CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Managing Disruptive Events: Demand for an Integrated Approach to Better Manage Risk

Key Message:Governments and markets are calling for the integration of plans for and responses to disruptive events.

Executive Summary

Organizations, large or small, public or private, civilian or federal, continue to invest in a variety of independent system protection and sustainment activities including information security, business continuity, IT disaster recovery, crisis management, workforce continuity, and emergency management. However, given the extreme complexity of today's system of systems, and the global socio-economic challenges faced by organizations, a traditional disjointed stovepipe approach to protection planning is no longer viable; neither operationally nor financially. Successful protection of one's enterprise and its systems now requires a fully integrated approach that incorporates unification, standardization, automation, and training while balancing affordability and risk management. Operational resilience provides an integrated approach to protect and sustain systems and associated operations [1].

In this podcast, Nader Mehravari, a member of CERT's Cyber Resilience Center, discusses principles and practice of operational resilience as applied to today's increasingly high-risk, disruptive events. This podcast is the second in a three part series based on Nader's tutorial at the IEEE Conference on Technologies for Homeland Security, presented in November 2012. Part 1 is available here.

PART 1: CHALLENGES WHEN USING MULITPLE PREPAREDNESS PLANS

Summary of the First Podcast

Nader discussed a broad range of destructive events:

- natural such as Hurricane Sandy
- manmade such as the nationwide failure of the power grid in India
- intentional such as terrorist bombings or cyber attacks
- physical such as explosions and shootings
- virtual such as data corruption and fraud

The risk environment is changing and rapidly expanding. As a result, the impact of destructive events is increasing and becoming more of an issue. Organizations can fail after making one mistake.

The question is "What should organizations do to deal with destructive events going forward?"

Proliferation of Preparedness Plans: Some Examples

Japan experienced a triple disaster in 2011: a major earthquake followed by a tsunami followed by a nuclear incident. This event required the execution of many types of plans, some of which were successful and some which were not:

- disaster recovery
- business continuity
- crisis management and communication

In 2011, the Sony PlayStation network security breach required the execution of information security/cyber protection and crisis communication plans.

A major flood in Thailand required the execution of a supply chain contingency plan, given their role as a global developer and manufacturer of computer hard drives.

An employee of British Petroleum lost a laptop that contained personal information of thousands of oil spill claimants. This required the execution of their privacy breach incident plan.

Increasing Risk, Mitigated by Coordination and Collaboration

From these examples, we see that public and private organizations are being forced to develop an increasing number of mostly independent and stovepiped preparedness plans. Multiple plans are more expensive to manage, execute and maintain; this increases an organization's risk exposure.

Coordination and collaboration among plans provide an opportunity to reduce or eliminate redundant activities, which would increase an organization's effectiveness when responding to a disruptive event.

The Need for an Enterprise-wide Role

Disaster recovery plans may be the responsibility of the CIO or IT. Business continuity plans may be the responsibility of operations or manufacturing.

Having a central role at a higher level in the organization (enterprise-wide), responsible for all plans, may allow for more effective integration and reduce the need to develop new plans in the future.

PART 2: GOVERNMENT AND MARKET DEMAND; INCREASING STANDARDS

National Government Demand

The US Cyberspace Policy Review calls for "game-changing technologies that have the potential to enhance the security, reliability, **resilience**, and trustworthiness of digital infrastructures." This is a change from four or five years ago, now calling for plans for all operational risks, not just one type of risk.

The US Department of Defense research priorities for 2013-2017 include a new area titled "Engineered **Resilience** Systems."

The United Kingdom Cyber Security Strategy calls for "safe, secure, and **resilient** systems" and includes funding for integration activities.

Academic Degree Programs

New degree programs such as Master of Science in Resilience Management and Disaster Resilience Leadership are being offered as well as other post-graduate degrees in resilience.

Job Postings

New job postings are looking for subject matter experts in both information security and disaster recovery, and cyber security and resilience.

US Federal Standards

As part of the response to 9/11, those developing the 9/11 Commission report realized that 80% of the critical infrastructure in the US is owned and operated by the private sector. In addition, there is no mechanism to assess how prepared that infrastructure is when dealing with a disruptive event.

The US Congress designated the US Department of Homeland Security to be responsible for putting a program in place, called PS-Prep™ Private Sector Preparedness. Private sector entities can use PS-Prep standards and

specifications to measure their capability.

Financial Ratings

Firms like Standard & Poor's, Moody's, and Fitch that rate organizations based on their financial performance are now including enterprise risk management in their annual assessment. Enterprise risk management includes operational risk, specifically business continuity and disaster recovery.

An Increasing Number of Standards

The number of standards from national and international organizations such as ISO (International Standards Organization) dealing with preparedness planning has quadrupled from 2002 to 2005/2006 and beyond.

Preview of Part 3 in this Series

- Address these questions: Are there proven ways to do things better? Are there better ways to integrate different preparedness planning activities?
- Provide some examples of where this is being done successfully

Resources

[1] Mehravari, Nader. "Principles and Practice of Operational Resilience." IEEE Conference on Technologies for Homeland Security, November 2012.

CERT Podcast, Part 1: Managing Disruptive Events: Making the Case for Operational Resilience

CERT Podcast, Part 3: Managing Disruptive Events - CERT-RMM Experience Reports

CERT Resilience Management website