DRI2018
The Professional's Conference

February 11–14, 2018
Gaylord Opryland Resort and Convention Center, Nashville
#DRI2018

Cybersecurity: Data Breach Live – Future of Ransomware & Social Engineering

Ross Albert, CAMS, CFE
HUB International

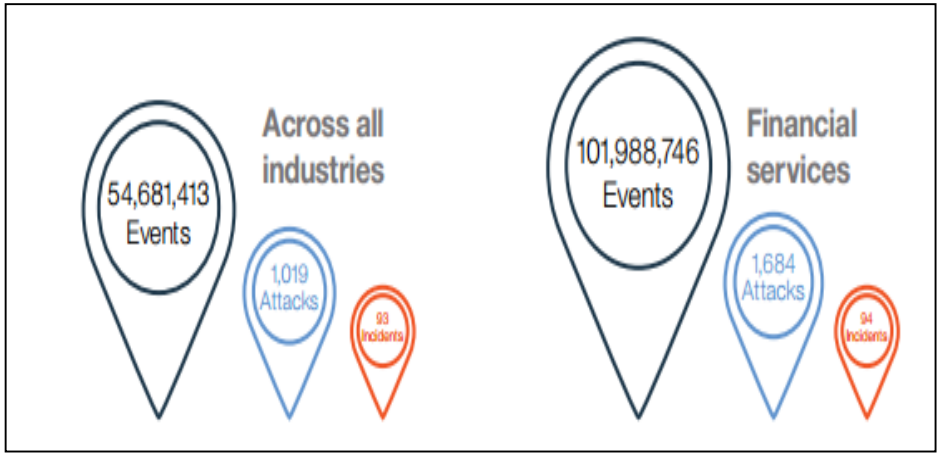
Agenda

1. Emergent Trends/Threats
2. Live Hack Demos
3. Prevention & Response

Trends & Threats

Cybercrime Trends

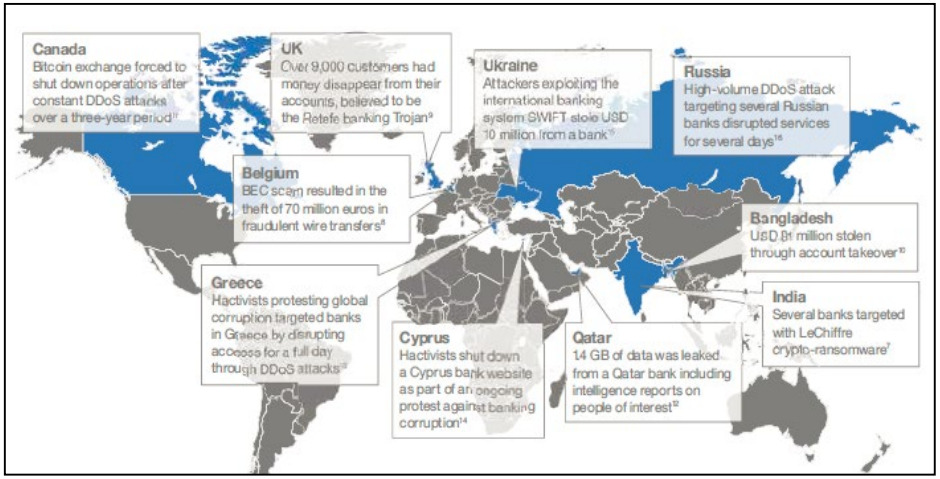
- Financial services was the most attacked sector in 2017
- Ransomware on the rise
  - 2 large scale global attacks in the past three months
- Social engineering continues to be primary method of attack
- Underground economy offers readily available market for stolen data



Source: IBM Security Trends 2017

Cybercrime – A Global Perspective

- Cybercrime knows no boundaries
- Complaints in every U.S. state and 70 countries
- Wire transfers made to 72 countries, majority in Asia

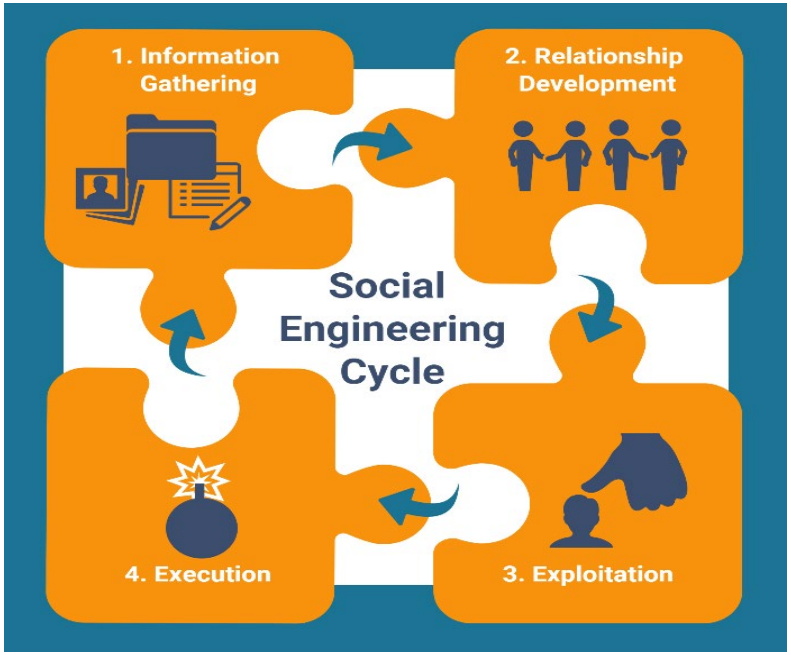


Source: IBM Security Trends 2017

Cyber Actors and Motivations

Social Engineering

1. Information gathering
   - Collecting information to identify attack vectors
2. Relationship Development
   - Develop rapport with target
3. Exploitation
   - Use information and relationships to infiltrate target
4. Execution
   - Accomplish ultimate goal



Business Email Compromise (BEC)

- Attempt to trick C-level executives into making large wire transfer payments
- Easier to scam out of large amounts
- Approximately $5 billion in losses between 2013-2016
- Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 103 countries
- Examples:
  - Business working with foreign supplier
  - Exec receives or initiates wire transfer
  - Business executive and attorney impersonation

Ransomware

- Form of digital blackmail
- Delivered in a number of different ways (phishing, internet download, remote access)
- Ransom demands – increase daily and threats to destroy data
- Average payment = $679 in 2016
- Growing tendency to pay ransom

Future of Ransomware

- Cyber criminals may threaten to publish data online to extort additional ransom from the victim
- Ransomware as a Service will likely increase number of attacks
- Ransomware attacks will likely expand to include targeting of Internet of Things (IoT) devices
- Social engineering will remain one of the easiest ways for a cybercriminal to gain access
- Moving beyond financial gain: ransomware for political/ideological motivations

Internet of Things (IoT)

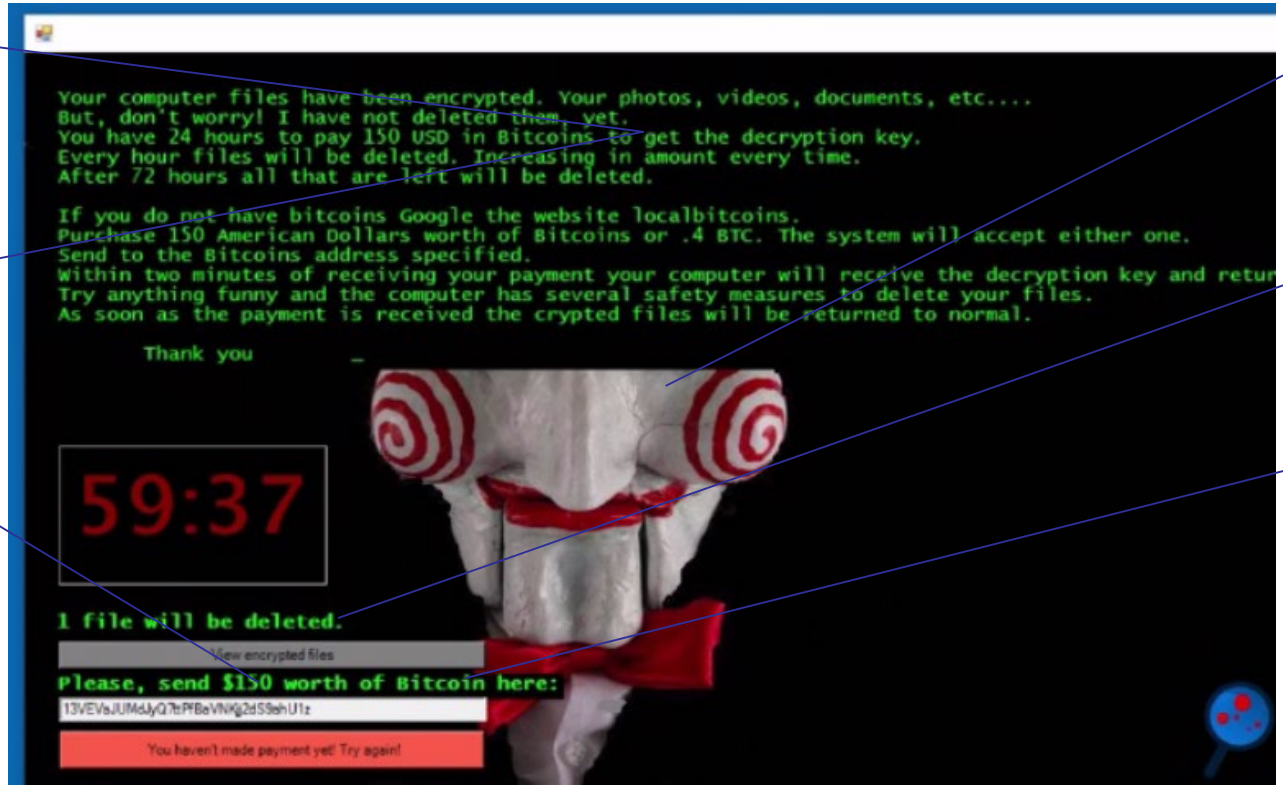
- Devices that are "smart" or connected to internet
- By 2020, more than 20 billion connected devices
- Challenges: devices are often rushed to market without property security

Ransomware – Key Considerations

Do you have backups?

Do you need the data?

To pay or not to pay?



What type of ransomware?

Decryption tool available?

Accepted payment type?

Live Hack Demos

Hacking Process

- Reconnaissance
- Scanning
- Exploitation
- Privilege Elevation
- Establish Persistence
- Move Laterally
- Extract Data
- Cover your Tracks

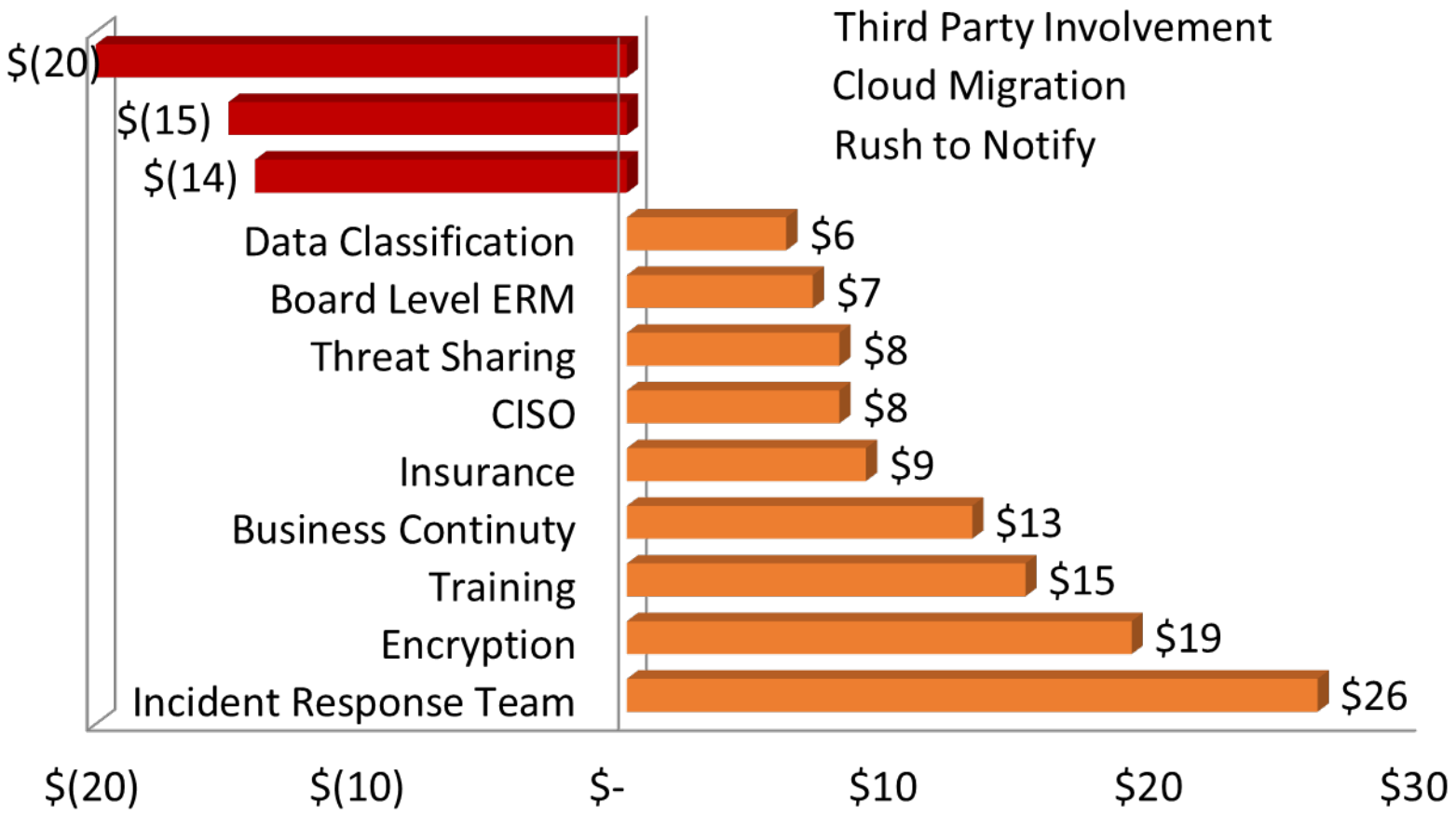
Algorithm, The Hacker Movie, 2014

Social Engineering – Client Side

- Spear Phishing
- Website Attack Vectors
- Infectious Media
- SMS Spoofing
- Wifi
- Vishing

Prevention & Response

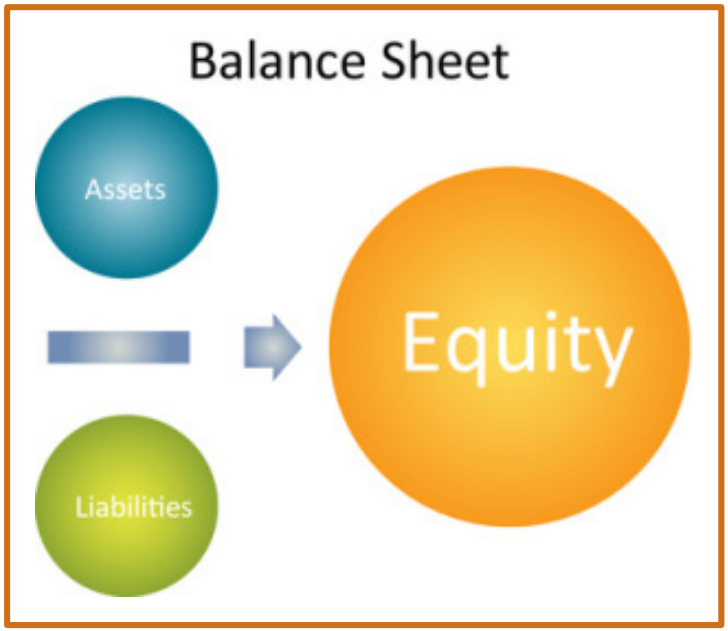
Response Differentiators



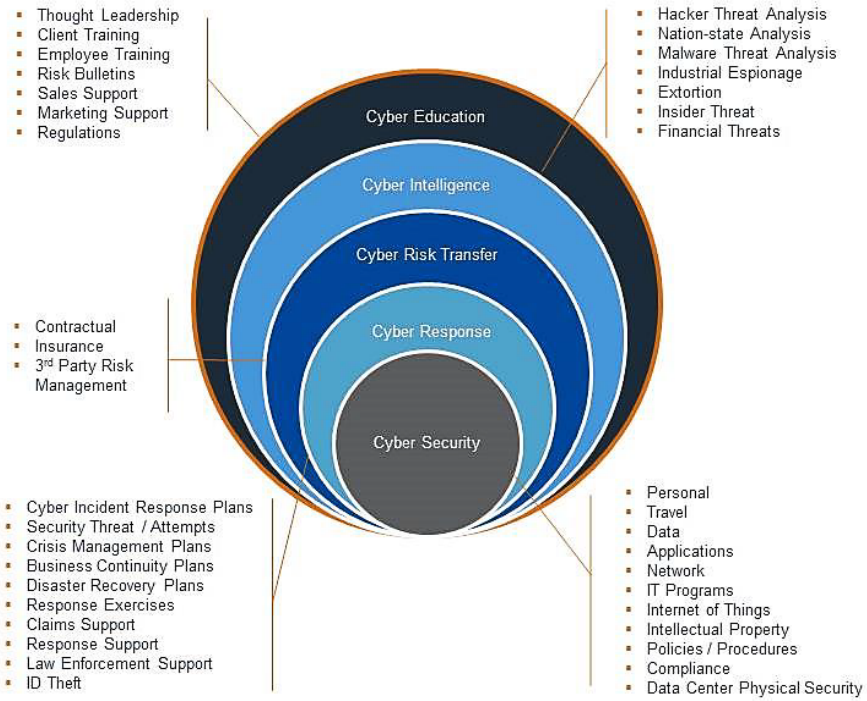
Source: Ponemon 2016 Cost of Data Breach Study

3 Step Approach – Prevent, Mitigate, Transfer

1. Prevent
   - Firewalls, anti-viral ware, encryption, software-patch management
   - Vet your vendors
2. Mitigate
   - Business Continuity/Disaster Planning & Testing
   - Incident Response Planning
3. Transfer
   - Insurance Coverage



Cyber Risk Services



Cyber Service Overview

- Approach risk treatments as an advocate
- Able to be utilized as part of an overall marketing strategy with the carrier community
- Conduct scenario based assessments, including financial risk calculations
- Assess current programs
- Develop plans, policies, procedures, programs
- Available to deliver bespoke services, as needed
- Deliver training and educational events demonstrating actual cyber threats for employee and enterprise protection
- Deliver response analysis and advice during large scale disruptions
- Actively respond to client cyber events such as theft, social engineering, malware, ransomware, rogue employees, and employee mistakes

Additional Resources

HUB Crisis Management
https://www.hubinternational.com/products/risk-services/crisis-management/

HUB Cyber Risk Management
https://www.hubinternational.com/business-insurance-insights/cyber-risk-solutions/

FBI Internet Crime Complaint Center (IC3)
https://www.ic3.gov/default.aspx

US-CERT (United States Computer Emergency Readiness Team)
https://www.us-cert.gov/

Thank You

Ross Albert
VP – Organizational Resilience
(o) 212-338-2228
Ross.albert@hubinternational.com