



Cyber Security for Non-Profit Organizations

Scott Lawler
CISSP-ISSAP, ISSMP, HCISPP



May 2015



Agenda

- IT Security Basics
- e-Discovery
- Compliance
- Legal Risk
- Disaster Plans
- Non-Profit Cyber Security Issues
- What should you do?



Protecting Tomorrow – Non-Profit

PROTECTING TOMORROW'S GENERATIONS

– Our volunteers provide real solutions to protect our children from cyber threats in school and at home

PROTECTING TOMORROW'S COMMUNITIES

– Educate women, small and medium size businesses, and help Veterans transition into cyber warriors to fight the online cyber battle

PROTECTING TOMORROW'S TECHNOLOGIES

-- New technologies are exciting and sometimes disturbing. We find ways to protect America's emerging and discriminating innovations.



<http://www.protectingtomorrow.org>



IT Security Lifecycle Basics

Inventory Assets

Hardware, software, mobile devices, communications links, processes, procedures, checklists, documents, contacts, donor lists

Identify Risk

Create discrepancy reports and act on them

Remediate Risk

Assign actions and close them

Monitor and triage alerts

Continuous analysis and support

Execute and Test Backups

Data, configurations, processes documentation





Cyber Criminals – No Rules!

- 2015 Verizon Data Breach Investigations Report

“estimated financial loss from 700 million compromised records is \$400 million and that the most common attack vector continues to be compromised credentials”

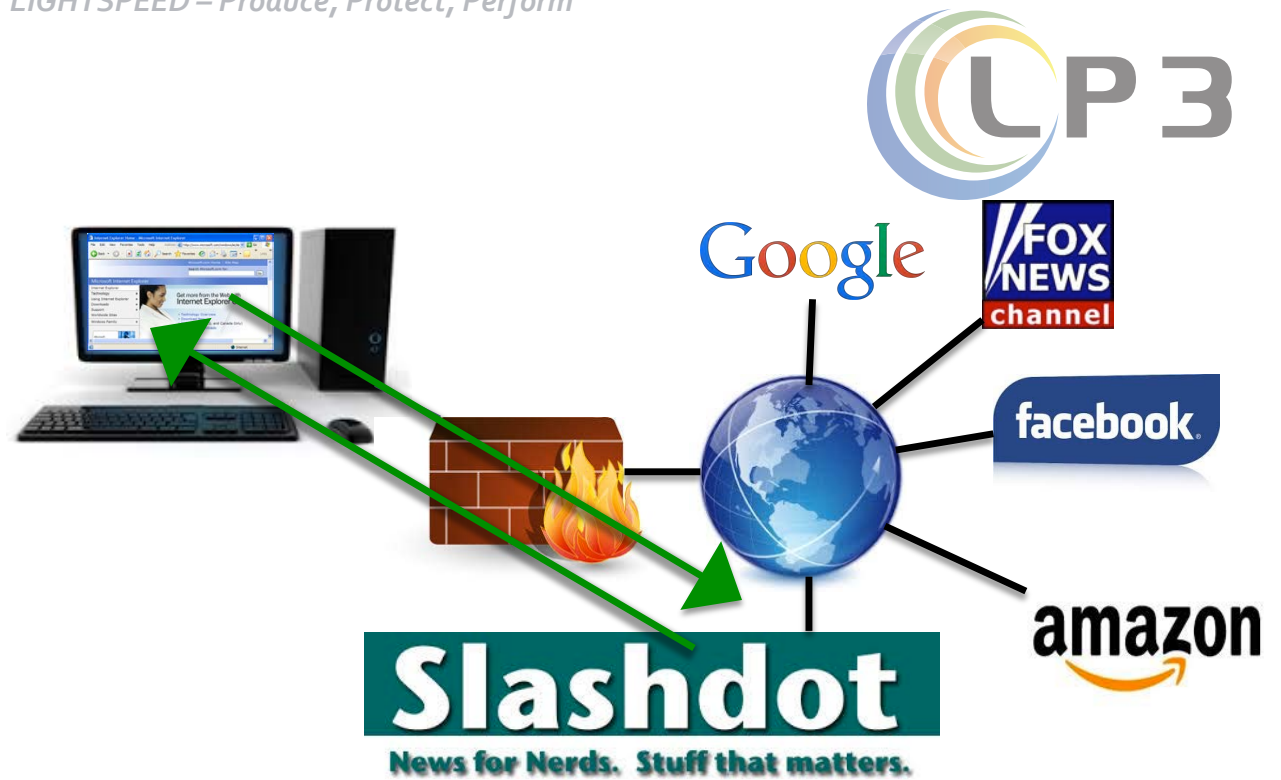
- Critical non-profit issues
 - Reputation – key donor information
 - Fines/penalties – Privacy violations, HIPAA/HITECH
 - Litigation – identity theft, negligence, due diligence
 - Compliance
 - Continuity of Operations



“60% of the small businesses victimized by a cyber attack closed permanently within six months”

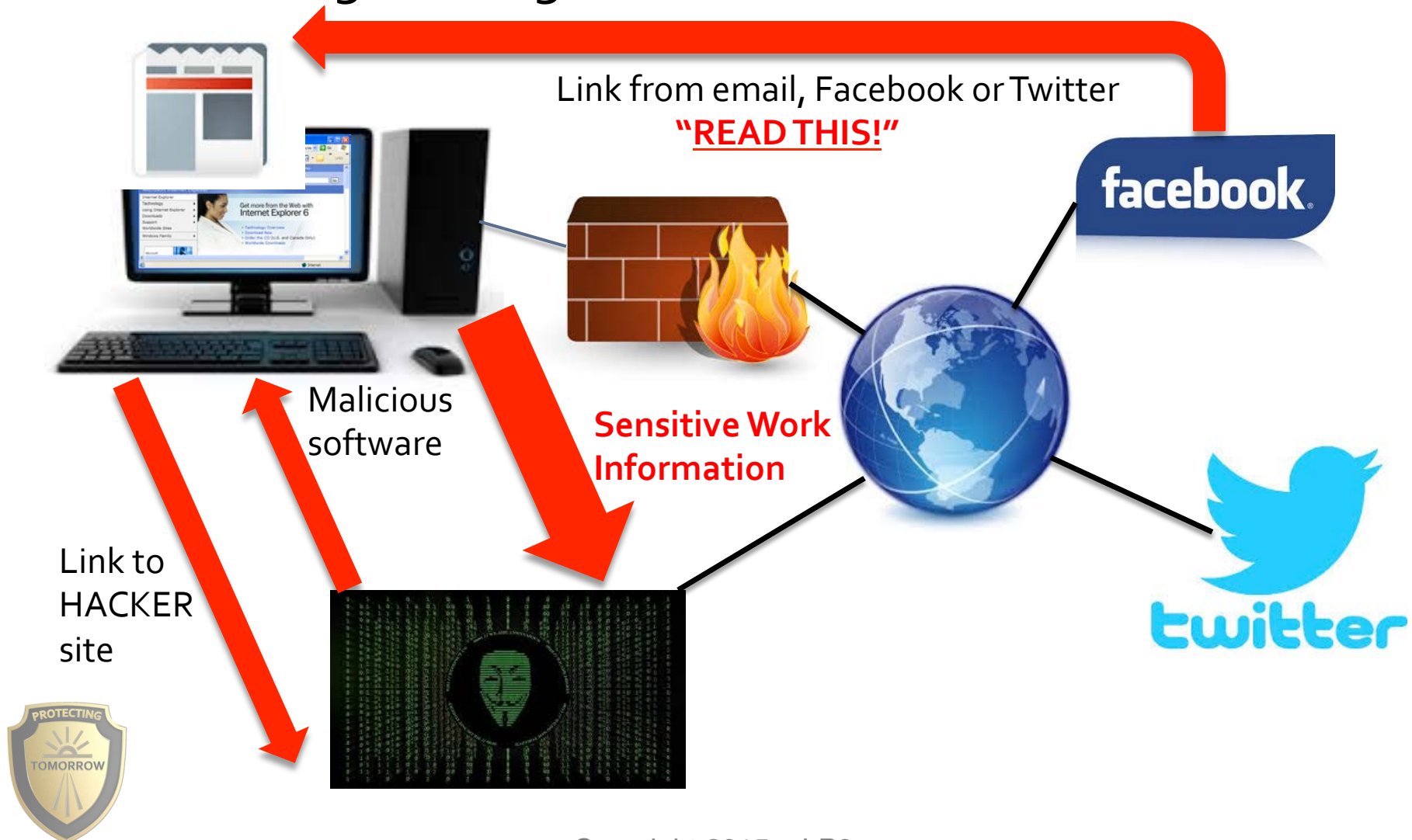
Web Surfing

- How it works



Web Surfing at Work

- What can go wrong?

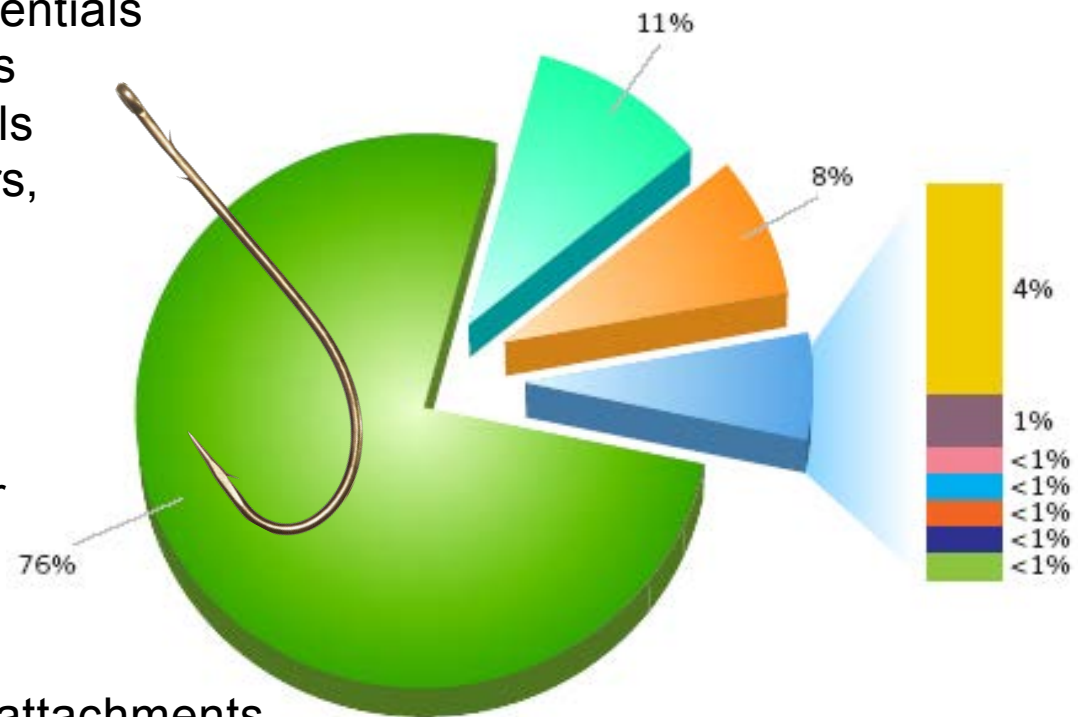




Phishing

- Fake emails seeking to get credentials
- Financial assets: 76% of targets
- Spear phishing – by-name emails
 - Executives, key decision makers, celebrities, names on website

Red Flag Words: account locked, suspended, verification required, suspicious transaction, protect your computer, funds due to you



Countermeasures:

- Don't click on emailed links and attachments
- ONE careless person can compromise the entire organization
- **Security Awareness Training**





Documents Safe Online?



Work server

Home computer



“full take,” “bulk access” and “high volume” operations on Yahoo and Google networks. (WashPost, 4 Nov 13)



Google Drive



iCloud



Dropbox

Countermeasures:

- Encrypt data and know where it goes
- Use redundant automated backups and test them





ABA Formal Op 08-451

Model Rule 1.6: “...prevent...unauthorized disclosure...”

I Agree

“When you upload...you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works...communicate, publish, publically perform, publically display, and distribute...”

Google Drive



How do hackers crack businesses?

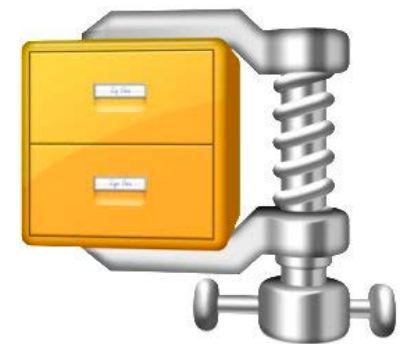


[“click here”](#) emails

Business Associate Connections

Social Engineering: “Please reset my password!”

Mr. Smith is yelling at me to get this proposal in now!”



Thumb Drives – The Truth

Key business risks

- Can carry large volume of sensitive data out very easily
- Carry in malicious code bypassing firewalls, content filtering, anti-virus scanning
- Encrypted USB – still have same security issues
- Best to not use them
- Turn OFF & use alerts



e-Discovery Risk

What is it?

- Mandated electronic discovery in litigation or investigations with electronically stored information (ESI)

Deliver all documents with the name "John Smith" or "Company XYZ" from 2008 to 2014...

Why do I care?

- If you cannot find documents and metadata then you may lose the case – significant financial risk

e-Discovery Actions

What should I do?

1. Identify
2. Preserve and ~~Retain~~
3. Collect
4. Process
5. Review
6. Produce



PCI (Payment Card Industry) Data Security Standards (DSS)

WHAT:

Standards and requirements for payment card data security
Non-legislative – enforceable through fines and penalties
Obligation on merchants and service providers



WHO:

“Payment Card Industry (PCI) Data security requirements apply to all Members (banks), merchants and service providers that store, process or transmit cardholder data.”

HOW:

Sensitive authentication data cannot be stored
Cardholder data must be protected
New requirements from PCI DSS 2.0 to 3.0 came out in Nov 2013






Requires Qualified Security Assessor (QSA) validation annually or Self-Assessment

Lack of COMPLIANCE:

Fines: **Up to \$500k per incident** (VISA), government fines, insurance costs, and litigation
Brand reputation: Share price falls, loss of customer confidence
Revocation: **Inability to process credit card transactions**
More compliance: Additional PCI validation required



PCI DSS 2.0 Requirements

PCI Requirement	Description
1 	Install and maintain a firewall configuration to protect cardholder data.
2	Do not use vendor-supplied defaults for system passwords and other security parameters.
3 	Protect stored cardholder data.
4	Encrypt transmission of cardholder data across open, public networks.
5	Use and regularly update anti-virus software.
6 	Develop and maintain secure systems and applications.
7	Restrict access to cardholder data by business need to know.
8	Assign a unique ID to each person with computer access.
9 	Restrict physical access to cardholder data.
10	Track and monitor all access to network resources and cardholder data.
11	Regularly test security systems and processes.
12 	Maintain a policy that addresses information security.



Health Insurance Portability & Accountability Act (HIPAA) Compliance



WHAT:

- Uniform rules for protecting Health Info
- Written or Oral communications
- **E-mail, computerized and electronic information** (computer records, faxes, voicemail, PDA entries, etc.)

WHO:

- Comes from a health care provider or a health plan
- Could be used to identify an individual
- Describes the health care, condition, or payments or demographics of an individual

HOW:

Physical Safeguards

- Computer terminals are not placed in public areas

Technical Safeguards

- Every associate must keep his/her password confidential

Administrative Safeguards

- Policy and procedure for release of patient information

COMPLIANCE:

- \$100 fine per day for each standard violation. (Up to \$25,000 per person, per year, per standard.)
- \$50,000 fine + up to one year in prison for improperly obtaining or disclosing health information.
- **\$100,000 fine + up to five years in prison** for obtaining or disclosing health information under false pretenses.
- **\$250,000 fine + up to ten years in prison** for obtaining health information with the intent to sell, transfer or use for commercial advantage, personal gain or harm.

HITECH (Health Information Technology for Economic and Clinical Health Act)



Purpose

- **Makes massive changes to privacy and security laws**
- **Mandatory Breach Notification requirements** (Patient, Department of Health and Human Services, and Media)
- Applies to covered health care entities and business associates.
- Creates a nationwide electronic health record
- Increases penalties for privacy and security violations



Criminal Penalties

Criminal provisions

- **Executives: up to 10 years in prison**
- Fines started at \$100 and could reach up to \$25,000 for all identical violations of the same provision

HITECH - Harsher Penalties

- Tiers established for civil penalties
- Maximum penalty of **\$1.5 Million**
- **The higher the level of culpability, the higher the penalty**

Organizations close and
people lose jobs



Legal Risk and IT Security

What is the risk?

- Failure to meet the **standard of reasonable care**
- PA Bar Formal Opinion 2011-200

Why do I care?

- Risk of civil litigation loss
- Significant financial impact for defense even if you win a case; losing can put you out of business





Legal Risk Mitigation

What should I do?

- Secure IT systems, patch, and update periodically
- Backup, encrypt, audit, monitor, verify periodically
- Assess third party vendor and service provider agreements
- Document your Data Breach Notification Process
- Create an Incident Response Plan
- Validate volunteer/employer/employee privacy practices and enforcement technologies
- Review and Revise Access Policies and Procedures
- Implement Risk Transfer / Insurance Assessment



Disaster Preparation



- **Assess Risks**
 - Hurricane, fire, flood, terrorism, disgruntled employee, malicious volunteer, inattentive staff member
- **Identify Critical Resources**
 - Processes, computer systems, information, documents, employee contact info, client/customer contact lists
- **Develop Plans and Procedures**
 - Simple step-by-step emergency and restoral procedures
 - Minimize downtime, lost donations, lost services
- **Train and Test**
 - Ensure key staff know the procedures
 - Execute both tabletop and actual failover testing





Cyber Incident Handling

1. **Preparation:** Set up systems to detect threats and create policies for action; including public info release decisions
2. **Threat Identification:** Effects it is having on your systems
3. **Containment:** Limit effects by confining to as few systems as possible; freezing the scene for investigation
4. **Eradication:** Get rid of whatever the attacker might have left behind – rebuild from original media if possible
5. **Recovery:** Restore the system, reconnect to the network, restore data from known clean backups if necessary.
6. **Follow-up:** Root cause identification, deploy countermeasures, improve processes, proceed with prosecution, etc.



Non-Profit Cyber Security Issues



- Volunteers – train, acknowledge and follow secure processes
 - Turnover, mobile staff, remote access to sensitive data
- Bring Your Own Device (BYOD) – is that laptop secure?
- Partner organizations
- Compromises or Leaks
 - Donor list
 - Donation amounts
 - Clients
- Reputation Management
 - Web site hack
- Social Media Compromise



Compliance and Cyber Security



Excessive Security

Effective Security

Compliant

No Security



for now



GOING OUT OF BUSINESS



What should I do?

1. Do it yourself
2. Ask for help
3. Hire support

Expert



Not an Expert



**Can
You
Spot the
Difference?**



Do it yourself

1. Train IT staff on critical security issues with CISSP, SANS GIAC, MCSE-Security
2. Patch workstations, laptops, servers
3. Train staff regularly
4. Update anti-virus and spyware
5. Use firewalls to limit access
6. Backup key systems
7. Create Incident Response Plan
8. Continuously monitor security posture

**You
shouldn't
share your
passwords
either.**



Be vigilant. Stay safe online.





Ask for help

1. Web information services
2. Local colleges and universities
3. Part-time IT security employees
4. Volunteers or Consultants
5. Virtual CIO/CISO/CPO



Security**Focus**.com



Software Engineering Institute
Carnegie Mellon



Protectingtomorrow.org
Schools, Business, Vets



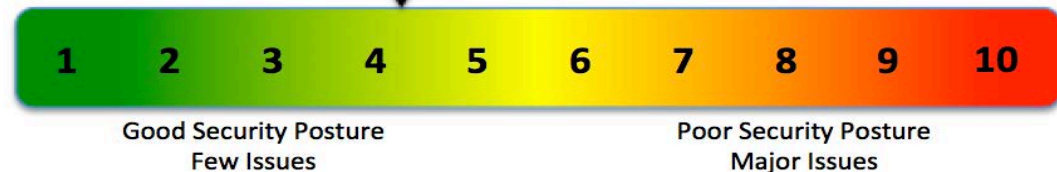
Hire Support...but who?

1. Trust
2. Experience with Advanced Persistent Threats
3. No software or hardware vendors
4. Industry experience
5. Technically current



4.1

199 critical vulnerabilities in
a Financial Services Firm





Non-Profit Cyber Security

**“In 60% of cases,
attackers are able to
compromise an
organization in
minutes”**

2015 Verizon Breach Report

- Must have IT and privacy policies including temp staff access
- Secure infrastructure and separate BYOD access
- Trust but Verify – monitor, log, audit, and review access
- Monitor IT security posture – what you don't know CAN significantly damage your organization





**Striking the critical balance
between protection and
performance**

Thank you!

Comments?

Questions?



sales@LP3.com
<https://protectingtomorrow.org/>