MAKING AN IMPACT ON U.S. MANUFACTURING

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Cybersecurity

Patricia Toth

NIST MEP

What is Information Security?

Confidentiality

Unauthorized Access, Disclosure

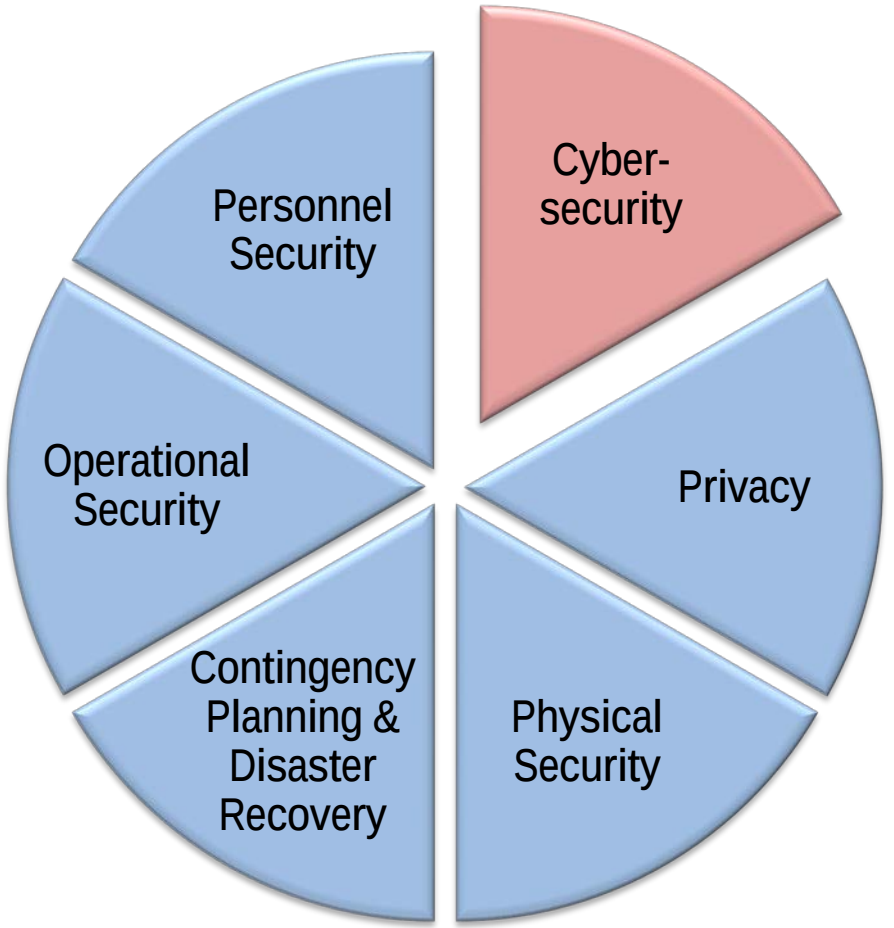
Integrity

Unauthorized Modification, Use

Availability

Disruption, Destruction

What is Information 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

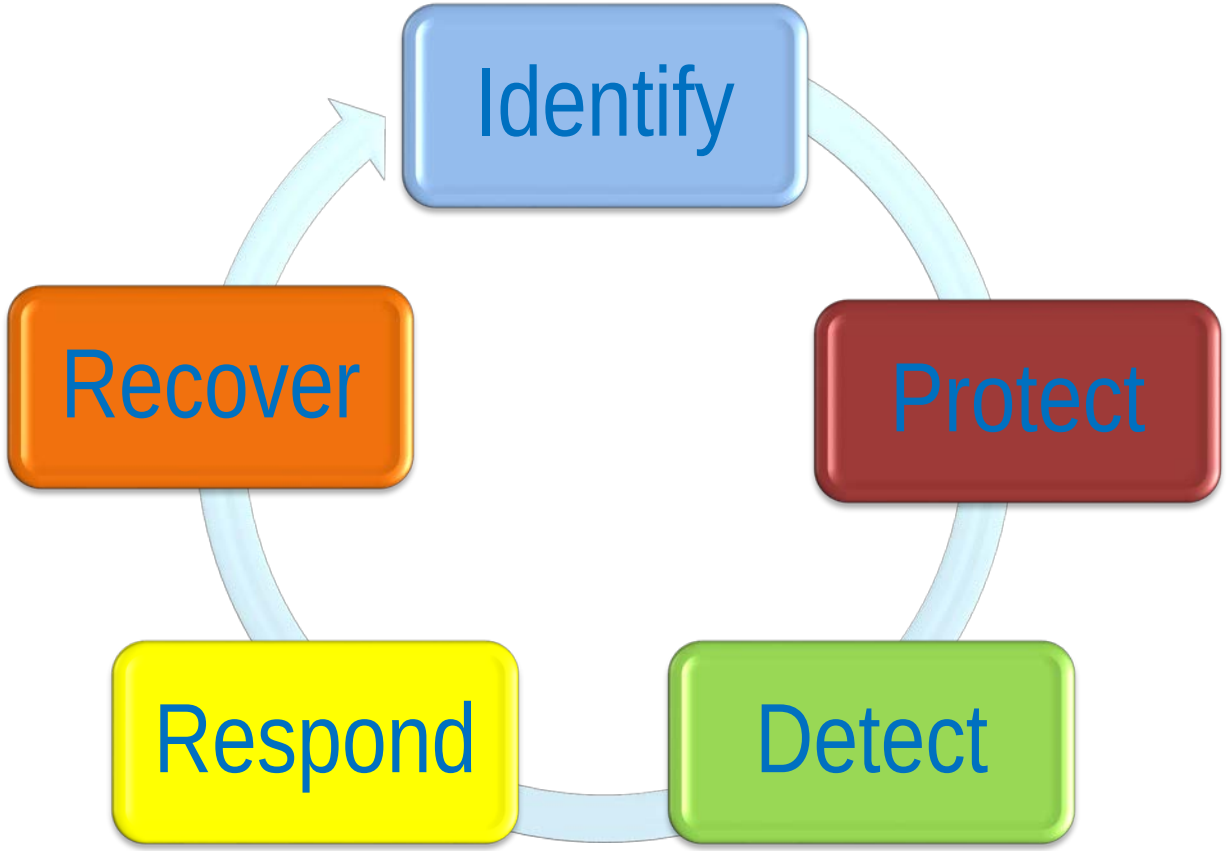
What is a Threat?

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

NIST Cybersecurity Framework



Guide for Small Business

NISTIR 7621 Rev 1

Small Business Information Security: The Fundamentals

http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

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

NIST Special Publication 800-171 Rev 1

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

December 2016

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

Controlled Unclassified Information

Supports federal missions and business functions…

…that affect the economic and national security interests of the United States.

Why is this all necessary?

- Over 100 different ways of characterizing SBU information.
- No common definition or protocols.
- Information inconsistently marked.
- Common definition and standardize processes and procedures.

The CUI Registry

www.archives.gov/cui/registry/category-list.html

- Online repository for information, guidance, policy, and requirements on handling CUI, including issuances by the CUI Executive Agent.
- Identifies approved CUI categories and subcategories (with descriptions of each) and the basis for controls.
- Sets out procedures for the use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.

CUI Registry

- Manufacturing

Category-Subcategory:	Proprietary Business Information-Manufacturer
Category Description:	Material and information relating to, or associated with, a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications.
Subcategory Description:	Relating to the production of a consumer product to include that of a private labeler.
Marking:	MFC

Applicability

- CUI requirements apply only to components of nonfederal information systems that process, store, or transmit CUI, or provide security protection for such components.

Assumptions

Nonfederal Organizations —

- Have information technology infrastructures in place.
  - Not developing or acquiring systems specifically for the purpose of processing, storing, or transmitting CUI.
- Have safeguarding measures in place to protect their information.
  - May also be sufficient to satisfy the CUI requirements.
- May not have the necessary organizational structure or resources to satisfy every CUI security requirement.
  - Can implement alternative, but equally effective, security measures.
- Can implement a variety of potential security solutions.
  - Directly or through the use of managed services.

Security Requirements *14*

Families

Obtained from FIPS 200 and NIST Special Publication 800-53.

- Access Control.
- Audit and Accountability.
- Awareness and Training.
- Configuration Management.
- Identification and Authentication.
- Incident Response.
- Maintenance.
- Media Protection.
- Physical Protection.
- Personnel Security.
- Risk Assessment.
- Security Assessment.
- System and Communications Protection
- System and Information Integrity.

Structure of Security Requirements

Security requirements have a well-defined structure that consists of the following components:

- *Basic security requirements section.*
- *Derived security requirements section.*

Security Requirement

Awareness and Training Example

Basic Security Requirements:

3.2.1 Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those organizational information systems.

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Derived Security Requirements:

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Security Requirement

Awareness and Training Example 3.2.2

Basic Security Requirements:

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Meeting the Requirement:

- Basic security awareness training to new employees.
- Security awareness training to users when information system changes.
- Annual security awareness refresher training.

Security Requirement

Awareness and Training Example 3.2.2

Basic Security Requirements:

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Meeting the Requirement:

- Security awareness and training policy.
- Security awareness training materials.
- Security plan; training records; other relevant documents or records.
- Personnel with responsibilities for security awareness training.

Security Requirement

Configuration Management Example

Basic Security Requirements:

3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational information systems.

Derived Security Requirements:

3.4.3 Track, review, approve/disapprove, and audit changes to information systems.

3.4.4 Analyze the security impact of changes prior to implementation.

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

3.4.5 ……

Security Requirement

Configuration Management Example 3.4.1

Basic Security Requirements:

3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Meeting the Requirements:

- Develops, documents and maintains a current baseline configuration of the information system
- Configuration control in place.

Security Requirement

Configuration Management Example 3.4.1

Basic Security Requirements:

3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Meeting the Requirements:

- Configuration management policy; procedures and plan.
- Documentation for Enterprise architecture or information system design.
- Information system configuration settings and associated documentation.
- Change control records.
- Personnel with configuration management responsibilities.
- System/network administrator.

Security Requirement

Access Control Example

Basic Security Requirements:

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Derived Security Requirements:

3.1.3 Control the flow of CUI in accordance with approved authorizations.

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

3.1.6 Use non-privileged accounts or roles when accessing non-security functions.

3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

3.1.8 Limit unsuccessful logon attempts.

Security Requirement

Access Control Example 3.1.8

Derived Security Requirements:

3.1.8 Limit unsuccessful logon attempts.

Meeting the Requirements:

- Limit number of consecutive invalid logon attempts allowed during a time period.
- Account lockout time period automatically enforced by the information system when max number of unsuccessful logon attempts is exceeded.
- Locks the account/node until released by an administrator.
- Delays next logon prompt according to the organization-defined delay algorithm.
- Access control policy and procedures addressing unsuccessful logon attempts.
- Personnel with information security responsibilities; system developers; system/network administrators

Security Requirement

Access Control Example 3.1.8

Derived Security Requirements:

3.1.8 Limit unsuccessful logon attempts.

Meeting the Requirements:

- Access control policy and procedures addressing unsuccessful logon attempts.
- Personnel with information security responsibilities; system developers; system/network administrators

DFARS 252.204.7008

"If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that are in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—

(A) Why a particular security requirement is not applicable; or

(B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection."

Meeting SP 800-171

- Some security controls may not be applicable to your environment.
- Build off you are currently doing.
- Other ways to meet the requirements.

Meeting SP 800-171

- More cost effective approach
  - Isolate CUI into its own security domain by applying architectural design concepts
  - Security domains may employ physical separation, logical separation, or a combination of both.
  - Use the same CUI infrastructure for multiple government contracts or agreements.

Questions?

MAKING AN IMPACT ON U.S. MANUFACTURING

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Pat Toth

ptoth@nist.gov

301-975-5140