AAFCPAs

great minds | great hearts

CyberSecurity

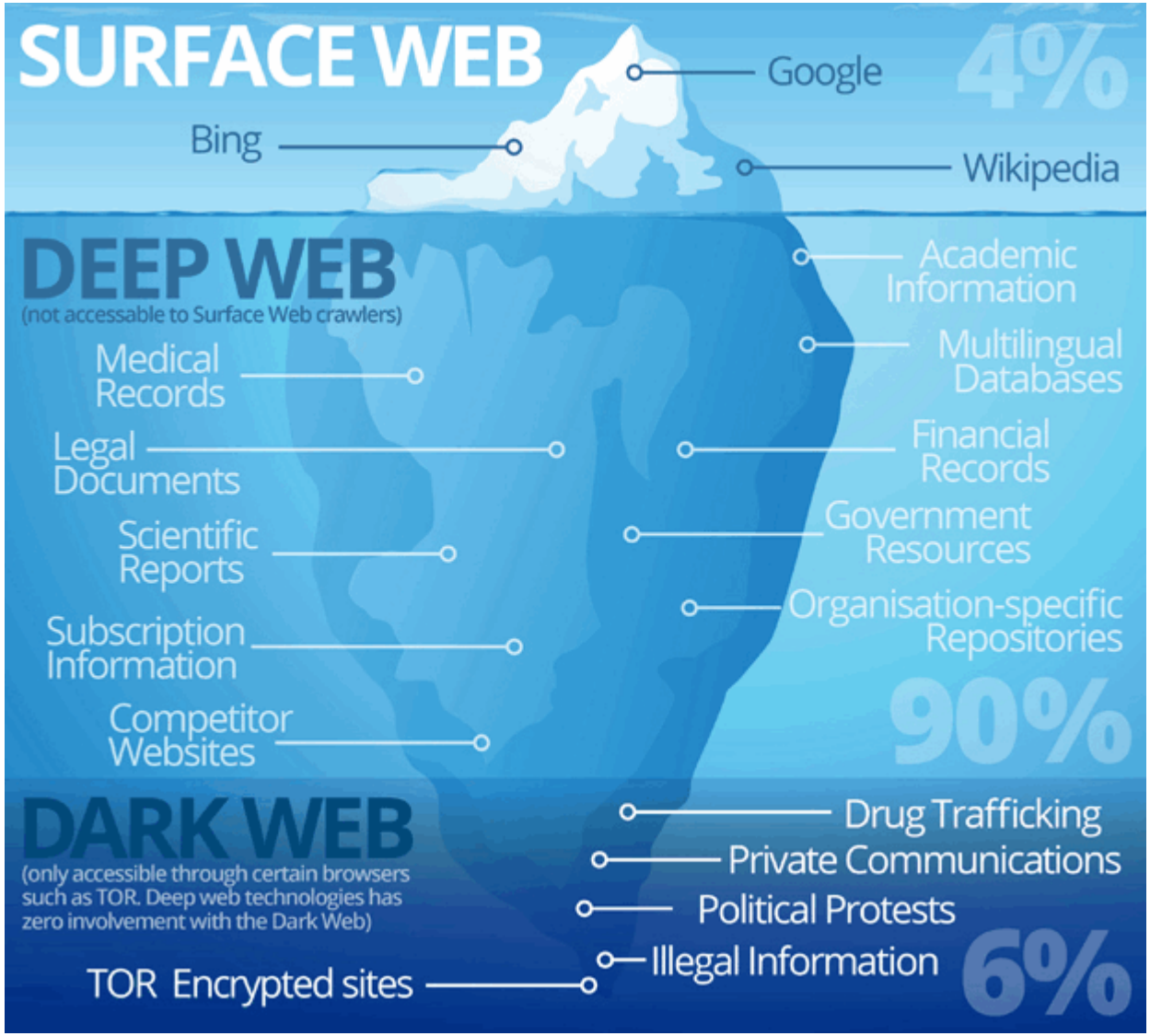
2018 Year in Review & Recommendations

Vassilis Kontoglis

Defining the Discussion

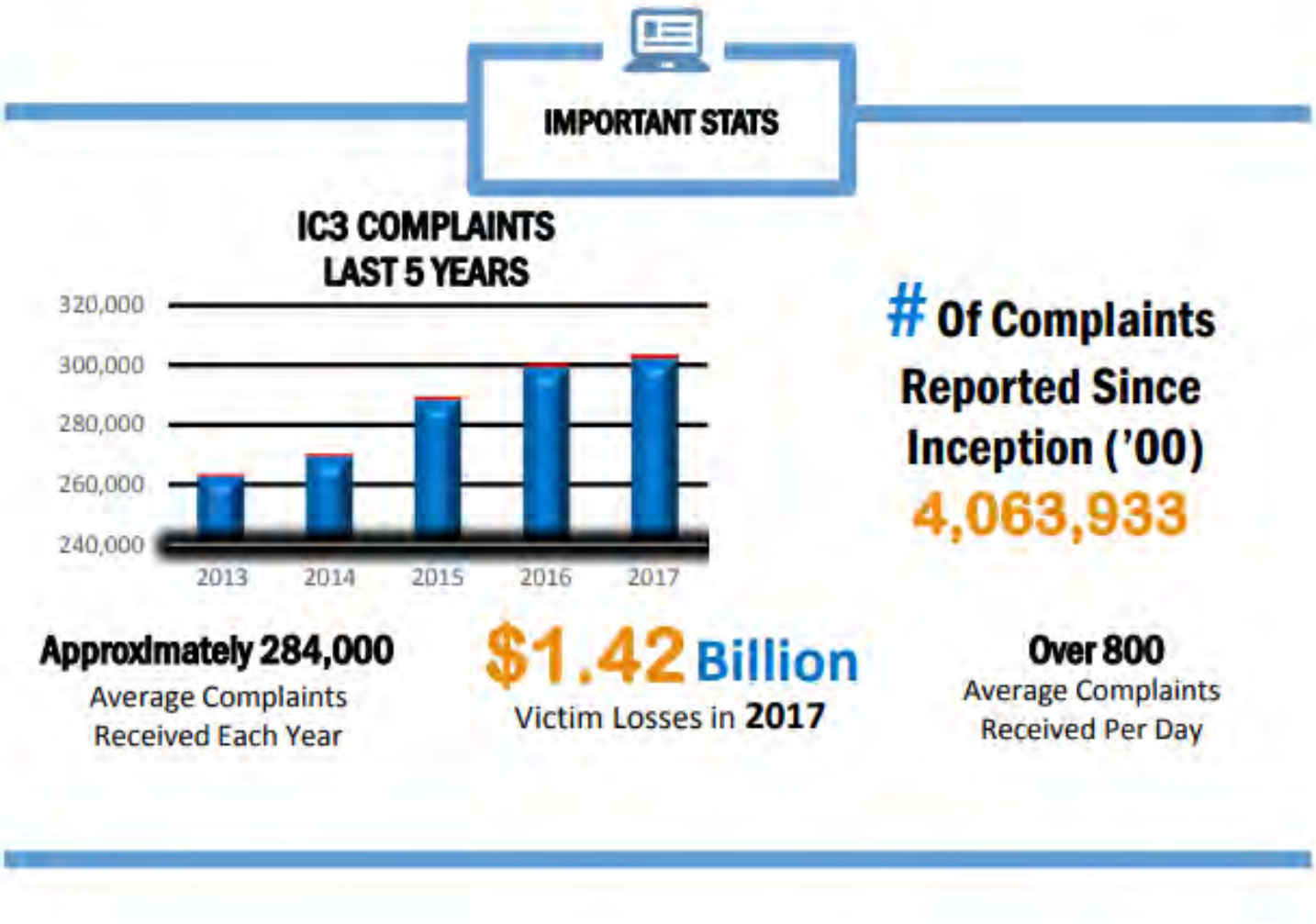
Cybersecurity Technologies, Processes and Practices to Protect our Environments from Unauthorized Access	**Data Breach** Incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
Personal Identifiable Information (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.

Dark Web



The part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.

2017 FBI Report - Internet Crime Complaint Center (IC3)



https://pdf.ic3.gov/2017_IC3Report.pdf

2017 FBI Report - Internet Crime Complaint Center (IC3)

By Victim Count			
Crime Type	**Victims**	**Crime Type**	**Victims**
Non-Payment/Non-Delivery	84,079	Misrepresentation	5,437
Personal Data Breach	30,904	Corporate Data Breach	3,785
Phishing/Vishing/Smishing/Pharming	25,344	Investment	3,089
Overpayment	23,135	Malware/Scareware/Virus	3,089
No Lead Value	20,241	Lottery/Sweepstakes	3,012
Identity Theft	17,636	IPR/Copyright and Counterfeit	2,644
Advanced Fee	16,368	Ransomware	1,783
Harassment/Threats of Violence	16,194	Crimes Against Children	1,300
Employment	15,784	Denial of Service/TDoS	1,201
BEC/EAC	15,690	Civil Matter	1,057
Confidence Fraud/Romance	15,372	Re-shipping	1,025
Credit Card Fraud	15,220	Charity	436
Extortion	14,938	Health Care Related	406
Other	14,023	Gambling	203
Tech Support	10,949	Terrorism	177
Real Estate/Rental	9,645	Hacktivist	158
Government Impersonation	9,149		

Descriptors*		
Social Media	19,986	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.
Virtual Currency	4,139	

2017 FBI Report - Internet Crime Complaint Center (IC3)

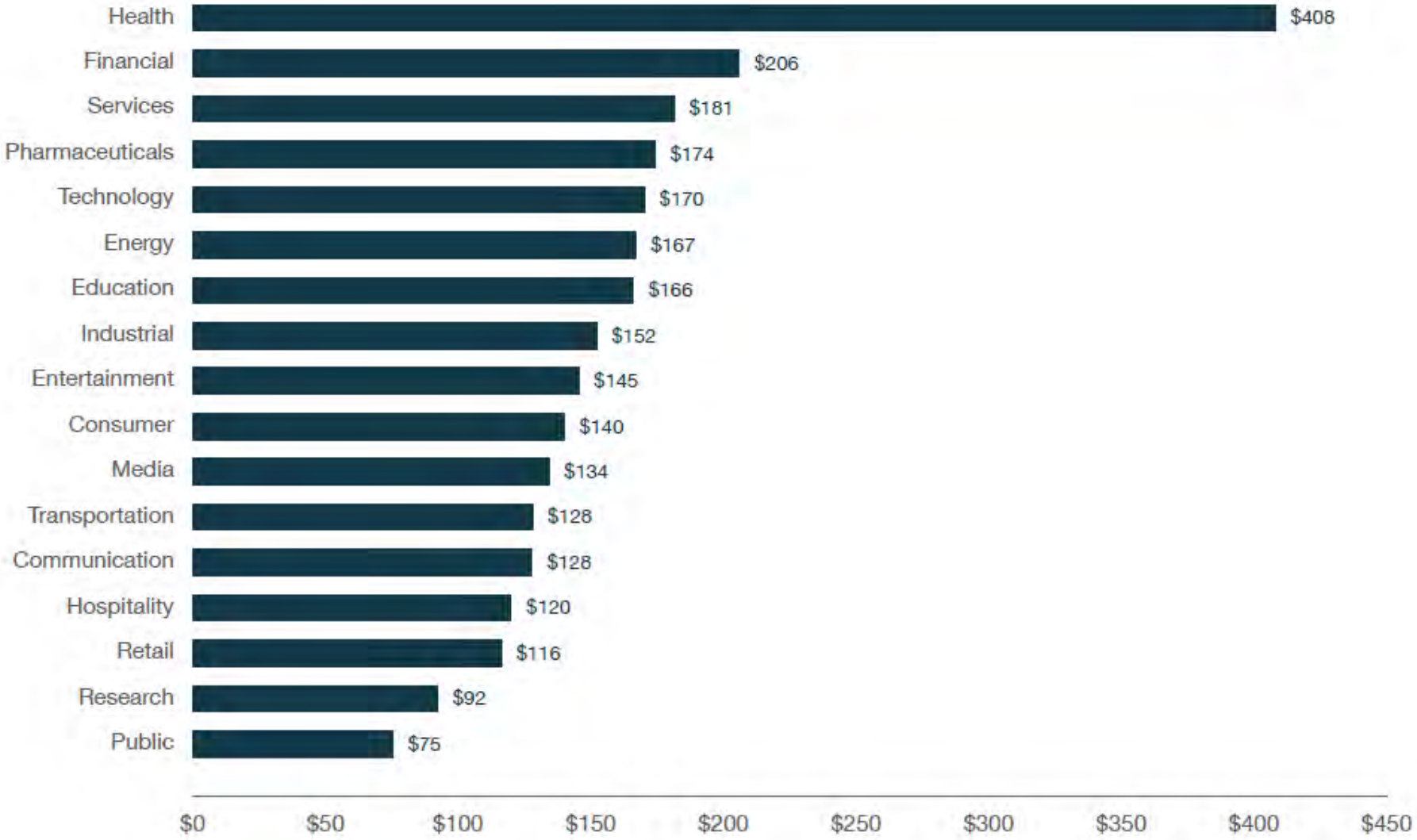
By Victim Loss			
Crime Type	**Loss**	**Crime Type**	**Loss**
BEC/EAC	$676,151,185	Misrepresentation	$14,580,907
Confidence Fraud/Romance	$211,382,989	Harassment/Threats of Violence	$12,569,185
Non-Payment/Non-Delivery	$141,110,441	Government Impersonation	$12,467,380
Investment	$96,844,144	Civil Matter	$5,766,550
Personal Data Breach	$77,134,865	IPR/Copyright and Counterfeit	$5,536,912
Identity Theft	$66,815,298	Malware/Scareware/ Virus	$5,003,434
Corporate Data Breach	$60,942,306	Ransomware	$2,344,365
Advanced Fee	$57,861,324	Denial of Service/TDoS	$1,466,195
Credit Card Fraud	$57,207,248	Charity	$1,405,460
Real Estate/Rental	$56,231,333	Health Care Related	$925,849
Overpayment	$53,450,830	Re-Shipping	$809,746
Employment	$38,883,616	Gambling	$598,853
Phishing/Vishing/Smishing/ Pharming	$29,703,421	Crimes Against Children	$46,411
Other	$23,853,704	Hacktivist	$20,147
Lottery/Sweepstakes	$16,835,001	Terrorism	$18,926
Extortion	$15,302,792	No Lead Value	$0
Tech Support	$14,810,080		
			Descriptors*
Social Media	$56,478,483	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.	
Virtual Currency	$58,391,810		

2018 Research (Ponemon Institute) Impact Statistics

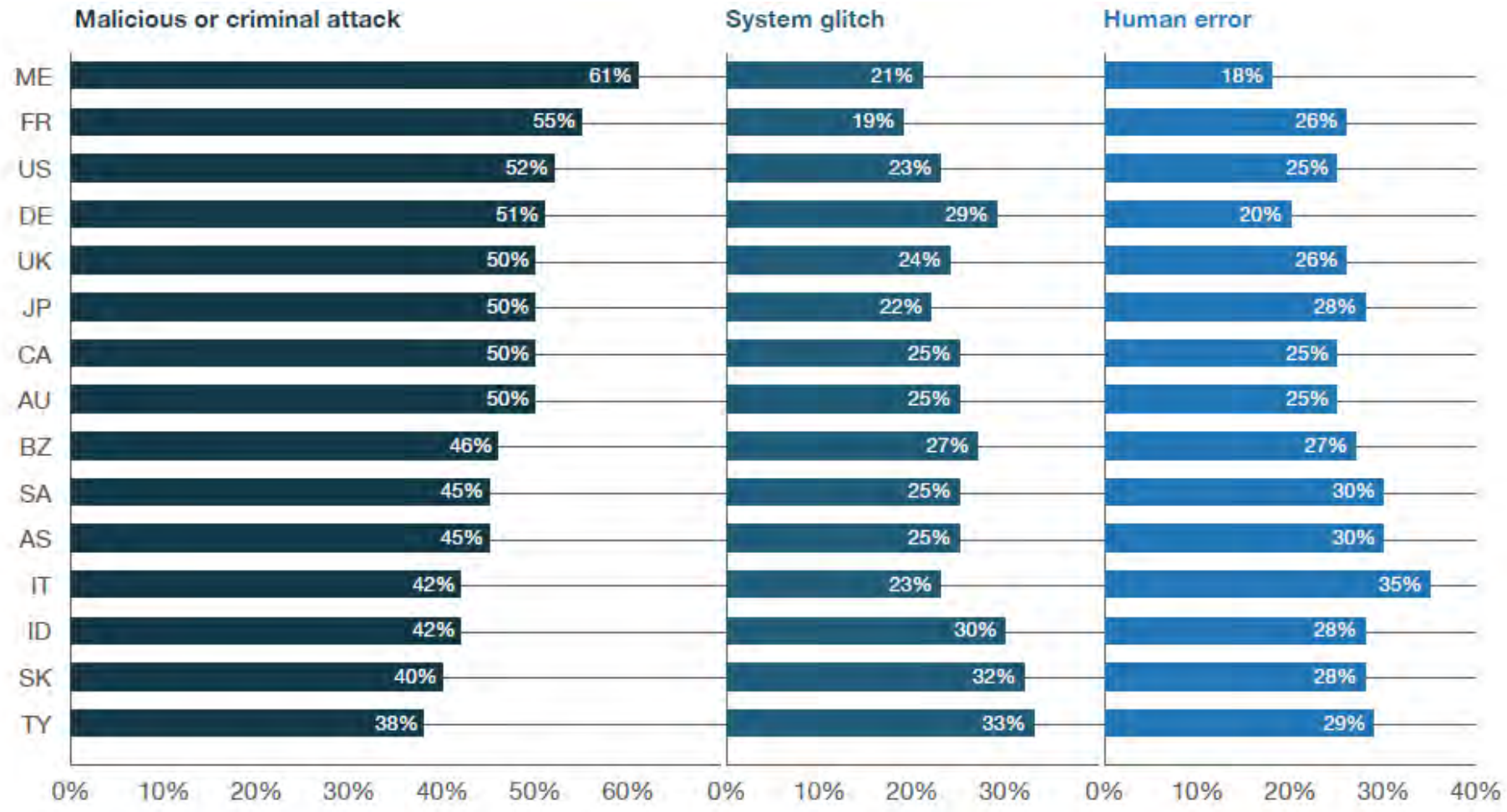
- 477 Companies in 15 Countries
- 197 (2018) vs 191 (2017) Days to Identify the Breach
- 69 (2018) vs 66 (2017) Days to contain the Breach
- Regulated industries of Financial Services, Healthcare, and Education are Targeted (higher value=higher risk)
- $148 (2018) vs $141(2017) Avg Cost per stolen record

Costs= Forensics fees, Lost Business Value, Lawsuits, Recovery fees

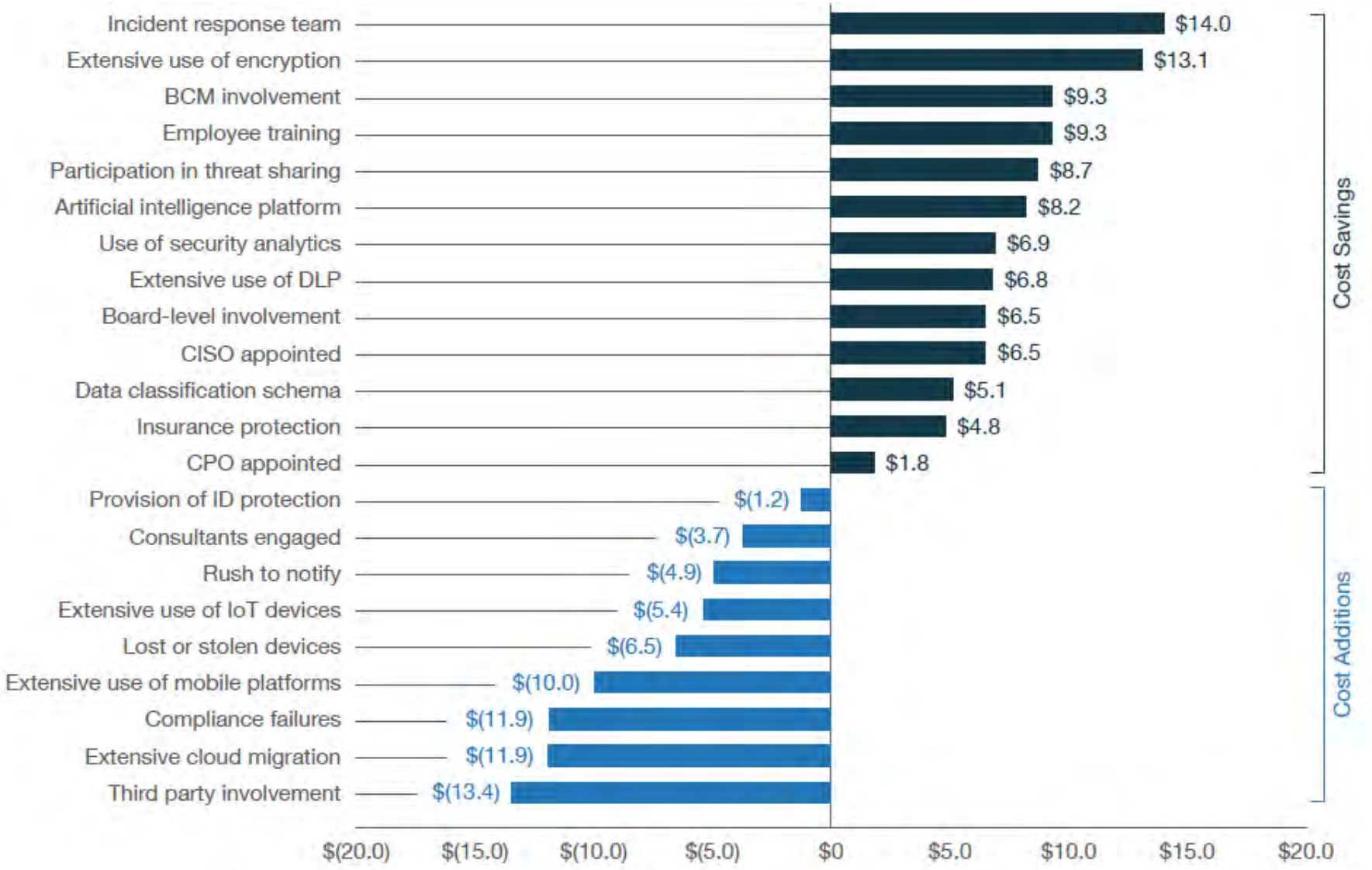
Data Breach Record Cost / Industry Segment



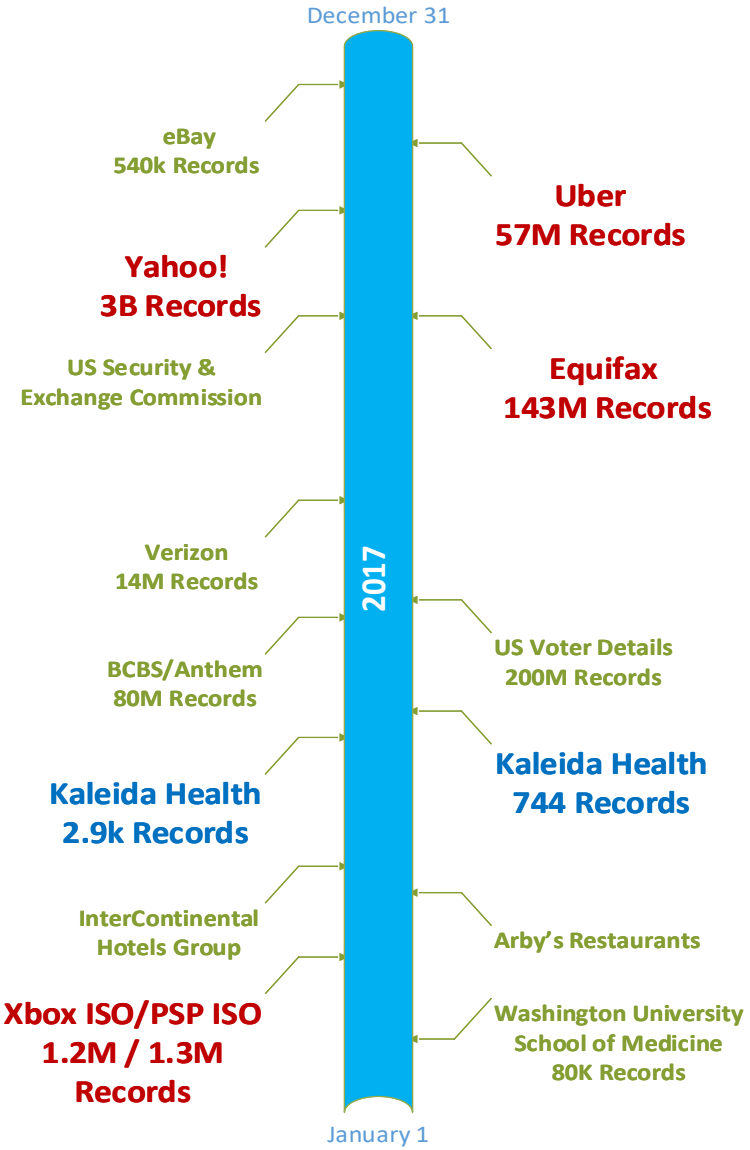
Data Breach Causes / Country & Region



Data Breach Capita Cost Impact Factors



Notable Data Breaches in 2017



Notable Data Breaches in 2018 so far

- Sacks, Lord & Taylor (Luxury Department Stores)
  - 5 Million Records – April 2018
- PumpUp (Fitness App.)
  - 6 Million Records – May 2018
- Sacramento Bee (Daily Newspaper)
  - 19.5 Million Records – June 2018
- TicketFly (Online Ticketing)
  - 27 Million Records – June 2018
- Panera Bread (Restaurant)
  - 37 Million Records – April 2018
- Facebook (Online Social Platform)
  - At least 87 Million Records – March 2018
- MyHeritage (Online genealogy platform)
  - 92 Million Records – June 2018
- Under Armour (Retail Store)
  - 150 Million Records – May 2018
- Exactics (Marketing/Data Aggregation Firm)
  - 340 Million records – June 2018
- Aadhaar
  - 1.1 Billion Records – January 2018

Discussion

- What is the one thing that **struck** you?
- Is **anyone** safe?
- Were you **surprised** by the facts?
- Where do you think the **highest risk** is?
- Any **real life** experiences to be shared?

How These Attacks Occur

- Socially Engineered Attacks
  - Hacking (Unauthorized Access)
  - Phishing (Trying to Obtain Unauthorized Access)
  - 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)
- 3rd Party Providers (IT Services, Cloud Provisioned)
- Unsecured Backup / Recovery Media
- A Lack of Cyber Threat Training and Awareness

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
- Protect Yourself from Phishing Scams (know how to spot them)
- Use Caution when Receiving Unexpected email
- Check that Web Forms are Secure (https://)

Protecting Ourselves and Reducing our Risks

- Exercise Caution when Using Wireless Networks / Charging Stations
- Limit the amount of Information you Provide about Yourself online
- 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

Discussion

- Where do you think you get the best ROI on tackling cybersecurity?
- Do you think an Enterprise Risk Assessment would help you and your organization to minimize the risk of a breach?
- Have you thought of having a dedicated cybersecurity team?
- You've had a security incident. Are you ready to deal with it?

Take-a-Ways & Questions

- Any Organization with PII/ PHI Carries Risk. Know your Profile.
- Cyber Aware Education is Important.
- The Multi-Layered Approach towards Protecting our Castles and Ourselves is Necessary.
- Skills and Technologies Exist to Help you.

Thank You

AAFCPAs

aafcpa.com