Cyber Security for the “Small” Business
for
NDIA / GoldCoast Conference

Mike Davis,
MSEE, EE, CISSP
mike@sciap.org

Chris Simpson
MS IS, CISSP, SANS Intrusion Analyst
Chris@brightmoonsecurity.com

www.sciap.org/SmallBizSecurity/
www.twitter.com/CyberWarriors

Stop... Think... Connect!
SMB Security Seminar
(specific “how to” details, settings, etc)

1 – Introduction / overview
2 - Regulations / instructions
3- Security Tools
4- Cloud security
5- Mobile devices
6- Wireless
7- Client
8- Server
9- Network / services
10- Web / Browser / apps
11- IA/CND/crypto/key mgmt
12 – C&A overview / facility security
13 - Recovery / incident response
14 – Summary

Detailed topics... each covers:
settings, best practices, & resources
IA / security covers more than Networks

- Land-mobile radio cryptographic and key management systems (high and medium assurance)
- SONAR buoy and other disposable sensor clandestine communications
- Aircraft wireless intercom systems
- Software cryptography (medium & basic) assurance
- Software anti-tamper systems
- RF identification devices (RFID) security
- OPSEC/COMSEC monitoring systems (i.e., email monitoring software)
- Spectrum management inclusion of TRANSEC
- Emanations security (TEMPEST and other vulnerability assessments)
- VoIP integration with E-911 services
- Security markings standards & software
- Open Source software security (freeware and shareware)
- Secure CHAT (XMPP) systems

WE need an enterprise “protections” risk management approach
IA/Security Axioms

to consider / accommodate / educate

• Security and complexity are often inversely proportional.
• Security and usability are often inversely proportional.
• Good security now is better than perfect security never.
• A false sense of security is worse than a true sense of insecurity.
• Your security is only as strong as your weakest link.
• It is best to concentrate on known, probable threats.
• Security is an investment (insurance), not an expense.
• Security is directly related to the education and ethics of your users.
• Security is a people problem - they cause problems, don't just happen.
• Security through obscurity is wrong & We can NOT always add security later

Work through all these in your “Risk Management Plan!”
DoD Security Requirements

- Clinger-Cohen Act (CCA), 1996
- Government Information Security Reform Act (GISRA), 2000
- Federal Information Security Management Act (FISMA), 2002
- OMB Circular A-130, 2000
- DoDD 8500.01E - Information Assurance (IA), April 2007 (changed from 8500.1)
- DoDI 8500.2 - IA Implementation, Feb 03
- DoDI 8580.1 - IA in the Defense Acquisition System, July 04
- Information Assurance Technical Framework (IATF), Sep 2000 (www.iatf.net)
- NSTISSP 11 - National Security Telecommunications and Information Systems Security
- DoDI 8510.01 - DoD Information Assurance Certification and Accreditation (C&A) Process (DIACAP)
- DoDD 5000.1 - The Defense Acquisition System, May 03
- DoDI 5000.2 - Operation of the Defense Acquisition System, May 03
- NIST SP 800-37, “Guide for the Certification and Accreditation (C&A) of Federal Information Systems”
- NIST SP 800-53a - “Guide for Assessing the Security Controls in Federal Information Systems”
- IA documents in general: http://iase.disa.mil/policy-guidance/index.html#DoD

Key resources
https://infosec.navy.mil/docs/index.jsp (requires a CAC)
http://iase.disa.mil/index2.html (has restricted “.mil” in some areas)

More resources / web sites are provided in backup

Proving / verifying security capabilities (C&A) is all about “IA controls”
SANS top 20 controls (ver 3)

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5: Boundary Defense
6: Maintenance, Monitoring, and Analysis of Security Audit Logs
7: Application Software Security
8: Controlled Use of Administrative Privileges
9: Controlled Access Based on the Need to Know
10: Continuous Vulnerability Assessment and Remediation
11: Account Monitoring and Control
12: Malware Defenses
13: Limitation and Control of Network Ports, Protocols, and Services
14: Wireless Device Control
15: Data Loss Prevention
16: Secure Network Engineering
17: Penetration Tests and Red Team Exercises
18: Incident Response Capability
19: Data Recovery Capability
20: Security Skills Assessment and Appropriate Training to Fill Gaps
Security Main Factors
Given ALL these guides - *What MUST WE DO?*

• Implement the **NIST “absolutely necessary” elements** – first and foremost to protect your data (Encryption and back ups)
• **Effective passwords** – still the bane of basic security... and policy is still poor! *(tokens / two-factor IA&A should be used for critical data / processes)*
• **Securing the client, fortifying the browser**... buying trusted business apps, services... *the browser / client is THE largest malware entry point!*
• **Minimal security suite:** antivirus, firewall, connection security (ISP & wireless)
• **Monitoring tools**... need to manage CM/hygiene, track users / data, provide alerts, preplanned SoPs / COOPs, etc
• **Quantify the Insider threat** – quantify actual risks, strict need to know,
• **DATA protection** - encryption and access control - minimize IP loss, data loss prevention
• **A robust and adaptive security strategy = risk management plan (RMP)**
  – to keep pace with the fast-evolving nature of IT security, *including cloud services / SLAs, etc*

*Collectively, with industry, academia and government teaming,*
*we can “implement” small business security effectively / affordably!*
NIST - The “absolutely necessary”
small business security activities to protect information, systems, and networks.

2.1 Protect information/systems/networks from damage by viruses, spyware, and other malicious code.
2.2 Provide security for your Internet connection.
2.3 Install and activate software firewalls on all your business systems.
2.4 Patch your operating systems and applications.
2.5 Make backup copies of important business data/information
2.6 Control physical access to your computers and network components.
2.7 Secure your wireless access point and networks.
2.8 Train your employees in basic security principles.
2.9 Require individual user accounts for each employee on business computers and for business applications.
2.10 Limit employee access to data and information, and limit authority to install software.

NIST - Small Business Information Security: The Fundamentals
Selecting SMB Security Tools

• Selecting the right security tools and finding those tools at a reasonable price is difficult for SMB’s.

• SMB’s should look for tools that:
  – Prevent loss of data to remove potential legal liability
  – Prevent loss of “work hours” removing malware
  – Are free with support or low cost
  – Easy to set up and monitor

• Take the time to properly set up and monitor the tools you choose
How to pick tools

• Read reviews
• Identify assets and data that you want to protect before picking tools
  – NISTIR 7621 Worksheets can help you
• Consider a combination of free and pay
• Consider Software as a Service (SAAS) tools
• Establish budget for purchase, installation and monitoring
• Consider all in one solution or managed security services provider
  – Caveat, single point of failure
• Consider initial cost set up time and maintenance costs
“Must have” SMB Security Tools

• Anti Virus Program
  – NISTIR 7621 2.1 Protect from viruses and malware
  – Best Practices
    • Set up Auto scanning daily
    • Set up email alerts and review logs
    • Use different “brands” for gateways/servers and workstations
    • Use caution if running more than one on computer
    • Make sure has rootkit detector
“Must have” SMB Security Tools

• Firewall (Host and network)
  – NISTIR 7621 2.1 and 2.3 Secure you Internet connection
  – Best Practices
    • Change default passwords
    • Monitor logs and use email alerts
    • Don’t allow any/any
    • Block Unnecessary ports
      – 6667 IRC, unless you use IRC
      – 20/21 FTP
    • Use your PC-based firewall to restrict “cookies” as allowed by your password login websites
    • Use Blacklist service to block known bad IP addresses
    • Update firmware/hardware and software
Router and Firewall Security Configuration

• Enable Intrusion Detection System (IDS). This will detect known high-risk attempted intrusions.
• Log data packets “trying” to go to ports you have closed.
• Enable “Boot Time Protection”. This will prevent attacks on your PC during the sensitive bootup interval.
• Enable “Web Filtering”. This will further restrict hostile content from reaching your PC.
• Enable “Bad Website Filtering”. Websites known to deliver hostile content are blocked.
• Block “VB Scripts”. VB Scripts are often used to deliver hostile content.
• Block “ActiveX Downloads”. Hackers use these powerful small programs to deliver hostile content. NOTE: Many legitimate software programs are themselves ActiveX programs!
“Must have” SMB Security Tools

• Back up and Encrypt sensitive data***
  – NISTIR 7621 2.5 Back up data
  – Best Practices
    • Encrypt data at rest and offsite back up
    • Cloud is ok if encrypted (protect your keys)
    • Rotate back ups

• Workstation and server patching
  – NISTIR 7621 2.4 Patch your operating systems and applications
    • Use built in functionality of Windows and Mac
    • Periodically scan for unpatched machines
    • Don’t forget other software (Java, Adobe, Flash etc)

***DoD Contractors must encrypt sensitive DoD data at rest on mobile devices, including notebook computers
Cloud Overview for SMB

• Benefits
  – Low cost
  – Easy access
  – Flexibility
  – Great for back up
  – Redundancy

• Risks
  – Data loss / compromise
  – No access to data during network outage
  – Data in transit
  – Weak SLAs
  – Unclear location of data
Types of Cloud Services

• Infrastructure as a Service
  – Amazon EC2
  – Rackspace Cloud
**You are responsible for security

• Platform as a Service
  – Amazon SimpleDB
  – Force.com
**Shared security responsibility

• Software as a Service
  – Salesforce.com
**Provider responsible for most of security
**SLA and contracts are critical
SMB Cloud Considerations

- For IAAS same take the same security measures as you do for non cloud servers
- Protect your keys
- Encryption of data in transit and at rest
- Read and understand service level agreements
  - Know service levels
  - Who is responsible for back ups and how they happen
- Know who has access to your data
  - Who on the providers staff
- Consider local back ups and Geo location of your data and jurisdiction
- Is your data movable
  - If you change provider.... Provider goes out of business
- Multi-tenancy
  - Understand how / where you share computing assets

Cloud Security Alliance Guidance - https://cloudsecurityalliance.org/

http://www.sdissa.org/
Mobile Devices

• Risks
  – Loss of device
  – Phishing
  – Data interception
  – Network access by unauthorized devices
  – Malware
    • Embedded in app
    • Social engineering
  – Mixing of personal and company data on personally owned devices which don’t meet company standards
    • People forwarding company email to personally owned device
    • Accessing company data from personally owned device

Mobile Device “Must Dos”

- Set strong password (NISTIR 7621 2.6)
- Encrypt data at rest
  - This is automatic with a password in some devices
- Have enforceable policy on use of personally owned devices
- Conduct training (NISTIR 7621 2.8)
- Use malware detection tools (NISTIR 7621 2.1)
- Separate employee and company data (NISTIR 7621 2.9)
  - Sandboxing
  - Manage native environment for compliance
  - Host data in data center or cloud and access via desktop virtualization

From: Fishnet Security “Securing the Mobile Workforce”
Mobile Device Considerations

• Use mobile device management tool
• Use device tracking tools
• Block network access or use vlan for mobile devices
• Validate app store products
• Endpoint security
  – Anti Malware....  Network access control
• Remote Wipe Capability
• Logging, audit, compliance aspects
• Data leakage controls

Wireless Internet (Wi-Fi) Security Must DO

• **NSTIR 7621 2.7 Secure Your Wireless Access Point and Network**
  – Conduct initial configuration and any configuration changes only when connected via LAN Cable
  – Turn off transmitter when changing configuration
    • Don’t forget to turn back on
  – Turn Off SSID (Network name) Broadcast
  – Change SSID name to something obscure and not related to your business name
  – Select “WPA-2” and “AES” for encryption
  – Older encryption (WEP or WPA/TKIP) is weak and can be broken in minutes
  – Change default administrator username and password
  – Change WiFi “User” password (PSK, or “Pre-Shared Key”)
  – Use strong password and It’s OK to write down password and keep it in a secure place

• These recommendations apply to guest networks and mobile hotspots (MiFi, iPhone etc)
  – Consider separate VLAN for guest access
Wireless Internet (Wi-Fi) Security
Router Security Configuration

• Consider MAC address filtering
• Only allows access to pre-approved systems
• Use Wireless Intrusion Detection/Prevention System
• Use Network Access Control (NAC) System
• Checks for authorized systems, patch level and latest anti-virus updates
Wireless Internet (Wi-Fi) Laptop Security Practices

1. Disable “Automatic Wireless Connections”

2. Disable Wireless “Internet Connection Sharing”. With some operating systems, this feature is always “on”, causing your PC to become a WiFi “Access Point”

3. Connect *manually* to the WiFi network in your business workplace. This means that you should enter your username (SSID) and password (Passphrase) every time you need to wirelessly connect to your corporate computer network - to verify that it matches your company’s stated requirements, such as encryption, to make sure your data is *not* being sent and received in “clear text”.

4. Never connect to WiFi networks with simple SSIDs (WiFi usernames) such as “Free Public WiFi”. Hackers often use high-powered “rogue” WiFi transmitters broadcasting bogus usernames (SSIDs) such as “Free Public WiFi,” “Airport WiFi,” etc. If you connect your WiFi laptop to one of these “rogue” networks your sensitive data will be stolen.

http://www.sdissa.org/
Client-side Vulnerabilities:

Web Browser Protection

• Configuration control is critical
  – Use Active directory or other tools to monitor configurations
• Restrict desktop User browsing privileges to avoid attacks from hostile websites
• Block ActiveX downloads if Internet Explorer is being Used
• Restrict so-called “cookies” (tracking text files)
• Train Users in proper website security practices
• Always update desktop web browser software with newest security updates
• Use pop up blockers and script blocking tools like no script
• Always update Adobe Flash Player, Java and Adobe PDF Reader browser plugins with latest versions
• Never browse the web with an admin account or from servers
• Use multiple browsers, where needed
  – i.e. Internet Explorer for banking and Firefox for general browsing
• Consider a more effective bolt-in access control add-on (re: HP’s free “Polaris”)
Client-side Vulnerabilities:

**Office Software Protection**

- Keep the systems updated with all the latest patches and service packs. If possible enable Automatic Updates on Windows systems.
- Do not open attachments from unknown. Practice caution when opening unexpected e-mail attachments even from known sources.
  - Use content management systems to share files
- To avoid opening documents from unknown web sites do not “click browse”. “Click browsing” is a habit of browsing the web by clicking on links in e-mails or online forums. Use the bookmark feature in every browser to create links to your frequently used web sites.
- Disable the Internet Explorer feature of automatically opening Office documents.
- Configure Outlook and Outlook Express with enhanced security.
- Use intrusion prevention/detection systems and anti-virus and malware detection software to prevent malicious server responses and documents from reaching end users.
- Use mail and web filtering systems at the network perimeter to prevent malicious Office documents from reaching end-user systems.
Client-side Vulnerabilities:

Email Client Protection

• Remove all e-mail client software from production server systems, or where otherwise unnecessary.
• Do not to run any email client on servers or workstations with confidential information unless you use encryption.
• Use the latest version of the email client and enable the automatic update feature provided by the application or operating system.
• Do not run the email client as an administrative user, or other user account with elevated privileges.
  – If you absolutely must run email while logged on as Administrator on Windows system, use tools like Microsoft’s “Drop My Rights” for lowering privileges available to the email application.
• Do not open any email messages from unknown or suspicious sender
• Do not answer junk mail (spam), even if there is an option to unsubscribe
• View email messages as plain text, or with as little formatting as possible: HTML and RTF (two common enhanced formatting schemes for email messages) can allow scripting and other avenues for exploitation
• Do not open any attachments without scanning them first with anti-virus
• Configure your email client to not send return receipts or read confirmations
• For secure email exchange use digital signatures or/and encryption
Server-side Vulnerabilities

Today’s Internet Security Environment For Home/Small Business

• Users Dependent Upon Internet for Personal and Business Communications (Email/Teleconferencing, Skype, Facebook, Twitter, etc)
• Users Dependent Upon Internet for Personal/Business Transactions (Bill Payments, Purchases)
• Increasing Number of Small Businesses Run Partially (or Totally) From Home
• Time and Financial Resources for Cyber Security Measures May Be Limited
• Cybercrime revenues have been increasing rapidly

Increasingly Sophisticated Cybercriminal Attacks: In 2009, one single rogueware network made an estimate $10,800 a day, or approximately $40 million per year

• THE SOLUTION: PROPER SECURITY CONFIGURATION AND USER TRAINING!
Server-side Vulnerabilities:
Web Applications Cross-Site Protection

Network Administrators

• For Internet browsers, disable access to data sources across domains to avoid cross-site scripting attacks.
• Ensure that no un-trusted sites are in the Trusted sites or Local intranet zones as these zones have weaker security settings than the other zones.

Developers

• Validate User textbox input to avoid cross-site scripting attacks
• Follow good application coding security practices

ALL

• Follow OWASP Web / XML security best practices (see followon slide)
Server-side Vulnerabilities:

Web Applications PHP Protection

- Use latest version of PHP
- Develop with the latest PHP release and a hardened configuration (see above)
- Validate all input according to the variable type it is being assigned
- Follow OWASP (Open Web Application Security Project) secure coding guidance (more details on a later slide)
- Test your apps using the OWASP Testing Guide with tools like WebScarab, Firefox's Web Developer Toolbar, Greasemonkey, and the XSS Assistant
- Use a testing environment and test applications before deploying
- Train/hire developers with security experience and certifications
Server-side Vulnerabilities:

Server Virtualization Protection

- Follow same practices for securing real machines as virtualized
- Machines
- Monitor v-switches and virtual network
- Segment network based on data protection requirements
- Principle of least privilege – unnecessary services turned off,
  necessary services reduced in privileges
- Require secure user authentication when accessing resources across the network
- Secure backup and disaster recovery resources from internal attack
- Encrypt communications across your virtualized network
- Encrypt “virtual snapshots”
Server-side Vulnerabilities: Backup Software Protection

ALWAYS IMPLEMENT PRINCIPLE OF LEAST PRIVILEGE!

• Ensure the latest vendor supplied software patches are installed on the clients and servers.
• The ports being used by backup software should be firewalled from any untrusted network, especially the Internet.
• Data should be encrypted when stored on backup media and while being transported across the network.
• Host- or network-based firewalls should be run to limit the accessibility of a system's backup software to ensure that only the appropriate backup hosts can communicate on the backup server ports.
• Segregate your network to create a separate backup network VLAN.
• Backup media should be stored, tracked and monitored like other IT assets to deter and detect theft or loss.
• Backup media should be securely erased, or physically destroyed at the end of its useful life.
Server-side Vulnerabilities

Management Servers Protection

• Keep the systems updated with all the latest patches and service packs. If provided, use an automatic update system.

• Use Intrusion Prevention/Detection Systems to prevent/detect attacks exploiting these vulnerabilities.

• Ensure that only authorized users and systems have access to these systems - THE PRINCIPLE OF LEAST PRIVILEGE!

• Collect and monitor log data
Server-side Vulnerabilities:

Database Software Protection

- Ensure that all DBMS patches are up to date.
- Remove/change default passwords on the database's privileged and system accounts before deploying the system on the network. Lists of default accounts are readily available on the Internet.
- Rotate passwords
- Use minimal privileges.
- Use stored procedures where possible. Remove/disable unnecessary stored procedures.
- Set length limits on any form fields to minimize the possibility of buffer overflow attacks.
- Use database activity monitoring tools
  - They operate independently of the DBMS
- Encrypt database
Cybercriminal’s Ultimate Weapon: The BOTNET: Army of Zombie Computers

DEFINITION: A botnet consists of:

1. A least one “bot server”, often an Internet Relay Chat (IRC) server, acting as a command and control center. IRC is a simple interactive protocol that facilitates two-way communications. Existing IRC servers are easy to access, easy to construct, and are linked together to achieve redundancy.

2. An army, or “botherd” of infected target botnet client computers, referred to as “zombies” or “drones”, that obediently stay in contact with the bot server and obey its commands.

BOTNET ACTIVITY: Theft of sensitive data, Distributed Denial of Service (DDoS) attacks, directed at specified financial or national/political targets. Deactivation of Antivirus software on the infected system.

APTs – advanced persistent threats
The bane of poor security hygiene / controls!
Minimizing the risk of Extortionware

“Extortionware” is a now rampant form of malware, usually a Trojan virus, that is automatically downloaded when visiting a “corrupt” web page or after clicking on a document or link within a corrupt email. The extortionware, true to its name, behaves as follows:

1. A bogus “Virus Infection warning! You must buy our product to disinfect your PC!” message is constantly (and annoyingly) displayed.
2. Your PC’s existing AV software is immediately crippled. Internet access usually still works.
3. A message appears demanding that you pay about $300 via credit card using the extortionist’s conveniently available form. After payment, the attackers graciously will download their AV “cure” to your PC – and then proceed to sell your credit card information to their criminal network.

THE SOLUTION: Visit www.malwarebytes.org and download and install the free version of “Malwarebytes” AV software. Then, run Malwarebytes and update it to the newest version, then scan your entire PC. Remove the detected viruses, then reboot your PC.
Email Security Configuration

• Use the latest version of the email client (such as Thunderbird) and enable the automatic update feature provided by the application or operating system.

• Use Anti-Virus (AV) software with the latest update (virus signatures). Configure the anti-virus software to monitor files in real-time if possible, and configure automatic daily update of AV software, if possible.

• TRAIN ALL USERS TO QUESTION ALL HYPERLINKS WITHIN EMAILS
  — AS AN OPTION, TRAIN USERS AND EMPLOYEES TO COPY SUSPECT LINKS AND PASTE INTO SEARCH ENGINES FOLLOWED BY THE EXPRESSION “COMPLAINTS”

• Remove all e-mail client software from production server systems, or where otherwise unnecessary
Browser and Web Surfing Security

“COOKIE” Management:

**Persistent Cookies**, as the same implies, expire several years into the future! They are often referred to as “tracking cookies” because they provide Internet usage information. They are a potential security and privacy risk.

**3rd Party Cookies** are also small text files that reside on your PC. 3rd party cookies are generated by entities other than the primary owner of the website you are visiting. 3rd party content is used extensively throughout the Web, particularly in news sites. 3rd party cookies are also required by some password-protected websites.

- Follow best practices from CERT, Microsoft and Mozilla
- Automate with active directory or scripting
- Things to consider
  - History
  - Notifications
  - Pop up blocking
Browser and Web Surfing Security

OWASP Top Ten Web/XML Risks

1: Injection
2: Cross-Site Scripting (XSS)
3: Broken Authentication and Session Management
4: Insecure Direct Object References
5: Cross-Site Request Forgery (CSRF)
6: Security Misconfiguration
7: Insecure Cryptographic Storage
8: Failure to Restrict URL Access
9: Insufficient Transport Layer Protection
10: Unvalidated Redirects and Forwards

Mitigating OWASP top 10 without any code

OWASP Top 10 And Security Flaw Root Causes
http://www.slideshare.net/marco_morana/owasp-top-10-and-security-flaws

Application Abuse:
The World of Web 2.0

Instant Messaging, Social Media, Facebook, Twitter etc

- Protect like other applications
  - Patching
  - User training
  - Monitoring
- Same risks as email like social engineering, phishing, bogus links etc
- Possible source of data leakage from malicious insider
- Malware -- Worms, viruses, and Trojans transferred through instant Messaging.
- Data not encrypted in transit
- Another way to get into your systems
- Don’t use with admin/privileged account
Application Abuse:
The World of Web 2.0

PEER-TO-PEER (P2P) MUSIC / FILE SHARING PROGRAMS: RISKS
- Illegal sharing of copyrighted material or confidential data
- Exposure of users to unwanted illicit content
- Distribution and execution of malware (viruses, spyware, bots, etc.)
- Network overload
- Network surveillance by cybercriminals

IMPLEMENT PRINCIPLE OF LEAST PRIVILEGE!
- Turn on Egress filtering
- Use Data Loss prevention tools
- Monitor Firewall and Intrusion Detection System logs, including outbound
- Disable the Simple File Sharing feature (Windows XP)
- Monitor system for presence of unknown executables and unauthorized modification of system files
Top 25 SW development errors

[1] Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[2] Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[3] Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4] Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[7] Use of Hard-coded Credentials
[8] Missing Encryption of Sensitive Data
[9] Unrestricted Upload of File with Dangerous Type
[10] Reliance on Untrusted Inputs in a Security Decision
[12] Cross-Site Request Forgery (CSRF)
[13] Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[14] Download of Code Without Integrity Check
[15] Incorrect Authorization
[16] Inclusion of Functionality from Untrusted Control Sphere
[17] Incorrect Permission Assignment for Critical Resource
[18] Use of Potentially Dangerous Function
[19] Use of a Broken or Risky Cryptographic Algorithm
[20] Incorrect Calculation of Buffer Size
[21] Improper Restriction of Excessive Authentication Attempts
[22] URL Redirection to Untrusted Site ('Open Redirect')
[23] Uncontrolled Format String
[24] Integer Overflow or Wraparound
[25] Use of a One-Way Hash without a Salt

http://cwe.mitre.org/top25/
Minimizing Network Attacks

• Configure systems, from the first day, with the most secure configuration that your business functionality will allow, and use automation to keep users from installing/uninstalling software

• Use automation to make sure systems maintain their secure configuration, remain fully patched with the latest version of the software (including Java SE and anti-virus software updates)

• Use proxies on your border network, configuring all client services (HTTP, HTTPS, FTP, DNS, etc.) so that they have to pass through the proxies to get to the Internet

• Allow for filtering and monitoring

• Protect sensitive data through encryption, data classification mapped against access control, and through automated data leakage protection
IA/CND/crypto (FW, IDS, etc) - Overview

A whole extensive disciple by itself... the basic tools / systems are:

IA = information assurance – covers the whole protection continuum = “C I A N A = confidentiality, integrity, availability, nonrepudiation and authentication”

CND = Computer network defense = an overall capability set focused on network protection through a suite of integrated IA programs.
Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction

Encryption - a fundamental protection capability, not hard, but you need a top down strategy. Where the harder part is key management (rotation, escrow, etc)

Firewall – covered earlier, but you must have one, best to have a host and network version, there are many types, but KISS is best for SOHO

IDS – intrusion detection system – like it sounds, this monitors for abnormal, unauthorized activity and transactions... checking for things that got past the FW
IPS – protection - The active version of an IDS, can take actions to limit transactions
IA / CND Examples

• **Encryption**
  - [PGP Freeware](http://thesecuritynetwork.org/) offers basic PGP encryption capability for messages and files, but does not include many features available in other PGP products. There are versions available for both Windows and Mac environments
  - [File Buddy](http://www.sdissa.org/) – the encryption used by File Buddy has no known successful attacks against it.
  - [Iron Key](http://thesecuritynetwork.org/) - is a program for encrypting files, that you can safely send over the Internet. The encrypted file is a self-extracting executable - your correspondent must run it and enter the right password for decrypting. No crypto software needs to be installed on the receiving side!

• **IDS**
  - [SNORT](http://thesecuritynetwork.org/) - is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection (Snort is the most widely deployed IDS/IPS technology worldwide)
  - [Prevx Home](http://thesecuritynetwork.org/) - helps minimize computer users vulnerability to each new (‘Zero Day’) cyber-attack during the critical period between the launch of a new attack and a “signature” update becoming available.
  - [AIDE](http://thesecuritynetwork.org/) (Advanced Intrusion Detection Environment) is a free replacement for Tripwire., It does the same things as the semi-free Tripwire and more.
Same rules apply to Mac!
More built in, and easier to implement

Mac OS X Built-in Security aspects
http://www.apple.com/macosx/what-is/security.html

Mac OS X Security configuration guides
https://ssl.apple.com/support/security/guides/

The truth about APPLE security
Macs are plagued with as many (and sometimes more) vulnerabilities as other operating systems. These are the doors attackers use to exploit our systems, and Macs are far from invulnerable. But in the real world, Macs suffer from far fewer compromises

Mac Security Threats: How Vulnerable Is Apple?
http://www.time.com/time/business/article/0,8599,2075218,00.html
Mac Protector is real, ... So is it time for Mac aficionados to admit defeat and install security software? ... Some are running utilities from Symantec and Sophos. The vast majority, however, including professional savants like Macworld editors, said they still don’t.....

Experts weigh in on Mac vs. PC security
ESET released the results of a survey in November related to awareness of cybercrime in the U.S. More than 1,000 people responded that while both PC and Mac users perceive the Mac as being safer, Mac users are victims of cybercrime just as frequently as PC users.

http://www.thexlab.com/faqs/malspyware.html

Ensure your Mac security set-ups are indeed adequate, common

http://www.sdissa.org/
DoD C&A (DIACAP)

“C&A” Package = System Identification profile (SIP), Implementation Plan, Certification Documentation, Scorecard, and POA&M.
Certification Procedure - Facilities

• For most DoD components, facilities and systems processing National Security Information must follow procedures for TEMPEST certification.
• As a part of the certification procedure, some facilities and systems are required to have a TEMPEST countermeasures evaluation as well.
  — However, this does not mean that all facilities and systems must implement TEMPEST countermeasures.
• Certified TEMPEST Technical Authorities (CTTAs) are U.S. government employees that:
  — Perform TEMPEST countermeasures evaluations
  — Determine the TEMPEST requirements
  — Recommend TEMPEST countermeasures.
• Program Managers should not implement TEMPEST countermeasures that entail a significant cost without the recommendation of a CTTA.
• CTTAs can also assist in the design of systems or facilities, and validate TEMPEST countermeasures.

Facility security – get a SME, they know the rules (same as in C&A!)
Recovery / incident response

Why Bother?

- Cost recovery and damages
- Effectively terminating a corrupt employee
- Good cyber-citizenship and domain leadership
- Due diligence, CYA in liability, legal process
- Avoid ending up on a cyber-mooch list (easy pickings)
- Support FBI, US CERT, etc in data collection to stop hackers, nation states - build new rules / laws
- California Civil Code section 1798.81.5
What Will This Cost?

• Hardware/Software
  – Image or retain hard drives from employees who leave under less than amicable circumstances or who had access to confidential data
  – Take offline or image and then restore from backup compromised servers

• Invest in strong backup technology to include offline storage of important computer and network logs.

• Invest in basic training in IT security for your IT staff or retain an IT consultant with security skills who can be available in an emergency.

• Create acceptable computer use policies and procedures and disseminate to all employees

• Optional: IT Security Audit; system upgrades; incident response planning.
What do I do BEFORE attacked?

• Have IT staff enable computer and network logging and actually READ the logs
• Have backups and logs stored offline – (can’t change them!)
• Treat every cyber-incident as potentially malicious until it is determined that it is not
• Regularly confirm compliance with policies and procedures
• Consistently backup data and test that backup worked
• Train end-users
• Plan for incident response, have a written checklist

BTW, Got your identity stolen? Contact the ID theft resource center
1 (888) 400-5530 http://www.idtheftcenter.org/

http://www.sdissa.org/
What do I do AFTER hacked?

• Preserve the original compromised system's hard drives if possible, and provide documentation on anything that has been done to the system since the discovery of the incident. MUST show “chain of custody” of digital evidence!!!

• Provide copies of any network diagrams or system documentation showing the environment in which the system operated. And.. identify and provide copies of any externally generated log files, such as intrusion detection system or firewall logs.

• Consider monitoring the system's network connections prior to taking it offline. Other compromised systems or suspect Internet protocol addresses can frequently be identified.

Industrial Controls cyber incident response  (great overall and in depth practices)

Company cyber security incident response checklist

Your company TEAM makeup (lawyer, et al)

Computer Security Incident Response Team (CSIRT) FAQs
http://www.cert.org/csirts/csirt_faq.html

FIRST = Forum for Incident Response and Security Teams (full listing)
http://www.first.org/about/organization/teams/

More Cyber security incident response templates / tips

In SD, Contact local FBI cyber team 858.565.1255 / 858.499.7991.
IA / Security “Best Practices” Overview

(Best practices are not a panacea, complete or only what you need to do – but a decent guide)

– Quantify your business protection needs – do you have an asset inventory?
– Determine what is “good enough” or minimally acceptable
– Quantify your environment’s threats and vulnerabilities
  • your list should have 10 – 50 or so threats assessed
– Have a security policy that’s useful, complete, CEO/leadership endorsed
  • yes, that’s actually HAVE A POLICY, choose a model, then enforce it too!
– Run self-assessment on security measures (use accepted tests, STIGs, etc) and compliance (HIPAA, PCI, CFR, SOX, etc)
– Training and awareness programs – much needed, but not a guarantee
– TEST your continuity, recovery plans, backup – have you ever you restored?
– Encrypt where you can - asses where / how you need it : IM, e-mail, file transfer, storage, backup, etc
– Be familiar with the “NIST” IA/Security series – they are very useful!
– Always use capabilities from approved / preferred products lists (A/PPLs)
– A risk management plan (RMP) should roll all these into one effort

As, you can somewhat control what you plan,
but you usually ONLY get what you enforce!
Reducing SM Business Cyber Risks

ANY IA/security environment or capability should include these top-ten elements to ensure a well-integrated and “best value” data & system protection approach.

1 - Comprehensive **security policy**  
2 - Distribute **clear governance**  
3 - Build in **defense-in-depth**  
4 – Follow a **strategy**, master plan  
5 - **Configuration management**  
6 - Develop an effective **tool suite**  
7 - Guard major **threat entry points**  
8 - Guard **malware entry methods**  
9 - **Test** critical elements  
10 – **Risk management plan**

(and communication & **enforcement**)  
(R&R, resources, swim lanes, ROE)  
(PC to POP, several layers, enterprise CND...)  
(use key business metrics in decisions)  
(automated reporting -> **enforcement**)  
(use **APLs**, use automation / suites, USCERT, etc)  
(phased attacks, root kit, APTs, Phishing)  
(browser, content filters, Block URLs)  
(COOPs, **backup**, compliance, vulnerabilities)  
(current threats, vulnerabilities and impacts)

*define what is “good enough” or minimally acceptable  
minimize what you don’t know you don’t know*

*Doing the basics well; collaborate;  
THEN monitor / control / **enforce**!*
FREE / Low Cost Products to Support NIST Guidance

2.1 Protect information/systems/networks from damage by viruses, spyware, and other malicious code.

Antivirus
Microsoft Security Essentials (suite)

Malware Bytes (Removal tool)
http://www.malwarebytes.org/


2.2 Provide security for your Internet connection.

Astaro Security Gateway Essential Firewall Edition

Intrusion Detection System
Snort http://www.snort.org/

2.3 Install and activate software firewalls on all your business systems.

Built into Windows and Mac
Zone Alarm

2.4 Patch your operating systems and applications.

Microsoft Security Baseline Analyzer

Nessus http://www.nessus.org/products/nessus

http://www.sdissa.org/
FREE / Low Cost Products

2.10 Limit employee access to data and information, and limit authority to install software.

TrueCrypt
http://www.truecrypt.org/

Built in to Windows and Mac

Logging
Snare

Event Log Explorer
http://www.eventlogxp.com/

Splunk (Up to a certain storage limit)
http://www.splunk.com/

Reviews and comparisons
http://sectools.org/
http://www.av-comparatives.org/
http://netsecurity.about.com/od/freesecuritytools/Free_Tools_and_Utillities_To_Help_You_Secure_Your_Computer_or_Network.htm

(we have a companion paper with more details, products, links, etc)
Not all Security Tools Are Equal!

Do the research on products before you buy... even FREE may not be a good deal!

**MALWARE / Antivirus** Products need to improve – some more dramatically than others. Tested products slipped performance by 6% on average from 2009 to 2010. And the notion that —you’re fine as long as you keep your AV updated - is completely false. Note that in most cases we found considerable differences between a vendor’s corporate product and their consumer version. It is not safe to assume the results are identical


- Malware protection is far from commodity, *with effectiveness ranging between 54% and 90%, a 36% spread.*
- Cybercriminals have between a 10% - 45% chance of getting past your AV with Web Malware (depending on the product).
- Cybercriminals have between 25% - 97% chance of compromising your machine using exploits (depending on the product).
- Expect use of exploits to increase since it is far more effective than traditional malware

**Browsers** are not equal either... turns out IE9 is much better than most...


Summary

Q&A

Do the security basics ASAP

Engage a security group, get started!

For more information - contact

Security, Cyber and IA Professionals

Mike@sciap.org
Glenn@sciap.org
Chris@brightmoonsecurity.com

www.sciap.org/ SmallBizSecurity/
IA/security resources

Main IA and C&A sites

https://infosec.navy.mil/docs/index.jsp


http://iase.disa.mil/ditscap/

Other IA/Security sites:

https://www.us.army.mil/suite/portal/index.jsp

http://csrc.nist.gov/

http://www.nsa.gov/ia/index.cfm

http://www.iatf.net/

Other IA/Security sites (cont):

http://www.cert.org/

http://www.sse-cmm.org/lib/lib.asp

http://www.commoncriteriaportal.org/


https://www.sans.org/about/sans.php

http://iac.dtic.mil/iatac/

http://www.cerias.purdue.edu/

http://security.sdsc.edu/


http://www.sdissa.org/
Preferred Product Lists (PPL)

Generally programs should strive to use PPL devices / processes in building their systems. Other than the type-1 COMSEC devices, which require individual certification letters held by the companies, the list below is probably the 90% solution without getting industry groups such as ICSA labs.

- **NIST FIPS 140 certifications**: http://csrc.nist.gov/groups/STM/cmvp/index.html
- **NIST algorithm certifications**: http://csrc.nist.gov/groups/STM/cavp/index.html
- **NIAP/Common Criteria**: http://niap.bahialab.com/cc-scheme/
- **DISA IASE**: http://iase.disa.mil/index2.html
- **NSA IAD**: http://www.nsa.gov/ia/index.cfm

**NOTE** - A PPL list can range from algorithms to specific equipment configurations. For example, one radio might have FIPS approval when ordered using model number 123 and an NSA type-1 certification when ordered using model number 456. Same is true for a router, IPS,... Yet even if a device has a CC EAL-4 certification, you still need to ensure that the protection profile used and the security target meets your specific application.