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

Getting Real About Security Governance

Key Message: Enterprise security governance is not just a vague idea – it can be achieved by implementing a defined, repeatable process with specific activities.

Executive Summary

For an organization that lacks a cohesive enterprise security governance program, establishing one may seem like an overwhelming endeavor. In fact, however, this is not the case. By breaking down enterprise security governance into its component activities, organizations can design and build a security governance program over time, tailoring it to suit their needs.

Toward this goal, Julia Allen, a senior researcher with CERT, has co-authored an implementation guide for enterprise security governance. In this podcast, we discuss that research and how organizations can use it as a framework for establishing effective, sustainable security governance programs.

PART 1: AN EVOLUTION TOWARD PRACTICALITY

Bridging the Implementation Gap

Thinking about security in a governance context is one thing, but actually implementing it is another.

To bridge that gap, the Governing for Enterprise Security Implementation Guide series presents a framework and road map that leaders can use to implement a governance-based security program.

This framework defines:

- a set of activities
- a set of roles and responsibilities
- a set of results, outcomes, and artifacts

Activities are described in sequence, and the description of each activity also includes the results, outcomes, and/or artifacts that are produced by that activity.

For example, for the activity to develop high-level policies, the result is a set of robust policy statements. For the activity to inventory your information assets, then one resulting artifact is the means to capture that inventory.

A Framework, Not a Recipe

This is not a cookbook that contains a definitive recipe for enterprise security governance.

It is a framework that gives business leaders a way to see what a security governance program entails, delegate necessary tasks appropriately, and make conscious decisions such as:

- Should I include or exclude this activity?
- Should I do it in this order?
- Should I combine roles, or should I better distinguish or differentiate roles to preserve segregation of duties?

In other words, it is a tangible guide that can be acted on.

PART 2: A GUIDE TO EFFECTIVE GOVERNANCE

Establish a Governance Culture

What is the difference between organizations that have successful security governance programs and those that struggle with it?

One big difference is that organizations with successful security governance programs have made security a part of their culture. For example:

- There is an appreciation of security roles and responsibilities.
- People understand that they need to be conscientious about protecting sensitive data.
- Segregation of duties is used to avoid conflicts of interest.

Here are some other core essentials for effective enterprise security governance:

- Tone from the top – senior leadership needs to understand that security is important for the well-being, survival, and thriving growth of the organization.
- Establishing a governance structure
- Delineating key roles and responsibilities
- Establishing top-level policies
- Conducting an inventory of the assets to be protected
- Assessing the degree to which those assets are at risk

Form a Cross-Functional Team

Several roles need to be involved for a successful effort. These may include:

- Chief security officer or chief information security officer
- Chief risk officer, if there is one
- Legal counsel
- Human resources
- Public relations
- The owners of the organization’s most critical assets

Once you’ve identified all relevant roles within your organization, form a cross-functional team that meets regularly to:

- Identify risks
- Develop strategies to mitigate those risks

Brainstorm Benchmarking Solutions

One difficulty: Because security is a new discipline, there’s no standard or commonly accepted set of security benchmarks against which you can gauge your organization’s level of security.

Some possible solutions:

- Develop your own benchmarks
- Benchmark against peer or lead competitor organizations

The cross-functional team may be in the best position to do this. Make sure team members take into account the varying laws among U.S. states and different countries.

PART 3: MAKING SECURITY A MAINSTREAM PROCESS

Security Is Just a Business Process

Eventually, in implementing a security governance project, something is likely to go wrong. This can be almost anything, from a major security incident to a lack of cooperation by a particular group or division in the rollout process.

How can an organization deal constructively with these problems?

One of the best ways to minimize problems is to make sure security is mainstreamed – treated like any other business process.

For example, if an organization uses balanced scorecard for quarterly performance measurement, security should be one of the performance metrics that is measured.

For major security incidents, apply existing business processes for business continuity, crisis communication, incident handling for non-security situations (such as a product recall), and so on. Simply extend these existing processes to embrace and integrate security considerations.

Here's another example: If a key champion of the security governance program were to leave the organization, normal business processes would kick in and other business leaders in the organization would:

- Reassign roles and responsibilities
- Craft the key messages that are going to be delivered to the press and/or employees

A Repeatable, Consistent Process

How possible is it, really, to make security governance a repeatable process?

Note that in the organizations that are most successful with security, security is just assumed. Just as it's assumed that employees will fill out their timesheets or make purchase requests in the standard way, it's also assumed that employees will follow security policies and procedures.

So, yes, it is possible to make security a repeatable, consistent process within an organization. Each organization, of course, will tailor its security efforts to its particular mission and critical assets.

Future Outlook

In the future, more regulation is likely until the business community demonstrates they have security issues handled at an acceptable level.

More and more, organizations may be willing to talk about their success stories so that other organizations can learn from them. This would create a rising tide that lifts all boats.

Resources

CERT Governance Portal

Institute of Internal Auditors

IT Governance Institute and Information Systems Audit and Control Association

National Association of Corporate Directors
