

**Emerging Cyber Threats:
Risk Mitigation Strategies**

Sean B. Hoar, Partner & Chair
Data Privacy & Cybersecurity Team
Lewis Brisbois Bisgaard & Smith LLP

CIS Annual Conference
February 27, 2020

LewisBrisbois.com

1

**Social Engineering –
You are a target**




- Email Account Compromises
 - Credential harvesting
 - Spear phishing
- Data Monetization
 - Sensitive data sales
 - Wire transfer redirects
 - Direct deposit redirects
 - W-2 image exploits
- Prevention
 - Two-factor authentication
 - External email flagging
 - Employee training / testing
 - Spam filtering

2

2

**Encryption Attacks -
Your organization is a target**




- Sophisticated use of malware
 - Preceding attacks with credential stealing Trojans
 - Back up data encrypted
 - Increasing ransom demands
- Ransomware Ruse
- Prevention
 - RDP ports
 - Endpoint monitoring
 - Employee training / testing
 - Patch management

3

3

Network Intrusions – Data and property are targets 

- Payment Card Data
 - E-Commerce site hacks
 - POS systems
- Malicious Network Use
 - BotNet launching sites
 - Stolen records storage
 - Cryptojacking
- Intellectual Property Theft



4

4

Create a human firewall 

- You cannot mitigate all technological risk with technology ... the human user is essential
- The human user of technology – the employee - is essential to protecting network resources
- You may be critical to establishing a culture of security
 - Safe environment in which to communicate
 - Effective training programs
 - Efficient reporting protocols
 - Create a human firewall

5

5

The dark web ... criminal marketplace 

- **A sophisticated cyber underground where criminals, working in syndicates or individually, sell their services including:**
 - **Online Forums:** Criminals operate through a variety of online forums used to buy and/or sell products and services.
 - **Bullet Proof Hosting:** Criminals provide a vital infrastructure (including by operating dedicated servers and domains) to host malicious websites, malware, botnet command and control stations, VPNs and proxies.
 - **Data Monetization:** Criminals utilize the dark web for sensitive data sales.
 - **Coding Services:** Criminals customize malware, tailoring it to impact specific targets and improve its ability to bypass anti-fraud mechanisms.
 - **Anti-Virus Checking Services:** Criminals run malware through numerous anti-virus products to maximize infection rates.
 - **Exploit Kits:** Criminals utilize a variety of tools to identify /exploit vulnerabilities on victim systems.
 - **Anonymization:** Criminals employ means to communicate securely and to receive payment through untraceable systems (i.e. virtual currencies).

6

6

The regulatory environment – A reason for a sense of urgency



- Self-funded operations budgets - funded by assessments ...
- State Regulations
 - 50 state data breach notification statutes (plus Washington D.C., Guam, Puerto Rico, and Virgin Islands) – All cover electronic, 10 also cover paper;
 - Require notification of consumers regarding breaches of unencrypted personal information;
 - Notification obligation determined by residential location of consumer, not location of business
 - Personal information generally defined as first name or initial and last name, combined with one or more of the following data sets:
 - All states include SSN, DL or State ID Card Number, or financial account with means to access the account;
 - 20 add medical information; 16 add health insurance; 16 add online credentials; 14 add biometric information; etc.



7

The regulatory environment – A reason for a sense of urgency




- Self-funded operations budgets - funded by assessments ...
- State Regulations
 - Timing of notification: 40 require "most expedient time possible"
 - 17 also have outer time limit (2 at 30 days; 11 at 45 days; 3 at 60 days; 1 at 90 days;
 - Notice content requirements: 19 have specific notice content requirements;
 - Regulatory notification: 32 require notification of state regulatory officials;
- Information security standards
- Federal Regulations
 - HIPAA – Privacy Rule, Security Rule, Breach Notification Rule;
 - FTC Act;
 - Securities Exchange Act,
- PCI DSS industry regulations




8

Standard of care for information security



Threshold for "Reasonable" Security




Excerpt from California Data Breach Report, Feb. 2016

The CIS Critical Security Controls for Effective Cyber Defense

CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	Email and Web Browser Protection
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocols, and Services
CSC 10	Data Recovery Capability
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account monitoring and Control
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

9

The financial implications – Another reason for urgency 

- **First-party costs:**
 - Data loss; software loss; hardware loss;
 - Income loss; business interruption costs; restoration costs;
 - Cyber extortion; other crime loss.
- **Third-party costs:**
 - Media liability (copyright and trademark infringement); privacy liability for breach of privacy; bodily injury;
 - Defensive litigation: class actions; derivative actions; and regulatory actions.
- **Remediation costs:**
 - Legal services; forensics services; crisis management services; consumer and regulatory notification – The actual hard copy costs; call center services; credit monitoring and identity theft protection services.
- **Fines and penalties:**
 - Expenses of regulatory investigations; civil judgments; fines and penalties levied by regulatory authorities; and fines and penalties for payment card industry compliance violations.

10

10

The insurance implications – Economic risk mitigation 

- Incident response planning should include a review of cyber insurance needs and coverage;
- Cyber insurance review should include consideration of:
 - Crime coverage;
 - Fraudulent funds transfer coverage;
 - Data restoration; and
 - Business interruption coverage.
- Sublimits should be sufficient for substantial digital forensics and consumer remediation; and
- Aggregate limits should sufficient for catastrophic incident.

11


11

Most troubling trends 

- **Targets:** Entities in all locations, all business sectors, all sizes, including governmental entities.
 - Especially accounting & human resources
- **Sophistication:** Attacks are increasingly sophisticated.
 - Extortion: Attacker due diligence / Increasing ransom demands
 - Social engineering: Attacker "spear phishing"
- **Frequency:** Entities are targeted daily by social engineering and brute force attacks.
- **Success:** Increasingly successful encryption attacks with limited ability to negotiate ransom demand.
- **Regulatory Action:** Increasingly aggressive state regulatory agencies.

12

12

Lessons learned 

- **Human resources personnel are targets**
 - Do not respond to any email messages requesting sensitive information, especially W-2 information
 - Always confirm request for sensitive information in-person, or by telephone with known number
 - Personally authenticate direct deposit change requests
 - Be aware of any changes in “your baseline” – i.e. the number of email messages or the type of email traffic normally received
 - Forward any suspicious messages to IT security
 - Don’t be embarrassed to approach superiors or IT security if you have questions

13

Lessons learned 


- **Financial personnel are targets**
 - Financial officers or controllers will be targets of attackers to monetize contents of accounts and to redirect wire transfers
 - Accounts payable personnel will be targets of compromised accounts to redirect outbound wire transfers to malicious accounts
 - Accounts receivable personnel will be targets of attackers to compromise their accounts and redirect inbound wire transfers to malicious accounts
 - Be aware of any changes in “your baseline” and forward any suspicious messages to IT security

14

Lessons learned 

- **If a ransomware incident occurs:**
 - Call your insurance broker/carrier immediately;
 - Use appropriately skilled and resourced forensics firm:
 - Do not initiate contact with attacker from victim domain;
 - Do not disclose information about victim infrastructure;
 - Do not pay ransom without exhausting other resources for decryption keys;
 - Do not pay ransom directly – use vetted third party – and ensure Dept. of Treasury laws are followed;
 - Do not wipe devices without obtaining forensic image;
 - Deploy endpoint monitoring before enabling operations to ensure vulnerabilities are identified and secured; and
 - Do not make unnecessary public statements.


15

Lessons learned 

- If an email account compromise or system intrusion occurs:
 - Call insurance broker/carrier immediately;
 - Take appropriate security measures:
 - Do not use compromised email account without reviewing and clearing rules, changing passwords, and enabling dual factor authentication;
 - Use appropriately skilled forensics firm;
 - Do not wipe devices without obtaining forensic image;
 - Extend event logging to retain relevant evidence; and
 - Do not make unnecessary public statements.

16

16

Lessons learned 

- If you discover a fraudulent wire transfer:
 - Immediately initiate "financial fraud kill chain":
 - Report it immediately to originating bank;
 - Report it immediately to local FBI;
 - File written report immediately at IC3.gov;
 - Action must be taken within 72 hours of actual monetary transfer;
 - Continue to follow up with bank after initial report is filed to ensure they have attempted to stop payment.

17


17



Lessons learned 


- It is essential that all businesses develop and implement information security programs with proactive measures to mitigate the risk of attack:
 - Security control assessments;
 - Enhanced endpoint monitoring;
 - Enhanced intrusion detection systems;
 - Incident response planning;
 - Table top exercises;
 - Employee training;
 - Detailed policies and procedures that follow best practices and provide functional implementation guidance; and
 - Third party contract review and management to limit liability.

18

18


Lewis Brisbois resources 

- 24/7 telephonic & email hotline:
 - 844.312.3961
 - breachresponse@lewisbrisbois.com
- Digital Insights blog; 
- Interactive maps:
 - data breach notification statute maps; 
 - information security standards;
- Data Privacy & Cybersecurity Handbook; and
- “Lewis Brisbois Cyber Practice” App:
 - Available in App Store.




19

19

Questions? 

Sean Hoar, CISSP, GISP, CIPP/US, is a Partner and Chair of Lewis Brisbois' national Data Privacy & Cybersecurity Practice. Sean has extensive experience managing responses to digital crises, and the Lewis Brisbois Rapid Response Team has managed thousands of data security incidents. Sean served as the lead cyber attorney for the U.S. Attorney's Office in Oregon, and worked closely with the Computer Crime & Intellectual Property Section in Washington D.C. He holds the Certified Information Systems Security Professional (CISSP), the Global Information Security Professional (GISP), and the Certified Information Privacy Professional/United States (CIPP/US) credentials. He taught courses in cybercrime at the University of Oregon School of Law and the Lewis & Clark Law School, and he serves as the Executive Director of the Financial Crimes & Digital Evidence Foundation.



Sean B. Hoar
 Partner, CISSP, CIPP/US
 Lewis Brisbois Bisgaard & Smith LLP
Sean.Hoar@lewisbrisbois.com
 971.712.2795

20

20