CERT PODCAST SERIES: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Managing Disruptive Events: CERT-RMM Experience Reports

Key Message: Four experience reports demonstrate how the CERT Resilience Management Model can be applied to manage complex and diverse operational risks.

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 and Measurement Center, discusses four experience reports in applying the CERT Resilience Management Model to enact operational resilience principles and practices. This podcast is the third in a three-part series based on Nader's tutorial at the IEEE Conference on Technologies for Homeland Security, presented in November 2012. The first podcast is available here, and the second podcast is available here.

Part 1: U.S. DEPARTMENT OF HOMELAND SECURITY CYBER RESILIENCE REVIEW

Summary of Podcasts One and Two

In Nader's first podcast, he discussed:

- operational stress experienced by organizations on a minute-by-minute basis
- examples of recent disruptive events and some surprising consequences
- shortcomings in today's business processes when dealing with complexity
- dependence on global resources

In Nader's second podcast, he discussed:

- the question "Are there better ways to deal with disruptive events?"
- concepts of operational resilience
- the CERT Resilience Management Model (CERT-RMM) as an overarching framework to manage operational resilience

DHS Cyber Resilience Reviews (CRR)

Eighty five percent of U.S. critical infrastructures are owned and operated by private sector organizations. Department of Homeland Security (DHS) initiated Cyber Resilience Reviews to determine the extent to which such organizations are prepared to deal with a disruptive event.

The purpose of CRRs is to assess the cybersecurity risks to U.S. critical infrastructures and associated key resources.

The CRR method is based on CERT-RMM. It supports DHS in determining the health of an organization's cybersecurity program. In using CERT-RMM as the basis, DHS:

- determined that the organizational scope for the CRR would be critical infrastructure and key resource providers and state, local, and tribal government agencies
- selected 10 domains relevant to assessing cybersecurity preparedness and security posture

CRRs have been regularly performed for the past three years and continue today.

CRR Domains

The 10 domains that are addressed in the CRR method include

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

Conducting a CRR

The steps for conducting a CRR include the following:

- DHS selects an organization to be reviewed.
- The organization is provided with and fills out a pre-assessment questionnaire.
- Subject matter experts perform a one-day site review, which consists of a facilitated interview and data collection.
- At the end of the one-day review, a report is generated that identifies strengths and weaknesses, and recommends areas for improvement.

Part 2: U.S. DEPARTMENT OF ENERGY ELECTRICITY SUBSECTOR CYBER CAPABILITY MATURITY MODEL

Background

Early in 2012, the White House asked the U.S. Department of Energy, “Is there an efficient and economic way to assess the strength of the cybersecurity capabilities of owners and operators of the U.S. electrical grid?” This includes generation, distribution, transmission, and control of electricity.

The objectives included

- assess the strength of owner/operator cybersecurity capability
- have a consistent method for evaluation
- benchmark current capabilities
- identify and share best practices

ES-C2M2 Development and Use

The model was developed very quickly – in 3-4 months in early 2012. This was possible due to the use of CERT-RMM as the starting point. Pilot uses of the model commenced in April 2012 with 19-20 being conducted.

Electricity Subsector Cyber Capability Maturity Model (ES-C2M2) is now being used on a regular basis by DOE, in a fashion similar to DHS's use of the CRR. Several subject matter experts conduct a one-day review and provide feedback on strengths and shortcomings, and recommendations for improvement.

The model is publicly available. Owners and operators can use the model to conduct a self-assessment of their capabilities. The ES-C2M2 website includes self-assessment spreadsheets and tools.

This derivative of CERT-RMM has become widely publicized and is being considered as an example to assess and improve cybersecurity for other critical infrastructure sectors. The U.S. National Institute of Standards and Technology (NIST) is considering the experiences that organizations have had in applying ES-C2M2 as part of their response to the recent Executive Order and the development of their cybersecurity framework.

PART 3: U.S. POSTAL INSPECTION SERVICE - PROTECTING THE MAIL

Background

The U.S. Postal Inspection Service (USPIS) is the law enforcement arm of the U.S. Postal Service (USPS). Its mission is to ensure that all U.S. mail is safely transported and delivered. As a result, they are faced with a wide range of operational risks that need to be managed and selected CERT-RMM to assist in doing this.

A summary of experiences in applying CERT-RMM to a range of USPIS projects is described in the August 2012 podcast by Greg Crabb, Inspector in Charge of Revenue, Product, and Global Security.

Safety and Security of International Mail

Using a Universal Postal Union (UPU) standard for the physical security of international mail as requirements, USPIS and CERT developed a risk-assessment instrument that provides postal inspectors with a method to assess the physical safety and security of international mail in other countries. This is important as these facilities serve as the origination point for mail entering the United States.

This instrument was based on CERT-RMM assessment experiences. It has been well received by USPS personnel and is recommended by the UPU as the accepted assessment method.

Assuring Express Mail Revenue

CERT-RMM describes four types of assets: information, technology, people, and facilities. The model is designed to allow users to include new types of assets. In the case of the USPIS, the asset they care most about is mail. The USPIS and CERT have collaborated to develop a complementary set of mail-specific process areas that address mail as a new type of CERT-RMM asset.

This new content has been used to develop and pilot a customized instrument for assessing Express Mail, specifically risks to revenue generated by express mail. This is important to the USPIS, given the revenue generated by Express Mail in comparison to other classes of mail.

PART 4: LOCKHEED MARTIN CORPORATE BUSINESS RESILIENCY STRATEGIC INITIATIVE

Assess Resilience Posture Across the Enterprise

Lockheed Martin selected CERT-RMM to assess their current resilience posture to determine if it was sufficient for their business needs. Once improvements were implemented, the model was used to continuously assess and measure if goals were achieved.

CERT-RMM provided a common and consistent “ruler” to use across the enterprise. It was also helpful in establishing a common vocabulary for use by participating business units.

The model has also been used to integrate existing risk management activities including disaster recovery, business continuity, and crisis management.

Assess Intent of Policies

Lockheed Martin used CERT-RMM to assess intent, i.e., determine if a planned improvement will produce the desired result. They assessed their resilience-related policies (referred to as command media) that drive risk-management activities to determine if they would result in the intended actions and behaviors.

Such an assessment can identify major shortcomings and strengths in one policy that should be replicated in others.

Resources

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

Mehravari, Nader. "Achieving Organization Mission Through Resilience Management." A Discussion with CERT Experts: Constructing a Secure Cyber Future, SEI Webinar Series, 30 April 2013. Video also available.

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

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

CERT Resilience Management website.