How to be Cyber Safe!

Maximize your security level – protect yourself and clients too!

NDIA
SMB Cyber *(and more)*

15 May, 2015

Moderated by:
Mike Davis
http://**ACMEcyber**.com/home/

Chris Simpson
http://**brightmoonsecurity**.com

Bottom Line Up Front (*BLUF*)

1 – Use decent **passwords** (use a pass phrase to construct it). Don't use the same passwords on other accounts (as once they hack one account, your others will fall too).

2 – **Encrypt** your data! (we suggest free sources).

3 – **Separate work and personal space / accounts**: (work data is much less likely to be hacked)
Best to use 2computers at home = (1) general use (kids / web browse, etc) and (2) work / financial. Protect #2 with tight security controls and don't web surf – do business only.
Two different accounts with logical separation works, is less effective the separate PCs.

4 – Use the **free security tools** your ISP / cable provider offers, then add other free tools.

5 – Your **mobile phone** is an extension of your office – and most likely a very easy threat vector to hack and get into your accounts. Follow the mobile security guides and best practices .

6 – **Back up your data onsite and offsite** – cloud based back will provide quicker recovery. This includes home computers (Don't want to lose your family photos).

7 – **Wireless** – select strong encryption (WPA2) , don't broadcast SSID and change the default password. On FREE wireless - assume it's unsecure (FYI - in southern San Diego over half the access points are owned by one Mexican criminal). Generally never use 'free Wi-Fi.

Your computer is your job – protect them both!

Overall precautions and security/privacy good habits

This is great list of habits for personal and business protections! Common sense ways to be cyber safe – and go beyond just the PC security we cover below. *''AS You ARE going to get hacked!''* (…if not already)(…well at least your data will be)

1. Enable some form of credit monitoring
2. Subscribe to a personal credit and reputation monitoring services: LifeLock, Reputation.com
3. Close all old and non-used internet accounts.
4. Subscribe to a data reduction service such as Abine DELETE M

5. Setup GOOGLE ALERTS to key on your name, username and email
6. Keep your home systems secure with anti-virus, firewall, and privacy protection
7. Backup your data! - This is extremely important with ransomware
8. Subscribe to your bank notifications for any transaction to email you or text you as they occur
9. Go through your credit report at least 2 times a year.
10. Reduce giving out your information as much as possible to retailers
11. Know and understand the privacy implications of mobile social apps

12. Be careful and cognizant of social media contacts on ALL sites
13. NEVER open unusual looking or unsolicited email that you can not recognize
14. Enable two factor authentication (2FA) for all social sites https://twofactorauth.org/
15. Buy a SHREDDER, and USE IT.
16. Turn off your devices and systems when you do not need them on
17. Connect to only trusted WIFI hotspots. Do not enable Bluetooth unless needed.

https://www.linkedin.com/today/post/article/20140926230113-113107450-you-are-going-to-get-hacked

You MUST have a security policy

YES, you need a simple policy even at home

(for the kids, family, anyone using those PC/internet resources (for those of you who did a 'driving contract' with your kids – same principle applies here).

Remote employees, SOHO, small and medium business (SMB), etc must have a security policy to feed cyber safe practices (of course so does everyone else)

As policy drives requirements and processes.

Never start from scratch, l*everage good practices*! State of Delaware has almost every policy a business needs!!!

https://dti.delaware.gov/information/standards-policies.shtml

The SANS (a major security group) has many policy examples, they more specifically cover cyber security.

http://www.sans.org/security-resources/policies/

Individuals, remote workers, SOHO and SMB cyber safe set-up guides.

Several good overall guidance articles exist – skim them to see the overall cyber security guidance / key steps:
https://www.sba.gov/blogs/**9-cyber-security-tips-small-business**-owners
http://www.zdnet.com/article/**10-security-best-practice-guidelines-for-businesses/**

These links have other suggestions to configure your PC / SOHO / SMB clients.
https://www.dhs.gov/sites/default/files/publications/**FCC**%20**Cybersecurity**%20**Planning**%20**Guide**_1.pdf
http://windowsitpro.com/networking/**8-steps-secure-soho**

Passwords – they are still quite useful – especially "IF" well-constructed (and you don't need to change them a lot either, if strong).
You have heard that the best method is to use a "pass phrase" (some short catchy few words that only you know). Then use the first letter of words, with numbers and symbols in-between, start and end. *These are easy additional rules to follow*:
https://blogs.mcafee.com/consumer/**15-tips-to-better-password-security**

For sensitive data – strongly consider adding in **two-factor-equivalent** methods:
E.g., many banks use a 6 digit PIN sent as a text for a 'session" key – EASY!

Encrypt!

This may seem obvious, but very few folks actually DO it in practice.

FYI - the California Attorney General's # 1 privacy recommendation? ***Encrypt****, encrypt,* encrypt = protects your data, minimizes liability too!

Ponemon Institute released their second annual study on corporate data breach preparedness – so DO IT!

http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

So, what are some of the better free / low cost encryption tools?

Use OS tools: Bitlocker & FileVault. Or free tools: Open GPG, AcCrypt, or from these sites– just pick one & use it!

http://www.gfi.com/blog/the-top-24-free-tools-for-data-encryption/

http://listoffreeware.com/list-best-free-file-encryption-software/

BTW - Do you have a "cyber go bag" – e.g., scanned all your key / personal documents and uploaded into your cloud?

Firewalls – Cable / ISP and home router

USE your ISP / Cable firewall and the one in your home router. First change the password – do not leave it as the default. (and as we'll suggest later, use the other security tools your ISP provides for free too).

There are free firewalls you can use as well. Just pick one and USE it! (Caveat – not all cyber programs interact well.)
http://www.pcmag.com/article2/0,2817,2422144,00.asp

BTW… IF you have an older router at home, OR need more BW (who doesn't?) Check out this ASUS RT-AC68U gigabit wireless router with firewall. While a consumer level product – it has extensive built in firewall / malware protection. Where even if you get a "bot" behind the network, *it* ***prevents outgoing connections*** *to command and control nodes*! Get this feature in your router! http://www.asus.com/support/FAQ/1008719/

cyber security suite

USE an integrated cyber security suite.

Your ISP offers a free one! MS essentials is also good good (built into later windows OS). Again, always use the FREE cyber suite your ISP / cable company provides.

For the most part the key action here is to just turn on and configure the one that come with the OS and ISP!

BTW, a quick scan for best cyber suite brings up this list (where in this case "BitDefender" was rated No 1.)

http://internet-security-suite-review.toptenreviews.com/small-business-internet-security/

Regardless if you use your home computer for work, it's also **YOUR computer / DATA**; thus **buy** a decent cyber suite for your home PC, as they are inexpensive and also use the free security tools listed herein for home use.

http://finance.yahoo.com/news/spyhunter-voted-best-antivirus-anti-153400129.html

Add separate anti-virus host / PC tools

two FREE anti-virus suites are **SOHOS & AVG.**

https://secure2.sophos.com/en-us/Pages/DownloadRedirect.aspx?downloadKey=e793e22e-34d9-4fac-9f8d-f7a6371ae802

http://download.cnet.com/AVG-AntiVirus-Free-2015/3001-2239_4-10320142.html?hlndr=1&part=dl-avg_free_us

NOTE –keep selecting the FREE version, as they try to have you select the 'free trial' version of the paid product. The free version contains the same signature base for virus detection, so you're only adding bells and whistles.

A couple of other well-known free assessment tools are: **"CCcleaner" and "Ad-aware"**

https://www.piriform.com/ccleaner/download/standard

http://www.lavasoft.com/download/adaware_download.php?lang=en&inter=3875_1009709_digitalrivercomparativelp_null_null_null&src=free_install

Set up your browsers for maximum protection

--- **Firefox** – tighten the browser controls to the max… so web sites can't capture your info - and use this browser as your main one, unless it won't work on a site.

https://support.mozilla.org/en-US/products/firefox/privacy-and-security

--- **Chrome** – you can lighten up on the security controls here a bit so you can get it to work on more sites.

https://support.google.com/chrome/answer/114836?hl=en

--- Overall browser security setting support / guidance for all three

https://www.veracode.com/blog/2013/03/browser-security-settings-for-chrome-firefox-and-internet-explorer

SOHO / SMBs must go further **to minimize the browser threat vector**

We know the browser is "THE" malware threat vector entry point

Upwards of 80% of malware comes through the browser. Where of course all those files are downloaded using HTTPS; so files are encrypted right to the end device - bypassing the cyber suite..;-((R*ecommendations to reduce the browser threat space in your SMB / SOHO*!

Tighten up your **browser controls** - especially limit active code (JAVA, Active-X, etc). As recommended above, disable most tracking functions, put the browser into "guest" mode (or equivalent) and force all files to the same user download directory to be automatically scanned.

Then use '**white listing**' for both applications (require certs to run) and URL / web sites (this greatly minimizes access to infected IP addresses and most phishing vectors too) http://en.wikipedia.org/wiki/Whitelist

And then **disable executables** from being installed on end devices by users (e.g., require privileged / SysAdmin rights to add software), this makes sure any files put on end devices cannot load / execute (aka, malware / rootkits).

DO these steps and you have **greatly minimized the impact / risks of the browser threat vector**!

Wireless

Typically supplied by your ISP, router or separate device – Always select the strongest encryption (WPA2), disable SSID broadcast, and use a strong password.

Best to use cable / ISP / wired connections at home.

As for free wireless – generally assume it's unsecure. Best to not use them to be on the safe side, even as with VPNs, etc the risk is lower.

Essentially hackers set up shop in SBX & airports with fake access points that transmit they are the free wireless point. So once you log on, they have your passwords, etc. You can review the dangers here:
http://safeandsavvy.f-secure.com/2014/09/29/danger-of-public-wifi/

There are several good set-up guides / support that are easy to use:
http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm
http://lifehacker.com/the-most-important-security-settings-to-change-on-your-1573958554

GAO report on mobile vulnerabilities

KEY *risks* / concerns:

- Mobile devices often do not have passwords enabled.
- Two-factor authentication is not always used when conducting sensitive transactions.
- Wireless transmissions are not always encrypted.
- Mobile devices may contain malware.
- Mobile devices often do not use security software.
- Operating systems may be out-of-date.
- Software / patches on mobile devices may be out-of-date.
- Mobile devices often do not limit Internet connections. Many mobile devices do not have firewalls to limit connections.
- Mobile devices may have unauthorized modifications. (known as "jailbreaking" or "rooting")
- Communication channels / Bluetooth may be poorly secured.

--- BYOD is NOT 'freee / cheap' ---

Major *protection* methods:

Enable user authentication: Enable two-factor authentication for sensitive transactions: Verify the authenticity of downloaded applications: Install antimalware and a firewall: Install security updates: Remotely disable lost or stolen devices: Enable encryption for data on any device or memory card: Enable whitelisting *(on phones too!)* : Establish a mobile device security policy: Provide mobile device security training: Establish a deployment plan: Perform risk assessments: **Manage hygiene = configuration control and management**:

http://www.networkworld.com/news/2012/091912-mobile-security-262581.html

Mobile Security Practices

1. **Use a pin**, password or pattern to lock your phone.
2. Download apps only from trusted stores.

The McAfee® SiteAdvisor® with the Verizon Mobile Security app can help assess app activities.

3. Back up your data.

With Verizon's Backup Assistant Plus and Verizon Cloud, for example, you can save your contacts, music, pictures, videos and documents to the cloud.

4. Keep your operating system and apps updated.
5. Use a mobile A/V app (or two)
6. Use a secure messaging / text app
7. Log out of sites after you make a payment.
8. Turn off Wi-Fi and Bluetooth® when not in use.
9. Avoid giving out personal information (texts can be sent elsewhere!)
10 . Install a security app.

Verizon Mobile Security includes free protection from viruses and malware—all powered by McAfee. For a monthly fee, *you can upgrade to Premium Security*: you'll get App Alert to learn what personal data your apps are accessing and recovery features to remotely locate, lock, alarm or wipe a lost or misplaced device.

11. Protect your investment, consider replacement insurance

Cloud Security Factoids

The cloud security challenges are principally based on:

a. Trusting vendor's security model
b. Customer inability to respond to audit findings
c. Obtaining support for investigations
d. Indirect administrator accountability
e. Proprietary implementations can't be examined
f. Loss of physical control

Areas that will mature soon, enhancing enterprise risk management (*re: Gartner*):

- Consensus on what constitutes the most significant risks,
- Cloud services certification standards,
- Virtual machine governance and control (*orchestration*),
- Enterprise control over logging and investigation,
- Content-based control within SaaS and PaaS, and
- Cloud security gateways, security "add-ons" based in proxy services

Cloud Security Alliance (CSA) nine critical threats:

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

We recommend following both the **NIST and CSA cloud guidance**:

https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf
http://csrc.nist.gov/publications/PubsSPs.html

AND an overall, *enterprise, e2e, risk management approach* (e.g., RMF & FedRAMP)

Cloud Security Summary

Security in the cloud is **likely better than you have in-house**

* Security is the **SAME** everywhere – '*WHO does which*' IA controls changes

* Few are "all in" the cloud @ 100% - Hence **TWO** environments **to manage**

* ALL must use the same **cloud security *standard*s** (and QA in SLA)
http://www.sciap.org/blog1/wp-content/uploads/Cloud-Security-Standards-SEP-20131.xlsx

* Implement **SCM / SIEM** – *integrate cloud metrics* / status (& QA the SLAs)

* **S**ervice **L**evel **A**greements (SLA) not sufficient – trust but verify (*Orchestration SW* ?)

* **Encrypt** everywhere - Yes more key management, but risks greatly reduced

* Data owners always accountable for PII / privacy / compliance (& *location*)

* *Update Risk management Plan (**RMP**)* = Comms, COOP…. with *cloud R&R*
http://media.amazonwebservices.com/**AWS_Risk_and_Compliance_Whitepaper.**pdf

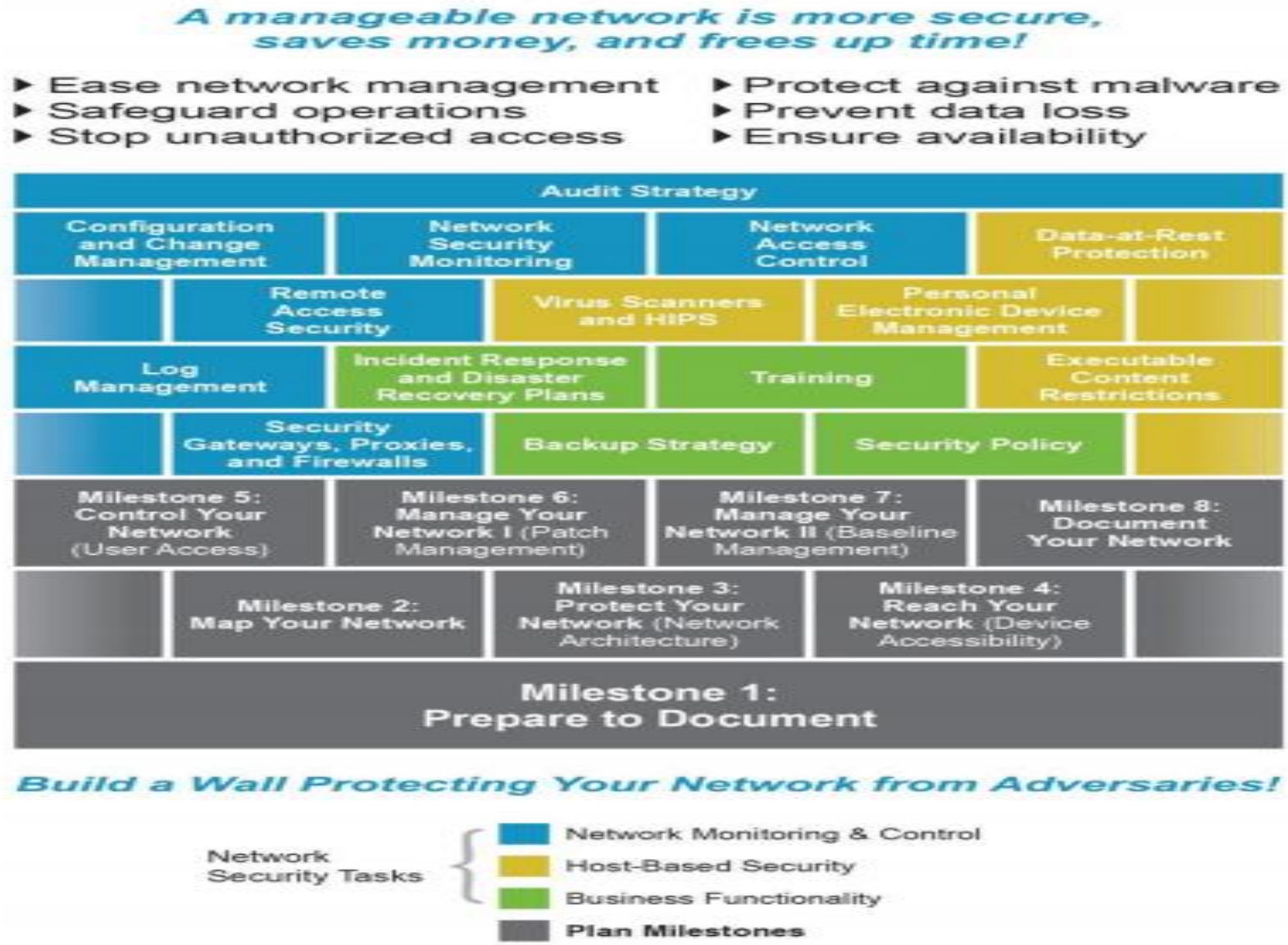
For more details see paper: **Cloud Security – What really matters?**
At http://www.sciap.org/blog1/ (under *Cyber Body of Knowledge)*

Tips for Avoiding Social Engineering from US-CERT

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly.

Source: https://www.us-cert.gov/ncas/tips/ST04-014

START by Building a Manageable Network – including clients.



Many of these functions map to NIST 800-53 controls

Source: https://www.nsa.gov/ia/_files/vtechrep/**ManageableNetworkPla**n.pdf

So how do you KNOW what your security posture / baseline actually is?

Knowing your security baseline is really JOB ONE for your cyber safe approach.

Security posture and impacts can be invisible to most, unless you have the right tools and someone who knows how to read and interpret them correctly (e.g., separate out the false positives from critical vulnerabilities for example).

The best, most assured way to know your baseline is to have an independent security expert do a vulnerability scan, using an authoritative reference of what's critical in security (for example, the NIST Framework and SMB security publication).

--- There are self-assessments to use – which help you be aware of your general security posture at least - answer the questions as best you can for your 'approximate' cyber status – the holes / vulnerabilities will be quite apparent!

The Cyber Security Evaluation Tool (CSET) is from the DHS

https://ics-cert.us-cert.gov/Assessments

US-CERT - DHS - Cyber Resilience Review (CRR) (this is a self-assessment package)

http://www.us-cert.gov/sites/default/files/c3vp/csc-crr-self-assessment-package.pdf

NIST Security Self-Assessment Guide (based on 800-53)

http://csrc.nist.gov/groups/SMA/fisma/documents/Security-Controls-Assessment-Form_022807.pdf

Top-Level guidance / recommendations

Our "CISO Fundamentals / Cybersecurity Essentials" paper is one place to start.
An introduction page with the cyber background, where the 2nd page provides a specific dozen or so recommendations for an affordable, effective and "due diligence" set of cyber tenets.
http://www.sciap.org/blog1/wp-content/uploads/CISO-Fundamentals.pdf

• Employ **well proven security products**, which entails at least: anti-virus, firewall, VPN, IDS, encryption (with robust key management) and SCM (note - buy security programs from only formal, approved product lists).
• **Continuously monitor, manage mitigate and automate** your IT/security baseline (use tools, dashboards) – the key here is "visibility" – KNOW your security environment - as you can't manage what you don't see.

FIVE key 'operational" activities can reduce security incidents by well over 90%:

- O Effective application upgrade and patch management (track and prioritize business apps);
- O Controlling network and data access (enforce "least privilege" & minimal privileged accounts);
- O Application whitelisting / secure configurations (software certs needed to execute);
- O Current hardware and software inventories (with the current versions / IOS / patches); and
- O Employing SCM / SIEM (on premise and the cloud – effective monitoring SLAs).

• **Secure backup** is paramount, using multiple locations – most storage should be encrypted, and address cloud security in SLAs. **Encrypt all data** at rest and data in motion (internet / wireless / external connections).

Top-Level guidance / recommendations (cont)

"CISO Fundamentals / Cybersecurity Essentials" paper recommendations (continued)

• **Manage access to the company**, both physical and virtual - use strong passwords, changing periodically - consider a token/biometrics for sensitive data. *Strictly limit "privileged access."*

• As IP / data defines your business, **focus on data security, privacy by design** – categorize it and know where it is – use "Data Loss Prevention (DLP) / Data Rights Management (DRM) " to manage access and track key data.

• Proactively **manage business risk using your RMP**, complemented with a well-communicated, **enforced security policy**. ---- Use a **cyber insurance policy** to transfer known accepted and unknown risks - base coverage on a risk assessment (*ISO 27000 series*) – use the insurance policy to harmonize management, broker and counsel.

• Robust resiliency and recovery –a **Business Continuity Plan** – and an incident response plan.

• Provide ongoing training and education on security awareness and business risks, tailored to all key stakeholders**. Make the training personal**, with natural work applications, as it will last longer.

• **KNOW your security status / metrics** – periodically, independently test and assess the: security suite, ongoing processes including back-ups, security policy enforcement, and all major elements in your RMP.

• *What about forensics, ethical hackers, etc* – of course, just do the basics well first, then work damage control.

Detailed guidance / recommendations

For an in-depth set of key security recommendations (distilled from our "CISO Fundamentals" paper), and how to best to execute them, review our our **"Executing an effective security program."** It includes several examples of a 90-100 day timeline - with added recommendations / points on each key cyber tenet – all in 3 pages ("it's in there!"). With these priority tasks, hints and resources, your effective, prioritized, security plan is almost written.

http://www.sciap.org/blog1/wp-content/uploads/Executing-an-effective-security-plan.pdf

Epilog - For an overall small business security approach - **skim this NIST 7621 pub**. As always, NIST has a great pub on small business security. Make it a point to read this and "just DO IT" – that is, implement their absolutely necessary" security steps – and - for added measure and security also implement their "highly recommended" steps. *DOING these 11 + 10 or so activities gets you as close to a formal "**due diligence**" level of security as you can get*!!!

http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf

Summary

1 – Use effective passwords

2 – Encrypt ALL your data!

3 – Separate accounts - work and personal. 2 computers is safest.

4 – Free security tools your ISP / cable offers, add other free tools.

5 – Protect your mobile phone (it's your data too)

6 – Wireless – Strong encryption, avoid free wireless

7 – Firewalls / anti-virus

8 – Security policy

9 – **KNOW your baseline**

10 – **Remote workers are a critical weak link!**

11 - Prevention is not enough:

Active and continuous monitoring… what's on that remote PC?

Conduct your own OSINT / Consider Threat Intelligence tools

Make it easy for employees to report cybersecurity incidents

12 – Manage to your **Enterprise Risk Management plan**!!

Questions / Challenges / Other viewpoints!!!

Cyber security URLs / links of interest..

Major cyber / IA sites

https://infosec.navy.mil
http://www.doncio.navy.mil/TagResults.aspx?ID=28
http://iase.disa.mil/Pages/index.aspx
http://csrc.nist.gov/publications/PubsSPs.html
http://www.nsa.gov/ia/index.shtml
https://cve.mitre.org/
http://www.cisecurity.org/
http://www.cert.org/
http://www.commoncriteriaportal.org/
https://www.thecsiac.com/resources/all
http://www.dhs.gov/topic/cybersecurity
http://iase.disa.mil/stigs/Pages/index.aspx
http://niccs.us-cert.gov/
https://www.sans.org/programs/
http://www.cerias.purdue.edu/
https://www.cccure.org/
http://www.rmf.org/
http://nvd.nist.gov/

Others of interest

https://www.cool.navy.mil
http://www.threatstop.com/
http://www.darkreading.com/
http://www-03.ibm.com/security/xforce/
http://www.iso27001security.com/
http://iac.dtic.mil/csiac/ia_policychart.html
http://www.nascio.org/

Mike.davis.sd@gmail.com

some training sites:

http://doc.opensuse.org/products/draft/SLES/SLES-security_sd_draft/cha.aide.html
http://iase.disa.mil/eta/online-catalog.html#fsotools
http://iase.disa.mil/eta/cyberchallenge/launchPage.htm
http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html
http://www.microsoft.com/security/sdl/default.aspx