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

Dual Perspectives: A CIO's and CISO's Take on Security

Key Message: Given that you can't secure everything, managing security risk to a "commercially reasonable degree" can lead to the best possible solution.

Executive Summary

Launching or strengthening an enterprise security program can seem a daunting task. Funds are always limited, so it is impossible and impractical for an organization to secure every system or piece of data at the optimal level. In such an environment, what are the roles of the CIO and CISO, and what can these executives do to manage security risks in an acceptable way?

In this podcast, Motorola CIO Patty Morrison and CISO Bill Boni share their experiences in their respective roles and offer advice for listeners who are faced with building a security program or strengthening their current one.

PART 1: ROLES, RESPONSIBILITIES, AND REPORTING

Three CIO Challenges

At Motorola, three challenges facing the CIO, who is responsible for infrastructure and applications worldwide, include:

1. Keeping a worldwide organization rowing in the same direction at all times, through constant communication of strategy and plans.
2. Supporting the business through strategic direction setting and helping to solve immediate business issues and challenges.
3. Prioritization and portfolio management

Why the latter?

- CIO responsibilities include keeping up with constant changes in business environment, customer demands, and need for improvement in earnings and gross margins.
- In most cases, this requires support from the IT organization, and demand for IT services always exceeds supply in monetary terms.

Security is very high on the CIO’s radar screen, in terms of participating in steering committees and evangelizing security to corporate officers.

The CISO’s Role

Compared with the CIO’s role of raising awareness and providing resources, the CISO’s role is to

- identify and direct attention to security investments that will allow the company to achieve its strategic goals with the minimum amount of acceptable risk
- develop business context, road maps, timelines, and priorities for each initiative

The CIO then can take this information, at a broader level, to internal and external executives, managers, and other stakeholders.

Avoiding Conflicts of Interest

Are there possible conflicts of interest when the CISO reports to the CIO?

To avoid such conflicts, it’s vital to be clear about roles. Even if reporting to the CIO, the CISO must **maintain independence and objectivity**.

For example, at Motorola, the CISO works closely with internal audit, legal, and loss prevention departments on efforts that the CIO does not necessarily need to know about.

Essential fundamentals include trust, leadership quality, and building a partnership.

For the CISO, reporting to a senior leader who is engaged, articulate, and understands information and its value to the organization provides opportunity and leverage.

PART 2: SELLING SECURITY AND PINPOINTING ACCEPTABLE RISK

Evangelizing Security

Effective strategies to position security in the organization include:

- Developing a vision and then discussing potential security investments in the context of that vision.
- Using real-world incidents as opportunities to educate about the importance of security investments.
- Managing risk as a portfolio, and making clear to management the consequences of a choice to manage or to accept each given set of risks.

Benchmarking Acceptable Risk

How do you determine acceptable levels of risk? How much security is enough?

One solution is to focus on achieving a **commercially reasonable degree of security**, based on what comparable organizations have done. This is a good indicator that you're exercising due diligence.

And one good way to benchmark your performance against your peers' is to have a relationship with those peers or with trusted third-party organizations.

Working with Limited Resources

How do you choose among potential security investments?

One answer: Understand the total picture of what needs to be accomplished. Attain this understanding through strategy planning sessions and developing an operating plan.

At Motorola, the goal is to protect a constant level of investment in security – “Here’s the amount that we need to invest year over year” – a specified "run-rate," if you will, instead of having security viewed as a one-time investment.

Security as Business Process

Also, keep in mind that security doesn’t have to be an isolated discipline.

For example, the CISO can help business leaders understand how security investments will enable work that the business leaders want to accomplish.

Compliance and auditing departments are a possible source of organizational support as well, in terms of identifying risks and pushing for funding to mitigate those risks.

One good strategy is to treat security investment decisions like any other business investment.

Mapping It Out

As such, a multi-year road map of estimated investments can help. If you plan for eventualities and something happens earlier than anticipated, a plan for dealing with it already exists, so you can say, “This risk has manifested sooner than we expected, so this is how we’re going to control it going forward.”

Conversely, funding may need to slow down, not accelerate. A road map can be useful in this circumstance, as a guide to keeping planned future investments front and center. Trade-offs are made as part of the portfolio management process.

PART 3: ROLE-BASED ADVICE

Enterprise Roles for Security

What roles are most essential to the success of a security program? It’s not just IT!

At Motorola, a cross-functional team exists with representatives from HR, legal, finance, audit, and marketing. This allows the CIO and CISO to gain sponsorship and engagement from various divisions, so that funding for potential security investments is easier to obtain.

The CISO's information protection team uses a service model focused on:

- Planning
- Overall road map
- Architecture and its supporting framework
- Ensuring compliance with standards and controls identified for various applications, environments, platforms, and so on

The team is organized around:

- Governance
- Data protection and privacy
- Enterprise resiliency, business continuity, and disaster recovery
- Security solutions engineering
- Risk management (including measuring the organization's degree of compliance)

Sharing Expertise

What advice is there for CIOs and CISOs who are:

- Trying to get their security program off the ground?
- Struggling to have security viewed like any other business process?

Some strategies include:

- Utilize available resources that can help you assess your situation and develop a road map

- Lay out a vision and strategy for the next two to three years
- Build a case for each step along the way, and incrementally fund your way to the end state

No matter how long it takes, **make security a priority**. It is vital for business success.

Security as Business Partnership

Also, keep in mind:

- You can't do a security program to an organization or *for* an organization, only *with* an organization.
- The more the management team understands and accepts accountability for risks, the more their commitment to security will improve. Therefore, security professionals must engage in outreach and communication – speaking in business language to the business leadership about security and the consequences of its absence.

The Commercially Reasonable Test

How do you answer the question, "Are we secure?"

Focus on what is commercially reasonable.

Security professionals may want all possible risks mitigated with all possible controls in all possible places. That is not practical. Instead, ask yourself: "Have we done what's responsible under the circumstances?"

To answer that question, find out if what you have done is equivalent to what comparable organizations have done. More specifically:

- Do benchmarking
- Participate in Carnegie Mellon University's CyLab or other similar organizations
- Get reference documentation for best practices
- Map control frameworks and risk areas
- Make the business case

Once you have a road map, you know where to go – even if it takes you a while.

Final Advice

The field is constantly changing – threats, technology, unexpected accidents – so leaders, security, and IT staff need to keep learning and keep on their toes.

Resources

Carnegie Mellon University's CyLab