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

Resiliency Engineering: Integrating Security, IT Operations, and Business Continuity

Key Message: By taking a holistic view of business resilience – similar in many ways to classical engineering – business leaders can help their operations stand up to known and unknown threats.

Executive Summary

As threats proliferate, organizations have a choice: They can scramble to fix vulnerabilities one by one, or they can increase their overall resilience so that even unexpected threats have less impact on their ability to fulfill their business mission.

It can seem daunting to embark on an enterprise-wide business resiliency project, however.

In this podcast, Lisa Young, a senior member of CERT's Resiliency Engineering Team, discusses what resiliency engineering means – and how organizations can put it to practical use to resist threats more effectively.

PART 1: THE RESILIENCY ENGINEERING MODEL

Strategy vs. Tactics

In many cases, problems exist with security management today. It is often:

- Seen as a technical problem
- Bolted on as an afterthought
- Burdened by poorly defined and measured goals

Resiliency engineering differs from traditional approaches. It:

- Provides a way to align various business activities – such as security, business continuity, and IT operations – so they all help the organization meet its strategic goals
- Takes a proactive, enterprise-level approach to what previously might have been a tactical area
- Gives you a degree of control over the **outcome** of any threat scenario (even unexpected ones) – you can't control the threat environment, but you can mitigate against the potential impact of even unknown threats

An Engineering Analogy

An analogy from classical engineering may be helpful. If you want to build a bridge, you need to coordinate many different project aspects: requirements, funding, disparate skill sets. The objective is achieved in a **multidisciplinary** way.

Managing operational resiliency requires the same type of multidisciplinary, systematic approach. Tasks must be performed under the constraints of:

- Changing requirements
- Limited funding
- Regulatory demands

- Accounting and budgeting rules

In addition, many roles and perspectives must interact to accomplish tasks.

For such a complex process to succeed at an enterprise-wide level, security must be built into the fabric of the organization. This means:

- Security-related processes are designed in the context of the organization's requirements.
- Security is owned across the organization.
- The organizational culture is risk-aware.

Beyond Securing Assets

Building on this enterprise-wide perspective, resiliency engineering goes beyond the traditional security approach of securing assets. Instead, it takes a services view. This is a building-block approach in which:

- Each organization has core services that it performs or provides as part of its business mission.
- Each core service is supported by (sometimes many) business processes.
- Assets underlie those business processes. Assets include people, information, technology, and facilities.

The argument is that **for true business resiliency – for core, mission-critical services to be made resilient – the business processes also need to be made resilient, as well as the assets**.

PART 2: APPLYING THE MODEL TO OPERATIONS

Setting up an Example

How would resiliency engineering help a company if something were to happen – say, if a customer database were attacked?

First: If the company has resiliency engineering in place, it likely already will have invested in asset security based on the assets' value to the business.

Specifically, assets will be protected in terms of their value to various business processes and, ultimately, the core services provided or performed by the business.

In other words, assets have been evaluated in the context of what they do for the business, and secured commensurate with their value.

A Proactive Approach for a Positive Outcome

This means: adequate protection and sustainability already will be in place for the customer database. If it is vital to the services provided by the business, it will be protected to such a degree that it may not be compromised even if it is attacked.

One end goal of this proactive approach is to meet compliance requirements not by throwing money at them, but rather as a byproduct of overall operational resiliency.

In a nutshell: With resiliency engineering, security is funded not because an incident has occurred (reactive), but instead because certain assets, business processes, and services were deemed important to the business (proactive).

PART 3: RESILIENCY AND RISK

A Tool to Manage Operational Risk

How do resiliency engineering and risk management tie together?

Executives already have tools to manage credit risk, finance risk, market risk, etc.

However, they have fewer tools to manage operational risk.

Resiliency engineering is not a silver-bullet operational risk management method, but it does help a great deal in three major areas of operational risk:

- Security
- Business continuity
- IT operations

Recognizing When Resiliency Engineering Is Working

What might resiliency engineering look like in practice?

The key is active management and control. You would see:

- Smooth-running security and business continuity processes
- Proactive efforts to prevent outages, data breaches, data loss, and other disruptions
- Fast, effective response to manage impacts if incidents do occur

Good resiliency engineering also can lead to cost avoidance in the form of **fewer but more effective** controls for compliance.

This is a natural result of combining some traditionally stove-piped efforts such as security, business continuity, and IT operations.

Evolution over Time

This realization that these traditionally stove-piped disciplines had significant overlap emerged organically.

Originally, the Financial Services Technology Consortium, which has participated with CERT in building this resiliency engineering framework, wanted a maturity model for business continuity that could be used to benchmark suppliers.

However, as work progressed, it became clear that business continuity was inextricably tied to security and IT operations as well.

Resources

Caralli, Richard A.; Stevens, James F.; Wallen, Charles M.; White, David W.; Wilson, William R.; and Lisa R. Young. "Introducing the CERT Resiliency Engineering Framework: Improving the Security and Sustainability Processes." Software Engineering Institute, Carnegie Mellon University, May 2007.
http://www.sei.cmu.edu/library/abstracts/reports/07tr009.cfm

CERT Resiliency Engineering portal