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

An Alternative to Risk Management for Information and Software Security

Key Message: Standards, compliance, and process are more effective than risk management for ensuring an adequate level of information and software security.

Executive Summary

Assessing, analyzing, and mitigating risk are considered effective means for managing information and software security. Security literature is filled with a wide range of methods, techniques, and tools for conducting security risk assessments and acting on their outcomes. That said, as a community, we've made little progress in moving from qualitative to quantitative risk management.

In this podcast, Brian Chess, Founder and Chief Scientist at Fortify Software, discusses why the concept of risk is a poor foundation for tackling software security and assurance, a view which runs counter to popular wisdom. Brian will present an alternative approach drawing from what has worked well in other disciplines: standards, compliance, and process.

PART 1: WHY RISK MANAGEMENT IS A POOR FOUNDATION FOR SECURITY

The Utility of a Risk Management Approach

Risk management allows us to tame something that is essentially unpredictable and that we cannot control (those who seek to do us harm).

Nothing can ever be 100% secure so risk management aids in addressing these types of conditions.

Security professionals use risk management to make their efforts relevant to business leaders. If they can translate security problems into risk management problems, they can demonstrate financial consequences and grab business leaders' attention.

Where Risk Management Breaks Down

Brian heard a reputable CISO present his highly quantitative approach to risk management-focused security based on, in part:

- assets to protect
- threats against assets
- vulnerabilities requiring compensating controls
- defense-in-depth
- attacks blocked by firewalls and anti-spam systems.

The speaker concluded with "this is why we're adequately secure."

Brian questioned the assumptions made given the high rate of constant fluctuation in assets, threats, attacks, and vulnerabilities.

One of the key problems with assessing and addressing individual risks is that most risks are interdependent and cannot be successfully mitigated in isolation, let alone quantified.

As a result organizations must make numerous estimations, many of which may be wrong.

Quantitative versus Qualitative

The math works well when you can be quite precise about things such as the value of assets or the probability of a successful attack. But such precision is not possible in practice.

In the face of this, most approaches revert to high, medium, low or some other type of relative ranking for risks. This creates new problems such as “does a high trump four lows, or four lows plus a medium?”

This challenges the perceived strength that security problems can be converted into business problems.

PART 2: LEARNING FROM OTHER DISCIPLINES: STANDARDS, COMPLIANCE, AND PROCESS

Examining What Others Do

Brian started asking the questions “How do other people build systems? And how do they account for what they don’t know for sure?”

Construction is one example. How do they prepare for low probability, high impact events?

Approaches include building codes and fire codes. A fire marshal uses a fire code to determine if a building is fire safe based on historical lessons learned. Meeting a fire code does not mean that the building will not burn down or that no one will be hurt by fire.

Standards and Compliance

From this examination, Brian formed a hypothesis that perhaps standards and compliance are more effective than risk, given that we really don’t know asset values and the threats against them.

However, building codes and fire codes are for physical, tangible assets while systems and software are intangible. So does this argument work given that we really don’t know how to measure security for software in the same way we do for buildings?

Another Analogy – Food Safety

How do we know whether or not it is safe to eat in a particular restaurant? Customers cannot measure all of the food that comes out of its kitchen.

What is the essence of our public health system when it comes to food safety?

While it may not be initially apparent, protecting food served in restaurants does have parallels to security:

- Restaurants are constantly under attack from diseases in their global food supply
- Food-born diseases are adaptive

The Importance of Process

Restaurants make sure that their food is as safe as possible by following and measuring well-defined processes.

This is analogous to developing software using well-defined processes that are constantly measured and improved.

Arguing the Case Against the (Mis)Use of Risk

Another noted security expert, Donn Parker, argues that intangible risk reduction is a weak justification for security. He

states that the real tenets of strong security are due diligence, compliance, and enabling the business.

In his book, *The Black Swan*, Nassim Nicholas Taleb, a specialist in financial derivatives, writes about the effect of low probability, catastrophic events and how solid assumptions we all make can turn out not to hold.

Another example is the current worldwide economic crisis led by the decline in housing prices. Risk management doesn't help us deal with these types of events.

If you perform risk management by monitoring the historical attacks on your firewall, you will be focused on yesterday and will likely overlook a catastrophic or highly disruptive event.

PART 3: A CASE IN POINT; EXAMINE YOUR ENVIRONMENT

The Payment Card Industry Data Security Standard

When it comes to standards, compliance, and process, there are many sources to consult – sometimes too many although there is much commonality among them.

Brian cites PCI DSS as a big success based on his experience with Fortify customers. He believes its success comes from keeping its scope small and manageable: "We want to talk about software that handles credit card numbers."

Because PCI is a requirement that credit card providers impose on their merchants, it creates a market-driven incentive to comply.

This has been a boon for security staff because they don't have to sell the business relevance of PCI; it's a requirement if you handle credit card data and want to continue to do so.

Effective Risk Management

Risk management adds value where the math works; where you know all of the possible outcomes and can measure them. Examples include:

- establishing the rules for casino gaming payouts
- evaluating behavior over a large population such as all of the hosts connected to the Internet

Learn from Your Environment

Take a look around your immediate environment to learn how people are managing risk around you all of the time:

- Request a copy of an elevator inspection report for one of your office buildings. Understand the guidelines for making elevators safe.
- Spend time with a fire marshal or building inspector as they inspect your location. Find out about their checklists and how they work.
- Get a copy of your favorite restaurant's health inspection report.

Other Considerations

People, in general, are just not that good at the gut check form of risk management, as reflected in Daniel Gilbert's book Stumbling on Happiness. Gilbert asserts that people are not very good at predicting their own futures, including improbable events.