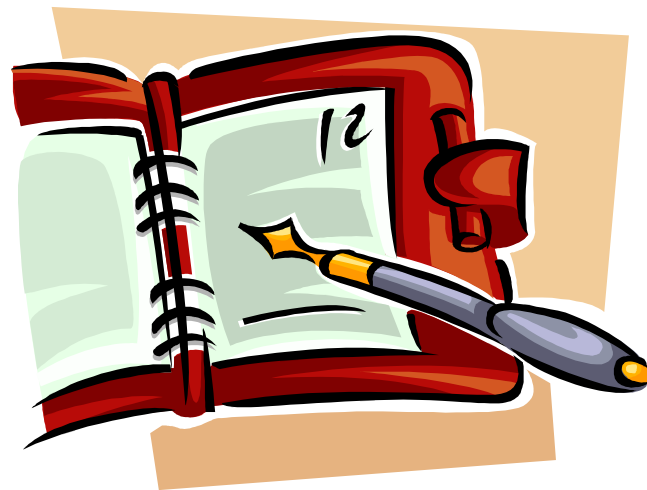


# Security Planning



**December 2004**

# Why Plan?

## The Risks are Real

- Every 5 Minutes All the IP Addresses on the Internet are Scanned by Attackers
- Every Day Companies Lose Data, Money, and Customers Due to Security Breaches
- 75% of All Companies Experience Financial Loss, but Only 47% can Quantify the Loss

# Why Plan?

## Risk Defined

- Vulnerability + Threat = Risk
- Vulnerability is Software, Hardware, Policy, and/or Process Weakness that can be Exploited
- Threat is Someone who has Motive, Expertise, and/or Lack of Knowledge to Exploit Vulnerabilities
- The Resulting Risk is a Loss

# Two Types of Planning

- **Reactive Security**
  - Risks of Reactive Security
  
- **Proactive Security**
  - Benefits of Proactive Security

# Two Types of Planning

## Reactive Security

- Wait for Event or Audit
- Fix the Surprise Problems
- Hopefully Deploy Security Measures and/or Pay Penalties

# Two Types of Planning

## **Risks of Reactive Security**

- Cost Planning is Difficult
- Incidents Likely to go Undetected
- Incidents Likely to be Pervasive
- Organization is Unaware of Risks
- Attackers Take Control
- Regulatory Non-Compliance Issues

# Two Types of Planning

## **Proactive Security**

- Annual Security Planning
- Regular Vulnerability Assessments
- Security Policies and User Education
- Technology Deployments
- Incident Response, Business Continuity, and Disaster Recovery Planning

# Two Types of Planning

## **Benefits of Proactive Security**

- Risk Reduction
- Early Incident Detection / Remediation
- Less Downtime
- Fewer Financial Losses
- More Accurate Security Budgeting
- Organization Asserts more Control
- Regulatory Compliance

# How to Plan

## **PART 1: What to Plan For**

- **Identify Critical Assets and Services**
- **Evaluate Potential Losses and/or Penalties**
- **Check for Vulnerabilities**
- **Stay Informed of Security Risks**

# How to Plan

## Identify Critical Assets and Services

- What Services are Necessary for Business Operation?
- Which Servers Store Sensitive Data?
- What Network Equipment (Routers, Firewalls, Switches) is Needed to Access Data and Services?

# How to Plan

## Evaluate Potential Losses and/or Penalties

- What is the Cost if Data is Read, Modified, or Deleted by Unauthorized Persons?
- What is the Cost if Critical Services are Unavailable for an Hour, Day or Week?
- What is the Cost if a Server Fails?
- What is the Cost if Network Equipment Fails?
- What is the Penalty of Non-Compliance?

# How to Plan

## Check for Vulnerabilities

- Learn Where the Organization is Vulnerable
- Perform Security Assessments
- *External Vulnerability Assessment* – Discovers where Outsiders Could Attack
- *Internal Vulnerability Assessment* – Discovers where Insiders (and Successful Outsiders) Could Attack

# How to Plan

## Stay Informed of Security Risks

- Subscribe to Security Publications
  - *Information Security Magazine*
  - SANS @ Risk Newsletter: <https://portal.sans.org/>
  - SearchSecurity.com:  
<http://searchsecurity.techtarget.com/>
  - [www.cert.org](http://www.cert.org)
  - <http://gocsi.org>

# How to Plan

## Stay Informed of Security Risks, cont.

- Subscribe to Current Updates
  - Microsoft
  - Unix
  - Linux
  - Software
  - Hardware
- Set Up Cassandra to Send Alerts
  - <https://cassandra.cerias.purdue.edu/main/index.html>

# How to Plan

## **PART 2: Create a Security Plan**

- **Address Vulnerabilities in Critical Assets and Services First**
- **Address Other Vulnerabilities**
- **Implement Security Policies**
- **Deploy Security Enhancing Technologies**
- **Make Contingency Plans**
- **Educate Users**
- **Management Involvement**

# How to Plan

## Address Critical Vulnerabilities

- Apply Security Patches / Upgrades
- Simplify Operations and Reduce Risk by Eliminating Extraneous Services
- Tighten Application and Operating System Configuration Settings

# How to Plan

## Address Other Vulnerabilities

- Limit Information in Public Databases (DNS, Whois, etc.) and on Web Site
- Get Documentation from Outsourced Partners that they Adequately Address Security
- Review Service Level Agreements for Areas Affecting Security

# How to Plan

## Implement Current Security Policies and Processes

- Acceptable Use
- Remote Access
- Passwords
- Incident Response
- Laptop
- Wireless Access

# How to Plan

## Deploy Security Enhancing Technology

- Strong Passwords
  - Firewall with NAT
  - Anti-Virus / Anti-Spam
  - Anti-Spyware
  - Web Filter
  - Virtual Private Networks
  - Wireless Access
  - E-mail Encryption
  - Intrusion Detection
  - Intrusion Protection
  - Patch Management
  - Network Monitors
  - Event Log Aggregators
- Detection and Prevention

# How to Plan

## Make Contingency Plans

- Back-up Critical Data
- Ensure Back-ups Restore Properly
- Use Redundancy for Critical Servers and Network Components
- Keep Standby Equipment On-Hand
- Document Configuration and Incident Recovery Processes
- Test Incident Recovery Processes Regularly
- Review Documents Annually

# How to Plan

## Educate Users

- Keep Security on Users' Minds with Regular Security Bulletins that Describe the Latest Risks
- Stress the Importance of Strong Passwords
- Stress the Need to Keep Passwords Private
- Explain the Threat of Social Engineering
- Describe Safe E-Mail, Web Browsing, and Instant Messaging Practices
- Explain how to Eradicate Spyware and Adware
- Explain Safe Wireless Networking

# Winning Support

***Knowing what to do is only half the battle***

- **Enlist Management Support**
- **Create a On-Going Cycle**
- **Security ROI and How to Calculate**
- **Six Secrets of Highly Secure Organizations**

# Winning Support

## Enlist Management Support for Security

- **Include Tangible Benefits**
- **Include Intangible Benefits**
- **Create a Cost-Benefit Analysis**
- **Know if your Organization uses Hurdle Rates and Ensure Projects Meet or Exceed Them**

# Winning Support

## Include Tangible Benefits

- Business Partners Justify the Need
- Regulated Industries are Required to have Executives Responsible for Security
- Operating Efficiencies

# Winning Support

## Include Intangible Benefits

- Risk Reduction
- Customer Satisfaction
- Employee Morale
- Good Will
- Competitive Advantage

# Winning Support

## Create an On-Going Cycle

- Deploying Good Security that Breeds Confidence
- Confidence Translates into Support
- Support Results in Resources
- Resources can be Invested in Good Security

# Winning Support

## Security ROI

The Goal is to Show One or More of:

- **Increased Productivity** – highly likely, when security can be shown to improve system uptime
- **Cost Savings** – likely, especially when:
  - *security is already a priority*
  - *security projects will reduce costs or protect against regulatory non-compliance penalties and fees*
- **Revenue Generator** – unlikely, unless security is an enabler for revenue generating activities

# Winning Support

## How to Calculate Security ROI

- Calculations are Easier if Hard Data is Available
- Determine Worth of IT and Data Assets
- Measure the Total Number of Incidents and Total Loss for the Previous Year
- Calculate the Loss Per Incident Percentage
- Visit Pivot Group website ([www.pivotgroup.net](http://www.pivotgroup.net)) for more information including links to various calculators

# Winning Support

## Six Secrets of Highly Secure Organizations

Information from CIO magazine, 9/15/04 says that the most secure organizations:

1. Spend More than the Average on Security (14% of IT Budget)
2. Separate IT Security IT and Merge it with Physical Security Under an Executive Security Committee
3. Conduct Annual Penetration Tests and Complete Security Audits
4. Create Comprehensive Risk Assessment Processes
5. Design an Overall Security Architecture and Plan
6. Establish a Quarterly Security Review

# Conclusion

Take an active approach to your planning

**LOOK PLAN ACT REPEAT**

For more information about the **LPAR<sup>SM</sup>** Methodology,

Contact Pivot Group:

(404) 419 2160

*[info@pivotgroup.net](mailto:info@pivotgroup.net)*

*[www.pivotgroup.net](http://www.pivotgroup.net)*