Cybersecurity Workshop

February 10, 2015

E. Andrew Keeney, Esq.
Kaufman & Canoles, P.C.

The Credit Union League of Connecticut

KAUFMAN & CANOLES
attorneys at law

E. Andrew Keeney, Esq.

Kaufman & Canoles, P.C.

150 West Main Street, Suite 2100

Norfolk, VA 23510

(757) 624-3153

eakeeney@kaufcan.com

http://www.kaufmanandcanoles.com/movies/credit-unions.html

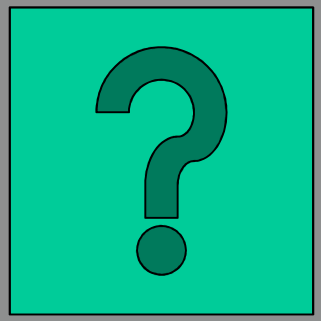
Overview and Agenda

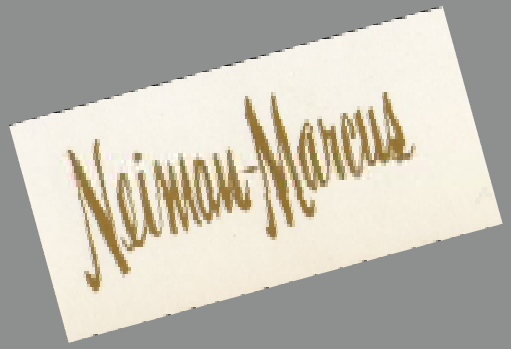
- Value
  - What electronically stored data has value to thieves?
  - Why is cybersecurity critically important to credit unions?
- Breaches
  - External vs. Internal Threats
  - Hackers/Employee error/Rogue Employee

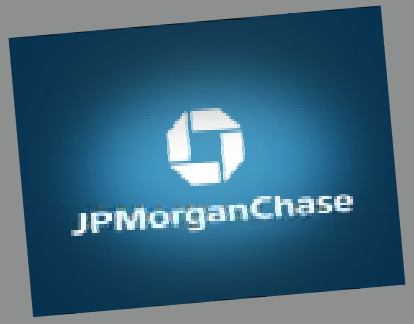
Overview and Agenda – continued

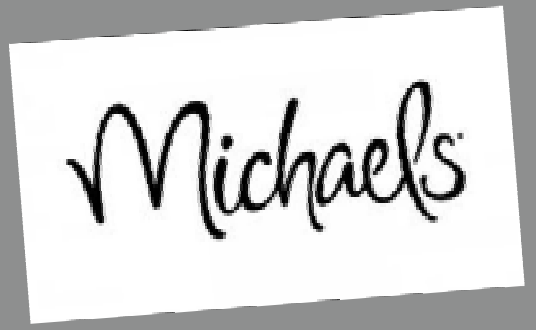
- Responses
- Prevention
- Insurance
- Laws and regulations
- Key takeaways/Best practices

Horror Stories









Data Security

Data & Cybersecurity: the practice of protecting data and systems from unwanted use.

Data breach: security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

Why only a general awareness?

- Complacency seems to still be the norm.
  - There is a view that cybersecurity measures do not add to the bottom line; rather, it is a cost.
  - There is a dearth in knowledge among management-level individuals about actual, current risks.
  - There is a general misunderstanding of specific risks that are known.
  - Belief abounds that “it won’t happen to our business.”

"We're in a day when a person can commit about 15,000 bank robberies sitting in their basement."

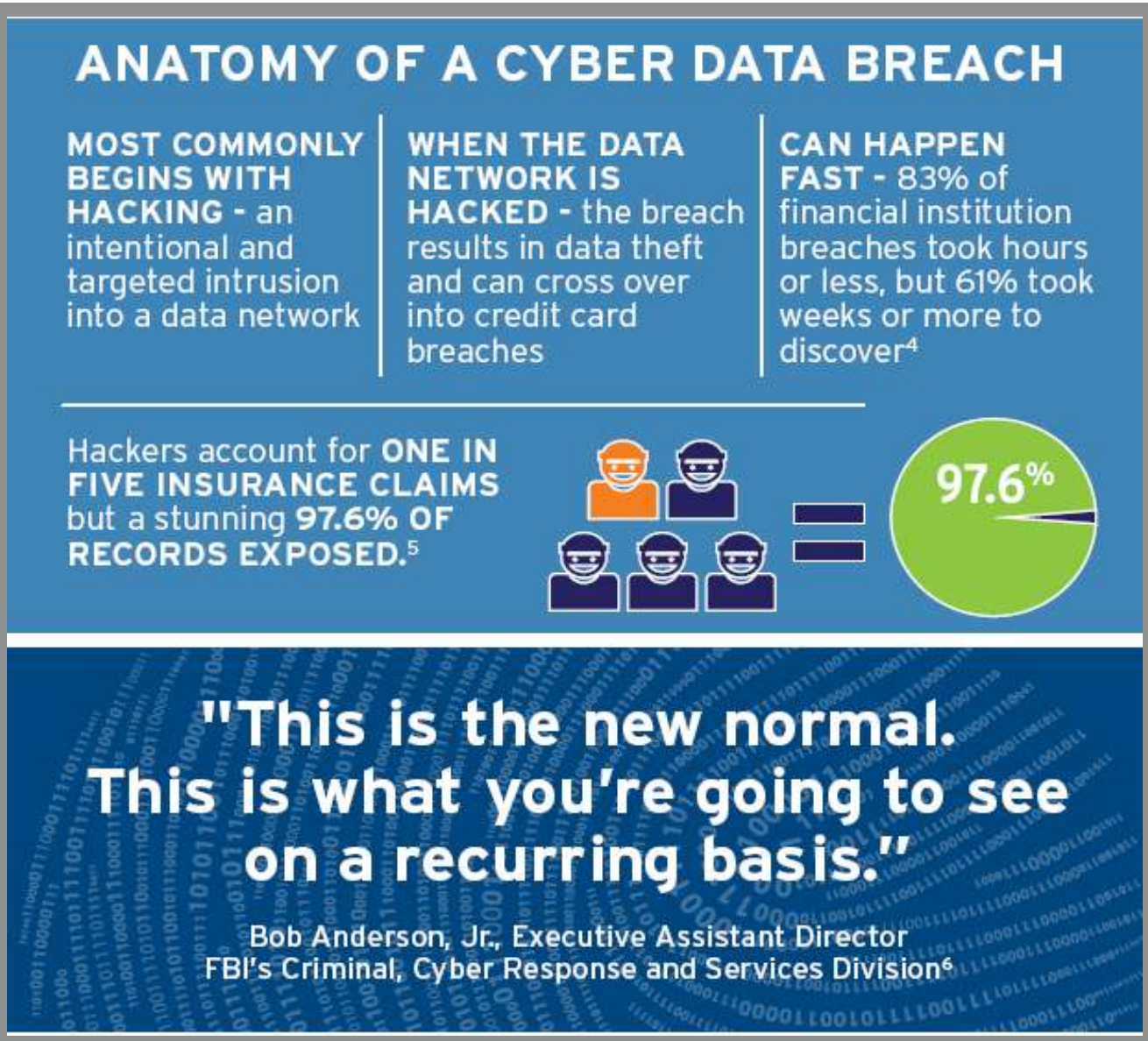
-Robert Anderson
Executive Assistant Director of the FBI's Criminal Cyber Response and Services Branch

"You're going to be hacked."

-Joseph Demarest
Assistant Director of the FBI's Criminal Cyber Response and Services Branch

Categories of Business Organizations

- Those that will suffer a breach.
- Those that have suffered a breach.
- And those that will suffer a breach again.
- **No** business organization is spared.



Source: CUNA Mutual Group and NetDiligence 2013 Cyber Liability & Data Breach Insurance Claims

Busy Year 2013

- 617 documented breaches
  - Average costs of these 317 breaches:
    - $5 dollars per customer notification multiplied by millions
    - $30 per card cancellation/related monitoring of credit PER customer
    - $2000 per hours in forensic examinations and data security analysis costs
    - $500,000 per breach in legal expenses
    - 1 million dollars per breach in corporate settlement costs
      - 1 million dollars per breach in regulatory fines or related expenses

https://www.privacyrights.org/data-breach

2014

- Identity Theft Resource Center reports that between 2005 (when record keeping commenced) and **October 14, 2014 there were 4,854 recorded breaches exposing 669,680,671 records**.
- Major data breaches are reported almost weekly
  - JP Morgan Chase; Target; Home Depot; eBay; Michaels; Neiman Marcus; Citibank; Sony, etc.

Data Breach Basics (cont'd)

- If large-scale breaches are regularly reported, then the number of smaller-scale breaches necessarily must be larger.
- Average cost to a company that suffers a breach now is approximately $200.00 per compromised record .

Data Breach Basics (cont'd)

- Average cost of lost laptop containing personally identifiable information now has approached $50,000, with only 2% representing the actual cost of the device.
- Forensic experts hired to identify, contain, and respond to data breaches easily cost 6-figures within the first two weeks of engagement.

Target Breach Expenses

(does not include legal expenses)

- Severance for CEO amounted to 15.9 million dollars alone
- Regulatory fines 1 billion dollars – for negligence to the government
- Fraudulent credit card charges – whopping 2.2 billion dollars
  - Was to be refunded by the company for losses from those 40 million card accounts
  - The retail chain suffered 440 million dollars in revenue losses fueling 2014 so far as a result of lowered consumer confidence from the hacks

Vulnerability of So-Called "Secure" Systems

- Viruses, spyware, worms, or Trojans
- Malware, including zero-day malware
- Web-based attacks
- Employee actions (both negligent and intentional)
- phishing

Simple Data Loss

- Lost or stolen devices
  - Smartphones with weak or no password protection
  - Laptops with weak or no password protection
  - Flash drives or other portable memory devices
- Improper disposal of documents
- Improper disposal of computers and other devices
- Improper disposal of system components
- Palm Springs Federal Credit Union

Financial Sector Threats

- The number of incidents and level of sophistication has increased dramatically in recent years triggering active Cyber Division of the FBI to take larger active role.
- Account Takeovers
  - Exploitation of online financial and market systems, such as Automated Clearing House systems, payment card transactions, and market trades.

Threats (cont'd)

  - Compromise typically is accomplished by accessing an authorized user's weak account credentials.
- Third-Party Payment Processor Breaches
  - Bad actors target these companies' systems, because the volume of personally identifiable information and payment card information is massive, and because such information has immediate value on the black market.

Threats (cont'd)

- Payment Card Skimming and Point of Sale Schemes
  - Steal card data to sell or create fake payment card
  - Obsolete operating systems for ATMs and POS machines is easily compromised

Threats (cont'd)

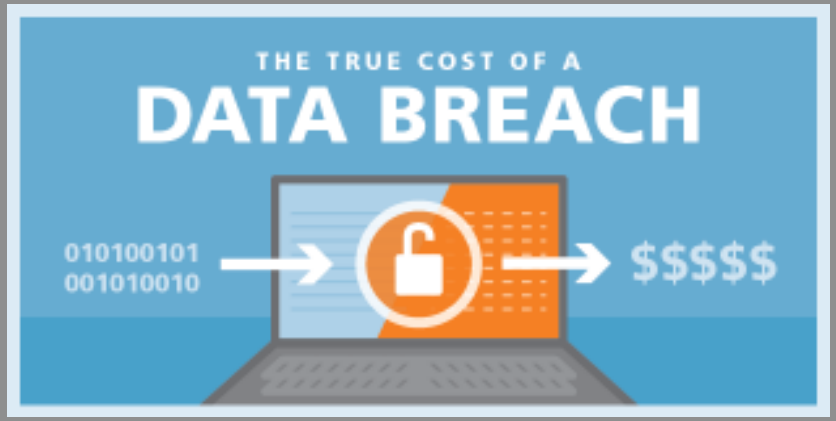
- Mobile Banking Exploitation
  - Increased risks
  - Malware starting to show up
    - Man-in-the-middle attacks utilizing special malware sent via texts
    - More prevalent in Androids
  - Apple's mobile payment system

Threats (cont'd)

- Insider Access
  - Direct access to confidential information, data, and other insider information.
- Supply Chain Infiltration/Vendor Management
  - Bad actors can gain physical and technical access to credit union by compromising trusted suppliers of technical, computer, and security equipment, software, and hardware.

Consequences of Inaction

- Loss of goodwill
- Reputation risk
- Transactional costs associated with loss mitigation
- Forensic expert fees
- Civil liability exposure
- Exposure to fines and other penalties



FFIEC Cybersecurity Assessment

- Inherent risk
  - Connection types
  - Technologies used
- Preparedness
  - Risk management and oversight
  - Collaboration and controls
  - Incident management

FS-ISAC

- Financial Services Information Sharing and Analysis Center
- Launched in 1999 as the global go-to resource for cyber threat
- www.fsisac.com

Consumers

- “Breach fatigue”
- Complacency
- Not likely to impact shopping habits
- Credit unions should educate members and encourage monitoring of account

Laws and regulations

Risk Assessment/Prevention

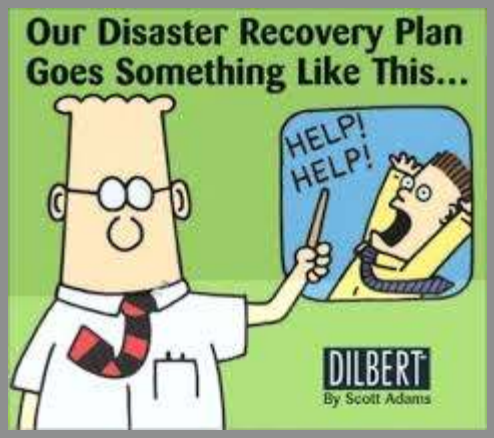
- Preventive measures
- Including
  - Identifying foreseeable threats
  - Assess likelihood and danger of potential threats
  - Assess sufficiency of policies, procedures
  - Proper disposal of information

Loss Prevention

- Employee Awareness Training
- Patch Management
- Encryption
- Periodic Testing of Computer Security

Loss Prevention (cont'd)

- Strengthen Account Credentials
  - Pass-phrases, rather than passwords
  - Combine various character types
- Limit and restrict administrative access
- Cybersecurity and Data Protection Policies and Procedures



Breach Response

- Assess incident
- Notify NCUA or state supervisory authority
- Notify law enforcement
  - File Suspicious Activity Report ("SAR"), if applicable
- Preservation of records and evidence
- Member notification
- 12 C.F.R. Parts 748 and 1016

Breach Response (cont'd)

- Cybersecurity and Data Breach Response Plan
- Upon notice of a potential data compromise, immediately contact a law firm with cybersecurity expertise.
- Permit law firm to coordinate retention of forensic experts.

State Regulation

- Only 3 states do not currently have a law requiring notification of security breaches
- Minnesota and Washington have statutes that require a merchant to reimburse a financial institution for reissuance of cards under certain circumstances
- NJ bill introduced this year requires reimbursement for costs incurred by financial institutions

Connecticut Consumer Security Breach Notification

Any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security following the discovery of the breach to any resident of this state whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through such breach of security. Such notice shall be made without unreasonable delay, subject to the provisions of subsection (d) of this section and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system. Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.

Connecticut Consumer Security Breach Notification

Any person that maintains such person's own security breach procedures as part of an information security policy for the treatment of personal information and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section, provided such person notifies, as applicable, residents of this state, owners and licensees in accordance with such person's policies in the event of a breach of security and in the case of notice to a resident, such person also notifies the Attorney General not later than the time when notice is provided to the resident. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or functional regulator, as defined in 15 USC 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided (1) such person notifies, as applicable, such residents of this state, owners, and licensees required to be notified under and in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or functional regulator in the event of a breach of security, and (2) if notice is given to a resident of this state in accordance with subdivision (1) of this subsection regarding a breach of security, such person also notifies the Attorney General not later than the time when notice is provided to the resident.

Federal Regulation

- Tax Identity Theft Awareness Week: www.mycreditunion.gov/protect/Pages/taxidtheft.aspx
- Prevent Identity Theft: www.mycreditunion.gov/protect/Pages/Prevent-Identity-Theft.aspx
- Frauds and Scams: www.mycreditunion.gov/protect/fraud/Pages/default.aspx
- Cybersecurity Awareness: www.ffiec.gov/cybersecurity.htm
- NCUA Consumer Report: Frauds, Scams and Cyberthreats - Part I: http://youtu.be/3Zlfy7_97Vc
- NCUA Consumer Report: Frauds, Scams and Cyberthreats - Part II: http://youtu.be/5XfyfRgxsLE

What Constitutes Cyber Liability

Insurance

"The vast majority of credit unions in the U.S. don't have adequate insurance coverage in the event of another online data breach."

-*Credit Union Journal*, November 10, 2014

What Can You Do?

- Is your data security adequate?
- What does your insurance cover?
- What insurance is available for credit unions that may experience data breach exposure?

Cyber Insurance

- Approximately 50 companies in the U.S. offer cybersecurity insurance
- $2 billion is expected to be spent in the United States in 2014 on cyber insurance
  - 67% increase from 2013
  - In 2010 cyber insurance premiums totaled $600,000
- Notifying affected customers of a credit card breach can cost up to $500,000

Cyber Insurance – continued

- $166,000
  - average cost of a breach to credit unions
  - according to CUNA Mutual
- CUNA Mutual's cybersecurity policy includes access to:
  - Resources to help credit unions manage risks
  - Insurance protection
  - Breach recovery services

- Employee Awareness Training
- Patch Management
- Encryption
- Periodic Testing of Computer Security
- Policies and Procedures
- Proactive and quick response
- Review current insurance coverage

E. Andrew Keeney, Esq.

Kaufman & Canoles, P.C.

150 West Main Street, Suite 2100

Norfolk, VA 23510

(757) 624-3153

eakeeney@kaufcan.com

http://www.kaufmanandcanoles.com/movies/credit-unions.html

Cybersecurity Workshop

February 10, 2015

E. Andrew Keeney, Esq.
Kaufman & Canoles, P.C.

The Credit Union League of Connecticut

KAUFMAN & CANOLES
attorneys at law