ABCs of Operational Resilience

September 11, 2011

Dr. Nader Mehravari, MBCP, MBCI

Executive Vice President
Resiliency Practice
IT Cadre
nader.mehravari@ITCadre.com

Nonresident Affiliate
CERT Cyber Resilience Center
Software Engineering Institute (SEI)
Carnegie Mellon University

Adjunct Professor
School of Electrical and Computer Engineering
Cornell University
nm40@cornell.edu

Contents

Part 1
• Concepts of resilience and operational resilience

Part 2
• Why is it important?
• What are the relevant challenges faced by organizations?

Part 3
• How is it related to traditional and ongoing preparedness planning activities?

Part 4
• Who is talking about it?
• Who is asking for it?

Part 5
• Cornerstones of operational resilience
• Techniques for improving and managing operational resilience
• CERT Resilience Management Model (RMM)

Nomenclature & Background

Business & Operational Drivers

Techniques, Methods & Frameworks
What do you see here?

A set of well looking evergreens?

Look Again!
Origin of the Word “Resilience”

resilio, resilire, resilui, -ı, v
1. leap or spring back
2. rebound
3. recoil
4. shrink (back again)

re·sil·i·ence noun [ri-ˈzil-yəns]
power or ability to return to the original form, position, etc., after being bent, compressed, or stretched
ability of an ecosystem to return to its original state after being disturbed
physical property of a material that can return to its original shape or position after deformation that does not exceed its elastic limit
ability to recover from or adjust easily to misfortune or change
ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation
capability of a strained body to recover its size and shape after deformation
ability to recover readily from illness, depression, adversity, or the like
Operational Resilience

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

- The ability of an organization to
  - Prevent disruptions from occurring;
  - And when struck by a disruption, the ability to quickly respond to and recover from a disruption in the primary business processes.

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
A Case Study – The Fire That Changed an Industry

About 6 p.m. on March 17, 2000, a lightning bolt struck a high voltage electricity line in New Mexico. As power faltered across the state, a fire broke out in a fabrication line of the Royal Philips IT frequency tuned chip manufacturing plant in Albuquerque.

Part 1
• Concepts of resilience and operational resilience

Part 2
• Why is it important?
• What are the relevant challenges faced by organizations?

Part 3
• How is it related to traditional and ongoing preparedness planning activities?

Part 4
• Who is talking about it?
• Who is asking for it?

Part 5
• Cornerstones of operational resilience
• Techniques for improving and managing operational resilience
• CERT Resilience Management Model (RMM)

Contents

Nomenclature & Background

Business & Operational Drivers

Techniques, Methods & Frameworks

© 2012 NM
Challenges to Operational Resilience

- The operational resilience of organizations is under stress on a regular basis.
- The stress comes from disruptive events affecting business operations.

Disruptive Events

<table>
<thead>
<tr>
<th>Natural or Manmade</th>
<th>Accidental or Intentional</th>
<th>Small or Large</th>
<th>Information Technology or Not</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire</td>
<td>Fire</td>
<td>Fire</td>
<td>Fire</td>
</tr>
<tr>
<td>Flooding</td>
<td>Flooding</td>
<td>Flooding</td>
<td>Flooding</td>
</tr>
<tr>
<td>IT failures</td>
<td>IT failures</td>
<td>IT failures</td>
<td>IT failures</td>
</tr>
<tr>
<td>Earthquakes</td>
<td>Earthquakes</td>
<td>Earthquakes</td>
<td>Earthquakes</td>
</tr>
<tr>
<td>Cyber attacks</td>
<td>Cyber attacks</td>
<td>Cyber attacks</td>
<td>Cyber attacks</td>
</tr>
<tr>
<td>Severe weather</td>
<td>Severe weather</td>
<td>Severe weather</td>
<td>Severe weather</td>
</tr>
<tr>
<td>Network failures</td>
<td>Network failures</td>
<td>Network failures</td>
<td>Network failures</td>
</tr>
<tr>
<td>Technology failures</td>
<td>Technology failures</td>
<td>Technology failures</td>
<td>Technology failures</td>
</tr>
<tr>
<td>Organizational changes</td>
<td>Organizational changes</td>
<td>Organizational changes</td>
<td>Organizational changes</td>
</tr>
<tr>
<td>Loss of service provider</td>
<td>Loss of service provider</td>
<td>Loss of service provider</td>
<td>Loss of service provider</td>
</tr>
<tr>
<td>Strikes or other labor actions</td>
<td>Strikes or other labor actions</td>
<td>Strikes or other labor actions</td>
<td>Strikes or other labor actions</td>
</tr>
<tr>
<td>Loss of customer or trading partner</td>
<td>Loss of customer or trading partner</td>
<td>Loss of customer or trading partner</td>
<td>Loss of customer or trading partner</td>
</tr>
<tr>
<td>Chemical, biological, nuclear hazards</td>
<td>Chemical, biological, nuclear hazards</td>
<td>Chemical, biological, nuclear hazards</td>
<td>Chemical, biological, nuclear hazards</td>
</tr>
<tr>
<td>Unavailability of workforce</td>
<td>Unavailability of workforce</td>
<td>Unavailability of workforce</td>
<td>Unavailability of workforce</td>
</tr>
<tr>
<td>Failed internal processes</td>
<td>Failed internal processes</td>
<td>Failed internal processes</td>
<td>Failed internal processes</td>
</tr>
<tr>
<td>Supply chain disruption</td>
<td>Supply chain disruption</td>
<td>Supply chain disruption</td>
<td>Supply chain disruption</td>
</tr>
<tr>
<td>Employee kidnappings</td>
<td>Employee kidnappings</td>
<td>Employee kidnappings</td>
<td>Employee kidnappings</td>
</tr>
<tr>
<td>Workplace violence</td>
<td>Workplace violence</td>
<td>Workplace violence</td>
<td>Workplace violence</td>
</tr>
<tr>
<td>Data corruption</td>
<td>Data corruption</td>
<td>Data corruption</td>
<td>Data corruption</td>
</tr>
<tr>
<td>Product failure</td>
<td>Product failure</td>
<td>Product failure</td>
<td>Product failure</td>
</tr>
<tr>
<td>Power outages</td>
<td>Power outages</td>
<td>Power outages</td>
<td>Power outages</td>
</tr>
<tr>
<td>Civil unrest</td>
<td>Civil unrest</td>
<td>Civil unrest</td>
<td>Civil unrest</td>
</tr>
<tr>
<td>Terrorism</td>
<td>Terrorism</td>
<td>Terrorism</td>
<td>Terrorism</td>
</tr>
<tr>
<td>Fraud</td>
<td>Fraud</td>
<td>Fraud</td>
<td>Fraud</td>
</tr>
</tbody>
</table>

Result in

Interruption of Business Processes
Have you noticed much news about disruptive events recently?
Micron Chief Dies in Crash
Steve Appleton, Cohead of Intel Corp., Dies; 'I'd Rather Be Taking Them the Highways'

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

The National Transportation Safety Board has not yet released an accident report, which happened soon after Mr. Appleton took off in an experimental aircraft - his plane, from a marina, crashed into a popular fishing spot.

St. Jude Wrestles With Image Woes

By CHRISTOPHER WIEGER AND DANA MCKINLEY

St. Jude Medical Inc. is struggling to present a better impression of its management in firearms image problems.

The problems involve the Holata lead, a wire that connects defibrillators to heart tissue and that St. Jude stopped selling in 2010. A recent medical study tied a malfunction in Holata to at least 20 deaths, and some victims are questioning the company’s new president, Tom Hawkins. The $21 billion has some concerns about Holata’s safety, though it hasn’t been linked to patient problems to date.

I decided to stay away from it until the dust settles and we know more about how the Holata problem happens,” said Damir Dzabic, director of electrophysiology at the University of Pittsburgh Medical Center, who has financial relationships with St. Jude and its competitor Medtronic Inc.

Doubts about Durata could weigh on St. Jude’s foothold in the nearly $7 billion global market for defibrillation technologies.
**April 16, 2012**

**Tornadoes Hamper Boeing Supplier**

A supplier said it was so rainy and windy in at least one of the states that tornadoes occurred that it was not able to ship parts.

**April 17, 2012**

**Nolan-19 Haunts Car Makers**

An explosion at a supplier of diesel for automotive parts in Italy has caused shortages of the component.

**Chemical plant explosion brakes car makers’ production**

The explosion at a chemical plant in Italy, which supplies the global automotive industry, has caused shortages of a key component, prompting an emergency meeting in Detroit.
LinkedIn Defends Reaction in Wake of Password Theft

LinkedIn Corp. moved to reassure customers about the security of their data, following a password theft that raised a black eye for the social-networking service.

LinkedIn said on a blog post that it had reviewed log files that revealed accounts that had been logged in from locations, such as China and Vietnam. The company has come under criticism and published on an unauthorized website.

LinkedIn Says It Spent $1 Million Trying To Solve Its Password Theft

Some security experts questioned the adequacy of LinkedIn’s procedures for prohibiting passwords, and once users complained about delays in receiving information about the breach.

Vincenzo Silvano, a LinkedIn director, said the company has taken corrective action.

FREEZER GLITCH AT AUTISM BRAIN BANK SETS BACK RESEARCH

The world’s largest collection of autism brains at Harvard-affiliated McLean Hospital is badly damaged because of a freezer failure, delaying what could be a 10-year setback to autism research.

Frederick E. Newell, director of the Autism Research Center at McLean Hospital, said Monday that it is investigating what caused the temperature in a freezer to rise without sounding an alarm system.

The freezer had stored 106 brain specimens, including 58 earmarked for research into causes and treatments of autism, a condition characterized by poor social skills and difficulties with communication.

The brain specimens are part of a collection of 166 brains belonging to Autism Society donors.
Flu Pandemic's Toll Raised

By CHITMI HUK

Scientists now estimate that about 250,000 people died in the flu pandemic that swept the globe at the tail end of World War II, more than half of all reported deaths. This toll included the seasonal flu deaths, which are usually not recorded.

The big increase in estimated deaths from the H1N1 virus isn't a surprise, experts say. In any pandemic, the initial count typically is based on lab-confirmed figures that tend to significantly underestimate the true number of deaths. In the case of the H1N1 pandemic, there were 18,000 lab-confirmed deaths, while a more comprehensive estimate suggests that anywhere from 150,000 to 750,000 people may have died. The 560,000 figure is a rough median estimate for that range.

Higher Morality

Viral pandemics have their own toll on society, in part because they highlight the fragility of human cooperation. The Lao Cai, a minority group in Vietnam, has a saying that is relevant here: "The sick all die in the same place as the healthy. You must not fear it, because the dead are already dead."

The new study, published in the Lancet, is the first effort to calculate the global impact of the H1N1 virus, known at the time as swine flu. The outbreak was triggered by a recombination of bird, pig, and human viruses, and was the first flu pandemic in more than 40 years.

As Rivals Outsource, Lenovo Keeps Production In House

The difference is that in 2005, Lenovo and its employees were all part of a Beijing-controlled company that was a part of China and its global economy. The country's leaders have for years emphasized the importance of keeping factories inside the country.
Cybercriminals Sniff Out Vulnerable Firms

BY SARAH E. NITTI

With cybercriminals a greater threat to small businesses than ever before, more entrepreneurs are leaning toward technology solutions that are as innovative as they are affordable.

In May, Lifestyle C. & D. Supplys, Inc., a manufacturer of 65-year-old Mr. Pocket, had $1.2 million worth of its basic, through online transactions. The root of the problem? A small-time hacker.

Many smaller businesses find themselves vulnerable to cyber threats because they have limited budgets for IT security and fear of costs.

"Small businesses feel like they're immune from cybercrime and they're wrong," said Larry Tanenbaum, chairman of the Ponemon Institute, a private think tank in Traverse City, Mich. The

About 13% of the 862 data breaches that were analyzed last year by Verizon Communications Inc.'s forensic analysis unit were at companies with 1,000 or fewer employees. That is up from 6% of the 762 data breaches it analyzed in 2010. The figures included investigations conducted by Verizon's lawyers, as well as data breach investigations by various law enforcement groups around the globe, including the U.S. Secret Service.

Yahoo Passwords Stolen in Latest Data Breach

BY DREW FITZGERALD

Yahoo Inc. said it is investigating a data breach that allowed a hacker group to download about 450,000 unencrypted user names and passwords in another black eye for the internet company.

The Sunnyvale, Calif., company said it is working with Yahoo's own security team to determine the extent of the attack.

A hacking organization called DGSN, apparently in a state of mourning, is said to be responsible for the breach.

Yahoo hacked, 450,000 passwords posted online

Yahoo sued over stolen usernames and passwords

Some desire registered for the Yahoo e-mail addresses.
July 16, 2012

**JAPAN**

*Rains Kill Dozens, Force Evacuations in South*

Thousands of residents of southern Japan remained isolated Sunday after severe rains washed out roads, left more than 50 dead or missing, and forced the evacuation of some 780,000 people.

The peak of the rains had passed by Sunday, leaving those affected to clean up from flooding and mudslides in scorching temperatures above 95 degrees.

Coming during the country's rainy season, the storms prompted deadly floods and mudslides in parts of Kyushu, the southernmost of Japan's four main islands.

Japanese media said 75 people were killed, with eight missing in Kumamoto. Observers predicted moderate to heavy rain in the nation's southernmost prefectures.

*Guardian*

---

**DATA BREACH TO COST CARD PROCESSOR**

**July 26, 2012**

By HUBERT H. JOHNSON

Global Payments Inc. [NYSE: GPN] said a security breach that exposed consumers’ payment cards to fraud cost it $104.4 million.

The Atlanta-based company, which processes card transactions for banks and merchants, Thursday reported a net loss for the amount, equal to 65 cents of diluted per-share earnings in the fiscal fourth quarter. It includes expected fines from settlement payments such as Visa Inc. [V], but excludes settlement for the breach and expected costs related to its investigation and remediation.

The company that knows the breach in Atlanta, saying it involved a wide range of its merchants, required credit card numbers were taken from its networks.

Global Payments noted Thursday that personal information of merchants may have been exposed, primarily small merchants who applied to be a customer, requiring a credit check.
Data-Center Failures Hit Twitter Users

The Twitter blackout lasted up to 11:30 p.m. Eastern, president of engineering, said an issue with a network system in Twitter’s data center brought down systems at nearly 1 pm. 

The timing of the outage came as Twitter rolled out a new feature to its users. 

India's Power Grid Collapses Again

NLW ULC/I: Much of India's electricity supply network collapsed Tuesday in the eastern Indian state of Bihar, affecting more than 600 million people, double the population of the U.S. and causing business losses estimated to run into the hundreds of millions of dollars.

India electricity grids fail leaves 620 million people without power
August 3 & 5, 2012

Are there more disruptive events?

Federal Emergency Management Agency
US Declared Disasters
1975-2011

The International Disaster Database
Worldwide Disasters
1975-2010

There appears to be; But, is that right question to ask?
What is the Right Question to Ask?

- Pervasive use of technology
- Globalization
- Operational complexity
- Movement toward intangible assets
- Global economic pressures
- Geo-political pressures
- Regulatory and legal boundaries

Is the Risk Environment Expanding?

**risk** noun [risk]

- The possibility of suffering harm or loss
- Exposure to the chance of injury or loss
- A source of danger
- The possibility of suffering a harmful event

1. An event or condition
2. A consequence or impact from the condition
3. An uncertainty
Enterprise Risk Management

- Looks across all types of risk activities in the organization and considers all types of risks

Operational Risk Management

- A form of risk affecting day-to-day business operations
- Exacerbated by
  - Actions of people
  - Systems and technology failures
  - Failed internal processes
  - External events
  - Bad decisions

Operational resilience emerges from effective management of operational risk.
Actions of People

- Inadvertent or deliberate
- Direct or indirect
- Mistakes, errors, omissions
- Deliberate actions such as insider threat, sabotage, fraud
- Lack of skills or knowledge
- Lack of availability
- Poor leadership or guidance
- Poor governance
- Lack of training & education
- Etc., Etc., Etc…

Systems and Technology Failures

- Lack of proper system maintenance
- Poor configuration and change management
- Insecure, inefficient, or complex coding
- Lack of testing and remediation
- Poor software and systems engineering practices
- Interface failures
- Etc., Etc., Etc…
Failed Internal Processes

- Poor process design and execution
- Mistakes, errors, omissions
- Poor supply chain management
- Poor product development
- Poor capacity planning
- Lack of process controls
- Poor support processes (e.g., accounting, HR, education & training, risk management)
- Poor governance and compliance
- Etc., Etc., Etc...

External Events

- Natural disasters (e.g., hurricane, earthquake, flood, disease, volcano)
- Terrorism
- Supply chain failures
- Boycotts
- Economic pressures
- Political pressures
- Outsourcing
- Business cycles
- Etc., Etc., Etc...
## Risk and Resilience

- Where does the stress and disruption come from?
  - Realized risk

- Resilience is directly related to risk

- Organization’s ability to identify and mitigate operational risk affects its operational resilience.

- Why?
  - Known risk is addressed before it becomes disruptive.
  - Organization is able to make informed decisions about the sustainment of business processes under uncertain conditions (i.e., unknown risks).

- Poor risk management may make the organization less agile, flexible, survivable because the likelihood of disruption is increased.

## Operational Resilience Management

- It is the overarching (risk management) practice of planning, developing, integrating, executing, and governing activities to ensure that an enterprise and the environment that it operates in are able to:
  - Identify and mitigate operational risks that can lead to system disruptions before they occur,
  - Prepare for and respond to disruptive events (natural or man-made, accidental or intentional) in a manner that demonstrates command and control of incident response, and
  - Recover and restore mission-critical operations following a disruptive event within acceptable time frames.
What makes a service operationally resilient?

Operational Resilience is an emergent property;
It emerges from things that we do, like these:

- Identification and mitigation of risks to the service and related assets
- Service continuity processes and planning
- Management of IT operations practices
- Management and deployment of people
- Practices to protect (control) and secure important information and technology assets
- Management of external partners (that provide parts of the service)
- Environmental management (where the service “lives”)

Hurdles to Effective Operational Resilience Management

- Vague and abstract nature
- Compartmentalization
- Technology focus
- Practice proliferation
- Insufficient funding
- Insufficient success metrics
- Discrete nature of activity
- (Over)reliance on people
- Regulatory climate
- Head-in-the-sand
Summary of Part 2

- Organizational and operational complexities are creating a new and constantly changing risk environment.
- Organizations must manage operational risk to ensure operational resilience of services.
- Operational risk management is a foundation for operational resilience.
- New questions are being posed to the organization.
  - Are you equipped to manage in this new environment?
  - Do you have the appropriate mindset, tools, techniques, and methods?
- Successfully managing operational resilience may require a (significant) shift in thinking and approach to be successful.

What are some new ways of thinking and new approaches to managing risk in such a dynamic environment?

We will answer this question in Part 5.

Contents

- Part 1
  - Concepts of resilience and operational resilience
- Part 2
  - Why is it important?
  - What are the relevant challenges faced by organizations?
- Part 3
  - How is it related to traditional and ongoing preparedness planning activities?
- Part 4
  - Who is talking about it?
  - Who is asking for it?
- Part 5
  - Cornerstones of operational resilience
  - Techniques for improving and managing operational resilience
  - CERT Resilience Management Model (RMM)
Let's look at some real examples of how things generally work today.

Example

2011 Japan Earthquake & Tsunami

Continuity of Operation (COOP)

Emergency Management

Business Continuity

Crisis Communications

Crisis Management

IT Disaster Recovery
Example

Multiplicity of Preparedness Planning Efforts

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

Another Analogy
Objective

Objective: An Analogy

Convergence

© 2012 NM
Contents

Part 1
• Concepts of resilience and operational resilience

Part 2
• Why is it important?
  • What are the relevant challenges faced by organizations?

Part 3
• How is it related to traditional and ongoing preparedness planning activities?

Part 4
• Who is talking about it?
  • Who is asking for it?

Part 5
• Cornerstones of operational resilience
  • Techniques for improving and managing operational resilience
  • CERT Resilience Management Model (RMM)

Indications and Business Drivers from a Variety of Fronts

• Federal Government
• Other Countries
• Academic Institutions
• Publishing
• Job Market
• Standards
• Social Media
• Commercial Industry
• Business Continuity Community
• Today’s Business Environment
• Other External Drivers
White House Cyberspace Policy Review

Preface:
Research on new approaches to achieving security and resiliency in information and communications infrastructure is insufficient. The government needs to increase investment in research that will help defend cyberspace against threats while also meeting our economic, social, and national security requirements.

Executive Summary:
Cyberspace policy includes strategy, policy, standards regarding the security of and operations in cyberspace, and encompasses the full range of information, vulnerability reduction, detection, intelligence, engagement, incident response, monitoring, recovery policies and activities, including computer network operations, information assurance, the enforcement of policy, and law enforcement as they pertain to cyberspace and network defense and response to cyber attacks.

Near-Term Action Plan:
Working in collaboration with other agencies, develop a framework for research and development strategies that focus on emerging technologies that have the potential to enhance the security, reliability, and resiliency of digital infrastructure. The framework enables greater interagency access to critical tools and technologies, training resources, and identification of DoD Research & Engr. Priorities for 2013-17

DoD Research & Engr. Priorities for 2013-17

S&T Emphasis Areas

Seven areas were selected for research, development, and demonstration activities. These serve as a framework for investment in the strategic plans and initiatives of individual laboratories.

1. Core Technologies
2. Engineering, Services, and Tools
3. Cybersecurity, Risk, and Assurance
4. Information and Communication Technology (ICT) and Information Technology (IT)
5. Software and Systems Engineering
6. Science and Mathematics
7. Life Sciences, Environmental Science, and Health Science

The Department will pursue these priorities across the entire S&T Community, and has begun to gather priorities across all DoS to focus investment on areas of greatest potential for defense and national security.
National Infrastructure Advisory Council
A Framework for Establishing Critical Infrastructure Resilience Goals
Final Report and Recommendations by the Council

October 19, 2010

The Homeland Security Blog
Upgrading homeland security strategy emphasizes resilience
DHS Reorienting Around Resilience
2006, APRIL 23

Department of Homeland Security

Ensure Resilience to Disasters

Cyber Resiliency Engineering
The Cyber Security Evaluation Program (CSEP) within the Department of Homeland Security's (DHS) National Cyber Security Division (NCSD) conducts no-cost, voluntary Cyber Resilience Review (CRR) to evaluate and enhance cyber security capabilities and protection and availability of critical Key Sectors (KIS) sectors, as well as State, Local, Tribal, and Territorial (SLTT) governments. The CRR seeks to understand cyber security management of services and associated critical aspects for assessing and enhancing the protection and sustained preparedness of key domains that contribute to the overall cyber resilience of an organization.

Overview

The CRR is based on the CERT Resilience Management Model (CERT RMM) developed by Carnegie Mellon University's Software Engineering Institute (www.cert.org/cert_rmm). The goal of the CRR is to develop a standardized methodology that allows organizations to assess their operational resilience and ability to continue to operate during normal operations and during times of operational stress and stress.

The CRR is a tool to help organizations identify potential risks and vulnerabilities in their operational processes and recommend improvements to enhance resilience.

The CRR results in a report that summarizes observed strengths and weaknesses in each business function of the organization, including a general guideline or advice aimed at improving the cyber security posture and preparedness of the organization.

CRR Services & Asset Types

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

The CRR addresses the following CSEs:
1. People
2. Process
3. Technology
4. Facilities

What to Expect

- The CRR is a step-by-step process that involves consultation and engagement with the organization's stakeholders.
- The participants will review a draft report within 45 calendar days to review and provide feedback on the results. The CRR will subsequently issue a final report.
- CSEs are provided with a detailed assessment of the organization's cyber security capabilities and recommendations for improvement.

Contact Information for CSE Issues

Please address inquiries regarding the CSE on Cyber Security Evaluation (CSE) at CyberSecurityEvaluation (CSE)@DHS.gov.
United Kingdom

The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world

- Work with the companies that own and manage our critical infrastructure to ensure key data and systems continue to be safe and resilient.


- Cabinet Office, public sector, and police
- Supporting economic growth
- Law enforcement
- Home Office, building cyber resilience
- Government IT, looking at 3rd party supply chains

United Kingdom

Cabinet Office

Cyber Security Strategy of the United Kingdom: Safety, security and resilience in cyberspace

- Stream 1: Safe, secure and resilient systems
- This stream will focus on enhancing protection and resilience from cyber attacks in all sectors, to provide the critical practical resilience required to mitigate the risks. It will also seek to understand potential vulnerabilities and impacts in all sectors, and to take appropriate mitigation measures. This will bring together ongoing work on resilience and reliability in the telecommunications sector, for example, and link to other sector-specific initiatives.
Beginning in the fall of 2012, the INI will offer an Executive Master of Science in Information Assurance (ExecMSIA) for current and aspiring information technology executives seeking to propel their careers in the information assurance arena. Flexible to fit easily with a career, the ExecMSIA offers a concentration in Cyber Forensics and Incident Response and Resilience Management. An option is available for non-degree students to pursue certificates in these two areas.

Workshop: What Businesses Need to Know About Harmonizing Resilience and Cyber Security

The Institute for Information Infrastructure Protection (I3P) and the University of Virginia Center for Risk Management present a workshop:

What Businesses Need to Know About Harmonizing Resilience and Cyber Security

November 13-20 • Darden School of Business, University of Virginia
**Tulane University**

**Tulane University’s Disaster Resilience Leadership Academy (DRLA)**

Tulane University's Disaster Resilience Leadership Academy (DRLA) is an interdisciplinary academic and research-oriented institute dedicated to the systematic strengthening of global leadership in the field of disaster risk and emergency management. The DRLA academic program specifically aims to develop a new generation of leaders who can lead their organizations, communities, and nations to strengthen the resilience of the people they support and reduce disaster vulnerability. We understand resilience as a critical issue for programs that focus on the role of leadership in all phases of disaster risk management.

- Master of Science in Disaster Resilience Leadership Studies (28 credit hours)
- Master's Terminal in Disaster Resilience Leadership (15 credit hours)

---

**UNLV**

**University of Nevada at Las Vegas - Proposed/Investigating a Ph.D. in Resilience**

The University of Nevada, Las Vegas (UNLV) is conducting exploratory research which could lead to the establishment of a Doctor of Philosophy (Ph.D.) in Resilience. The preliminary research includes this proposal:

**UNLV’s Proposed PhD in Resilience**

[Additional content regarding UNLV’s proposed PhD in Resilience]
Books

CERT Resilience Management Model
A Maturity Model for Managing Operational Resilience
Richard A. Caralli
Julia H. Allen
David W. White

Job Market

UCL DEPARTMENT OF SECURITY AND CRIME SCIENCE

Search UCL
UCL Home
DSCD
Research Assistant Cyber Security and Resilience

Research Assistant Cyber Security and Resilience CPD project
17 February 2012

Applications are invited for a Research Assistant to develop a CPD module for training professionals and decision-makers in cyber security. The module will focus on developing cyber resilience through the development and implementation of strategies and policies.

© 2012 NM

73

74
Standards

ISO 22302 Resilience in the Supply Chain Standard Approved

Standards Activities – # of Standards Issued

- Standards issued during 1995-2011 dealing with
  - Business Continuity
  - IT Disaster Recovery
  - Information Security
  - IT Operations
  - Emergency Mgmt.
  - Incident Management
  - Supply Chain Continuity
  - Pandemic Planning
  - And related areas

Preliminary data

- BS 7799-1
- NFPA 1600
Application of the CERT® Resilience Management Model at Lockheed Martin

Lockheed Martin Corporation has collaborated with the Software Engineering Institute to adapt and apply the CERT Resilience Management Model (CERT-RMM) to improve Lockheed Martin's corporate-wide business continuity, disaster recovery, crisis management, and pandemic planning activities. The CERT-RMM Class C approach has been conducted as part of the collaboration.

This presentation will provide an overview of the project, information about the approach, and a summary of the use of the approach results.
Conference Theme: The Evolution to Business Resilience

Occurrences of words “resilience” in DRJ Conference Program
Today’s Business Environment

Today’s Business Environment is Much Less Forgiving

A Sampling of Other External Drivers

- Department of Homeland Security
  - PS-PREP – (Voluntary) Private Sector Preparedness Accreditation and Certification Program

- Standard & Poor’s
  - Adding enterprise risk management as a criterion in their creditworthiness rating process for US (nonfinancial) corporations
  - DR and BC are considered key parts of enterprise risk management activities

Non-Traditional Drivers of Interest to Executive Leaders
Contents

Part 1
• Concepts of resilience and operational resilience

Part 2
• Why is it important?
  • What are the relevant challenges faced by organizations?

Part 3
• How is it related to traditional and ongoing preparedness planning activities?

Part 4
• Who is talking about it?
  • Who is asking for it?
  • Part 5
    • Cornerstones of operational resilience
    • Techniques for improving and managing operational resilience
    • CERT Resilience Management Model (RMM)

Cornerstones of Operational Resilience

• Risk Management
  • Operational Risk Management

• Convergence

• Organizational Construct for Resiliency Activities

• Protection and Sustainment Activities

• Institutionalization
Operational Risk Management

- A form of risk affecting day-to-day business operations
- Exacerbated by
  - Actions of people
  - Systems and technology failures
  - Failed internal processes
  - External events
  - Bad decisions

Operational resilience emerges from effective management of operational risk.

Cornerstones of Operational Resilience

- Risk Management
  - Operational Risk Management
- Convergence
- Organizational Construct for Resiliency Activities
- Protection and Sustainment Activities
- Institutionalization
Convergence directly affects the level of operational resilience.

Operational Risk Management

Enterprise Risk Management

Multiplicity of Preparedness Planning Efforts

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

Another Analogy
Objective

Objective: An Analogy

Convergence
Cornerstones of Operational Resilience

- Risk Management
  - Operational Risk Management

- Convergence
  - Organizational Construct for Resiliency Activities
  - Protection and Sustainment Activities
  - Institutionalization

Organizational Construct for Resiliency Activities

- Outputs of an organization
- Can be internally or externally focused
- Can be externally focused
- Collectively they enable an organization’s mission
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
- Business processes mission enable service/product mission

Something of value to the organization
- “Charged into production” of services
- Asset value relates to the importance of the asset in meeting the service mission.
Asset Types of Importance to Operational Resilience

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

Organizational Construct for Resiliency Activities

- Something of value to the organization
- “Charged into production” of services
- Asset value relates to the importance of the asset in meeting the service mission.

© 2012 NM
Organizational Construct for Resiliency Activities

Cornerstones of Operational Resilience

- Risk Management
  - Operational Risk Management
- Convergence
- Organizational Construct for Resiliency Activities
  - Protection and Sustainment Activities
  - Institutionalization
Operational Resilience Starts at the Asset Level

- **Asset**
  - **Protect**
    - Manage Conditions of Risk
      - (e.g., Fault-Tolerance & High-Availability Designs; Preparedness; Information Security)
  - **Sustain**
    - Manage Consequences of Risk
      - (e.g., Disaster Recovery, Business Continuity, Pandemic Planning, Crisis Management)
  - **Detect**

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 imbedded in IT operations activities

- **Sustainability Activities**
  - Translate into activities designed to keep assets productive during adversity
  - E.g., “business continuity” activities
Organizational Context for Resiliency Activities

Examples:
- Disaster Recovery Planning
- Business Continuity Planning
- Risk Management
- Information Security
- Crisis Management
- Emergency Management
- Pandemic Planning
- Supply Chain Continuity
- Etc, Etc, Etc…

Cornerstones of Operational Resilience

- Risk Management
  - Operational Risk Management
- Convergence
- Organizational Construct for Resiliency Activities
- Protection and Sustainment Activities
  - Institutionalization
What do these organizations have in common?

- Customer Service
- Customer Happiness
- Tradition
- Protection
- Chain of Command
- Unit Cohesion
- Regulations

Strong Culture
Culture has a huge impact on the organization’s ability to meet its mission.

- Organizations must provide explicit guidance for institutionalizing resilience activities so that they persist over time.

Ask not how well am I performing today?  
Ask do I have what it takes to sustain high performance beyond today?
Is there one place that I can go to see what are all the right things that an organization should be doing in order to improve and manage its operational resilience in a systematic, practical, and proven manner?

CERT Resilience Management Model (CERT-RMM)
What is CERT-RMM?

- Most modern and comprehensive framework for managing and improving operational resilience

- Guides implementation and management of operational resilience activities

- Enables and promotes the convergence of:
  - COOP, IT Disaster Recovery, Business Continuity
  - Information Security, Cyber security
  - IT Operations

- Applicable to a variety of organizations
  - small or large
  - simple or complex
  - public or private

How was RMM developed?

RMM codifies best practices for Info. Sec., IT DR, and BC from world leading organizations and numerous standards and codes of practice.
What drove development of RMM?

- Increasingly complex operational environments
- Siloed nature of operational risk activities
- Lack of common language or taxonomy
- Overreliance on technical approaches
- Lack of means to measure organizational capability
- Inability to confidently predict outcomes, behaviors, and performance under times of stress

Foundational Elements of RMM

- Operational Resilience
- Risk Management
  - Operational Risk Management
- Convergence
- Organizational Construct for Resiliency Activities
- Capability Dimension
  - Process Institutionalization
- Code of Practice Crosswalk
RMM – The Model

- Guidelines and practices for
  - Converging of security, business continuity, disaster recovery, and IT ops
  - Implementing, managing, and sustaining operational resilience activities
  - Managing operational risk through process
  - Measuring and institutionalizing the resiliency process

- Common vernacular and basis for planning, communicating, and evaluating improvements

- Focuses on “what” not “how”

- Organized into 26 process areas

RMM Process Areas

<table>
<thead>
<tr>
<th>Access Management</th>
<th>Measurement and Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Definition and Management</td>
<td>Monitoring</td>
</tr>
<tr>
<td>Communications</td>
<td>Organizational Process Focus</td>
</tr>
<tr>
<td>Compliance</td>
<td>Organizational Process Definition</td>
</tr>
<tr>
<td>Controls Management</td>
<td>Organizational Training &amp; Awareness</td>
</tr>
<tr>
<td>Enterprise Focus</td>
<td>People Management</td>
</tr>
<tr>
<td>Environmental Control</td>
<td>Resiliency Requirements Development</td>
</tr>
<tr>
<td>External Dependencies</td>
<td>Resiliency Requirements Management</td>
</tr>
<tr>
<td>Human Resource Management</td>
<td>Risk Management</td>
</tr>
<tr>
<td>Identity Management</td>
<td>Service Continuity</td>
</tr>
<tr>
<td>Incident Management &amp; Control</td>
<td>Technology Management</td>
</tr>
<tr>
<td>Knowledge &amp; Information Mgmt</td>
<td>Vulnerability Analysis &amp; Resolution</td>
</tr>
</tbody>
</table>
RMM Combines Two Approaches

Operational Resilience Management System

+ Process Institutionalization and Improvement

What to do

Comprehensive non-prescriptive guidance on what to do to manage operational resilience

Making it stick

Proven guidance for institutionalizing processes so that they persist over time

Process Dimension

Capability Dimension

Code of Practice Crosswalk

- Links RMM practices to common used codes of practice and standards

- Including:
  - ANSI/ASIS SPC.1-2009
  - BS25999
  - COBIT 4.1
  - COSO ERM Framework
  - CMMI
  - FFIEC BCP Handbook
  - ISO 20000-2
  - ISO/IEC 24762
  - ISO/IEC 24762
  - ISO/IEC 27005
  - ISO/IEC 31000
  - NFPA 1600
  - PCI DSS
  - Etc…
Extensive Tabular Crosswalk between RMM’s 26 Process Areas and 251 Specific Practices and Key Industry Standards

Distinguishing Features of RMM

- **Converges** key operational risk management activities: security, BC/DR, and IT operations

- Guides **implementation and management** of operational resilience activities

- **Descriptive** rather than prescriptive - focuses on the “what” not the “how”

- Provides an organizing convention for effective selection and deployment of codes of practice and standards

- Guide for improvement in areas where an organization’s capability does not equal its desired state
Distinguishing Features of RMM (Cont.)

- Improves confidence in how an organization responds in times of operational stress
- Baseline from which to perform an appraisal
- Enables measurements of effectiveness
- Process improvement model
- Enables institutionalization
- Not a proprietary model

Variety of Ways to Use RMM

- Starting point for socializing important harmonization and convergence principles across security, business continuity, and IT operations activities
- Reference model for understanding the scope of managing operational resiliency
- Process improvement model to catalyze a process improvement effort
- Baseline from which to perform an appraisal of an organization’s capability
- Guide for improvement in areas where an organization’s capability does not equal its desired state
- Organizing construct for codes of practice
- Taxonomy
Contents

Part 1
- Concepts of resilience and operational resilience

Part 2
- Why is it important?
- What are the relevant challenges faced by organizations?

Part 3
- How is it related to traditional and ongoing preparedness planning activities?

Part 4
- Who is talking about it?
- Who is asking for it?

Part 5
- Cornerstones of operational resilience
- Techniques for improving and managing operational resilience
- CERT Resilience Management Model (RMM)

Nomenclature & Background

Business & Operational Drivers

Techniques, Methods & Frameworks

Thank you for your attention…
References


© 2012 NM