά διατηρούνται σε μικρότερη από δέκα χιλιόμετρα απόσταση ενώ τα ημιενεργά και τα ενεργά σε αποστάσεις άνω των τριάντα χιλιομέτρων.

Στο τρίτο σκέλος ο υπεύθυνος μας πληροφορεί ότι οι κτηριακές κατασκευές όπου στεγάζονται τα αρχεία διαθέτουν σύγχρονα συστήματα πυρασφάλειας και αποφυγής πλημμυρών. Όσο για τον έλεγχο της θερμοκρασίας υπάρχει το αυτοματοποιημένο σύστημα BMS[1] και σύστημα FANCOIL για τις μονάδες κλιματισμού. Υπάρχουν

[1] Building management system είναι ένα σύστημα που αποσκοπεί στον αυτοματοποιημένο έλεγχο ενός κτιρίου. Ελέγχει και παρέχει πληροφορίες για τα συστήματα HVAC, για την ύπαρξη καπνού, σκόνης, το επίπεδο καθαριότητας, θερμοκρασία, υγρασίας, ξέσπασμα διαρροής, βλάβης ηλεκτρολογικών εγκαταστάσεων καθώς και για την κατάσταση των συστημάτων καταιονισμού (Joseph, 2018).

αισθητήρες καπνού και νερού για να υπάρχει η δυνατότητα σύντομης αντιμετώπισης μιας πλημμύρας ή μιας φωτιάς. Οι σωλήνες των υδραυλικών του κτηρίου δεν περνούν μέσα από το χώρο του αρχειοστασίου ενώ επίσης υπάρχει πρόληψη και το αρχείο τοποθετείται σε απόσταση 30 εκατοστών από το πάτωμα. Η κτηριακή κατασκευή διαθέτει πυράντοχες πόρτες για να μην μεταδίδεται η θερμότητα. Το σύστημα καταιονισμού που χρησιμοποιείται είναι το FM200 (μη τοξικό αέριο που φυλάσσεται σε υγρή μορφή υπό πίεση) ενώ επίσης για την κατάσβεση υπάρχουν πυροσβεστήρες χειρός σε όλους του χώρους. Επίσης το κτίριο αφενός δεν βρίσκεται σε σεισμογενή περιοχή και αφετέρου διαθέτει κατάλληλες αντισεισμικές προδιαγραφές. Τα πατώματα έχουν κατάλληλη αντοχή για το βάρος ενώ τα τοιχώματα που διαχωρίζουν τους χώρους παρακωλύουν τη μεταφορά θερμότητας. Τέλος αναφέρεται ότι υπάρχει κεντρικό σύστημα εξαερισμού με ιονιστή που αποτρέπει την εισβολή βλαπτικών παραγόντων.

Στο τέταρτο σκέλος αναφέρεται ότι κάποια από τα αρχειοστάσια της Eurobank βρίσκονται σε πυκνοκατοικημένες περιοχές παρόλα αυτά όμως δεν φέρουν τον κίνδυνο μόλυνσης από απορρίμματα και τον κίνδυνο πυρκαγιάς από βενζινάδικα που βρίσκονται πλησίον τους. Πρόβλεψη υπάρχει και για τις απεντομώσεις και τις απολυμάνσεις που πραγματοποιούνται δυο ανά έξι μήνες. Επίσης κανένα από τα αρχειοστάσια δεν βρίσκεται κοντά σε διυλιστήρια.

Στο πέμπτο σκέλος αναφέρεται ότι δεν υπάρχει risk assessment. Στο πλαίσιο των γνώσεων του προσωπικού σημειώνεται ότι υπάρχει διαθέσιμος γιατρός σε κάθε κτίριο ενώ πραγματοποιούνται σεμινάρια για την ορθή χρήση των μέσων κατάσβεσης. Τα πλάνα είναι γνωστά στο προσωπικό και εκτελούνται από συντονιστή για τον οποίο υπάρχει και αντικαταστάτης. Δοκιμές των πλάνων γίνονται κάθε χρόνο ενώ οι υπάλληλοι έχουν πρόσβαση σε υλικά για τον περιορισμό πλημμύρας μικρής έκτασης (στυπόχαρτα, πλαστικά γάντια και ρόμπες που δεν είναι αγώγιμα στο ρεύμα).

Στο έκτο σκέλος αναφορικά με τα τις υπηρεσίες ηλεκτρονικών συστημάτων διαπιστώνεται ότι έχουν ληφθεί όλα τα σύγχρονα μέσα προστασίας των υπολογιστών σε επίπεδο λογισμικού και υλισμικού. Η συχνότητα με την οποία δημιουργούνται τα αντίγραφα ασφαλείας είναι δυο φορές το χρόνο ενώ δεν γίνεται χρήση της τεχνολογίας του υπολογιστικού νέφους. Υπάρχουν περιορισμοί στα συστήματα IT τα οποία προστατεύουν τους υπαλλήλους οι οποίοι όμως δεν γνωρίζουν στο σύνολό τους τους πιθανούς κινδύνους διαδικτυακής απάτης που ενδέχεται να εκτεθούν.

Στο έβδομο σκέλος δεν αποτελεί έκπληξη το γεγονός ότι ένας φορέας σχετικός με τα τραπεζικά συστήματα γνωρίζει και εφαρμόζει το R.B.A.C. στον ψηφιακό και στον φυσικό

χώρο. Επίσης πληροφορούμαστε ότι υπάρχει και προσωπικό υπεύθυνο για την προστασία του κτιρίου (security).

Τέλος στο όγδοο σκέλος γίνεται αναφορά στο πλάνο επιχειρησιακής συνέχειας που εφαρμόζεται στο αρχείο της Eurobank καθώς έχουν επιλεχθεί μέθοδοι και τρόποι λειτουργείας ώστε οι υπηρεσίες να μην διακόπτονται σε περιπτώσεις ανάγκης. Τα αρχειοστάσια διαθέτουν γεννήτριες ηλεκτρισμού με χρήση πετρελαίου. Επίσης σε περίπτωση βλάβης ενός υπολογιστή υπάρχουν εφεδρικοί. Τέλος αναφέρεται ότι υπάρχει και εφεδρικός server όμως αυτό δεν αφορά τις λειτουργείες του αρχειακού φορέα, ενώ επίσης δεν υπάρχει πρόβλεψη και για εφεδρικούς παρόχους ηλεκτρισμού και διαδικτύου.

7.4 Συμπεράσματα

Η συμμετοχή των φορέων ήταν ιδιαίτερα χαμηλή καθώς στην πλειοψηφία τους δεν διέθεταν κάποιον υπάλληλο αποκλειστικά αφοσιωμένο στην εκπόνηση των πλάνων. Έγινε λοιπόν σαφές ότι το βάρος της συμπλήρωσης του ερωτηματολογίου επιβάρυνε εργαζομένους που δεν είχαν αρκετό χρόνο να απαντήσουν στο πλαίσιο των καθημερινών τους υποχρεώσεων. Ενώ ταυτόχρονα φάνηκε ότι υπήρχε αδυναμία από όλους τους φορείς καθώς τα πλάνα εκτάκτων αναγκών είναι κάποια πρόχειρα σχέδια χωρίς να έχει δοθεί η επιμέλεια που τους αναλογεί. Σημαντική ήταν και η παρατήρηση που προέκυψε από την τηλεφωνική επικοινωνία, καθώς όταν οι απλοί υπάλληλοι των φορέων, οι οποίοι θα κληθούν να εκτελέσουν τα πλάνα, δεν γνώριζαν καν περί τίνος πρόκειται. Επίσης από γενικότερη εμπειρία που δεν αποτυπώθηκε σε επίσημη μορφή απάντησης, έγινε αντιληπτό ότι μόνο στο πλαίσιο των συστημάτων πληροφόρησης υπήρχε ενημέρωση και εκπαίδευση προσωπικού, χωρίς όμως να είναι γνωστό αν ήταν συστηματική και ανά τακτά χρονικά διαστήματα.

Συγκριτικά τα στοιχεία που συγκεντρώθηκα από τους δυο φορείς (Βιβλιοθήκη Βέροιας και αρχείο Eurobank) αποτύπωσαν μια μικρογραφία των συνθηκών που επικρατούν γενικότερα. Αφενός μια βιβλιοθήκη δεν χρειάζεται να έχει τόσο αυστηρά σχέδια αναφορικά με τα πλάνα επιχειρησιακής συνέχειας καθώς η διακοπή παροχής των υπηρεσιών της δεν θα προκαλέσει τεράστια αναστάτωση σε εκατοντάδες χρήστες που δεν θα μπορούν να εκτελέσουν τις καθημερινές τους διαδικασίας (πληρωμές, μεταφορές χρημάτων, αλλαγές σε πληροφορίες προσωπικών δεδομένων).Τα πλάνα διαχείρισης πρόσβασης επίσης μπορούν να είναι πιο ελαστικά σε μια βιβλιοθήκη καθώς υπάρχει μικρότερη πιθανότητα να διαθέτει έγραφα με προσωπικά δεδομένα ατόμων. Όσον αφορά όμως τα πλάνα εκτάκτων αναγκών, τόσο στις υποδομές του κτιρίου όσο και στο κομμάτι της πληροφορικής, και στη μελέτη των πιθανών κινδύνων δεν θα έπρεπε να συναντάμε σημαντικές διαφορές. Παρόλα αυτά παρατηρείται ότι ο τραπεζικός φορέας διαθέτει υπεύθυνο για τον σχεδιασμό των πλάνων, ο οποίος μάλιστα έχει επιλέξει σύγχρονα συστήματα προστασίας και έχει λάβει όλα τα κατάλληλα προληπτικά μέτρα.

Συνοψίζοντας η διαφορά μεταξύ των δυο φορέων επηρεάζεται σε έναν σημαντικό βαθμό και από τη χρηματοδότηση. Παρόλο που η βιβλιοθήκη μπορεί να δέχεται δωρεές ανά διαστήματα, τα έξοδα για τη διατύπωση των πλάνων, τη συντήρηση των μέτρων προστασίας, του κατάλληλου προσωπικού που θα επωμιστεί την ευθύνη για την εκπόνηση των παραπάνω καθώς και την εκπαίδευση του προσωπικού είναι πολύ μεγαλύτερης κλίμακας από το χρηματικό ποσό που μπορεί να συγκεντρώσει μια

βιβλιοθήκη μέσω μια κρατική χρηματοδότησης. Γίνεται λοιπόν κατανοητό ότι εύλογα οι δυο φορείς απέχουν παρασάγγας καθώς η τεχνική κατάρτιση και οι θεωρητικές γνώσεις έχουν μεγάλο κόστος στην εφαρμογής τους.

Τέλος αξίζει να σημειωθεί ότι υπήρχαν και κάποιοι φορείς που δεν διέθεταν σχέδια για διαδικασίες σε περιπτώσεις κινδύνων. Επίσης με εξαίρεση τη βιβλιοθήκη της Βέροιας, οι φορείς που δεν έστειλα ξεκάθαρη απόρριψη για την κατάθεση των απαντήσεών τους, αφήσαν την επικοινωνία μονόπλευρη χωρίς να αναφέρουν έστω ότι υπήρχε αδυναμία απάντησης την παρούσα χρονική περίοδο.

Παράρτημα – Ερωτηματολόγιο

Σχετικά με το ερωτηματολόγιο

Το ερωτηματολόγιο διατυπώθηκε με σκοπό να διαπιστωθεί η συνέπεια των ελληνικών φορέων στις προδιαγραφές που ορίζει η διεθνής βιβλιογραφία. Επίσης εξετάζεται κατά πόσον υπάρχει η κατάλληλη μέριμνα για τα πλάνα εκτάκτων αναγκών, μια θέση ευθύνης για έναν έμπειρο υπεύθυνο για την εκπόνησή τους καθώς και την επικοινωνία τους στους υπαλλήλους του φορέα. Επίσης λειτουργεί και ως μια μέθοδος συλλογής πληροφοριών. Έπειτα από έρευνα διαπιστώθηκε ότι έρευνα με αποκλειστική θεματολογία τα πλάνα εκτάκτων αναγκών αρχειακών φορέων απουσιάζει από τον ελληνικό χώρο.

Στόχος είναι η σκιαγράφηση των μεθόδων λειτουργείας των φορέων σε καθημερινή βάση καθώς και η λεπτομερής αποτύπωση των αποφάσεων που έχουν ληφθεί από τους αρμόδιους. Φερειπείν μέσα από τους κανόνες που εχουν οριστεί από έναν υπεύθυνο ή τις αποφάσεις για θέματα όπως η γεωγραφική τοποθεσία, οι κτιριακές εγκαταστάσεις κ.α. προβάλεται η οργάνωση και η εκ προοιμίου πρόθεση του φορέα για πρόληψη από πιθανούς κινδύνους. Επιπροσθέτως υπάρχουν ερωτήσεις που εξετάζουν ενδελεχώς τις πρακτικές που έχουν επιλεχθεί στα πλάνα εκτάκτων αναγκών, τόσο για τα φυσικά όσο και για τα ψηφιακά υποστρώματα, τα πλάνα διαχείρισης πρόσβασης και τέλος τα πλάνα επιχειρησιακής συνέχειας.

Οι ερωτήσεις που επιλέχθηκαν είναι όλες ανοιχτού τύπου, όπως προαναφέρθηκε διότι σκοπός ήταν η άντληση πληροφοριών στο μέγιστο δυνατό βαθμό και όχι η συγκέντρωση μαθηματικών δεδομένων για σύγκριση. Παρακάτω ακολουθεί μια σύντομη ανάλυση περιεχομένου από τα οκτώ σκέλη του ερωτηματολογίου.

Στο πρώτο σκέλος του ερωτηματολογίου εξετάζεται αν υπάρχει κάποια θέση εργασίας στο φορέα με αποκλειστική αφοσίωση τα πλάνα εκτάκτων αναγκών, διαχείρισης πρόσβασης και επιχειρησιακής συνέχειας καθώς και την αποκλειστική ευθύνη για τη σωστή διεξαγωγή και την αναβάθμισή τους. Πιο συγκεκριμένα ζητούνται πληροφορίες αναφορικά με την εμπειρία και την τεχνογνωσία του υπεύθυνου.

Στο δεύτερο σκέλος προβάλλεται ο τρόπος διαχείρισης του συνόλου του αρχειακού υλικού σε σχέση με την τοποθέτησή του στις κτιριακές εγκαταστάσεις του φορέα. Επίσης αναφέρονται κάποια σχετικά παραδείγματα από τη βιβλιογραφία με στόχο να κατευθύνουν τους διερωτόμενους στην επιθυμητή απάντηση.

Το τρίτο σκέλος εξετάζει τις αρχιτεκτονικές προδιαγραφές που έχουν δοθεί μέσα από μελέτες στις κτιριακές εγκαταστάσεις ανάλογα με το πώς προορίζεται να χρησιμοποιηθούν. Έπειτα από μελέτη της βιβλιογραφίας διαπιστώθηκε ότι τα πλάνα εκτάκτων αναγκών και διαχείρισης πρόσβασης, για να εφαρμόζονται και να εκτελούνται με επιτυχία, κρίνεται αναγκαίο να έχουν δοθεί κατάλληλες προδιαγραφές στα κτίρια των αρχειακών φορέων πριν αρχίσει η ανέγερσή τους.

Το τέταρτο σκέλος περιέχει ερωτήσεις που εξετάζουν τη γεωγραφική τοποθεσία του αρχειακού φορέα. Οι κατάλληλες κτιριακές προδιαγραφές πρέπει να έχουν εκτελεστεί και στη σωστή γεωγραφική τοποθεσία. Με άλλα λόγια η περιοχή ανέγερσης διαδραματίζει σημαντικό ρόλο στην αποφυγή διαφόρων βλαβερών περιβαλλοντικών παραγόντων για το αρχειακό υλικό καθώς και πιθανών εξογενών κινδύνων.

Το πέμπτο σκέλος του ερωτηματολογίου περιέχει τις βασικότερες ερωτήσεις που καταδεικνύουν την οργάνωση ενός φορέα και τα προληπτικά μέτρα που έχει λάβει στο πλαίσιο των πλάνων εκτάκτων αναγκών. Εξετάζεται επίσης η γνώση του προσωπικού σε ο,τι αφορά τα πλάνα κι τους πιθανούς κινδύνους, καθώς το τελευταίο πρόκειται να κληθεί να εφαρμόσει τα πλάνα σε μια κρίσιμη στιγμή.

Έπειτα στο έκτο σκέλος αφού προηγουμένως προβάλεται αν υπάρχουν κατάλληλες κτιριακές εγκαταστάσεις που προστατεύουν κυρίως τα φυσικά αρχειακά υποστρώματα, εξετάζονται οι μέθοδοι προστασίας από κυβερνοεπιθέσεις και πιθανές αστοχίες των πληροφοριακών συστημάτων.

Προχωρώντας το έβδομο σκέλος διαθέτει ερωτήσεις σχετικές με τα πλάνα διαχείρισης πρόσβασης βάσει ρόλων. Παραπάνω έγινε αναφορά στο κατά πόσον θα μπορούσε να φανεί χρήσιμο ένα τέτοιο πλάνα και σε έναν αρχειακό φορέα. Μέσα από τις ερωτήσεις λοιπόν διαπιστώνεται σε ποιο βαθμό έχει υιοθετηθεί και εφαρμόζεται ένα τέτοιο πλάνο.

Τέλος στο όγδοο σκέλος εξετάζεται η ύπαρξη πλάνου επιχειρησιακής συνέχειας. Υπάρχουν ερωτήσεις για να διαπιστωθεί αν έχει γίνει μελέτη των παρεχόμενων υπηρεσιών που κρίνονται αναγκαίες από το φορέα να συνεχίζουν να είναι αδιάλειπτα διαθέσιμες.

Ακολουθεί το ερωτηματολόγιο:

A. Ερωτήσεις σχετικές με το υπόβαθρο του υπευθύνου για τα Πλάνα Εκτάκτων αναγκών

1. Ηλικία:

   i)20-30 ii)31-40 iii)41-50 iv)51+

2. Επίπεδο σπουδών, υπάρχει σχετικότητα με τα πλάνα διαχείρισης εκτάκτων αναγκών (Δευτεροβάθμια εκπαίδευση, Τριτοβάθμια εκπαίδευση, Μεταπτυχιακό, Διδακτορικό)
3. Υπάρχει προϋπηρεσία σε σχετικό φορέα με αντίστοιχες ευθύνες; Αν ναι πόσα χρόνια προϋπηρεσία

B. Επιλογές που σχετίζονται με την τοποθέτηση του αρχείου:

1. Το αρχείο του φορέα βρίσκεται στο σύνολό του σε ένα κτήριο;

   (Κοινός χώρος ενεργού και ανενεργού αρχείου, συνέπειες από επισκέπτες ή από τη μεταφορά του ενεργού αρχείου με φορτηγά)
2. Ποια είναι τα μορφότυπα – υποστρώματα του αρχείου;

   (Κοινό αρχειοστάσιο για έντυπα, φωτογραφίες, σκληρούς δίσκους, κ.τ.λ. Εξασφαλίζονται οι κατάλληλες συνθήκες θερμοκρασίας – υγρασίας για κάθε κατηγορία αρχείου;)
3. Διατηρούνται αντίγραφα ασφαλείας των αρχείων ή μέρους των αρχείων; Αν ναι, στον ίδιο χώρο; (Διεθνής βιβλιογραφία αναφέρει: το εφεδρικό κτίριο πρέπει να βρίσκεται σε απόσταση 30 χιλιομέτρων από το βασικό κτίριο του φορέα για να μην πληγεί από τις ίδιες φυσικές καταστροφές)

C. Προδιαγραφές κτιριακής εγκατάστασης:

1. Τα υλικά κατασκευής έχουν κατάλληλες προδιαγραφές για αντοχή σε περίπτωση σεισμού, διατήρηση θερμοκρασίας εσωτερικών χώρων;
2. Υπάρχουν αισθητήρες για έλεγχο θερμοκρασίας και υγρασίας στο αρχειοστάσιο;

   (Σύντομη αντιμετώπιση πιθανής πλημμύρας ή φωτιάς)
3. Ποια υλικά κατασκευής χρησιμοποιήθηκαν κυρίως; (οπλισμένο σκυρόδεμα, τούβλα, ξύλο, πέτρα)
4. Τα πατώματα έχουν κατάλληλη αντοχή για το βάρος;

5. Τα τοιχώματα που διαχωρίζουν τους χώρους του αρχείου έχουν προδιαγραφές για τη διατήρηση σταθερής θερμοκρασίας μεταξύ των δωματίων σε περίπτωση πυρκαγιάς;
6. Τι συστήματα πυρασφάλειας χρησιμοποιούνται;

   (Σκόνης, Co2, νερού; Αν είναι νερού τα dexion έχουν την κατάλληλη αντοχή για το παραπάνω βάρος;)
7. Το σύστημα εξαερισμού είναι κατάλληλο για την μη μεταφορά του καπνού; Έχει ιονιστή και αφυγραντήρα ;

   (Αποφυγή εισαγωγής ρύπων και σκόνης)

D. Ερωτήσεις σχετικά με την τοποθεσία του αρχείου:
   1. Το αρχείο βρίσκεται σε πυκνοκατοικημένη περιοχή;

      (Πιθανότητα μόλυνσης από απορρίμματα/σκουπίδια, πιθανότητα φωτιάς σε κοντινή τοποθεσία π.χ. βενζινάδικο ή βανδαλισμός)
   2. Με τι συχνότητα γίνονται απεντομώσεις, καθαρισμοί στους εξωτερικούς και στους εσωτερικούς χώρους καθώς και στα φρεάτια της εγκατάστασης;
   3. Το αρχείο βρίσκεται κοντά σε βιομηχανική περιοχή η διυλιστήρια;

      (Αυξημένη ατμοσφαιρική μόλυνση)

E. Πλάνα έκτακτων αναγκών και τρόποι αντιμετώπισης και ανάκλησης καταστροφών και απολεσθέντων - Εκπαίδευση προσωπικού
   1. Υπάρχει αναλυτική μελέτη πιθανών κινδύνων και αν ναι, υπάρχει κλιμάκωση κινδύνων με βάση την πιθανότητα εκδήλωσης; (Risk Assessment)
   2. Υπάρχουν μέλη του προσωπικού με γνώσεις πρώτων βοηθειών και/ή κατάσβεσης;
   3. Το πλάνο εκτάκτων αναγκών είναι γνωστό στο σύνολο του προσωπικού ή είναι επιφορτισμένο με την εκτέλεσή του σε περιορισμένο αριθμό ατόμων;
   4. Γίνονται δοκιμές εφαρμογής του σχεδίου;
   5. Υπάρχει κατάλογος με χώρους ή τεκμήρια που πρέπει να διασωθούν κατά προτεραιότητα σε περίπτωση έκτακτης ανάγκης;
   6. Το προσωπικό έχει πρόσβαση σε ειδικό εξοπλισμό;

      (Σε περίπτωση πλημμύρας: μπότες και ποδιές από υλικά που δεν αποτελούν αγωγούς ηλεκτρισμού. Σε περίπτωση μεταφοράς-συντήρησης μουχλιασμένου υλικού υπάρχουν στολές, γάντια, πλαστικά γυαλιά και μάσκες (τύπου N,R, P-95))

7. Υπάρχουν μέτρα περιορισμού της έκτασης των καταστροφών (π.χ. αντιμετώπιση φωτιάς μέχρι να φτάσει η πυροσβεστική, γενικός διακόπτης παροχής νερού/ηλεκτρισμού)

F. Πλάνα εκτάκτων αναγκών για τις υπηρεσίες ηλεκτρονικών συστημάτων DRP-IT
   1. Υπάρχει σύστημα τύπου LAN στο οποίο να είναι συνδεδεμένοι οι υπολογιστές του φορέα για να προστατεύονται από εξωτερικές επιθέσεις;
   2. Υπάρχουν UPS σε κάθε υπολογιστή;
   3. Με τι συχνότητα δημιουργούνται αντίγραφα ασφαλείας (backups) ψηφιακών αρχείων;
   4. Χρησιμοποιείται cloud για αποθήκευση αντιγράφων ασφαλείας;
   5. Χρησιμοποιούνται τεχνολογίες όπως firewall, proxy server, Network Address Translation και VPN;
   6. Το προσωπικό εκπαιδεύεται για τους πιθανούς κινδύνους που ενδέχεται να κληθεί να αντιμετωπίσει; (ransomware, phishing, trojans, dumpster diving)

G. Διαχείριση Πρόσβασης βάσει ρόλων (Role Base Access Control)
   1. Υπάρχει R.B.A.C.; Αν ναι σε επίπεδο φυσικής πρόσβασης ή και σε ψηφιακό επίπεδο;
   2. Πως γίνεται η πρόσβαση; (καρτελάκια barcode, QR, NFC)
   3. Υπάρχει προσωπικό υπεύθυνο για την ασφάλεια του χώρου (security);

H. Πλάνο Επιχειρησιακής Συνέχειας - Business Continuity Plan
   1. Υπάρχει πλάνο επιχειρησιακής συνέχειας;
   2. Αν ναι, υπάρχουν προτεραιότητες υπηρεσιών που κρίνεται αναγκαίο να παραμένουν αδιάλειπτες ακόμα και στο διάστημα ανάκτησης του προβλεπόμενου συστήματος λειτουργείας;
   3. Υπάρχουν γεννήτριες ηλεκτρισμού (πετρελαίου, αερίου, μπαταρίες);
   4. Υπάρχουν εφεδρικοί υπολογιστές για να χρησιμοποιηθούν σε περίπτωση αστοχίας του συστήματος;
   5. Υπάρχει εφεδρικός server με ψηφιακά αντίγραφα ασφαλείας; Αν ναι, πόσος χρόνος θα χρειαστείς για την πλήρη λειτουργεία του;
   6. Υπάρχουν εφεδρικοί προμηθευτές και πάροχοι (ηλεκτρισμού, διαδικτύου);

Βιβλιογραφία

Πανεπιστήμιο Πατρών. (2005). Εργαστήριο Πληροφοριακών Συστημάτων Υψηλών Επιδόσεων. Στο *Οδηγός Καλών Πρακτικών για την Ψηφιοποίηση και τη Μακροπρόθεσμη Διατήρηση Πολιτιστικού Περιεχομένου.* Πάτρα.

Adrienne Muir, S. S. (2002). If the worst happens: the use and effectiveness of disaster plans in libraries and archives.

Albright, G. (1999). Emergency Salvage of Wet Photographs. NEDCC.

Al-Saadoon, G. M. (2011). A Comparison of Trojan Virus Behavior in Linux and Windows Operating Systems. *World of Computer Science and Information Technology Journal (WCSIT), 1*(3), 56-62.

Andreas Schaad, J. M. (2001). The Role-Based Access Control System of a European Bank: A Case Study and Discussion. *ymposium on Access Control Models and Technologies. 1*, σσ. 3-9. Chantilly: ACM.

Artim, N. (1999). *NEDCC*. Ανάκτηση 09 01, 2021, από https://www.nedcc.org/free-resources/preservation-leaflets/3.-emergency-management/3.2-an-introduction-to-fire-detection,-alarm,-and-automatic-fire-sprinklers

Brahim Herbane, D. E. (2004). Business Continuity Management: Time for a Strategic Role? *Long Range Planning, 37*, 435–457. doi:10.1016/j.lrp.2004.07.010

Brosius, M. (2004). Ancient Archives and Archival Traditions: Concepts of Record-keeping in the Ancient World. Oxford University Press.

Brosius, P. (2004). *Seeing natural and cultural communities: Technologies of visualization in conservation.* (University of California εκδ.). Berkeley: Paper delivered at EP colloquium.

Brothy, P. (2007). *The library in the twenty-first century.* London: Facet Publishing.

C.A. Ardagna, M. C. (2006). A Privacy-Aware Access Control System. *Annual IFIP WG 11.3 Working Conference on Data and Applications Security.* Sophia Antipolis.

Chongbin Tang, S. C. (2019). *A Large-Scale Empirical Study on Industrial Fake Apps.* Pwnzen Infotech Inc, Nanyang Technological University, Singapore, China.

Dareste, R. .. (1882). Bulletin de Correspondance Hellénique,.

Dinesh Alawanthan, M. D. (2017). Information Technology Disaster Recovery Process Improvement in Organization Problem Diagnosis and Research Gap. *ICRIIS .*

Dorge, V. (1999). *Building an Emergency Plan.* Los Angeles: The Getty Conservation Institute.

Douglas Steigerwald, G. V. (2011). *The Underground Economy of Fake Antivirus Software.* UC Santa Barbara. Departmental Working Papers. Ανάκτηση 11 10, 2020, από https://escholarship.org/uc/item/7p07k0zr

Duran, M. (2013). An Archaeology of Mediterranean Diplomacy: the Evidence of Paradiplomacy. *International Journal of Euro-Mediterranean Studies, 5*, 147-158. doi:https://doi.org/10.1007/s40321-013-0007-y

DURHAM CIVIL CONTINGENCIES UNIT. (2002). Small Business And Voluntary Organisation Business Continuity Template.

Echezona, R. I. (2012). Disaster management in university libraries: Perceptions, problems and strategies. Στο *Journal of Library & Information Science* (Τόμ. 2).

Editors, TheFamousPeople.com. (χ.χ.). Ανάκτηση 11 05, 2021, από TheFamousPeople.com: https://www.thefamouspeople.com/profiles/kevin-mitnick-37791.php

Fennelle, E. (1998, September 22). The harsh law of averages. *The Times*, σ. 41.

G. Morgan, J. S. (1997). Disaster management in libraries: the role of a disaster plan.

Gallagher, M. (2003). *Business Continuity Management.* Gosport, Hants, Great Britain: Pearson Education Limited .

Graham Matthews, P. E. (1996). Disaster management training in libraries. MCB University Press.

Hanung Nindito Prasetyo, N. S. (2020, 01 15). Information Technology Disaster Recovery Plan (IT-DRP) Model-Based on NIST Framework in Indonesia. *Journal of Applied IT, 03*(01), 35-45. doi:https://doi.org/10.25124/ijait.v3i01.2317

Harrar, J. H. (1975). Photographs, pictures and prints. Στο S. P. Grove (Επιμ.), *Non-print media in academic libraries* (σσ. 173-192). Chicago: American Library Association.

Hecht, J. A. (2002). BUSINESS CONTINUITY MANAGEMENT. *Communications of the Association for Information Systems, 8*, 444-450.

Huahong Tu, A. D. (2019). Users Really Do Answer Telephone Scams. *28th USENIX Security Symposium*, (σσ. 1327-1340). Santa Clara, CA, USA.

Hussain Aldawood, G. S. (2020, 01 30). An Advanced Taxonomy for Social Engineering Attacks. *International Journal of Computer Applications, 177*(30).

IBM Services. (2020). *IBM - services business continuity plan*. Ανάκτηση 10 01, 2021, από https://www.ibm.com/services/business-continuity/plan

Ilo, P. I. (2018). Measuring disaster preparedness and response practices in university libraries in Nigeria: The role of disaster equipment. Elsevier. doi:https://doi.org/10.1016/j.ijdrr.2018.04.007

Jaffer Kabir Najar, Z. A. (2021). A study of disaster preparedness of archives & museum in seismic zone - v, flood prone and conflict ridden Kashmir. Srinagar, India: Department of Library and Information Science, University of Kashmir. doi:10.1108/CC-02-2020-0003

K Budiman, F. Y. (2020). Disaster recovery planning with distributed replicated block device in synchronized API systems. *6th International Conference on Mathematics, Science, and Education (ICMSE 2019).* IOP Publishing. doi:10.1088/1742-6596/1567/3/032023

Kasim Randeree, A. M. (2012). A business continuity management maturity model for the UAE banking sector. *Business Process Management, 18*(3), 472-492. doi:10.1108/14637151211232650

Khalid, S. J. (2015). Disaster Preparedness for Academic Libraries in Malaysia: An Exploratory Study. *International Journal of Social, Behavioral, Educational, Economic and Management Engineering, 9*(10).

Kirkendall, K. (1998). Teaching the online catalogue users. *Library Review, 19*(4), 27-28.

KLEINKNECHT, S. W. (2003). *HACKING HACKERS.* Hamilton, Ontario: McMaster University.

Kostagiolas, P. (2011). Disaster management approaches for academic libraries: An issue not to be neglected in Greece. Researchgate. doi:10.1108/01435121111187888

Kwasinski, A. (2010, 06). Technology Planning for Electric Power Supply in Critical Events Considering a Bulk Grid, Backup Power Plants, and Micro-Grids. *IEEE SYSTEMS JOURNAL, 4*(2), 167-178. doi:10.1109/JSYST.2010.2047034

Langan Engineering. (2013). *Avoiding Trap Doors.* Emerson Network Power. Ανάκτηση 10 10, 2021, από https://www.itssolution.com/wp-content/uploads/white-papers/Avoiding-Trap-Doors-Associated-With-Purchasing-A-UPS-System-E-Book.pdf

Lawson, S. (2017). Access, ethics and piracy. *UKSG, 30*(1), 25-30.

Long, J. (2007). No-Tech Hacking.

Luciana Duranti, H. M. (1996). The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project.

Lyu, M. R. (2001, 07). Firewall Security: Policies, Testing and Performance Evaluation. *CiteSeer*. doi:10.1109/CMPSAC.2000.884700

Ma, Q. (2005). ISO 17799: "Best practices" in information security managment. *Communications of the Association for Information Systems*, 577-591. doi:10.17705/1CAIS.01532

Millar, F. (1964). The Aerarium and Its Officials under the Empire. *The Journal of Roman Studies, 54*(1), 33-40.

Minnesota Historical Society. (2007). *EMERGENCY PREPAREDNESS & RECOVERY PLAN.* Minnesota.

MOSSE CLAUDE, S.-G. A. (2015). Επίτομη Ιστορία της Αρχαίας Ελλάδας (2.000-31π.Χ.).

Musiliu O. Oseni, M. G. (2013). The Economic Costs of Unsupplied Electricity: Evidence from Backup Generation, among African Firms. Cambridge: EPRG 1326.

Muthu Ramachandran, V. C. (2016). Towards Validating Cloud Service Providers Using Business Process Modelling and Simulation. Leeds Beckett University, Leeds.

National Institute of Standards and Technology. (2010). Contingency Planning Guide for Federal Information Systems. Ανάκτηση 10 10, 2020, από http://csrc.nist.gov/publications.

Nicholas, D. (1998). *Hacking the net.* Ανάκτηση 9 22, 1998, από Ariadne: http://www.ariadne.ac.uk/issue16/cover

Official Journal of the European Union. (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. European Union.

Ogbulezie, J. C. (2016, 03). Local Area Network (Lan) Mock-Up And The Prevention Of Cybernetics Related Crimes In Nigermills Company Using Firewall Security Device. *International Journal of Scientific and Engineering Research, 7*(3), 1124-1130. Ανάκτηση 10 10, 2021, από https://www.researchgate.net/publication/303919593

Pashel, B. A. (2006). Teaching Students to Hack: Ethical Implications in Teaching Students to Hack at the University Level. Kennesaw: Kennesaw State University.

Patricia Y. Logan, A. C. (2005). Teaching students to hack: curriculum issues in information security. *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education*, (σ. 157). St. Louis, Missouri. doi:10.1145/1047344.1047405

Posner, E. (1972). *Archives in the Ancient World.* Harvard University Press. doi:https://doi.org/10.4159/harvard.9780674437005

Posner, E. (1972). *Rome Archives in the ancient world.* Harvard University Press.

R. S. Sandhu, P. S. (1994, 09). Access control: principle and practice. *IEEE Communications Magazine, 32*(9), 40-48. doi:10.1109/35.312842

Rogers, M. (2000). *A New Hacker Taxonomy.* Manitoba, Canada: University of Manitoba.

Ronny Richardson, M. M. (2017, 01 01). Ransomware: Evolution, Mitigation and Prevention. *International Management Review, 13*(1), 10 - 21.

Sara Rouhani, V. P. (2019). Physical Access Control Management System Based on Permissioned Blockchain. IEEE. doi:10.1109/Cybermatics_2018.2018.00198

Shepard, E. (2018). COMPILING A DISASTER PLAN FOR ARCHIVAL COLLECTIONS. Στο H. A. CHRISTOPHER HARTTEN (Επιμ.), *MID-ATLANTIC REGIONAL ARCHIVES CONFERENCE*, *13*, σ. 45.

Steve M. Hawkins, D. C. (2020, 08 05). Disaster recovery planning: a strategy for data. *Information Management & Computer Security*, 222-229.

Sukhai, N. B. (2005). Hacking And Cybercrime. *InfoSecCD* (σσ. 128 - 132). Kennesaw, USA: ACM. Ανάκτηση 10, 2021

Treadgold, W. (2013). *The Middle Byzantine Historians.* London: Palgrave Macmillan. doi:https://doi.org/10.1057/9781137280862

V. Selvi, R. S. (2014). The Design and Implementation of On-Line Examination Using Firewall security. *IOSR Journal of Computer Engineering, 16*(6), 20-24.

Varlamoff, M.-T. (2005). Preservation & Conservation, Asia & Oceania & PAC &. Oslo, Norway: IFLA.

Wenjin Hu, T. Y. (2020, 08). The good, the bad and the ugly of consumer cloud storage. *ACM SIGOPS Operating Systems Review*. doi:10.1145/1842733.1842751

Workman, M. (2007). Gaining Access with Social Engineering: An. *Information Systems Security*, 315-331. doi:10.1080/1065898070178816

Xiaoyi Sun, K. C. (2019). System-level hardware failure prediction using deep learning. *2019 56th ACM/IEEE Design Automation Conference (DAC).* Las Vegas, NV, USA: IEEE.

Γεώργιος Γιαννακόπουλος, Β. Μ. (2016). *Εισαγωγή στην Αρχειονομία.* Αθήνα: Αθήνα:Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Ανάκτηση από http://hdl.handle.net/11419/6320

Γιαννακόπουλος, Γ. (2015). Εισαγωγή στην Αρχειονομία.

Γιαννακόπουλος, Γ. (2016). *Ο κόσμος των αρχείων.* Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Ανάκτηση από http://hdl.handle.net/11419/6322

Ζερβός, Σ. (2002). *Συντήρηση και Διατήρηση Χαρτιού, Βιβλίων και Αρχειακού Υλικού.* Αθήνα: ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ.

Καρεκλάς, Ν. (2016). Τεχνικές Προδιαγραφές εγκαταστάσεων Αρχείου σε περίπτωση μελλοντικής μετεγκατάσταση.

Μπάγιας, Α. (1999). Αρχειονομεία. Στο *Βασικές έννοιες.* Αθήνα.

Μπαλτά, Ε. (1989). *Τα Οθωμανικά Αρχεία στην Ελλάδα.* doi:https://doi.org/10.12681/mnimon.440

ΣΒ. Καρουμπάκου, Σ. Κ. (2017). Τεκμήρια ζωτικής σημασίας και σχέδια αντιμετώπισης καταστροφών. Στο *Εντοπισμός, διαχείριση και ανάκτηση κρίσιμων επιχειρησιακών αρχειακών τεκμηρίων.* Αθήνα.