Fraud Management

NAFCU Compliance School

November 5, 2015

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

KAUFMAN & CANOLES
attorneys at law

NAFCU

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

Fraud Management Strategies

- Types of fraud
- How to avoid
- How to minimize
- Data Security, Data Breach, Tools Available
- Some checklists and self-assessment tools
- Best Practices

Main Barriers to Fraud Protection

- Lack of staff resources
- Complexity and understanding of the risk
- Cost of implementing fraud detection tools/solutions
- Consumer data privacy issues/concerns
- Lack of a compelling business case (cost vs. benefit) to adopt or change existing fraud layers/methods

Strategies

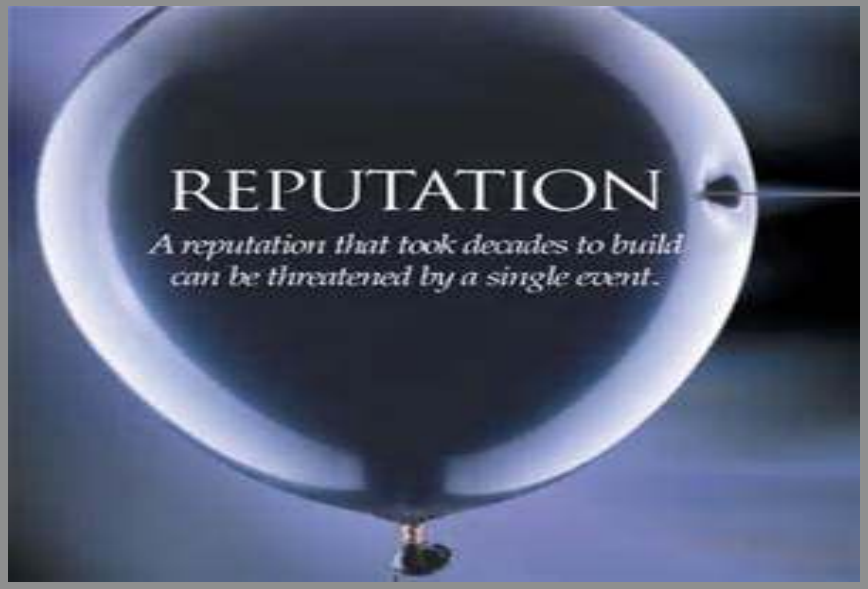
- Commitment to make tough choices
- Forward looking strategy
- Well developed and integrated risk management
- Balance appetite for risk
- Evaluate the threat landscape to prioritize a treatment strategy. Don’t buy into a “one-size fits all” approach to security

Strategies, Continued

- Without deemphasizing prevention, focus on better and faster detection through a blend of people, processes, and technology
- Collect, analyze and share incident data to create a rich data source that can drive security program effectiveness
- Let's keep preventing, but enhance our ability to detect threats that slip through our defenses

Enterprise Risk Management – Fraud Strategy

- Don’t wait until your members notice or experience fraud
- Act early by having a holistic approach in place to help detect suspicious activity
- Reputation risk is critical when it comes to fraud



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”

"Where in a day can a person 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

Data Breach Basics

- If large-scale breaches are regularly reported, then the number of smaller-scale breaches necessarily must be larger
- Damages associated with large-scale data breaches now are estimated to be in the 8- to 9-figure range
- 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

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

Threats

- 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

Threats, continued

- Mobile Banking Exploitation
  - Increased risks
  - Malware starting to show up
  - Apple's mobile payment system

Consequences of Inaction

- Loss of goodwill and public trust for the breached organization
- Transactional costs associated with loss mitigation
- Forensic expert fees
- Civil liability exposure
- Exposure to fines and other penalties

Five Ways a Credit Union Can Fight Cyber Security Risks

1. Employee awareness training
2. Cyber security and data protection policies and procedures
3. Encryption
4. Due diligence of third party providers
5. Participation in financial services information sharing and analysis center ("FS-ISAC")

Members

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

Member Relations and Education of Members

- Repeatedly inform the members
- Accessed information is restricted to employees with specific business purposes
- Employees trained to maintain confidentiality and member privacy
- Description of sharing of information, if any
- Assurance that credit union procedures comply with Federal regulations and leading industry practices

Member Relations and Education of Members, Continued

- Reaffirmation that systems are equipped with computer virus protection, intrusion detection and firewalls which strive to block access by unauthorized users
- Strive to have a website design or site that has a VeriSign (SSL) certified which means information exchange with any address beginning with “https” is encrypted before it is transmitted
- Offer members the option to enroll in ID protection plan

What Members Can Do to Protect Themselves

Repeated education of the members to do at least the following:

- Enter personal information only on secure websites
- Never respond to emails asking for personal credit union or credit card information
- Never use email to send confidential information since internet email is not secure
- Do not open emails if you do not recognize the sender's name
- When in doubt, delete!

What Members Can Do to Protect Themselves, Cont'd

- Change passwords regularly using a mixture of upper, lowercase characters and numbers
- Use passwords that are not easily guessed
- Do not share password information with anyone
- Be wary of promotional scams
- Update anti-virus software and security patches to your system regularly
- Tear up or shred any pre-approved credit offers that you do not want

FFIEC Cybersecurity Assessment

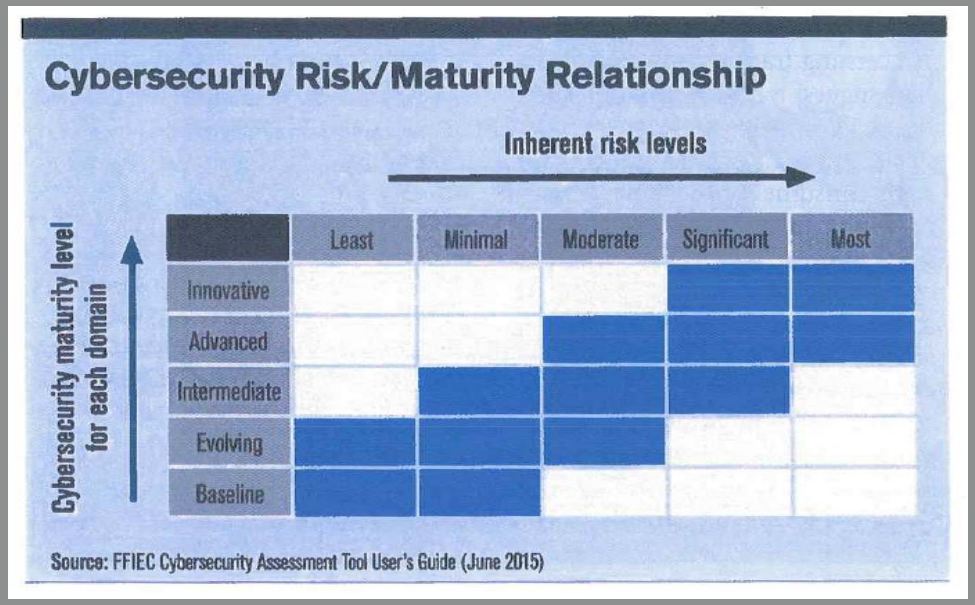
- Inherent risk
  - Connection types
  - Technologies used
- Preparedness
  - Risk management and oversight
  - Collaboration and controls
  - Incident management

The inherent risk profile identifies the amount of risk posed to a credit union by the types, volume and complexity of its activities, products and services

- Technology and connections
- Delivery channels
- Online/mobile products and technology services
- Organizational characteristics
- External threats

FFIEC Definition of Five Risk Levels

- Least inherent risk
- Minimal inherent risk
- Moderate inherent risk
- Significant inherent risk
- Most inherent risk



FS-ISAC

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

Training and Guidance

- Training
  - SANS Institute – http://www.SANS.org
  - Multi-State Information Sharing & Analysis Center
    - https://msisac.cisecurity.org/resources/videos/free-training.cfm
  - NCUA/OSCUI
- Guidance
  - NCUA Rules & Regs:
    - 12 CFR Part 748: Security Program, Report of Crime and Catastrophic Act, Bank Secrecy Act Compliance, and
    - 12 CFR Part 749: Records Preservation Program
  - FFIEC – Information Technology Manuals

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
- Cybersecurity and Data Breach Response Plan

NCUA Regulations/Guidance

- IT Related Letters to Credit Unions - http://www.ncua.gov/Resources/CUs/IT/Pages/ISTltcu.aspx
- IT Related Legal Opinion Letters – http://www.ncua.gov/Resources/CUs/IT/Pages/ISTLegalOpinions.aspx
- Examiners Guide Chapter 6 Provide Guidance on Informational Systems and Technology
- AIRES IT Exam Questionnaire
- Federal Financial Institutions Examination Council (FFIEC) Examination Handbook
- FFIEC Regulatory Resources by IT Handbook – http://ithandbook.ffiec.gov/resources.aspx

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

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

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

- Member Relations and Education of Members
- Employee Awareness Training
- Encryption
- Periodic Testing of Computer Security
- Policies and Procedures – (“FS-ISAC”)
- Due Diligence of Third Party Providers
- Proactive and quick response
- 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

Fraud Management

NAFCU Compliance School

November 5, 2015

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

KAUFMAN & CANOLES
attorneys at law

NAFCU