Redefining Security Leadership in a Riskier World

Security and risk management today represent a key strategic concern for many companies. Without adequate planning and risk management, companies leave themselves vulnerable to intellectual property theft, fraud, physical or Internet-based attacks — and potentially crippling business disruptions or reputational damage.

As threats have become more sophisticated, so too have companies' strategies for mitigating security risks. Organizations are looking closely at their potential risks and asking tough questions about their preparedness: What could threaten the viability of the company? How prepared are we to avoid those risks? What are our business continuity plans should one of those threats comes to pass?

Security and risk management also have become much more complex. As a result, many organizations have concluded that they need to improve coordination and collaboration between the previously separate sectors of security, including information technology security, physical security, fraud and non-financial risk management, to effectively manage the wide range of risks facing their organizations.

To learn more, Spencer Stuart consultants spoke with senior security and information security leaders about how their organizations approach the security function and the skills required for security executives today.

SpencerStuart

COORDINATION ACROSS THE SECURITY FUNCTIONS

More and more companies see the benefit of increasing the coordination among risk management, IT security and physical security, both in reducing risks to the organization and streamlining policies and procedures. For these reasons, Equifax undertook a three-year strategic plan to align non-financial risk and security programs and projects, said Tony Spinelli, chief security officer of Equifax. "When it was three separate groups — physical security, IT security, and fraud investigation and compliance, each of those groups had an organization that did risk assessments. Physical security would go out and, for example, do risk assessments of our Latin American data centers, so would IT security and the fraud group. We'd be hitting the business three times, with three times the cost."

While Equifax has taken the approach of consolidating non-financial security functions under a single leader and consolidated strategic plan, other companies promote coordination in other ways. Ally Financial (formerly GMAC), for example, has an executive risk committee, into which leaders of different security disciplines informally report. "Due to our scale, we do not have one person who has overall responsibility for all security. Instead, we have put together a governance model that brings together multiple domains, including IT-type security, which I represent, physical security, corporate risk management, privacy and internal audit," said Debbie Wheeler, chief information security officer for Ally Financial. "We work very closely together and the common thread if you look across all of those entities is the identification and management of risk, whether you're talking about physically protecting assets or logically protecting assets, we all have the same sort of role."

More and more companies see the benefit of increasing the coordination among risk management, IT security and physical security, both in reducing risks to the organization and streamlining policies and procedures.

Genworth Financial moved to enhance the coordination of its security and risk functions when it went public in 2004. "We knew that, as a stand-alone company, the name of the business was going to be more visible than it had been in the past — so we anticipated increased exposure to potential fraud. We also needed our security approach to incorporate what we saw as a growing interdependence between physical security and cyber-security," said Scott McKay, the company's chief information officer and senior vice president of operations and quality. Led by a security strategist, the company embarked on a multi-year initiative to develop a new security framework and improve interaction among the security functions. With that framework in place, the company no longer has a single leader overseeing all of security. Instead, the

chief technology officer, the facilities leader and operations controller report to a risk committee that has an integrated view of the whole range of risk issues.

Security leaders said no single security framework or organizational structure will work for every organization. When deciding how to structure security within their companies, leaders should look at considerations such as the size and complexity of the organization, the potential financial or operational efficiencies to be gained by integrating security functions, the organizational structure and culture and the nature of the business and its primary security risks. "The important thing is to understand how your organization functions, where it wants to go and, fundamentally, how things get done, both formally and informally," said Andre Gold, former chief information security officer for MoneyGram International who is now with AutoTrader.com.

"The IT security strategy has to come from the business strategy. A CSO could come in and lock down all the assets in the name of security, but that doesn't work well for the business."

Furthermore, the security strategy must be shaped by the business strategy, and have the support and buy-in from the CEO and, in some cases, the board of directors. "The IT security strategy has to come from the business strategy. A CSO could come in and lock down all the assets in the name of security, but that doesn't work well for the business," said Eric Litt, chief information security officer for General Motors.

The approach Spinelli took to forging a common understanding of the security priorities when he started in the role was to meet with the CEO and Equifax board to define the appropriate level of security for the company. "The first thing I did in my 90-day plan was ask our senior leadership team what they wanted security to be. Should we benchmark our security against financial services firms? Should it be fully ISO-compliant? Do we want to have a world-class security organization? It's very important for the security leader to separate decision making from execution and be measured in a way that everyone agrees to," said Spinelli. "The senior leadership team, including the CEO, should collaborate to support the goals and aspirations on the level of security, but once they make that decision, the execution is my job."

Finally, security has to be an organization-wide concern because even the most comprehensive security policies and strongest security team won't be effective without an informed and alert workforce, executives said. "The weakest link can be your people," said Litt. "All of your employees are a potential threat; all of your employees also are a potential ally in protecting the assets of the corporation. So the CSO's focus cannot just be on deploying new processes, it also has to be on the people side to secure the environment."

Wheeler agreed: "Driving awareness about security is 90 percent of the battle. Nothing is more effective or more powerful than an educated workforce that understands the value of the information they have access to, the need to protect it and the willingness to do so. The tools and the processes you wrap around that really should be there just to catch the exceptions."

REDEFINING SECURITY LEADERSHIP

What does it take to be an effective security leader? While the exact role requirements depend on an organization's specific situation, several core skills have emerged as critical to a security leader's success. An effective security leader will be a strategic thinker, knowledgeable about IT and physical security issues, as well as the business. He or she will have superior communications skills and be able to make decisions quickly based on the available information, whether in day-to-day operations or in crisis situations. It's assumed that the information security leader has both the technical and tactical/operational skills to do the job. Strategic and business acumen will distinguish the successful security leaders.

Security leaders must have the broad-based knowledge and skills to develop a strategic vision, communicate the vision and sell it effectively to people across the organization and at all levels. This requires the nurturing of key partnerships at all these levels and building a robust network of relationships.

"It's helpful to have a broad and diversified background. I never set out to become a security expert, but I enjoyed solving complex problems. Having worked in an operational environment, understanding the limits of what one can do operationally, and having worked across multiple organizations all have been very helpful to me," said Litt.

Excellent communication skills also are critical for security leaders. "You have to be able to convert what you're seeing from a security perspective into the business context of the organization and talk about how that impacts P&L, the ability to enter new markets and other core business initiatives," said Gold. The CSO/CISO must be credible. He or she must be capable of objectively recognizing and communicating the risks, consequences and mitigations, but be mature enough to accept that business leaders' risk/reward calculations may differ — and sometimes decisions may not go his or her way.

Opinions have shifted about the degree of technical experience that is required for senior security leaders. While most executives we interviewed agreed that it may not be necessary to be an engineer or to have spent one's entire career in IT, a good understanding of IT networks and systems is important, particularly as an increasing percentage of most businesses relies on technology. "I've seen the role swing in a couple

of different directions over the past 10 years. Early on, the mindset was that you needed a very technical individual as your security leader. But this can be a drawback if the individual has a difficult time communicating risk issues to the business. Then the pendulum swung all the way back to having lawyers or other leaders without a technical background fill the role. That wasn't successful either, because they didn't speak the language of the technology teams and, therefore, didn't have the knowledge to ask the appropriate questions of their teams," said Wheeler. "I think you really need something in the middle. You have to combine strong technical background with strong business acumen and excellent communication skills."

REQUIRED TRAITS FOR A CHIEF SECURITY OFFICER

- Diversified and broad background
- Problem-solving skills
- Analytical
- Exposure to operations
- Strong network of relationships
- Understanding of how things get done in the organization, work, both formally and informally
- Effective communication skills

Analytical skills are growing in importance for security leaders, as security is expected to develop relevant metrics that not only track activity but also quantify the impact of security initiatives on the financial performance of the business. "A CSO must drive a process that formulates relevant metrics that measure impact, not just output or work flow volumes, and the value proposition that security provides must be translated into profit-and-loss terms," said Christopher E. Swecker, former chief security officer for Bank of America Corporation. "These measurements could include incident preventions/reductions, fraud avoidance, recovery of dollars lost to crimes or fraud, elimination of costly false alarm fines and so on. For example, how much is a fraud prevention worth in losses avoided, investigative time saved and loss reserves freed up? What are the savings associated with a 10 percent reduction in laptop thefts or employee malfeasance because you screened effectively on the front end before hiring the employee with a bad history? The CSO must stay on this message and always have an elevator speech ready to show the value of security to the business when dealing with the 'c-suite' executives."

Other skills and domain expertise required for the senior security leader will depend on the organization's risk profile, culture, reporting structure and the sophistication of its current security profile. A banking system, for example, looks for candidates with experience dealing with money laundering and other financial crimes, while the physical security of plants and pipelines is paramount for a variety of manufacturing and distribution companies, requiring a completely different security executive profile, possibly a law enforcement background.

As one executive told us, "Security is a journey." As long as there is money to be made by being able to compromise assets, there will be people looking for ways to go around whatever controls an organization puts in place. No company or security leader will be able to predict all vulnerabilities on the horizon, but will have to be prepared to deal with whatever new vulnerabilities arise. This will require a security strategy and approach that:

Is driven by the business strategy
Has the support and sponsorship of the CEO, senior leadership team and board of directors
Recognizes that security needs to be part of everybody's job
Effectively coordinates the full range of security and risk management activities

ABOUT SPENCER STUART

Spencer Stuart is one of the world's leading executive search consulting firms. Privately held since 1956, Spencer Stuart applies its extensive knowledge of industries, functions and talent to advise select clients — ranging from major multinationals to emerging companies to nonprofit organizations — and address their leadership requirements. Through 51 offices in 27 countries and a broad range of practice groups, Spencer Stuart consultants focus on senior-level executive search, board director appointments, succession planning and in-depth senior executive management assessments. For more information on Spencer Stuart, please visit www.spencerstuart.com.

THE INFORMATION OFFICER PRACTICE

Formed in response to the rising demand for world-class information technology leadership, Spencer Stuart's fully integrated global Information Officer Practice was the first of its kind. As the market leader in chief information officer searches, we conduct key information technology assignments for Fortune and FTSE companies across all industries.

Our global team of experienced consultants are recognized technology experts and have a comprehensive overview of and unmatched access to the world's leading IT talent. As a result, Spencer Stuart conducts close to 200 senior-level information officer searches annually. In addition to recruiting CIOs, we provide concentrated expertise across the following information technology functions:

- Applications Development
- Architecture
- E-Commerce
- Infrastructure
- Program Management
- Security

North America Practice Leader
Carl Gilchrist
cgilchrist@spencerstuart.com
+1 404.504.4442

EMEA Practice Leader
Olof Pripp
opripp@spencerstuart.com
+44 (0)20.7298.3540