Security in Cyberspace
Protecting Critical Communications Infrastructures

FCC's Broadband Workshop on Cyber Security

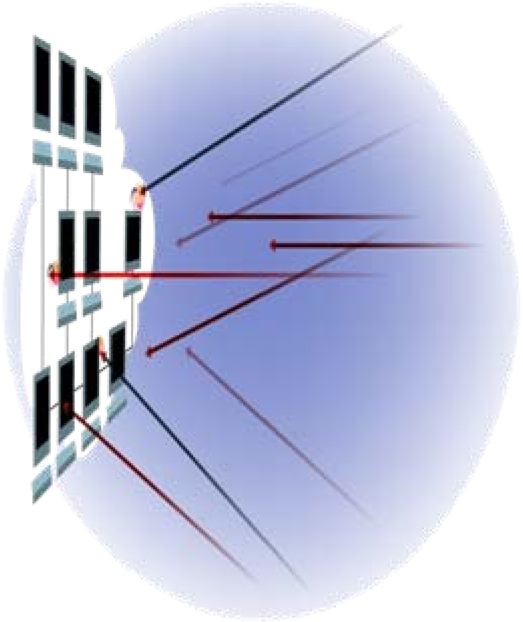
Rich Pethia
September 30, 2009

The Evolving Cyber Threat

“Perhaps the most significant challenge we face is the constantly evolving nature of the threat in cyberspace. Threats in cyberspace move at the speed of light, and we are literally under attack every day as our networks are constantly probed, and our adversaries seek to exploit vulnerabilities in our network enterprise. To keep pace with the efforts of our adversaries, we need a robust research and development effort to keep us ahead of those who would seek to damage our information networks.”

- Lieutenant General William L. Shelton, USAF, 5 May 2009

Chief, Warfighting Integration and Chief Information Officer in testimony before the House Armed Services Committee



Strategic Relevance

Attacks on National critical information infrastructures are common and increasing

A complex cyber ecosystem has evolved

Systems

- Today’s software and systems are typically vulnerable to many forms of attack – new vulnerabilities are found every day
- The technologies we use come from hundreds of vendors
  - Questionable provenance and integrity – poorly understood supply chain

Unbounded Systems of Systems Issues

- Operational interdependence of elements that are managed independently
- Open, dynamic, evolving networks with unexpected emergent behavior
- No central administrative control
- No global visibility

Information Operations

- Computer Network Defense techniques, tactics and practices largely protect individual systems and networks rather than critical operations (missions)
- Unclear mapping between critical national functions and their underlying systems
- Attack technology outpacing defense technology
- Growing body of cyber attackers & mercenaries (theft, espionage, destruction)
- Large scale coordinated attacks

Workforce Development

- Short supply and inability to retain qualified cadre of cyber professionals
- Lack of awareness and understanding of cybersecurity issues among many cyber decision makers

One Dilemma we face

A robust, resilient broadband communications infrastructure is needed to deliver bits and provide services to critical national information infrastructure operators

The same communications infrastructure is being used by attackers to robustly deliver attacker’s bits to the organizations they target

Defending the communications infrastructure is necessary, but not sufficient to defend against attacks on other critical information infrastructures

Communications infrastructure operators have a key role to play in improving the security of the overall ecosystem

An effective defense requires an ongoing process

High levels of security and resiliency can be achieved by managing a process that harmonizes **operational risk management activities** that have similar objectives and outcomes

Operational risk management activities include

- Security planning and management
- Business continuity and disaster recovery
- I/T operations and service delivery management

- Note: see http://www.cert.org/resiliency for more information on resiliency management

Existing codes of practice and standards provide a strong foundation

- BS25999-1:2006
- CMMI v1.2
- CMMI for Services
- CobiT 4.1
- COSO ERM
- DRII GAP
- FFIEC Handbooks (Security, BCP)
- ISO 20000-1:2005(E)
- ISO 20000-2:2005(E)
- ISO 24762:2008(E)
- ISO 27001:2005
- NFPA 1600 (2007)
- PCI DSS v1.1
- Val-IT

ISO SE7 Application Security Std

HR1-Title 9 Voluntary Standard

NIST standards/FISMA provisions

Resiliency Management Model at a Glance

Requirements Management

RRD – Resiliency Requirements Development

RRM – Resiliency Requirements Management

Asset Management

ADM – Asset Definition and Management

Establishing Resiliency

SC – Service Continuity

CTRL – Controls Management

RTSE – Resilient Technical Solution Engineering

Governance, Risk, & Compliance

COMP – Compliance

EF – Enterprise Focus

RISK – Risk Management

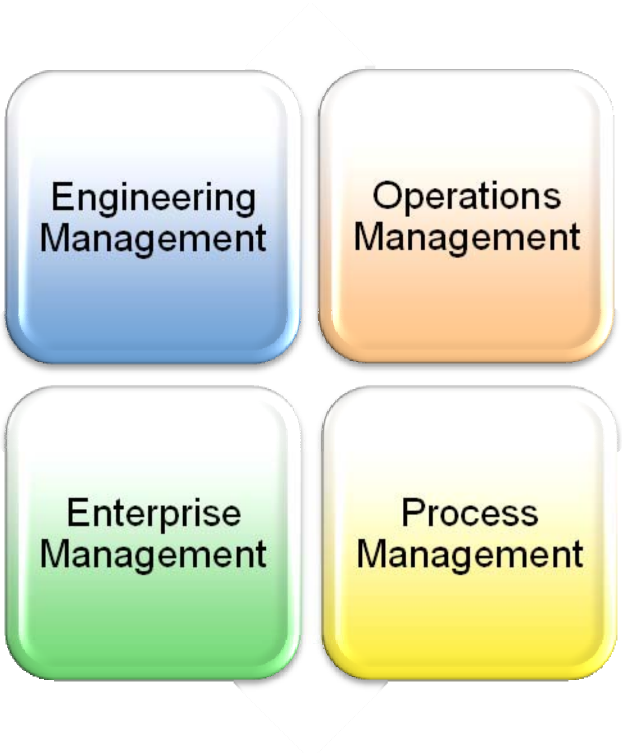
Supporting Resiliency

COMM – Communications

FRM – Financial Resource Management

HRM – Human Resource Management

OTA – Organizational Training & Awareness



Engineering Management

Operations Management

Enterprise Management

Process Management

Asset Resiliency Management

EC – Environmental Control

KIM – Knowledge & Information Management

PM – People Management

TM – Technology Management

Sourcing

EXD – External Dependencies

Threat, Incident, & Access Management

AM – Access Management

ID – Identity Management

IMC – Incident Management & Control

VAR – Vulnerability Analysis & Resolution

Data Collection & Logging

MON – Monitoring

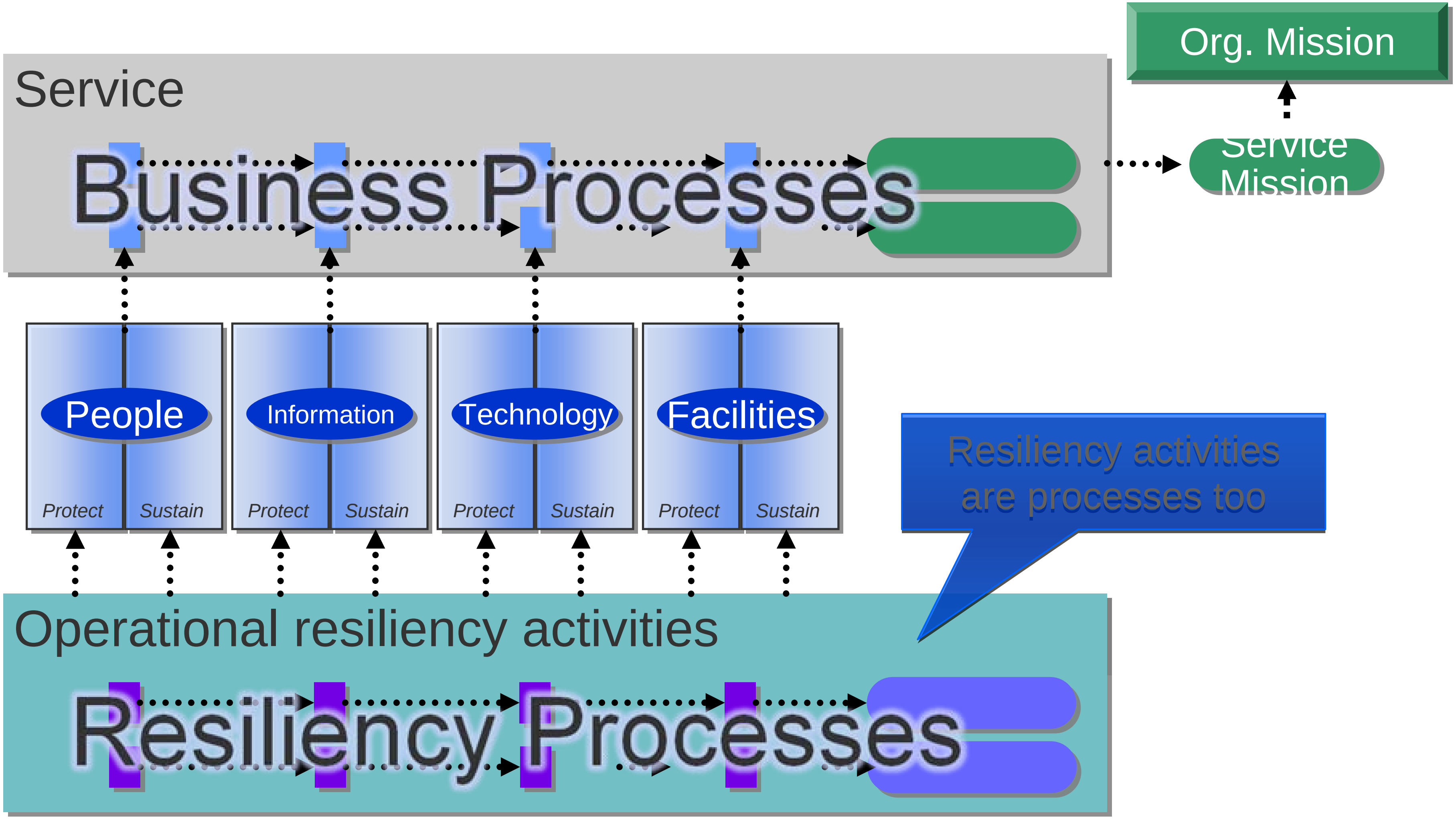
Process Management

MA – Measurement and Analysis

OPD – Organizational Process Definition

OPF – Organizational Process Focus

Enterprise view of resiliency management



Service Providers can help Improve the Cyber Ecosystem

Building awareness and understanding

- Publications to customers to build awareness of security issues
- Timely alerts on new threats, vulnerabilities, mitigation practices
- “How to’s” that promote effective security practices

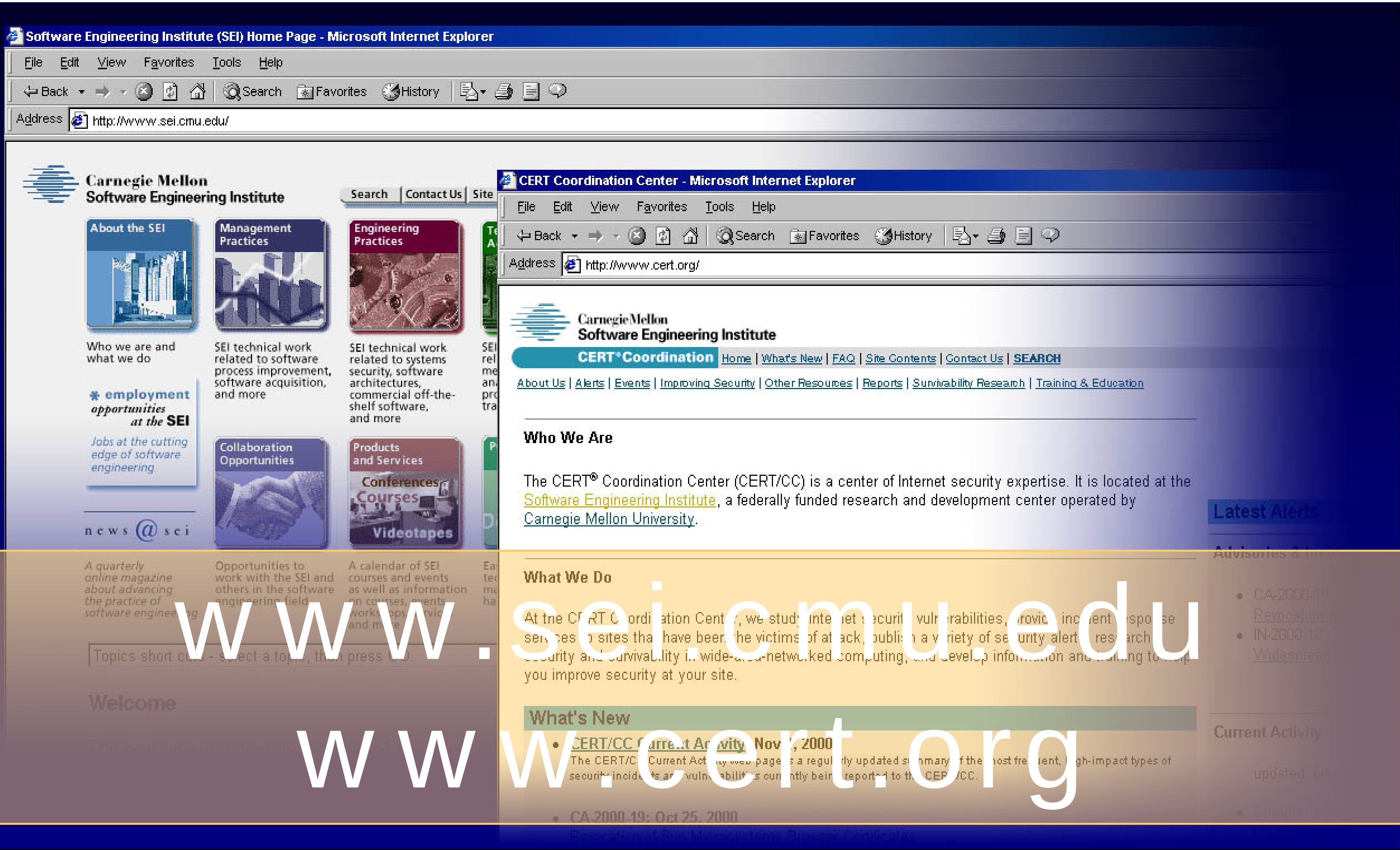
Active network defense

- Ingress filtering to
  - –Filter out packets with spoofed IP addresses
  - –Filter out packets from distributed denial of service attacks
- Cooperation with response organizations in locating and disabling botnet nodes
- Cooperation with law enforcement in cyber attack investigations

Security services

- Direct support to customers to defend against and respond to attacks
  - –Security assessments
  - –Monitoring for and responding to attacks and intrusions
  - –Managing network connections, firewalls, etc.

For more Cyber Security Information


Software Engineering Institute (SEI) Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://www.sei.cmu.edu/
Carnegie Mellon Software Engineering Institute
Search | Contact Us | Site
About the SEI
Management Practices
Engineering Practices
Collaboration Opportunities
Products and Services
Conferences Courses Videotapes
employment opportunities at the SEI
news @ sei
Welcome

Who we are and what we do

SEI technical work related to software process improvement, software acquisition, and more

SEI technical work related to systems security, software architectures, commercial off-the-shelf software, and more

Jobs at the cutting edge of software engineering

A quarterly online magazine about advancing the practice of software engineering

Opportunities to work with the SEI and others in the software engineering field

A calendar of SEI courses and events as well as information on courses, events, workshops, services and more

Topics short cuts - select a topic, then press GO.

CERT Coordination Center - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://www.cert.org/
Carnegie Mellon Software Engineering Institute
CERT® Coordination
Home | What's New | FAQ | Site Contents | Contact Us | SEARCH
About Us | Alerts | Events | Improving Security | Other Resources | Reports | Survivability Research | Training & Education
Latest Alerts
Advisories & Inc
Current Activity

Who We Are

The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise. It is located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

What We Do

At the CERT Coordination Center, we study Internet security vulnerabilities, provide incident response services to sites that have been the victims of attack, publish a variety of security alerts, research security and survivability in wide-area-networked computing, and develop information and training to help you improve security at your site.

What's New

- CERT/CC Current Activity Nov , 2000
  The CERT/CC Current Activity web page is a regularly updated summary of the most frequent, high-impact types of security incidents and vulnerabilities currently being reported to the CERT/CC.
- CA-2000-19: Oct 25, 2000
  Revocation of Sun Microsystems Browser Certificates

- CA-2000-19 Revocation
- IN-2000-10 Widespread

updated

www.sei.cmu.edu

www.cert.org