Cybersecurity and Risks Associated with IT

Jay Brietz, CPA and CIA
Richard Cook, CISA, CISM and CRISC
Agenda

• I’m not an IT Specialist – Where Do I Start?
  - IT 101: An Introduction to Some Basic IT Concepts and Suggestions Regarding How to Increase Your IT Comfort Level

• Icebergs Ahead!

• Overview of Cyber Terrorism

• Common Data Breaches/Threats

• Strategies to Mitigate Cyber Terrorism Risks
I’m not an IT Specialist – Where Do I Start?
IT 101

• IT 101: An Introduction to Some Basic IT Concepts and Suggestions Regarding How to Increase Your IT Comfort Level
Key Concepts for this IT introduction:

• To assist non-technical (non-IT) management to gain a better understanding of IT and Security related processes
• How to increase your comfort level when interacting with the IT security Group
• Increase your knowledge set of specific IT security topics
• Leave the session with several good references to increase your knowledge and follow new trends in IT/Security that can be understood by non-technical (non-IT) management
How can I increase my comfort level when interacting with the IT security Group?

- Ask questions to gain knowledge, thus increasing your comfort level. (Ex. new, Reader’s Digest)
- Try to not be afraid of IT, many people have limited knowledge in this area. As we move forward into the future, IT will become a larger part of our lives and our jobs.
- Individuals that have both IT and functional knowledge are highly prized by their employers. (Ex. Dual resource, junior staff, part of management team)
- Teams that incorporate an integrated approach (business and IT groups working together) have a much higher chance for success when using IT/Security related processes.
- Your IT team will appreciate your efforts to learn their language as well as understand their challenges. (Ex. junior staff, pre-set questions)
- Generally most IT members are more than glad to share their knowledge.
How can I increase my comfort level when interacting with the IT security Group?

- Join committees with an IT component
  - IT Steering Committee
    - General focus is on application system changes
  - IT Strategic Planning Committee
    - Ensure the enterprise and IT are aligned
  - Incident response team
  - Participate in risk assessment projects (provided the project has an IT component)
  - Participate in system selection team
  - Be a part of the Disaster Recovery Planning (DRP) Team – or Business Continuity Planning (BCP) Team
  - Show up prepared and be ready to ask questions
How can I increase my comfort level when interacting with the IT security Group?

- Be curious
  - When you hear an IT term that you are not familiar with, write it down and look it up later.
  - Read IT or security related articles from professional publications.
  - Periodically listen to webinars related to IT/Security.
  - Practice your craft to increase your skill set and develop your baseline knowledge.
  - When you go to training – sign up for classes out of your comfort zone.
What is an Internal Network Vulnerability Assessment?

• The assessment is performed by using an automated tool (app) that “scans a range of IP addresses” and produces an automated report which will show risk-rated vulnerabilities that were identified and potential fixes.

• Each device has an IP address and each type of device has known vulnerabilities that are easily accessible on the internet.
  
  - To prevent – all systems must be appropriately patched as vulnerabilities are identified (patch management applies to network, operating system, application and database layers). Patches are provided by the vendors.
Mobile Device Security

• iPads and tablets are difficult to secure.
• Remote access to systems should be appropriately restricted and remote access should be via a secure path, such as VPN (virtual private network).
• Mobile (smart) phones should be required to have passwords and remote wipe capabilities if the mobile device can access email or other systems.
  - This still applies even if the device is not owned by the enterprise. BYOD – bring your own device.
• All laptops should have encrypted hard drives and remote wipe capabilities.
  - There is free ware available to perform this task.
Basic Security (layers of an onion)

• Most secure should be the center of the onion (database).
User Security

• If the systems allows – use group or role based security – as opposed to menu based security.
• Apply the concept of “least privilege” for system access rights.
• Business users should not be performing the user provisioning function for systems. This process should be performed by the IT/IS group.
• Privileged user access rights should be limited.
• Third party access should be temporary, logged and monitored.
• System access rights for users should be explicitly requested. We should not use the “copy same as X” system access request process.
Password Security

• Heartbleed – did you change passwords? Often times we use the same passwords in our personal lives that we use at work.

• Be cautious – social media is a mecca for hackers.
  - Information available via just facebook: name, birthday, family member names and home towns, pet names, addresses, anniversary dates. Is any of this public information part of your passwords?
  • Example of email chain with family member names, birthdays, etc.
So many passwords – how can I remember them all?

A few tips for creating and remembering passwords

• Use a password creation methodology
  - Ihbbxxx! ERP (2 letter phrase, 2 letter common theme – **this is the part that changes**, random number, special character)
  - Ihfbxxx! Payroll
  - Ihswxxx! SharePoint

• Storing passwords (save in benign document – maybe titled recipes – or in a spreadsheet with other data).
  - xxbb# ERP
  - xxfb# Payroll
  - xxsw# SharePoint
Vendor Management

SOC Report Reviews

• User Control Considerations must be validated to ensure the bank has appropriate controls in place.

• If the SOC1 or SOC2 has carveouts, the content and impact of the carveout should be reviewed to determine if additional procedures need to be performed (could be obtaining an additional SOC report or determining how your third party provider gained comfort over the carveout content).

• Did you know? Often times your third party provider sets up your accounts with minimal password security configurations.
Sample of Observations

• User reviews – using a tracking spreadsheet. All user access reviews should start with a system generated list.
• Most common observations related to user security are because temporary workers and contractors are not paid through the regular payroll process. Often times the provisioning of temps and contractors follow an inconsistent process. Generally contractors have privileged access rights.
• User IDs for online banking – was SSN for 80% of users. You should require that user IDs be alphanumerics.
Sample of Observations

- User had same passwords for 25 years. She was distraught when she realized they would be expiring.
- Controller had the company’s most sensitive passwords on a note pad in top desk drawer (no lock on drawer, no lock on door).
- COO resisted adding an inactivity timeout to the domain because he thought his employees would lose all the work that they were working on. Then he insisted the setting be set to 120 minutes. In the end he relented and we set it at 30 minutes. Rumor had it that he did not know any of his passwords and his EA had to log in for him.
• Hall of Fame!
  - Client three person IT staff assigned passwords that could not be changed by the users. The IT staff maintained a running list of passwords and user IDs for all users of ALL systems, including financial users. Under this scenario, the company was unable to validate that any single financial transaction was appropriate as there was no individual accountability.
  - A C-level executive lost laptop that had all his passwords on a sticky note pasted to the key pad. When a new laptop was issued – he added an new sticky note with his new passwords!
Icebergs Ahead!

• So many risks...so little time
  - Credit risk
  - Market risk
  - Interest rate risk
  - Liquidity risk
  - Regulatory risk
  - Legal risk
  - Fraud risk
  - And so on...
Icebergs Ahead!

• Cyber criminals are targeting all banks
• So...don’t forget about cyber risks
  - Financial risk
  - Reputational risk
  - Regulatory risk
  - Legal risk
Overview of Cyber Terrorism

• Cyber Terrorism defined....

Criminal acts using computers and networks as tools or targets
Overview of Cyber Terrorism

- Quotes from Verizon’s Data Breach Investigations Report:
  - “Some organizations will be a target regardless of what they do, but most become a target because of what the do.”
  - “87% of all breaches were avoidable through simple or intermediate controls.”
  - 37% of all breaches affected financial institutions.
  - 66% of all breaches took months to discover.
  - 69% of all breaches were discovered by third parties.
Overview of Cyber Terrorism

• Regulators will be looking at how banks are addressing cyber risks:
  - In a June, 2013 webinar on *The Evolving Cyber Landscape: Awareness, Preparedness and Strategy for Community Banks*, the Office of the Comptroller of the Currency (OCC) warned that the number of cyber attacks continues to grow and that smaller banks are being targeted.
  - SEC’s cyber security disclosure guidelines.
• More from the OCC...
  - “The cyber threats continue to increase in both sophistication and volume and require a heightened awareness and appropriate resources to be able to identify and mitigate the associated risks,” said Carolyn DuChene, the OCC’s deputy comptroller of operational risk, in a conference call with reporters. “We continue to implement a broader strategy that involves increased outreach to all of the banks we supervise in an effort to increase their ongoing awareness and preparedness strategies.”
Overview of Cyber Terrorism

Cyber terrorism video 1
Common Data Breaches/Threats

The chart below shows the percentage of tactics utilized across all data breaches:

- Hacked in: 53%
- Leveraged malware: 40%
- Physical attack: 35%
- Social engineering: 29%
- Privelege abuse: 13%

Hacked in breaches

- Leading culprits are:
  - Use of stolen credentials
  - Brute force
  - Backdoor or C2

- Brute force is particular an issue for small organizations and for financially motivated groups
Malware threats

- Malware is software designed to infiltrate, damage or obtain information from a computer system without the owner’s consent *(as defined by ISACA)*

- The biggest malware culprits:
  - Spyware/Keylogger – 75% of cases
  - Backdoor – 66%
  - Export Data – 62%
  - Captured Stored Data – 55%
Use of physical attacks

- Physical threats encompass deliberate actions that involve proximity, possession, or force.

- Skimmers installed inside ATM’s, POS devices, and gas pump terminals comprise almost all incidents in the physical category.
Common Data Breaches/Threats

• Speaking of “Skimming”
  - Been around for a while, but the skimmers keep getting more sophisticated.
  - Beginning to leverage 3D printing technology to improve efficiency and adapt to changes in card reader design.

Pictures: from Krebs on Security
Common Data Breaches/Threats

• Nordstrom Case
  - Found 6 skimmers attached to their point-of-sale computers back in the fall of 2013.
  - Team of 3 individuals used devices similar to this to collect/store/transmit credit card data.

Wi-Fi Premium PS/2 Hardware Keylogger 2GB - Wireless PS2 keylogger!

$145 online

Wireless hardware keylogger with built-in WLAN support! The KeyGrabber Wi-Fi Premium PS/2 comes with 2 Gigabytes of internal memory and contains an embedded Wireless LAN module, enabling it to connect to a Wi-Fi Access Point, and send E-mail reports. You can also connect to the ... more »
Common Data Breaches/Threats

Social Engineering

- Gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.

- Phishing is the most common threat.
  - Usually accomplished through email or phone call schemes.
Common Data Breaches/Threats

Social Engineering

- Washington Post announced in August 2013 that its website was hit by a phishing attack.
  - Accomplished through an Outlook Web phishing app.
  - Resulted in readers being redirected to site hosted by The Syrian Electronic Army.
  - Key aspects of this hack included the use of a third-party application and Twitter.
Common Data Breaches/Threats

Misuse actions

- Top three misuse cases are:
  • Embezzlement
  • use of unapproved hardware
  • privilege abuse
Strategies to Mitigate Cyber Terrorism Risks

There are so many risks...where to start?

- Phishing
- Skimming
- Social Engineering
- Wire Fraud
- Malware
- Hacking
- Keylogging
- Physical Attacks
Cyber terrorism video 2
Strategies to Mitigate Cyber Terrorism Risks

The Bank

Core Processor

Customers

The Bad Guys
Strategies to Mitigate Cyber Terrorism Risks

• The three-legged approach to protection
  - Secure the bank
  - Secure the core processor
  - Secure the customer

• Each leg has to work together in order to be successful

• Each leg considers controls around people, process and technology
Strategies to Mitigate Cyber Terrorism Risks

Securing the Bank

• Implementing IT security controls
  - Examples: firewalls, patched, physical protections, etc.

• Training, training, training
  - Examples: IT security issues, social engineering, social networking, passwords, etc.

• Monitoring
  - Examples: review of security logs, current developments in IT security, etc.
Strategies to Mitigate Cyber Terrorism Risks

Securing the Core Processor

• Implementing IT security controls
• Review the SOC reports
  - User control considerations
  - Exceptions and suitability of controls
• Communication
  - Frequent conversations with core processor regarding IT security measures they are implementing
Securing the Customer

• Implementing IT security controls
  - Examples: ensuring secured communications, updated patches, password security, etc.
  - Wire transfer call back procedures

• Customer training
  - Examples: IT security issues, social engineering, passwords, etc.
Other strategies to consider

• Create a response team to handle issues, often called a Computer Emergency Response Team (CERT)
  - Much like a Business Continuity/Disaster Recovery Plan

• Network with local cyber experts to understand emerging threats
Summary

• While banks face many different risks, cyber terrorism is quickly becoming a challenge

• The way that banks address the risks of cyber crimes is becoming a focus of the regulators

• While it is important to put IT security controls in place, training and periodic reminders about the threats of cyber terrorism are also very important
Did you know?

• The biggest violators of IT Security are the senior members of the IT/IS team – this is the team that is directly responsible for securing the enterprise.

Final thoughts:

- How do you know that your enterprise is secure?
- Has an independent assessment been performed to validate the IT controls? Is an appropriate audit trail in place?
- Auditors and examiners will generally conclude that if no audit trail exists the control is not operating effectively.
Questions
Resources

- http://ithandbook.ffdiec.gov/
  - FFIEC handbook – really nice framework
  - SOC1 and SOC2 information – from American Institute of CPA’s
- http://whatis.techtarget.com/
  - Reference for IT terms/glossary – in most cases Google will do
- https://www.isaca.org/Pages/default.aspx
  - ISACA (information Systems Audit and Controls Association) - webinars and cpe
- https://na.theiia.org/Pages/IIAHome.aspx
  - Institute of Internal Auditors
- http://www.journalofaccountancy.com/
  - Journal of Accountancy
We may need some help!

Some IT and Security related services provided by Elliott Davis

- Internal and External Audit Support (ITGCs)
- Co-Sourcing
- Compliance Reviews (FFIEC, SOX, PCI)
- SOC1 and SOC2 reviews – Service Organization Control
- HIPAA Reviews
- Cyber Security (Internal Network Vulnerability Assessments, External Penetration Testing, Social Engineering Reviews – physical and remote) Reviews
- SOX/Process Optimization
- Pre and Post System Implementation Reviews
- System Selection
Elliott Davis, LLC/PLLC is one of the largest accounting, tax and consulting services firms in the Southeast and ranks among the top 50 CPA firms in the U.S. With offices in SC, NC, GA and VA, the firm provides clients across a wide range of industries with smart, customized solutions and its people with rewarding opportunities. Founded in 1925, Elliott Davis is a member of The Leading Edge Alliance, an international professional association of independently owned accounting firms based in the U.S. and is strategically aligned with LEA Europe and LEA Asia Pacific, a worldwide network of more than 450 offices in 100 countries around the globe. For more information about Elliott Davis and its services, visit http://www.elliottdavis.com.