Maturing Your Approach to “Security Management”

Richard A Caralli, William R Wilson
Survivable Enterprise Management Team

Networked Systems Survivability
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Sponsored by the U.S. Department of Defense
© 2004 by Carnegie Mellon University
Key topics

Challenges for doing “security”

Security approach roadblocks

New perspectives on the problem

Maturing your security approach
Organizational challenges - 1

Scope of security is the entire organization

Requires management and technologists to work together

Industry bias toward technology solutions

Forces constant risk vs. reward trade-offs

Not naturally a profit-centric activity
Organizational challenges - 2

Not a core competency of an organization

Requires everyone in the organization to play a part

Everyone has a different view and objective

Lack of common language and lexicon

Lack of data and metrics
Why do we fail?

There are several natural barriers to effectiveness

May be unlike any problem organizations have had to solve (somewhat resembles Y2K)

Complex problem requires an adaptive, flexible approach
Common problems

Defining the wrong target

Focusing too narrowly

Treating security as a technical specialty

Managing to regulations

Failure to recognize complexity
## Defining the wrong target

### Problem

The desired outcome of the security approach is ambiguous.

### Symptoms

- Unclear security goals
- Goals not well communicated
- No measures for success
- Can’t assure stakeholders that “security” has been accomplished
## Narrow focus

<table>
<thead>
<tr>
<th>Problem</th>
<th>Symptoms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus of security approach technology-centric</td>
<td>Security viewed as a technology problem</td>
</tr>
<tr>
<td></td>
<td>Assumption that secure technology = secure organization</td>
</tr>
</tbody>
</table>
Technical specialty

Problem

Implementation and monitoring of security approach is a technical specialty.

Symptoms

CSO/CISO and security professionals in technical roles

IT is exclusive domain of security activities

IT owns security approach or strategy

“Windows will approach 100 million lines of code, and the average PC, while it may cost $99, will contain nearly 200 million lines of code. And within that code, 2 million bugs.”

Source: Scott Berinato, CIO Magazine, December 15, 2003
Regulation-driven

**Problem**

Regulatory compliance defines the purpose and direction of the security approach.

**Symptoms**

- Regulations overly influence the approach
- Comply with regulations = secure organization
- Security standards derived from regulations
# Lack of flexibility

## Problem

The security approach cannot adapt to changing environmental conditions.

## Symptoms

<table>
<thead>
<tr>
<th>Security approach quickly obsolete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approach out of synch with organization’s strategic objectives</td>
</tr>
<tr>
<td>Time spent on securing assets that are not critical to accomplishing the mission</td>
</tr>
</tbody>
</table>

"The chief security officer should now be positioned as a trusted advisor to the business, moving away from operational delivery towards understanding and managing risk."

Organizational impacts

Misalignment of operational and security goals

False sense of accomplishment

Failure to utilize all necessary skills/resources

Compliance at the expense of effectiveness

Approach breaks at every twist and turn

Overall ability to manage security is impaired
Maturing your approach
Change your perspective

Expand your objective

Let the organization drive

Embrace the resiliency concept
Expand your objective

View the organization as the benefactor of “security” not IT

Change perspective from technical “network” to organizational “network”

Aim to make the organization’s mission both sustainable and adaptable to its environment
Let the organization drive

Use organizational drivers—mission, strategic objectives, goals, CSFs—as the foundation for security

Align security strategy and approach with drivers and ensure they are adaptable to changes

Aim for sponsorship as high in the organization as possible
Move from security to resiliency
What is resiliency?

Physical property of a material that allows it to spring back after deformation that has not exceeded its elastic limit \[www.cogsci.princeton.edu\]

“. . .ability to withstand systemic discontinuities”
[Booz Allen]

“. . .ability to adapt to new risk environments”
[Booz Allen]

Source: Booz Allen - Enterprise Resilience: Managing Risk in the Networked Economy
Security vs. resiliency

Security
- Asset-focused
- Reactive
- Protective (defensive posture)
- Maintain and sustain
- Active

Resiliency
- Organization-focused
- Proactive
- Adaptive (offensive posture)
- Sustain and improve
- Transparent
Resilient organizations

Align capabilities to collaborate

Elevate risk management to organizational level

Rely on the system of internal controls

Sense, respond, and improve

Establish transparency
Moving toward resiliency - 1

Sharpen the target

Utilize critical success factors for alignment

Utilize and mobilize the capabilities of the organization

Involve the right people—spread responsibility throughout organization
Moving toward resiliency -2

Rely on operational excellence

Rely on strong system of internal controls

Manage as a process and improve

Select metrics for success and measure!
Questions?
For more information

Networked Systems Survivability Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA  15213 USA

www.sei.cmu.edu
www.cert.org

Rich Caralli
rcaralli@sei.cmu.edu
Presentation references

