CyberSecurity for Non-Profits

Episode 1: Don’t Be Scared, Be Prepared!

codestar, inc.

Getting Started with Cybersecurity and Privacy

In this 3-part series, we aim to demystify cybersecurity by answering common questions and showing small organizations how to prioritize and make improvements even with limited resources. Though geared for nonprofits, it will be helpful to other small businesses as well.

"Your company's **digital information** – *such as customer data, financial records, and business correspondence* – is, quite literally, the crystallized **value of your business**."

Part 1 is for decision-makers and implementers who are responsible for cybersecurity.

We Know It’s Not That Easy

- Time
- Money

- Know-How
  - Recognizing risks and responsibilities
  - Getting started with risk management
  - What you can do immediately to become safer

Evolving Risk Landscape

- Disasters – fire, flood, earthquake, lightning strikes
- Hardware failures – power supplies, hard drives, backup
- Software bugs – firmware, applications, web servers
- Internet-borne vulnerabilities – phishing, hacking, poisoned advertisements
- The Internet of Things – TVs, refrigerators, power plants
- Insiders with access
- Third-party providers with inadequate safeguards

Risk Trends

- Attacks on people, not boxes. Anti-virus and a firewall are no longer sufficient

- Seeking profit directly, or through the sale of identities
  - Social attacks
  - Ransomware
  - E-commerce website attacks

Consequences

- Down-time
- Loss of reputation
- SMBs go out of business after cyber attacks

Possible Additional Responsibilities

- HIPAA/HITECH
- PCIDSS
- State privacy and breach law

Managed Services – Top 4 Questions to Ask

May not be training for privacy or compliance!

1) HIPAA Business Associate Agreement (BAA)
2) Access control
3) Encryption of stored data
4) Assurance of security practices

Risk Management

- Risk assessment
- Gap analysis
- Remediation plan

Good News

- Risk management process
- Backups
- Training
- Free Resources
- Grants

Risk Management Process

- A tool for improving cybersecurity generally, by reducing risk and planning for emergencies
- Risk assessment is likely the first requirement during a regulatory audit or data-breach investigation
- A documented risk-management process *might* reduce penalties, fines, or punitive damages

Backups

- The truth about disaster recovery
- Any backup is better than no backup
- Cloud cautions

Training

- Recognizing fraudulent emails and notifications
- Participating in privacy controls
- Recognizing and reporting breaches

Free and Open-Source Solutions

- Anti-malware and scanners/cleaners
- Vendor-supplied OS updates
- Email software with smart spam filters
- Web browsers with plugins
- Tech Soup

Grants

- Administrative cost
- Foundation Center
- Cybersecurity is in the headlines

- Strategies
    1) Information security as a line item
    2) Make the people connection

If You Only Do One Thing

- Backup
- Your backup is not as good as you think
- Verify regularly

- Q&A – submit your questions to info@codestar.us
  or on our Facebook page

- Mark your calendar! Part 2 - same time, same place
  “Think You’re All Set? Think Again!”

- Slides, survey, and our “10 for 10 Guide” are posted at www.codestar.us/nonprofits

- While there, sign up for our Security Tips Newsletters!