

Pirates Aren't Only Looking for Gold: Remember Your Information Security Program When Implementing New Technologies!

by Jim Soenksen



look

plan

act

repeat



PIVOTGROUP

SOLUTIONS TAILORED, NOT RESOLD.



look

plan

act

repeat

Introduction

- What is an information security assessment?
- Why do you need information security assessments?
- How do you implement an information security program?
- When implementing new technology, perform an information security assessment.
- Conclusion



look

plan

act

repeat

Information Security Program

- An Information Security Program is a combination of:
 - a ***risk assessment*** that identifies the potential threats to mission critical assets of an organization
 - a ***vulnerability scan*** of applications, ports, and systems
 - ***policies, procedures, and training***



look

plan

act

repeat

Information Security Program

- Set up a program
 - To protect the organization's assets
 - On a regular, ongoing basis
- Adaptable program
 - Easily revised when adopting new technology



look

plan

act

repeat

Information Security Program

- **look** – business assessment and vulnerability assessment
- **plan** – strategy for a proactive plan
- **act** – action to take in order to protect assets
- **repeat** – life cycle of information security



look

plan

act

repeat

VoIP Security Considerations

Security issues:

- Wire tapping
- Eavesdropping
- Hijacking of telephone calls
- Network attacks



look

plan

act

repeat

VoIP Security Considerations

All network threats prevalent in data networks:

- Packet sniffing
- Man-in-the-middle attacks
- Phishing
- Denial-of service (DoS) attacks
- Viruses
- Worms
- Trojans
- Spam



look

plan

act

repeat

VoIP Security Considerations

Encryption of the VoIP network:

- Essential protection
- Protects against the monitoring of telephone conversations.
- Available in AES
- Can be done in block cipher or stream
 - in order to protect the privacy of the call and the authenticity of the call.



look

plan

act

repeat

VoIP Security Considerations

Defense-in-depth:

- In order to protect a company's tangible assets of electronic documents, software, and hardware, the company needs to implement
 - Firewalls to protect the gateways, routers, and endpoints
 - Intrusion detection systems (IDS)
 - Intrusion prevention systems (IPS)
 - Encryption
 - Access controls



look

plan

act

repeat

VoIP Security Considerations

Defense-in-depth (con't.):

- **Cryptographic protocols and applications** provide measures for securing telecommunication
 - Transport Layer Security Protocol (TLS) – the latest Secure Socket Layer (SSL) – to encrypt messages in real-time and prevent eavesdropping.
 - Internet Protocol Security (IPSec)
 - Secure Shell (SSH), and
 - Pretty Good Privacy (PGP)



look

plan

act

repeat

VoIP Security Considerations

Defense-in-depth (con't):

- **Physical security** is another layer of defense-in-depth
 - includes reviewing the physical components
 - as well as the telecommunication element that could be susceptible to any potential threats to a company's business assets.



look

plan

act

repeat

VoIP Security Considerations

Wireless telephone usage with Voice over Wi-Fi (VoWiFi) :

- Laptops, cell phones, and/or PDAs.
- VoWiFi should include the 802.11i Wi-Fi Protected Access (WPA) standard
 - Encrypts conversations
 - Provides some protection from hackers intercepting calls.



look

plan

act

repeat

VoIP Security Considerations

For wireless networks – defense-in-depth security technologies:

- 802.11 Wired Equivalent Privacy (WEP)
- 802.11i WiFi Protected Access (WPA)
- Advance Encryption Standard (AES) with a key size of up to 256 bits



look

plan

act

repeat

Risk Assessment – look

Identify the threats and vulnerabilities to accomplish CIA:

- **Confidentiality** – the information is kept safe from accidental or intentional disclosure to unauthorized users
 - Organization’s reputation at stake
 - Exposure to the organization could range in the millions of dollars
- **Integrity** – the information is as intended and has not been changed
 - If data becomes corrupt or is inadvertently disclosed:
 - Lose the trust of the client
- **Availability** – the information is available whenever needed by authorized users to do their job



look

plan

act

repeat

Risk Assessment – **look**

Evaluate threats by:

- Potential **threats**
- **Likelihood** of these threats **occurring**
 - ranked high, medium, or low
- The **impact analysis** should these threats transpire
 - ranked high, medium, or low



look

plan

act

repeat

Risk Assessment – **look**

Identification of the following threats to the organization's network:

- *Natural Threats*
- *Human Threats*
- *Environmental Threats*



look

plan

act

repeat

Risk Assessment – **look**

Higher Probability Natural Threat Areas:

- Backup data to remote offices outside of the same threat area
- Contract with a third party provider to store backup
- **Hurricanes** along Eastern and Gulf Coasts
- **Tornadoes** in the Midwest
- **Earthquakes** in the West
- **Volcanoes** in the West
- **Fire and Floods** can be common threats to any location
- **Snowstorms** most prevalent in the Midwest, Plain States, East, and Northwest



look

plan

act

repeat

Risk Assessment – **look**

Human threats can be accidental or intentional:

- Workplace violence
- Internet/Intranet security breaches
- Untrained employees
- Fraud white collar crimes



look

plan

act

repeat

Risk Assessment – **look**

Insider Threats:

- **Trade secrets and intellectual property** information must be protected
- **Employee access control**
 - Weak passwords are vulnerable
- **Removable media**
 - CDs and floppy disks
 - USB flash drives



look

plan

act

repeat

Risk Assessment – **look**

Types of environmental threats:

– **Temperature of the server closets**

- If a server closet is too hot, the servers could be damaged – making the data unavailable.
- Air conditioning is critical to protecting the data.

– **Massive grid power outage**

- In 2003, there was a massive grid outage from the East to the Midwest
- Satellite offices also down due to main offices supplying network services
- Redundancy of systems should be addressed in disaster recovery and business continuity plan



look

plan

act

repeat

Risk Assessment – **look**

Disaster recovery preparations and business continuity planning must include:

- Preparation of **backups at an off-site location**
 - Hurricane Alley states should have off-site backup facilities in different state
 - NYC firms began remote backups in caves in Appalachian Mountains after 9/11
- **Testing the backups** to assure that they would work to recover from a disaster



look

plan

act

repeat

Risk Assessment – **look**

Business assessment of your needs through a risk assessment:

- Identify critical assets, such as:
 - patient health information
 - customer personally identifiable information
 - intellectual properties
 - trade secrets
 - financial information
 - sensitive and/or confidential information to be protected



look

plan

act

repeat

Risk Assessment – **look**

Vulnerability assessment of your needs by:

- Identification of the mission critical assets requiring the utmost protection
- The level of risk accepted by management



look

plan

act

repeat



Strategy for a Proactive Plan – **plan**

Proactive and ongoing Information Security plan based on:

- Risk assessment findings
- Regulatory compliance
- Resource availability
- Budget guidelines



look

plan

act

repeat

Strategy for a Proactive Plan – **plan**

- Identify how to mitigate risks
 - Technical controls
 - Management controls
 - Operational controls
- Draft or revise security policies to cover these risks
- Train employees and customers



look

plan

act

repeat

Strategy for a Proactive Plan – **plan**

Security policy development:

- Prepare written security policies and procedures
- Identify critical assets to be protected
- Describe what types of downloads are allowed and how many sensitive files can be taken out of the office at one time
- Indicate how sensitive and confidential information is to be protected when removing it from the company network or computers



look

plan

act

repeat

Strategy for a Proactive Plan – **plan**

Security policy development (con't):

- Characterize the persons who are permitted to place sensitive and confidential information on laptops and/or massive storage devices
- Outline incident response procedures should a breach occur
- Identify who is to receive notification when confidential information is to be removed from the office
- Distribute these policies and procedures to all employees



look

plan

act

repeat

To Protect Assets – **act**

- **Take action on the plan**
 - Implement the controls and recommendations to mitigate the vulnerabilities found
- Guidance through information security roadmap
- Protect critical assets
 - Against constant stream of current and future threats
- Revise security policies as necessary
- Train customers and employees on security best practices



look

plan

act

repeat

To Protect Assets – **act**

- **Train employees on security best practices**
 - Provide examples of personally identifiable information that must not leave the building
 - Mandate that password protected screensavers be used on laptops
 - Illustrate how easily a removable media device can be lost or stolen – have the users write down what they think would be the ramifications of this information becoming public
 - Educate the users about the hazards of using cars as a locker for laptops and removable media devices
 - Require employees to sign a document stating they have read the computer acceptable use security policy and will abide by its terms



look

plan

act

repeat

Life cycle of Information Security – **repeat**

Continuously Monitor and Adjust:

- Ongoing basis – repeat the entire process on a regular basis as best practices indicate
- Schedule yearly risk assessment
- If new technology is employed, schedule a risk assessment
- When there is a security breach, schedule a risk assessment



look

plan

act

repeat

Security Policies/Training

- How many people have:
 - Security policies for use of company computing devices?
 - Training on how to use and safeguard confidential and sensitive company data?



look

plan

act

repeat

Next Steps

look, **plan**, **act**, **repeat**

First **look**:

- identify the critical assets
- assess the company's risk



look

plan

act

repeat

Next Steps

Next, **plan**:

- develop a proactive security program wrapped around
 - telecommunication technology selected
 - as well as the current system and network architecture



look

plan

act

repeat

Next Steps

- Then, **act** upon the chosen program swiftly
 - implement a company-specific tailored Information Security roadmap properly including:
 - Policies
 - Training
 - Technology



look

plan

act

repeat

Next Steps

- Once the overall plan has been put into action, **repeat** the entire process with:
 - on-going monitoring
 - auditing
 - updating
 - adjusting to business and technology changes



look

plan

act

repeat

Risk Assessment for Technology Deployment

- **look**
 - System Components
 - Users Features
 - Controls
 - Integration
 - Data
 - Communication
 - Back Up & Recovery



look

plan

act

repeat



Risk Assessment for Technology Deployment

- **plan**
 - Threats
 - Vulnerabilities
 - Risks
 - Impact Analysis
 - Risk Controls



look

plan

act

repeat



Risk Assessment for Technology Deployment

- **act**
 - Implementation
 - Test Plan
- **repeat**
 - Life Cycle of Testing
 - Risk Management



look

plan

act

repeat



PIVOTGROUP

SOLUTIONS TAILORED, NOT RESOLD.



Repeat



look

plan

act

repeat

Conclusion

- *Pivot Group can assist you with developing a security plan.*
- *Pivot Group provides risk assessment services.*
- *Each security program and assessment is customized to match the needs of the particular organization independent of the systems utilized.*



look

plan

act

repeat



PIVOTGROUP
SOLUTIONS TAILORED, NOT RESOLD.

What Questions Do You Have?



look

plan

act

repeat

Contact Information

Jim Soenksen - CEO

Pivot Group - **look**, **plan**, **act**, **repeat**

O: 404-419-2163

C: 404-668-6734

E: jsoenksen@pivotgroup.net

W: www.pivotgroup.net



look

plan

act

repeat



PIVOTGROUP
SOLUTIONS TAILORED, NOT RESOLD.

THANK YOU



look

plan

act

repeat