What Is My Role in Information Survivability?

Why Should I Care?

Julia H. Allen
Networked Systems Survivability
CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

© 2002 by Carnegie Mellon University
CERT, CERT Coordination Center and Carnegie Mellon are registered in the U.S. Patent and Trademark Office
Survivability

Focuses on sustaining the mission in the face of an ongoing attack; requires an enterprise-wide perspective

Depends on the ability of networks to provide continuity of service, albeit degraded, in the presence of attacks, failures, or accidents

Requires that only the critical assets need the highest level of protection

Complements current risk management approaches that are part of an organization’s business practices

Includes (but is broader than) traditional information security
Agenda

Motivation

Perspectives/Questions

Protecting critical assets

Identifying risks to critical assets

Role of SEPG?
The Problem

“We wouldn’t have to spend so much time, money, and effort on network security if we didn’t have such bad software security.” [Viega, McGraw 02]

“It is bad software that results in [security] vulnerabilities in the first place.” [Viega, McGraw 02]

“There is little evidence of movement toward improvement in the security of most products. We continue to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on the security of their products.” [Pethia, 2001]
The Problem

“We wouldn’t have to spend so much time, money, and effort on network security if we didn’t have such bad software security.” [Viega, McGraw 02]

“It is bad software that results in [security] vulnerabilities in the first place.” [Viega, McGraw 02]

“There is little evidence of movement toward improvement in the security of most products. We continue to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on the security of their products.” [Pethia, 2001]
“Security models should be easy for developers to understand and build into their applications.”

“Our products should emphasize security right out of the box.”

“As software has become ever more complex, interdependent and interconnected, our reputation as a company has in turn become more vulnerable.”

“So now, when we face a choice between adding features and resolving security issues, we need to choose security.”

“Eventually, our software should be so fundamentally secure that customers never even worry about it.”
E-commerce sales soar

“Business-to-business electronic commerce grossed more than $100 billion in 1999, and this figure is expected to reach the $1 trillion mark by 2003.

“Total e-commerce, including both business-to-business and business-to-consumer transactions will account for an estimated $6.8 trillion by 2004.”

[Brian L. Stafford, director of the United States Secret Service, Roll Call, July 23, 2001]
Growth in Number of Incidents Reported to the CERT/CC

Number of Incidents:
- 45,000
- 60,000

Total Reported Incidents: 52,658
Attack Trends

Increased automation, speed of attack tools
Increased attack tool sophistication
Faster discovery of vulnerabilities
Increasing permeability of firewalls
Increasing asymmetric threat
Increasing threat from infrastructure attacks
Attack Impacts

- Loss/compromise of sensitive data
- System downtime; lost productivity
- System damage
- Financial loss
- Loss of reputation, customer confidence
- Other organizations’ systems affected
**Agenda**

Motivation

Perspectives/Questions

Protecting critical assets

Identifying risks to critical assets

Role of SEPG?
SPI Perspective

Dealing primarily with software developers and their management chain

End objective is to produce quality systems and products, on schedule and on budget

Security typically addressed

- during the software development life cycle
- during the O&M phase as an add-on/after the fact consideration
- for COTS software, as a provider responsibility
Security Improvement Perspective

Typically dealing with an organization’s infrastructure provider, their management chain, and the CIO

End objective of providing a functional and secure operational infrastructure for all users, within tight budget constraints (competing for internal dollars)
Questions to Consider

As a software developer, am I responsible for:

• Following secure programming practices?
• Protecting my work from viruses and other compromises?
• Identifying suspicious behavior on my system and network?
• Minimizing rework and downtime?
• Backup and recovery of my critical data?
• Ensuring that the software I rely on (such as the operating system, applications packages, tools, other COTS) is secure?
Questions to Consider (cont.)

As a SEPG member

- Do I consider security improvement as within my area of interest/responsibility? If not, why not?
- What have I learned about making SPI work that could aid in bringing about a continuous security improvement process?
- Am I not in one of the best possible positions to help make this happen?
Why Is Security Improvement So Hard?

Abstract, concerned with hypothetical events

A holistic, enterprise-wide problem; not just technical

No widely accepted metrics

Disaster-preventing rather than payoff-producing (like insurance)

Installing security safeguards can have negative aspects (added cost, diminished performance, inconvenience)
Agenda

Motivation

Perspectives/Questions

Protecting critical assets
  • Security Knowledge in Practice

Identifying risks to critical assets

Role of SEPG?
Security Improvement

Security

• preserving confidentiality, integrity, availability
• avoiding critical asset disclosure, modification, loss/destruction, interruption

Improvement

• assessment
• action planning
• taking action
• feedback

Risk management (enterprise-wide, not at KPA level)
Security Knowledge in Practice℠
Security Knowledge in Practice℠

Security Knowledge in Practice and SKiP are service marks of Carnegie Mellon University

© 2002 by Carnegie Mellon University
Vendor Provides:

- “One Size Fits All” mentality
- Abundant services and features
- Open access to data objects
- Emphasis on ease of use
- Vulnerabilities
- Little to no guidance on how to securely configure
Vendor Provides:

- “One Size Fits All” mentality
- Abundant services and features
- Open access to data objects
- Emphasis on ease of use
- Vulnerabilities
- Little to no guidance on how to securely configure
Harden/Secure:

- Configure operating system as the minimum essential (disable/remove unneeded software/services)
- Install applicable patches
- Use secure applications where available
- Install tools such as virus scanners
- Close lenient access controls (deny first, then allow)
- Enable logging
Harden/Secure:

• Configure operating system as the minimum essential (disable/remove unneeded software/services)
• Install applicable patches
• Use secure applications where available
• Install tools such as virus scanners
• Close lenient access controls (deny first, then allow)
• Enable logging
Security Knowledge in Practice

Prepare:

- Characterize files and directories, the operating system, processes, network traffic and performance, and inventory all hardware
- Develop intrusion detection and response (IDR) policies/procedures
- Manage data collection mechanisms
- Select, configure, and install IDR tools
Security Knowledge in Practice

Prepare:

- Characterize files and directories, the operating system, processes, network traffic and performance, and inventory all hardware
- Develop intrusion detection and response (IDR) policies/procedures
- Manage data collection mechanisms
- Select, configure, and install IDR tools
Security Knowledge in Practice

Detect:

Unexpected changes
  • Acceptable – update characterization
  • Unacceptable - intrusion?

External stimulus
  • Patches/new versions for OS and applications
  • New versions of tools
Detect:

Unexpected changes
  • Acceptable – update characterization
  • Unacceptable - intrusion?

External stimulus
  • Patches/new versions for OS and applications
  • New versions of tools
Security Knowledge in Practice

Respond:

To an intrusion
• Analyze; protect evidence
• Contain
• Return systems to normal operation
• Increase monitoring
• Communicate

To an external stimulus
• Install patch
• Install new tools
Security Knowledge in Practice

Respond:

To an intrusion
- Analyze; protect evidence
- Contain
- Return systems to normal operation
- Increase monitoring
- Communicate

To an external stimulus
- Install patch
- Install new tools
Security Knowledge in Practice

Improve:

• Post mortem
• Update policies and procedures
• Update response tools
• Support business case
Security Knowledge in Practice
Agenda

Motivation

Perspectives/Questions

Protecting critical assets

Identifying risks to critical assets
  • OCTAVE

Role of SEPG?
Identifying Risks to Critical Assets: OCTAVE<sup>SM</sup>

Self-directed method for evaluating information security risks

Conducted in three phases

Elicits knowledge from multiple levels of the organization

Identifies critical assets and threats to assets

Identifies vulnerabilities that expose threats

Develops a protection strategy and risk mitigation plans

Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University
Identifying Risks to Critical Assets: OCTAVE<sup>SM</sup>

Self-directed method for evaluating information security risks

Conducted in three phases

Elicits knowledge from multiple levels of the organization

Identifies critical assets and threats to assets

Identifies vulnerabilities that expose threats

Develops a protection strategy and risk mitigation plans

Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University
OCTAVE\textsuperscript{SM} Process

**Phase 1**
Organizational View
- Assets
- Threats
- Current Practices
- Organization Vulnerabilities
- Security Requirements

**Phase 2**
Technological View
- Key Components
- Technical Vulnerabilities

**Phase 3**
Strategy and Plan Development
- Risks
- Protection Strategy
- Mitigation Plans

Preparation

Progressive Series of Workshops
Phase 1: Organizational View

**Process 1:** Identify Senior Management Knowledge

Senior Management view of critical assets, security requirements, current protection strategy, organizational vulnerabilities

**Process 2:** Identify Operational Area Management Knowledge

Operational Area Management view of critical assets, security requirements, current protection strategy, organizational vulnerabilities

**Process 3:** Identify Staff Knowledge

Staff view of critical assets, security requirements, organizational vulnerabilities

**Process 4:** Create Threat Profile

Consolidated view of critical assets, security requirements, current protection strategy, organizational vulnerabilities, threats to critical assets
Evaluating Practices

Current protection strategy evaluated using surveys and discussions

Provides an understanding of staff behavior in relation to a collection of good security practices

Identifies

• current security practices
• organizational vulnerabilities
Evaluating Threats

Range of threats to critical assets identified using a threat profile

- people using network access
- people using physical access
- system problems
- other problems

Provides an understanding of which threats could affect critical assets

Identifies threat profile for each critical asset
Human Actors - Network Access

Asset-Based Risk Profile

<table>
<thead>
<tr>
<th>asset</th>
<th>access</th>
<th>actor</th>
<th>motive</th>
<th>outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>asset</td>
<td></td>
<td>physical</td>
<td>inside</td>
<td>disclosure, modification, loss/destruction, interruption</td>
</tr>
<tr>
<td></td>
<td>network</td>
<td>system</td>
<td>inside</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>other</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>outside</td>
<td>deliberate, accidental</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Networked Systems Survivability
Human Actors - Network Access

Asset-Based Risk Profile

- Asset: network, physical, system, other
- Access: inside, outside
- Actor: deliberate, accidental
- Motive: disclosure, modification, loss/ destruction, interruption
Phase 2:  
Technological View

- Process 5: Identify Key Components  
  - Key components for critical assets
- Process 6: Evaluate Selected Components  
  - Technology vulnerabilities for key components

Catalog of Vulnerabilities
Phase 2: Technological View

Process 5: Identify Key Components

Process 6: Evaluate Selected Components

Catalog of Vulnerabilities

Key components for critical assets

Technology vulnerabilities for key components
Evaluating Technology Vulnerabilities

Identify key infrastructure components
  • critical asset access paths
  • how threat actors might access a critical asset

Identify technology vulnerabilities using
  • software tools
  • catalog of known vulnerabilities
Phase 3: Risk Analysis

Process 7: Conduct Risk Analysis
- Risks to critical assets

Process 8: Develop Protection Strategy
- Development: Proposed protection strategy, mitigation plans, action
- Selection: Approved protection strategy, mitigation plans, action

Next Steps:
Evaluating Risks

Asset-Based Risk Profile

<table>
<thead>
<tr>
<th>asset</th>
<th>access</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>inside</td>
</tr>
<tr>
<td>physical</td>
<td>outside</td>
</tr>
<tr>
<td>system</td>
<td></td>
</tr>
<tr>
<td>other</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>actor</th>
<th>motive</th>
</tr>
</thead>
<tbody>
<tr>
<td>inside</td>
<td>deliberate</td>
</tr>
<tr>
<td>outside</td>
<td>accidental</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>outcome</th>
<th>impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>loss/destruction</td>
<td>low medium high</td>
</tr>
<tr>
<td>modification</td>
<td>low medium high</td>
</tr>
<tr>
<td>disclosure</td>
<td>low medium high</td>
</tr>
</tbody>
</table>

Outcome | Impact  | Description
---|---------|-----------------
Interruption | High    | Inability to access prescription order system disrupts sales and harms reputation
Building Strategy and Mitigation Plans

Protection strategy provides direction for future information security efforts

• structured around a catalog of practices

Risk mitigation plans focus on activities to

• recognize or detect threats as they occur
• resist or prevent threats from occurring
• recover from threats if they occur
Risk Mitigation Plans

Mitigation Actions

1. Establish vulnerability management practice
2. Define policies for security management across the organization
3. Define and enforce sanctions for security violations
4. Establish defined roles and responsibilities for all personnel
5. Build awareness briefing and deliver to all employees
6. Identify required security-related training for IT personnel
Some Keys to Success
[sound familiar?]

Get senior management sponsorship (visible, continuous)

Select the right analysis team

Scope OCTAVE to address most important operational areas

Select committed participants, willing to openly communicate
Agenda

Motivation

Perspectives/Questions

Identifying risks to critical assets

Protecting critical assets

• Security Knowledge in Practice

Role of SEPG?
Questions to Consider

As a SEPG member

- Do I consider security improvement as within my area of interest/responsibility? If not, why not?
- What have I learned about making SPI work that could aid in bringing about a continuous security improvement process?
- Am I not in one of the best possible positions to help make this happen?
Net Present Value of Information Security

Value that is created when barriers to e-business are removed

Realized when appropriate access is facilitated
Six Tips for Selling Security

Establish Need Before Cost
Hit 'Em with Numbers
Use Others' Loss to Your Advantage
Put It in Legal Terms
Keep It Simple
Six Tips for Selling Security

- Establish Need Before Cost
- Hit 'Em with Numbers
- Use Others' Loss to Your Advantage
- Put It in Legal Terms
- Keep It Simple
Opportunity for SEPGs

Next big improvement push?

A legitimate technology improvement process, with heightened visibility since 9/11?

Career opportunity? SEPG members are in the ideal position.
For More Information

CERT web site

OCTAVE Method Implementation Guide

The CERT Guide to System and Network Security Practices

CERT Security Improvement Modules
For More Information

CERT web site

OCTAVE Method Implementation Guide

The CERT Guide to System and Network Security Practices

CERT Security Improvement Modules