



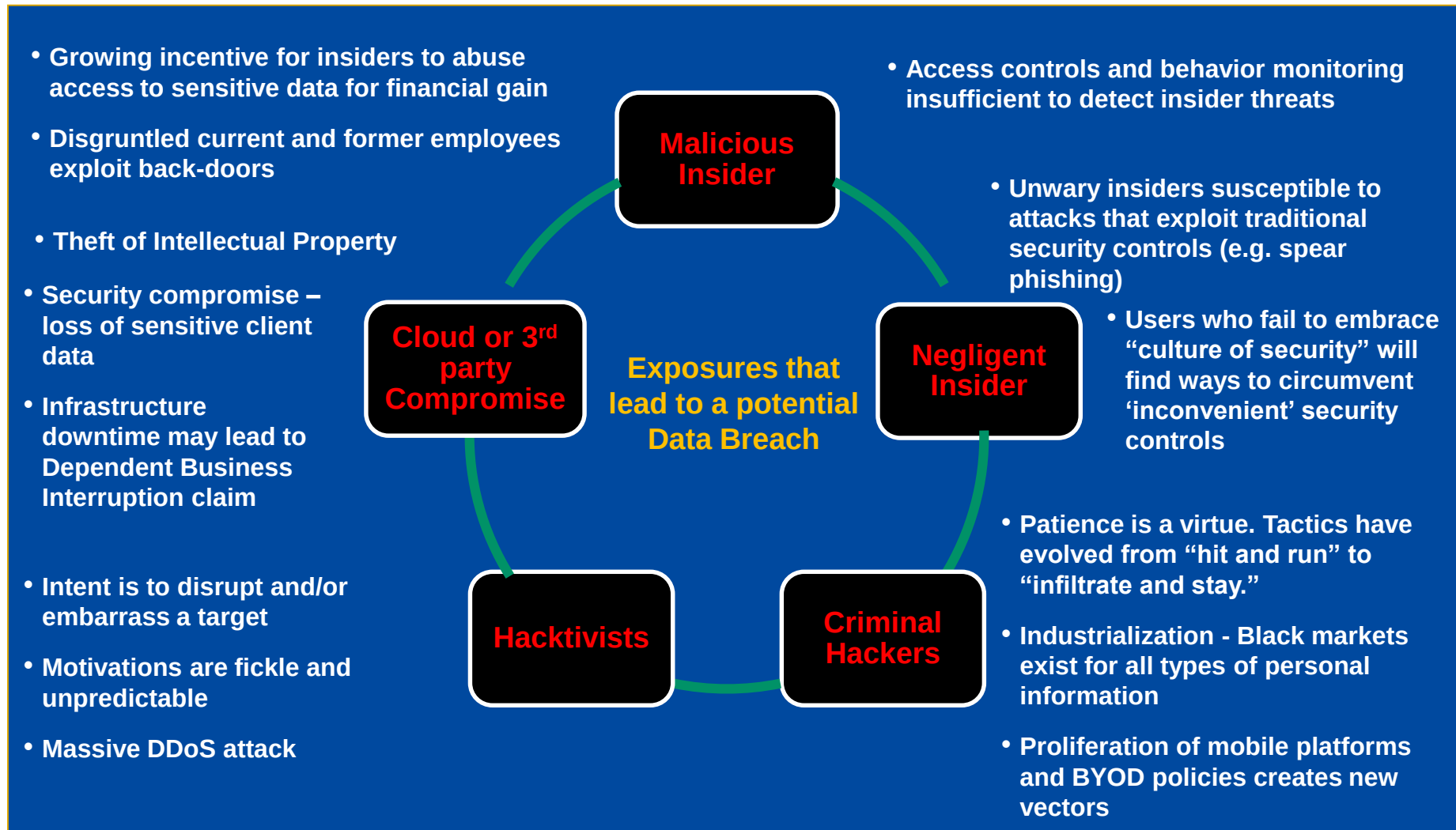
Cyber 101: A Brave New World - Mitigating Cyber Risk in Public Organizations

Dominic Keller, Vice President

FINEX Cyber E&O Team, Willis Towers Watson

November 2016

Threat Environment



Key Trends and Recent Developments

3,930

Number of prior year security incidents per Risk Based Security 2015 Data Breach trends Report

41%

The percentage of cyber claims related to rogue employee and hacking per ACE/Chubb USA 2015 data.

34%

The percentage of cyber incidents occurring from a Denial of Service per Verizon 2016 Data Breach Investigation Report

237

Million personal records breached in 2015 alone

205

Median # of days from first evidence of compromise and discovery of compromise

69%

The percentage of compromises detected by an external entity

24

Zero Day Attacks each year according to Symantec 2016 (295 days average time to identify and mitigate)

Evolving Threats

Business interruption/Cryptolocker type attacks

- 2015 – number of cryptolocker attacks doubled and forecast to increase in future*
- Cyber extortion/cryptolocker examples:
 - Hollywood Presbyterian Medical Center, March 2016 – \$17,000 paid. Often low amount sought, aim is to simply have extortion paid
 - Costs from these attacks
 - Payment of extortion demand
 - Payment of forensic expenses to isolate the malware and remove it from system
 - Payment to 3rd parties whose information may have been compromised due to the breach

Risks are constantly evolving

- 24 Zero day attacks annually (295 days to identify and respond)*
- 50-60% of cyber attacks against small and medium sized companies*

*(Symantec Survey, 2016)

People and social engineering threats

Criminal attackers are increasingly relying on psychology and personal motivation. This new style of attack is very difficult to detect and defend against.

February 25, 2016: Phishing Scam Leaks Employee Information at NJ Facility

Healthcare system in New Jersey announced that more than 5,000 employees at some of its facilities may be at the risk of identity theft following a phishing scam that potentially compromised their information.

Symantec 2015 Internet Security Threat Report (ISTR)

- Five out of six large (2,500 + employees) companies were targeted with spear-phishing attacks during 2014 – a 40% increase over the previous year.
- Small and medium-sized businesses also saw an uptick, with attacks increasing 26% and 30%, respectively

Ponemon Report: The Cost of Phishing & Value of Employees

- Businesses that roll out training programs see improvements of between 26 and 99% in their phishing email click rates, with an average improvement of 64%.

Now and Into the Future

- **Familiar Mediums**
 - SQL injections; spear phishing; malware, spyware & ransomware (“CryptoLocker”); denial of service attacks; web site defacing
 - Loosely formed groups who hacking together (e.g., Anonymous, Lulzsec)
 - State actors (China, Iran, US, Israel, Russia)/ APT’s
- **Newer Culprits and Methods**
 - Home grown terrorists
 - Asymmetrical attacks
 - Disgruntled employees
- **Newer Information Targeted**
 - Social Media (for impersonation purposes)
 - IP/Trade Secrets
 - Targeted Individuals
- **Newer Targets**
 - Cars
 - Smartphones
 - Medical devices
 - Industrial Control Systems
- **Newer Motives**
 - Political, ideological, personal, war/terrorism, revenge
 - “Hacktivism”
 - Public embarrassment
 - Corporate Espionage

Identify Key Exposures

Identify the Network Security and Privacy Risks to the Organization

- Privacy breaches – release of confidential information
- Network interruption/system outage risks
- Cyber extortion/Ransomware risks
- Vendor management/vendor breach risks
- Data loss through property damage

Develop an Action Plan

Build a Detailed Overview of the Enterprise's Risk

Quantify the particular enterprise risk to the organization, viewed as a financial and operational risk:

- How many records are held/collected by the organization and where are they held - what are the reporting requirements in the event of these records being disclosed?
- How reliant is the organization on 3rd party service providers? What contractual obligations/indemnifications are in place to protect the organization as comprehensively as possible?
- What, and how much of the organization's operations are reliant on a functioning network?
 - What is the financial loss from a network event?
 - Based on a 50% outage, what is the effect? 100%?
 - How long is the network outage likely to occur?
 - How are backups stored and activated?
- What steps have been taken to proactively respond to cyber events?
 - Incident response, business continuity plans
 - Table Top Exercises (Cross Functional approach is key)
 - Leadership engagement in cyber risk

Risk Transfer

“Cyber-insurance cannot protect your institutions from a cyber-incident any more than flood insurance can save your house from a storm surge or D&O insurance can prevent a lawsuit, but what cyber-risk insurance can do is provide some measure of financial support in case of a data breach or cyber-incident. And, significantly, cyber-risk insurance and the associated underwriting processes can also help bolster your other cybersecurity controls.”

*Sarah Bloom Raskin, Deputy Secretary, U.S. Department of the Treasury
The Texas Bankers' Association Executive Leadership Cybersecurity
Conference
December 3, 2014*

Cyber Liability Insurance – Main Coverage Parts

Loss Mitigation Coverage (Breach Response/Crisis Management Costs)

- Legal Data Breach Coach
- Forensics Investigation Expenses
- Notification of Affected Individuals and Call Center Services
- Public Relations/Crisis Communications Costs
- Credit Monitoring/Credit-Fraud Remediation Services

First-Party Coverage

- Network Extortion - Covers extortion payments and additional expenses arising out of a criminal threat to release sensitive information or bring down a network unless extortion amount is paid;
- Business Interruption - Indemnification for loss of income and extra expenses incurred from a network security breach that causes financial loss to a company from an inability to carry out normal business activities;
- Digital Asset Loss - Indemnification for costs to recreate, rebuild or recollect digital information assets that were directly damaged as a result of a network security breach affecting a company's network;
- Regulatory Fines/Penalties – Covers financial penalties imposed by regulators, and associated defense costs, from alleged or actual failure to comply with state or federal laws relating to privacy or obligations to protect sensitive information;
- PCI DSS Violation Coverage - Covers monetary penalties imposed by Payment Card Networks resulting from the failure to comply with PCI DSS requirements.

Cyber Liability Insurance – Main Coverage Parts

Third-Party (Liability) Coverage

- Network Security Liability - Covers legal defense costs and damages payable to 3rd party third-party claims alleging failure to protect against transmission of malicious code, denial of service attacks and unauthorized access and/or use of computer systems;
- Privacy Liability - Covers legal defense costs and damages payable to third-party claims alleging unauthorized use or disclosure of non-public personally identifiable information (PII) and confidential corporate information;
- Internet Media Liability - Affords legal defense costs and indemnity for third-party claims alleging wrongful acts (i.e. defamation, disparagement, copyright/trademark infringement) in the dissemination of internet content and media.

Connecting the dots: cyber risk management for the future

A multifaceted approach

- Ensure enterprise-wide governance is in place
- Assume hackers are already inside
- **Invest in making your whole workforce cyber-smart**
- Consider technology one of several lines of defense
- **Insure for cyber threats you can't mitigate**
- Allocate enough capital to the right cyber defenses – protect your crown jewels