



Information Security as an Institutional Priority

Julia H. Allen
Networked Systems Survivability/CERT
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

What Might Security as an Institutional Priority Look Like?

Leaders direct and control the institution to establish and sustain a culture of security in the institution's conduct

- beliefs, values, behaviors, capabilities, and actions

Security is viewed as a non-negotiable requirement of being 'in business.' [Allen 05]

In institutions of higher education: [EDUCAUSE 03]

- Leadership purported to be reactive rather than proactive
- Lack of clearly defined goals
- Goals of security, academic freedom, intellectual freedom viewed as antithetical

Allen, Julia. "Governing for Enterprise Security: An Introduction." June, 2005.
EDUCAUSE Center for Applied Research. "Information Technology Security: Governance, Strategy, and Practice in Higher Education." 2003.

What Might Security as an Institutional Priority Look Like? (cont)

Information security is a human enterprise

- “lack of security awareness by users” cited as top obstacle
- overriding impact of human complexities, inconsistencies, and peculiarities

People can become the most effective layer in an organization's defense-in-depth strategy

- with proper training, education, motivation

The first step is making sure they operate in a *security conscious culture*.

Ernst & Young. "Global Information Security Survey 2004."
[http://www.ey.com/global/download.nsf/UK/Survey_-_Global_Information_Security_04/\\$file/EY_GISS_%202004_EYG.pdf](http://www.ey.com/global/download.nsf/UK/Survey_-_Global_Information_Security_04/$file/EY_GISS_%202004_EYG.pdf)

American Council on Education

Letter to Presidents Regarding Cybersecurity

- Set the tone
- Establish responsibility for campus-wide cybersecurity at the cabinet level
- Ask for a periodic cybersecurity risk assessment
- Request updates to your cybersecurity plans on a regular basis

From ACE President David Ward (February 28, 2003)

<http://www.acenet.edu/washington/letters/2003/03march/cyber.cfm>

EDUCAUSE Framework for Action

- Make IT security a priority in higher education
- Revise institutional security policies; improve the use of existing security tools
- Improve security for future research and education networks
- Improve collaboration between higher education, industry, and government
- Integrate work in higher education with the national effort to strengthen critical infrastructure

Called for in EDUCAUSE “Higher Education Contribution to National Strategy to Secure Cyberspace,” Jul 02 and [EDUCAUSE 03]

Cited in *The National Strategy to Secure Cyberspace*, Feb 03.

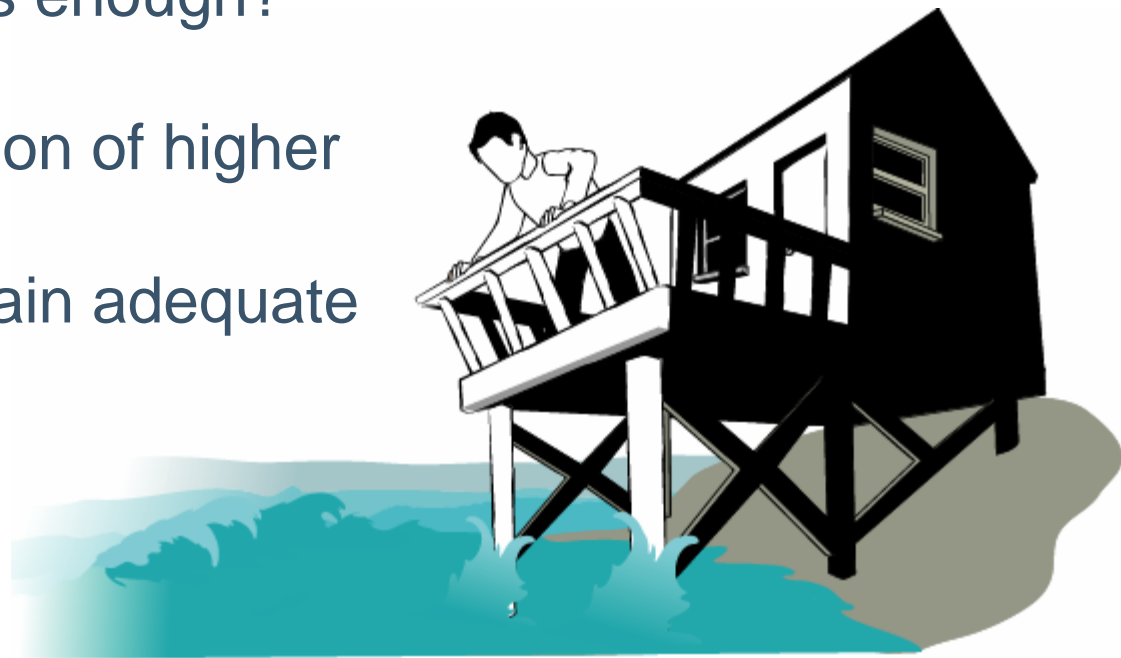
Questions to Ask

What is at risk?

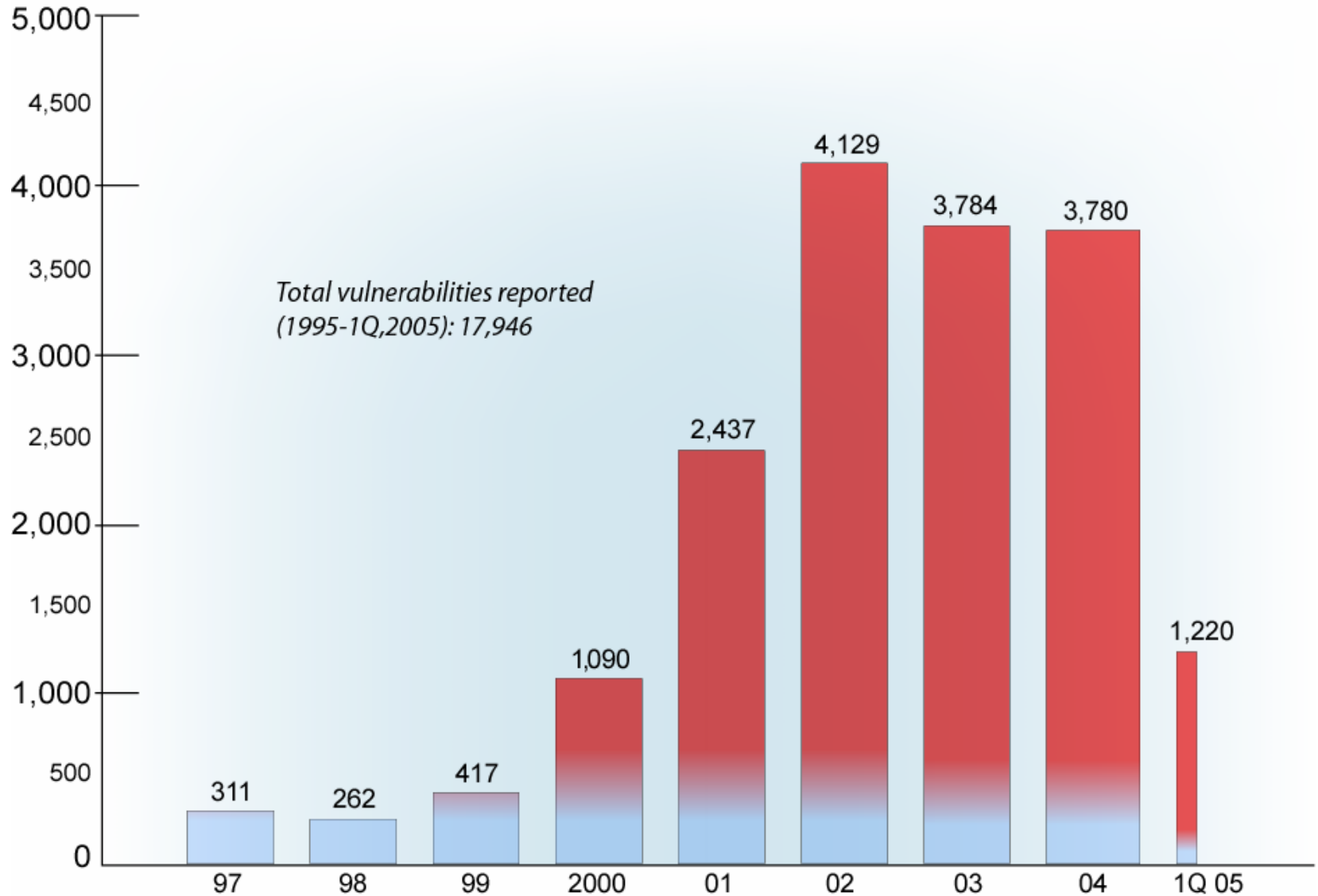
How much security is enough?

How does an institution of higher education (IHE)

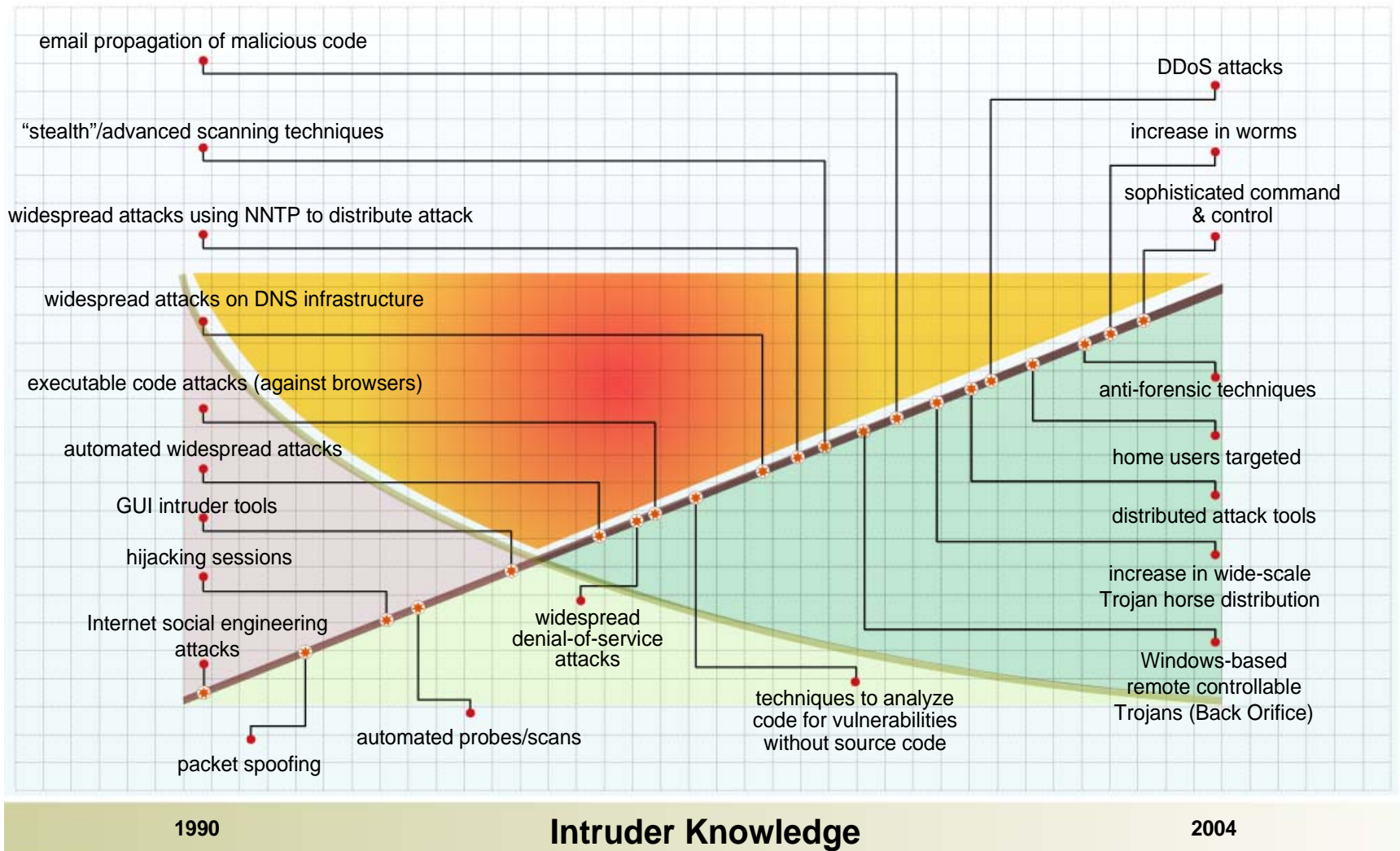
- achieve and sustain adequate security?



Growth in Number of Vulnerabilities Reported to the CERT/CC

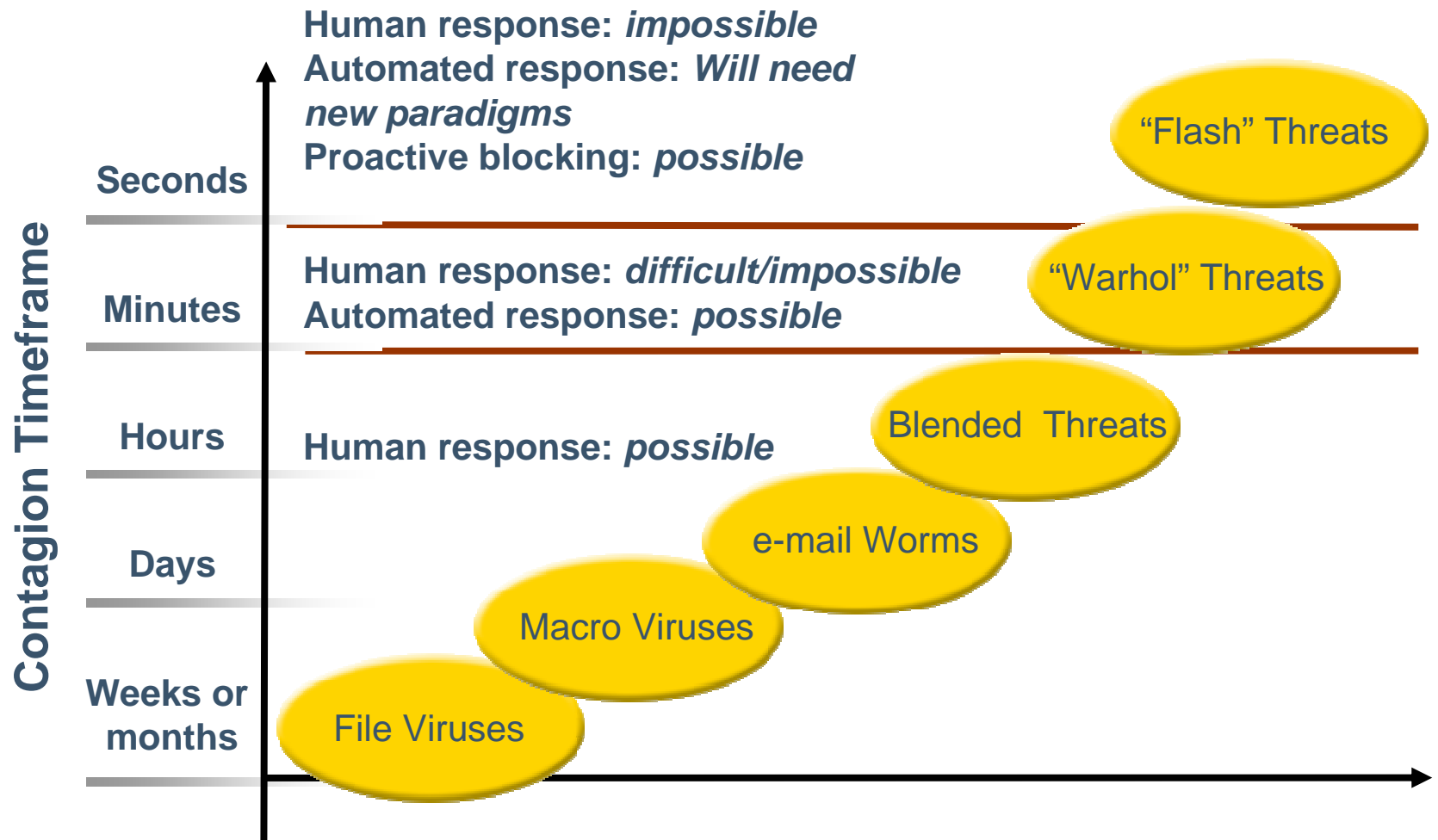


Attack Sophistication vs. Intruder Knowledge



Attack Sophistication

Response Time



What Is At Risk?

- Trust
- Reputation; image
- Stakeholder value
- Community confidence
- Regulatory compliance; fines, jail time
- “Customer” retention, growth (staff, faculty, students, alumni, funding agencies)
- “Customer” and partner identity, privacy
- Ability to offer, fulfill transactions
- Staff, student 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.”

Geer, Daniel E. “Why Information Security Matters.” Cutter Consortium Business-IT Strategies Vol. 7, No. 3, 2004.

Responsibility to Protect Digital Assets

In excess of 80 percent of an organization's intellectual property is in digital form [Business Week]

Duty of Care: Governance of Digital Security

- Govern institutional operations
- Protect critical assets and processes
- Govern employee conduct
- Protect reputation
- Ensure compliance requirements are met

Business Judgment Rule: That which a reasonably prudent director of a similar institution 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)



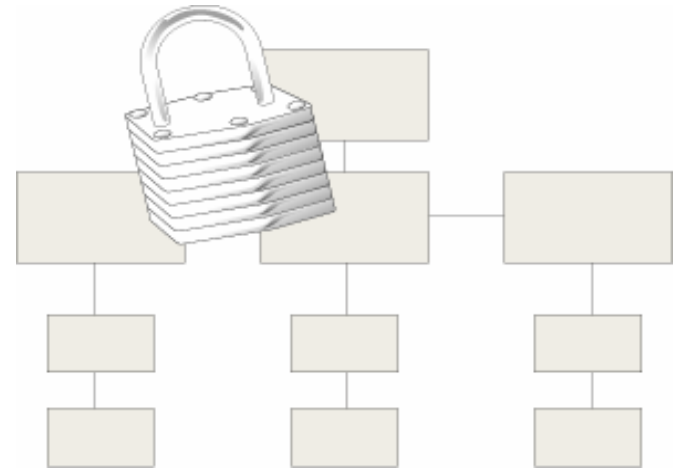
Questions to Ask

What is at risk?

How much security is enough?

How does an IHE

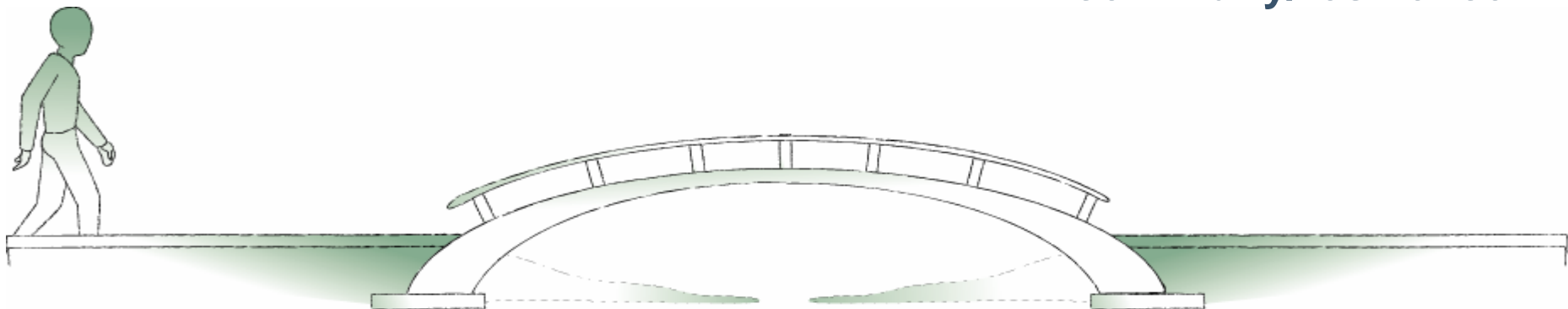
- achieve and sustain adequate security?



Shift the Security Perspective

From  *To*

Scope:	Technical problem	Institutional problem
Ownership:	IT	Institutional
Funding:	Expense	Investment
Focus:	Intermittent	Integrated
Driver:	External	Institution
Application:	Platform/practice	Process
Goal:	IT security	Institutional continuity/resilience



Security *to* Resiliency

Managing to threat and vulnerability

No articulation of desired state

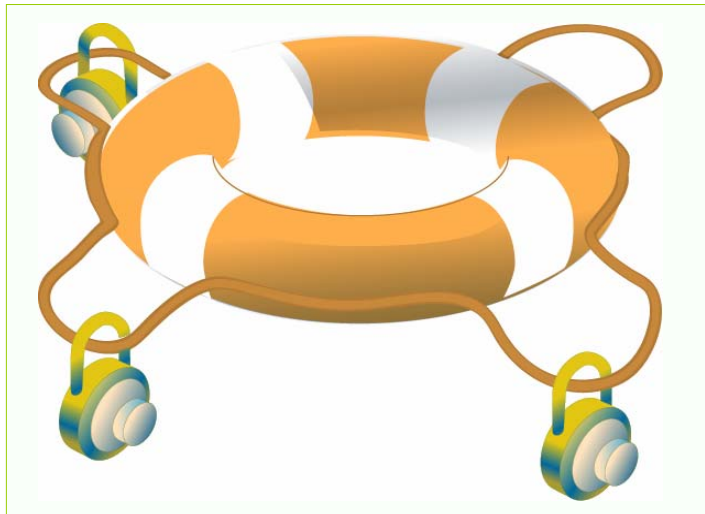
Possible security technology overkill

to
→

Managing to impact and consequence

Adequate security defined as desired state

Security in sufficient balance to cost, risk



A Resilient Institution Is Able To . . .

- withstand systemic discontinuities and adapt to new risk environments [Starr 03]
- be sensing, agile, networked, prepared [Starr 03]
- dynamically reinvent institutional 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?

Defining Adequate Security

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

Risk appetite and risk tolerance as defined by COSO's Enterprise Risk Management Integrated Framework, September, 2004.

[Allen 05]

Determining Adequate Security Depends On . . .

- Organizational factors: size, complexity, asset criticality, dependence on IT, impact of downtime
- Market 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.

[Allen 05]

Adequate Security and Operational Risk

“Appropriate security is that which protects the organization from undue operational risks in a cost-effective manner.”

[Sherwood 03]

“With the advent of regulatory agencies assessing a organization’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>]

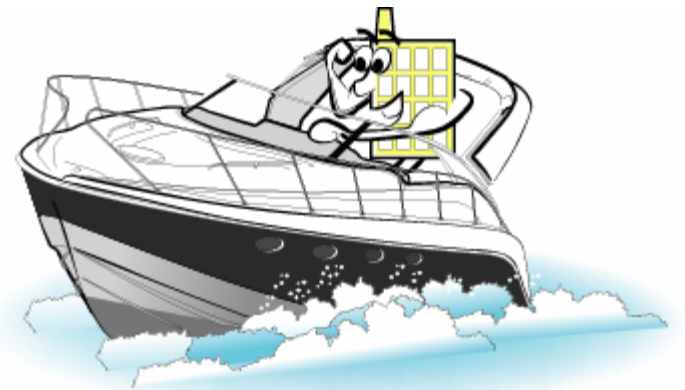
Questions to Ask

What is at risk?

How much security is enough?

How does an IHE

- achieve and sustain adequate security?

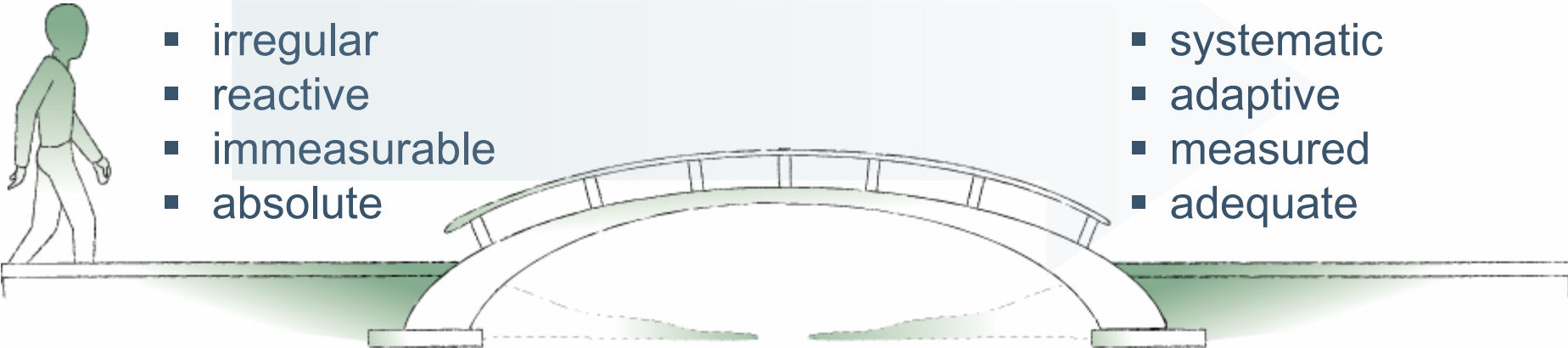


Shift the Security Approach

Ad-hoc and
tactical

to

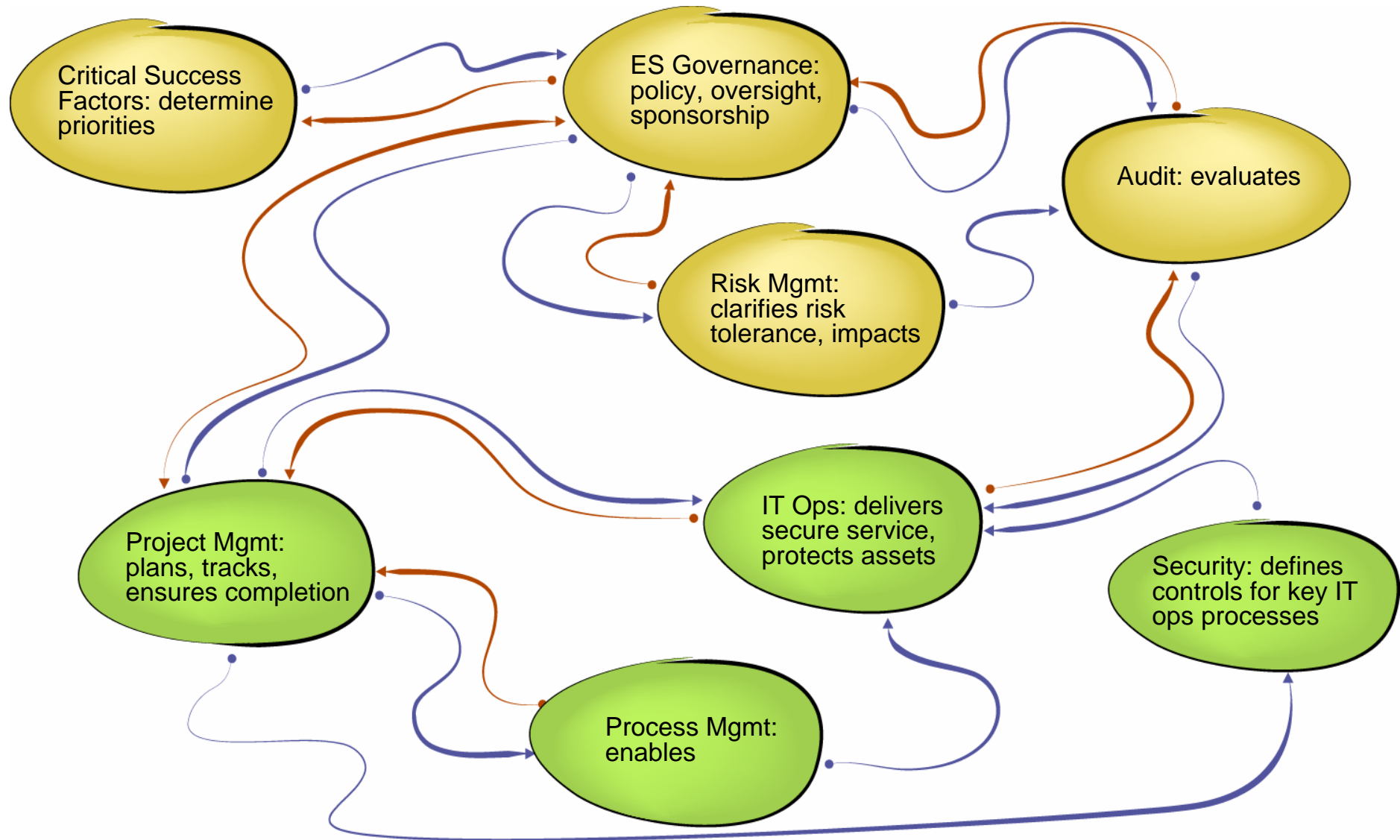
Managed and
strategic

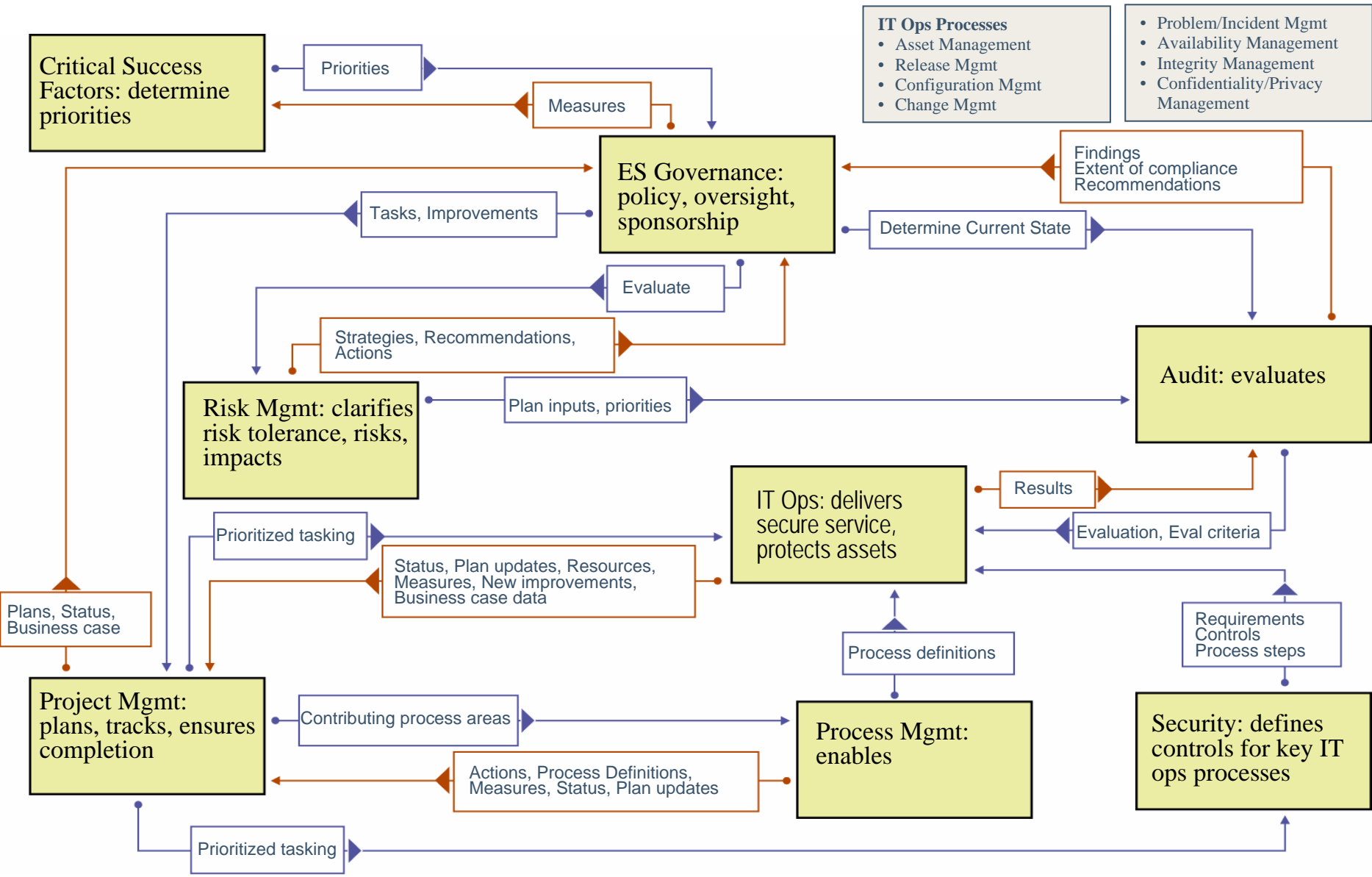
- 
- irregular
 - reactive
 - immeasurable
 - absolute

- systematic
- adaptive
- measured
- adequate

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

Mobilizing Capabilities to Achieve/Sustain Adequate Security





What Might Security as an Institutional Priority Look Like? (cont)

- No longer solely under IT's control
- Achievable, measurable objectives are defined and included in strategic and operational plans
- Departments/functions across the institution view security as part of their job (e.g., HR, Audit) and are so measured
- Adequate and sustained funding is a given
- Senior leaders visibly sponsor and measure this work against defined performance parameters
- Considered a requirement of being 'in business'

Information Security Governance Resources

April 2004: Corporate Governance Task Force report on Information Security Governance (Appendix E)

<http://www.cyberpartnership.org/init-governance.html>;

November 2004: EDUCAUSE ISG Assessment Tool for Higher Education

<http://www.educause.edu/LibraryDetailPage/666?ID=SEC0421>

Section I: Organizational Reliance on IT

Section II: Risk Management

Section III: People

Section IV: Processes

Section V: Technology

Legal Perspective: IT Security for Higher Education

- Analyze applicable state laws and municipal ordinances
- Assess IS vulnerabilities and risks
- Review and update IS policies & procedures
- Review personnel policies & procedures for access to sensitive information
- Scrutinize relationships with third-party vendors
- Review the institution's insurance policies
- Develop a rapid response plan & incident response team
- Work together with higher education associations & coalitions to develop standards relating to IS

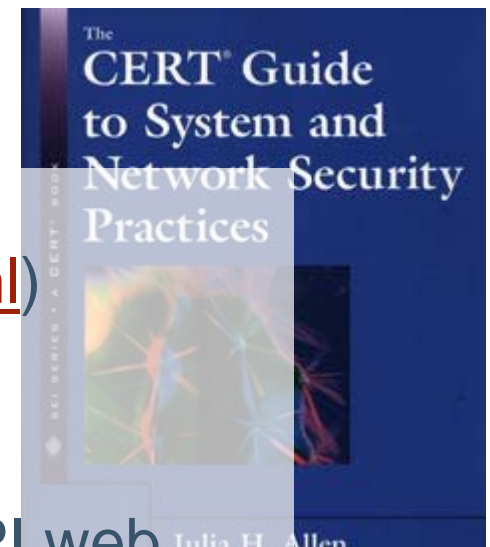
“IT Security for Higher Education: A Legal Perspective.” Salomon, Kenneth; Cassat, Peter; Thibeau, Briana. Dow, Lohnes & Albertson, PLLC. EDUCAUSE/Internet2 Computer and Network Security Task Force, 2003. <http://www.educause.edu/ir/library/pdf/csd2746.pdf>

EDUCAUSE Resources

- Center for Applied Research (ECAR):
<http://www.educause.edu/ecar>
- Security Task Force:
<http://www.educause.edu/security>
- The Effective IT Security Guide for Higher Education
- Computer and Network Security in Higher Education
- Security Discussion Group
- Security Professionals Conference

For More Information

- Governing for Enterprise Security (<http://www.cert.org/governance/ges.html>)
- 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

[Hamel 04] Hamel, Gary; Valikangas, Liisa. “The Quest for Resilience,” Harvard Business Review, September 2003.

[Milus 04] Milus, Stu. “The Institutional Need for Comprehensive Auditing Strategies.” Information Systems Control Journal, Volume 6, 2004.

[Sherwood 03] Sherwood, John; Clark; Andrew; Lynas, David. “Systems and Business Security Architecture.” SABSA Limited, 17 September 2003. Available at http://www.alctraining.com.au/pdf/SABSA_White_Paper.pdf.

[Starr 03] Starr, Randy; Newfrock, Jim; Delurey, Michael. “Enterprise Resilience: Managing Risk in the Networked Economy.” strategy+business, Spring 2003. Also appears in “Enterprise Resilience: Risk and Security in the Networked World: A strategy+business Reader.” Randall Rothenberg, ed.

[Westby 04] Westby, Jody. “Information Security: Responsibilities of Boards of Directors and Senior Management.” Testimony before the House Committee on Government Reform: Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, September 22, 2004. Available at <http://www.reform.house.gov/UploadedFiles/Westby1.pdf>.