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

Integrated, Enterprise-Wide Risk Management: NIST 800-39 and CERT-RMM

Key Message: Business leaders must address risk at the enterprise, business process, and system levels to effectively protect against today’s and tomorrow’s threats.

Executive Summary

“The complex relationships among missions, mission/business processes, and the information systems supporting those missions and processes require an integrated, organization-wide view for managing risk,” specifically information security risk [1]. Senior leaders need to ensure that the organization’s risk management process is being effectively conducted across these three tiers by framing a robust business context, regularly assessing risk, determining appropriate mitigation strategies, and monitoring to ensure that today’s actions are sufficient to address tomorrow’s risks.

In this podcast, Dr. Ron Ross, with the U.S. National Institute of Standards and Technology (NIST), discusses how to organize a robust information security risk management program as described in NIST Special Publication 800-39 Managing Information Security Risk: Organization, Mission, and Information System View. Ron is the Project Leader for the FISMA (Federal Information Security Management Act) Implementation Project. Ron is joined by Jim Cebula, a member of the Resilience Enterprise Management team at CERT. Jim will discuss connections between 800-39 and the CERT® Resilience Management Model (CERT®-RMM).

PART 1: MANAGING ENTERPRISE RISK VS. CHASING VULNERABILITIES

Strategic, Enterprise Risk Management vs. Information System Risk Management

NIST 800-39 addresses information security risks that primarily come from the operation and use of information technologies.

Given that

- adversaries intent on compromising information systems use very sophisticated tools, techniques, and procedures, and
- organizations depend heavily on information technology for business success,

addressing information security as an enterprise-wide risk management concern is essential.

NIST 800-39 takes a holistic view of risk management versus a checklist view. The checklist view typically uses a list of controls or a controls catalogue. In most cases, a controls view of risk management is a compliance activity focused at the information system level (necessary but not sufficient).

The CERT Resilience Management Model (CERT-RMM) enterprise focus (EF) process area aligns well with the enterprise-wide view of NIST 800-39. EF addresses

- setting organizational strategic objectives
- establishing critical success factors
- identifying key services
- providing governance
- providing financial resources

These are all business issues that senior managers need to address before doing a deeper dive into technical controls at the system level.

Chasing Vulnerabilities vs. a Three-Tiered Approach to Risk Management

The NIST 800-39 approach to risk management evolved from a great frustration in seeing organizations chase one vulnerability after another. The supply of weaknesses and deficiencies is limitless, so this chase never ends. This current state has no up-front strategy for increasing the security or resilience of today's operational systems.

The three tiers described in NIST 800-39 are as follows:

- Tier 1: Organization View. This is the strategic and governance level, where core missions and business functions are defined. Each is prioritized according to its importance to mission and business success. Tier 1 includes
  - creating a risk management strategy
  - identifying tools, techniques, and procedures for assessing risk
  - evaluating risk
  - defining the risk management strategy at the enterprise level (accept, reject, share, transfer, and/or mitigate risks to an acceptable level)
  - defining tolerances for risk
  - monitoring risk over time to ensure that previously accepted risks are still valid today
- Tier 2: Mission/Business Process View. Business processes are the steps and actions taken to carry out the missions. This tier includes enterprise architecture (reducing, consolidating, standardizing, optimizing) toward the end objective of effective, secure information technologies that support the architecture.
- Tier 3: Information System View. This tier derives from Tiers 1 and 2. It includes specific security controls for specific systems based on the importance, sensitivity, or criticality of the information that resides on each system.

Dealing with Today's Operational and Legacy Environments

Many organizations today are firmly entrenched in Tier 3, given their current operational environment. The NIST 800-39 approach requires organizations to rethink their approach to risk management based on determining what approaches would be most effective given the organization's culture.

Organizations need to start organizing efforts at the strategic level and ask the hard questions. This likely includes reengineering mission and business processes to become more risk-aware, based on a greater understanding of vulnerabilities and threats.

PART 2: RISK MANAGEMENT AND RESILIENCE; KEY STAKEHOLDERS

CERT-RMM and Risk Management

CERT-RMM is a maturity model for managing operational resilience. The operational resilience management system defined in CERT-RMM has four objectives, many of which directly support the three tiers in NIST 800-39. These are:

1. Prevent operational risks to a high value service – a protection strategy.
2. Sustain the operation of a high-value service if a risk is realized – a sustainment strategy.
3. Deal with the consequences of a realized risk to return to a normal state.
4. Optimize objectives 1, 2, and 3.

Resilience is an organizational property that emerges from the effective management of operational risks, which occur in four categories:

- actions of people

- failures of systems and technology
- failed internal processes
- external events

Operational risk is more than just system and technology failures.

Operational resilience as defined by CERT-RMM reflects the convergence of three disciplines, which typically operate as silos within most organizations:

- security
- business continuity
- IT operations
- failed internal processes

The CERT-RMM risk management process area covers many of the same topics as NIST 800-39, including identifying risk tolerances. Risk management decisions are being made routinely in all three tiers, whether the organization realizes this or not. If these decisions are not informed by enterprise-level guidance on risk tolerances, consequences, and impacts, they are likely being made in an uncoordinated, inconsistent manner.

Key Participants and Stakeholders

The following key participants and stakeholders are essential when establishing an enterprise-wide risk management program:

- senior leaders, including the CEO (Chief Executive Officer), CFO (Chief Financial Officer), CTO (Chief Technology Officer), heads of agencies, and second-level bureau chiefs. Without senior leader commitment and involvement, this effort will not be successful.
- CIO (Chief Information Officer), CISO (Chief Information Security Officer)
- procurement officers, who are pivotal in making well-informed investment decisions to ensure that acquired systems are designed to support core missions. Procurement officers are typically not IT experts, security experts, or risk managers.
- system developers, to build better functionality into commercial products in support of more secure systems
- system operators who are on the front line, detecting and responding to cyber attacks and making necessary improvements
- assessors and auditors

PART 3: RISK MANAGEMENT PROCESS; FOCUS ON THE RED ZONE; GETTING STARTED

The Information Security “Red Zone”

In football, the red zone is the final 20 yards before the end zone. This is a useful analogy for information security. Up to this point in time, the profession has focused on best practices to take care of the 80 percent – known cyber attacks that exploit known vulnerabilities. We need to shift our focus to the more sophisticated, advanced persistent threat – those 20 percent of attacks that can bring organizations to their knees: those that occur in the red zone.

Four Components of a Risk Management Process

These are

- Frame risk: Establish the business context for making risk-based decisions. Identify constraints (budgetary, operational). Establish risk tolerances. Prioritize activities and perform tradeoffs.
- Assess risk: Determine threats, vulnerabilities, likelihood, and impacts.
- Respond to risk: Determine how to respond to/mitigate identified risks (accept, reject, transfer, share with partners; mitigate with additional safeguards, countermeasures, and controls)

- Monitor risk: Determine if today's assessment is consistent with tomorrow's. Anticipate new actions taken by adversaries where possible.

Getting Started

Here are some useful first steps for getting started:

- Get senior leadership involved. They need to truly understand what the risks are and commit to reengineering the organization's processes to manage information security risk as identified in NIST 800-39.
- Examine and prioritize the core missions and business functions of the enterprise.
- Determine the current commitment to enterprise architecture (consolidation, standardization, and optimization) for managing IT complexity and identifying the most effective controls. Integrate security into the enterprise architecture.

The threat space is increasingly sophisticated, organizational resources are constrained, and leaders need to work smarter by

- understanding what's most important to the enterprise
- understanding the threat space
- making appropriate investments
- implementing the most effective controls
- reducing risk to mission success

Cloud Computing as One Example

According to the Federal CIO's office, there are compelling business and financial benefits for transitioning selected services to the cloud. Agencies are being encouraged to think "cloud first" when redeploying existing services and acquiring new services.

With these actions, new security risks are likely to arise. These need to be analyzed as part of the decision process for moving to cloud services. The three tiers and four-step process in NIST 800-39 provide guidance to do this.

The CERT-RMM enterprise focus, risk, and external dependencies process areas provide additional guidance that is compatible with NIST 800-39.

Resources

[1] Joint Task Force Transformation Initiative. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39, National Institute of Standards and Technology, March 2011.

Federal Information Security Management Act (FISMA) Implementation Project web site

CERT Resilience Management Model web site

CERT Podcast Series: podcasts in the Risk Management and Resilience category