Governing for Enterprise Security

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

© CERT, CERT Coordination Center, OCTAVE, CMM, CMMI, and Carnegie Mellon are registered in the U.S. Patent and Trademark Office

Sponsored by the U.S. Department of Defense
Definition

“Directing and controlling an organization to establish and sustain a culture of security in the organization's conduct (beliefs, behaviors, capabilities, and actions)”

Builds upon and expands commonly described forms of governance including corporate governance, enterprise governance, and information technology (IT) governance
Questions to Ask

What is at risk?

How much security is enough?

How does an enterprise
  • evolve its approach to security?
  • achieve and sustain adequate security?
Questions to Ask

What is at risk?

How much security is enough?

How does an enterprise
  • evolve its approach to security?
  • achieve and sustain adequate security?
What Is At Risk?

• Trust
• Reputation; brand
• Shareholder/stakeholder value
• Market confidence, share, capitalization
• Regulatory compliance; fines, jail time
• Customer retention, growth
• Customer and partner identity, privacy
• Ability to offer, fulfill business transactions
• Staff morale
Trust

“The central truth is that information security is a means, not an end. Information security serves the end of trust. Trust is efficient, both in business and in life; and misplaced trust is ruinous, both in business and in life.

Trust makes it possible to proceed where proof is lacking. As an end, trust is worth the price. Without trust, information is largely useless.”

[Dan Geer; “Why Information Security Matters”]
Responsibility to Protect Digital Assets

Duty of Care: D&O Governance of Corporate Digital Security
• Govern business operations; protect critical assets
• Protect market share, stock price
• Govern employee conduct
• Protect reputation
• Ensure compliance requirements are met

Business Judgment Rule: That which a reasonably prudent director of a similar corporation would have used

[Jody Westby, PricewaterhouseCoopers, Congressional Testimony; case law]
Barriers to Tackling Security

- Abstract, concerned with hypothetical events
- A holistic, enterprise-wide problem; not just technical
- No widely accepted measures/indicators
- Disaster-preventing rather than payoff-producing (like insurance)
- Installing security safeguards can have negative aspects (added cost, diminished performance, inconvenience)
Questions to Ask

What is at risk?

How much security is enough?

How does an enterprise
  • evolve its approach to security?
  • achieve and sustain adequate security?
### Shift the Security Perspective

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope: Technical problem</td>
<td>Enterprise problem</td>
</tr>
<tr>
<td>Ownership: IT</td>
<td>Enterprise</td>
</tr>
<tr>
<td>Funding: Expense</td>
<td>Investment</td>
</tr>
<tr>
<td>Focus: Intermittent</td>
<td>Integrated</td>
</tr>
<tr>
<td>Driver: External</td>
<td>Enterprise</td>
</tr>
<tr>
<td>Application: Platform/practice</td>
<td>Process</td>
</tr>
<tr>
<td>Goal: IT security</td>
<td>Enterprise continuity/resilience</td>
</tr>
</tbody>
</table>
Security to Resiliency

Managing to threat and vulnerability
No articulation of desired state
Possible security technology overkill

Managing to impact and consequence
Adequate security defined as desired state
Security in sufficient balance to cost, risk
A Resilient Enterprise Is Able To. . .

• withstand systemic discontinuities and adapt to new risk environments [Starr 03]
• be sensing, agile, networked, prepared [Starr 03]
• dynamically reinvent business models and strategies as circumstances change [Hamel 04]
• have the capacity to change before the case for change becomes desperately obvious [Hamel 04]
Security Strategy Questions

• What needs to be protected? Why does it need to be protected? What happens if it is not protected?

• What potential adverse consequences need to be prevented? At what cost? How much disruption can we stand before we take action?

• How do we effectively manage the residual risk when protection and prevention actions are not taken?
Defining Adequate Security

The condition where the protection strategies for an organization's critical assets and business processes are commensurate with the organization's risk appetite and risk tolerances.


http://www.cert.org/governance/adequate.html
Determining Adequate Security Depends On . . .

- Enterprise factors: size, complexity, asset criticality, dependence on IT, impact of downtime
- Market sector factors: provider of critical infrastructure, openness of network, customer privacy, regulatory pressure, public disclosure
- Principle-based decisions: Accountability, Awareness, Compliance, Effectiveness, Ethics, Perspective/Scope, Risk Management, etc.

http://www.cert.org/governance/ges-aware.html
http://www.cert.org/governance/stakeholder.html
Adequate Security and Operational Risk

“Appropriate business security is that which protects the business from undue operational risks in a cost-effective manner.” [Sherwood 03]

“With the advent of regulatory agencies assessing a business’s aggregate operational risk, there needs to be a way of looking at the organization as a whole rather than its many parts.” [Milus 04]

[According to Basel II, operational risks are risks of loss resulting from inadequate or failed internal processes, people, and systems or from external events. http://www.bis.org/publ/bcbs107.htm]
Questions to Ask

What is at risk?

How much security is enough?

How does an enterprise
  • evolve its approach to security?
  • achieve and sustain adequate security?
Evolving the Security Approach
Questions to Ask

What is at risk?

How much security is enough?

How does an enterprise
  • evolve its approach to security?
  • achieve and sustain adequate security?
Shift the Security Approach

Ad-hoc and tactical  to  Managed and strategic

- irregular
- reactive
- immeasurable
- absolute

- systematic
- adaptive
- measured
- adequate

Security activities and measures of security performance are visibly aligned with strategic drivers and critical success factors.
Deriving a Framework

- Standards, guidelines, & practices
- Fieldwork & experience
- High performing organizations
- Capabilities Framework

High performing organizations → Capabilities Framework → Fieldwork & experience → Standards, guidelines, & practices
Notional Set of Capabilities

Asset Management
Audit
Crisis Management
Enterprise Security Governance
IT Operations
Partner Management

Physical/Facilities Management
Process Management
Project Management
Risk Management
Security Operations
Systems Development
User Management
Mobilizing Capabilities to Achieve/Sustain Adequate Security

Critical Success Factors: determine priorities

ES Governance: policy, oversight, sponsorship

Risk Mgmt: clarifies risk tolerance, impacts

Audit: evaluates

IT Ops: delivers secure service, protects assets

Project Mgmt: plans, tracks, ensures completion

Process Mgmt: enables

Security: defines controls for key IT ops processes
Critical Success Factors: determine priorities

ES Governance: policy, oversight, sponsorship

Audit: evaluates

IT Ops Processes
- Asset Management
- Release Mgmt
- Configuration Mgmt
- Change Mgmt

Risk Mgmt: clarifies risk tolerance, risks, impacts

Audit: evaluates

Determine Current State

Findings
- Extent of compliance
- Recommendations

IT Ops: delivers secure service, protects assets

Mobilizing to Achieve/Sustain Adequate Security Security: defines controls for key IT ops processes

Project Mgmt: plans, tracks, ensures completion

Prioritized tasking

Prioritized tasking

Process Mgmt: enables

Contributing process areas

Process definitions

Status, Plan updates, Resources, Measures, New improvements, Business case data

Prioritized tasking

Tasks, Improvements

Strategies, Recommendations, Actions

Plan inputs, priorities

Findings

Results

Evaluation, Eval criteria

IT Ops Processes
- Problem/Incident Mgmt
- Availability Management
- Integrity Management
- Confidentiality/Privacy Management

Requirements
- Controls
- Process steps

Actions, Process Definitions, Measures, Status, Plan updates

Security: defines controls for key IT ops processes

© 2005 by Carnegie Mellon University
What Does Effective Security Look Like at the Enterprise Level?

• No longer solely under IT’s control
• Achievable, measurable objectives are defined and included in strategic and operational plans
• Functions across the organization view security as part of their job (e.g., Audit) and are so measured
• Adequate and sustained funding is a given
• Senior executives visibly sponsor and measure this work against defined performance parameters
• Considered a requirement of being in business
What Is Internal Audit’s Role?

• Leverage Audit’s professionalism and enterprise-wide scope
• Supplement compliance activities with risk assessment and process improvement
• Create an enterprise-wide risk-based audit program(*)
• Broaden audit scope to address third-party and vendor risk
• Collaborate with IT to mitigate information systems risk proactively

(*) including enterprise security

Why Should Internal Audit Care?

Responsible for evaluating the adequacy and effectiveness of controls
  • Reliability and integrity of financial, operational information
  • Effectiveness, efficiency of operations
  • Safeguarding assets
  • Compliance with laws, regulations, contracts

Brings a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes

[IIA, Tone at the Top, Issue 23, October 2004.]
For More Information

- Enterprise Security Management (http://www.cert.org/nav/index_green.html)
- CERT web site (http://www.cert.org); ITPI web site (http://www.itpi.org); SEI web site (http://www.sei.cmu.edu)
- jha@cert.org
References


