AMERICAN FRATERNAL ALLIANCE

Managing Cybersecurity Risk

Thursday, November 9, 2017
11:00 a.m. Central

Please Stand By…

STINSON LEONARD STREET

AMERICAN FRATERNAL ALLIANCE

Managing Cybersecurity Risk

American Fraternal Alliance Webinar
November 19, 2017

Todd Martin

David Axtell

Stinson Leonard Street LLP

STINSON LEONARD STREET

Agenda

- Current cybersecurity environment and new threats
- Developments cybersecurity law
- Key elements of an effective cybersecurity program
- Mitigating liability and harm in the event of a breach
- Cyber liability insurance issues

STINSON LEONARD STREET

Current Cybersecurity Environment and New Threats

STINSON LEONARD STREET

Breaches Over Time

- January 1, 2005 – November 1, 2017*
  - Number of Breaches: 8,037
  - Number of Records Exposed: 1,055,156,161
- Definition for above: Name + Social Security Number, DL Number, Medical Record or Financial Record (credit/debit included) is potentially at risk (this is fairly consistent with state data breach laws)

*All data from Identity Theft Resource Center, http://www.idtheftcenter.org/data-breaches.html

STINSON LEONARD STREET

Comparison of 2005 to 2016

Entity	2005	2016
Business	25	495
Educational	75	98
Military/Government	21	72
Health/Medical	16	374
Banking/Credit/Financial	20	52

STINSON LEONARD STREET

How Did It Happen?

Category	2007	2016
Insider Theft	27	77
Hacking/Skimming/Phishing	63	607
Data on the Move	123	53
Accidental Web/Internet Exposure	90	101
Subcontractor/3rd Party/Business Associate	52	70
Employee Error/Negligence/Improper Disposal/Lost		95
Physical Theft		69

STINSON LEONARD STREET

What Type of Data Is Exposed?

- Roughly half involve Social Security Numbers
- 10-20% Involve Financial Account Numbers

STINSON LEONARD STREET

2017 Numbers as of Nov. 1

- Total Breaches: 1,140
- Records Exposed: 171,638,592
- Equifax Skews the data heavily (145,500,000)
- These numbers are gathered from numerous sources, but are almost certainly LOW

STINSON LEONARD STREET

Sources of Threats (GAO Threat Table)

- National Governments
- Terrorists
- Industrial Spies and Organized Crime Groups
- Hacktivists
- Hackers
- GAO Threat Table (catch all, that lists Bot-network operators, criminal groups, foreign intelligence services, hackers, insiders, phishers, spammers, spyware/malware authors, and terrorists)

STINSON LEONARD STREET

A Few Common Types of Social Engineering Intrusions

- Phishing – tricking victims into sharing sensitive information
- Spear-Phishing – tricking a victim into thinking the information request is coming from a specific person the victim knows (CEO, CFO, etc.)
- Pretexting – intruder builds trust over time with victim, often through a form of spear-phishing

STINSON LEONARD STREET

Some Statistics

- 64% of Americans willing to pay a ransom if victim to rasomware; Average demand = $1,077/victim; WannaCry and Petya notable
- Organizations with 251-500 employees had a malware rate of 1 out of every 202 e-mails (1/273 for smaller organizations)
- 1/2,644 e-mails were phishing
- Approximately 50 million malware variants

Source: https://www.symantec.com/security-center/threat-report

STINSON LEONARD STREET

Developments in Cybersecurity Law

STINSON LEONARD STREET

Current Applicable Law for Fraternals

- GLB
- HIPAA
- State Laws

STINSON LEONARD STREET

New Environment for Cybersecurity Regulation

- Broader focus than just privacy and security
- Three Key Elements
  - Privacy/ Security
  - Integrity
  - Access

STINSON LEONARD STREET

New York Cybersecurity Regulation

- Applies To Individuals and Entities Licensed to Do Business in NY (would include fraternals and fraternal agents if licensed in NY)
- Covered entities required to maintain cybersecurity program designed to protect information systems:
  - Confidentiality
  - Integrity
  - Availability

STINSON LEONARD STREET

New York Cybersecurity Regulation

- Cybersecurity Program based on Risk Assessment
  - Identify and assess internal and external risks
  - Use defensive infrastructure and implementation of policies and procedures to protect
  - Detect cybersecurity events
  - Respond to identified or detected cybersecurity events
  - Recover from cybersecurity event
  - Reporting to Superintendent

STINSON LEONARD STREET

New York Cybersecurity Regulation

- Other requirements
  - Written policies and procedures
  - Chief information security officer
  - Penetration testing and vulnerability assessments
  - Audit trail
  - Access privileges
  - Application security
  - Risk assessment
  - Qualified personnel
  - Third party compliance
  - Multi-factor authentication
  - Data retention/ disposal
  - Testing/ monitoring
  - Encryption
  - Written incident response plan

STINSON LEONARD STREET

New York Cybersecurity Regulation

Key Dates:

- August 28, 2017 - covered entities required to comply
- Feb. 15, 2018 - first certification
- March 1, 2018 – 1 year transitional period ends – additional requirements apply
- March 1, 2019 – 2 year transitional period ends – full compliance required

http://www.dfs.ny.gov/about/cybersecurity.htm

STINSON LEONARD STREET

NAIC Cybersecurity Model Law

- Similar to NY Regulation
- Applies to individual or organization required to be licensed under the insurance laws of the state
- Required to develop information security program in compliance with requirements
  - Protect security and confidentiality
  - Protect against threats to security or integrity
  - Protect against unauthorized access or use and minimize harm to consumer
  - Define schedule for retention and destruction

STINSON LEONARD STREET

NAIC Cybersecurity Model Law

- Risk assessment
- Risk management
- Board oversight
- Service provider oversight
- Program adjustments
- Incident response plan
- Commissioner certification

STINSON LEONARD STREET

NAIC Cybersecurity Model Law

Security Incident Response

- Investigation
- Reporting
  - To the commissioner
  - To consumers

STINSON LEONARD STREET

Key Elements of Effective Cybersecurity Program

- Governance oversight
- Broad scope – including service providers
- Risk assessment and monitoring
- Incident response planning
- Reporting & compliance
- Insurance

STINSON LEONARD STREET

Mitigating Steps

- Identify leak and plug it
- Contact counsel for privilege protection
- Limit what you put in writing outside of attorneys
- Identify information compromised
- Identify individuals impacted by at least names, addresses, information compromised
- Hire vendors to investigate and plug leak
- Isolate and preserve data compromised and identify timeline of incident

STINSON LEONARD STREET

Mitigating Steps

- Change security passwords and protocols if needed
- Start the clock/determine when it started/discovery timeline
- Review credit card and other contractual obligations
  - Often require immediate notification
  - May have audit and monitoring rights
  - May have fines or other significant impacts
- Review insurance and tender claim as soon as possible/work with insurer regarding vendors

STINSON LEONARD STREET

Considerations Regarding Insurance

- Coverage Limits
  - Forensic Consultants
  - Attorneys
  - Breach Notification Vendors
  - PR Vendors
  - Claims (relatively rare)
- Generally Excluded: New Software, Systems, Code Re-writes, and Improvements
- Vendor pre-qualification and choice

STINSON LEONARD STREET

Todd Martin
612.335.1409
todd.martin@stinson.com

David Axtell
612.335.7247
david.axtell@stinson.com

AMERICAN
FRATERNAL
ALLIANCE

Thank You!

Please stand by as we launch a brief survey…