ΕΝΩΣΗ
ΑΣΦΑΛΙΣΤΙΚΩΝ
ΕΤΑΙΡΙΩΝ
ΕΛΛΑΔΟΣ

Διαχείριση Cyber Claims & η Ελληνική πραγματικότητα στις ζημιές

CYBER RISK INSURANCE
30 Οκτωβρίου 2018

Κώστας Βούλγαρης
• *Μέλος Επιτροπής Αστικής Ευθύνης & Επαγγελματικών Ευθυνών*

Δυο μύθοι…

Countries in which a breach was confirmed

Australia	France	Jordan	Poland	United Arab Emirates
Austria	Germany	Kuwait	Romania	Ukraine
Bahamas	Ghana	Lebanon	Russian Federation	United Kingdom
Belgium	Greece	Luxembourg	South Africa	United States
Brazil	India	Mexico	Spain	
Bulgaria	Ireland	Netherlands	Taiwan	
Canada	Israel	New Zealand	Thailand	
Denmark	Japan	Philippines	Turkey	

Verizon 2012 Data breach investigations report

Κίνδυνος των «μεγάλων»;

Οι Διαδικτυακές απειλές δεν είναι πια προνόμιο των μεγάλων επιχειρήσεων

- Ολοένα και αυξανόμενο ποσοστό μικρομεσαίων επιχειρήσεων πιστεύει ότι οι διαδικτυακοί κίνδυνοι αποτελούν μια σοβαρή απειλή για τις ίδιες
- Οι ΜΜΕ είναι επίσης πιο εκτεθειμένες σχετικά με τη χρήση φορητών ηλεκτρονικών συσκευών από τους υπαλλήλους τους.
- Έχουν χαμηλότερο budget στη διάθεση τους για συστήματα IT
- Είναι πιο ευάλωτες οικονομικά

Και μια αλήθεια…

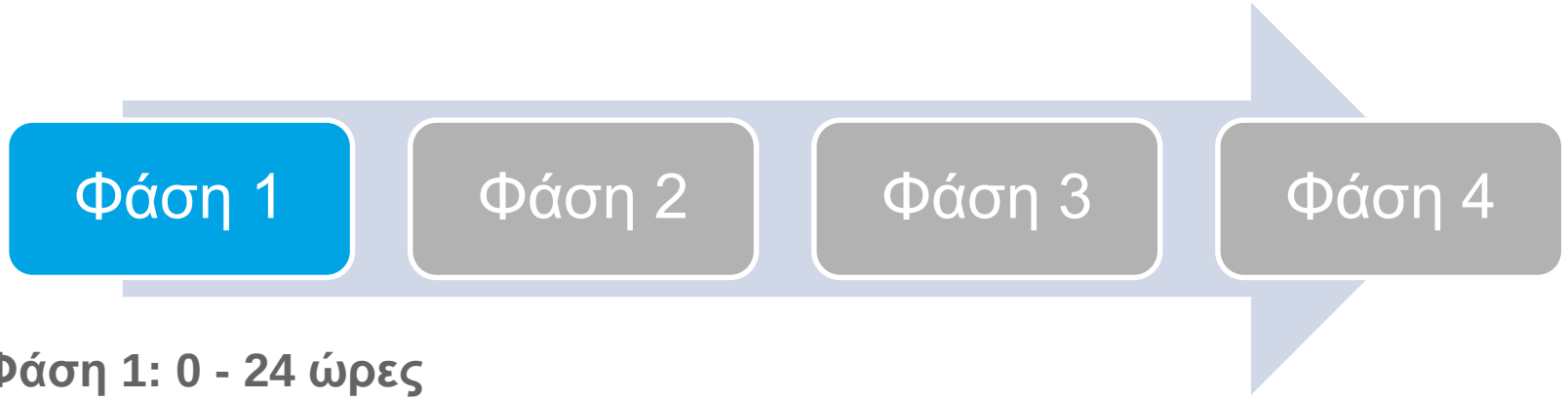
Οι «ελληνικές» Ζημίες

- Ψυχολογικός εκβιασμός
- Διακοπή εργασιών
- Malware
- Ransomware
- Ανθρώπινο λάθος

Ανατομία ενός Cyber Claim

Τι συμβαίνει και πότε;

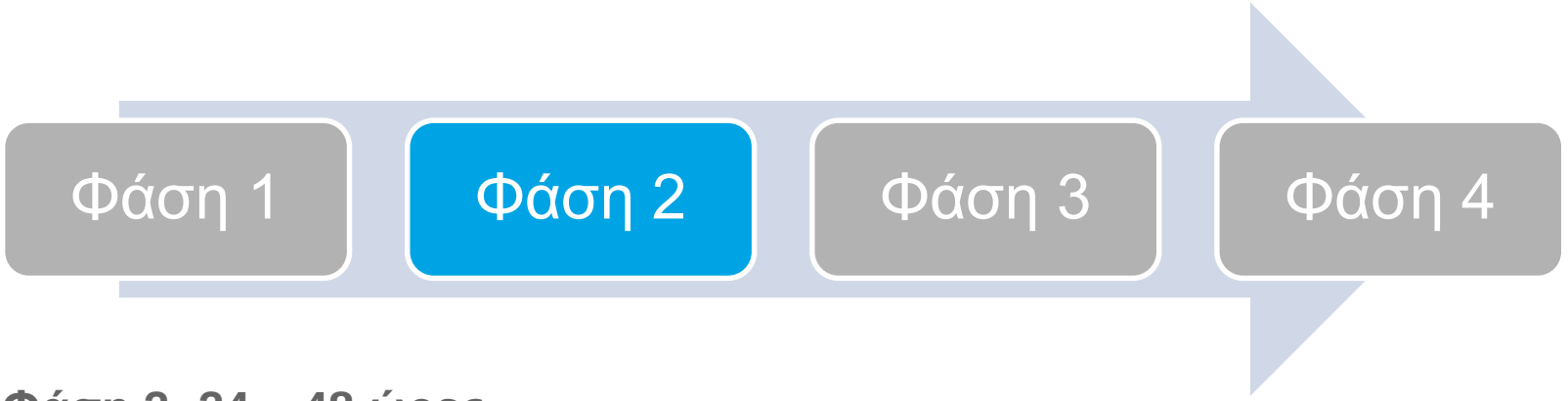
Ανατομία ενός Cyber Claim



Φάση 1: 0 - 24 ώρες

- Ενεργοποίηση της τηλεφωνικής υποστήριξης / αναγγελίας
- Οι Σύμβουλοι Ασφαλείας Πληροφορικής και οι δικηγόροι αντιδρούν με αυστηρά SLAs
- Εκτίμηση γεγονότος και πρώτες συμβουλές
- Διατήρηση εμπιστευτικότητας
- Διαχείριση κρίσης
- Ανάλυση της διαρροής και προσπάθεια κατανόησης του σκοπού της
- Εντοπισμός των στοιχείων που έχουν διαρρεύσει

Ανατομία ενός Cyber Claim



Φάση 2: 24 – 48 ώρες

- Εκτίμηση του προβλήματος και δημιουργία σχεδίου αντίδρασης
- Συμβουλές σχετικά με την ενημέρωση των ανθρώπων που χάθηκαν τα δεδομένα τους
- Συμβουλές σχετικά με την επικοινωνία με ρυθμιστικές αρχές
- Συνέχιση της ανάλυσης του περιστατικού
- Επιλογή συμβούλου επικοινωνίας και διαχείρισης του γεγονότος
- Διαχείριση περιστατικών εκβιασμού

Ανατομία ενός Cyber Claim

Φάση 3: 48 to 72 ώρες

- Αναλυτικό σχέδιο για την ενημέρωση των παθόντων
- Ενημέρωση Αρχών και «διαπραγμάτευση» μαζί τους
- Συνέχιση των ενεργειών από της ομάδες των Συμβούλων (PR /IT forensic/ διαχείρισης εκβιασμού) σύμφωνα με τις ανάγκες
- Συμβουλές για την παρακολούθηση των συστημάτων και την ενίσχυση της ασφάλειας τους

Ανατομία ενός Cyber Claim

Φάση 4: 72+ ώρες

- Εκτίμηση του κόστους και των ζημιών
- Συνέχιση των ενημερώσεων των παθόντων και των επαφών με τις Αρχές
- Διαχείριση σχέσεων με τρίτους που επηρεάστηκαν
- Συνεργασία με αστυνομικές αρχές
- Αναγνώριση πιο μακροπρόθεσμων ζητημάτων που πρέπει να αντιμετωπιστούν
- Ενέργειες για αποζημιώσεις και περιορισμού της ζημιάς
- Ποσοτικοποίηση της απαίτησης για διακοπή εργασιών

Σύνοψη της ανατομία μιας ζημιάς και της ασφαλιστικής αντίδρασης

1. **Παραβίαση** → Άμεση αντίδραση
2. **IT Forensics** → Ειδικοί εντοπίζουν τι έχει επηρεαστεί, πώς μπορεί να περιοριστεί η διαρροή και πώς να αποκατασταθεί η ζημιά
3. **Νομική Υποστήριξη & PR** → Ειδικοί αναλαμβάνουν να περιορίσουν την νομική έκθεση σε κίνδυνο και να προστατέψουν τη φήμη της εταιρίας
4. **Ενημερώσεις** → Κόστος ενημέρωσης όσων επηρεάστηκαν
5. **Πρόστιμα & Έρευνες** → προετοιμασία για έρευνες από αρχές και κάλυψη ασφαλίσιμων προστίμων
6. **Ευθύνες** → Έξοδα υπεράσπισης και αποζημιώσεις για διαρροή δεδομένων
7. **Εκβιασμός** → Διαπραγμάτευση και κάλυψη «λύτρων» εκβιασμού
8. **Διακοπή Εργασιών** → Αποζημίωση απώλειας κερδών