Cybersecurity Assistance
Pat Toth
NIST MEP
What is Information Security?

Confidentiality
Unauthorized Access, Disclosure

Integrity
Unauthorized Modification, Use

Availability
Disruption, Destruction
What is Information Security?

- Cybersecurity
- Privacy
- Physical Security
- Contingency Planning & Disaster Recovery
- Operational Security
- Personnel Security
Small Business on Cybersecurity

– “That doesn’t affect me”
– “I’m not a target”
– “I can’t afford it” / “It costs too much”
– “It’s impossible” / “We’re doomed”
– “Not sure what to do”
Why Small Businesses?

- In 2015, 43 percent of all Spear-Phishing attacks targeted businesses with fewer than 250 employees*

* Symantec 2016 Threat Report
Cost of an incident

The average cost of a data breach for SMBs and Enterprises stands at $38k and $551k respectively and 60% of businesses that suffer a breach find their ability to function severely impaired.

**Kaspersky Labs, Global Corporate IT Security Risks: 2015**
Which would YOU go after?

- Motion & impact sensors
- Video cameras
- 24/7/365 Professionals

- Simple lock
- Many windows
- Owners often away
RISKS
Vulnerability:
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source
What is a Threat?

Threat: a circumstance or event (source) with the potential to adversely impact business assets
Types of Threat Vectors

- Spoofing
- Snooping
- Social engineering
- Increasing the level of system privileges
- Ransomware
Types of Threat Vectors

- **Identity Theft** - steal & misuse your identity ($$$)

- **Phishing** - Email tricking YOU or your employees into giving personal or business/customer information (a form of social engineering)

- **Spear Phishing** - Email with specific company details and targeted at specific employees to deceive you/the target into responding

- **SPAM** - Unsolicited and unwanted Email

- **Compromised web pages** - invisible code planted on legitimate web pages which will attempt to install malware on your personal or business computer(s)
Malicious Attacks - What are they after?

- Access to business information / money
- Personally Identifiable Information (PII)
  - Your own
  - Your employees’
  - Your customers’
- To use your personal or business resources for their own purposes / activities
- Disrupt business operations
Disaster & Business Resource Threats

• Disasters
  – Fire (natural or man-made)
  – Flooding (natural or man-made, e.g., from burst pipes)
  – Hurricane, tornado, earthquake (natural, locality-based)

• Business Resource Threats
  – Equipment (hardware) failure
  – Network/communications failure
  – Application (software) failure
  – Supply Chain Disruption
  – Lack of protections (e.g., no fire protection in place)
Humans

• Malicious Attack
  – Hacking business systems to steal information
  – Theft of computer hardware
  – Website defacement
  – Installing malicious programs onto business computers
  – Destroying a system to disrupt operations

• Human Error
  – Destruction of data and resources
  – Disclosure of proprietary / sensitive information
NIST Cybersecurity Framework

Identify

Protect

Detect

Respond

Recover
Where to Start

• Identify what information your business uses
• Determine how much your information is worth
• Understand your threats and vulnerabilities
• Get help when needed
Identify

- Inventory
- Access control
- Background checks
- Individual user accounts
- Policy and procedures
Protect

- Limit employee access
- Install surge protectors and UPS
- Patch operating systems and applications
- Install and activate firewalls
- Secure wireless access points
- Set up web and email filters
- Encrypt sensitive information
- Safe disposal
- Train employees
Detect

- Install and update anti-virus, and anti-spyware
- Maintain and monitor logs
- Train your employees
Respond

- Develop a plan for disasters and security incidents
  - Roles and responsibilities
  - Who to call
  - What types of activity constitutes a security incident
Recover

• Make full backups
  – Removable media
  – Separate server isolated from the network
  – Online storage/Cloud service providers

• Test your backups

• Consider Cyber Insurance
Cost Benefit/Avoidance Analysis

Potential Loss

versus

Protection Costs
Potential Impact (Consequences/Loss)

- Embarrassment (credibility/reputation)
- Repair costs (& down time)
- Misinformation or worse (misled customers)
- Weakened ability to innovate
- Loss of personal assets
- Loss of customers
- Out of Business!
Things to do

• Train your employees
  – Phishing
  – Social Media

• Clean machines
  – Patches
  – Latest security software
  – Browsers
  – Operating Systems

• Use firewalls
Things to do

Mobile Devices
- Passwords
- Encrypt
- Install Security Apps
- Avoid Public Networks
- Report if lost or stolen
Things to do

• Make backups
  – Automatically
  – Weekly
  – Store offsite or in the cloud

• User Accounts for each employee
  – Strong passwords
  – Admin privileges limited
Things to do

- Secure Your Wi-Fi
  - Encrypt
  - Do not broadcast network name
    - Service Set Identifier (SSID)
  - Password protect router
Things to do

- Payment Cards
  - Trusted and validated tools
  - Anti-fraud services
  - Isolate payment systems
- Limit Access
  - No one has access to all
  - Based on roles
  - SW Install needs permission
Things to do

- Strong Passwords
  - Change every three months
  - At least 12 characters
    - Number
    - Special character
  - Multi-factor Authentication
  - Train Employees
Questions?
More Cybersecurity Webinars Coming Soon!

Pat Toth
ptoth@nist.gov
301-975-5140