

# Cyber-Threats and Countermeasures in Financial Sector



**Michael Mavroforakis, PhD**  
**Group CISO & CDO**

**SEV: “Workshop on Digital Enablers”**  
**(Cloud & Cybersecurity)**

**27th March 2018**



## CYBERSECURITY

- Potential Targets
- Attack Examples
- Insider vs Outsider
  - Threats' Origin, Motives, Targets, Methods, Attacks
- Target: Customers (Methods & Impact)
- Countermeasures for Internal and External Threats
- Cybersecurity Architecture
- Steps Taken to Address Cybersecurity Risks

# Potential Targets: All Types of Industries



## AIRLINE CYBER ATTACKS

### VIETNAM AIRLINES 29 July 2016

A website breach by hackers released confidential customer data, including the names, addresses and birthdates of 400,000 members of Vietnam Airlines' frequent flyers' club. The hackers accessed screens displaying Vietnam Airlines' flight information, and took over the tannoy system, airing political messages regarding China's claims to the South China Sea.

### LOT 21 June 2015

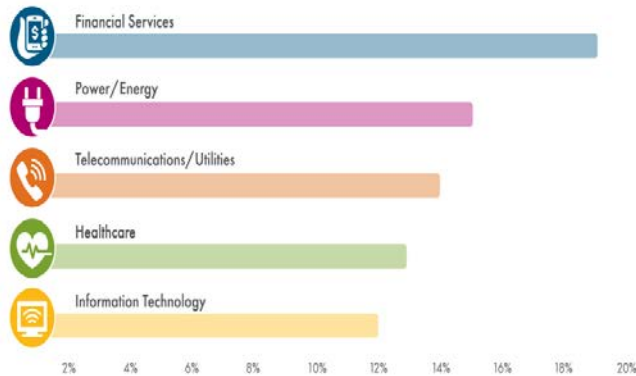
More than 1,400 passengers at Warsaw's Frederic Chopin Airport were grounded due to a cyber-attack. The incident prevented the airline from creating flight plans, grounding scheduled flights until the issue was resolved.

### BRITISH AIRWAYS 27 March 2015

British Airways reported that the accounts of its frequent flyer programme were compromised, as members were sharing credentials on another online service that could have been hacked. Tens of thousands of British Airways Executive Club accounts were broken into via credentials stolen from a third party – and the attackers managed to redeem members' reward points.

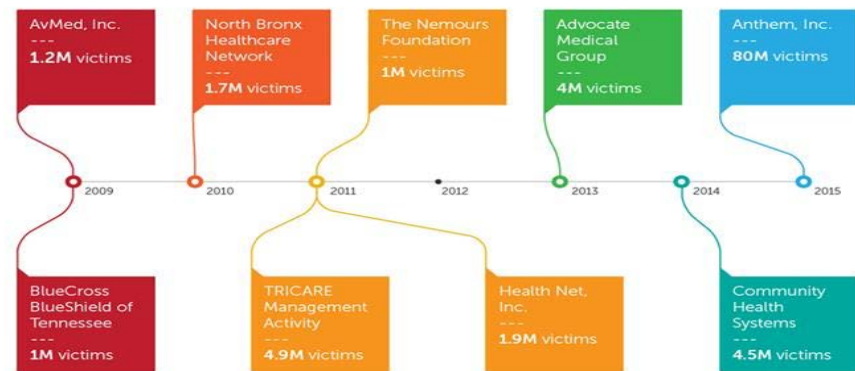


## Industries Most Likely to Face a Systemic Attack



SOURCE: Is Cyber Risk Systemic?, April 2017. Industries identified by experts as most likely to face an attack in 2017.

## NOTABLE HEALTHCARE BREACHES



# Attack Examples: Money & Capital Loss



## “How Hackers Stole \$80 Million from Bangladesh Bank”

18<sup>th</sup> of May, 2016



“The attack on Bangladesh's central bank that let **hackers stole over \$80 Million** from the institutes' Federal Reserve bank account was reportedly caused due to the **Malware** installed on the Bank's computer systems”

“A typo in some transaction prevented a further **\$850 Million Heist**”

September, 2017



“Massive Equifax Data Breach Could Affect Half of the U.S. Population” (145,5M)

Equifax, Inc. Stock Chart



“US-based credit ratings firm says records of UK citizens were among those unlawfully accessed during cyber-attack in July”

Potential **GDPR** Fines



The screenshot shows a ransomware message with a dark background and red and yellow text. At the top, there are seven small flags: France, Spain, Denmark, Germany, Netherlands, Italy, and the United States. The main text is in red, stating that personal files are encrypted by CTB-Locker. Below this, white text explains that documents, photos, and databases are encrypted with a unique key. A yellow warning states that the private decryption key is on a secret server and that the user has 96 hours to pay. At the bottom, there are three yellow buttons: 'View', a timer showing '95:59:29', and 'Next >>'. A red warning triangle with an exclamation mark is on the left side of the bottom section.

**Your personal files are encrypted by CTB-Locker.**

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

**You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.**

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

**WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.**

**View**      **95:59:29**      **Next >>**

# Insider vs Outsider: Threats' Origin



**Insider Threats:** Originate from within a business. Can include any party that introduces risk through malicious or unintentional behavior.

**Outsider Threats:** Originate from external sources. Can be any threat actor that isn't affiliated with the business directly.



Employees



Cybercriminals



Business Partners



Hackers



Contractors



Competition - sponsored attackers



Compromised Internal Accounts



Nation - sponsored attackers



## Insider Threats



Financial Gain



Personal Advantage



Professional Revenge



Outside Influence  
(Competitor/Nation  
State/Criminals)

## Outsider Threats



Financial Gain



Corporate or Nation –  
Sponsored espionage



Political or Military  
Advantage



Political or Social  
Change



## Insider Threats



Intellectual Property and Trade Secretes



Business Plans and Corporate Secrets



Products and R&D Information



Source Code



Personal Information



Financial Information

## Outsider Threats



Cybercriminals

- Likely Targets:
  - Financial and Personal information



Hackivists

- Likely Targets:
  - Corporate Secrets & Business Information



Competition Sponsored Attackers

- Likely Targets:
  - Trade Secrets & Business Plans



Nation - Sponsored Attackers

- Likely Targets:
  - Trade secrets
  - Business Information
  - Critical Infrastructure
  - Employee/Customer Personal Information





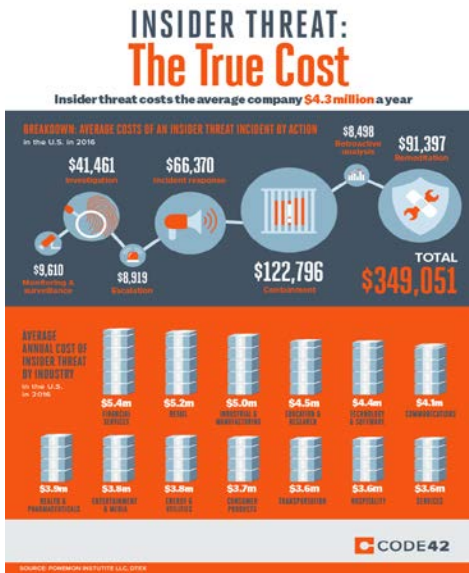
## Insider Threats

-  Social Engineering
-  Physical Theft
-  Privileged Abuse
-  Copying or Offloading Sensitive Data to Personal Accounts/Drives
-  Unintentional Data Leaks or Loss of Company Property

## Outsider Threats

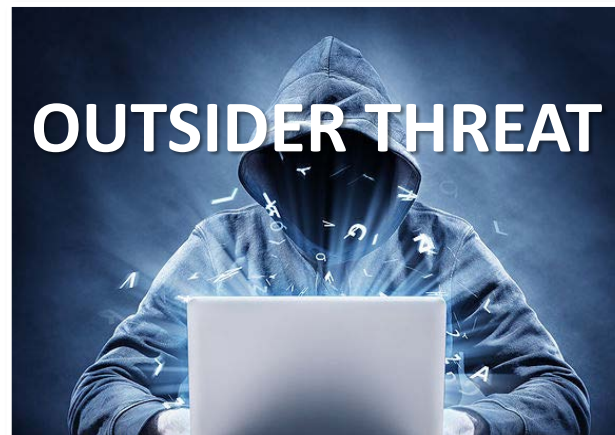
-  Social Engineering
-  Hacking
-  Malware
-  Distributed Denial Of Service (DDoS)
-  Malicious USB Drops
-  Physical Theft

# Outsider Insider vs Outsider: Threats' Attacks



Malicious Insider Attacks Are:

Much More Costly than Outsider Attacks

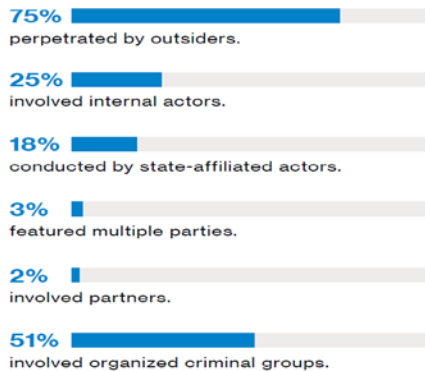


Outsider Attack Methods like DDoS and Web Attacks Are:

More Prevalent Than Attacks By Malicious insiders

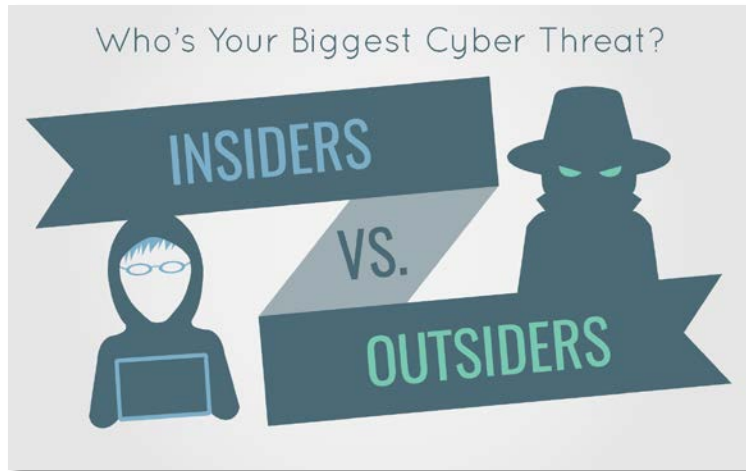
Source: 2016 Ponemon Institute

## Who's behind the breaches?



Source: 2017 Verizon, Data Breach Investigation Report

# Are Insiders or Outsiders BIGGER Threat to Your Business?



Careless Insider



Malicious or Criminal Insider



External Attacker



Combined Insider and External Attacker



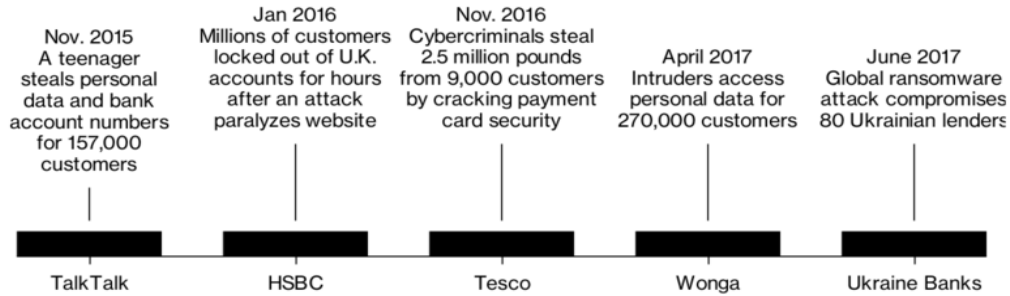
THE MOST LIKELY ROOT CAUSES OF DATA BREACHES ARE:

# Target: Customers

## Attack Methods & Impact



### Cybercriminals use many methods to penetrate lenders and bank accounts



Bloomberg

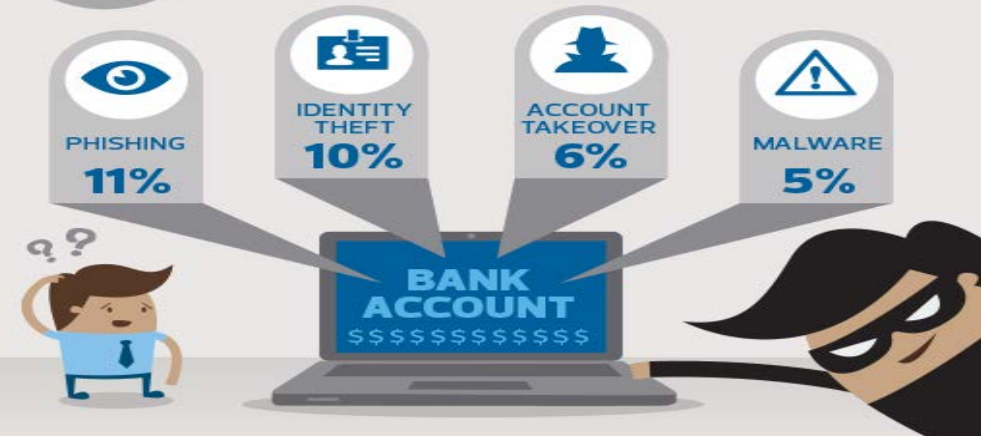
## Attack Methods

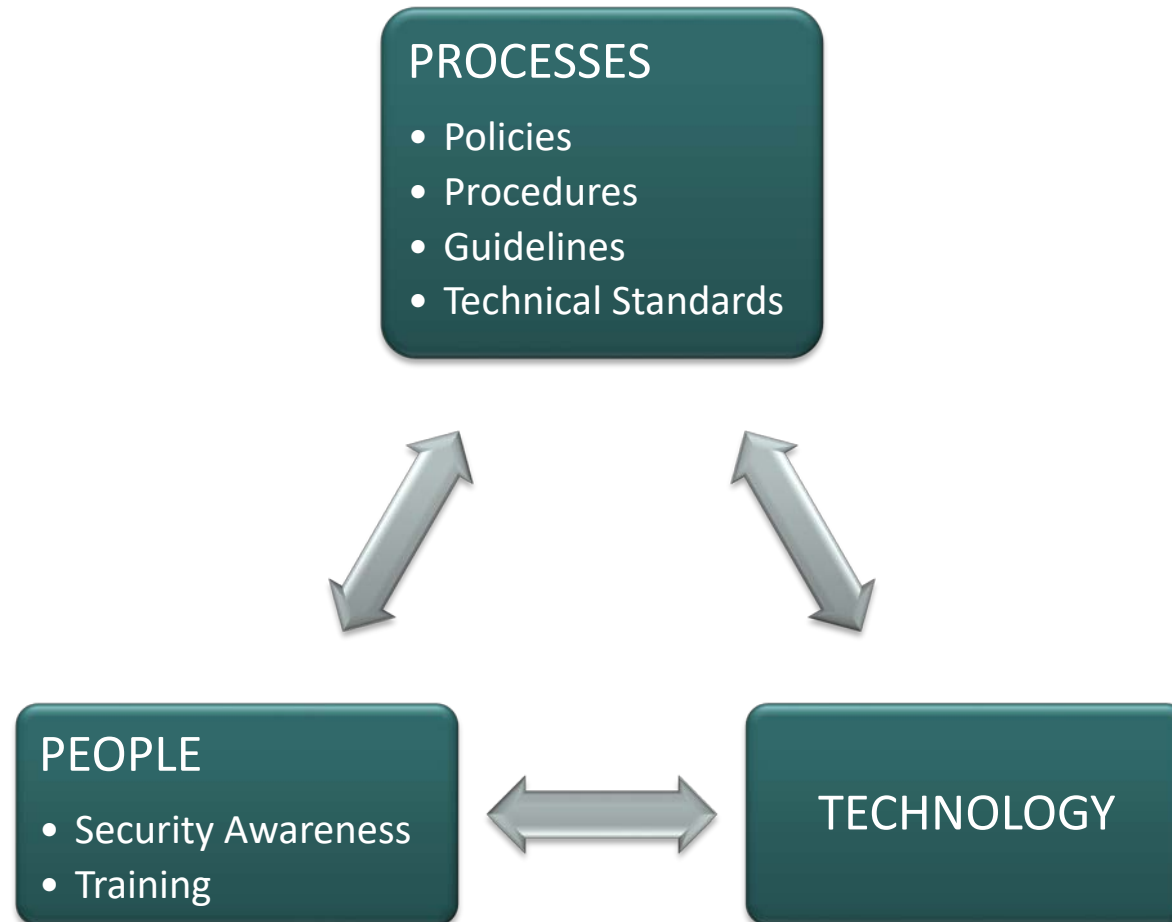
- Phishing
- Identity Theft
- Account Takeover
- Malware
- Card Fraud

## Impact

- Financial Loss
- Reputational Damage
- (Dramatic) Customer Base Shrinkage
- Penalties / Compensations
- Legal Implications

**28%** Customers that say their personal bank account has been the target of a cyber attack



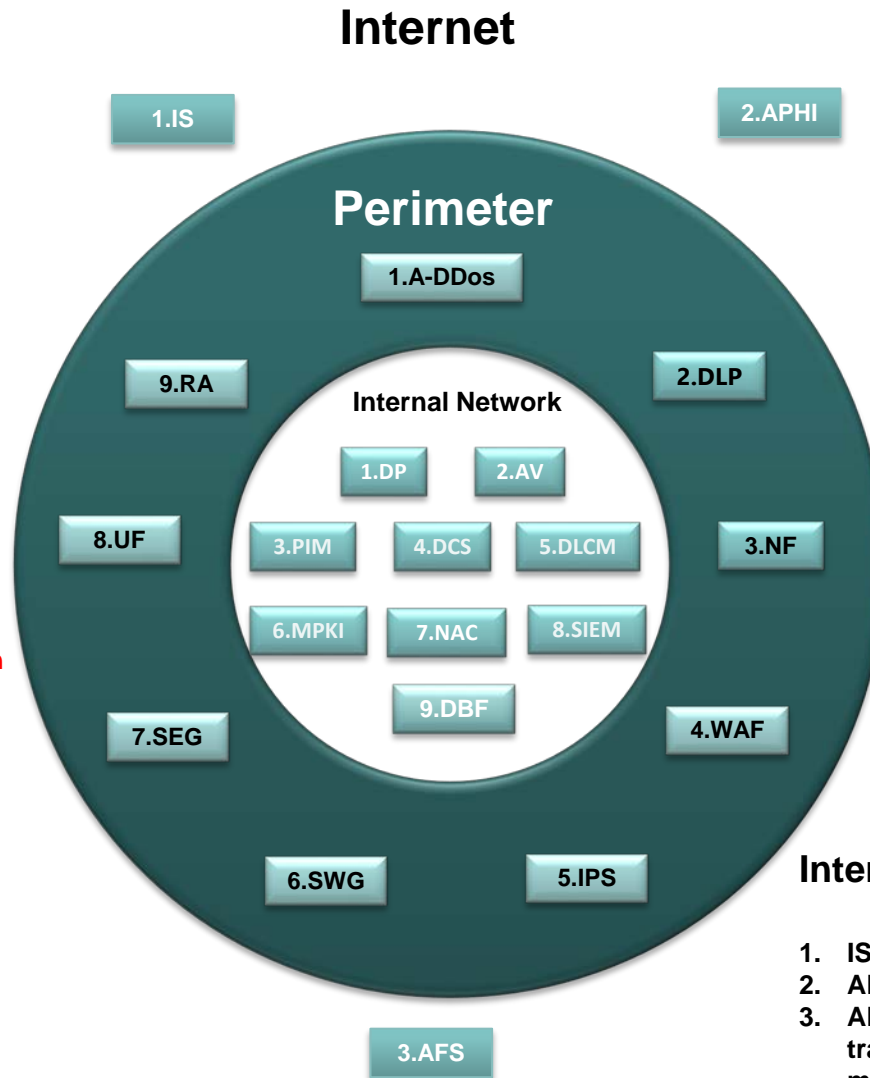


# Cybersecurity Architecture: Typical Example



## Internal Network

1. **DP** - Directory Policies
2. **AV** – AntiVirus
3. **PIM** - Privileged Identity Management
4. **DCS** - Database Compliance System
5. **DLCM** - Data Life-Cycle Management
6. **MPKI**-Managed Public Key Infrastructure
7. **NAC** - Network Access Control: **Allow only authorized Devices to Connect to Network (wired or wireless)**
8. **SIEM** - Security Information & Event Management: **From several billion alerts per month a few cases are investigated leading to successful resolution of all high severity incidents**
9. **DBF** - Data Base Firewall



## Perimeter

1. **A-DDoS** - Anti-Distributed Denial of Service: **Up to Tenths of serious DDoS attacks per month**
2. **DLP** - Data Loss Prevention
3. **NF** - Network Firewall: **Several million attacks per month, are successfully confronted**
4. **WAF** - WEB Application Firewall: **Thousands attacks per week are successfully confronted**
5. **IPS** - Intrusion Prevention Systems: **Thousands of attacks per week are successfully confronted**
6. **SWG** - Secure Web Gateway: **Several billion attacks per month, are successfully confronted**
7. **SEG** - Secure Email Gateway: **Millions rejects per week**
8. **UF** - URL Filtering
9. **RA** - Remote Access

## Internet

1. **IS** - Internet Surveillance
2. **APHI** - Anti-Phishing
3. **AFS** - Anti-Fraud Services: **From several million transactions per month several thousand malicious transactions are blocked**



We can't eliminate the risk of cyber attacks, but we can minimize their consequences. Five (5) things we do to combat cybersecurity risks:

- **1** ***Own the Risk***
  - Cyber risk is owned by leadership and is not relegated to the IT function.
  - Periodic cybersecurity briefings are provided to the Board and C-Suite.
- **2** ***Prioritize Initiatives***
  - Leadership prioritizes and monitors cybersecurity investments.
  - Investments are made in new capability, not just technology.
  - Critical Assets are identified and their protection prioritized.
- **3** ***Learn and Incorporate***
  - Work with leading various external parties, share information on current threats and incorporate learnings into our own cybersecurity strategy and tactics.
- **4** ***Enhance Culture***
  - A security culture and mindset is established through training, measurement and evaluation.
  - Behaviors and capabilities of the organization are established and reinforce the importance of cybersecurity.
- **5** ***Secure the Business***
  - Security of the business value chain including suppliers, third party providers and high-risk interconnection points is considered.
  - Adapt to the challenges of new and emerging digital business models.

Source: PwC