ABCs of Operational Resilience

Nader Mehravari
Research Scientist, CERT® Division

Dr. Nader Mehravari is with the CERT® Program at the Software Engineering Institute (SEI), a unit of Carnegie Mellon University in Pittsburgh, PA. His current areas of interest and research include operational resilience, protection and sustainment of critical infrastructure, preparedness planning, and associated risk management principles and practices.

Nader was with Lockheed Martin from 1992 through 2011. In his most recent assignment, he was the Director for Business Resiliency. In this capacity, he led and oversaw all preparedness planning and associated governance and compliance activities. He was responsible for building and leading Lockheed Martin’s resiliency program where he successfully implemented a modern, integrated, risk management based approach to disaster recovery, business continuity, pandemic planning, crisis management, emergency management, and workforce continuity for all of Lockheed Martin.
Notices

Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Capability Maturity Model® and CERT® are registered marks of Carnegie Mellon University.

DM-0000900
Contents

Organizational Mission
  • Setting the Stage

Operational Stress
  • Disruptive Events

Yesterday vs. Today
  • Expansion of Risk Environment

Operational Resilience
  • Operational Risk & Mission Success

Organizational Mission – Revisited
  • Approach for Resilience Management, Protection, and Sustainment

Success Stories
  • A Sampling of Real-Life Applications

Closing
Organizational Mission
"The American Red Cross prevents and alleviates human suffering in the face of emergencies by mobilizing the power of volunteers and the generosity of donors."

- Disaster Relief
- Safe and Adequate Blood Supply
- Health and Safety Education
“To provide postal services to bind the Nation together … To provide prompt, reliable, and efficient services to patrons in all areas and … render postal services to all communities.”
“Provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint Warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations.”

DISN, NIPRNET, SIPRNET…

Enterprise Email Services

Spectrum

Tactical InfoSec Services
Contributing positively to the earth’s natural ecosystem.

- Shade
- Habitat for Birds
- Climbing Opportunity
- Beauty
Operational Stress
Micron Chief Dies in Crash

Steve Appleton Loved Fast Jets, Cars; 'I'd Rather Die Living Than Die Dying'

By SHARA TIBKEN and DON CLARK

Steven R. Appleton, chairman and chief executive of Micron Technology Inc. and one of the most prominent figures in the semiconductor industry, died Friday when the high-performance airplane he was piloting crashed at Boise, Idaho's airport.

The death of the 51-year-old stunned Micron, the well-known maker of memory chips based in the same city, and comes at a time of rapid change for the company and its industry.

The National Transportation Safety Board is investigating the accident, which happened soon after Mr. Appleton took off alone in a single-engine Lancair. The plane, from a maker of aircraft kits, had taken off and landed once and was

CERT® Operational Resilience: Manage, Protect, and Sustain
Twitter #CERTopRES
© 2014 Carnegie Mellon University
Tornadoes Hamper Boeing Supplier

Spirit Says Output Suspended 'At Least' Through Tuesday, Deliveries Could Resume Rest of Week

By JON OSTROWER

WICHITA, Kan. — A key Boeing Co. [BA +2.51%] supplier said it aims to resume deliveries by the end of the week after tornadoes battered its factories here, highlighting the fragility and resilience of the aerospace giant's global supply chain as it works to sharply increase production.

The storms late Saturday caused significant-to-major damage to 10 buildings on the flagship campus of Spirit AeroSystems Inc., which makes fuselages and other components for Boeing's hot-selling 737, 777 and 787 Dreamliner passenger jets. Spirit said production—which normally runs seven days a week—would be suspended "at least" through Tuesday, and that it expects "near-term production disruptions including delivery impacts" to customers.

Spirit spokesman Ken Evans said assessments found most of its machinery and inventory intact. "We believe we can use the facilities we've got," he said in an interview here in Wichita, a major manufacturing hub for the aerospace industry. "We don't think we're going to have a long-term disruption."
Nylon-12 Haunts Car Makers

Explosion at Big Supplier of Resin for Automotive Parts Has Industry in Shortages

By JEFF BENNETT And JAN HROMADKO

Production shortfalls at a single German auto-parts supplier are beginning to ripple through the global auto business.

More than 200 auto executives met in a Detroit suburb on Tuesday to evaluate a looming shortage of a relatively obscure resin essential to modern auto production.

Inventories of the resin are being depleted at a rate of 120 tons a day at the Evonik Industries AG plant in Marl, Germany, that itself is the only integrated maker of the resin.

"We expect to have production before the winter this year and expect that the works to fully repair the plant will take at least three months," an Evonik spokeswoman said.

Several Evonik executives attended the meeting on Tuesday.

WHAT ‘OBSCURE’ BUT ESSENTIAL COMPOUND SHORTAGE HAS THE AUTO INDUSTRY WORRIED ABOUT PRODUCTION?
India's Power Grid Collapses Again

By SAURABH CHATURVEDI And SANTANU CHOUDHURY

NEW DELHI--Much of India's electricity supply network collapsed Tuesday in the country's second major outage in two days, affecting more than 680 million people —double the population of the U.S.—and causing business losses estimated to run into the hundreds of millions of dollars.

Thousands of offices and factories had to switch to generators or shut shop, more than 200 trains were brought to a standstill while hospitals had to ask nurses to manually work critical equipment such as ventilators as 21 provinces experienced a near-total power failure.

India electricity grids fail leaves 620 million people without power
The Federal Aviation Administration is holding all American Airlines flights at their origin airports until at least 5 p.m. Eastern time on Tuesday while the carrier tries to resolve a nationwide outage to its reservations system.
SANDY SHUTS DOWN THE CITY

By JOHN ANNESE and JILLIAN JORGENSEN

STATION ISLAND ADVANCE

The city is in a virtual lockdown as a storm of unprecedented character slammed into the East Coast.

Tracking the storm
The worst of the powerful hurricane is expected Monday night into Tuesday.

Hospital evacuated.
THE WALL STREET JOURNAL. ▶ WORLD

Powerful Typhoon Haiyan Hits Philippines

By CRIS LARANO and JOSEPHINE CUNETA
Nov. 7, 2013 10:44 a.m. ET
Train Halt From Boston Stretches to Manhattan

The Marathon Bombing: Gunfights, Blasts and a Manhunt Shut Down Boston

Boston transit shut down, nearly 1 million sheltering in place amid terror hunt
Advanced persistent threat

From Wikipedia, the free encyclopedia

Advanced persistent threat (APT) usually refers to a group, such as a foreign intelligence gathering techniques to access sensitive information[1], but appear. Other recognized attack vectors include infected media, supply chain compromise, usually referred to as an APT as they rarely have the resources to be both advanced and a specific target.[2]
Chinese Hackers Hit U.S. Media

Wall Street Journal, New York Times Are Breached in Campaign That Stretches Back Several Years

By SIOBHAN GORMAN, DEVLIN BARRETT and DANNY YADRON

WASHINGTON—Chinese hackers believed to have government links have been conducting wide-ranging electronic surveillance of media companies including The Wall Street Journal, apparently to spy on reporters covering China and other issues, people familiar with the incidents said.

Journal publisher Dow Jones & Co. said Thursday that the paper's computer systems had been penetrated by Chinese hackers, apparently to monitor its China coverage.

New York Times Co. (NYT +0.11%) disclosed Wednesday that the newspaper also had been the victim of cyberspying.
More companies reporting cybersecurity incidents

By Ellen Nakashima and Danielle Douglas, Published: March 1

At least 19 financial institutions have disclosed to investors in recent months that computers were targets of malicious cyberassaults last year, adding to a growing chorus among corporations about the breadth of cybersecurity incidents in the financial sector.

In their annual financial reports, such as Bank of America and JPMorgan Chase and other institutions, have reported computer systems were targets of cyber intrusions.

Are the ongoing DDoS attacks against U.S. banks just the calm before the storm?

by Avivah Litan | March 14, 2013 | 1 Comment

That's a viable hypotheses after hearing that the attackers only used one third of the bandwidth they had staged for their latest round of attacks against U.S. banks last Tuesday. Reportedly, on Tuesday the total size of the DDoS attack was 190 gigabits at one time, with the largest attack against a single bank at 110 gigabits.

Interestingly, the attackers could have easily done even more damage but they chose not to. 9200 bots were identified as attack-capable but the total number of bots actually involved in sending the DDoS traffic to the banks numbered only about 3200. The other 6000 bots sat there doing nothing.
False AP Twitter Message Sparks Stock-Market Selloff

By SHIRA OVIDE

The Associated Press said Tuesday its Twitter account was compromised, resulting in a false message on the service that explosions in the White House had injured President Barack Obama. The message briefly sparked selloff on U.S. stock markets.

"The Twitter account has been hacked," the AP said in a statement Tuesday.

"I tweet about an attack on the White House is false."

Other Twitter accounts associated with Associated Press were quick to deny the false Twitter message, which was posted just after 1 p.m. Eastern time. Afterward, the news organization's main Twitter account was suspended

The Associated Press said Tuesday its Twitter account was compromised, resulting in a false message on the service that explosions in the White House had injured President Barack Obama. The message briefly sparked selloff on U.S. stock markets.

"The Twitter account has been hacked," the AP said in a statement Tuesday.

"I tweet about an attack on the White House is false."

Other Twitter accounts associated with Associated Press were quick to deny the false Twitter message, which was posted just after 1 p.m. Eastern time. Afterward, the news organization's main Twitter account was suspended.
 Pacemaker hack can deliver deadly 830-volt jolt

Pacemakers and implantable cardioverter-defibrillators could be manipulated for an anonymous assassination

By Jeremy Kirk

October 17, 2012 — IDG News

a deadly, 830-volt shock from some medical device companies.

The Food and Drug Administration is warning makers of heart monitors, mammogram machines and myriad other medical devices that their gear is at risk of being hijacked by hackers, putting patients at risk.

By CHRISTOPHER WEAVER

The Food and Drug Administration is warning makers of heart monitors, mammogram machines and myriad other medical devices that their gear is at risk of being hijacked by hackers, putting patients at risk.
Challenges to Organizational Mission

Operational mission of organizations is under stress on a minute-by-minute basis.

The stress comes from

• pervasive use of technology
• globalization
• complexity of business processes
• operational complexity
• movement toward intangible assets
• global economic pressures
• open borders
• geo-political pressures
• regulatory and legal boundaries
• intertwining of cyber and physical domains

…and is exasperated by increased intertwining of cyber and physical domains.
Disruptive Events

Natural or Manmade
- Fire
- Flooding
- IT failures
- Earthquakes
- Cyber attacks
- Severe weather
- Network failures
- Technology failures
- Organizational changes
- Loss of service provider
- Strikes or other labor actions
- Loss of customer or trading partner
- Chemical, biological, and nuclear hazards
- Unavailability of workforce
- Failed internal processes
- Supply chain disruption
- Employee kidnappings
- Workplace violence
- Data corruption
- Product failure
- Power outages
- Civil unrest
- Terrorism
- Fraud
- Etc.

Accidental or Intentional

Small or Large

Information Technology or Not

Cyber or Kinetic

Result in

Interruption of Business Processes

...through which operational risks are realized
Yesterday vs. Today
# Ever-Increasing Capability & Complexity

<table>
<thead>
<tr>
<th>Biplane</th>
<th>Apollo Lunar Module</th>
<th>SR-71</th>
<th>F-35</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 SLOC</td>
<td>2K SLOC</td>
<td>500K SLOC</td>
<td>9.9M SLOC</td>
</tr>
</tbody>
</table>
Yesterday’s mission success would have been...
Today mission success is about ...

- Application complexities
- Business process complexities

and more...
Yesterday’s Mission Protection

- Continuity of Operation (COOP)
- Business Continuity
- Emergency Response
- IT Disaster Recovery
Today’s Mission Protection

- Continuity of Operation (COOP)
- Contingency Planning
- Business Continuity
- Emergency Management
- Preparedness Planning
- IT Operations
- Crisis Management
- IT Disaster Recovery
- Supply Chain Continuity
- Operational Risk Management
- Pandemic Planning
- Cyber Protection
- Information Security
- Workforce Continuity
- Privacy
- Enterprise Risk Management
- Crisis Communications
- Operational Risk Management
Today’s Business Environment

Today’s Business Environment Is Much Less Forgiving

Yesterday

Today

Severity of Operational Glitches

Business Consequences of Operational Glitches

Today’s Business Environment Is Much Less Forgiving
Operational Resilience
Operational Risk

A form of risk affecting day-to-day business operations

A very broad risk category
- from high-frequency low-impact to low-frequency high-impact

Exacerbated by
- actions of people
- systems and technology failures
- failed internal processes
- external events
- bad decisions
Why do operational risks matter?

Trust and confidence of employees and customers
Reputation and image
Regulatory compliance, fines, and legal penalties
Customer retention and growth
Life, safety, and health of customers and employees
Productivity and profitability
Organizational survival

… because they have explicit and direct IMPACT
**Resiliency**

- **noun** [ri-ˈzil-yəns]

- Power or ability to return to the original form, position, etc. after being bent, compressed, or stretched.

- Physical property of a material that can return to its original shape or position after deformation that does not exceed its elastic limit.

- Ability of an ecosystem to return to its original state after being disturbed.

- Ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.

- Ability to recover from or adjust easily to misfortune or change.

- Ability of an strained body to recover its size and shape after deformation.

- Capability of a strained body to recover readily from illness, depression, adversity, or the like.
Operational Resilience

The *emergent* property of an entity

- that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit

- to meet its mission under times of disruption or stress *and* return to normalcy when the disruption or stress is eliminated
Operational Resilience

The **emergent** property of an entity

- that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its limit
- to meet its mission under times of disruption or stress *and* return to normalcy when the disruption or stress is eliminated
An Analogy: Health

Is there a place that you can purchase health?

Is there a place where health is manufactured?

How do you become healthy?

Health & Resilience: They are both emergent properties.
To be operationally resilient, cyber- and/or kinetic-enabled missions must address operational risk on a number of “planes.”

Operational Efforts Must Consider and Enable Such Multidimensionality
Organizational Mission - Revisited
Services and Products

Outputs of an organization can be internally or externally focused.
Collectively they enable an organization’s mission.
Example: U.S. Postal Service
Productive Activities or Business Processes

Activities that the organization (and/or its suppliers) perform to ensure that services and products are generated

A service or product is made up of one or more business processes.
Example: U.S. Postal Service

Domestic Mail Delivery

- Payroll Services
- IT Services
- HR Services
- Inspection Services
- Software Development
- Engineering
- Mail Sorting
- UPS & FedEx Services
- Vehicle Fleet Services
- Airline Services
- Etc.
Assets

Something of value to the organization

Asset value relates to the importance of the asset in meeting the service mission.
Asset Types of Importance to Operational Resilience

- People
- Technology
- Supply Chain / Raw Material
- Information
- Facilities
Asset Types

Something of value to the organization

Asset value relates to the importance of the asset in meeting the service mission.
Example: U.S. Postal Service

<table>
<thead>
<tr>
<th>Domestic Mail Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll Services</td>
</tr>
<tr>
<td>IT Services</td>
</tr>
<tr>
<td>HR Services</td>
</tr>
<tr>
<td>Inspection Services</td>
</tr>
<tr>
<td>Software Development</td>
</tr>
<tr>
<td>Engineering</td>
</tr>
<tr>
<td>Mail Sorting</td>
</tr>
<tr>
<td>UPS &amp; FedEx Services</td>
</tr>
<tr>
<td>Vehicle Fleet Services</td>
</tr>
<tr>
<td>Airline Services</td>
</tr>
<tr>
<td>Etc.</td>
</tr>
</tbody>
</table>

**People Assets**
- 574,000 employees
- Mail carriers
- Postal inspectors
- Postmasters
- Truck drivers
- Mechanics
- Software developers
- Network engineers
- Postmaster general
- Inspector general

**Info. Assets**
- National address database
- National zip code database
- Customer PII
- Employee PII
- Data associated with each piece of mail
- Information processed by USPS.com

**Tech. Assets**
- APC kiosks
- AFCS/OCR
- APPS machines
- AFSM, APBS, UFSM, PARS
- Computers
- Servers
- Laptops
- 300K+ handheld scanners
- PBX

**Facility Assets**
- 30,000+ facilities
- 200,000+ vehicles
- HQ building
- Raleigh data center
- Eagan data center
- P&DCs
- 70,000+ stores, banks, and ATMs that sell stamps

CERT® Operational Resilience: Manage, Protect, and Sustain
Twitter #CERTopRES
© 2014 Carnegie Mellon University
Operational Resilience Starts at Asset Level

Realized operational risk resulting in asset disruption
Operational Resilience Starts at Asset Level

- **Protect**
  - Manage Conditions of Risk
    - *Keep assets from exposure to disruption*
    - (e.g., Fault-Tolerance & High-Availability Designs; Preparedness; Information Security)

- **Sustain**
  - Manage Consequences of Risk
    - *Keep assets productive during adversity*
    - (e.g., Disaster Recovery, Business Continuity, Pandemic Planning, Crisis Management, COOP)
Analogy - Protection and Sustainment Strategies

Protection Activities

- Translate into activities designed to keep assets from exposure to disruption
- Example: “security” activities, but may also be embedded in IT operations activities

Sustainability Activities

- Translate into activities designed to keep assets productive during adversity
- Example: “business continuity” activities
Asset Disruption

Realized operational risk resulting in asset disruption
Organizational Context for Resilience Activities

This is where operational resilience management, protection, and sustainment begin.
Is there one place that I can go to see what are all the right things that an organization should do in order to improve and manage its operational resilience in a systematic, practical, and proven manner?
CERT Resilience Management Model (CERT-RMM)

Framework for managing and improving operational resilience

“…an extensive super-set of the things an organization could do to be more resilient.”
—CERT-RMM adopter

http://www.cert.org/resilience/
Desired Integrated Approach

- Continuity of Operation (COOP)
- Business Continuity
- Contingency Planning
- Cyber Protection
- Information Security
- Pandemic Planning
- Privacy
- Supply Chain Continuity
- Enterprise Risk Management
- Cybersecurity
- IT Disaster Recovery
- Crisis Communications
- Emergency Management
- Crisis Management
- Risk Management
- Operational Risk Management
- Information Security
- Workforce Continuity
- Workforce Continuity
- Supply Chain Continuity
- Workforce Continuity
- Information Security
- Crisis Management
- Cybersecurity
- Emergency Management

Operational Resilience
Research on new approaches to achieving security and resiliency in information and communications infrastructures is insufficient. The government needs to increase investment in research that will help address cybersecurity vulnerabilities while also meeting our economic needs and national security requirements.

The Department has identified seven priorities:
- Defense Strategic Guidance
- Autonomy
- Counter Weapons of Mass Destruction
- Cyber Sciences
- Data-to-Decisions
- Electronic Warfare
- Engineered Resilient Systems
- Human Systems
Success Stories
A Sampling of CERT-RMM Applications and Derivatives

CERT® Operational Resilience: Manage, Protect, and Sustain
Twitter #CERTopRES
© 2014 Carnegie Mellon University
The Cyber Security Evaluation Program (CSEP), within the Department of Homeland Security’s (DHS) National Cyber Security Division (NCSD), conducts a no-cost voluntary Cyber Resilience Review (CRR) to evaluate and enhance cyber security capacities and capabilities within all 18 Critical Infrastructure and Key Resources (CIKR) Sectors, as well as State, Local, Tribal, and Territorial (SLTT) governments. The CRR seeks to understand cyber security management of services (and associated assets) critical for an organization’s mission success by focusing on protection and sustainment practices within ten key domains that contribute to the overall cyber resilience of an organization.

Overview

The CRR is based on the CERT Resilience Management Model (CERT-REMM) developed by Carnegie Mellon University’s Software Engineering Institute [www.cert.org/resilience/remm.html]. The goal of the CRR is to develop an understanding of an organization’s operational resilience and ability to manage cyber risk to its critical services and assets during normal operations and during times of operational stress and crises.

The CRR seeks to elicit the current state of cyber security management practices from key cyber security personnel—Chief Information Officers, Chief Information Security Officers, and those responsible for management of IT Security, IT Operations, and Business Community.

The CRR results in a report that summarizes observed strengths and weaknesses in each domain and provides options for consideration containing general guidance or activities aimed at improving the cyber security posture and preparedness of an organization.

The CRR focuses on the following ten domains:
1. Asset Management
2. Configuration and Change Management
3. Risk Management
4. Controls Management
5. Vulnerability Management
6. Incident Management
7. Service Continuity Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

The CRR addresses the following four asset types:
1. People
2. Information
3. Technology
4. Facilities

What to Expect

- The CRR is a one-day, on-site facilitation and interview of key cyber security personnel.
- The participants will receive a draft report within 45 calendar days to review and provide feedback. DHS will subsequently issue a final CRR Report.
- CRR results are afforded protections under the DHS Protected Critical Infrastructure Information (PCII) Program [www.dhs.gov/PCII] — the results are for organization use and DHS does not share results.

Contact Information for CRR-related Inquiries

Please address inquiries regarding the CRR to: CRR@hq.dhs.gov (Cyber Security Evaluations).

About DHS and NCSD

DHS is responsible for safeguarding our Nation’s critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. NCSD leads DHS’s efforts to secure cyberspace and cyber infrastructure. For additional information, please visit www.dhs.gov/cyber.
ELECTRICITY SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Version 1.0
31 May 2012
U.S. Postal Inspection Service (USPIS)

The law enforcement arm of the U.S. Postal Service

The USPIS has used CERT-RMM to address such operational risks as

- export screening
- new product security
- measuring and monitoring risks associated with fraud
- physical security and aviation screening for international mail
- improved processes for investigative response to network security incidents
Lockheed Martin Corporation has collaborated with the Software Engineering Institute on the application of the CERT Resilience Management Model (CERT-RMM) to improve Lockheed Martin’s corporate-wide business continuity, IT disaster recovery, crisis management, and pandemic planning activities. Two CERT-RMM Class C appraisals have been conducted as part of the collaboration. This presentation will provide an overview of the project, information about the appraisals, and a summary of the use of the appraisal results.
In Closing
Hurricane Sandy Surprised Us in Many Ways

- Devastating Fire
- Blizzard
- Sandstorm
- Run on Power Strips
Most Talked-About Subject Afterward…

**Arctic ice loss amplified Superstorm Sandy violence**

By Blaine Friedlander

If you believe that last October’s Superstorm Sandy was a freak of nature—the confluence of unusual meteorological, atmospheric and celestial events—think again.

Cornell and Rutgers researchers report in the *Environment* section of the New York Times.

---

**It’s Global Warming, Stupid**

By Paul M. Barrett on November 9, 2012

Yes, yes, it’s unsophisticated to blame any given storm on climate change. Men and women in white lab coats tell us—and they’re right—that many factors contribute to each severe weather episode. Climate deniers exploit scientific ambiguity to avoid the discussion.

---

**How Does Climate Change Make Superstorms Like Sandy More Destructive?**

By Joe Romm on Oct 31, 2012 at 5:03 pm

---

**Hurricane Sandy Damage Partly Caused By Climate Change, Scientists Say**

Posted: 11/06/2012 10:06 am EST Updated: 11/06/2012 10:06 am EST

---
Most Talked-About Subject Afterward…

Is this the most important question to ask?
A better question to ask: How has the national risk environment changed?

Movement from traditional wireline telephony to cell phones and broadband cable telephony

“… As of 2003, 153 million Americans lived in coastal counties – an increase of 33 million since 1980 – and 3.7 million lived within a few feet of high tide…”

—Bryan Walsh, Time Magazine, November 12, 2012

… and there are many more.

Dependency on large number of mobile devices needing frequent recharging

Cutting The Lifeline
The percentage of cellphone-only households is growing

Source: CDC/NCHS surveys of 136,228 households conducted Jan. 2008–Dec 2011; 95% confidence interval
The Wall Street Journal

July – Dec. 2011: 34%
Expansion of National Risk Environment

- Globalization
- Operational complexity
- Pervasive use of technology
- Intertwining of cyber and physical domains
- Increased role of cybersecurity in securing physical assets
- Movement toward intangible assets
- Global economic pressures
- Regulatory and legal boundaries
- Geo-political pressures

Successful management of operational risk may require a (significant) shift in thinking and approach.
Protecting the enterprise remains a complex and multifaceted challenge.

**Disruptive events, through which risks are realized, will continue to surprise us.**

Traditional tools, techniques, and methods may not work as well in this environment.

How should an enterprise deal with (and plan for) such surprises?

How should an enterprise operate in such an environment?
Promising Approaches

Next generation of integrated cyber-resilience management frameworks?

Resilience Engineering – A new engineering discipline?

Re-shaping (not fighting with) the risk landscape?

Should organizations be legally allowed to fight back when under cyber attack?

Mechanisms to compose resilient systems from brittle components?
“The oak fought the wind and was broken, 
the willow bent when it must and survived.”

Robert Jordan, The Fires of Heaven

Thank you for your attention…
As projects continue to grow in scale and complexity, effective collaboration across geographical, cultural, and technical boundaries is increasingly prevalent and essential to system success. SATURN 2012 will explore the theme of “Architecture: Catalyst for Collaboration.”

**Introduction to the CERT Resilience Management Model**

February 18 - 20, 2014 (SEI, Arlington, VA)
June 17 - 19, 2014 (SEI, Pittsburgh, PA)

See Materials Widget for course document