How To Audit Information Security Programs

Cerone F. “Cy” Sturdivant, CISA
Senior Managing Consultant|BKD,LLP
csturdivant@bkd.com

BKD LLP
CPAs & Advisors

TODAY'S AGENDA

- Threat Landscape Overview
- Information Security Program (ISP) Overview
- Auditing the Functional Areas of an ISP
- Examiner Expectations
- Final Thoughts and Resources
- Questions

Open discussion is encouraged!

THREAT LANDSCAPE OVERVIEW

There are only *three* types of companies:

Those that have been hacked
Those that will be hacked
Those that don’t know they have been hacked

Data Breaches – A Major Cost

IBM 13th Annual Cost of a Data Breach Study

This year's study reports the global average cost of a data breach is up 6.4 percent over the previous year to

$3.86 million

The average cost for each lost or stolen record containing sensitive and confidential information also increased by 4.8 percent year over year to

$148 per record.

IBM X-Force Threat Intelligence Report

Financial Services, you're still Number 1!

"Financial services tops the targeted industry charts for the second year in a row. Financial services experienced the highest volume of security incidents and the third highest volume of cyber attacks"

Are We Paying Attention?

The 2018 Verizon Data Breach Report indicates that we are not.

“Over 80% of the hacking breaches discussed in the 2018 Report fall into the same categories identified in the 2014 Report”

Small Businesses *(YOU)* Are Under Attack

Almost 90% of small business owners don’t feel like they’re at risk of experiencing a breach…….

Small Businesses (YOU) Are Under Attack

"58% of all data breach victims noted in the 2018 VDB Report are business with under 1,000 employees"

INFORMATION SECURITY PROGRAM OVERVIEW

Overview of IS Program Requirements

Per GLBA, Financial Institutions are required to develop a written Information Security Program that describes their plans to protect member information. The plan must be appropriate to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of the member information it handles. As part of this plan, each institution must:

- involve the board of directors;
- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The requirements are designed to be flexible!

Information Security Program Contents

- Information Security Policy / Cybersecurity (Establish policies and procedures)
  - data governance & classification;
  - user assess rights administration;
  - access controls & dual control;
  - systems operations & availability concerns;
  - systems & network security monitoring;
  - data encryption standards;
  - systems & application development & quality assurance;
  - physical security & environmental controls;

- Incident/Breach Response Plans (Response Programs)

- Business Continuity & Disaster Recovery Plans (Hazards and technical failures)

- Third-Party Risk Management/Cyber Resiliency Plans (Oversight of servicer providers)

Information Security Program Contents

- Information Security Risk Assessment (Assess Risk)
  - Identification of information assessments (prioritize)
  - Identification of foreseeable threats
  - Determination of likelihood of occurrence
  - Determination of magnitude of impact
  - Assessment of inherent risk
  - Identification of mitigating controls
  - Calculation of residual risk
- Annual Report to the Board of Directors (Oversight)
  - Risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations and management's responses; and recommendations for changes in the information security program.
- Adjusting the Overall Program
  - Audits and examinations
  - Updates to regulation/guidelines, changes in risk profile, etc.

Information Security Awareness “Training”

- Tailor based on specific area:
  - Employees
  - Senior Management
  - Board of Directors
  - Customers/Members

Note: More than just annually is the expectation.

Top Vulnerability – People

Phishing Attacks

Verizon Data Breach Report:

- 7.3% of users across multiple data contributors were successfully phished—whether via a link or an opened attachment.

- 95% of Phishing attacks resulted in software installation

Note: Old-school awareness training does not cut it anymore. Your email filters have an average 10-15% failure rate; you need a strong human firewall as your last line of defense.

P@33WORDS!

- 81% of confirmed breaches are due to weak, reused, or stolen passwords

- 91% of people understand the risk of reusing passwords; however, 61% still reuse them

Why? On average, an individual keeps track of over 190 passwords.

Note: Do not use the same password over multiple sites

INFORMATION SECURITY PROGRAM - AUDIT PREPARATION

Audit Functional Areas – Focus Efforts Here!

- Management / Oversight
- Information Security / Cybersecurity
- Physical Security
- Network Logical Security
- User Administration
- Change Management
- Business Continuity / Disaster Recovery
- Mobile Device Management
- Electronic Banking
- Vendor Management

IT vs IS – Both Have Their Place

Information Technology	Information Security
Top priority: Ensuring hardware, software, network, etc. remains functional	**Top priority:** Protecting data and assets at all costs
Responsible for new technology implementations and maintenance	Responsible for systems, processes and risks posed by end users
Puts controls in place	Monitors controls to ensure they work as designed
Stays up-to-date on new hardware, software and solutions	Stays up-to-date on new threats and developments that emerge daily
Often measured in uptime and response times	Recommends and prioritizes action steps and solutions
“Fix-it” mentality	“Secure-it” mentality

Focus on The Top Areas of Vulnerability

- Network –Unpatched/Outdated Systems
  - Windows and Applications
- Accounting/Wire Department
  - Payments - Wires, ACH, Checks, etc.
- Business Customers
  - Email compromise, CATO, etc.
- Vendors & Third Parties
  - Core provider, ATM, DR host. etc.

Focus on Governance Controls

Board & Senior Management Responsibilities, Duties & Best Practices

- Incorporate key IS areas into the **risk-based audit plan**
- **Track all** IT audit, vulnerability assessments, penetration tests, and social engineering findings and recommendations **until final resolution**
- Ensure Information Security / Cybersecurity information is communicated to the Board **frequently** (at least quarterly)
- Ensure **Business Continuity/DR, Vendor Management** and **Incident Response Policies** & **Procedures** address Information Security

Governance Continued…

- Ensure awareness training is performed regularly (educate & motivate)
- Ensure the **Information Security Officer** has adequate authority, resources and independence (**Management Booklet** November 2015)
- Include **IS / Cybersecurity events** in annual Disaster Recovery and Incident Response tests
- Join **Financial Services – Information Sharing & Analysis Center (FS-ISAC)** or other information sharing forums – filter reports based on each employees' role
- Ensure **threat intelligence** is timely, ongoing, risk focused, reported & actionable

Audit Risk Mitigation Strategy

FREE Solution to a more Secure IT Environment

Guaranteed to reduce your risk of data breach by 99%

The Answer Is……

Delete all user accounts

EXAMINER EXPECTATIONS

Regulatory Landscape

Examination Preparation

Completing the FFIEC Cybersecurity Assessment annually

- Address Baseline gaps promptly!
- Don’t settle for just Baseline, strive for Evolving or higher.

Key Factor: Stress test all Baseline and Evolving criteria. Don’t answer “Yes” unless you can document/validate the control is in place.

NCUA – ACET Examination Process

Starting in 2018, NCUA examiners have used the Automated Cybersecurity Examination Tool (ACET) to assess the cyber posture of credit unions over $1 billion in assets.

- The Excel spreadsheet tool, constructed by the NCUA for examiner use, employs over 530 Statements and over 200 unique document requests to establish an institution's Inherent Risk Profile and Cybersecurity Maturity level.
- While it resembles the FFIEC Cybersecurity Assessment Tool (CAT), the ACET's focus is assessing cybersecurity posture through documentary evidence substantiating the answers to the 530 Statements.

Notes: Feedback from 2017 pilot testing has shown that completing this in-depth assessment may take up to 3 weeks of examiner on-site time.

Message From Examiners

- Inventory – “A good inventory is paramount”
- Application Lifecycle Management – Too many institutions with unsupported software
- Configuration Management – This should include systems, applications, and other technology
- Application Access Reviews – risk based and frequent
- Log Management / Anomaly Detection - log aggregation alone is not enough

Message From Examiners

- Audit tracking should include root cause analysis information
- Project management – Defined processes and practices needed
- Identification of breakdowns in corporate governance will be strongly emphasized – education is a must
- Successful organizations – All departments have a voice in the IT Steering Committee.
- Cybersecurity is integrated among IT and all departments

Message From Examiners

"Management and oversight of the IT environment is deficient and represents a serious regulatory concern….

The current information security posture of the institution is hazardous to the security of sensitive organizational, member, and employee data.

Senior management and the Board have not been committed to the security of sensitive institutional and member data entrusted to them…"

FINAL THOUGHTS AND RESOURCES

Perform Frequent Assessments

IT General Control Assessment – Tests your compliance.

- Verifies you are following your Information Security Program, FFIEC Guidelines, NCUA, etc.
- Ensures its adequate to meet regulatory requirements & implements industry best practices

Vulnerability Assessments – A comprehensive assessment that checks for:

- Missing patches or updates
- Default settings & passwords
- Vulnerable systems

Internal/External Penetration Testing – An assessment that replicates a hacker. Identifies:

- Identifies vulnerable systems
- Exploits vulnerabilities
- Finds sensitive information
- Test IDS/IPS systems

Social Engineering Assessment – Tests your people using various human techniques.

- Phishing, Pretext calling, on-site visits, etc.

Critical Elements for Successful IS Programs

- Management and Board commitment in understanding key information security issues - #1
- Information security planning prior to the implementation of new technologies
- Integration between business lines and information security
- Alignment of information security with the organization’s strategic objectives
- Executive and line management ownership and accountability for implementing, monitoring and reporting on information security matters

The Information Security Officer is only successful if the above items are met!

Final Thoughts

- ✓ Make sure Information Security is embedded into every layer of the organization – not bolted on here and there
- ✓ This is now a Board Room issue, not a server room issue
- ✓ Project an attitude of importance at all times
- ✓ Maintain high levels of engagement with employees
- ✓ Make employees your first line of defense

Remember: Never stop being vigilant; the IS/Cybersecurity threats are dynamic and ongoing!

Cybersecurity Resources

- The Top Cyber Threat Intelligence Feeds – thecyberthreat.com/cyber-threat-intelligence-feeds/
- CUInfoSecurity – http://www.cuinfosecurity.com/
- Financial Services-Information Sharing & Analysis Center (FS-ISAC) – http://www.fsisac.com/
- FFIEC Cybersecurity Awareness – http://www.ffiec.gov/cybersecurity.htm
- US-CERT – https://www.us-cert.gov/

Questions?

BKD LLP
CPAs & Advisors

Thank You!

BKD LLP
CPAs & Advisors

Cy Sturdivant, CISA
csturdivant@bkd.com
(P) 615-988-3596