
WELCOME
NIST'S 800-171 AS A CYBERSECURITY SYSTEM FOR SMB'S

Presentation by:

Zane Patalive, MCSE, Partner
zanep@realitcare.com

Real IT Care, LLC
www.realitcare.com

(570) 323-2650 x120

SESSION OBJECTIVES

- Advantage of Establishing a Cybersecurity Program in Every Company
- Introduction to NIST's 800-171 Cybersecurity Compliance Standard
- Free Tools Available to Create and Implement a Cybersecurity Program
- Discussion of Real-World Assessments using a Consultant (Jason McNew)

Cyber Compliance Requirements

- *PCI (Credit Cards)*
- *HIPPA (Health Care)*
- *SOX (Financial)*
- *NIST 800-171 (DoD)*
- *GDPR (EU)*

HOW DOES THIS AFFECT SMALL BUSINESSES?

WHAT IS ADEQUATE SECURITY?

HOW DO SMALL BUSINESSES ATTAIN THESE STANDARDS?

WHAT IF THERE IS A POTENTIAL BREACH?

WHERE CAN SMALL BUSINESSES GET ADDITIONAL HELP?

Source: Office of Small Business Programs, U.S. Department of Defense

WHY DO I NEED A CYBER SECURITY PLAN?

1

Avoid Ransomware, Malware, Viruses, Theft, Downtime, …

2

Protect my company's data in case of a crash or attack. Enable recovery from failure

3

Ensure my private data stays private

4

Protect my customer's data that is under my roof

THE COST OF DATA LOSS

- 93% OF COMPANIES THAT LOST THEIR DATA CENTER FOR 10 DAYS OR MORE DUE TO A DISASTER, FILED FOR BANKRUPTCY WITHIN ONE YEAR OF THE DISASTER. 50% OF BUSINESSES THAT FOUND THEMSELVES WITHOUT DATA MANAGEMENT FOR THIS SAME TIME PERIOD FILED FOR BANKRUPTCY IMMEDIATELY. (NATIONAL ARCHIVES & RECORDS ADMINISTRATION IN WASHINGTON)

IMPACTS OF DATA LOSS

- Lost productivity
- Legal action
- Breach notification costs
- Bad publicity
- Distrustful customers
- Brand damage
- Poor employee morale

SO WHERE DO WE START?

- Baseline your company against a standardized set of security controls
- Create a GAP analysis of where you fall short
- Make a plan to close the gaps that make sound business sense
- Create a company culture of Security (Employee training)

Special Publication 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

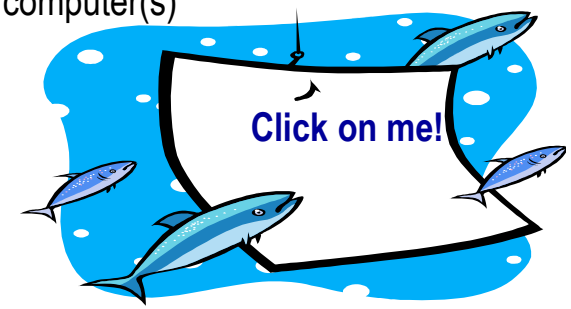
Our appetite for *advanced technology* is rapidly exceeding our ability to protect it.

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)

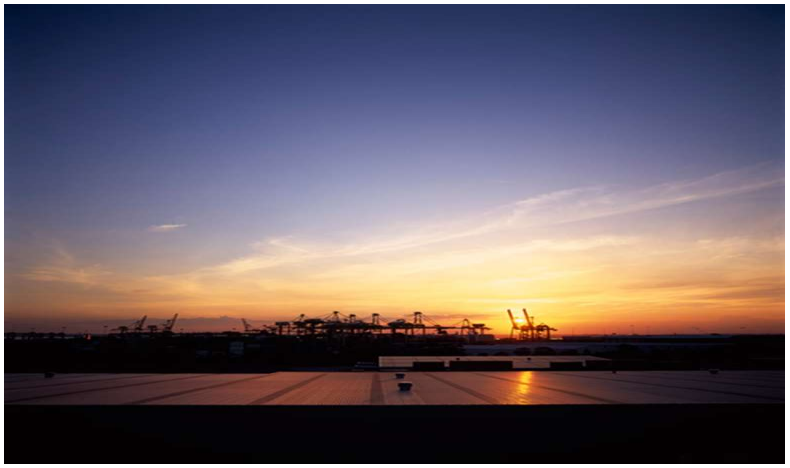


Controlled Unclassified Information

Supports federal missions and business functions…

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

Purpose



- To provide federal agencies with recommended requirements for protecting the confidentiality of CUI —
  - ***When the CUI is resident in nonfederal information systems and organizations.***
  - ***Where the CUI does not have specific safeguarding requirements prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.***
  - ***When the information systems where the CUI resides are not operated by organizations on behalf of the federal government.***

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

Security Requirements

14 Families

- 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.

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

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:

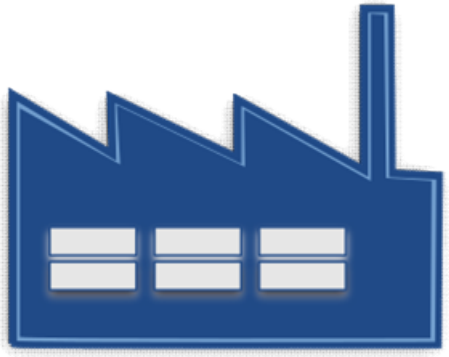
- Access control policy and procedures addressing unsuccessful logon attempts.
- Personnel with information security responsibilities; system developers; system/network administrators

Meeting SP 800-171

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

NIST MEP Activities (IMC is our local MEP Center)

- Help MEP Centers assist small manufacturers meet 800-171
  - Training
  - FAQs
  - Guidance
  - Tools

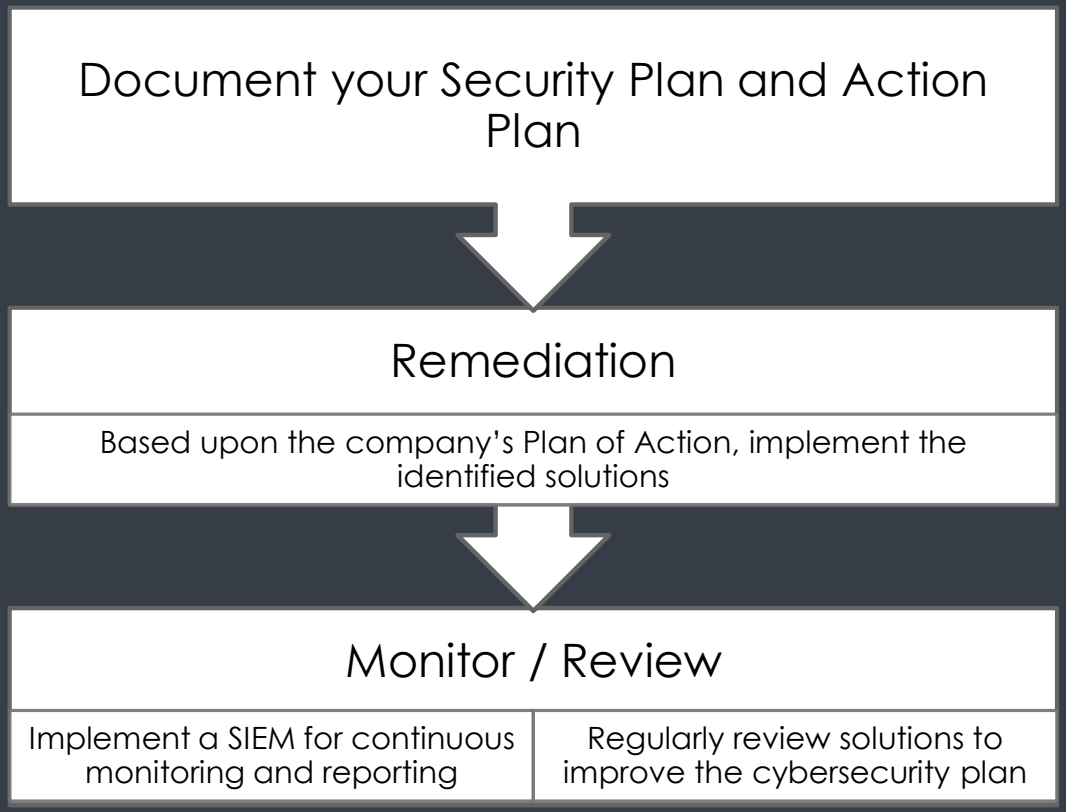


- Work with NIST to develop 800-171A
- Develop criteria for selecting cybersecurity assessors
- Closely monitor DFAR developments

COMPLIANCY DIY (DO-IT-YOURSELF)

Assess	Conduct an Assessment of the current-state as compared to the standard. "Where are we today?" • Called the System Security Plan, which documents how the company is meeting defined standards
GAP	Create a GAP Analysis of where the company falls short as compared to the standard
Plan	Create a Plan of Action • A document that states how and when the company will achieve the standard, using a reasonable timeframe

COMPLIANCY DIY (DO-IT-YOURSELF)



FREELY AVAILABLE TOOLS

- Download the NIST 800-171 Self Assessment Handbook for guidance
  - https://www.nist.gov/publications/nist-mep-cybersecurity-self-assessment-handbook-assessing-nist-sp-800-171-security
- Download the CSET Cybersecurity Evaluation Tool from DHS
  - https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET
- Document the System Security Plan and Plan of Action
  - http://gtpac.org/cybersecurity-training-video/?mc_cid=6dc296c3d8&mc_eid=1dc343e71a

Questions?