V502 Electronic Fraud and Security

By Robin J Wybenga,
TBA Credit Union
robinw@tbacu.com
231.946.7090

Electronic Fraud & Security

- Objectives

1. Better understand the roles and legal responsibilities of the board, supervisory committee, and management in dealing with technology risks;

2. Identify the main step in assessing risk;

3. Understand the concept of life cycle technology security;

4. Be more aware of the types of technology-related risk that credit unions face.

Electronic Fraud & Security

- TRUST – the foundation of financial services

  Job of the board, management and staff is to be mistrustful.

  Part of building trust is to be aware of what can, and will, go wrong.

Setting Technology Policy

- Each day, billions of dollars flow through the financial system – most in the form of bytes and bits – not currency or coin.

- Credit unions are entrusted to safeguard the information and the money it represents. This information is one of the credit union's most important asset.

Protecting that information is necessary to establish and maintain trust between the credit union and its members, to be in compliance, and preserve the reputation of the credit union.

Setting Technology Policy

- Electronic security is an ongoing process, not an event.
- Electronic fraud and security are included under risk management.
- The board is responsible for all policies including the security policy.
- Boards need to ask simple, commonsense questions before putting their stamp of approval on any recommended security policy.

Setting Technology Policy

- What constitutes a good policy?
  *Applicable to your organization;
  * Practical and do not attempt to achieve an impossible level of protection;
  * Enforceable;
  * Simple and understandable to the least-educated person affected by it;
  * Feasible for the average person to follow;
  * Positive, not negative, in its approach.

Legal & Regulatory Responsibilities and Liabilities

- NCUA Rules and Regulations, Part 748 and the Federal Credit Union model bylaws explicitly mandate that a security program be designed to protect each federal credit union office from robbery, burglary, larceny, and embezzlement.

- There must be a written security program that also ensures the security and confidentiality of member records.

Legal & Regulatory Responsibilities and Liabilities

- Today's robbers and burglars are CYBERTHIEVES!
- Cybercrimes are insidious because they occur unwitnessed, and they can go undetected for a long time.
- Internal and external threats exist.

Legal & Regulatory Responsibilities and Liabilities

- Two areas of technology risk management are

  1) Implementing a technology program and mobilizing the supervisory committee in the detection of electronic crime

  2) Initiating controls to minimize the credit union's exposure to such crimes

Legal & Regulatory Responsibilities and Liabilities

- The board must be vigilant in keeping informed of all laws, regulations, and directives that impact technologies.

- Being a volunteer does not absolve the individual of liability. Liability can be established through criminal or civil statutes or common case law.

- The Bank Secrecy Act is made up of several statutes, including the Money Laundering Control Act; the Anti-Drug Abuse Act; the Financial Recordkeeping and Reporting ACT; and the Patriot Act.

Legal & Regulatory Responsibilities and Liabilities

- In the majority of electronic transactions, more than one law may be applicable.

  * Is there a contractual relationship involved in the transaction?
  * Is there an international component to the transaction?
  * Is this a wire transfer transaction?
  * Did the transaction involve improper access to stored data?
  * Did the transaction involve electronic signatures?

Legal & Regulatory Responsibilities and Liabilities

- Impact of the Financial Institutions Reform Recovery and Enforcement Act (FIRREA)

  Responsible individuals or parties can be held personally liable

  Insurance coverage for directors and officials generally does not cover FIRREA fines and penalties.

- Fidelity Bond – provides coverage for losses caused by both insiders and outsiders.

- CUNA's eGuide provides a comprehensive list of federal laws and regulations.

Technology Risk & Its Assessment

- Technology is Neutral.
- Every technology has a certain set of risks associated with it.
- While technology extends the power of credit unions, it also offers opportunities for fraud, embezzlement, and other criminal behavior.

Technology Risk & Its Assessment

- Human factor – Insiders use to account for 60% of the fraud reported by financial institutions. Now external fraud schemes have replaced insider abuse as the dominant problem.

- In its 2010-2011 Global Fraud Report, Kroll found that theft of information and electronic data overtook physical theft as the most frequently reported fraud.

Technology Risk & Its Assessment

- Technology Risk Management

1. Assign responsibility
2. Identify the systems in use in the credit union
3. Determine what risks the credit union faces.

An important par to risk assessment is to look at:

* The probability of each type of risk event;
* The amount of potential loss involved;
* The cost of guarding against the event.

Life-Cycle Security

- Monitoring – regularly monitor its technology systsm to ensure that they are operating properly
- Audit Trails – Well-designed technology systems create records of their own activity called audit trails. Helps to discourage improper activities.
- Auditing – Test the security of the data; test the security of the equipment; test the ability to reconstruct in case of a disaster

Internal Risk in Computer Operations

- The importance of People
- Good security is a pact among the board, management, and staff
- IS employees have particularly demanding jobs
- Computer security grows complex
- Isolation still works

Internal Risk in Computer Operations

- Protection of equipment5 and data
- Viruses and other pests
- Sabotage
- Theft of equipment
- Release of information

Internal Risk in Computer Operations

- Staff use of telephones, email, and Internet

A good policy should include:

*Main purpose if for business
*Deleting an item does not mean it's not stored somewhere
*Email messages can be used as legal evidence
*Broadcast messages should be restricted to management
*Communication may be monitored
*Email is NOT a secure way to transact business

Internal Risk in Computer Operations

- Staff use of telephones, email, and Internet

A good policy should include:

*Main purpose if for business
*Deleting an item does not mean it's not stored somewhere
*Email messages can be used as legal evidence
*Broadcast messages should be restricted to management
*Communication may be monitored
*Email is NOT a secure way to transact business

External Risk in Computer Operations

- Catastrophes
- Burglary and Theft
- Hackers
- Intruders

Telecommunications

- Remote Voice Mail
- Using zero in your phone system
- Cell phones
- Voice over Internet Protocol (VoIP)
- Faxes

Other Technologies

- Credit and Debit cards
- ATM Security
- Wire Transfers

Summing up

- Risks change as technology evolves even though technology is neutral.

- Board considers the following:
  1. Is there a policy/procedures that spell out what our IT structure should look like?
  2. Do we have an information security policy/ procedures?
  3. Do we have a policy/procdedures for regular data backup?
  4. How is change management handled?
  5. What role does IT play in the strategic plan?