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

US Postal Inspection Service Use of the CERT Resilience Management Model

Key Message: CERT-RMM can be used to establish and meet resilience requirements for a wide range and diverse set of business objectives.

Executive Summary

"The mission of the U.S. Postal Inspection Service (USPIS) is to support and protect the U.S. Postal Service and its employees, infrastructure, and customers; enforce the laws that defend the nation's mail system from illegal or dangerous use; and ensure public trust in the mail [1]. The USPIS has used the CERT Resilience Management Model (RMM) and its appraisal method to address export screening, new product security, measuring and monitoring risks associated with fraud, and physical security and aviation screening for international mail.

In this podcast, Greg Crabb, Inspector in Charge of Revenue, Product, and Global Security for the USPIS, discusses his organization's experiences in tailoring RMM for a wide range of Postal Service and USPIS business objectives.

PART 1: MOTIVATION FOR USING RMM – PROCESS VS. CONTROLS

Motivation

In their work with Carnegie Mellon University's Software Engineering Institute, USPIS staff were encouraged to examine RMM to help improve their processes for investigative response to network security incidents.

While doing so, Greg recognized that RMM could be applied to other resilience and investigative activities.

USPIS provides investigative response to a range of incidents including:

- hurricanes and their impact on postal operations
- carrier robberies or thefts where employees are threatened

In the presence of these types of events, resilience means being able to respond to such situations as they affect postal assets.

Roles

Greg's organization is responsible for:

- revenue investigations (assuring proper payment by mailers of $64 billion of postal revenue)
- product security (delivery of letter and package products)
- global security for international mail

Greg is using RMM to assure structure and completeness in the Postal Service and USPIS's process management over these activities.

Process vs. Controls

By using a process approach, Greg has observed that he can be a better partner to business owners as they expand the Postal Service product base to meet customer needs.

A controls-based approach often forces controls upon a business unit, which they resist and question. When using a process approach, the focus is on meeting goals without the requirement of a specific control objective.

A process approach is more flexible and often reduces the costs associated with implementing specific, more prescriptive, and often more costly controls.

PART 2: USING RMM TO ADDRESS THREE DIVERSE USPIS OBJECTIVES

Export Screening

On a weekly basis, the Postal Service processes well over one million packages to overseas locations. USPIS is responsible for assuring that mailers comply with specific export control requirements.

By using RMM, Greg was able to identify RMM process areas (PAs) (including process maturity) that were applicable to this compliance objective. These included:

- HRM: Human Resource Management
- COMP: Compliance
- OTA: Organizational Training and Awareness
- MA: Measurement
- and a few others

Using these PAs, Greg's team:

- defined specific goals and practices that neeed to be achieved and a project plan for doing so
- defined work products to guide decision-making on what outputs to produce
- took a complex, overwhelming task and managed it using common criteria

With this structure, the team understood their goals, what they needed to do, and the work products that were to be produced.

RMM Is A Reference Model

RMM has 26 process areas that cover the disciplines of information security, business continuity, and aspects of IT operations. The intent for users of the model is that they select those PAs, specific goals, and specific practices that are applicable to a specific objective (such as export screening) and ignore the rest.

It is critical to identify which model content is most relevant based on the specific project need (referred to as model scope).

New Product Security

USPIS is often called upon to assess new products that the Postal Service is considering. RMM is useful in evaluating the risks and rewards associated with new products.

For the new product that Greg discussed, analysis, scoping, and risk considerations were important. His team selected the relevant PAs and then applied the RMM Risk Management (RISK) process area to each of these PAs for the new product.

The team:

- developed strong risk statements consistent with PA specific goal and practice criteria, exercising the RISK PA goal "identify asset-level risks."
- developed a catalogue of risk statements for the product

- prepared a briefing to the CFO based on these statements

Given these actions, decision makers were able to properly define and apply risk mitigation strategies. This was accomplished in less than 3 business days, which would not have been possible without the use of RMM.

Measurement and Monitoring

Greg's team has used RMM to develop new measurement and monitoring activities for examining revenue resilience, by defining performance reporting capabilities against these activities.

One example is a relative risk rating for each customer. The risk rating helps USPIS examine what each organization represents to the Postal Service from a fraud perspective. Using this rating, USPIS can apply procedures to:

- identify criminal misconduct
- reduce relative risk by applying appropriate control procedures

---

PART 3: MAIL-SPECIFIC PROCESS AREAS; APPRAISAL FOR INTERNATIONAL MAIL

Development of Mail-Specific Process Areas

USPIS has contracted with CERT to develop four mail-specific process areas that cover the transportation, management, and delivery of mail. These are intended to compliment (be used with) the existing 26 process areas in RMM.

The purpose of this project includes:

- defining common criteria for assuring that Postal Service products are resilient
- evaluating business partners and customer operations in their handling of mail
- assess resilience practices for all Postal Service activities

Using this approach, Greg's team will be able to communicate across USPIS and the Postal Service using a common framework to drive improved performance for investigative and security operations (his areas of responsibility).

Assessing the Security of International Mail

For the past 16 years, the USPIS has chaired the Postal Security Group of the Universal Postal Union (UPU). The UPU is a United Nations Specialized Agency for postal affairs of 192 postal administrations worldwide. The UPU manages over 600,000 facilities and delivers mail to every address around the world.

The USPIS and CERT have applied the RMM appraisal method to a new UPU draft standard to assess the physical security and aviation screening practices for international mail.

At a congress in Doha, Qatar this September, UPU members will vote to mandate minimum physical and process security standards. Compliance with these pending mandates will be assessed using this new method.

The new appraisal method has been piloted with 2 postal administrations. This included:

- providing pre-assessment questionnaires to the postal administrations being assessed, which aided in preparation
- generating heat maps from the appraisal that were well understood by managers from security operations to chief executive officers

Adopting and Using RMM

The RMM book is over 1000 pages and is very daunting upon first introduction. Greg has encouraged his team to

become familiar with the content and gain some level of understanding.

More pragmatically, applying RMM to a specific situation or objective helps Greg frame the appropriate response that USPIS should apply, on a weekly basis.

From the first CERT-RMM Users Group, members observed that it is often best to "put the book in the drawer." It is more effective for a small team to take an organizational objective, determine which RMM PAs are most applicable, and perhaps not communicate to the larger organization that RMM was the source for the improvement approach.

In Greg's experience, the business units have a strong appreciation for the work products that are generated by using the model.

Resources

[1] United States Postal Inspection Service website

CERT website

CERT-RMM website (which include links to RMM webinars and podcasts)

Caralli, Richard; Allen, Julia; White, David. *The CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience*. Addison-Wesley, 2011.

Joch, Alan. "Operational Resilience: Bringing Order to a World of Uncertainty." FCW.com, July 8, 2013.