Ο ρόλος του CFO στην αντιμετώπιση του κυβερνοεγκλήματος

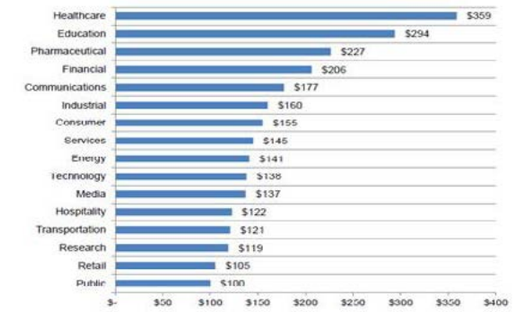
Του Γιάννη Μουρατίδη

Οι περισσότεροι όταν διαβάζουμε ένα δημοσίευμα σχετικά με παραβίαση συστημάτων ασφάλειας, φανταζόμαστε τον CIO να κάθεται σε αναμμένα κάρβουνα. Αυτό που δεν φανταζόμαστε είναι πως σε ανάλογη κατάσταση βρίσκεται και ο CFO.
Ανέκαθεν ο σχεδιασμός ενός περιβάλλοντος ασφάλειας για τα ψηφιακά δεδομένα της επιχείρησης ήταν στην αρμοδιότητα του CIO. Επειδή όμως τα σχέδια υλοποιούνται με επενδύσεις, ο CFO είναι αυτός που θα επιβάλει περικοπές στους προϋπολογισμούς, αλλά και αυτός που θα χρειαστεί να ενημερώσει τους stake holders για τις οικονομικές επιπτώσεις του περιστατικού. Και επιπλέον είναι αυτός που θα ερωτηθεί αν φρόντισε για την ασφάλεια της εταιρείας. "Μα η ασφάλεια είναι θέμα του IT", δικαιολογημένα θα σκεφτείτε, όμως εμείς αναφερόμαστε στην ασφάλεια της ασφάλειας. Μπερδευτήκατε;

Ο **Νίκος Γεωργόπουλος**, ένας από τους λίγους ειδήμονες σε θέματα Cyber Insurane στην ελληνική αγορά μας εξηγεί πώς εξελίσσεται το ζήτημα του κυβερνοεγκλήματος και με ποιον τρόπο η αρμοδιότητα του CFO εμπλέκεται στη λήψη των επιχειρηματικών αποφάσεων.

Ακούγεται από πολλά δημοσιεύματα ότι το κυβερνοέγκλημα έχει πάρει πολύ ανησυχητικές διαστάσεις. Πρόκειται για υπερβολές ή υπάρχουν κάποια στοιχεία που τεκμηριώνουν μια γραμμική ή ίσως και εκθετική αύξηση;
Το κυβερνοέγλημα είναι μια από τις πιο αναπτυσσόμενες κατηγορίες εγκλήματος και όσο εξελίσσεται η τεχνολογία και η χρήση της στην καθημερινότητά μας θα μεγαλώνει εκθετικά. Σήμερα το μεγαλύτερο μέρος της επιχειρηματικής δραστηριότητας έχει μεταφερθεί στο διαδίκτυο.
Αυτό άλλωστε είναι και το σημαντικότερο πλεονέκτημα από τη χρήση του κυβερνοχώρου. Όμως σε αυτόν δραστηριοποιούνται και κυβερνοεγκληματίες, οι οποίοι έχουν στόχο να υποκλέψουν δεδομένα και εμπιστευτικές πληροφορίες που διατηρούν οι εταιρείες, όπως: οικονομικές εκθέσεις, μισθοδοσίες υπαλλήλων, βάσεις δεδομένων πελατών, κωδικούς πρόσβασης, εμπορικά μυστικά (π.χ. συμβάσεις συνεργασίας με παρόχους υπηρεσιών υγείας), σχέδια μάρκετινγκ, σχέδια δημιουργίας νέων προϊόντων και υπηρεσιών, συμβάσεις συνεργασίας με ασφαλιστικούς διαμεσολαβητές, δεδομένα υγείας των ασφαλισμένων, δεδομένα συνταξιοδοτικών προγραμμάτων, αριθμούς των πιστωτικών καρτών και τραπεζικών λογαριασμών, περιουσιακά στοιχεία πελάτη, προσωπικά οικονομικά στοιχεία πελατών.

Επίσης, μπορούν να δημιουργηθούν προβλήματα στην ομαλή λειτουργία της εταιρείας μέσω κυβερνοεπιθέσεων που οδηγούν σε άρνηση παροχής υπηρεσίας (DDos) των συστημάτων εξυπηρέτησης πελατών. Το τελευταίο καιρό παρατηρείται το φαινόμενο η άρνηση παροχής υπηρεσίας να συνοδεύεται και με την απαίτηση καταβολής λύτρων στους κυβερνοεκβιαστές.
Η χρήση του κυβερνοχώρου δημιουργεί σημαντικό λειτουργικό κίνδυνο στις εταιρείες. Οι κίνδυνοι που συνδέονται με τη χρήση του κυβερνοχώρου (Cyber Risks) πρέπει να αντιμετωπιστούν, όπως όλοι οι κίνδυνοι, και μετά την ανάλυσή τους να αποφασιστεί τι ποσοστό μπορεί να αναλάβει η εταιρεία και τι ποσοστό θα μεταφερθεί σε εξειδικευμένους ασφαλιστές.
Οι μηχανισμοί προστασίας των δεδομένων που εφαρμόζαμε μέχρι σήμερα μπορούν εύκολα να παρακαμφθούν ακόμη και από μια απροσεξία ενός εργαζόμενου που μπήκε σε μια μολυσμένη ιστοσελίδα ή απάντησε σε ένα e-mail phishing.
Στο γράφημα μπορούμε να δούμε πόσο μπορεί να κοστίσει η απώλεια ανά record στους διάφορους οικονομικούς τομείς δραστηριότητας σύμφωνα με μελέτη του Ponemon Institute.



Πηγή 2014 – Cost of Data Breach Study Global – Ponemon Institute Research Report

Ειδικότερα για την Ελλάδα σύμφωνα με μελέτη που εκπόνησε η αγορά των Lloyd's σε συνεργασία με το Κέντρο Μελετών Κινδύνων του Πανεπιστημίου του Κέμπριτζ το κόστος των κυβερνοεπιθέσεων που θα δεχτούν επιχειρήσεις και οργανισμοί την επόμενη δεκαετία (2015-2025) ανέρχεται σε $1.06 δισ. δολάρια του εκτιμώμενου Α.Ε.Π της Ελλάδας. Το πόσο αυτό υπολείπεται ελάχιστα σε σχέση με τα 1.07 δισ. δολάρια του εκτιμώμενου Α.Ε.Π που βρίσκονται σε κίνδυνο λόγω σεισμού.

Ήταν έκπληξη για εμάς, όταν πριν από λίγο καιρό σας ακούσαμε να μιλάτε για το ρόλο του CFO στην πρόληψη και την αντιμετώπιση του κυβερνοεγκλήματος. Πόσο καθοριστικός είναι πραγματικά ο ρόλος του;
Το κυβερνοέγκλημα δημιουργεί απρογραμμάτιστες άμεσες και έμμεσες δαπάνες για την αντιμετώπιση των οποίων δεν μπορούν να γίνουν ασφαλείς προβλέψεις στον προϋπολογισμό.
Τα περιστατικά παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών μπορεί να έχουν αρνητική επίπτωση στη ρευστότητα και τις ταμειακές ροές της εταιρείας. Το πρόβλημα μεγαλώνει, γιατί το κόστος των συμβάντων δεν μπορεί να προσδιορισθεί ακριβώς, και ο CFO δεν μπορεί να κάνει μια πρόβλεψη για αυτό ούτε να δεσμεύσει αντίστοιχα κεφάλαια της εταιρείας για την αντιμετώπισή του χωρίς τη χρήση ασφάλισης Cyber Insurance.
Τον τελευταίο καιρό έχουμε επίσημη καταγραφή περιστατικών κυβερνοεγκλήματος στην Ελλάδα σε διάφορους τομείς της οικονομίας, όπως οι τράπεζες, ο τουρισμός και το ηλεκτρονικό εμπόριο.
Για την αντιμετώπιση των χρηματοικονομικών επιπτώσεων, αποτελεσματικό εργαλείο διαχείρισης των περιστατικών παραβίασης αποτελεί η ασφάλιση Cyber Insurance, δίνοντας εκτός από τις χρηματικές αποζημιώσεις και πρόσβαση σε ομάδες ειδικών, οι οποίες έχουν αντιμετωπίσει πλήθος περιστατικών.
Ενώ η ασφάλιση δεν μπορεί να αποτρέψει ένα περιστατικό παραβίασης, μπορεί να βοηθήσει ελαχιστοποιώντας την οικονομική καταστροφή και τη βλάβη της φήμης που μπορεί να συντελεστεί σε σύντομο χρονικό διάστημα.

Πρέπει να τονιστεί ότι αύξηση των χρηματοοικονομικών επιπτώσεων θα έχουμε με την εφαρμογή της νέας ευρωπαϊκής νομοθεσίας για την προστασία των προσωπικών δεδομένων.
Σύμφωνα με την νέα νομοθεσία, οι εταιρείες που δε θα καταφέρουν να διατηρήσουν την ασφάλεια των δεδομένων τους κινδυνεύουν με διοικητικά πρόστιμα για παραβίαση των κανόνων που φθάνουν μέχρι 20 εκατομμύρια ευρώ ή έως 4 % του ετήσιου παγκόσμιου κύκλου εργασιών της εταιρείας, όποιο από τα δυο είναι μεγαλύτερο.
Ο ρόλος του CFO είναι καθοριστικός στη διαχείριση των χρηματοοικονομικών επιπτώσεων ενός περιστατικού παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών. Ας μην ξεχνάμε ότι πάντοτε ο CFO είναι μέλος της Ομάδας Διαχείρισης Κρίσεων κάθε εταιρείας.

Οπότε με βάση αυτά που μας λέτε ο CFO πρακτικά ενδιαφέρεται περισσότερο για ένα Cyber Insurance συμβόλαιο σε σχέση με τον CIO; Το έχει συνειδητοποιήσει όμως αυτό;

Τόσο ο CIO όσο και ο CFO φροντίζουν πάντα για τη σωστή διαχείριση των κινδύνων που απειλούν μια εταιρεία. Είναι και οι δυο μέλη της Ομάδας Διαχείρισης Κρίσεων και οι λύσεις που προτείνει ο CIO απαιτούν εξοικονόμηση πόρων από τον CFO και ένταξή τους στον προϋπολογισμό.
Στην Αμερικανική αγορά που το κυβερνοέγκλημα είναι καθημερινότητα, το American National Standards Institute έχει δημιουργήσει ειδικό οδηγό για τους CFO με τίτλο "Financial Management of Cyber Risks". Ο οδηγός αυτός είναι διαθέσιμος στην **ιστοσελίδα**.
Αν θέλουμε να κατηγοριοποιήσουμε τον βαθμό συνειδητοποίησης των κινδύνων και την προτεραιοποίηση αγοράς Cyber Insurance από τους CFOs θα έλεγα ότι πρώτα έρχονται οι CFOs από τις τηλεπικοινωνίες και τις τράπεζες και μετά όσοι ανήκουν στις εταιρείες κρίσιμων υποδομών, όπως: νοσοκομεία, λιμάνια, αεροδρόμια και ενέργεια.
Στην Ευρώπη χρειάζεται ακόμα να γίνει αρκετή δουλειά σε θέματα δημιουργίας πολιτικών και διαδικασιών ασφάλειας πληροφοριών στις εταιρείες, κάτι που θα γίνει αναγκαστικά τους επόμενους μήνες λόγω της νέας νομοθεσίας περί προστασίας προσωπικών δεδομένων και αντιμετώπισης κυβερνοεπιθέσεων.

Ποια θα ήταν τα βήματα που θα συμβουλεύατε να ακολουθήσει ένας CFO, ο οποίος θα διαβάσει αυτό το άρθρο;
Να έχει γνώση των κινδύνων που διατρέχει η εταιρεία του, να υπολογίσει τις τυχόν χρηματοοικονομικές επιπτώσεις τους και να φτιάξει ένα σχέδιο αντιμετώπισής τους χρησιμοποιώντας τις δυνατότητες που του προσφέρει η ασφάλιση.

Αν θέλουμε να δούμε ειδικά τι πρέπει να γίνει για περιστατικά παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών, θα πρέπει να έχει μια καταγραφή των κατηγοριών δεδομένων που διαχειρίζεται η εταιρεία του, τον όγκο τους και τις ευθύνες που έχει λόγω της νέας νομοθεσίας περί προσωπικών δεδομένων.
Επιπλέον, να δημιουργήσει σε συνεργασία με τα άλλα ανώτατα στελέχη της εταιρείας ένα σχέδιο αντιμετώπισης περιστατικών και να εξετάσει με έναν εξειδικευμένο ασφαλιστή τη δυνατότητα ασφαλισιμότητας της εταιρείας του και το κόστος ασφάλισής της.
Η εταιρεία Cromar, η οποία λειτουργεί ως Ανταποκριτής των Lloyd's, δημιουργούμε ασφαλιστικές λύσεις διαχείρισης περιστατικών παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών, οι οποίες υποστηρίζονται από την αγορά των Lloyd's.
Πιο συγκεκριμένα μέσω της λύσης Cyber Secure Solution διαθέτει στην ελληνική αγορά σε συνεργασία με τους Beazley μια από τις καλύτερες ασφαλιστικές λύσεις διαχείρισης περιστατικών απώλειας εμπιστευτικών πληροφοριών και προσωπικών δεδομένων παγκοσμίως, το "Beazley Global Breach Solution".
Το "Beazley Global Breach Solution" προσφέρει, εκτός από τις χρηματικές αποζημιώσεις, πρόσβαση στην Ομάδα Διαχείρισης Περιστατικών του, η οποία έχει αντιμετωπίσει άνω των 3.000 περιστατικών παγκοσμίως και έχει βραβευθεί από την Advisen ως η καλύτερη ομάδα διαχείρισης για το 2015.

Εργαλεία Risk Management και ενημέρωσης μπορείτε να βρείτε στα παρακάτω:

The Data Breach Toolkit

Με τη βοήθειά του μπορείτε:

* να βρείτε Οδηγούς αντιμετώπισης περιστατικών
* να υπολογίσετε το ενδεικτικό κόστος τους
* να βρείτε αναλύσεις ζημιών ασφαλισμένων εταιριών
* να δείτε το νομικό πλαίσιο που ισχύει διεθνώς

LinkedIn Groups Cyber Risks Advisors
Cyber Insurance Greece

Web sites
www.cromar.gr
www.cyberrisksadvisors.com
www.privacyrisksadvisors.com
www.cyberinsurancegreece.com
www.cyberinsurance.gr

Οι CFO χάνουν την εμπιστοσύνη τους στην αξία υποβολής χρηματοοικονομικών αναφορών

Σύμφωνα με έρευνα της Ernst & Young μόνο 55% των CFO είναι πλήρως ή αρκετά βέβαιοι ότι οι αναφορές που υποβάλλουν συμμορφώνονται με όλες τις ανάγκες.

Της Αγγελικής Θεοδωρακοπούλου

Ανάμεσα σε ένα ολοένα πιο απαιτητικό εταιρικό περιβάλλον, οι CFO χάνουν την εμπιστοσύνη τους στην αποτελεσματικότητα που παρουσιάζει η υποβολή χρηματοοικονομικών αναφορών. Μάλιστα, πολλοί διατυπώνουν ρητά παράπονα για υπερβολικό όγκο εργασίας στο συγκεκριμένο πεδίο, σύμφωνα με νέα έρευνα της EY.

Σε **έρευνα** που διεξήχθη μεταξύ 1.000 CFO σε 25 χώρες, σε οργανισμούς με έσοδα άνω των 500 εκατομμυρίων δολαρίων διαπιστώθηκε ότι η εμπιστοσύνη σε όλες τις βασικές πτυχές των εταιρικών αναφορών έχει μειωθεί σε σύγκριση με το 2014. Η μεγαλύτερη πτώση σημειώνεται στην "εμπιστοσύνη στο βαθμό συμμόρφωσης". Μόνο 55% των ερωτηθέντων αναφέρουν ότι είναι πλήρως ή κάπως ικανοποιημένοι ως προς το συγκεκριμένο δείκτη, έναντι ποσοστού 84% το 2014.
Καταγράφονται και άλλες αισθητές πτώσεις, όσον αφορά στην έκταση των αναφορών συγκριτικής αξιολόγησης (44% σήμερα έναντι 66% το 2014), της σαφήνειας και καταλληλότητας των μηνυμάτων (45% έναντι 67%), και της συνέπειας στην εφαρμογή των κύριων δεικτών επίδοσης (44% έναντι 65%).
Μόλις 39% των CFO αντιλαμβάνονται την υποβολή χρηματοοικονομικών αναφορών ως οικονομικώς αποδοτική, έναντι 68% το 2014. Εξάλλου, μόνο 48% των ερωτηθέντων είπαν ότι η υποβολή αναφοράς υπήρξε αποτελεσματική στο να εξασφαλίσει την εμπιστοσύνη του Διοικητικού Συμβουλίου, μια σημαντική πτώση από το ποσοστό 71% του προηγούμενου έτους.

"Οι CFO οφείλουν να κάνουν ένα βήμα πίσω και να αξιολογήσουν το έργο τους, καθώς και να εξετάσουν τις ανησυχίες τους σχετικά με την εμπιστοσύνη και την αποτελεσματικότητα γρήγορα", υποστηρίζει σε Δελτίο Τύπου ο Peter Wollmert, επικεφαλής της Διεύθυνσης Financial Accounting & Advisory Services της EY. "Τυχόν καθυστέρηση σημαίνει ότι η έγκαιρη και με ακρίβεια υποβολή της αναφοράς θα εξακολουθήσει να έχει επιπτώσεις στην απόδοση. Η υποβολή εταιρικών αναφορών θα εξυπηρετήσει τον σκοπό της, μόνο εφόσον ο CFO είναι βέβαιος για την αξία της".

Η EY εντόπισε διάφορες ακόμα αιτίες για την απώλεια εμπιστοσύνης στις χρηματοοικονομικές αναφορές, συμπεριλαμβανομένης της αυξανόμενης περιπλοκότητας στη δομή των αναφορών. Μια άλλη αιτία είναι η αυξανόμενη ζήτηση, την ίδια στιγμή που οι επικεφαλής των Οικονομικών Διευθύνσεων ανησυχούν για το διευρυνόμενο χάσμα μεταξύ των αναφορών που απαιτούν οι κανονισμοί και εκείνων που ζητούν οι υπόλοιποι ενδιαφερόμενοι (stakeholders), όπως οι επενδυτές. Επίσης, υπάρχει και η πίεση που ασκείται στους πόρους.
Η έρευνα επίσης καταλήγει στο συμπέρασμα ότι οι CFO αισθάνονται την αλυσιδωτή αντίδραση που επιφέρει ο εξονυχιστικός έλεγχος που εφαρμόζεται στις επιτροπές λογιστικού ελέγχου και τα εποπτικά συμβούλια. Οι ερωτηθέντες σε ποσοστό 84% ισχυρίζονται ότι οι επιτροπές ελέγχου και τα εποπτικά συμβούλια έχουν εντείνει τη γενική προσοχή τους στην υποβολή αναφορών κατά τα τελευταία τρία χρόνια, ενώ το 34% επισημαίνει ότι η προσοχή έχει ενισχυθεί σημαντικά.
"Οι επιτροπές λογιστικού ελέγχου βρίσκονται στο επίκεντρο αναφορικά με τον τρόπο με τον οποίο υλοποιούν τις αρμοδιότητές τους, και οι CFO με τη σειρά τους δέχονται πίεση ώστε να προσφέρουν όλο και περισσότερες πληροφορίες", τονίζει ο Wollmert. • • •