MINNESOTA COUNCIL OF NONPROFITS

Nonprofit Technology & Communications Conference
16 March 2012, 10.30-11.45am

Security on a Shoestring Budget

Matthew J. Harmon
Natascha Shawver
IT Risk Limited, LLC

IT RISK LIMITED

Hello!

- Matthew J. Harmon & Natascha E. Shawver
- Matthew has been doing this since the early 90's
- Natascha has been working with non-profits on technology projects since 2002

Why we are here today.

- Raise awareness on what impact lack of security could have for your organizations mission and why risk matters to decision making
- Explain why security is not exclusively a matter of money
- Help you to reduce organizational risk and improve resiliency

What we are going to talk about...

- Information security principles & commonly used terms
- Introduction to fundamental security techniques
- Methods to improve your overall security posture

...and what not.

- We're not here to sell you any of the products mentioned, they just happen to be what we use and we like them.
- People are afraid of what they don't know. We want to change that for you.

Terms and Definitions

- **Impact:**
  To have an effect upon the confidentiality, integrity or availability of an asset

- **Risk:**
  Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. [NIST 800-30]
  ... or how long can you get away without patching before something bad happens. [MJH]

Reference: Federal Information Processing Standard (FIPS) 199. 2004. http://csrc.nist.gov/publications/fips
Source: NIST Special Publication 800-30 "Risk Management Guide for Information Technology Systems"

Terms and Definitions

- **Threat (or threat agent):**
  Anything that is capable of acting against an asset in a manner that can result in harm. [FAIR]
  The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. [NIATEC]
  A threat agent has Capability, Intent and History [OWASP]

- **Vulnerability:**
  A weakness that could be exploited by a threat. The presence of a vulnerability does not in itself cause harm. [NIATEC]

National Information Assurance Training and Education Center (NIATEC) niatec.info
Factor Analysis of Information Risk (FAIR) fairwiki.riskmanagementinsight.com
Open Web Application Security Project (OWASP) https://www.owasp.org/index.php/Category:Threat_Agent

Terms and Definitions

- **Controls:** Measures taken to prevent, correct or detect a threat.

National Information Assurance Training and Education Center (NIATEC) niatec.info
Factor Analysis of Information Risk (FAIR) fairwiki.riskmanagementinsight.com
Open Web Application Security Project (OWASP) https://www.owasp.org/index.php/Category:Threat_Agent

So why security?

Attacks put your mission at risk:

- Loss of reputation
- Loss of funding
- Loss of members
- Loss of productivity
- Loss of organizational memory
- Legal consequences
- Fines for compliance violations

Information Security Fundamentals

- Information security is more than just "computer stuff"
- Why security through obscurity is bad
- Confidentiality, Integrity and Availability

Information Security Fundamentals *ctd.*

- Knowledge is everything - ask yourself:
  - What are you protecting?
  - What are you protecting it from?
  - Why are you protecting it?
  - What are your options?
  - Is the protection effective?

So what SHOULD I be doing?

The list may seem endless, but there is hope.

- The following list are the bare necessities, a merged list of NIST and SANS, simplified to make them applicable
- Tackle one item every couple of weeks
- Use the attached worksheets to find your most vulnerable assets

https://www.sans.org/critical-security-controls/

#0. Start writing down your passwords. Safely.

We all have a ridiculous number of passwords to remember. Or do we? I don't know most of mine.

- Use a tool such as LastPass, Password Safe or KeePass.
- Two-factor authentication doesn't have to be hard.
- Also... enable account lockout after a reasonable number of attempts. Even a value as high as 10, if you frequently mistype, will significantly inhibit brute force attempts.
- Since you don't need to remember your password anymore, change it every season or so
- See if YubiKey would work for you.

http://yubico.com/yubikey

#1: Create an asset inventory & identify your important information types

Know what you are trying to protect

- Inventory of Authorized (and Unauthorized) Devices
- Inventory of Authorized (and Unauthorized) Software
- Inventory of information types you are trying to protect
- Spreadsheets work well, no need to get fancy
- Needed for financial audits anyway

Example...

ASSET	Make & Model	Serial #	Operating System	Location & Owner	Last updated	Data stored on device
Desktops						
Laptops						
Software						
Peripherals						

#2: Secure your internet connection

Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

- Establish a secure perimeter.
- Enable the security features on the existing hardware from your ISP.
- Change the default passwords
- Use unique passwords for all your devices

nvd.nist.gov sans.org have configuration checklists

#3: Secure your Wireless

When using wireless (WiFi) use WPA2 with AES

- WEP or "Wired-Equivalent Privacy" is easy to compromise.
- Disable "SSID Broadcast" to hide your network
- Keep track of the devices connected to your wireless just as you would people working in your office.

#4: Defend against malware

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

- This is a tricky one. Don't blow your whole budget on anti-virus. Training people to not do things that put them at risk is much more effective.
- Microsoft Security Essentials - free and effective.
- VirusTotal.com, virusscan.jotti.org, www.metascan-online.com for checking one-off files

#4: Defend against malware

- This cute kitten is harboring malicious code.
  No anti-virus engine found it and no fancy tricks were used to hide it. It is a test string called EICAR.
- Only go to sites you know and trust. Use a "guest" computer for Facebook and going to new sites.
- If in doubt: Disable JavaScript.
- If it sounds too good to be true, it is. Just accept that.
- If you **must** use AV, use tools with the least impact such as ESET NOD32 or Microsoft Security Essentials

#5: Secure your network

Turn on the software firewall on workstations and servers.

- If you have the budget, install a hardware firewall directly behind your ISP's modem/router.
- Open source solutions such as pfSense, Smoothwall and Untangle can be installed on inexpensive hardware
- "Unified Threat Management" is the new term for a firewall that does a lot more. WatchGuard and SonicWall both deliver quality UTM devices.

#6: Patch & update

Patch your operating systems and applications on a regular schedule.

- Enable Auto-Update where possible
- Enable Software Update and Check for Updates: Weekly
- Check your current state with Secunia PSI or CSI.
- Most vulnerabilities today are in client side software such as Acrobat Reader, Java, Internet Explorer, Safari, Firefox

#7: Make (automated) backups

Make sure you have backup copies of important business data/information.

Make sure you know how to recover from backups.

- An external USB drive works well. Store it off-site.
- A file server is not a backup server, it is a file server
- Backups should be off-line and scanned for malicious code
- Use the built in tools such as Apple Time Machine and Microsoft's Backup Utility
- If you need your backups online, use a service like rsync.net

#8: Limit physical access

Control physical access to your computers and network components, and other sensitive assets.

- Change locks on doors if there is an issue, change PINs regularly
- Have a machine set aside for guests to use
- Build guest accounts with timed auto-logout

#9: Limit user access

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

- Day-to-day user accounts should not have administrator rights.
- Restrict access to financial data and personnel data and don't carry it around with you.
- Limiting "rogue installations" helps support your asset inventory

#10: Limit user privileges

Require individual user accounts for each employee on business computers and for business applications.

- Each individual should have their own account.
- Every time you share your password you are authorizing someone to impersonate you.

#11: Educate yourself about email security and how to behave online

- Only open attachments from people you know
- Don't click on links in emails from people you don't know
- Don't download applications/documents from untrusted sources
- Make sure your staff knows how to use the internet/social media safely
- If it sounds too good to be true, it is.

#12: Dispose of old equipment (and data!) safely

- Erase hard drives before discarding them, wipe computers before given them to the next employee or to goodwill

- Shred documents containing sensitive data

#13: Have a disaster recovery plan

Have a recovery plan in place, should an emergency occur despite your best efforts and make sure people know how to access it.

- Know who to contact (in-house staff, vendors, etc.)
- Know where your backups are
- Prepare for physical disasters as well (flood, fire, tornado, etc.), or contingencies (power outage, sewer backup)

#14: Have policies and procedures in place

Define acceptable and unacceptable practices and expectations for employees and general business when using your equipment and network.

#15: Beware of social engineering

- Train your staff & have policies and guidelines in place
- Do some social engineering yourself to see where your weak spots are
- Don’t send sensitive info over email, don’t give it out over the phone either
- Be a friendly nosy nelly and check out peoples story

#16: Train your staff and volunteers

Train your staff and volunteers in basic security principles as they apply to your organization.

- Brown bag lunch to introduce staff to your security policies

- Industry groups such as: ISSA, the Small Business Association, and SANS have local one-on-one training

#17: Know what your allies & vendors are doing

Make sure your allies & third party vendors adhere to the same standards you set for yourself.

- Data you share with allies/volunteers should be handled with care
- Web hosting/email hosting/cloud based applications: confirm that your vendors store your data safely
- Contract review allowing auditing, data security policies, check privacy policy

Final comments

As non-profits, you do quite a bit of strategic thinking already, start doing that for technology, too.

Security doesn't have to be expensive. There are a lot of best practices & common sense things you can implement to make you much safer.

Tailor your security efforts around your needs, i.e. the data you need to protect.

You don't need to change over night, you just need to take the first step.

IT Risk Limted, LLC

matthew@itriskltd.com
natascha@itriskltd.com

IT Risk Ltd. performs IT risk assessments, advanced security testing, incident response,
IT Security Training,
leads security research and participates in international standards development,
and if you couldn't tell, we are passionate about what we do.

Thank you!

Questions?

I hope you enjoyed this presentation, it can be downloaded after the Conference from:

https://github.com/itriskltd

SAMPLE WORKSHEET 1 -
Asset Inventory

ASSET	Make & Model	Serial #	Operating System	Location & Owner	Last updated	Data stored on device
Desktops						
Laptops						
Software						
Peripherals						

SAMPLE WORKSHEET 2 - Identify and prioritize your organizations information types

Priority	Type of information	Stored where?
1	*Membership list*	*With third party vendor*
2	*Individual donors list*	*Spreadsheet on Sarah's laptop*
3	*Employee & Vendor records with SS#s and EINs*	*Unlocked file cabinet*
4	...	...

Identify and prioritize information types

- What information is used by your organization?
- Where is it located?
- What is its priority?

SAMPLE WORKSHEET 3 -
Identify the needed protection for your organizations information types

Priority	Type of information	C	I	A
1	*Funder database*			*x*
2	*Employee files*	*x*		
3	*Credit card receipts from a fundraiser*	*x*		
4	*Membership list*	*x*	*x*	*x*

Identify and prioritize information types

- What information is used by your organization?
- What is its priority in the organization?
- What are you trying to protect? Confidentiality, Integrity, or Availability?

SAMPLE WORKSHEET 4 -
Identify the cost from bad things happening to your important information - monetary and otherwise

	<data type> Problem: data released	<data type> Problem: data modified	<data type> Problem: data lost
Cost of revelation			
Cost of lost availability			
Cost of repair/replacement			
Legal costs/fines			
Cost of loss of confidence			
Cost of loss of productivity			

- What important information is used by your organization?
- What is the cost to the organization should something bad happen to this information?