



Υγιείς Εργασιακές Σχέσεις, Σύγχρονες Επιχειρήσεις

6^η Συνάντηση Δικτύου Επαγγελματιών Εργασιακών Σχέσεων και Διεύθυνσης Ανθρώπινου Δυναμικού

Το έργο συγχρηματοδοτείται από την
Κυπριακή Δημοκρατία και το Ευρωπαϊκό
Κοινωνικό Ταμείο της Ευρωπαϊκής Ένωσης





Ασφάλεια Δεδομένων

Πρακτικές Συμβουλές: Παρουσίαση χρήσιμων και πρακτικών συμβουλών για την ασφάλεια δεδομένων οι οποίες μπορούν να εφαρμοστούν στο χώρο εργασίας.

Θεράπων Θεράποντος DataKnights

Το έργο συγχρηματοδοτείται από την
Κυπριακή Δημοκρατία και το Ευρωπαϊκό
Κοινωνικό Ταμείο της Ευρωπαϊκής Ένωσης



Ασφάλεια Δεδομένων στο HR

- Το HR είναι, το ίδιο ως τμήμα, επεξεργαστής μεγάλου όγκου προσωπικών δεδομένων και έχει πρόσβαση σε κρίσιμης σημασίας δεδομένα.
 - Ασφάλεια για το ίδιο το τμήμα
- Το HR διαχειρίζεται τους ανθρώπους, τον μεγαλύτερο παράγοντα ασφάλειας δεδομένων
 - Ανθρώπινος Παράγοντας
- Το θέμα Ασφάλειας της Πληροφορίας είναι κατ' εξοχήν θέμα κουλτούρας και το HR έχει σημαντικό ρόλο στην ανάπτυξη της
 - Ανάπτυξη Κουλτούρας
- Πιθανά περιστατικά ασφάλειας χρίζουν άμεσης και πολλές φορές πειθαρχικής έρευνας και αφορούν εργαζόμενους
 - Έρευνα Περιστατικών



Υγιείς Εργασιακές Σχέσεις, Σύγχρονες Επιχειρήσεις

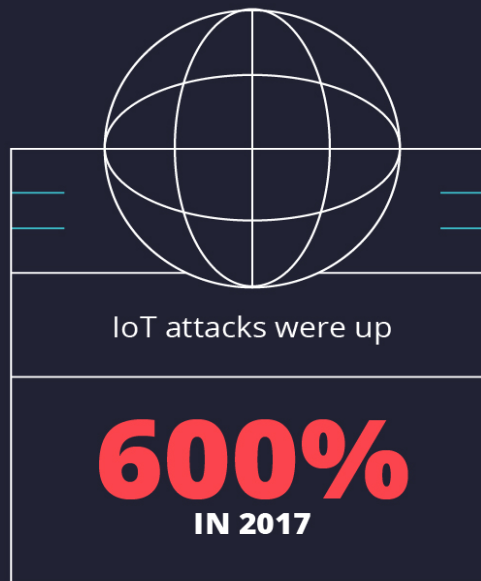


Ασφάλεια της Πληροφορίας

- **Εμπιστευτικότητα (Confidentiality):** Διασφάλιση ότι πρόσβαση στην πληροφορία έχουν μόνο όσοι έχουν κατάλληλη εξουσιοδότηση.
- **Ακεραιότητα (Integrity):** Διασφάλιση ότι η πληροφορία είναι πλήρης, ακριβής και έγκυρη.
- **Διαθεσιμότητα (Availability):** Διασφάλιση ότι η πληροφορία είναι διαθέσιμη κάθε στιγμή που ένας εξουσιοδοτημένος χρήστης επιχειρεί να αποκτήσει πρόσβαση σε αυτή.

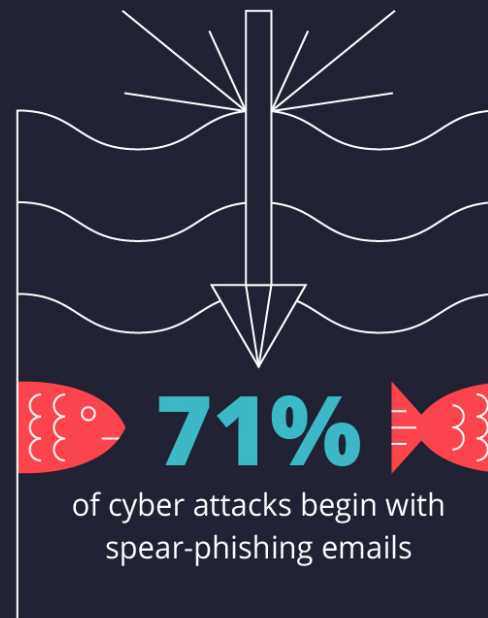
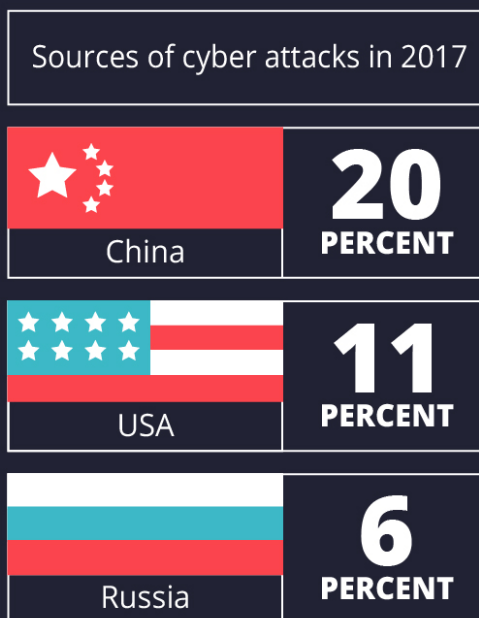
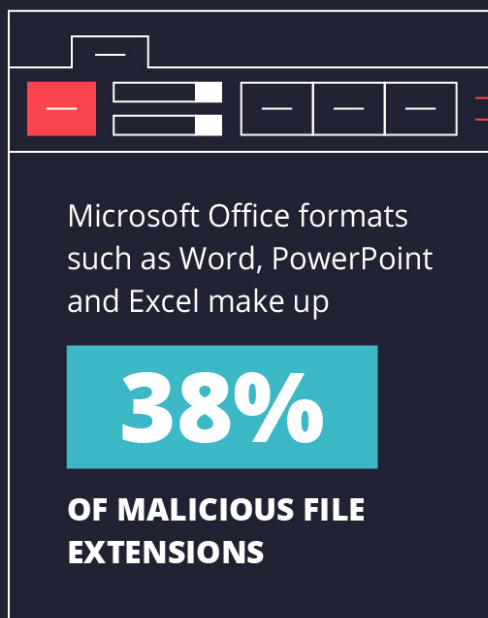
Τι συμβαίνει σήμερα?

DATA BREACHES BY THE NUMBERS



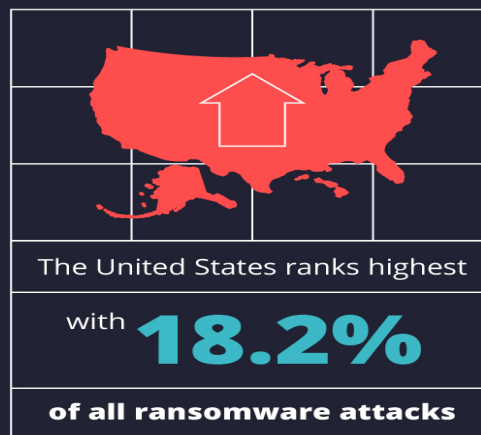
Τι συμβαίνει σήμερα?

WHERE DO CYBER ATTACKS COME FROM?



Τι συμβαίνει σήμερα?

WHO IS AFFECTED?



attacks on the healthcare
industry are expected to

QUADRUPLE
by 2020



The **FINANCIAL SERVICES INDUSTRY**

sees the highest cost from cyber crime.
It costs the average business

\$18.3
MILLION

Τι συμβαίνει σήμερα?

WHAT'S THE COST?



The average cost of a malware attack on a company is

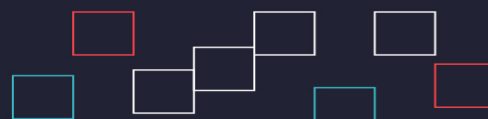
\$2.4
MILLION

The average cost of

**LOST/STOLEN
RECORDS**

per individual is

\$141.00



Information loss represents

43

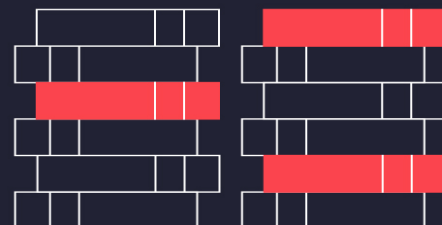
PERCENT

of costs

Damage related to cybercrime is projected to hit

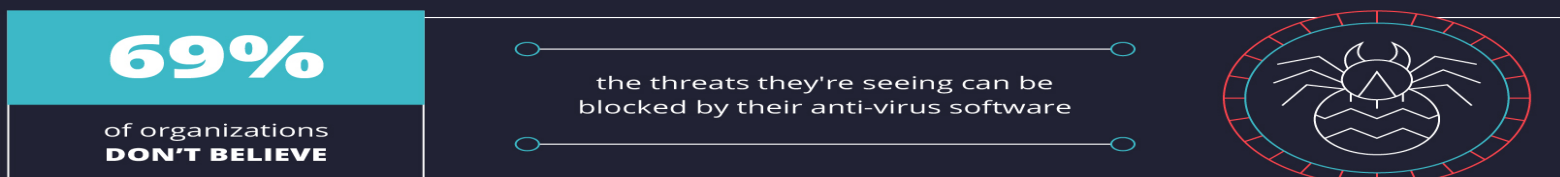
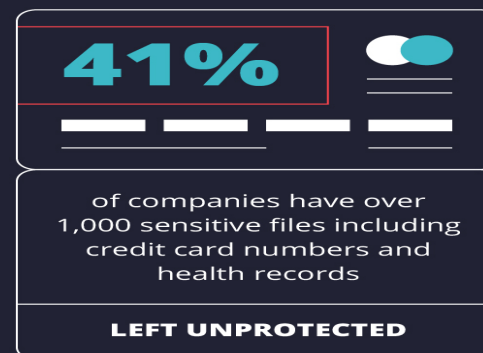
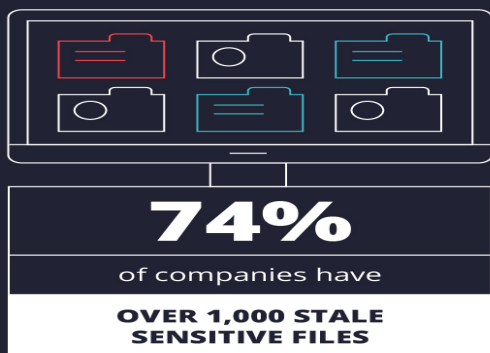
\$6
TRILLION

ANNUALLY BY 2021



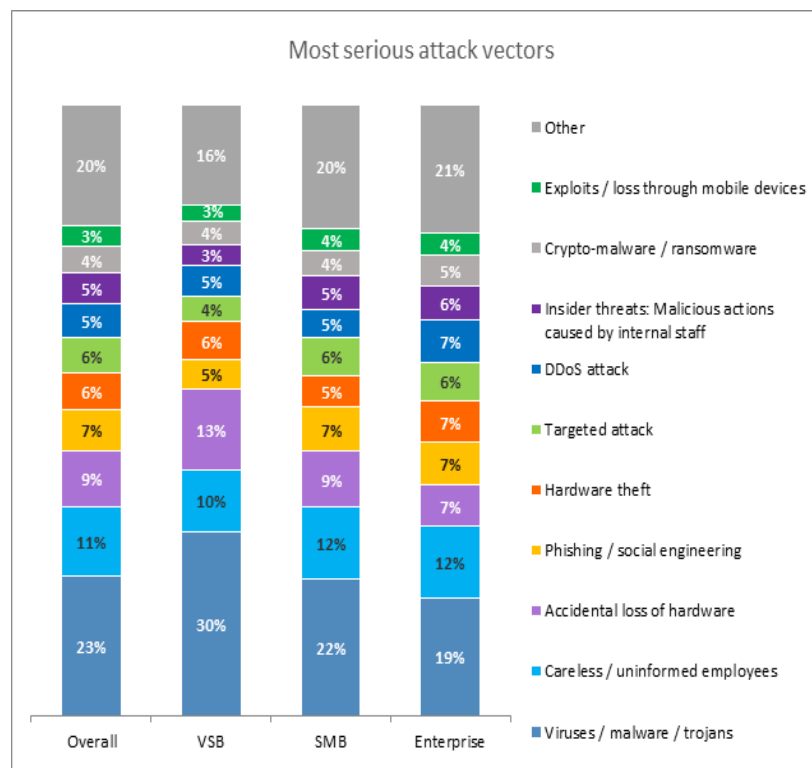
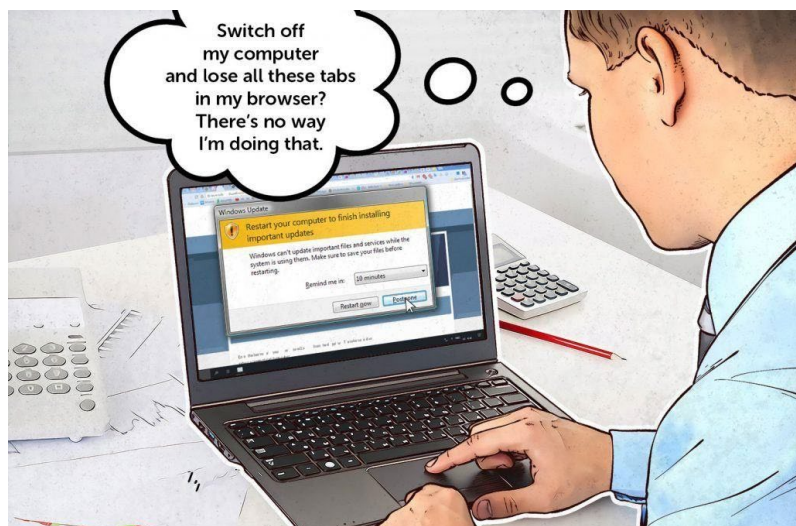
Τι συμβαίνει σήμερα?

IS YOUR COMPANY AT RISK?



Ανθρώπινος Παράγοντας

Το 2017, κατά μέσο όρο 51% οφείλονταν στον ανθρώπινο παράγοντα



Από τι πρέπει να προστατευτούμε?

Οι τύποι των κυβερνο-επιθέσεων εξελίσσονται συνεχώς. Μερικοί από τους κοινές επιθέσεις είναι:

1. Malware
2. Phishing
3. Password Attacks
4. “Man in the Middle” (MITM)
5. Drive-By Downloads
6. Ransomware



Υγιείς Εργασιακές Σχέσεις, Σύγχρονες Επιχειρήσεις



Malware

Malware is a broad term for a variety of cyber threats like Trojans, viruses and worms. In a simple words it is a code with the intent to steals data or destroys something on the PC.



Μέτρα Προστασίας

- ✓ Install Anti-Virus/Malware Software.
- ✓ Keep Your Anti-Virus Software Up to Date.
- ✓ Run Regularly Scheduled Scans with Your Anti-Virus Software.
- ✓ Keep Your Operating System Current.
- ✓ Secure Your Network.
- ✓ Think Before You Click.
- ✓ Keep Your Personal Information Safe.
- ✓ Don't Use Open Wi-Fi.
- ✓ Back Up Your Files.
- ✓ Use Multiple Strong Passwords.

Phishing

It is a request often sent via emails and ask the users to click on the link and enter the required data. Phishing emails have become more classy in recent years, and making it difficult for user to separate a true request from the illegitimate one.



Μέτρα Προστασίας

- ✓ Keep Informed About Phishing Techniques
- ✓ Think Before You Click!
- ✓ Install an Anti-Phishing Toolbar
- ✓ Verify a Site's Security
- ✓ Check Your Online Accounts Regularly
- ✓ Keep Your Browser Up to Date
- ✓ Use Firewalls
- ✓ Be Wary of Pop-Ups
- ✓ Never Give Out Personal Information
- ✓ Use Antivirus Software

Password Attacks

Password attacks are extremely common on these days. A third party attempts to gain access to your systems by cracking a user's password.



Μέτρα Προστασίας

- ✓ Control physical access to systems
- ✓ Control electronic access to password files
- ✓ Encrypt password files
- ✓ Create a strong password policy
- ✓ Use password masking
- ✓ Deploy multifactor authentication
- ✓ Use account lockout controls
- ✓ Use last logon notification
- ✓ Educate users about security
- ✓ Actively manage accounts

Man in the Middle Attack

Man in the Middle” (MITM) By imitating the endpoints in an online information exchange (i.e. the connection from receiver to a gainer), the MITM can attain details from the both, end user and the person/company he is interacting with.

Μέτρα Προστασίας

- ✓ Make sure that the websites you visit have HTTPS in front of the URL
- ✓ Before clicking on emails, check the sender of the email
- ✓ DO NOT make a purchase or send sensitive data on a public Wi-Fi network.
- ✓ Secure your website using SSL
- ✓ Don't click on malicious links or emails
- ✓ Do not download pirated content
- ✓ Secure your network



Drive-By Downloads

Through unwanted programs (malware) on a authentic website, a software is downloaded to the computer by visiting the site. It does not require any action to download the specific file.



Μέτρα Προστασίας

- ✓ Employees should keep their software up to date.
- ✓ Install web-filtering software.
- ✓ Don't give users admin access to their computers.
- ✓ Use minimum browser addons as they often get compromised
- ✓ Develop a habit of safe browsing and be selective about which sites you browse regularly.

Ransomware

A type of malicious advertising, use to spread malware and unwanted files to different sites. A file or code is downloaded to the computer system when click on the affected ad

Μέτρα Προστασίας

- ✓ Back up your files regularly and frequently
- ✓ Complete operating system and any software updates
- ✓ Do not click on email attachments or links from unconfirmed sources
- ✓ Disable Autorun for all devices and macro content in MS Office applications
- ✓ Run regular employee awareness programs



Τι πρέπει να κάνω ως HR?

1. Πολύ καλός έλεγχος υποψηφίων για εργοδότηση (background checks).
2. Υπογραφή Συμβάσεων Απασχόλησης και Όρων Εμπιστευτικότητας.
3. Πρόσβαση στους εργαζόμενους και συνεργάτες στη Πολιτική Ιδιωτικότητας Προσωπικών Δεδομένων (Personal Data Privacy Policy)
4. Ενημέρωση των εργαζομένων για το πλαίσιο ασφάλειας δεδομένων του οργανισμού το οποίο πρέπει να περιλαμβάνει τουλάχιστο τα εξής:
 - a. Πολιτική Πρόσβασης
 - b. Πολιτική χρήσης ηλεκτρονικού ταχυδρομείου
 - c. Πολιτική χρήσης διαδικτύου
 - d. Πολιτική διαχείρισης περιστατικού ασφαλείας
 - e. Διαδικασία επιχειρησιακής συνέχειας
 - f. Πολιτική χρήσης ιδίων συσκευών (BYOD)



Υγιείς Εργασιακές Σχέσεις, Σύγχρονες Επιχειρήσεις



Τι πρέπει να κάνω ως HR?

5. Ενημέρωση των εργαζόμενων για τις περιπτώσεις που επιτρέπεται χρήση εταιρικών μέσων για προσωπικούς σκοπούς.
6. Ενημέρωση για ελέγχους σε email, internet, access usage.
7. Πολιτική για υπάλληλους που αποχωρούν (όλη η εταιρική πληροφορία παραμένει στον οργανισμό, επιστροφή περιουσίας της εταιρείας, κλπ)
8. Διαδικασία διερεύνησης περιστατικού ασφαλείας και εμπλοκή του HR για πιθανές ευθύνες προσωπικού.
9. Ενημερωτικά σεμινάρια και σεμινάρια ευαισθητοποίησης για θέματα Ασφάλειας της Πληροφορίας (Security Awareness programs)
10. Καταγραφή διαδικασιών HR οι οποίες επεξεργάζονται δεδομένα (κυρίως προσωπικά) και προστασία των δεδομένων αυτών.



Υγιείς Εργασιακές Σχέσεις, Σύγχρονες Επιχειρήσεις



Συζήτηση - Ερωτήσεις

Ευχαριστώ

therapon@dataknights.eu



Υγιείς Εργασιακές Σχέσεις, Σύγχρονες Επιχειρήσεις

