

Information Security

Securing Your Infrastructure

Marty Stern
CIO
Texas Capital Bank
m@tcbna.com

Infrastructure Security Components

- ❖ Physical Security
- ❖ Logical Security
- ❖ Communication Security

Physical Security

- ✓ **Restrict Physical Access To:**
- ✓ Server Rooms
- ✓ Wiring Closets
- ✓ File Rooms
- ✓ **Keys:**
 - ✓ Lock Rooms Down
 - ✓ Limit Access To Only Those Who Must Have Access
 - ✓ Monitor and/or Log Access

Logical Security

- CRITICAL COMPONENTS:**
- Written Guidelines & Procedures
 - Security Policy
 - Security Standard
 - Security Guidelines & Procedures
 - Server OS Guidelines & Procedures (One For Each Type)
 - User Training / Social Engineering
 - Strict Application Access Policies
 - Local Access
 - Remote Access
 - Hierarchical File Level Security
 - Operating System Hardening
 - Windows NT/2000 / Novell / Unix / Linux
 - Remove ALL Unnecessary Services
 - Apply All Available Security Patches & Service Packs

Communication Security

- ❖ Firewalls
- ❖ Intrusion Detection Systems
 - ❖ Network Based
 - ❖ Host Based
- ❖ Virus Protection Systems
- ❖ Secure Communication & Encryption

Firewalls

- Install At All External Network Entry Points
 - Internet Connections
 - Application Service Provider (ASP) Connections
 - Vendors and Strategic Partners Connections
- Implement Strict Rule Policies
- Test Rule Sets
- Ensure Immediate Notification Of Critical Alerts
- Create Written Emergency Response Plan
- Test Emergency Response Plan

Intrusion Detection Systems

- Network Based (Monitors Network Traffic)
 - Install At External Network & Critical Subnet Entry Points
 - Internet Connections
 - Application Service Provider (ASP) Connections
 - Vendors and Strategic Partners Connections
- Host Based (Monitors Server Services and/or Logs)
 - Install On All Servers Running Critical Applications or Storing Sensitive Information

Important:

- Ensure Immediate Notification Of Critical Alerts
- Create Written Emergency Response Plan
- Test Emergency Response Plan

Virus Protection Systems

- Special Purpose Protection Systems
 - SMTP (e-Mail)
 - HTTP (Web Browsing)
 - FTP (File Transfers)
 - Attachment Filtering (*.exe, *.bat, etc)
- Application Specific Virus Protection Systems
 - Exchange
 - Lotus Notes
- Server Virus Protection
- Workstation Virus Protection

Important:

- Ensure Daily Updates Of All Virus Signature Files
- Ensure Automatic Updates Of Client Workstations
- Ensure That Anti-Virus Software Cannot Be Disabled By User

Secure Communication & Encryption

Ensure Secure Data Communication To
& From Destinations Outside Your Private
Network

- Virtual Private Networking (VPN)
- Encryption (SSL/PGP)
- Secure Shell (SSH)
- Secure FTP (SFTP)
- Secure Copy (SCP)

“Check List”

- ✓ Annual Risk Assessments
- ✓ Annual Review Of All Guidelines & Procedures

Recommended Minimums:

- ✓ Annual – Internal Security Scans
- ✓ Quarterly – External Security Scans
- ✓ Monthly – Review System Access Privileges
- ✓ Weekly – Review System Logs
- ✓ Daily – Update Virus Signatures