
Operational Integrity

Cost Effective Security Strategies for Community Banks

	<p>Security Checklist</p> <p>Summary Checklist for Common Issues</p>
--	--

Checklist

This checklist summarizes some common issues that can be addressed by financial institutions to target areas of probable risk. This is meant as a summary of common issues rather than a complete security guide.

LIMIT THREATS AGAINST EXTERNAL GATEWAYS

- Disable Unneeded Modems
- Filter Outbound Traffic
- Validate Firewall Rules

DON'T INVITE THE ENEMY IN

- Use Anti Virus On All Computers
- Use Patch Management Process (either automated software or manual/consistent process)
- Implement Web Content Filtering
- Limit User Rights
 - Don't allow normal users to run as *Administrator*
 - Limit user's installation rights/capabilities

CONTROL REMOTE ACCESS

- Ensure that VPN Uses Complex Passwords / Consider Multi-Factor Authentication
- Log all Remote Access
- Address Remote Access in Security Policy (i.e. home/hotel users)
- Terminate VPN Connections in DMZ

UTILIZE DMZ

- Host Email/Web Server in DMZ
- Filter Traffic from DMZ to LAN

DON'T LET CONFIDENTIAL INFORMATION GO OUT THE FRONT DOOR

- Educate Users on Confidential Information and Email
- Laptops:

- Encrypt Hard Drives
- Don't Cache VPN Authentication Credentials
- Limit Storage of Confidential Data as Practical
- Periodically Review Laptops to Verify Configuration
- Encrypt Backups Stored Offsite
- Implement Plan for Hardware Disposal
 - Computer Hard Drives
 - Tapes, CD ROM's, etc

LACK OF VALIDATION

- Implement Employee Peer Review Process
 - Firewall changes
 - Server deployment, patching
- Verify Vendors are Providing Services According to Contract
 - Outsourced servers: Verify hardening/patch/critical_updates
 - Many are insecure
 - Document shredding companies: Ensure proper document handling
 - Outsourced IT vendors

LIMIT TRUST RELATIONSHIPS WITH PARTNERS

- Terminate Partner Link into Separate DMZ

BUSINESS CONTINUITY CONSIDERATIONS

- Test the Business Continuity Plan
- Make Sure Dates are Current and there are no <INSERT BANK NAME HERE> Tags
- Address Critical Infrastructure, for example:
 - Fedline & Core Banking Application
 - Telephone Systems, Communications Links
 - File Server Data
 - Loan Documents / Information
 - Critical Hardware and Software (replacement file server, etc)
 - Physical Operations Location