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

The Path from Information Security Risk Assessment to Compliance

Key Message: Information security risk assessment, performed in concert with operational risk management, can contribute to compliance as an outcome.

Executive Summary

Information security risk assessment is a key practice for identifying and prioritizing security risks to critical information assets and key business processes. Determining which security controls mitigate key risks, for both business and compliance purposes, can only be determined through a continuous risk management process. Conducting security risk assessment in concert with operational risk assessment ensures that security risk identification and mitigation are determined based on impact to the business.

In this podcast, Bill Wilson, manager of CERT's Survivable Enterprise Management team, provides guidelines on how business leaders can use risk assessment as an effective tool for achieving compliance.

PART 1: ASSESSING SECURITY RISK IN A BUSINESS CONTEXT

Why Is Risk Assessment Relevant and Important for Information Security?

Risk assessment allows us to put information security issues in a business context, better understanding the impact to the business in the event of a security breach.

This allows leaders to better answer the "So what?" test, not in technology or security incident terms, but in terms of lost productivity, lost revenue, and potential business interruption – in other words, operational risk.

Leaders can then analyze and prioritize security risks in the context of all other operational risks, using business language and measures of effectiveness.

How Can Risk Assessment Be Used to Prioritize Compliance Requirements?

Current risk-based regulations and standards that call for security controls include:

- FISMA (Federal Information Security Management Act) for federal and civilian agencies
- ISO 27001 (in concert with ISO 17799, now ISO 27002)
- HIPAA (Health Insurance Portability and Accounting Act)
- ITIL (Information Technology Infrastructure Library)
- COBIT (Control Objectives for Information and related Technology)
- COSO (Committee of Sponsoring Organizations of the Treadway Commission)

All of these have many controls and requirements. How does an organization select which ones are most applicable and most important? And which ones can be justifiably eliminated from consideration?

Risk assessment provides an approach for ranking and stacking which security controls to implement, in a business context. It is generally accepted during a compliance review as a defensible basis for control selection and elimination.

An organization can state "We've covered our priority risks. Our budget limitations prevent us from implementing some controls. But because we've gone through a complete risk assessment process and have captured the results in a

defensible form, that's okay." What then remains is for a business leader to manage and track any residual risks.

This approach provides a strong basis for making security investment decisions.

PART 2: ZEROING IN ON A RISK ASSESSMENT METHOD

Examples of Common and Widely Accepted Methods for Assessing Information Security Risk

- NIST SP 800-30 Risk Management Guide for Information Technology Systems
- BSI 7799-3 (soon to become ISO 27003)
- CRAMM (CCTA (Central Computer and Telecommunications Agency) Risk Analysis and Method Management) – a qualitative risk analysis and management tool originally developed by the UK government
- MEHARI (Méthode Harmonisée d'Analyse de Risques Informatiques)
- FRAP (Facilitated Risk Analysis Process)
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Selecting a Useful Method

Consider available case studies, experience reports, and comparisons.

Find one that is most compatible with your organization's operational risk management process, risk criteria, language for assessing risk, and how risk data is typically analyzed and presented.

Make sure to integrate security risk tradeoffs with other organizational risks.

Key Elements of an Effective Security Risk Assessment Approach

Choose a method that recognizes its placement in the risk management and security management life cycles.

- As a diagnostic, to generate information for decision making and control selection

Follow through - make sure control implementation is managed and tracked over time.

Ensure that risk assessments are part of a continuous risk management process/cycle, and conducted periodically or as events warrant.

Treat security risk assessment as part of operational risk assessment and management.

Recognize that most methods in use today are qualitative but progress is being made in determining quantitative losses and impacts.

Focus more on *impact* and *loss*, and less on threat and vulnerability which are constantly shifting and changing. At the core of any risk-based approach is "What's important, and why do I care?"

PART 3: BUILDING A RISK-BASED COMPLIANCE PROGRAM

The Steps

Select an approach, using the guidelines we've covered.

Determine the scope of the assessment (typically a business unit or a selected set of business processes). It is important to bound the information assets and systems of interest, keeping this manageable.

Focus on the most critical assets first.

Select a multi-disciplinary team, including members outside of IT to represent the business/mission perspective and characterize the business impacts.

Perform preliminary analysis and present this to senior decision makers for action.

Make sure there is a well-defined connection to existing operational risk management activities, be it a risk committee or perhaps through internal audit.

Fund and implement risk mitigation controls.

Provide oversight and monitoring to ensure that controls are implemented correctly and are truly reducing risk.

Understand the relationship between risk assessment and compliance: It's not "I'm doing risk assessment to comply with regulation X" but "I'm doing risk assessment because its effective practice." Properly performed risk assessment will often result in compliance as an outcome or byproduct.

Challenges to Anticipate and Address

- Lack of patience – risk assessment takes time to collect information, interact with stakeholders, and conduct analysis.
- Rushing to solution mode – this will often happen as problems that need immediate attention are discovered along the way. This can cause the team and the organization to lose sight of the larger goal.
- Insufficient time spent on characterizing true impact – work with your business continuity and disaster recovery staff.
- The absence of well-defined risk evaluation criteria
- Failure to involve business line personnel, including the owners of critical information assets and key business processes