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

Business Resilience: A More Compelling Argument for Information Security

Key Message: A business resilience argument can bridge the communication gap that often exists between information security officers and business leaders.

Executive Summary

A language gap often separates information security officers and business leaders. Return on investment is one potential argument for bridging this gap in economic terms, but the numbers can be hard to pin down. Another argument involves business resilience, which is easily understood by both business leaders and information security officers as a vital part of the organization's ability to fulfill its business mission.

In this podcast, Scott Dynes, a senior research fellow at the Center for Digital Strategies within Dartmouth's Tuck School of Business, discusses how best to make the argument for business resiliency, why mutual education is key, and why the chances of bridging the communication gap in this way are good.

PART 1: BRIDGING THE BUSINESS-INFOSEC LANGUAGE GAP

Identifying the Language Gap

Among business leaders, various views of information security may exist:

- Information security is just a cost center.
- Information security is accepted a requirement of doing business, but it's not clear exactly *what* it is doing for the business.
- Information security is a core part of ensuring the business operates well and can achieve its goals.

In the case of the first view – that information security is just a cost center – what is the root of information security's image problem?

One problem may be a communication gap:

- The information security director is talking about security in IT terms rather than business terms, so the business leader does not understand security's importance.
- The business leader, meanwhile, is using terms that the information security director does not understand.

Why Speaking the Same Language Works

In contrast, at companies where business leaders and security managers communicate well, both parties understand the impact of information systems vulnerabilities on the core business processes that enable the business to achieve its goals.

In other words, they are both speaking the same language.

Financial services firms tend to be good at this, because most of the data they handle represents real money, so it's easy to make the connection as to why information security is important to the business.

Two Keys: Resilience and Reputation

In other fields, the relationship is not as clear.

Here's a real example: At an oil refinery, the information security manager wanted to increase the security of process control systems, but the vice president of refining didn't understand why doing so was important. He wanted to make better oil, period.

One argument that could have made a difference is a **business resilience** argument. Business leaders can identify with the need for business continuity (for example, having a redundant communication path to the distribution center), whereas an ROI argument might be less successful because the numbers are hard to pin down.

Another good argument is that an investment in security is an investment in reputation.

PART 2: THE IMPORTANCE OF MUTUAL EDUCATION

The Role of Education

Education is a core part of the solution – better than simply making a business resilience argument and hoping it works.

Here's a prime example continuing with the oil refinery.

The Dartmouth team worked with the information security manager and the vice president of refining, using a process called risk map to identify core business processes and then categorize the potential impact of losing each of those processes:

- Can the business still achieve a stated goal if business processes that support it fail?
- Is there a workaround?
- Does service degrade even if there is a workaround?

It turns out that each business process depends on information flows to work, so they mapped those, too.

Lastly, the team mapped assets (such as physical IT devices or networks) to each information flow.

The end result was a clear picture of where the greatest risk to the business was when IT assets were impacted. And this enabled the vice president of refining to see why investing in securing process control systems would increase business resilience, allowing him to make more oil (the core business).

Education Is a Two-Way Street

In the example above, rather than talking about bits and bytes, the team was talking about impact to the business.

This form of education is two-way:

- Business leaders learn to understand how IT assets affect information flows, core business processes, and, in turn, the overall business mission.
- IT managers learn to understand the business processes and how they are enabled (or put at risk) by technology.

Increasingly, boards of directors are becoming interested in their organizations' information security, and this is a great motivator to drive security awareness throughout the organization.

Evolving toward Enlightened Security

Several approaches to information security exist:

- Sore-thumb approach: If a problem occurs, handle it and then defend against future occurrences of it
- Proactively protect devices and networks
- Proactively protect business processes

The last is the most enlightened approach.

In this situation, there isn't even a separate budget for information security; it's just part of the budget for implementing any given business process. This approach reduces overall cost and increases resiliency.

Evolution toward this approach is similar to the movement toward designing in quality, which occurred a couple of decades ago.

PART 3: MOTIVATING BUSINESS LEADERS TO TACKLE SECURITY PROACTIVELY

How Information Sharing Can Help

What has gone right in those organizations that view security as part of the business process?

- Agility and open-mindedness may play a role.
- Or, a security incident such as a virus or crash can jolt an organization into awareness and change.
- One way to spark change without a disaster happening beforehand is for businesses to share information with each other.

Sharing information about security incidents can be difficult, because organizations may fear that their rivals will gain a competitive advantage by using any information provided (for example, to badmouth the organization that revealed information).

Anonymous information sharing might be one solution.

The data breach notification laws passed by many U.S. states since 2003 have helped. By mandating some level of breach disclosure, they created a market incentive for companies to do better in their security efforts.

Future Developments in the Security Landscape

In the future:

- Businesses likely will become:
  - Even more dependent on the information infrastructure
  - More integrated with each other
- The few businesses that still communicate with their supply chains via phone or fax probably will no longer do so.
- Business managers will have to become much more attuned to the information security landscape.
- Instead of protecting against specific vulnerabilities, business leaders will need to shift to protecting against unwanted outcomes – in other words, building business resilience.

Adapting to the New Environment

In this new environment, how can security managers better prepare to talk to business leaders?

1. Become very involved in the business. Specifically, place people as relationship managers within business units to learn what risks the organization is exposed to when using particular technologies
2. Based on that information, talk with business leaders about risks to and resiliency of existing business processes, and ensure that new business processes are managed effectively from a risk standpoint.

Resources

Center for Digital Strategies

CERT Resiliency Engineering portal