AUDIT TAX SYSTEMS RISK

Financial Institutions Roundtable

A complimentary webinar series for financial institutions.

Cybersecurity: Protecting your Endpoints

August 26, 2015

Presented by: **Mike Morris, Partner, Porter Keadle Moore**

Porter Keadle Moore

CPAs | Advisors | www.pkm.com

Objectives

- **By the end of this presentation, you will be able to:**
  - Learn how the bad guys are getting in
  - Understand the types of controls that need to be in place to reduce cyber risks
  - Ways to understand what your institution has implemented (and not implemented) to reduce risks
  - Understand the best practices for vendor management cyber security oversight
  - Obtain tips on implementing/modifying/improving cyber security controls at the current weakest link (your endpoints)
  - Obtain a high-level overview of the new FFIEC Cyber Toolkit

What are Endpoints?

- Any device connected to your internal network

- From a user perspective, they include:
  - Desktops
  - Laptops
  - Smart phones
  - Tablets
  - Thin clients
  - Printers/Copiers

- From a customer perspective, they include:
  - Remote deposit capture devices
  - Workstations used to access corporate cash management applications

What are the Threats?

- Hacking has come a long way in the last few years
- The proliferation of electronic payment systems has made cyber crime very profitable
- Advanced toolkits that can ‘hide’ from our current security tools
- Hackers prey on the weakest link – the end user (your employees and customers)
- Not knowing your vendors and their controls

Who Are Our Adversaries?

"If you know the enemy and know yourself you need not fear the results of a hundred battles."

-Sun Tzu

- **We are up against opponents that are:**
  - Highly skilled
  - Highly motivated
  - Well funded
  - Constantly looking for targets of opportunity regardless of size
  - Successfully attacking our endpoints (employees and customers)

Polling Question #1

- **In the last 18 months have you identified an instance where your endpoints were under attack?**
  - Yes
  - No
  - Unsure

Notable Cases/Events

- Choice Escrow versus BancorpSouth (“Corporate Account Takeover”)
- International hacking ring stole up to $1B from more than 100 banks in the U.S., Germany, China and the Ukraine
- State of South Carolina – Hackers stole tax records for 5.7 million current and former South Carolina taxpayers and their dependents

Notable Cases/Events

Choice Escrow versus BancorpSouth

- Choice Escrow was infected with malware (weak endpoint controls)
- The attackers gained access to Choice Escrow's online banking (through BancorpSouth) using a compromised username and password
- $440,000 was stolen and Choice escrow sued BancorpSouth
- BancorpSouth won the lawsuit because twice they offered Choice Escrow additional security controls, and twice, in writing, Choice Escrow declined

Notable Cases/Events

- **Lessons Learned:**
  - Never trust customer computers
  - Implement the recommended layered security controls outlined in the FDIC's FIL-50-2011: *FFIEC Supplement to Authentication in an Internet Banking Environment*
  - If your customers decline any of the security controls, ensure that you document it in writing!

Notable Cases/Events

- **$1B Bank Hack:**
  - Gained foothold to the banks through phishing attacks
  - Monitored the banks for months (taking screen shots and using the employees webcams to monitor their activities)
  - Once familiar with the bank operations, they used the knowledge to steal money (hacking ATMs, transferring money to fraudulent accounts, fraudulent wires, etc.)

Notable Cases/Events

- **$1B Bank Hack:**
  - According to forensics experts:
    - they appeared to limit their activities to $10M per bank before moving on to another target
    - Anunak/Carbanak malware was used to perpetrate the fraud
    - The attacks averaged two to four months per attack
    - In all cases observed, the attackers used spear phishing attacks to infect systems with the Carbanak malware.
    - The spear phishing emails contained attachments with weaponized Microsoft Word 97 – 2003 (.doc) and Control Panel Applet (.CPL) files.
    - After compromising a system, the attackers installed additional software (Ammyy Remote Administration Tool or breached SSH servers)

Notable Cases/Events

- **Lessons Learned :**
  - Block malicious emails using email filters
  - Continue to train end users the importance of protecting your institution from email attacks
  - Add additional security layers to check the validity of email attachments and embedded links

Notable Cases/Events

- **State of South Carolina Hack**
  - A Department of Revenue employee executed malware and became compromised after clicking on a link in an email
  - The attacker then obtained the employee's username and password
  - The attacker logged into the Department's remote access service (Citrix) using legitimate Department of Revenue user credentials
  - The attacker then used the employee's access to gain access to other Department of Revenue systems
  - The attacker stole 3.3 million bank account numbers, 3.8 million tax returns (which also included 1.9 million SSNs for children and other dependents)

Notable Cases/Events

- **Lessons Learned:**
  - Require multifactor authentication for all external connections

What was the Common Thread?

- In all instances, the attackers gained their foothold through social engineering access to the endpoints

- Traditional perimeter security devices can't stop these kind of attacks alone

How are the Endpoints Being Attacked?

- It is estimated that 80% of malware infections occur through email

- Clicking on links in Google can be dangerous:
  - *McAfee's most dangerous celebrity to search for online:*
    1. **Jimmy Kimmel Searches Yield a Nearly One-in-Five Chance of Landing on a Malicious Site**
    2. **Armin van Buuren 19.33% risk**
    3. **Ciara 19.31% risk**

- 30% of all cyber attacks target business with fewer than 250 employees

- Cyber crime has surpassed illegal drug trafficking as a criminal moneymaker

Polling Question #2

- **Have you read the 2015 Verizon Data Breach Investigations Report?**
  - Yes
  - No

Verizon 2015 Data Breach Investigations Report

- **Notable Statistics/Findings:**
  - In **60%** of the cases, attackers are able to compromise an organization within **minutes**
  - **23%** of recipients open phishing emails and **11%** click on the attachments
  - **99.9%** of the exploited vulnerabilities were compromised more than **a year after** the vulnerability was published

Verizon 2015 Data Breach Investigations Report

- **More Notable Statistics/Findings:**
  - Mobile devices are not a preferred vector in data breaches
  - Financial institutions and merchants slow to adopt terminals for the October 2015 Europay, MasterCard, and Visa (“EMV”) chip-and-PIN mandate bill bear the blame
  - 40% of the controls determined to be most effective will fall into the “quick wins” category

Our End Points are at Risk

- **The current targets that are our weak points:**
  - Our internal users
  - Our corporate cash management customers using eBanking

What We Are Seeing

- Weak email filter controls (especially MS 365 and other cloud-based email systems)
- Susceptible user security awareness
- Weak surf controls
- Users have local administrative rights
- institution’s relying solely on antivirus at the end point
- institution’s not remediating internal vulnerabilities timely

Email Filter Controls

- **Preventive control – stop the bad attachments before they hit the user's inbox (take away their ability to make bad decisions!)**

- **Key control activities:**
  - Ensure that all malicious file types are blocked
  - Don't allow spoofing (i.e. an internal email addresses coming from the outside)
  - Block the "one off" domains
  - Prevent users from being able release infected emails from quarantine

User Security Awareness

- **This is an ongoing battle**

- **Key control activities:**
  - Regularly test through social engineering and communicate the results (reward good behavior)
  - Formal, quarterly security awareness training
  - Constant reminders (share current events, best practices, etc.)
  - Watch for hard copies of sensitive information

Internet Usage Controls

- **Weak surf control filters**

- **Key control activities:**
  - Get more restrictive (and get Board support)
  - Monitor usage and follow up with users that appear to be abusing the system
  - Investigate additional software controls that can programs and embedded links that are pointing to the bad guys (Invincea, Gladiator AMP, Mimecast)

Local Administrator Rights

- **Helps to prevent malware from infecting the end point**

- **Key control activities:**
  - Beta a small group of users
  - Work with vendors who's applications are causing problems
  - Incorporate the requirement into your due diligence for new vendors
  - Use Group Policy to push out software distributions

E-Banking Services

- **Risk - anywhere large dollar amounts can leave the Bank:**
  - Corporate Cash Management – Wires and ACH
  - Bill Pay
  - Person to Person (P2P)

- **Risk - We don’t control the computers that initiate these transactions (unfortunately, hackers can and do)**

E-Banking Controls

- **Controls for e-banking:**
  - Multifactor authentication for customers
  - Out-of-band verification
  - Challenge questions – “out-of-wallet” vs. “personal”
  - Fraud detection and monitoring systems
  - Exposure limits
  - Employee security awareness
  - Customer security awareness training

Guidance

- FFIEC Cybersecurity Assessment Tool (https://www.ffiec.gov/cyberassessmenttool.htm)
- NIST Cyber Security Framework (http://www.nist.gov/cyberframework/)
- SANS 20 Critical Security Controls (https://www.sans.org/critical-security-controls/controls)

Inventory of Authorized/ Unauthorized Devices (SANS/NIST)

- **Detective control – Unauthorized devices (iPhones, Androids, Laptops, USB) can provide an attacker a point of attack**

- **Key control activities:**
  - Deploy an automated asset inventory discovery tool
    - Solar Winds, ManageEngine, AlienVault, MS Network Access Protection (NAP), etc.
  - Deploy dynamic host configuration protocol (DHCP) and monitor the service
  - Maintain a detailed asset inventory (Update your inventory when new assets are deployed)
  - Organizational communications and data flows are mapped (NIST and FFIEC)

Inventory of Authorized/ Unauthorized Software (SANS/NIST)

- **Detective control – Unauthorized software could be malware or contain security vulnerabilities. It could also pose licensing issues.**

- **Key control activities:**
  - Deploy application whitelisting technology (prevents execution of all other software on the system)
    - Bit9, Microsoft Software Restriction Policies, McAfee Application Control, etc.
  - Maintain a detailed software inventory and monitor the production environment for changes
  - Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system
  - Dangerous file types (i.e. .exe, .zip, .msi) must be blocked through email filters

Baseline Security Configurations (A.K.A Hardening Guides) (SANS/NIST)

- **Preventive control – Formal procedures for installing new endpoints to your network.**

- **Default configurations for operating systems and applications are normally designed for ease-of-deployment and ease-of-use, not security.**

- **Key control activities:**
  - Create formal policies and guidelines (make sure vendors follow them for anything they install in your environment)
  - Implement formal patch management for all network operating systems and patches
  - Maintain master images of key systems on a secure server
  - Includes printers and copiers!

Malware Defense (SANS/NIST)

- **Detective control – Malicious software is an integral and dangerous aspect of Internet threats, and is designed to attack your systems, devices, or your data**

- **Key control activities:**
  - Use automated tools to monitor for malware
  - Look for cloud-based options that checks the ‘reputation’ of software or monitors whether the software is trying to contact somewhere it shouldn’t
  - Limit ability to use removable media and monitor authorized usage

Control the Use of Administrative Privileges (SANS/NIST)

- **Preventive control – Administrative privileges is a primary method for attackers to spread inside a target enterprise**

- **Key control activities:**
  - Remove local administrator rights from servers, workstations and laptops
  - Minimize administrative privileges and only use administrative accounts when they are required
  - Configure all administrative passwords to be complex
  - Before deploying any new devices, change all default passwords

Boundary Defense (SANS/NIST/FFIEC)

- **Preventive control – Attackers focus on exploiting systems that they can reach across the Internet**

- **Key control activities:**
  - Deploy network-based IPS sensors on Internet
  - Ensure firewalls are configured to block incoming and outgoing traffic that is not specifically needed (use access control lists!)
  - Require all remote login access to use multi-factor authentication
  - Ensure email filters and email configurations block common threats
  - Make sure your border/Internet routers are secure
  - Enforce strong surf controls

Data Protection

- **Preventive control – Processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information**

- **Key control activities:**
  - Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data
  - Deploy automated tools on the network perimeter that monitors for certain sensitive information, such as account numbers
  - Disable USB ports
  - Consider data loss protection (DLP) software
  - Clean up your network drives of non-public customer information
  - Block known file transfer and mail systems

Don’t Forget Your Vendors

- Which vendors have access to non-public customer information?
- Which vendors have connectivity to your network?
- Which vendors are providing a web presence for you?
- How many vendors are using sub-vendors? How far does your risk extend?
- Have they documented their cyber resilience (Appendix J of the FFIEC BCP Handbook)?

Polling Question #3

- **Have you started using the FFIEC's Cyber Security Assessment tool?**
  - Yes
  - No
  - I don't know what that is

Cyber Security Assessment Tool

- **Designed by the FFIEC to help institutions identify their risks and determine their cybersecurity maturity**

- **The tool is designed to guide you through the five categories of your inherent risk profile:**
  - Technologies and Connection Types
  - Delivery Channels
  - Online/Mobile Products and Technology Services
  - Organizational Characteristics
  - External Threats

Cyber Security Assessment Tool

- **Next the tool guides you through your Cybersecurity Maturity level for these five domains:**
  - Cyber Risk Management and Oversight
  - Threat Intelligence and Collaboration
  - Cybersecurity Controls
  - External Dependency Management
  - Cyber Incident Management and Resilience

- **By reviewing your inherent risk profile and your maturity levels across the domains, you can determine whether your maturity levels are appropriate in relation to your risk**

Cyber Security Assessment Tool – Inherent Risk Profile

- **Risk Levels**
  - Incorporate the type, volume, and complexity of the institution's operations and threats directed at the institution. Inherent risk does not include mitigating controls

Figure 1: Inherent Risk Profile Layout

Risk Levels

Activity, Service, or Product	Category: Technologies and Connection Types	Risk Levels				
		Least	Minimal	Moderate	Significant	Most
	Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
	Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
	Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)

Cyber Security Assessment Tool – Inherent Risk Profile

▲ Determine Inherent Risk Profile

- You can determine your institution's overall Inherent Risk Profile based on the number of applicable statements in each risk level for all activities

Figure 2: Inherent Risk Summary

	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Number of Statements Selected in Each Risk Level					
Based on Individual Risk Levels Selected, Assign an Inherent Risk Profile	Least	Minimal	Moderate	Significant	Most

Cyber Security Assessment Tool – Cybersecurity Maturity Domains

- Domain 1: Cyber Risk Management and Oversight
- Domain 2: Threat Intelligence and Collaboration
- Domain 3: Cybersecurity Controls
- Domain 4: External Dependency Management
- Domain 5: Cyber Incident Management and Resilience

Cyber Security Assessment Tool – Cybersecurity Maturity

▲ Domains and Assessment Factors

- Within each domain are assessment factors and contributing components. Under each component, there are declarative statements describing an activity that supports the assessment factor at that level of maturity.

Table 1: Domains and Assessment Factors Defined

Domains and Assessment Factors Defined	
Domain 1 **Cyber Risk Management and Oversight** Cyber risk management and oversight addresses the board of directors' (board's) oversight and management's development and implementation of an effective enterprise-wide cybersecurity program with comprehensive policies and procedures for establishing appropriate accountability and oversight.	
Assessment Factors	**Governance** includes oversight, strategies, policies, and IT asset management to implement an effective governance of the cybersecurity program. **Risk Management** includes a risk management program, risk assessment process, and audit function to effectively manage risk and assess the effectiveness of key controls. **Resources** include staffing, tools, and budgeting processes to ensure the institution's staff or external resources have knowledge and experience commensurate with the institution's risk profile. **Training and Culture** includes the employee training and customer awareness programs contributing to an organizational culture that emphasizes the mitigation of cybersecurity threats.

Cyber Security Assessment Tool – Cybersecurity Maturity

▲ Maturity Levels Defined:

Maturity Levels Defined	
Baseline	Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.
Evolving	Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.
Intermediate	Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.
Advanced	Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.
Innovative	Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.

Cyber Security Assessment Tool – Cybersecurity Maturity

- The tool guides you through each domain and provides guidance for each maturity level

Domain 2: Threat Intelligence and Collaboration			
Assessment Factor: Threat Intelligence			
		Y,N	
THREAT INTELLIGENCE AND INFORMATION	Baseline		The institution belongs or subscribes to a threat and vulnerability information sharing source(s) that provides information on threats (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC], U.S. Computer Emergency Readiness Team [US-CERT]). *(FFIEC E-Banking Work Program, page 28)* Threat information is used to monitor threats and vulnerabilities. *(FFIEC Information Security Booklet, page 83)* Threat information is used to enhance internal risk management and controls. *(FFIEC Information Security Booklet, page 4)*
	Evolving		Threat information received by the institution includes analysis of tactics, patterns, and risk mitigation recommendations.
	Intermediate		A formal threat intelligence program is implemented and includes subscription to threat feeds from external providers and internal sources. Protocols are implemented for collecting information from industry peers and government. A read-only, central repository of cyber threat intelligence is maintained.

Cyber Security Assessment Tool – Analyzing Your Results

- You can review your institution's Inherent Risk Profile in relation to its Cybersecurity Maturity results for each domain to understand whether they are aligned

Table 3: Risk/Maturity Relationship

Cybersecurity Maturity Level for Each Domain	Inherent Risk Levels: Least	Minimal	Moderate	Significant	Most
Innovative				■	■
Advanced			■	■	■
Intermediate		■	■	■	
Evolving	■	■	■		
Baseline	■	■			

Cyber Security Assessment Tool – Analyzing Your Results

- As inherent risk rises, your institution's maturity levels should also increase

- This assessment should be reviewed regularly and updated as changes are identified or as controls mature

Cyber Security Assessment Tool – Summary

- Start the process now
- Provide your Board and Senior Management with Cyber Security Awareness training
- Include the Board in the process of completion of the tool and present the results

Polling Question #4

- **How often do you provide cybersecurity training for your Board members?**
  - Annually
  - Every other year
  - Sporadically
  - Never

Conclusion

- Hackers are preying on our weakest links – our endpoints (and have been successful)
- We (and our vendors) need to be constantly evaluating and implementing controls to reduce cyber risk – especially for our employees and high-risk customers
- We need to ensure that the board and senior management understand your inherent cybersecurity risks and maturity levels
- Your institution is securing the current weak link and is planning ahead for future attack types

Recommended Reading

- Mandiant APT1 Report
- Verizon 2015 Data Breach Investigations Report

Questions?

Mike Morris, Partner
Porter Keadle Moore, LLC
mmorris@pkm.com
(404) 420-5669

Sign up for our Next Webinar:

“New Developments in Taxation”

- **October 14, 2015 3:00 - 4:00pm (EST)**

http://pkm.com/events/webinars/