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

Managing Disruptive Events: Making the Case for Operational Resilience

Key Message:Today's high-risk, global, fast, and very public business environment demands a more integrated approach to not be surprised by 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 first 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: TRADITIONAL APPROACHES INSUFFICIENT: SURPRISES FROM HURRICANE SANDY

Recent Examples of Disruptive Events

- Hurricane Sandy, October 2012
- Gulf of Mexico Deepwater Horizon oil spill, 2010
- Japan earthquake and tsunami, 2011
- Sinking of the Costa Concordia, January 2012

Hurricane Sandy

Largest Atlantic hurricane on record: wind diameter of 1,100 miles

- Large impact but expected
  - flooding
  - wind damage
  - loss of power
  - demand for power generators

- Unexpected surprises
  - major devastating fire in Queens, NY; first responders to fires deployed elsewhere
  - blizzard in West Virginia
  - sandstorms in Seaside Heights, NJ

Disruptive events will continue to surprise us in ways that will disrupt business operations. We need more effective approaches for dealing with these unknowns.

PART 2: TRADITIONAL APPROACHES TOO STOVEPIPED; NOT SCALABLE

Traditional approaches exist for the following disciplines:

- business continuity and continuity of operations
- disaster recovery
- crisis management
- emergency preparedness and management

New approaches are being added for the following disciplines:

- pandemic planning
- workforce continuity
- supply chain continuity

Each of these disciplines requires comprehensive planning and the exercise and test of complex activities. Developing each of these in a silo creates duplication of effort. This approach is neither efficient nor affordable.

An operational resilience approach calls for coordination and integration across these related disciplines, including protection and sustainment activities.

PART 3: OPERATIONAL RESILIENCE TO BETTER DEAL WITH FAST, PUBLIC, GLOBAL DISRUPTIONS

Critical Question

In the presence of a disruptive event, how can organizations continue operating, continue developing products, continue operations under stress, and continue while preparedness plans are being executed to recover and restore capability?

An operational resilience perspective provides a more strategic approach for addressing these questions.

The Nature of Today's Disruptions

When a disruptive event occurs:

- It happens quickly.
- It is often highly publicized.
- It is impossible to ignore; a response is required.
- Customers can quickly migrate to competitors, resulting in a direct impact to the bottom line.

A Few 2012 Events

These types of events are causing business executives to pay more attention:

- Tropical storm Isaac, resulting in delays of the Republican National Convention
- Typhoon Haikui, resulting in the evacuation of about 1 million people
- Linked In security breach, which affected 6.5 million users
- Yahoo security breach, resulting in the release of almost half a million passwords
- Twitter data center failures
- India electric grid failure, affecting 600 million people

Ask the Right Questions

Some ask "Are more disruptive events occurring?" While useful, this may not be the best question to ask.

A better question may be “Even if the number of disruptive events is not increasing, is something else changing that is causing disruptions to be more important and more critical?” The answer is yes.

The Nature of Today's Risk Environment

Over the last 10-15 years:

- The global risk environment has changed and worsened. Organizations are globally inter-dependent. A small disruption can have significant ripple effects, for example, to supply chains.
- Business operations have become much more complex. Small disturbances can cause entire businesses to fail.
- Businesses are fully dependent on technology so when technology is disturbed, they feel the effects more.
- Events happen much more quickly, accelerated by automation (for both disruptions and potential solutions).
- The business environment has become very unfriendly and there may not be a second chance after a first major incident.

A refinement of the better question is “How should we deal with this expanding and worsening global risk environment?”

Preview of Future Podcasts in this Series

- Part 2: What are better ways to deal with disruptive events? What are organizations doing about this?
- Part 3: What are some concrete techniques and approaches that organizations can use to improve and measure their operational resilience?

Resources

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

CERT Resilience Management website

CERT Podcast, Part 2: Managing Disruptive Events: Demand for an Integrated Approach to Better Manage Risk

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