The Insider Threat

Rigas Angelou - Information Security Consultant
Panagiotis Georgiou - Information Security Specialist

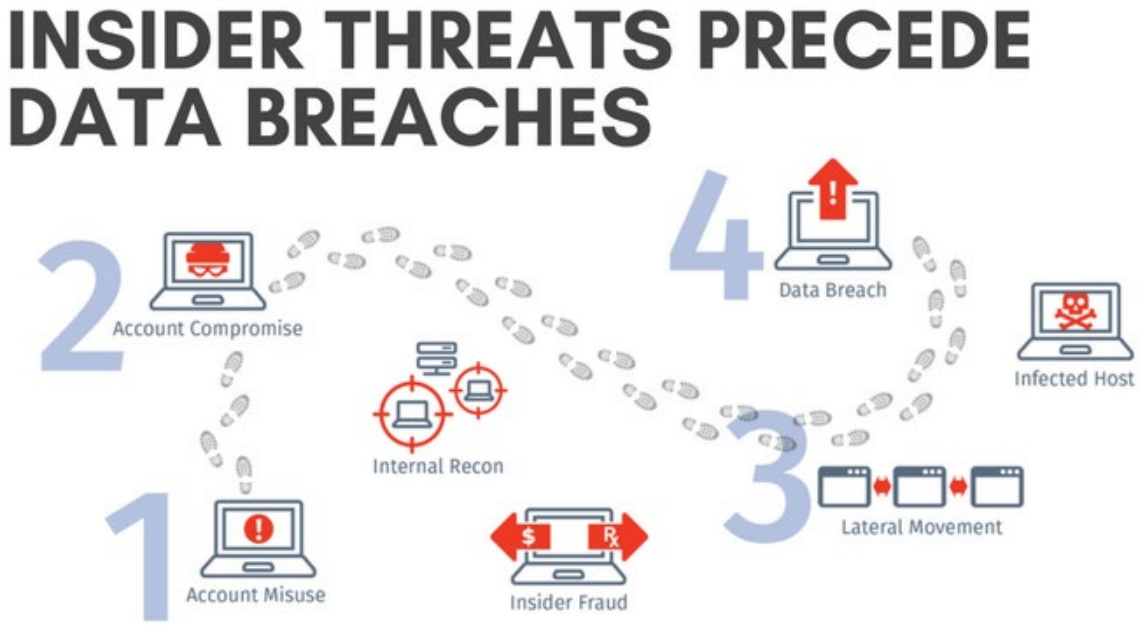
SPACE

Classification ISO 27001: Public

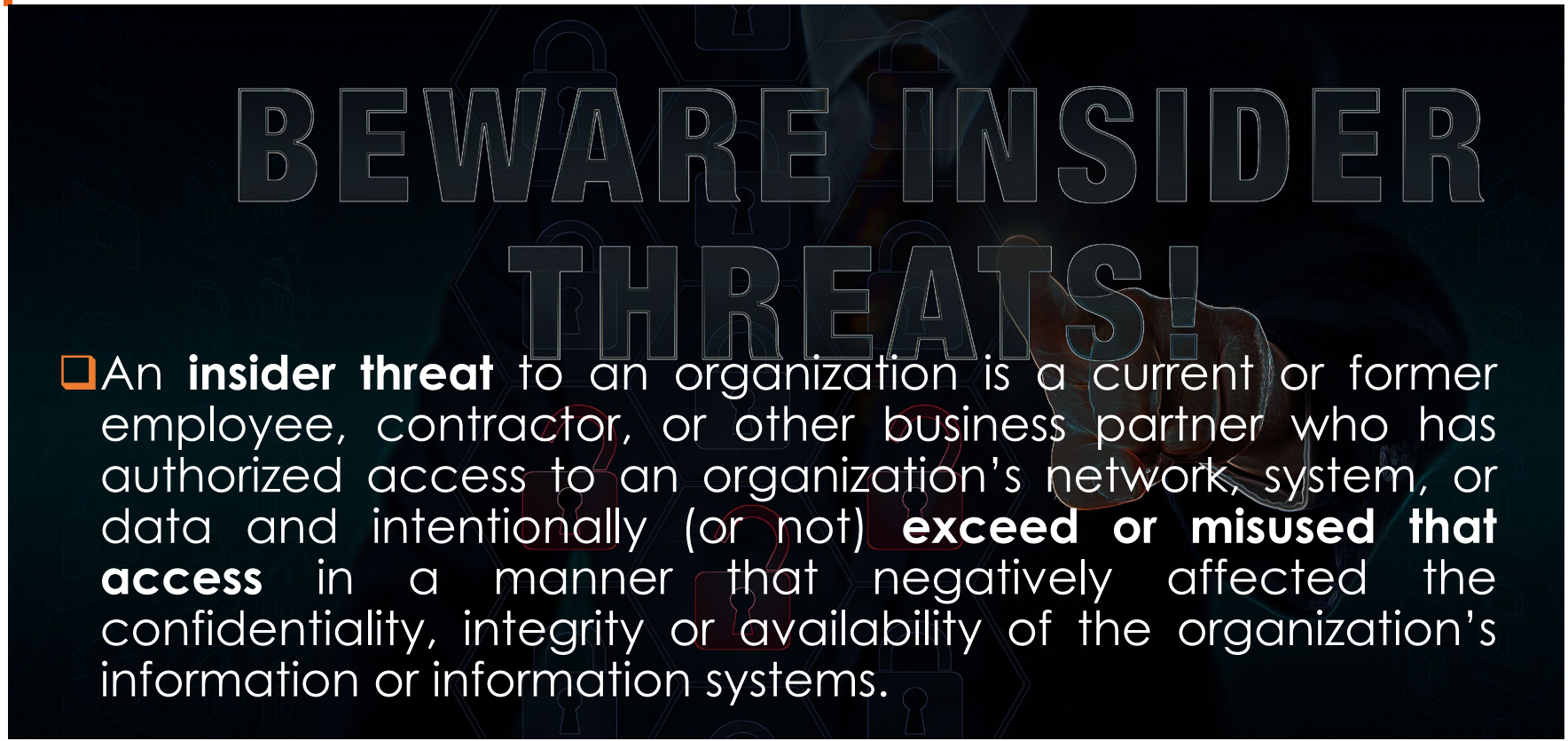
Athens, Greece 16-04-2019

www.space.gr

Why there is an Insider Threat



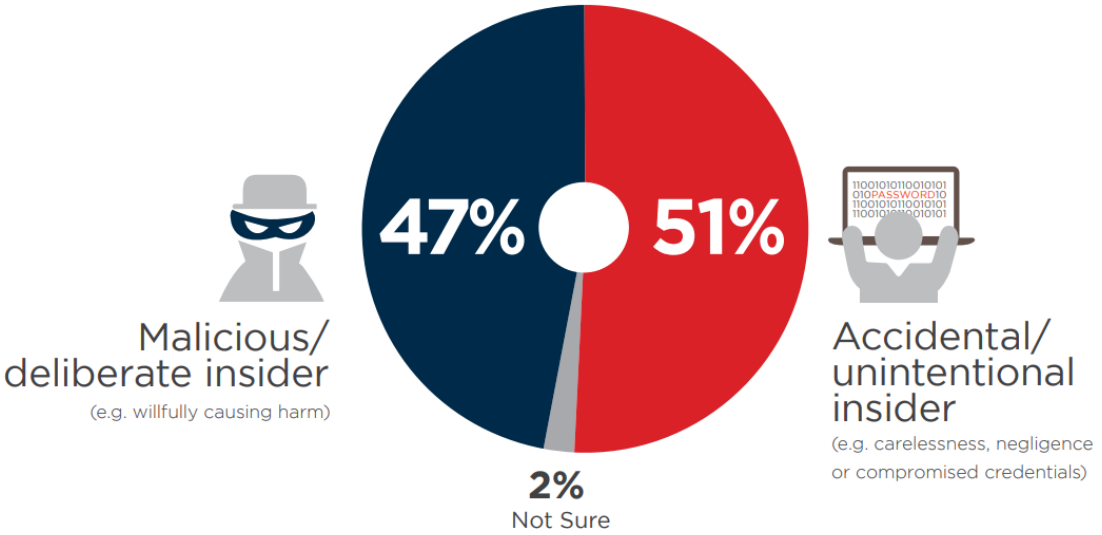
What it is…



- An **insider threat** to an organization is a current or former employee, contractor, or other business partner who has authorized access to an organization's network, system, or data and intentionally (or not) **exceed or misused that access** in a manner that negatively affected the confidentiality, integrity or availability of the organization's information or information systems.

The Insider Threat is...The Employee

- Employees who are disgruntled or seek to gain financially through illicit actions
- Employees with unintentional and unwise behavior

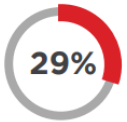


Risk per Type of Employees

56%
Regular employees

55%
Privileged IT users/admins

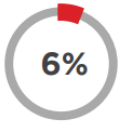
42%
Contractors/service providers/ temporary workers



Privileged business users/ executives

Customers/ clients

None



Not sure/ other

Result: Data Loss

57% Confidential business information

(Financials, customer data, employee data)

52% Privileged account information

(Credentials, passwords, etc.)

49% Sensitive personal information

(PII/PHI)

32% Intellectual property

(Trade secrets, research product designs)

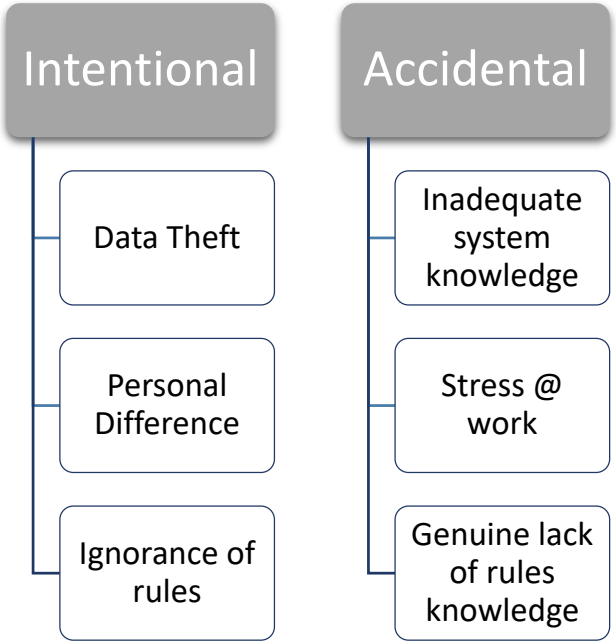
31% Employee data

(HR)

27% Operational/ infrastructure data

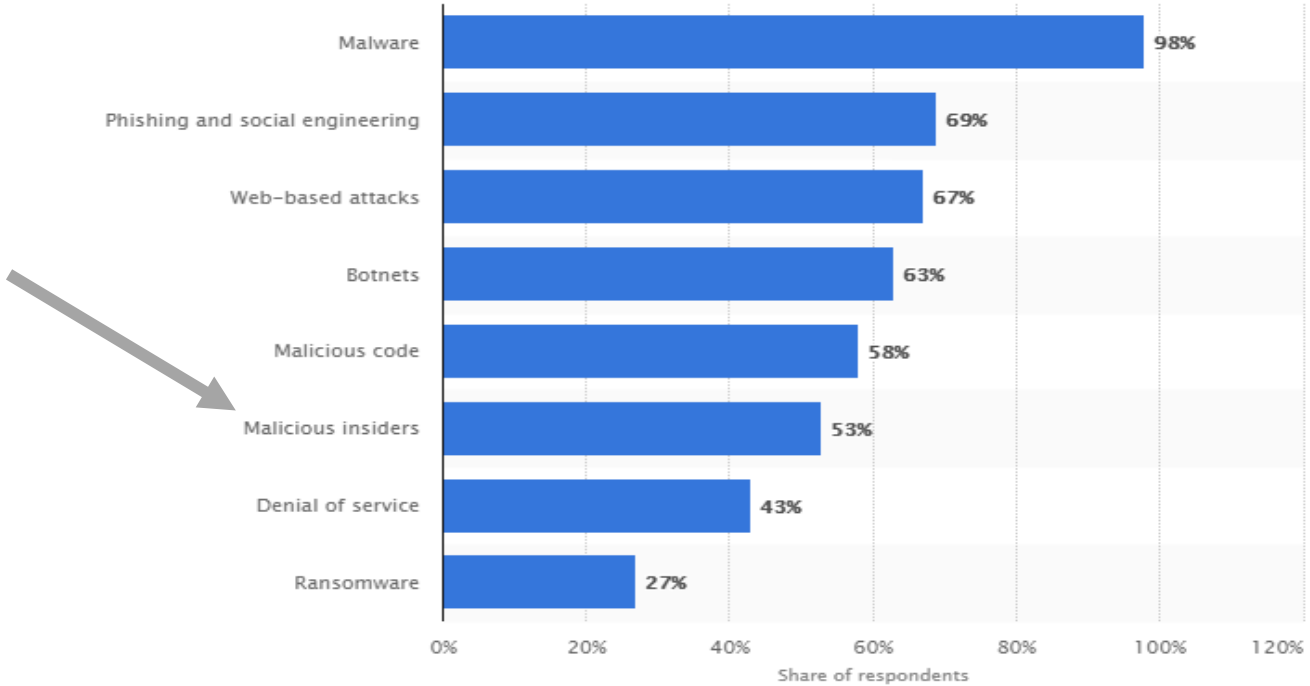
(Network, infrastructure controls)

Analysis: Misuse of Information



How big is the problem?

Analysis of malicious or criminal attacks experienced by companies worldwide as of August 2017



It’s in the news…

STROZ FRIEDBERG

DIGITAL RISK MANAGEMENT & INVESTIGATIONS

ABOUT US | SERVICES | PROFESSIONALS | MEDIA & EVENTS | RESOURCE CENTER | CONTACT

Home / Resource Center / Case Studies / Stroz Friedberg Investigates Insider Data Breach and Identity Theft at a Public Company

Back

Stroz Friedberg Investigates Insider Data Breach and Identity Theft at a Public Com

Two customer service representatives of a publicly-traded company that specialized in handling sensitive insurance claims were terminated and arrested after a check ca company alerted law enforcement to suspicious-looking checks. These customer service representatives had diverted checks from the accounts held for the company's c their own use. The company initially took steps on its own to respond to the data breach and then asked Stroz Friedberg to review the actions taken by the IT staff, evaluate of the breach, and determine what additional steps were required to ensure that the internal investigation was thorough and complete, in the most expeditious and cost-ef manner practicable.

Solar panel maker SunPower sues former staff for insider data theft

Five employees accused of connecting USB devices to steal data and trying to access email after leaving club

SunPower Corp has sued five of its former employees for stealing proprietary information from the solar panel manufacturer and using it to benefit a rival firm.

The five are accused of connecting personal USB storage devices to SunPower systems and stealing the data around the time they were leaving the company last year. SunPower did not notice the theft until December, when one of the former employees was caught attempting to use his email account a

Insider data theft costs Bank of America $10 million

By Robert McMillan

IDG News Service - A Bank of America insider who sold customer data to criminals cost the bank at least US$10 million in losses.

Bank of America began notifying customers of the incident recently, but is not providing many details of the case which is still under investigation. The theft, "involved a now former associate who provided customer information to people outside the bank, who then used the information to commit fraud against our customers," said Bank of America spokeswoman Colleen Haggerty, in an email message.

German state buys Swiss banking data

REUTERS

BERLIN, July 14 – Authorities in the German state of North Rhine-Westphalia have bought a CD from Switzerland containing wealthy Germans' bank details a part of a drive to identify tax evaders, the Financial Times Deutschland said in its online edition on Saturday.

It’s in the news…

Computershare insider loses USBs with stolen customer financial data

Posted on 09 November 2011

Computershare, one of the largest financial market services and technology providers in the world, has filed a suit with the Massachusetts District Court against former employee Kathyann Pace who stands accused of exfiltrating huge amounts of company documents following her resignation, reports Threatpost.

Pace, who resigned back in September, 2010, had kept the comp laptop for nearly a month after her resignation.

Wikileaks and data theft

January 28, 2011 | Data leakage

A colleague of mine, Bill Munroe, is VP Marketing at Verdasys, the first of the a most established of the independent pure play DLP technology companies. (No relationship with Verdasys). Bill has written a paper entitled "Protecting against *trusted insider threat*". The paper brings a number of important insights regardi State Department cables and why Wikileaks is different.

Malicious insider sells Fidelity National customer data

Bill Brenner, Senior News Writer

Published: 5 Jul 2007

Fidelity National Information Services Inc. admitted this week that Certegy Check Services Inc., a Fidelity subsidiary that provides check processing services, was "victimized" by a database administrator who stole and sold bank and credit card data on up to 2.3 million

Κύπρος | Λεμεσός

Προφυλακίστηκε ως ύποπτος υπεξαίρεσης ενός εκατομμυρίου

Τραπεζικός υπάλληλος υπεξαίρεσε 482.719

Potential Indicators

Create an Insider Threat Program NOW!

64%

Detection
(e.g., user monitoring, IDS, etc.)

58%

Deterrence
(e.g., access controls, encryption, policies, etc.)

49%

Analysis and post breach forensics
(e.g., SIEM, log analysis, etc.)

Post breach remediation
(e.g., backup/disaster recovery, etc.)

Deception
(e.g., honeypots, etc.)

How is the attack detected?

63% Intrusion Detection and Prevention (IDS/IPS)

62% Log management

51% Security Information and Event Management (SIEM)

40% Predictive analytics

User and Entity Behaviour Analytics (UEBA) 39% | Other 2%

How is the attack deterred?

60%

Data Loss Prevention
(DLP)

60%

Encryption of data
(at rest, in motion, in use)

56%
Identity and Access Management
(IAM)

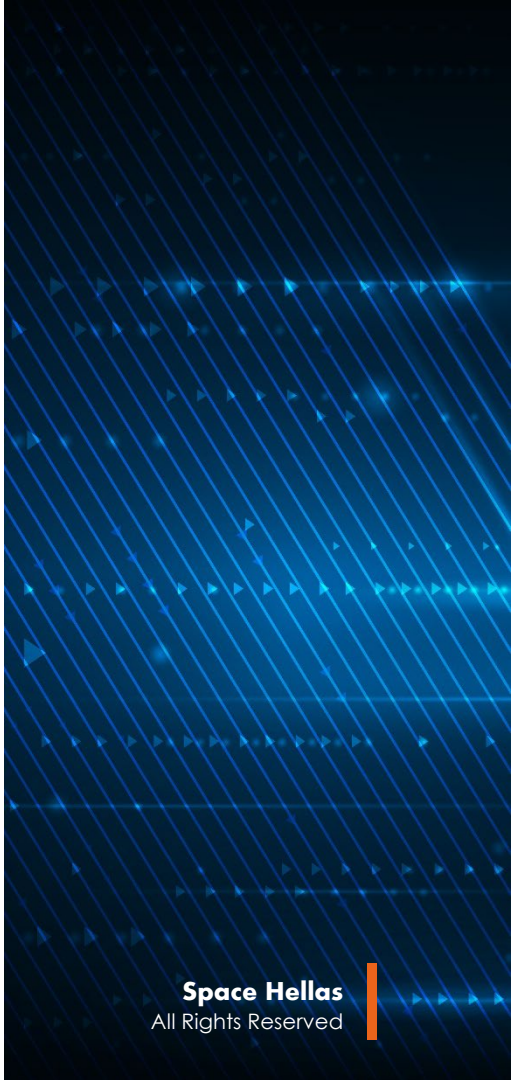
50%
Endpoint and mobile security

29%
Cloud Access Security
(CASB)

Enterprise Digital Rights Management Solutions (E-DRM) 29% | Privileged account vault 27% | Other 1%

Learn from past incidents

- Some organizations experience the same types of insider crimes more than once
- When you have an attack, implement controls to catch it next time
- Some organizations create formal teams to examine past incidents and implement new controls



Educate Employees

Educate Employees Regarding Potential Recruitment

- Carefully consider: do you have any systems or data that an insider could be paid to steal or modify?
  (Financial, Personally Identifiable Information (PII), identity documents, utility bills, credit histories)

- Security Awareness Trainings offering
- Exit Interview

Privacy Issues

Address Employee Privacy Issues with the Legal Department

- Employee privacy issues present a tricky legal issue
- Laws and regulations differ in private sector, government, and various critical infrastructure sectors
- Some organizations: Have created and implemented insider threat policies and processes by working with Human Resources, General Counsel, Information Security / Information Technology, Security, and Top Management

It’s a team work!

Work Together Across the Organization

- IT cannot do this alone!
- Need communication across Management, Information Security / Information Technology, Security, Data Owners, Software Engineering, General Counsel, and Human Resources
- Some organizations: Achieve this communication but only after significant suspicious activity warrants an investigation
- Proactive communication between organizational units

Space Hellas Insider Threat Portfolio

- User & Endpoint Behavior Analytics (UEBA)
- Identity and Access Management (IAM)
- Security Information Event Management (SIEM)
- Intrusion Detection/Prevention Systems (IDPS)

- Mobile Device Management (MDM)
- Endpoint Detection & Response (EDR)
- Encryption (At Rest, In Motion, In Use)
- Cloud Access Security Broker (CASB)
- User Security Awareness Services
- Data Loss Prevention (DLP)

References

- http://www.ponemon.org/index.php
- https://www.observeit.com/ponemon-report-cost-of-insider-threats/
- https://www.sei.cmu.edu/about/divisions/cert/index.cfm
- https://crowdresearchpartners.com/

Thank You !

For any questions feel free to visit
Space Hellas Booth

SPACE

Classification ISO 27001: Public

MK-23082018-1

www.space.gr