



# AAFCPAs

## Cybersecurity in 2018



Vassilis Kontoglis  
Manager, Business &  
IT Advisory  
AAFCPAs



Peter Sebilian  
Manager, Business &  
IT Advisory  
AAFCPAs

# Defining the Discussion

## Cybersecurity

Technologies, Processes, and Practices to Protect our Environments from Unauthorized Access.

## Data Breach

Incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

## Personal Identifiable Information (PII):

Information that can be used to distinguish or trace an individual's identity.  
(MA Reg. 201 CMR 17 & EU GDPR)

## Personal Health Information (PHI)

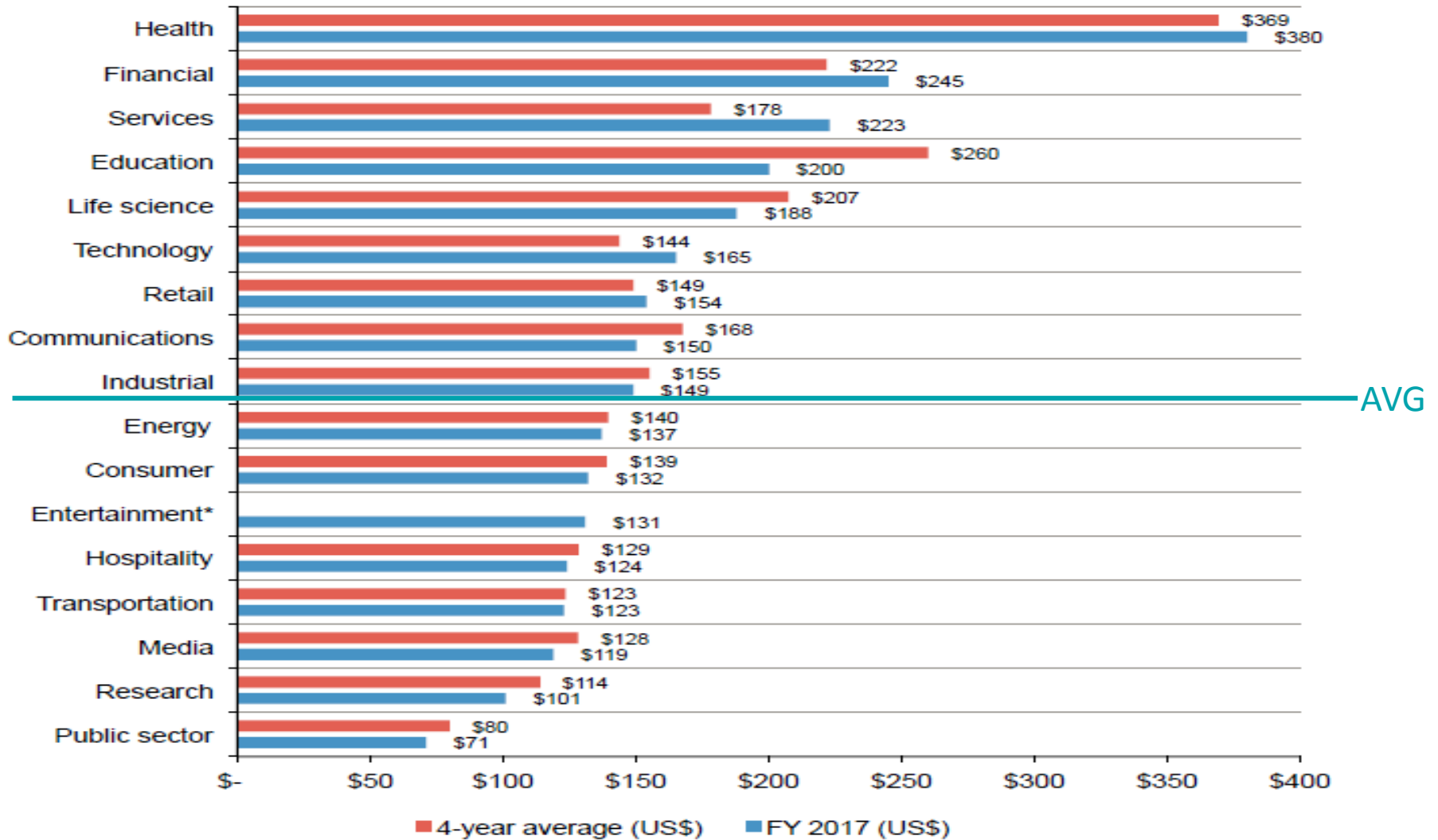
Information about health status, provision of care, or payment for care that can be linked to a specific individual.  
HIPPA 45 CFR 160.103

# 2017 Research (Ponemon Institute) Impact Statistics

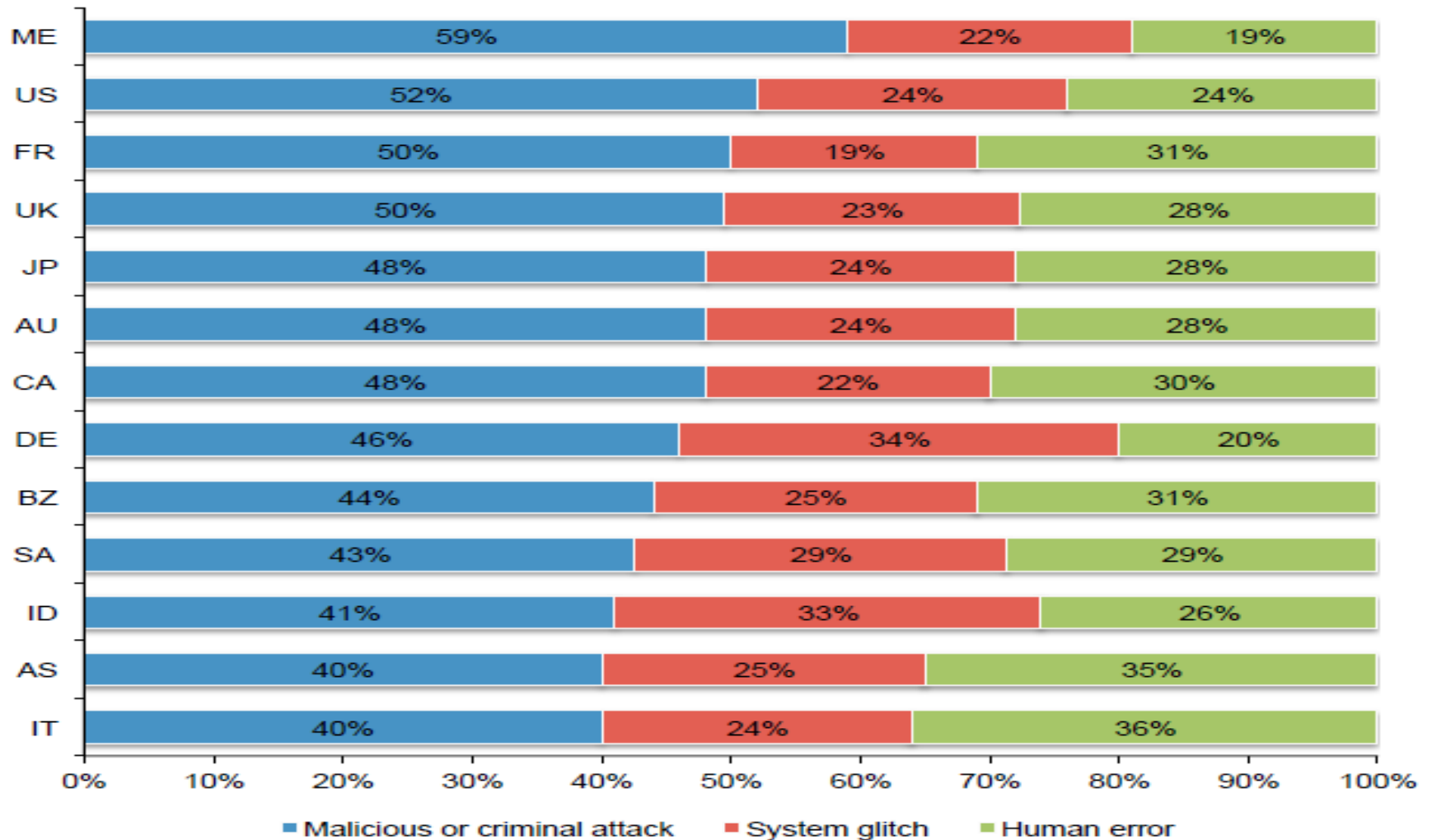
- 419 Companies in 13 Countries in Study
- Avg. Days to Identify the Breach – 191
- Avg. Days to Contain the Breach – 66
- Regulated industries of Financial Services, Healthcare, and Education are Targeted (higher value = higher risk)
- Avg. Cost per Breached Record – \$141

Costs= Forensics Fees, Lost Business Value, Lawsuits, Ransom Payment, Recovery fees

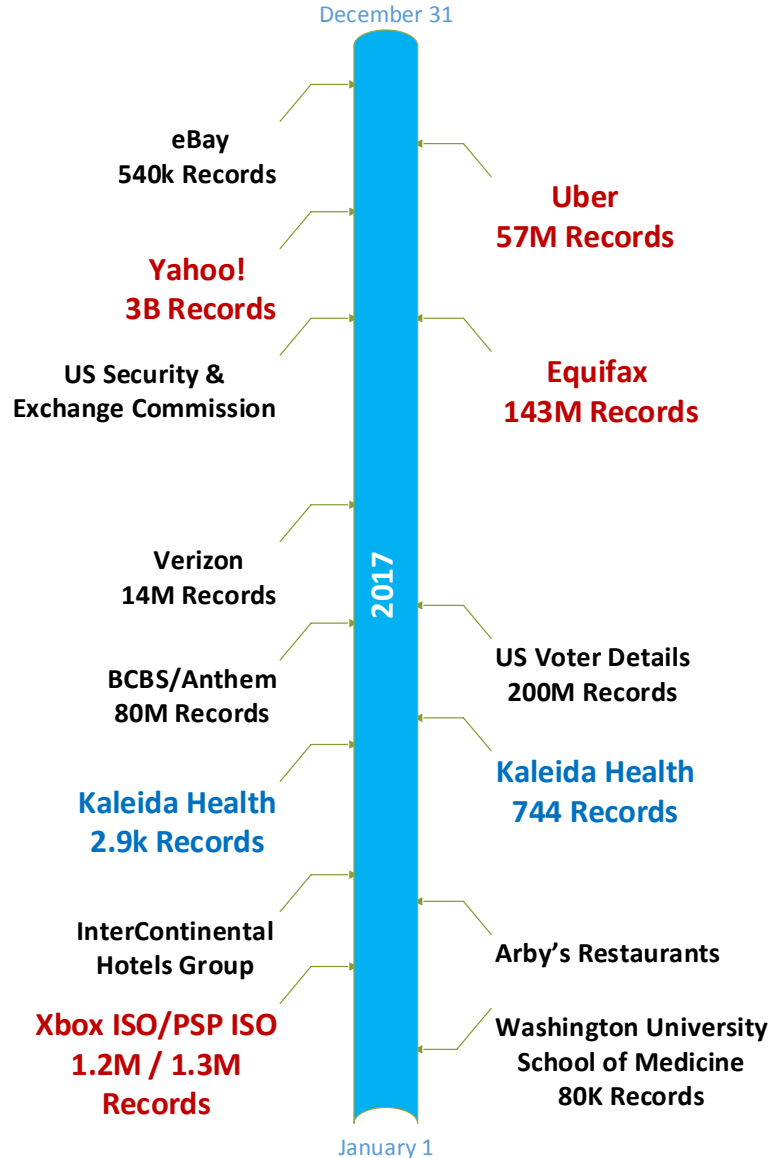
# Data Breach Record Cost / Industry Segment



# Data Breach Causes / Country & Region



# Notable Data Breaches in 2017



# How These Attacks Occur

- Socially Engineered Attacks
  - Hacking (Unauthorized Access)
  - Phishing (Trying to Obtain Unauthorized Access)
  - Spear Phishing (Targeting You Specifically)
  - Whaling (Targeting Decision Makers & Exec Level)
- Malicious Attacks
  - Malware (Ransomware/DOS Attack/Keystroke Logging)
  - Unauthorized Access or Disclosure of PII
  - Physical Security Breach
- Exploitation of Application Vulnerabilities
- Unprotected or Improperly Secured Devices (Laptops/Media)
- 3<sup>rd</sup> Party Providers (IT Services, Cloud Provisioned)
- Unsecured Backup / Recovery Media
- A Lack of Cyber Threat Training and Awareness

■ Malicious or criminal attack   ■ System glitch   ■ Human error

# Protecting Your Castle



- The Multi Layered Approach in 1518.
  - Moat, High Walls, Built on a Hill, Draw bridge that can be raised, Capable Defenders
- The Multi Layered Approach in 2018.
  - Threat Monitoring, Firewalls, Access Controls, AV/Patching, Education, Capable Defenders



# Protecting Our Organizations and Reducing Our Risks

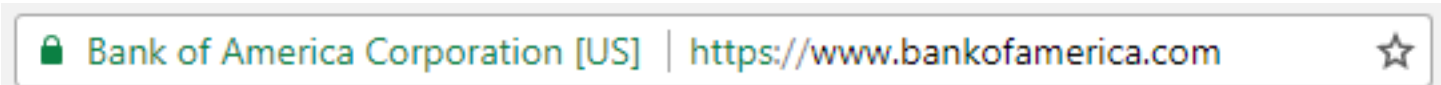
- Identify what needs to be protected (What and Where Are Your Risks)
- Define and implement access controls to data and applications (Least Privilege Concept)
- Maintain your capable defenders (Internal Staff & External Relationships)
  - AntiVirus, Patch Management, eMail & Web Filtering, Firewalls, Monitoring
- Create and review back-up & recovery strategy

# Protecting Our Organizations and Reducing Our Risks

- Have Good Password Management (tools & policies)  
(consider pass-phrase, not pass-word)
- Education – Create a Cyber Aware Community
- Have an Incident Response Plan and Test It
- Consider a Cyber Security Assessment
- Consider a Cyber Insurance Policy

# Protecting Ourselves and Reducing Our Risks

- Maintain your Capable Defenders (AV / Patching)
- Create and Review Back-Up & Recovery Strategy
- Protect Your Passwords and PINs
- Use Caution When Receiving Unexpected eMail
  - Protect Yourself from Phishing Scams (know how to spot them)
- Check That Web Forms Are Secure (<https://>)



# Protecting Ourselves and Reducing Our Risks

- Exercise Caution When Using Wireless Networks
  - Know what you are connecting to
- Limit the Amount of Information You Provide About Yourself Online
  - Contact Sharing within Mobile Applications
- Use Only One Credit Card for Online Purchases (debit cards have limited consumer protections)
- Enroll in Available Auto-Notification Services (free)
- Enroll in Monitoring Services (fee based)
- Monitor Your Financial Statements and Credit Reports Regularly

# Take-A-Ways & Questions

- Any Organization Carries Risk.  
Know your Profile.
- Cyber Awareness Education is Important.
- No Flags go up when a Breach has occurred and no Silver Bullet is Available to Remediate it should it Occur.
- The Multi-Layered Approach towards Protecting our Castles and Ourselves is Necessary.



# Questions & Comments



Vassilis Kontoglis  
Manager, Business &  
IT Advisory  
AAFCPAs



774.512.4069  
vkontoglis@aafcpa.com



Peter Sebilian  
Manager, Business &  
IT Advisory  
AAFCPAs



774.512.4183  
psebilian@aafcpa.com