Improving the Security and Resilience of U.S. Postal Service Mail Products and Services Using CERT®-RMM (Case Study)

Julia Allen
Principal Researcher, CERT® Division

Julia Allen is a principal researcher with Carnegie Mellon University Software Engineering Institute's (SEI) CERT Program. Her areas of research include operational resilience, security frameworks, and measurement. She is the author of The CERT Guide to System and Network Security Practices and co-author of Software Security Engineering: A Guide for Project Managers and CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience. She is the moderator of the CERT Podcast Series: Security for Business Leaders. Prior to joining CERT, Allen served as the SEI's acting, and deputy director and Chief Operating Officer. Prior to joining the SEI, she led software development for embedded systems at SAIC and managed large defense systems software development for TRW.

A Sampling of CERT® Resilience Management Model Applications and Derivatives

U.S. Postal Inspection Service (USPIS)

The law enforcement arm of the United States Postal Service (USPS)

One of the oldest federal law enforcement agencies in the United States, dating back to 1772

Mission of the USPIS:

- Support and protect the USPS and its employees, infrastructure, and customers
- Enforce the laws that defend the nation's mail system from illegal or dangerous use
- Ensure public trust in the mail

USPIS Sponsorship

USPIS sponsor 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

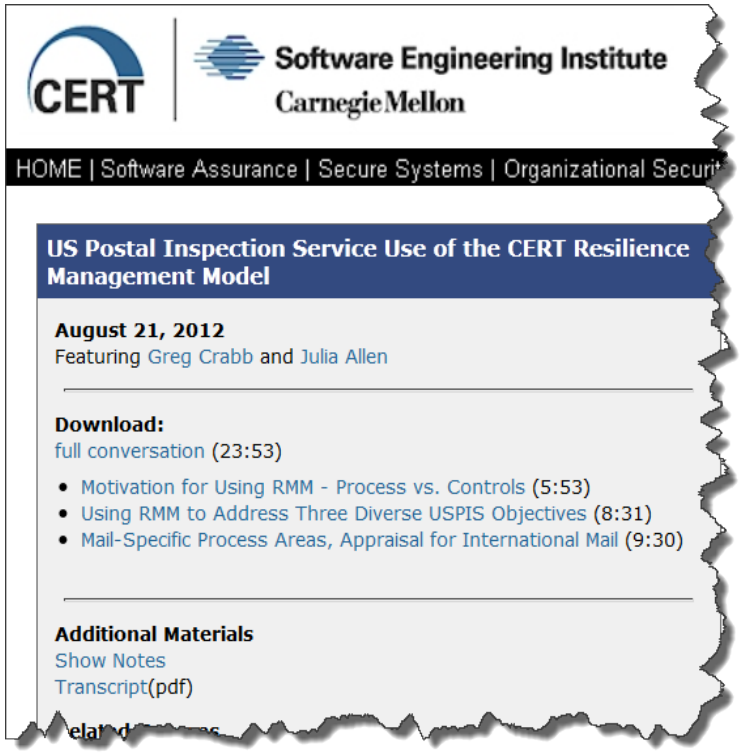
Using CERT-RMM to assure USPS/USPIS effective process management structure and completeness for these areas of responsibility

Benefits of a process approach (vs. controls)

- Can be a better partner to business owners as they add new products
- Can focus on meeting goals vs. implementing specific controls
- Is more flexible; reduces control implementation costs

Use of CERT-RMM by USPIS

- export screening
- new product security
- improved processes for investigative response to network security incidents
- measuring and monitoring risks associated with fraud
- development of mail-specific process areas (PAs) for mail induction, revenue assurance, and international mail transportation
- customized PA-based appraisal to identify Express Mail revenue risks
- physical security and aviation screening for international mail



http://www.cert.org/podcast/show/20120821crabb.html

*Improving the Security and Resilience of U.S. Postal Service Mail Products and Services Using the CERT® Resilience Management Mode*l, CMU/SEI-2013-TN-034, January 2014.
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=77277

Use of Mail-Specific Process Areas

Intended to complement (be used with) the existing 26 process areas in CERT-RMM

Purpose:

- define common criteria for assuring that USPS products and services are resilient
- evaluate business partners and customer operations in their handling of mail
- ensure the resilience of mail (availability, sanctity, custody, visibility, access)
- assess resilience practices for selected USPS activities using customized appraisal instruments

Communicate across USPIS and USPS using a common framework to drive improved performance for investigative and security operations

Mail Induction PA – Sample Content

Purpose	Goal/Practice	Practice, Subpractice
Ensure that all mailpieces (mail) are inducted (collected and accepted) in accordance with USPS standards	Accept Mail practice	• Assist mailers in preparing mail according to standards • Refuse prohibited and improperly prepared mail • Verify eligibility of the mailpiece (type, class, extra services) • Perform acceptance scans • Ensure that each mailpiece is properly marked and endorsed • Ensure that correct payment for postage is made • Perform verification • Identify discrepancies

Mail Revenue Assurance PA – Sample Content

Purpose	Goal/Practice	Practice, Subpractice
Ensure that the USPS is compensated for all mail that is accepted, transported, and delivered	Assure Mail Revenue goal	• Verify that postage affixed is sufficient • Verify that postage is not fraudulent • Verify receipt of payment for postage • Address mail revenue discrepancies

International Mail Transportation PA – Sample Content

Purpose	Goal/Practice	Practice, Subpractice
Ensure that all international mail is transported in accordance with UPU (Universal Postal Union) standards.	Transport Mail and Screen Mail goals	• Sort mail for transportation • Prepare mail for transportation • Transport mail to destination processing facilities (includes customs) • Identify mail to be screened • Screen mail (high-risk mail; dangerous/hazardous goods)

Express Mail Revenue Risk Identification

Users: USPIS postal inspectors and revenue fraud analysts

Objectives:

- Examine and evaluate Express Mail (EM) operations at USPS facilities to verify risks to EM revenue (unaccepted EM, shortpaid EM, use of fraudulent postage)
- Inform local improvements at the assessed facility
- Inform USPS decisions on targeting efforts to reduce risks of EM revenue loss across the postal system
- Identify cases requiring further investigation

Method:

- One-day scripted interviews and evidence collection
- Characterization of questions: fully implemented, largely implemented, partially implemented, not implemented
- Characterization of practices: heuristics to assign high, medium, low

Assessing the Security of International Mail

USPIS and CERT have applied the CERT-RMM appraisal method to two new UPU standards to assess the physical security and aviation screening practices for international mail.

Compliance with these mandates is being assessed using this new method.

This appraisal method has been piloted with several international postal administrations.

Pre-assessment questionnaires are provided to the postal administrations being assessed, which aids in preparation.

- Heat maps, generated from the appraisal, are well understood by managers from security operations to chief executive officers.

A Proven Method for Identifying Security Gaps in International Postal and Transportation Critical Infrastructure, CMU/SEI-2013-TN-033, January 2014.

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=77265

Lessons Learned – Key Takeaways

When properly interpreted, CERT-RMM can be applied to a wide range of business objectives.

New asset types can be added, such as mail.

New process areas can be developed and used in concert with existing CERT-RMM process areas. For example:

- Identification of discrepancies in mail-specific PAs invoke the Incident Management and Control PA.
- Identification of risks in mail-specific PAs invoke the Risk Management PA.

CERT-RMM appraisal and diagnostic methods can be customized to identify improvement actions that align with specific business objectives.

Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0000506

SEI Training

Introduction to the CERT Resilience Management Model

February 18 - 20, 2014 (SEI, Arlington, VA)

June 17 - 19, 2014 (SEI, Pittsburgh, PA)

See Materials Widget for course document