IT Policies & Procedures

Speakers:

Elizabeth Allison, CISA, CRISC, CFSA, Sr. Information Security Analyst, Keesler FCU
Michael Barrack, Director – IT Security and Compliance, D+H
How to Create an Effective Information Security Program

Elizabeth Allison, CISA, CRISC, CFSA
Sr. Information Security Analyst
Keesler Federal Credit Union
As the Sr. Information Security Analyst at Keesler Federal Credit Union, Elizabeth is responsible for development, management, and implementation of the Information Technology Security Program. Elizabeth has delivered many presentations on the successful implementation of IT Risk Management, Security Framework, and Employee Security Awareness Training programs. She has over 14 years of experience in Internal Audit, Information Security, and Risk Management, and has served on the board of directors for her local ISACA, Institute of Internal Auditors (IIA), and InfraGard chapters.

After serving on the IT recovery team after Hurricane Katrina, she retained her experiences and perfected the art of creating a policy and procedures framework that provides value in a real life environment and still meets regulatory requirements. She has designed and implemented numerous programs and processes including security incident response, and change management. She has performed and facilitated control and compliance reviews, risk assessments, social engineering, and cyber-crime table top exercises.
Agenda

• What is an Information Security Program?
• So Many Regulations, Where Do You Start?
• Effective Policies and Procedures
• Resources
INFORMATION SECURITY PROGRAM

WHAT IS IT?

A **Documented, Verifiable** Strategy

To Ensure Availability, Confidentiality, and Integrity of your Members’ Sensitive Information.

*If it is not written down, it does not exist!*
The Rapid Advancement of Technology is Driving the Increase in Regulatory Compliance

The definition of Security Programs is Evolving Just as Fast!

Organization Infrastructure and Related Data Protection Activities Outside of the Data Center Must be Documented, and Ongoing.
Security Program Benefits

• Ability to Defend the Organization Against Liability Lawsuits for Inadequate Preparation Against Cyber Attacks
• Costs of Responding to a Data Breach
• Employees Know What is Expected of Them
Security Program Benefits

The Auditors Job is to Audit Your Policies

What Do They Do When There Are No Programs/Policies Documented??

Documented Security Programs make us happy!
What Does Your Institution Do To Protect Sensitive Information?

- Security Cameras?
- Network Firewalls?
- User Name/Passwords?
- Data Backups?
- Windows Updates?
- Vendor Background Checks?
- Policies/Procedures?
- Internet Filters?
- Split Combinations?
- Controlled System Access?
- Software Installation Restrictions?
- Robbery Training?
- Check Member Identification?
- Mandatory Week Vacation?
Everyone Has A Security Program

It Just Needs To Be Documented
Or
Refreshed to Meet Current Requirements.
Key Elements of a Security Program

• Governance
• Policies & Procedures
• Risk Management
• Training & Awareness
• Security Controls
• Ongoing Monitoring
Sample Program Outline

A. Incident Management
   I. Security Incident Response Team (SIRT)
   II. Incident Escalation
   III. Incident Response

B. Security Awareness
   I. Security Portal
   II. Employee Training
   III. Testing and Benchmarking

C. Log Management

D. Risk Management

E. Vendor Management
Program Refresh

Where Do You Start?

Management Buy-In

Compile a List of Regulations

Perform an Assessment of Your Current Program
The Perfect Self-Assessment
NCUA Aires Checklists

**Scoping/Exam Prep:**
- IT-Items Needed
- IT-Pre-Exam Update

**Tier 1 Review:**
- IT-748 Expanded
- IT-Anti-Virus & Malware
- IT-Audit Program
- IT-Business Continuity
- IT-Electronic Banking
- IT-Networks
- IT-Policy Checklist

**Tier 2 Review:**
- IT-Firewalls
- IT-IDS-IPS
- IT-Pen Test Review
- IT-Physical & Environmental
- IT-Remote Access
- IT-Router
- IT-Servers
- IT-Virtualization
- IT-Wireless Networks
<table>
<thead>
<tr>
<th>Policies and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
</tr>
<tr>
<td>9a</td>
</tr>
<tr>
<td>9b</td>
</tr>
<tr>
<td>9c</td>
</tr>
<tr>
<td>9d</td>
</tr>
<tr>
<td>9e</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>10a</td>
</tr>
<tr>
<td>10b</td>
</tr>
<tr>
<td>10c</td>
</tr>
<tr>
<td>10d</td>
</tr>
<tr>
<td>10e</td>
</tr>
<tr>
<td>11</td>
</tr>
</tbody>
</table>

Audit and Accountability - Technical
POLICY VS PROCEDURES

- Best Practices
- Promotes Consistency: Quantifiable Measures
- Step-by Step Instructions: How to Achieve Policy.
- Mandatory - Set by Management: Reflects Organizations Objectives

Guideline
Standard
Procedures
Policy
Policies and Procedures

Policies and Procedures Are The Foundation
Must Be Consistent
Create Policy Templates

Auditors love to see progress in process
Tell them all about it!
Consistency is a **MUST!**

Key Elements of a Policy

- Objective
- Scope
- Policy
- Date of Last Revision
- Enforcement/Roles
- Review/Change History
- Resources
- Logo
- Policy Naming Convention
1.0 PURPOSE
   The purpose of this policy is...

2.0 SCOPE
   This policy applies to employees, contractors, consultants...

3.0 POLICY
   Authorized Use:
   3.1. Keesler Federal computing services are to be used primarily for business....
   3.2. The Information Technology Department is responsible for managing policies...

   Keesler Federal E-mail Accounts:
   3.3. In addition to the following items pertaining to Keesler Federal E-Mail Accounts, employees are required to obtain, read, understand, and adhere to the IT121-E Mail Archive Policy located on the Employee Portal under the Information Technology document area.
4.0 ENFORCEMENT:

4.1. Keesler Federal reserves the right to investigate suspected violations of this policy…

5.0 RELATED POLICIES/REFERENCES

5.1. IT-103 Data Classification Policy
5.2. IT-104 Mobile Device Policy
5.3. IT-106 Password Policy
5.4. IT-109 Remote Network Access Policy
5.5. IT-115 Software Management Policy
5.6. IT-121 Email Archive Policy
5.7. IT-124 Social Media Policy
5.8. IT-126 User Access Control Policy

6.0 DEFINITIONS

Computing Services: Computing services include any computer,

User: A user of a system or service is an individual who has been granted an
Policy Tips

• Management must review and approve all polices and procedures

• Policies should be approved by the Board of Directors.

• Evidence of Changes/Reviews/Approvals
Policy Tips

Communicate Policies to Employees

Employee Acknowledgement - Evidence

Acknowledgement - Physical or Digital
# Document Changes/Review History

<table>
<thead>
<tr>
<th>REVIEW/REVISION</th>
<th>PERFORMED BY</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Creation</td>
<td>Elizabeth Allison</td>
<td>6/13/2011</td>
</tr>
<tr>
<td>Reviewed &amp; Approved</td>
<td>Larry Mayo</td>
<td>6/16/2011</td>
</tr>
<tr>
<td>Reviewed &amp; Approved</td>
<td>Board of Directors</td>
<td>8/2/2011</td>
</tr>
<tr>
<td>Revised software &amp; VPN guidelines</td>
<td>Elizabeth Allison</td>
<td>1/31/2012</td>
</tr>
<tr>
<td>Reviewed &amp; Approved</td>
<td>Larry Mayo</td>
<td>2/7/2012</td>
</tr>
<tr>
<td>Reviewed &amp; Approved</td>
<td>Board of Directors</td>
<td>3/6/2012</td>
</tr>
<tr>
<td>Revised (new format)</td>
<td>Elizabeth Allison</td>
<td>6/1/2012</td>
</tr>
<tr>
<td>Reviewed &amp; Approved</td>
<td>Larry Mayo</td>
<td>6/20/2012</td>
</tr>
<tr>
<td>Reviewed &amp; Approved</td>
<td>Board of Directors</td>
<td>10/16/2012</td>
</tr>
</tbody>
</table>

This policy is maintained by the Information Technology Department. Any questions relating to this policy should be directed to the Information Security Analyst (Information Technology Department).

**Enforcement of this policy is the responsibility of all Department Management.**

Keesler Federal Credit Union reserves the right to revise, amend, or delete this or any other policy at any time with or without notice. Once revised, changes will take effect immediately.
Employee Acknowledgement

ACCEPTABLE USE POLICY
ACKNOWLEDGEMENT of UNDERSTANDING

My electronic signature acceptance signature acknowledges the following statements:

1. I have read, received a copy of, understood, and will adhere to the Keesler Federal Credit Union IT102-Acceptable Use Policy.

2. I understand that I am responsible for obtaining, reading, understanding, and adhering to the following Information Technology Security policies which are located on the Employee Portal under the Information Technology document area. I understand that if I can contact the IT Helpdesk at x4444 or 228-385-4444 should I need assistance.
   - IT-103 Data Classification Policy
   - IT-106 Password Policy
   - IT-109 Remote Network Access Policy
   - IT-115 Software Management Policy
   - IT-121 E Mail Archive Policy
   - IT-124 Social Media Policy
   - IT-126 User Access Control Policy
   - IT-104 Mobile Device Policy (if employee uses a mobile device to access Keesler Federal resources)
Policy Tips

Some Policies Have a Smaller Audience

For Example:

Acceptable Use Policy - All Employees

System Administrator Policy - IT Department
Ongoing Maintenance

Changes in Regulations, Processes, Systems, Controls

Annual Reviews and Approval by Management and the Board of Directors
Resources

**NCUA Aires Checklists**

Security Services-Consulting Benefits

College University Websites
Resources

- CUNA Technology Council File Library
- NIST (National Institute of Standards and Technology)
- SANS.org (Information Technology Institute)
- ISO (International Organization for Standardization)
Resources

• **ISACA (Information Security and Control Association)**
  – COBIT Framework

• **IIA (Institute of Internal Auditors)**
  – COSO Framework

• **FISMA (Federal Information Security Management Act)**
Keep Your Objectives Real

Compliance Alone Does Not Mean Your Institution is Secure

The Titanic Passed All Compliance Checks!
Introduction – Michael Barrack

- More than 25 years experience serving Financial Institutions
- Former CEO of iPay Technologies, LLC
- Former CIO of several Community Banks
- The responsible executive for IT regulatory examinations both as a Banker and service provider
- Has been serving FI Clients since 2007 by:
  - Delivering services to Banks and Credit Unions nationwide
  - Developing IT Compliance programs that meet the regs.
  - Providing advice, direction and solutions
- Lives outside of Las Vegas Nevada (and doesn’t gamble)
Agenda

- The dynamic IT regulatory/security landscape
- How Credit Unions should respond
- What are the implications for IT Policies
- Other drivers of change
- How to get the most out of your updated policies
IT regulations/threats never more dynamic

- FFIEC – CEO Webinar
- Pilot program assessing Cyber Risk
- Our experience
The question is: Why
“Exhibit A”
**Target by the Numbers**

<table>
<thead>
<tr>
<th>400 Million</th>
<th>The number of credit and debit cards stolen between Nov. 27 and Dec. 15, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 Million</td>
<td>Estimated dollar cost to credit unions and community banks for reissuing 21.8 million cards</td>
</tr>
<tr>
<td>53.7 Million</td>
<td>Estimated income generated by hackers</td>
</tr>
<tr>
<td>46%</td>
<td>Drop in profits in Q4, 2013 compared with 2012</td>
</tr>
</tbody>
</table>

*Source – Krebs on Security, Brian Krebs*
Smaller Financial Institutions Hit
Federal Financial Institutions Examination Council

Joint Statement

Cyber-attacks on Financial Institutions’ ATM and Card Authorization Systems

PURPOSE

The Federal Financial Institutions Examination Council (FFIEC) members1 (“members”) are issuing this statement to notify financial institutions of a type of large dollar value automatic teller machine (ATM) cash-out fraud characterized as Unlimited Operations by the U.S. Secret Service. The members are aware of a recent increase in cyber-attacks launched in connection with this fraud, to gain access to, and alter the settings on, ATM web-based control panels used by small- to medium-size financial institutions.

Unlimited Operations may cause financial institutions to incur large dollar losses. Therefore, the members expect financial institutions to take steps to address this threat by reviewing the adequacy of their controls over their information technology networks, card issuer authorization systems, systems that manage ATM parameters, and fraud detection and response processes.

BACKGROUND

Unlimited Operations are a category of ATM cash-out fraud where criminals are able to withdraw funds beyond the cash balance in customer accounts or beyond other control limits typically applied to ATM withdrawals. Criminals perpetrate the fraud by initiating cyber-attacks to gain access to web-based ATM control panels, which enables them to withdraw customer funds from ATMs using stolen customer debit, prepaid, or ATM card account information. A recent Unlimited Operations attack netted over $40 million in fraud using only 12 debit card accounts.

Criminals may begin the attack by sending phishing emails to employees of financial institutions as a means to install malicious software (malware) onto the institution’s network. Once installed, criminals use the malware to monitor the institution’s network to determine how the institution accesses ATM control panels and obtain employee login credentials. These control panels, often web-based, manage the amount of money customers may withdraw within a set time frame, the geographic limitations of withdrawals, the types and frequency of fraud reports.

1 The FFIEC is comprised of the principals of the following: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.
How Credit Unions Should Respond
One Path – Outsource to Specialists

1. Evaluate providers
2. Assess expertise
3. Select and standardize IT risk management methodology
4. Select automation
5. Focus on decision making
Select FI IT Compliance Providers

- Seek organizations who do this full time
- Entire department of professionals familiar with:
  - Financial Institution IT regulatory requirements
  - Changes in the IT Security Threat landscape
  - How other credit unions have met the challenge
- Experience with:
  - IT risk management
  - IT policy coverage
  - Making policy/risk assessment actionable
## Implications for IT Policies

### Vendor Summary

#### Contracts Requiring Review

<table>
<thead>
<tr>
<th>Vendor Name</th>
<th>Contract</th>
<th>Expiration</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT and T</td>
<td>No Contract Uploaded!</td>
<td>Jan, 29 2015</td>
</tr>
<tr>
<td>Aldrich &amp; Bonnefin</td>
<td>A and B contract.pdf</td>
<td>Mar, 08 2013</td>
</tr>
<tr>
<td>All Rite Leasing Company</td>
<td>Leasing.pdf</td>
<td>Mar, 27 2014</td>
</tr>
<tr>
<td>Fiserv</td>
<td>contract.docx</td>
<td>Jan, 16 2015</td>
</tr>
</tbody>
</table>

#### Vendors Requiring Review

<table>
<thead>
<tr>
<th>Vendor Name</th>
<th>Next Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aldrich &amp; Bonnefin</td>
<td>Jul, 17 2015</td>
</tr>
<tr>
<td>All Rite Leasing Company</td>
<td>Oct, 27 2014</td>
</tr>
<tr>
<td>D+H Harland/Cavion</td>
<td>Oct, 27 2014</td>
</tr>
<tr>
<td>D+H, Compushare Product Family</td>
<td>Apr, 17 2012</td>
</tr>
<tr>
<td>Deluxe Financial Services, Inc.</td>
<td>Oct, 27 2014</td>
</tr>
<tr>
<td>Fidelity Information Services</td>
<td>Jan, 17 2015</td>
</tr>
<tr>
<td>Fiserv</td>
<td>Mar, 01 2014</td>
</tr>
</tbody>
</table>

### Announcements

- **Technology Alert FIL-16-2014**
  
  FDIC Technology Alert FIL-16-2014 The FDIC has issued an alert advising financial institutions of a material security vulnerability. A copy of the alert is located in the Guidance and Resource section of Risk Director.

- **Reissuance - FIL-13-2014**
  
  The FDIC has reissued FIL-13-2014 Technology Outsourcing. The documents are not examination procedures or official guidance but, rather, informational tools. A copy of FIL-13-2014 is located in the Guidance and Resource section of Risk Director.

- **Press Release- PR-28-2014**
  
  FDIC Urges Financial Institutions to Use Available Cyber Resources A copy of the FDIC Press Release PR- 28 - 2014 is located in the Guidance and Resource section of Risk Director.
Updates to IT Policies

Unassigned

Risk Director User Guide
Risk Director is an online solution for performing vendor management, business continuity, information technology-related risk assessment, and audit finding tracking. This guide will provide a brief overview of the system, and identify key functional capabilities.

Audit Resources

There are currently no Audit Resources documents.

Business Continuity Documents

Damage Assessment Form
This form can be used to help assess and document damage to a facility after a disaster.

Policy and Procedure Samples

Policy Sample: Acceptable Use Policy
Provides requirements for end-user activities. Updated to include BYOD statement.

Policy Sample: Access Level Policy
Provides requirements for access level management and review.

Policy Sample: ATM Policy- Anti Fraud Measures
This policy is intended to address the threat of cyber-attacks by establishing policy for reviewing the adequacy of controls over the institution's information technology (IT) networks, card issuer authorization systems, systems that manage ATM parameters, and fraud detection and response processes.
Updates to IT Policies

Policy Sample: Personal Device Usage Policy - BYOD
This document provides additional guidance related to the use of non-company owned devices for accessing company systems and data.

Policy Sample: Remote Access Policy
Provides requirements for oversight of remote access.
Updates to IT Policies

Policy Sample: Wireless Policy

Provides requirements for wireless network management.
Updates to IT Policies

- **Server Build Guide**: Provides guidelines for server configuration.
- **Social Media Guidelines**: These guidelines are to augment existing policies and procedures to ensure employees understand the proper use of social media in relation to the institution's interests.
- **VOIP Guidelines**: Provides guidelines for VOIP activities.
- **Social Media Policy**: This policy is to augment existing guidelines and procedures to ensure employees understand the proper use of social media in relation to the institution's interests.
Updates to IT Risk Assessment

<table>
<thead>
<tr>
<th>Description</th>
<th>Probability</th>
<th>Impact</th>
<th>Mitigation/Control</th>
<th>Residual</th>
<th>Risk Type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CyberSecurity: Inadequate Cyber Resilience</td>
<td>Low</td>
<td>Low</td>
<td>Adequate</td>
<td>Low</td>
<td>C, I, A</td>
<td></td>
</tr>
<tr>
<td>CyberSecurity: Inadequate Third-party Dependency</td>
<td>Low</td>
<td>Low</td>
<td>Adequate</td>
<td>Low</td>
<td>C, I, A</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberSecurity: Lack of Cyber Threat Intelligence</td>
<td>Low</td>
<td>Low</td>
<td>Adequate</td>
<td>Low</td>
<td>C, I, A</td>
<td></td>
</tr>
<tr>
<td>and Collaboration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberSecurity: Inadequate Risk Management &amp;</td>
<td>Low</td>
<td>Low</td>
<td>Adequate</td>
<td>Low</td>
<td>C, I, A</td>
<td></td>
</tr>
<tr>
<td>Oversight</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberSecurity: Inadequate CyberSecurity Controls</td>
<td>Low</td>
<td>Low</td>
<td>Adequate</td>
<td>Low</td>
<td>C, I, A</td>
<td></td>
</tr>
</tbody>
</table>

Bulk Actions

Need Help?
Stay Current with Change
Other Drivers of Change

- Examination Currents
- What other Credit Unions are doing/experiencing
  - NCUA hot buttons
  - IT examination trends and focus
- Emerging IT controls
  - Data Encryption at rest
  - Mobile device management
Making IT Policies Effective - Training

- Information Security Training
- Website surfing
- Email protocol
- The power of policy comes when people connect it to their responsibilities
How do Information Security responsibilities vary by job function?
Making IT Policies Effective - Relevance
Questions?