ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Διεθνή περιστατικά παραβίασης προσωπικών δεδομένων στον τομέα της Υγείας: Μέτρα πρόληψης και αντιμετώπισης

Ανάργυρος Χρυσάνθου, Πληροφορικός, MSc.
Ειδικός Επιστήμων ΑΠΔΠΧ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Δομή Παρουσίασης

- Ορισμοί
- Νομικό καθεστώς
  - Ευρώπη
  - Ελλάδα
- Στατιστικά στοιχεία
- Πραγματικά περιστατικά
- Μέτρα ασφαλείας
- Συμπεράσματα

Ορισμοί

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ορισμοί (1/2)

Συμβάν ασφάλειας

☞ «Ένα αναγνωρισμένο συμβάν, με βάση το οποίο προκύπτει ότι σε ένα σύστημα, μια υπηρεσία ή ένα δίκτυο ενός οργανισμού (α) υφίσταται παραβίαση της πολιτικής ασφαλείας του οργανισμού ή (β) έχουν αποτύχει τα μέτρα ασφαλείας του ή (γ) υφίσταται μια πρωτύτερα άγνωστη κατάσταση, η οποία μπορεί να σχετίζεται με την ασφάλεια των πληροφοριών (information security)». (ISO/IEC 27000:2009)

http://cache-blog.credit.com/wp-content/uploads/2015/06/database-hack-680x430.jpg

Περιστατικό ασφάλειας

☞ «Ως περιστατικό ασφάλειας πληροφοριών ορίζεται ένα ή μια σειρά από ανεπιθύμητα ή απρόβλεπτα συμβάντα ασφάλειας των πληροφοριών τα οποία μπορούν να δημιουργήσουν πρόβλημα στην επιχειρησιακή λειτουργία ενός οργανισμού και να απειλήσουν την ασφάλεια των πληροφοριών (information security), δηλαδή την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών που ο οργανισμός επεξεργάζεται». (ISO/IEC 27000:2009)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ορισμοί (2/2)

Περιστατικό παραβίασης δεδομένων

- “Μη εγκεκριμένη διάδοση πληροφοριών, η οποία μπορεί να οφείλεται σε μια δικτυακή επίθεση, σε κλοπή εγγράφων, αποσπώμενων μέσων αποθήκευσης, φορητών υπολογιστών κ.ο.κ. Ευαίσθητες πληροφορίες μπορούν να εντοπιστούν και σε κάδους απορριμμάτων, μέσω εγγράφων (πχ. εμπιστευτικές επιτελικές αναφορές οργανισμών) που έχουν καταλήξει στους κάδους χωρίς να καταστραφούν με ασφαλή τρόπο.”

(http://www.pcmag.com/encyclopedia_term/0,1237,t=data+breach&i=61571,00.asp)

Περιστατικό παραβίασης προσωπικών δεδομένων

- «Η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή προσπέλαση προσωπικών δεδομένων που διαβιβάσθηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ’ άλλο τρόπο σε επεξεργασία. » (Βλ. Ευρωπαϊκό Κοινοβούλιο, 2012/0010(COD), άρθρο 3(9))

Νομικό καθεστώς

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ευρώπη (1/2)

- Οδηγία 2009/136/ΕΚ -> Πρώτη αναφορά του όρου «Παραβίαση Προσωπικών Δεδομένων»
- Υποχρεώσεις των παρόχων διαθέσιμων στο κοινό υπηρεσιών ηλ. επικοινωνιών
  - Ενημέρωση αρμόδιας εθνικής αρχής χωρίς περιττή καθυστέρηση
  - Ενημέρωση συνδρομητών ή ατόμων που θα μπορούσαν να επηρεαστούν αρνητικά χωρίς αδικαιολόγητη καθυστέρηση (υπό προϋποθέσεις)
  - Τήρηση αρχείου παραβιάσεων προσωπικών δεδομένων
    (Οδηγία 2002/58/ΕΚ όπως τροποποιήθηκε από την Οδηγία 2009/136/ΕΚ, άρθρο 3)
- **25/1/2012** – Πρόταση αναθεώρησης κανονιστικού πλαισίου προστασίας προσωπικών δεδομένων (Ευρωπαϊκή Επιτροπή)
- **15/12/2015** – Συμφωνία θεσμικών οργάνων της Ευρωπαϊκής Ένωσης στο αναθεωρημένο κανονιστικό πλαίσιο προστασίας των προσωπικών δεδομένων
- **Αρχές 2016** – Προβλεπόμενο χρονικό διάστημα επίσημης έγκρισης τελικών κειμένων από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο
- Έναρξη της ισχύος των κειμένων -> 2 χρόνια μετά

(Βλ. http://europa.eu/rapid/press-release_IP-15-6321_el.htm)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ευρώπη (2/2)

- Υποχρέωση υπευθύνων να αναφέρουν τα περιστατικά παραβίασης προσωπικών δεδομένων
  - Αρμόδια Εθνική Αρχή
  - Υποκείμενο των δεδομένων
  - Αμελλητί
  - «Πλήρη» αναφορά (είδος δεδομένων που διέρρευσαν, αριθμός υποκειμένων κ.ο.κ)
- Δικαίωμα του υποκειμένου να υποβάλει καταγγελία
- Πιθανώς τυποποιημένος μορφότυπος αναφοράς πανευρωπαϊκά (εφαρμοστέες διαδικασίες, μορφή / τρόπος τεκμηρίωσης κ.ο.κ.)
- Πιθανό πρόστιμο έως 1.000.000 Ευρώ (ή μέχρι το 2% του ετήσιου παγκόσμιου κύκλου εργασιών) για
  - Παράλειψη γνωστοποίησης περιστατικού
  - Ελλιπή / μη έγκυρη γνωστοποίηση περιστατικού

(Ευρωπαϊκή Επιτροπή, 2012/0010(COD), άρθρα 3 εδ. 9, 28-29, 32 εδ. ε και 50, 2012/0011(COD), άρθρα 4 εδ. 9, 30,31, 37 παρ. 1 εδ. ε, 73 και 79 παρ. 6 εδ. η)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ελλάδα

- Ενσωμάτωση των αλλαγών της Οδηγίας 2009/136/ΕΚ στο Ν.3471/2006 (μέσω του Ν.4070/2012)
- Υποχρέωση γνωστοποίησης για τους παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλ. επικοινωνιών
  - περιστατικών ασφαλείας εν γένει
  - περιστατικών παραβίασης προσωπικών δεδομένων
- Τήρηση αρχείου περιστατικών ασφαλείας και περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα

(1. *Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών,* Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών (ΦΕΚ Β΄ 2715/17-11-2011)*, άρθρο 9, 2. Ν. 4070/2012, άρθρο 37 & 3. Ν. 3471/2006 ως τροποποιήθηκε από τον Ν. 4070/2012, άρθρο 2 εδ. 11, άρθρο 12 εδάφια 5-10*)

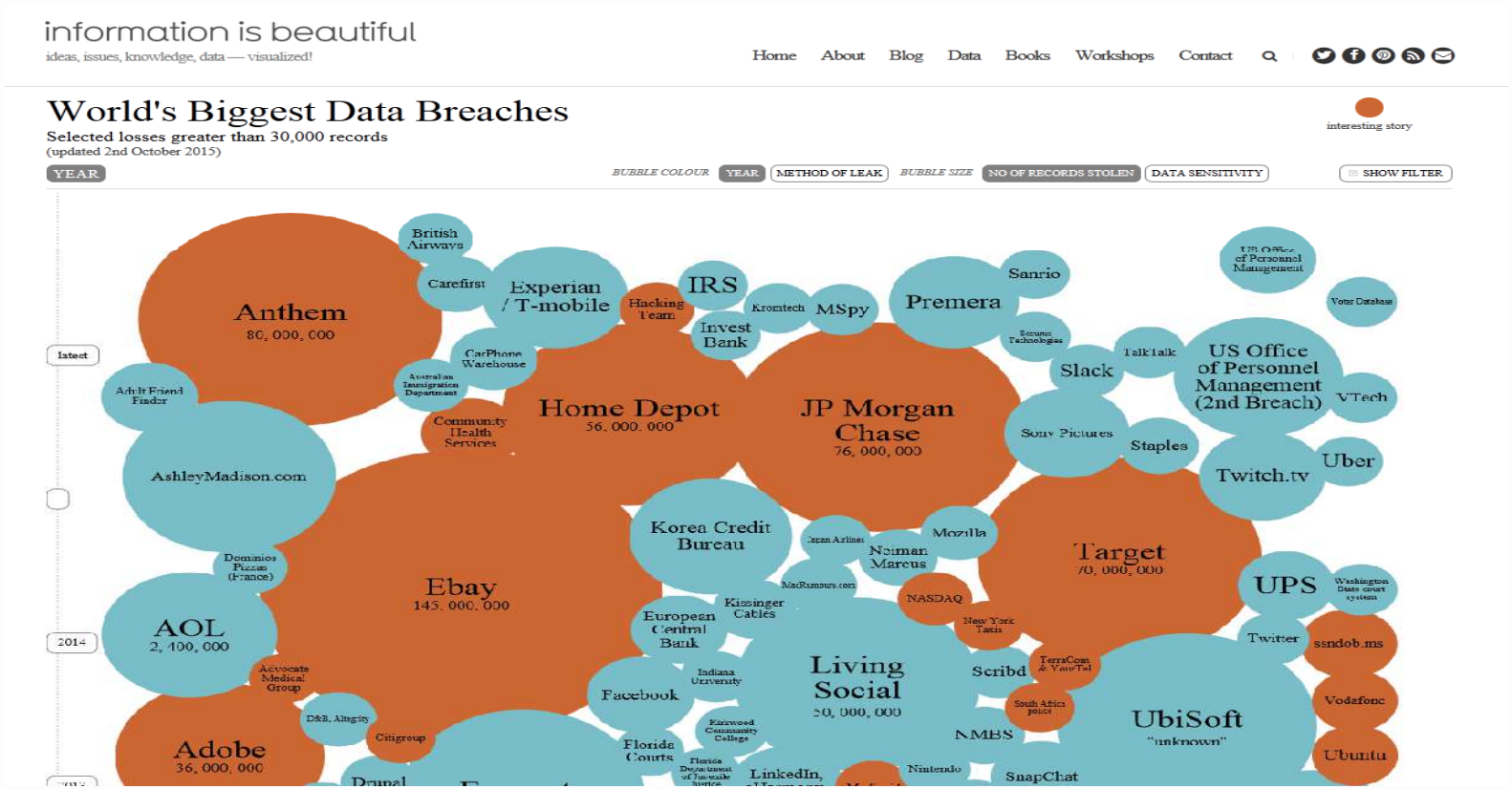
- Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα χειρίζεται περιστατικά παραβίασης προσωπικών δεδομένων στη βάση των:
  - Ν.2472/1997, αρ. 10, παρ. 3 -> υπεύθυνοι επεξεργασίας
  - Ν.3471/2006 ως τροποποιήθηκε από τον Ν.4070/2012, άρθρο 2 εδ. 11, άρθρο 12 εδάφια 5-10 -> πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλ. επικοινωνιών

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Στατιστικά στοιχεία

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Μεγαλύτερα περιστατικά παραβίασης προσωπικών δεδομένων (εν γένει)

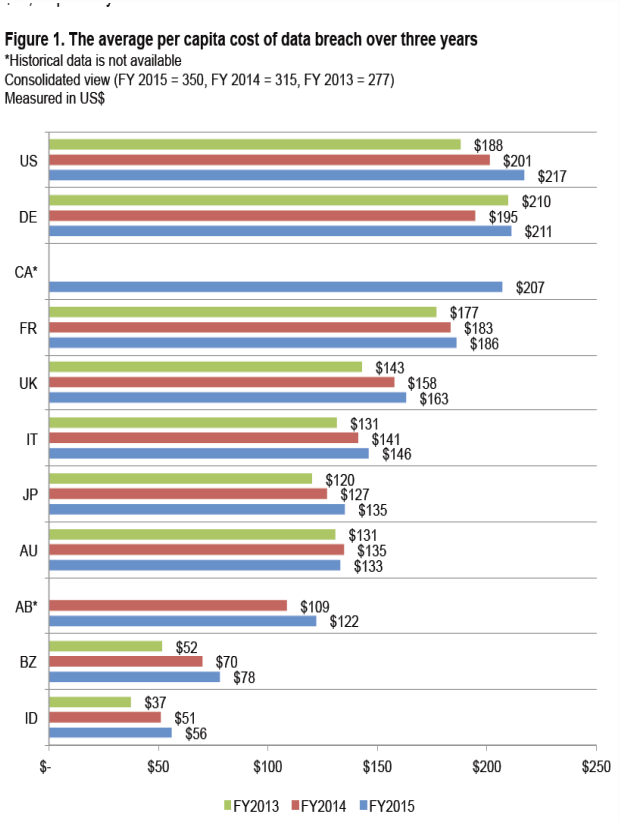


http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Στοιχεία από μελέτες (Γενικά) (1/2)

- Κυριότερη αιτία περιστατικών (47%) -> Κακόβουλη / εγκληματική ενέργεια (Ponemon)
- Μέσο κόστος / εγγραφή -> 154$ (Ponemon)
- Κυριότεροι παράγοντες μείωσης κόστους (Ponemon)
  - Εκπαίδευση προσωπικού (51%)
  - Ύπαρξη ομάδας διαχείρισης περιστατικών (48%)
  - Ορισμός CISO (45%)
  - Εκτεταμένη χρήση κρυπτογράφησης (44%)



Ponemon, 2015 Cost of Data Breach Study: Global Analysis

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

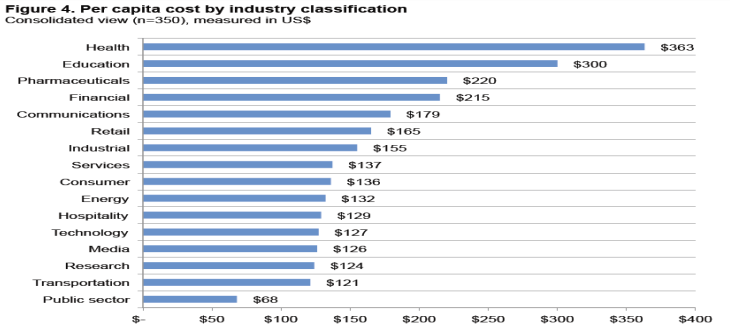
Στοιχεία από μελέτες (Γενικά) (2/2)

- 45% των συμμετεχόντων -> μη ενημέρωση των προγραμμάτων ευαισθητοποίησης σε θέματα προστασίας προσωπικών δεδομένων (Experian)
- 50% -> καθόλου εκπαίδευση κατά την πρόσληψη (Experian)
- 60% - μεγαλύτερο εμπόδιο για τη βελτίωση της αντιμετώπισης περιστατικών -> αδυναμία ουσιαστικού ελέγχου προσβάσεων σε ευαίσθητα / εμπιστευτικά δεδομένα (Experian)
- 97% Ελλήνων συμμετεχόντων -> επιθυμία ενημέρωσης αν γίνει περιστατικό παραβίασης προσωπικών δεδομένων (Eurobarometer)
- 65% συμμετεχόντων -> ευθύνη ενημέρωσης η εταιρεία που έχει τα δεδομένα τους (Eurobarometer)

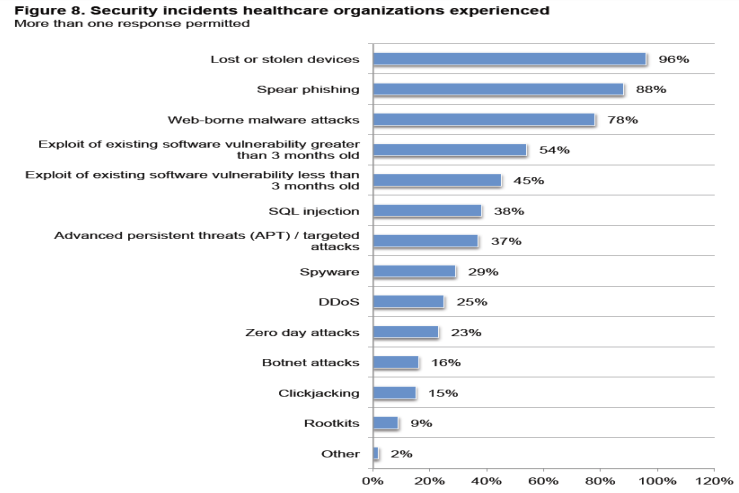
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Στοιχεία από μελέτες (Υγεία) (1/2)

- Κόστος / εγγραφή -> $363 (Ponemon)
- Ponemon US Study
  - 90 οργανισμοί υγείας (covered entities), 88 συνεργαζόμενες επιχειρήσεις (business associates)
  - Μεγαλύτερη ανησυχία -> αμέλεια υπαλλήλων
  - 91% οργανισμών υγείας -> τουλάχιστον 1 περιστατικό τα τελευταία 2 χρόνια
  - 40% εξ' αυτών -> παραπάνω από 5 περιστατικά!
  - Συνεργαζόμενες επιχειρήσεις -> 59 και 15% αντίστοιχα
  - Κυριότερη αιτία περιστατικών (45%) -> Κακόβουλη / εγκληματική ενέργεια
- Identity Theft Resource Center -> 277 επιβεβαιωμένα περιστατικά με δεδομένα υγείας, 112,832,082 έγγραφες



Ponemon, 2015 Cost of Data Breach Study: Global Analysis

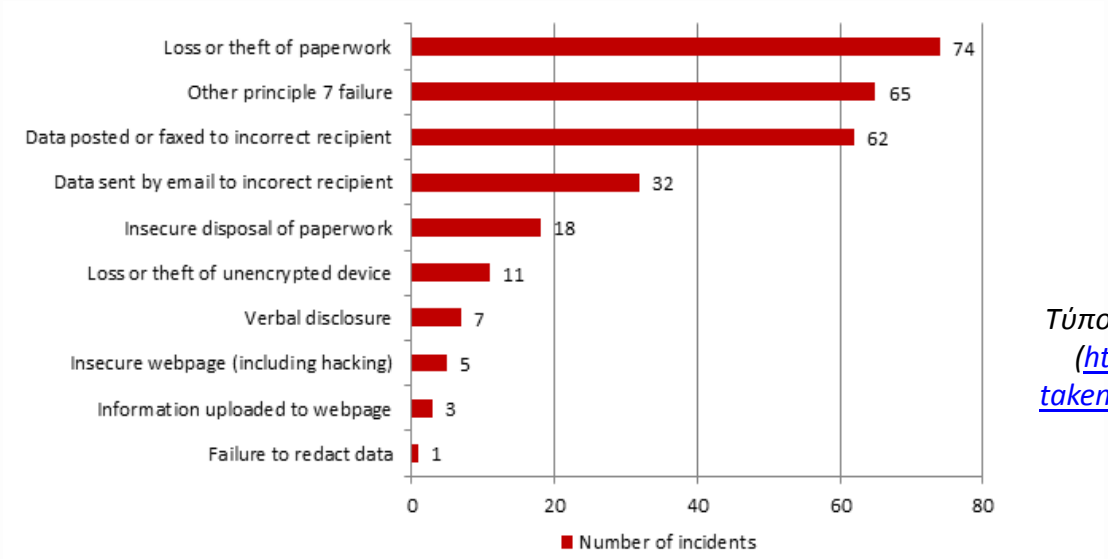


Ponemon, 2015, Benchmark Study on Privacy & Security of Healthcare Data

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Στοιχεία από μελέτες (Υγεία) (2/2)

- **ICO** (2ο εξάμηνο 2015)
  - Αύξηση περιστατικών που αφορούν δεδομένα υγείας (44% πάνω σε σχέση με 1ο εξάμηνο)
  - 471 περιστατικά το 2015 (193 + 278)
  - Κυριότερες αιτίες : Απώλεια εγγραφών (27%), αποστολή δεδομένων σε λάθος παραλήπτη (23%)
  - Υπ' αρ. 1 απολεσθέν έγγραφο : εισιτήριο / εξιτήριο / έντυπο μεταφοράς ασθενή (ward handover/discharge sheets) -> 91 περιστατικά



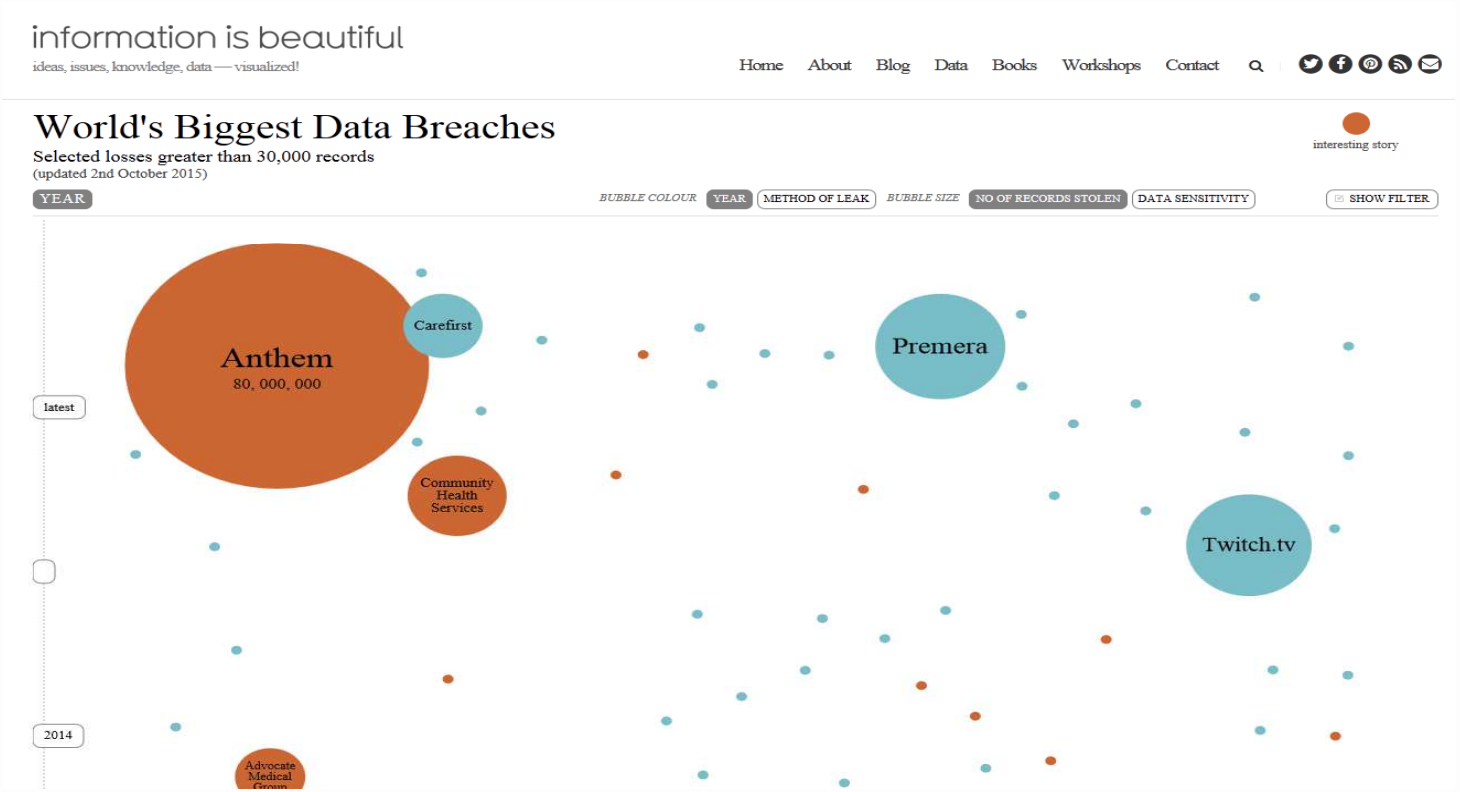
Τύποι περιστατικών – Τομέας υγείας (https://ico.org.uk/action-weve-taken/data-security-incident-trends/)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Πραγματικά περιστατικά

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Πιο σημαντικά περιστατικά παραβίασης προσωπικών δεδομένων (υγεία)



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

1. Premera (1/2)

- Αμερικάνικη ασφαλιστική εταιρεία υγείας
- Μη εγκεκριμένη πρόσβαση σε
  - Προσωπικά Δεδομένα 11 εκ. πελατών
  - Στοιχεία επικοινωνίας, αριθμός κοινωνικής ασφάλισης, αριθμός μέλους, δεδομένα αιτήσεων κάλυψης εξόδων για ιατρική περίθαλψη και, σε μερικές περιπτώσεις, στοιχεία τραπεζικού λογαριασμού
- Κυβερνοεπίθεση -> **5/5/2014**
- Ανακάλυψη περιστατικού -> **29/1/2015**
- Ανακοίνωση περιστατικού -> **17/3/2015**
- Τρόπος επίθεσης -> Κακόβουλο λογισμικό
- Κίνδυνος κλοπής ιατρικής ταυτότητας
- Αριθμός κοινωνικής ασφάλισης – **ΔΕΝ ΑΝΤΙΚΑΘΙΣΤΑΤΑΙ**

http://www.healthcareglobal.com/tech/1860/How-Premera-Blue's-Breach-Reveals-Weaknesses-in-Health-Care-Security

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

1. Premera (2/2)

- Πρόσληψη εξειδικευμένης εταιρείας αντιμετώπισης / διερεύνησης περιστατικών ασφαλείας
- Συνεργασία με FBI
- Δημοσιοποίηση περιστατικού
- Δημιουργία ειδικής σελίδας ενημέρωσης
- Προσωπική ενημέρωση πελατών
- Προσφορά δύο χρόνια δωρεάν
  - Υπηρεσία προστασίας από κλοπή ταυτότητας
  - Παρακολούθηση πιστοληπτικής δραστηριότητας (credit monitoring)
  - Σε πιθανά θύματα και ανήλικα παιδιά
- Περίπου την ίδια περίοδο -> παρόμοια επίθεση στην Anthem (78,8 εκ. εγγραφές) με ενδείξεις ότι οι επιθέσεις μπορεί να σχετίζονται (τρόπος επίθεσης, δράστες)

(Βλ. και 1. http://www.king5.com/story/money/consumer/2015/03/17/premera-cyber-attack/24911465/, 2. http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/, 3. https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/)

PREMERA BLUE CROSS

Log In

http://www.premeraupdate.com/faqs/#Collapse57

About the Cyberattack

On January 29, 2015, Premera discovered that cyberattackers had executed a sophisticated attack to gain unauthorized access to our information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on May 5, 2014. As part of our own investigation, we notified the FBI and are coordinating with the Bureau's investigation into this attack.

We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remove the infection created by the attack on our IT systems. Along with steps we took to cleanse our IT system of issues raised by this cyberattack, Premera is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

This incident affected Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and our affiliate brands, Vivacity and Connexion Insurance Solutions, Inc. Our investigation determined that the attackers may have gained unauthorized access to applicants and members' information, which could include member name, date of birth, email address, address, telephone number, Social Security number, member identification numbers, bank account information, and claims information, including clinical information. This incident also affected members of other Blue Cross Blue Shield plans who sought treatment in Washington or Alaska.

Some individuals that have done business with us and provided us with their email address, personal bank account number or social security number were also affected. The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately.

We sincerely regret the frustration and concern this incident may cause. The security of our members' personal information is a top priority.

Frequently Asked Questions

Q: What happened?

Premera has been the target of a sophisticated cyberattack that gained unauthorized access to our IT systems. Our investigation has not determined that any data was removed from our systems. To date there is no evidence that any data has been used inappropriately. The security of our members' personal information is a top priority, and we are taking proactive steps to address this issue.

Q: Has my information been accessed?

Our investigation determined that attackers may have gained unauthorized access to personal information, but we have not determined that any information was removed from our system. We understand that this may be concerning to those involved and mailed letters to everyone whose information was affected by this attack.

Q: What information may have been accessed?

Depending on your relationship with Premera, we may hold different types of information about you. The information that may have been accessed could include your name, address, email address, telephone number, date of birth, Social Security number, member identification number, medical claims information and in some cases, bank account information. Premera does not store credit card information for members, so your credit card information is not affected by this attack. Our investigation has not determined that any information was removed from our systems and there is no evidence to date that any such information has been used inappropriately.

Q: What else can I do to protect my personal information?

Premera will not email you or make unsolicited phone calls to you about this attack. You should not provide your personal information in response to an email or unsolicited phone call that claims to be related to this attack. You should review your Explanation of Benefits (EOB) statements when you receive them. If you see services on your EOB that you did not obtain, please contact us using the number on the back of your ID card.

Q: Did this attack affect all Premera lines of business?

This incident affected Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and our affiliate brands, Vivacity and Connexion Insurance Solutions, Inc.

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

2. New West Medicare (1/2)

- Αμερικάνικη Ασφαλιστική εταιρεία υγείας
- Εταιρικός φορητός υπολογιστής
- Δεδομένα 25.000 ασθενών
  - Στοιχεία επικοινωνίας
  - Αριθμός άδειας οδήγησης, κοινωνικής ασφάλισης, απαίτησης Medicare
  - (σε κάποιες περιπτώσεις) στοιχεία πληρωμών, δεδομένα υγείας (ιστορικό, διάγνωση, κ.ο.κ)
- Προστασία με κωδικό
- Μη κρυπτογραφημένος σκληρός δίσκος

http://www.cissp.com/images/332965832.jpg

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

2. New West Medicare (2/2)

- **15/1/2016** -> Κλοπή υπολογιστή
- Εκτός οργανισμού (off-site location)
- Καμία ένδειξη χρήσης δεδομένων
- Μέτρα αντιμετώπισης
  - Αναφορά περιστατικού (HHS)
  - Πρόσληψη εξειδικευμένης εταιρείας
  - Εκτίμηση έκτασης περιστατικού
  - Ανάρτηση ανακοίνωσης στην ιστοσελίδα του οργανισμού
  - Δημιουργία ειδικής γραμμής ενημέρωσης πιθανών θιγόμενων

http://www.homelandsecureit.com/wp-content/uploads/2012/07/NotebookThief.jpg

(Βλ. 1. http://www.databreaches.net/mt-new-west-medicare-notifying-25000-members-whose-unencrypted-phi-were-on-stolen-laptop/,
2. https://www.newwestmedicare.com/securityupdate)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

3. A Mobile leaking app

- Δωρεάν εφαρμογή για HIV positive ασθενείς
- Γύρω στους 5000 ασθενείς
- Κενό ασφαλείας στη βάση δεδομένων
- Δεδομένα ανοιχτά για 1 εβδομάδα (κατά τους διαχειριστές)
- Άγνωστο πόσοι τα προσπέλασαν
- Μη ενημέρωση χρηστών

Screenshots provided to DataBreaches.net on December 8 by Vickery revealed that **4,926** user accounts from **Dating App for HIV-positive Singles** were leaking. The personal information included date of birth, religion, relationship status, country, email address, ethnicity, height, last login IP address, username, orientation, number of children, and password hash. Users can also enter their nicknames, share their political views and sexual life experiences, and post their photo in their profile, as this redacted screencap illustrates:

Json Text of Documents:


```
},
"birthday" : "[redacted]",
"children" : "[redacted]",
"city" : [redacted],
"country" : "[redacted]",
"create_time" : ISODate("[redacted]"),
"email" : "[redacted]@hotmail.com",
"email_lower" : "[redacted]@hotmail.com",
"ethnicity" : "[redacted]",
"height" : "[redacted]",
"hobby" : "[redacted]",
"hobby_array" : [{
    "id" : [redacted]
  }, {
    "id" :
  }, {
    "id" :
  }, {
    "id" :
  }, {
    "id" :
  }, {
    "id" :
  }],
"last_login_ip" : "[redacted]",
"last_login_time" : [redacted],
"nickname" : "[redacted]",
"orientation" : [redacted],
"photo" : [{
    "photo_id" :
    "order_id" : [redacted]
  }, {
    "photo_id" :
    "order_id" :
  }, {
    "photo_id" :
    "order_id" :
  }, {
    "photo_id" :
    "order_id" :
  }, {
    "photo_id" :
    "order_id" :
  }, {
    "photo_id" :
    "order_id" :
```


The database also stores messages posted by members. The messages often contain very personal or sensitive information, e.g.,

> "Hi. I was diagnosed 3 years ago now. CD4 and Viral Load is relatively good. I'm therefore not on Meds yet. My 6-monthly blood tests are due in June. Planning to go in meds. I'm worried about the side effects. What kinds of side effect have you experienced? Xx",

1. https://nakedsecurity.sophos.com/2015/12/16/hiv-dating-app-leaks-sensitive-user-data-threatens-infection-when-alerted/, 2. http://www.databreaches.net/two-apps-with-health-info-found-leaking-researcher-part-2-hzone/

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

4. Bloomsbury Patient Network (1/2)

- Δίκτυο παροχής υποστηρικτικών υπηρεσιών σε ασθενείς HIV
- Έδρα : Λονδίνο
- Έμμεση αποκάλυψη στοιχείων των μελών του δικτύου σε μη εγκεκριμένους τρίτους
- Αποστολή από Αντιπρόσωπο Ασθενών (Patient Representative) μαζικού ενημερωτικού e-mail σε 60 έως 200 ασθενείς
  - Διευθύνσεις ηλ. ταχυδρομείου στο πεδίο "To:" του μηνύματος (όχι "Bcc")
- 1ο συμβάν – **17/2/2014**
- Αντιπρόσωπος -> πιο προσεκτικός

TO: Primary Addressee(s)
All recipients can see list
CC: Secondary Addressee(s)
All recipients can see list
BCC: Tertiary Addressee(s)
No recipients can see list

http://www.howtogeek.com/175530/htg-explains-what-bcc-is-and-why-youre-a-terrible-person-if-you-dont-use-it-correctly-or-at-all/

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

4. Bloomsbury Patient Network (2/2)

- **Όμως:**
  - Μη εκπαίδευση του Αντιπροσώπου Ασθενών ως προς τον ορθό τρόπο αποστολής
  - Μη αντικατάσταση λογαριασμού ηλ. ταχυδρομείου
  - Διευθύνσεις ηλ. ταχυδρομείου στο πεδίο "To:" του μηνύματος (όχι "Bcc")

- 2ο συμβάν – **6/5/2014** - Αποστολή μαζικού ενημερωτικού e-mail σε 200 ασθενείς

- **ICO:**
  - Έκρινε:
    - Συνεχής παραβίαση προσωπικών δεδομένων
    - Ευαίσθητα προσωπικά δεδομένα
    - Αποκάλυψη (εμμέσως) των ονομάτων τουλάχιστον 56 ασθενών
    - Διευθύνσεις ηλ. ταχυδρομείου -> δυνητική αποκάλυψη και άλλων ονομάτων
  - Έλαβε υπόψη:
    - 5 παράπονα ασθενών στο BPN
    - BPN -> μη ενημέρωση των μη εγκεκριμένων τρίτων να σβήσουν τα διαρρεύσαντα δεδομένα
  - Επέβαλε στο BPN 250 λίρες πρόστιμο

(https://ico.org.uk/media/action-weve-taken/mpns/1560365/bloomsbury-patient-network-monetary-penalty-notice.pdf)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Η «αγορά»

- **Δεδομένα υγείας**
  - Αξία στη μαύρη αγορά -> $10 και άνω
  - Ακριβότερα από έναν αριθμό πιστωτικής κάρτας
  - Να χρησιμοποιηθούν σε ιατρική απάτη / κλοπή ιατρικής ταυτότητας

(http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924)

- **8/4/2014** -> Το FBI προειδοποιεί
  - **Ιατρικά συστήματα** -> ευάλωτα σε κυβερνοεπιθέσεις
  - **Στόχος** -> οικονομικό κέρδος
  - $50 για κάθε «τμήμα» EHR (με βάση EMC²/RSA White Paper το 2013)
  - **EHR** -> πιθανή χρήση για
    - ψευδείς ασφαλιστικές απαιτήσεις (fraudulent insurance claims)
    - αγορά συνταγογραφούμενων φαρμάκων (obtain prescription medication)
    - κλοπή ταυτότητας (advanced identity theft)

(http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf)

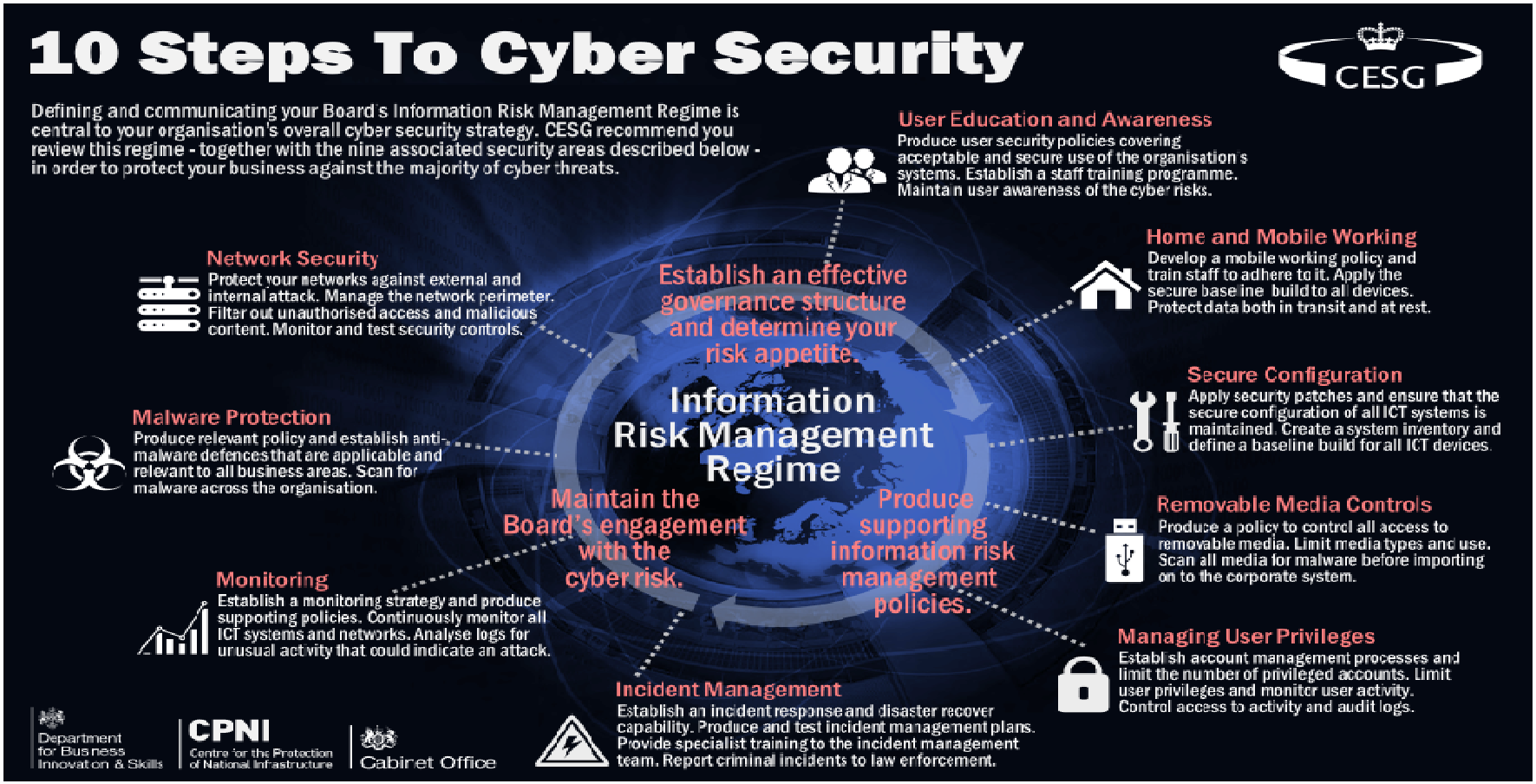
https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Μέτρα ασφαλείας

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

10 βήματα προς την ασφάλεια (GCHQ)



https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

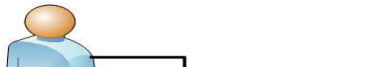
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Μετά το περιστατικό τι;

http://ddos.inforisktoday.com/blogs/breach-notification-framework-p-1631

http://www.3dsi.com/hs-fs/hub/306915/file-2334944601-jpg/blog-files/Databreachnotification-820x400.jpg

Ή;



http://panosec.com/sites/default/files/computer_forensics_investigations.jpg

http://blogs.creditcards.com/wp-content/uploads/data-breach-notice.jpg

http://healthitsecurity.com/news/which-states-have-a-data-breach-notification-law

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ενημέρωση ΑΠΔΠΧ

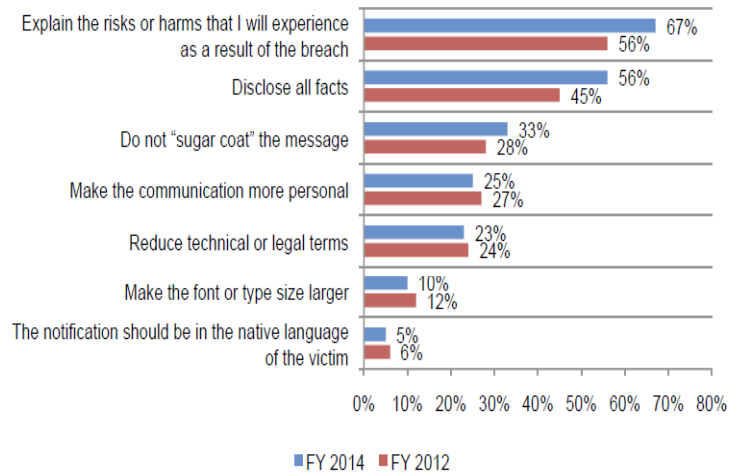
- Άμεση ενημέρωση από υπεύθυνο επεξεργασίας
- Ενημέρωση για
  - Αντικειμενικά στοιχεία (πχ. είδος δεδομένων, αριθμός θιγόμενων ατόμων, είδος / τρόπος παραβίασης, άτομα που έλαβαν γνώση των δεδομένων, τρόπος αναγνώρισης κ.ο.κ.)
  - Ενέργειες μετά το περιστατικό (πχ. εφαρμογή υπαρχόντων καταγεγραμμένων διαδικασιών αντιμετώπισης περιστατικού – διαδικασιών χειρισμού περιστατικού παραβίασης δεδομένων, διερεύνηση, διορθωτικά μέτρα, ενημέρωση θιγόμενων ατόμων, κ.ο.κ.)
  - Υπάρχοντα μέτρα ασφαλείας
  - Σημείο επαφής (Υπεύθυνος προστασίας προσωπικών δεδομένων – αν υπάρχει -)
  - Μελλοντικές ενέργειες

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ενημέρωση υποκειμένων

- Ενημέρωση θιγόμενων προσώπων
  - Με περισσότερους από 1 τρόπους (τηλ., συστημένη επιστολή)
- Δημιουργία κεντρικοποιημένου τρόπου ενημέρωσης (πχ. call center, ειδική ιστοσελίδα)
- Παροχή δωρεάν υπηρεσιών προστασίας (identity theft monitoring)
- Αναλυτική ενημέρωση
- Παροχή συμβουλών

Figure 5. What could the organization do to improve the communication?
Two responses permitted



Ponemon, The Aftermath of a Data Breach: Consumer Sentiment

Συμπεράσματα

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Συμπεράσματα

- **Υπ. Επεξεργασίας**
  - Σε συνεχή επιφυλακή
  - Προετοιμασμένος
  - Οργανωτικά (διαδικασίες, δομές, κ.ο.κ.)
  - Τεχνικά
  - Νομικά

https://www.fbi.gov/news/stories/2012/november/teaching-industry-how-to-protect-trade-secrets-and-national-security/image/protect-information-graphic

ΔΕΝ ΥΠΑΡΧΕΙ ΑΠΟΛΥΤΗ ΑΣΦΑΛΕΙΑ

- Το θέμα δεν είναι αν θα υπάρξει περιστατικό
- Το θέμα είναι:
  - **Πότε** θα υπάρξει
  - **Πως** θα το αντιμετωπίσετε
- Η ΑΠΔΠΧ είναι εδώ για να βοηθήσει

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Βιβλιογραφία - Χρήσιμοι σύνδεσμοι (1/3)

- Αναδιάρθρωση κανονιστικού πλαισίου για τα προσωπικά δεδομένα
- Οδηγία 2009/136/ΕΚ
- Οδηγία 2002/58/ΕΚ
- Νόμος 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα,

  http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal&_schema=PORTAL
- Νόμος 3471/2006 για την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97,

  http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%203471_06_NOV2011_.PDF
- Νόμος 4070/2012,

  http://www.sedek.gr/gr/attachments/article/133/nom-4070_2012.pdf

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Βιβλιογραφία - Χρήσιμοι σύνδεσμοι (2/3)

- Ενημερωτικό κείμενο της Αρχής για θέματα ασφάλειας πληροφοριών («Πολιτική Ασφαλείας, Σχέδιο Ασφαλείας και Σχέδιο Ανάκαμψης από Καταστροφές»)
- Experian Data Breach Resolution, "Third Annual 2016 Data Breach Industry Forecast", http://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-industry-forecast.pdf
- Ponemon Institute LLC, "Third Annual Study: Is Your Company Ready for a Big Data Breach?", http://www.experian.com/assets/data-breach/white-papers/2015-experian-data-breach-preparedness-study-final.pdf
- European Commission, "Special Eurobarometer 431, Data Protection", http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/ResultDoc/download/DocumentKy/66372
- Ponemon Institute LLC, "2015 Cost of Data Breach Study: Global Analysis", http://www-03.ibm.com/security/data-breach/
- Ponemon Institute LLC,2014,"The Aftermath of a Data Breach: Consumer Sentiment", http://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Βιβλιογραφία - Χρήσιμοι σύνδεσμοι (3/3)

- Ponemon, 2015, "Benchmark Study on Privacy & Security of Healthcare Data", http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf
- Experian Data Breach Resolution, "DATA BREACH RESPONSE GUIDE 2015-2016 Edition", http://www.experian.com/assets/data-breach/brochures/2015-2016-data-breach-response-guide.pdf
- Healthcare Information and Management Systems Society, "2015 HIMSS Cybersecurity Survey", http://www.himss.org/2015-cybersecurity-survey
- Identity Theft Resource Center, "Data Breach Reports", http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf
- CENTER FOR MEDIA, DATA AND SOCIETY, "Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005-2014", http://cmds.ceu.hu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope.pdf
- Information Commissioner's Office, Data security incident trends, https://ico.org.uk/action-weve-taken/data-security-incident-trends/

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ευχαριστώ για την προσοχή σας