PACB One-Day Cybersecurity Workshop

CYBERSECURITY IN YOUR RISK ASSESSMENT!

PRESENTED BY:
JON WALDMAN, SBS – CISA, CRISC

© Secure Banking Solutions, LLC
www.protectmybank.com
Agenda

• What is cybersecurity?
• What do I need to know about cybersecurity?
• What are some of today’s cybersecurity threats?
• How do I build a useful Information Security Program?
• How do I build a Risk Assessment that helps me make decisions?
• People are the weakest link; how do I prepare and train my people to mitigate risk?
• Bad things are going to happen; it’s inevitable. How do I plan for and prepare to respond to incidents?
HAVE YOU COMPLETED YOUR LAST MINUTE RISK ASSESSMENT?
# Organization Type

<table>
<thead>
<tr>
<th>Category</th>
<th>Basic Organizations</th>
<th>Progressing Organizations</th>
<th>Advanced Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Philosophy</td>
<td>Cybersecurity is a “necessary evil.”</td>
<td>Cybersecurity must be more integrated into the business</td>
<td>Cybersecurity is part of the culture.</td>
</tr>
<tr>
<td>People</td>
<td>CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.</td>
<td>CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and underskilled.</td>
<td>CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.</td>
</tr>
<tr>
<td>Process</td>
<td>Informal and ad-hoc. Subservient to IT.</td>
<td>Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors.</td>
<td>Documented and formal with an eye toward more scale and automation.</td>
</tr>
</tbody>
</table>

*Source: Enterprise Strategy Group, 2014.*
Security Maturity Model

InfoSec Maturity Model

**Reactive**
- **Blocking & Tackling**
  - Lack of Executive support
  - Underfunded
  - Understaffed
  - Lack of metrics for reporting
  - Set up for failure

**Proactive**
- **Compliance Driven**
  - Control-based security approach
  - Align to mandatory regulations
    - EU/PII Data protection
    - FFIEC
    - HIPAA
    - ISO 2700x
    - PCI
    - NCUA

- **Risk-Based Approach**
  - Multi-layered security and risk-based approach
  - Using behavior analytics and evaluating new technologies frequently
  - Linking events across multiple disciplines

Source: Blue Lava
FFIEC Observations

• **Inherent Risk**: Financial institutions need a solid methodology to identify inherent risk from cyber threats. Community banks should ensure the following:

• Asset-based IT Risk Assessment that identifies:
  ◦ Connection Types
  ◦ Products and Services offered
  ◦ Technologies implemented

• **Specific risks mentioned include:**
  ◦ **ATM** Fraud
  ◦ **BYOD** Risks
  ◦ **Wire and ACH** Fraud
  ◦ DDOS Attacks
FFIEC Observations

• **Preparedness:** Following a solid understanding of inherent risks to community banks, institutions need to focus on risk mitigating comments. The FFIEC highlights the following areas:
  ◦ Risk management and oversight – involves governance, allocation of resources, and training and awareness of employees.
  ◦ Threat intelligence and collaboration – is the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action to enhance decision making.
  ◦ Cybersecurity controls – controls can be preventive, detective, or corrective
  ◦ External dependency management – includes the connectivity to third-party service providers, business partners, customers, or others and the financial institutions’ expectations and practices to oversee these relationships.
  ◦ Cyber incident management and resilience – involves incident detection, response, mitigation, escalation, reporting, and resilience.
A. Information Security Program. Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

B. Objectives. A bank's information security program shall be designed to:

1. Ensure the security and confidentiality of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information;
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
4. Ensure the proper disposal of customer information and consumer information.
Why IT Risk Assessment?

• “The evaluation of the risks to information resources and the adequacy of current controls”

• Financial institutions must maintain an ongoing information security risk assessment program that effectively:
  ◦ Gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements;
  ◦ Analyzes the probability and impact associated with the known threats and vulnerabilities to their assets; and
  ◦ Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation. (FFIEC IS Booklet)
<table>
<thead>
<tr>
<th>Type</th>
<th>FDIC FIL #</th>
<th>Short Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT</td>
<td>FDIC-21-2014</td>
<td>Webinar on Senior Management’s Role in Cybersecurity</td>
<td>FDIC hosted a free webinar entitled Executive Leadership of Cybersecurity: What Today’s CEO Needs to Know About the Threats They Don’t See. The webinar is designed to deliver its message in plain language, tips on creating a cybersecurity culture, and details about partnerships such as FS-ISAC.</td>
</tr>
<tr>
<td>IT</td>
<td>FDIC-16-2014</td>
<td>Technology Alert: OpenSSL &quot;Heartbleed&quot; Vulnerability</td>
<td>The FDIC issued FFIEC guidance advising financial institutions of a material security vulnerability in OpenSSL, a popular cryptographic library used to authenticate Internet services and encrypt sensitive information.</td>
</tr>
<tr>
<td>IT</td>
<td>FDIC-13-2014</td>
<td>Technology Outsourcing: Informational Tools for Community Bankers</td>
<td>Three FDIC Technology Outsourcing documents are being re-issued as an informational resource to community banks on how to select service providers, draft contract terms, and oversee multiple service providers when outsourcing for technology products and services. The documents are not examination procedures or official guidance but, rather, informational tools.</td>
</tr>
<tr>
<td>IT</td>
<td>FDIC-11-2014</td>
<td>Distributed Denial of Service (DDoS) Attacks</td>
<td>The FDIC issued FFIEC guidance to notify institutions of the risks associated with the continued distributed denial of service (DDoS) attacks on public-facing Web sites and the steps institutions are expected to take to address the risks posed by such attacks.</td>
</tr>
<tr>
<td>IT</td>
<td>FDIC-10-2014</td>
<td>ATM and Card Authorization Systems</td>
<td>The FDIC issued FFIEC guidance describing risks related to recent cyber-attacks on automated teller machines (ATMs) and card authorization systems that have resulted in large dollar frauds. The FDIC expects financial institutions to take steps to address this threat by reviewing the adequacy of their controls over their information technology (IT) networks, card issuer authorization systems, systems that manage ATM parameters, and fraud detection and response processes.</td>
</tr>
<tr>
<td>IT</td>
<td>FDIC-56-2013</td>
<td>Social Media: Consumer Compliance Risk Management Guidance</td>
<td>FFIEC released final guidance on the applicability of consumer protection and compliance laws, regulations, and policies to activities conducted via social media by banks, savings associations, and credit unions, as well as nonbank entities supervised by the Consumer Financial Protection Bureau. The guidance provides considerations that financial institutions may find useful in conducting risk assessments and developing and evaluating policies and procedures regarding social media.</td>
</tr>
<tr>
<td>IT</td>
<td>FDIC-3-2013</td>
<td>Modifications to Section 19 of the Federal Deposit Insurance Act</td>
<td>Section 19 of the Federal Deposit Insurance (FDI) Act prohibits, without the prior written consent of the FDIC, a person convicted of a criminal offense involving dishonesty, breach of trust, money laundering, or who has entered into a pretrial diversion program, from participating in the affairs of an FDIC-insured institution. On December 11, 2012, the FDIC Board of Directors modified the de minimis exceptions regarding the potential fine and the number of days of imprisonment.</td>
</tr>
<tr>
<td>IT</td>
<td>FDIC-46-2012</td>
<td>Supervision of Technology Service Providers and Outsourcing Technology Services</td>
<td>FFIEC issued the revised Information Technology (IT) Examination Booklet on the Supervision of Technology Service Providers (TSP Booklet) and the updated IT Examination Booklet on Outsourcing Technology Services. The Federal Reserve, the FDIC, and the OCC issued new Administrative Guidelines—Implementation of Interagency Programs for the Supervision of Technology Service Providers (Guidelines).</td>
</tr>
<tr>
<td>IT</td>
<td>FDIC-14-2012</td>
<td>Copying and Removal of Confidential Financial Institution Information</td>
<td>The FDIC has observed a limited number of instances in which directors and officers of troubled or failing institutions have made copies of financial institution and supervisory records, and removed those copies from the institution in anticipation of litigation or enforcement activity against them personally. This is a reminder to directors and officers that this activity is a breach of their fiduciary duty to the institution and an unsafe and unsound banking practice, which may also violate applicable laws and regulations and contravene the financial institution’s information security program.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-50-2011</td>
<td>FFIEC Supplement to Authentication in an Internet Banking Environment</td>
<td>The FDIC, with the other FFIEC agencies, has issued the attached guidance, which describes updated supervisory expectations regarding customer authentication, layered security, and other controls in an increasingly hostile online environment. Financial institutions will be expected to comply with the guidance no later than January 1, 2012.</td>
</tr>
<tr>
<td>Type</td>
<td>FDIC FIL #</td>
<td>Short Description</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-6-2010</td>
<td>Update to FFIEC IT Examination Handbook Series</td>
<td>The Federal Financial Institutions Examination Council (FFIEC) has issued an updated Retail Payment Systems booklet. The booklet is part of the IT Examination Handbook series and serves as guidance for examiners, financial institutions, and service providers on identifying and controlling risks related to retail payment systems and related banking activities.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-4-2009</td>
<td>Risk Management of Remote Deposit Capture</td>
<td>The guidance addresses the necessary elements of an RDC risk management process - risk identification, assessment, and mitigation - and the measurement and monitoring of residual risk exposure.</td>
</tr>
<tr>
<td>3PM</td>
<td>FIL-44-2008</td>
<td>Third-Party Risk: Guidance for Managing Third-Party Risk</td>
<td>The attached FDIC guidance describes potential risks arising from third-party relationships and outlines risk management principles that may be tailored to suit the complexity and risk potential of a financial institution's significant third-party relationships.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-105-2007</td>
<td>Information Technology - Risk Management: Program Revised IT Officer's Questionnaire</td>
<td>As part of the revision, the IT Officer's Questionnaire was enhanced to provide greater coverage of vendor management and outsourcing topics, credit card and ACH (automated clearing house) payment system risks, and an institution's overall information security program.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-81-2005</td>
<td>Information Technology Risk Management Program (IT-RMP): New Information Technology Examination Procedures</td>
<td>The FDIC has updated its risk-focused information technology (IT) examination procedures for FDIC-supervised financial institutions.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-69-2005</td>
<td>Voice Over Internet Protocol: Guidance on the Security Risks of VoIP</td>
<td>The FDIC is providing guidance to financial institutions on the security risks associated with voice over Internet protocol (VoIP). VoIP refers to the delivery of traditional telephone voice communications over the Internet.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-66-2005</td>
<td>Spyware: Guidance on Mitigating Risks From Spyware</td>
<td>The FDIC is issuing the attached guidance to financial institutions recommending an effective spyware prevention and detection program based on an institution's risk profile. This guidance and the attached informational supplement discuss the risks associated with spyware from both a bank and consumer perspective and provide recommendations to mitigate these risks.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-114-2004</td>
<td>Risk Management of Free and Open Source Software</td>
<td>The Federal Financial Institutions Examination Council (FFIEC) has issued the attached guidance to help institutions identify and implement appropriate risk-management practices when using &quot;free and open source software&quot; (FOSS).</td>
</tr>
<tr>
<td>Type</td>
<td>FDIC FIL #</td>
<td>Short Description</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-84-2004</td>
<td>Guidance on the Risks Associated With Instant Messaging</td>
<td>The Federal Deposit Insurance Corporation (FDIC) has prepared the attached guidance to assist financial institutions in protecting themselves against the vulnerabilities of instant messaging (IM) and establishing policies and procedures concerning its usage.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-30-2003</td>
<td>Federal Bank and Credit Union Regulatory Agencies Jointly Issue Guidance on the Risks Associated With Weblinking</td>
<td>Federal bank and credit union regulatory agencies have issued guidance to assist financial institutions in identifying risks posed by the use of weblinks on their websites, and to suggest a variety of risk-management techniques that institutions should consider using to mitigate those risks. This guidance applies to institutions that develop and maintain their own websites, as well as institutions that use third-party service providers for this function.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-118-2002</td>
<td>New Examination Procedures for Assessing Information Technology Risk</td>
<td>Over the last several years, many financial institutions have moved away from traditional mainframe-oriented computer processing environments and increased their reliance on newer technologies, such as networks, the Internet and enterprise-wide processing. As a result, the Federal Deposit Insurance Corporation (FDIC) is launching a new program for assessing information technology (IT) risk at FDIC-supervised financial institutions. The program incorporates a new philosophy for categorizing institutions’ use of technology and their consequential exposure to technology risk, along with updated and more risk-focused IT examination procedures.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-68-1999</td>
<td>Risk Assessment Tools and Practices for Information System Security</td>
<td>The Federal Deposit Insurance Corporation (FDIC) is providing financial institutions the attached paper on information system security issues entitled &quot;Risk Assessment Tools and Practices for Information System Security.&quot; Bank management is responsible for ensuring that systems and data are protected against risks associated with emerging technology and computer networks.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-131-1997</td>
<td>Security Risks Associated with the Internet</td>
<td>In response to the ever-increasing number of financial institutions using the Internet, the FDIC has issued the attached paper identifying many of the risks to an institution's information system security associated with Internet use. The paper also describes several risk controls. The Internet offers financial institutions a wide array of opportunities to access resources and to deliver information, products and services. However, the principal benefits of Internet access, namely its global reach and open architecture, also present significant security risks.</td>
</tr>
<tr>
<td>IT</td>
<td>FIL-82-1996</td>
<td>Risks Involving Client/Server Computer Systems</td>
<td>The interagency Federal Financial Institutions Examination Council (FFIEC) has issued the attached statement on risk management of client/server computer systems. The statement addresses the risks and fundamental controls associated with a client/server environment. Financial institutions are increasingly placing more emphasis on departmental level client/server computer systems to develop, deliver and maintain critical information systems. Accordingly, it is important for senior management to understand the risks associated with this technology and to implement sound risk management policies, practices and controls for client/server systems.</td>
</tr>
</tbody>
</table>
Apply to ISP

- Bank
- Third Party
- Customer

Risk Assessment

Audit

Policy (ISP)
The Outcome

• What additional benefits does a good IT Risk Assessment give you?
  ◦ Helps you made **DECISIONS**
  ◦ Arms you with information that you can **USE**
  ◦ Guides your decision on where to spend your next security dollar
  ◦ **Drives** your Information Security Program
  ◦ The Information Security Program is the way management demonstrates to regulators that information security is **being managed** at the bank
IT Risk Management Tools

- Efficiency
- Repeatability
- Quality
- Automate processes
- Examiners like them

• Act as your security expert
• Allow bank to spend time examining information and making decisions (not compiling a risk assessment spreadsheet)
<table>
<thead>
<tr>
<th>Company</th>
<th>Website</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archer</td>
<td><a href="http://www.archer-tech.com">www.archer-tech.com</a></td>
<td>Kansas</td>
</tr>
<tr>
<td>bSECURE</td>
<td><a href="http://www.brintech.com">www.brintech.com</a></td>
<td>Texas</td>
</tr>
<tr>
<td>CoNetrix</td>
<td><a href="http://www.conetrix.com">www.conetrix.com</a></td>
<td>Texas</td>
</tr>
<tr>
<td>Modulo</td>
<td><a href="http://www.modulo.com">www.modulo.com</a></td>
<td>Seattle</td>
</tr>
<tr>
<td>Riskkey</td>
<td><a href="http://www.riskkey.com">www.riskkey.com</a></td>
<td>Texas</td>
</tr>
<tr>
<td>RiskWatch</td>
<td><a href="http://www.riskwatch.com">www.riskwatch.com</a></td>
<td>Maryland</td>
</tr>
<tr>
<td>Scout</td>
<td><a href="http://www.locknet-inc.com">www.locknet-inc.com</a></td>
<td>Wisconsin</td>
</tr>
<tr>
<td>TRAC</td>
<td><a href="http://www.protectmybank.com">www.protectmybank.com</a></td>
<td>South Dakota</td>
</tr>
<tr>
<td>WolfPAC</td>
<td><a href="http://www.wolfandco.com">www.wolfandco.com</a></td>
<td>Massachusetts</td>
</tr>
</tbody>
</table>
Components, Expounded

ASSET (PP) × THREAT = INHERENT RISK

INHERENT RISK − MITIGATING CONTROLS = RESIDUAL RISK
1. Inventory: Identify all assets, customers, and third parties (vendors).

2. Develop Priorities: Protection Profiles (CIAV)

3. Identify Threats: What are the threats to each asset (including probability and impact of each threat)?

4. Determine Inherent Risk: Which assets represent risk to the financial institution?

5. System Controls: What system safeguards does the financial institution have implemented?

6. Determine Residual Risk: What is the risk after applying controls?

7. Additional Action Measure Against Goal Identify Controls

8. Demonstrate Compliance: Reporting Improve the process

9. Document Information Security Program: Establish an effective set of IT policies
<table>
<thead>
<tr>
<th>Threat</th>
<th>I</th>
<th>P</th>
<th>TS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized System Access</td>
<td>4</td>
<td>4</td>
<td>18</td>
<td>x</td>
</tr>
<tr>
<td>Unauthorized Transactions</td>
<td>4</td>
<td>4</td>
<td>16</td>
<td>x</td>
</tr>
<tr>
<td>Connection Of Unauthorized Equipment</td>
<td>5</td>
<td>3</td>
<td>15</td>
<td>x</td>
</tr>
<tr>
<td>Skimming</td>
<td>5</td>
<td>3</td>
<td>15</td>
<td>x</td>
</tr>
<tr>
<td>Environmental Incident</td>
<td>3</td>
<td>4</td>
<td>12</td>
<td>x</td>
</tr>
<tr>
<td>Malicious Software</td>
<td>3</td>
<td>4</td>
<td>12</td>
<td>x</td>
</tr>
<tr>
<td>Unlimited Operations</td>
<td>3</td>
<td>4</td>
<td>12</td>
<td>x</td>
</tr>
<tr>
<td>Eavesdropping / Sniffing</td>
<td>5</td>
<td>2</td>
<td>10</td>
<td>x</td>
</tr>
<tr>
<td>Pandemic</td>
<td>5</td>
<td>2</td>
<td>10</td>
<td>x</td>
</tr>
<tr>
<td>Unauthorized Remote Access</td>
<td>5</td>
<td>2</td>
<td>10</td>
<td>x</td>
</tr>
<tr>
<td>Degraded / Unavailable</td>
<td>3</td>
<td>3</td>
<td>9</td>
<td>x</td>
</tr>
<tr>
<td>Unauthorized Physical Access</td>
<td>2</td>
<td>3</td>
<td>6</td>
<td>x</td>
</tr>
<tr>
<td>Unauthorized Viewing</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>x</td>
</tr>
<tr>
<td>Theft</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>x</td>
</tr>
</tbody>
</table>
### Controls (Importance ▼)

<table>
<thead>
<tr>
<th>Control</th>
<th>Implemented</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Enclosure</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Physical Security Awareness</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Formal Patching Process</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Secure Equipment And Cable Placement</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>User Privileges And Restrictions</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Assessment: Administrative Privileges</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Transaction Limits</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Assessment: Basic</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Surveillance Cameras</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Unique User Accounts</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Incident Response Program</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Monitored Location</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Incident Response Program Test</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Disable Unnecessary Services</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Fraud Detection And Monitoring</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Formal Access Review</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Encrypt Transmitted Data</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Firewall: Ingress Filtering</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Administrator Activity Log Monitoring</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Cross-Training</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

0 estimated controls needed to reach the risk mitigation goal of 65%
# IT Risk Assessment - Asset Risk Report

<table>
<thead>
<tr>
<th>Asset</th>
<th>Protection Profile</th>
<th>Total Threat Score</th>
<th>Inherent Risk Score</th>
<th>Residual Risk Score</th>
<th>Percent Mitigated</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Server</td>
<td>11</td>
<td>158</td>
<td>1738</td>
<td>1394</td>
<td>20%</td>
</tr>
<tr>
<td>New Core Banking System</td>
<td>12</td>
<td>185</td>
<td>2220</td>
<td>1193</td>
<td>46%</td>
</tr>
<tr>
<td>Wide Area Network (WAN)</td>
<td>10</td>
<td>128</td>
<td>1280</td>
<td>709</td>
<td>45%</td>
</tr>
<tr>
<td>Core Banking System</td>
<td>12</td>
<td>187</td>
<td>2244</td>
<td>690</td>
<td>69%</td>
</tr>
<tr>
<td>Android Phone</td>
<td>6</td>
<td>156</td>
<td>936</td>
<td>615</td>
<td>34%</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>7</td>
<td>229</td>
<td>1603</td>
<td>562</td>
<td>65%</td>
</tr>
<tr>
<td>Workstation</td>
<td>7</td>
<td>173</td>
<td>1211</td>
<td>548</td>
<td>55%</td>
</tr>
<tr>
<td>Internet Based Mobile Banking</td>
<td>10</td>
<td>156</td>
<td>1560</td>
<td>475</td>
<td>70%</td>
</tr>
<tr>
<td>Sign Workstation (XP)</td>
<td>5</td>
<td>229</td>
<td>1145</td>
<td>454</td>
<td>60%</td>
</tr>
<tr>
<td>Business Online Banking</td>
<td>10</td>
<td>179</td>
<td>1790</td>
<td>451</td>
<td>75%</td>
</tr>
<tr>
<td>Internet Banking</td>
<td>10</td>
<td>166</td>
<td>1660</td>
<td>446</td>
<td>73%</td>
</tr>
<tr>
<td>Desktop Workstation</td>
<td>7</td>
<td>173</td>
<td>1211</td>
<td>399</td>
<td>67%</td>
</tr>
<tr>
<td>ATM Machine</td>
<td>10</td>
<td>152</td>
<td>1520</td>
<td>398</td>
<td>74%</td>
</tr>
<tr>
<td>Application Server</td>
<td>10</td>
<td>161</td>
<td>1610</td>
<td>379</td>
<td>76%</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>8</td>
<td>161</td>
<td>1288</td>
<td>354</td>
<td>73%</td>
</tr>
<tr>
<td>Firewall</td>
<td>11</td>
<td>105</td>
<td>1155</td>
<td>204</td>
<td>82%</td>
</tr>
<tr>
<td>Facebook</td>
<td>5</td>
<td>81</td>
<td>405</td>
<td>197</td>
<td>51%</td>
</tr>
<tr>
<td>Item Imaging System</td>
<td>11</td>
<td>131</td>
<td>1441</td>
<td>195</td>
<td>86%</td>
</tr>
<tr>
<td>Terminal Workstation</td>
<td>7</td>
<td>49</td>
<td>343</td>
<td>174</td>
<td>49%</td>
</tr>
<tr>
<td>VPN Tunnel</td>
<td>9</td>
<td>63</td>
<td>567</td>
<td>132</td>
<td>77%</td>
</tr>
<tr>
<td>Statement Printer</td>
<td>8</td>
<td>34</td>
<td>272</td>
<td>74</td>
<td>73%</td>
</tr>
<tr>
<td>Symantec Amazon (AWS)</td>
<td>8</td>
<td>51</td>
<td>408</td>
<td>51</td>
<td>88%</td>
</tr>
<tr>
<td>Symantec NetBackup</td>
<td>8</td>
<td>29</td>
<td>232</td>
<td>49</td>
<td>79%</td>
</tr>
<tr>
<td>Ironcore Inc</td>
<td>8</td>
<td>44</td>
<td>352</td>
<td>18</td>
<td>95%</td>
</tr>
</tbody>
</table>
Ok, cool... I know my risks. Now what?

- What type of Bank are you?
  - Bleeding Edge
  - Leading Edge
  - “The Pack”
  - Followers

- What’s your IT Strategy?
- What’s your risk appetite?
- Risk Mitigation Strategy!
Risk Mitigation Strategy

• The more important the asset, the more risk you want to reduce.
CATO Risk Assessment

HOW DO I ASSESS THE RISK OF MY CUSTOMERS?
Risk Assessment

**FFIEC:**

Review commercial accounts and identify highest risk accounts, and consider:

- New or changing threats to your services
- Change in customer base
- Change in functionality offered
- Actual incidents from breaches, ID theft, and fraud in the industry or institution

**CSBS:**

**P1.** Expand the risk assessment to include corporate account takeover.

**P2.** Rate each customer (or type of customer) that performs online transactions.
Existing Customer

New Customer

Bank Contact

Customer Data
- Name
- Address
- Contact Info
- Industry Type
- # of Employees
- Avg Monthly Balance
- Online Credit
- Online EFT Services

Inherent Risk Score

Communicate Assessment

Residual Risk Score

Collect Implemented Controls
1. **Inventory:** Identify all assets, customers, and third parties (vendors).

2. **Develop Priorities:** Protection Profiles (CIAV)

3. **Identify Threats:** What are the threats to each asset (including probability and impact of each threat)?

4. **Determine Inherent Risk:** Which assets represent risk to the financial institution?

5. **System Controls:** What system safeguards does the financial institution have implemented?

6. **Determine Residual Risk:** What is the risk after applying controls?

7. **Additional Action:** Measure Against Goal

8. **Demonstrate Compliance:** Reporting
   Improve the process

9. **Document Information Security Program:** Establish an effective set of IT policies
1. Inventory: Identify all commercial customers

2. Develop Priorities: Protection Profiles (CIAV)

3. Identify Threats: What are the threats to each asset (including probability and impact of each threat)?

4. Determine Inherent Risk: Which assets represent risk to the financial institution?

5. System Controls: What system safeguards does the financial institution have implemented?

6. Determine Residual Risk: What is the risk after applying controls?

7. Additional Action Measure Against Goal Identify Controls

8. Demonstrate Compliance: Reporting Improve the process

9. Document Information Security Program: Establish an effective set of IT policies
1) Inventory
2) Develop Priorities
3) Threats
5) Controls

ACH Corporate Customer 2

Standard Questions

1) My organization uses anti-virus and anti-spyware (malware) software:
   - I am not aware of what kind of software we use
   - We do not use this type of software
   - We have it on some computers
   - We have it on all computers but it is not updated on a regular basis and I question the quality of the product
   - We update our software and scan all computers daily with a quality product

2) My organization secures our internet connection with a hardware firewall:
   - I am not aware if we have a hardware firewall
   - We do not use a hardware firewall
   - We have a hardware firewall but I am not sure on its quality
   - We have a commercial grade hardware firewall
   - We have a commercial grade hardware firewall that has all default security settings changed

PAR WACHA ACH

1) Do you know which Standard Entry Class (SEC) codes you are permitted to originate per your agreement?
   - True
   - False

2) Are you aware of and do you follow the specific authorization requirements?
   - True
   - False
Small Business Information Security: The Fundamentals

- October 2009 NIST 7621 was released
- December 2014 proposed update pending
- Assist small business management in understanding how to provide basic security for their information, systems, and networks.
- Provides commercially reasonable security measures which will reduce the likeliness of a security incident.
- Three basic areas which may reduce likeliness:
  - **Absolutely Necessary** (today's focus)
  - Highly Recommended
  - Other Considerations

NIST 7621

1. Malware Protection
2. Hardware Firewall
3. Software Firewall
4. Software/Firmware Patching
5. Data Backup
6. Physical Security
7. Wireless Security
8. Security Awareness Training
9. Unique User Account
10. Limited User Access to Data
1) Malware - Virus, Trojans, Spyware

• If your networks access the internet, then you have risk from Malware (Malicious Software).

<table>
<thead>
<tr>
<th></th>
<th>Q2: Scanned Computers</th>
<th>Infected Computers</th>
<th>Non Infected Computers</th>
<th>Banking Trojans / Password</th>
<th>Downloaders</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>18,321,456</td>
<td>9,215,692</td>
<td>9,105,764</td>
<td>3,220,911</td>
<td>1,533,506</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Symantec – 10/6/2014
Total Malware Signatures – 24 Million
2) Hardware Firewall

• Most small businesses have a broadband (high speed) internet connection which is always “on”. This leaves the network susceptible to network attacks on a 24/7 basis.
3) Software Firewall

• In addition to hardware firewalls, software firewalls should be used on all workstations.
• Software firewalls protect workstations from each other.
• Microsoft provides built in firewall
4) Software Patching

- All operating systems such as Microsoft Windows, Apple OSX, and all distributions of UNIX/Linux have patches that need to be installed on a regular basis.
- Most software products require patches, including Microsoft Office, Adobe, Java, QuickTime, Firefox.
- These patches fix compatibility issues and known security vulnerabilities, not applying them leaves you vulnerable.
5) Backup Data

- Backing up your data protects it from numerous threats:
  - Hackers destroying your computer
  - Malware corrupting your data
  - Fire and other natural disaster destroying your systems
  - Many other threats

- Include all your critical data, backup often.

- Store a copy offsite.

- Test your backup process to know you can restore data.
6) Physical Access Security

- Secure each entrance point
- Monitor areas for unauthorized people
- Escort visitors around the building
- Secure documents, computers, servers from theft
7) Wireless Security

- Do not use wireless unless required for business.
- Securely configure all wireless devices and access points.
- Most users implement with default settings
  - Default passwords - [http://cirt.net/passwords](http://cirt.net/passwords)
- WEP encryption can be hacked in hours (WPA2)
- Security vulnerabilities in wireless technology
  - [www.us-cert.gov/cas/techalerts/TA12-006A.html](http://www.us-cert.gov/cas/techalerts/TA12-006A.html)
- Update wireless software and firmware
- Users connect wireless devices to unsecured wireless, then conduct business.
8) Security Awareness Training

• Employees should read security policies
• Employees should sign Acceptable Use Agreement
• Employees should receive training on security threats:
  ◦ Malware
  ◦ Phishing
  ◦ Social Engineering
  ◦ Unauthorized Access

Email Traffic

- Legitimate Email 11%
- Phishing 15%
- Other Spam 74%
9) Unique User Accounts

- Users should have a unique login to all computers, programs, and websites.
- Users should not be administrators on their local machine. If users can install software, then malware can install itself to the computer when clicked.
- Complex passwords - the password **Spring08** can be cracked with on a normal computer in **24 seconds**.
- Secure Passwords - **73%** of users share the passwords which they use for **online banking**, with at least one **nonfinancial website**.
- If its easy to remember, its easy to guess. Try mnemonics

```
“Proud to be an American” + birth year = PtbaA!(*)
```

where the birth year 1980 is typed in using the shift key.
10) Limit Access to Data

• For all employees, provide access to only those systems and only to the specific information that they need to do their jobs.

• Do not allow a single individual to both initiate and approve a transaction (financial or otherwise).

• Limited access reduces the exposure of data to malware and hackers. Also reduces the impacts of malicious insiders.
Krebs Best Practices


- The surest way to do that is to maintain a clean computer: Start with a fresh install of the operating system and all available security updates, or adopt a “live CD” approach. Other suggestions:
  - Use a **dedicated system** to access the bank’s site.
  - If possible, use something **other than Microsoft** Windows
  - If you must use a multi-purpose machine where you will check email, **avoid clicking links** in email (see previous tip). Also, set **email to display without HTML** formatting if possible.
  - **If you installed it, patch it.** Keep the operating system **up-to-date** with patches. It’s equally important to update the **third-party software** on your system, especially browser plugins.
  - **Remove any unneeded** software from dedicated systems used to access the bank’s site. In particular, unneeded plugins (such as Java) should be junked.
  - **Avoid opening attachments** in email that you were not expecting.
  - **Use a bookmark** to access the bank’s site.
  - Remember that antivirus software is **no substitute for common sense.**
  - If your financial institution offers it, consider taking advantage of **ACH Positive Pay.**
  - **Require two people** to sign off on every transaction.