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

Real-World Security for Business Leaders

Key Message: Security is not an option – but it may be time to start viewing it as a business enabler, rather than just a cost of doing business.

Executive Summary

Businesses face increasing challenges from regulations that call for security controls but do not define exactly how those controls should be implemented. At the same time, the number and severity of threats are also on the rise. In this environment, security is a must-have. Fortunately, if approached correctly, it can serve as a business enabler rather than a drain on resources, even helping businesses achieve faster time-to-market in some cases.

In this podcast, Pam Fusco, former CISO for Citigroup and currently the executive director for security solutions at FishNet Security, discusses the top security challenges that business leaders face, especially in the financial services sector, and how to tackle them while building buy-in for security throughout the organization.

PART 1: TOP CHALLENGES AND THE EVOLVING SECURITY LANDSCAPE

Regulatory Drivers

One of the top information security challenges currently facing business leaders in the financial services sector involves regulatory requirements, especially those related to protecting personally identifiable information (PII).

Business leaders need to understand:

- The regulation
- Interpretation of the regulation (translating guidelines in the regulation into the reality of the business world)
- Implementation of the regulation (via technology, processes, procedures, policies, and governance)

Once implementation is complete, another task related to regulatory requirements is the need to abide by and manage oversight of implemented policies dealing with the requirements. This can be done by using a scorecard, for example.

The regulatory landscape changes frequently. One driver is California's Senate Bill 1386 privacy law, which has led to similar laws in other states and ultimately may result in a federal law.

Another top challenge for business leaders is communicating the rationale behind security requirements through initiatives like training and education.

An Attention-Balancing Act

How do you channel your attention appropriately to deal with various threats? Determine:

- Your likelihood of being affected by the threat
- The severity of the threat including how deep it could invade your network and systems

Keep in mind that the threat landscape is changing, with an evolution from relatively mild viruses like "I Love You" and simple denial-of-service attacks to more complex and severe threats.

For example, a virus today may be far stealthier and also may include a backdoor, trojan horse, or logic bomb.

Meanwhile, botnets have increased the potential severity of denial-of-service and other types of attacks.

As threats have evolved, so has people's understanding of the risks involved. Why is this?

- Risk is more widespread
- There are more threats than there were before
- Regulatory requirements are driving increased understanding

---

PART 2: PUTTING SECURITY INTO PRACTICE

Establish Pathways for Human Input

What are some effective approaches for putting in place an information security program and ensuring it remains viable?

1. Pull together an internal consortium of stakeholders from across the organization that meets periodically (once per month, quarter, etc.). Why? It gives people a chance to:
    - Vet ideas
    - Understand the extent to which security is IT-driven or business-driven within the organization
    - Feel that they have a say (and a stake) in the organization's security initiatives
2. Establish a policy steering committee and reach out across the organization with requests for comment on upcoming policies. Why?
    - It gives people insight into new policies.
    - It increases awareness of those new policies.
    - It provides an opportunity for leaders to say, "You knew this was coming. Don't turn a blind eye to it."
    - It gives people an opportunity to have input.

Overall, the keys are:

- Communication
- Coordination
- Collaboration

In contrast, trying to force a piece of technology or software down the pipeline often simply doesn't work. It's better to build buy-in internally.

Selling Security to the Highest Levels

When presenting security topics to senior management and boards of directors, marry information security and risk management (issues) with business initiatives (opportunities) because:

- It sets a precedent
- You are more likely to get buy-in
- It helps you learn from the past and build toward the future
- It adds the elements of strategy and innovation

Some statistics you can bring to boards of directors include:

- What the organization has done and done well with regard to security (from policy, governance, and operational perspectives)
- What you now want to put in place that will drive the business mission and objectives, and why these measures will be business drivers
- How security measures may enhance time-to-market

ROI can be difficult to calculate but some positive return can be demonstrated by demonstrating compliance with leading standards and regulations and highlighting incidents that affected other organizations but did not affect yours.

Working with the Reality of Trade-Offs

One harsh truth: You'll never have enough resources to do everything you want to do. So, trade-offs are inevitable.

One way to manage this is to build flexibility into plans.

For example, if you have a three-year plan, and you pull out the middle piece, does the whole plan crumble, or can you continue to move forward with the remaining pieces of the plan?

When making trade-offs, always understand what you're giving up and what the impact of doing that is.

- Know your priority for each of the elements of any given plan.
- Set reasonable expectations.
- Be willing to adopt a phased or staggered implementation approach
- Communicate the risk that remains based on what you're NOT doing

You also may be able to shift different portions of a security initiative to different departments, for funding reasons. For example, you may be able to shift a compliance portion of a security initiative to the legal department or risk department.

PART 3: SECURITY AS BUSINESS ENABLER

Security Is Just a Business Process

What are some first steps a business leader can take to develop an information security plan?

- Ascertain the organization's current state of security
- Lend your support to the information security plan (tone from the top)

It makes sense to support security, because security can actually reduce your time-to-market.

In one case, one pharmaceutical beat another to market by 30 days because it had better security in place (such as virtual private networks) and could communicate and share data more quickly, efficiently, and with assurance of integrity with its subsidiaries.

As a result of being 30 days earlier to market, it had a market advantage with that drug for the next 10 years over the pharmaceutical company that was second to market.

That is a business case for security.

Security has evolved into a true profession, with certifications, accreditations, reliability, accountability, and so on. If done right, it can be truly integrated with operations and systems as opposed to tacked on after the fact.

However, large organizations do face some special concerns when deploying security initiatives:

- Make sure you have buy-in across the board from a majority of people.
- Use a task-driven, phased approach.
- Keep communicating about successes so the security program benefits stay at the forefront of people's minds. And be candid about failures and get well plans.
- Stay on top of the project and don't let it slip through the cracks after two or three years.

Resources

Carnegie Mellon University's CERT

Carnegie Mellon University's CyLab

International Information Systems Security Certification Consortium (ISC2)

Information Systems Security Association (ISSA)
