Security at Center Stage

The Evolving Role of the Chief Security Officer— and **5 Secrets** to CSO Success

EXECUTIVE SUMMARY:

As security takes center stage in enterprises around the globe, the role of Chief Security Officer (CSO) has evolved from that of a corporate cop to a business enabler and security champion, assuming greater visibility, authority and responsibility with each passing success. It takes a new breed of security officer to take the helm. Read on to discover the five secrets to CSO success.

Remember the days in the not-so-distant past when the CSO operated mainly as a corporate cop or a compliance tactician? Well, a lot has changed in a short period of time.

Today's CSO has evolved into a strategic player with significant clout as a business champion – from the data center to the boardroom. And this evolution is only continuing.

"Security is no longer an afterthought, nor is the role of the security officer," says Bill Danigelis, president of the Information Systems Security Association (ISSA), Silicon Valley Chapter. "Today, both are front and center for very good reason."

CSO Custom Publishing

Cisco Systems

As security leaders inevitably assume greater visibility and authority, organizations must cultivate CSOs that are able to keep pace with the expanding responsibilities and growth.

The CSO Role Emerges Out of Necessity

So how has the role of CSO evolved?

Obviously, the sheer size and scope of modern businesses has contributed to the basic need for security. Even the smallest companies have expanded beyond traditional physical boundaries to create virtual businesses and transact globally at astounding speeds.

"With that growth, more and more companies became completely dependent on technology and the availability of their IT infrastructures to conduct business," says Brad Boston, senior vice pres-

ident and CIO at Cisco Systems. "And strong security defenses were required to make that availability a reality." Thus, the role of the CSO was born—a corporate cop tasked with policing access to IT resources.

Then, security and privacy legislation gained momentum. What once were merely mandates for government agencies quickly became strict guidelines for the public sector—the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley (GLB), to name but a few. So the CSO took on more of an oversight role.

"Any organization with state or federal regulations around protection schemes absolutely must have a security officer," says Felix Santos, CISO for Performant Financial, based in Livermore, Calif. Unfortunately, the CSO often became a mere compliance tactician or, worse, was served up as a "sacrificial lamb" in the event of a security breach.

Perhaps the greatest trigger in the evolution of the CSO role lies in the budding alignment between security and business objectives. Security is no longer just about patrolling the halls and slapping wrists. Rather, it is about enabling business – securely "webifying" and automating business applications so organizations can transact and compete at amazing new levels. Today's CSO is someone who can make all that happen, while balancing technical defense requirements with business value and scrutinizing any business move that jeopardizes security.

With so much riding on the function, a small team buried in the IT department simply isn't enough. Security demands an executive voice with the appropriate degrees of insight and muscle behind it.

Thus, the CSO role has emerged to the forefront of business, says Danigelis, "necessarily rising through the ranks with visibility at the board and CEO levels."

Five Secrets to CSO Success Unlocked

When it comes to finding or cultivating a CSO to fit this newly expanded role, Cisco's Brad Boston says he found the right stuff in John Stewart. Boston points to the following mix of attributes, which he says contribute to Stewart's noteworthy success:

1 More Than the Average Techie. A senior security officer isn't going to be the traditional "techie," but rather a well-rounded individual with a strong technical aptitude who surrounds himself with a team of specialists that can fill in the gaps with expertise in specific areas. Of course, this individual must be grounded in asset protection and information systems. But he must also have "a firm grasp of legal implications, knowledge of the compliance landscape and the ability to implement appropriate controls to mitigate risk," says Santos. A CSO needs to understand the business goals, keep current with technology and leverage the IT specialists. "The CSO must maintain breadth and depth in his knowledge of technologies, and understand how all the technologies and defenses relate to each other," says Boston. Perhaps most important, a CSO must be able to effectively communicate highly technical concepts to business-oriented audiences.

2 Focus on Business. A CSO's repertoire can't start and end with technology. "A successful CSO will also possess strong business acumen," says Boston. This new breed of CSO – and his team – is heavy on skills that one might attribute to a more "general" business role. In a recent survey by *CSO* Magazine, "The Role and Influence of the CSO," 60 percent of the nearly 500 CSO respondents rated communication skills as the number one requirement for success in the CSO role. Other important skills cited include strategic thinking/planning (44 percent), leadership (38 percent), understand-

"SECURITY is no longer an AFTERTHOUGHT, nor is the role of the security officer."

—Bill Danigelis, president, Information Systems Security Association (ISSA), Silicon Valley Chapter

Q&A: Hiring the Right CSO

We asked Brad Boston, Cisco SVP and CIO, for his insight into hiring the right CSO. Here's what he had to say.

Q: What are the primary responsibilities of a CSO?
A: As a leader in the risk management process, the CSO and his team are tasked with evaluating a threat, calculating the probability of said threat occurring, and communicating its potential effect on business. Then, it's the business manager's responsibility to determine if it's an acceptable risk. CSOs can't be "Dr. No"—this results in a narrow perspective and a helplessness to effect change. Fortunately, John Stewart looked at security differently when he was appointed to the role of CSO at Cisco. His philosophy: "If you want to enjoy the corporate network, then these are the rules to help me protect it." He and his team set the rules, but with flexibility—ultimately enabling [rather than inhibiting] business operations.

Q: How does a company decide when it's time to hire a CSO?
A: You know it's time to hire a CSO when you fully realize that much of your business relies on technology. Many of us are already at that point—meaning organizations in today's virtual economy are deeply dependent on the availability of the IT infrastructure for day-to-day operations. That infrastructure can't be accessible without proper security controls, so you need a CSO to ensure business continuity and to defend your organization against emerging threats.

Q: What are your thoughts on the evolution of the CSO role —the "up-leveling" of security to a C-level position?
A: I'm a very strong advocate of up-leveling the security role to a C-level position. Because security is so important to maintaining a successful business, the security officer must assume the visibility, authority and responsibility of a senior-level role. The CSO appointment—in and of itself—validates the importance of security. Security is a company-wide responsibility, but it's hard to get that message out while it's buried in the IT organization. At Cisco, John Stewart has become a true evangelist for security, raising awareness in the boardroom, across the company and throughout the industry. With this kind of momentum in the industry, we will likely see the CSO role evolve quickly to even greater heights.

Q: What are the qualities to look for in a CSO? And how did you know that John Stewart was right for the job at Cisco?
A: Any CSO candidate needs a working knowledge of technology combined with sound business judgment. When it comes to threats and their defenses, the CSO not only needs the book smarts but also the battle experience to back it up. John Stewart bubbled to the top of our list because , in addition to his experience, he is extremely passionate about security and has strong communication skills. He has the unique ability to translate technical messages for the not-so-technically versed. John also demonstrates a keen grasp of our business and understands the importance of involving business managers in decision making. He's changed Cisco's whole perspective on security.

Q: How do you create a competent CSO?
A: Today, we're facing a shortage of security talent, so we need to cultivate the right mix of attributes in our people—both as an organization and as an industry. It's in all of our best interests to create competent security professionals so we can continue to deal with threats as they develop. That's why Cisco likes to share our experiences with others by participating in various industry forums. Cisco additionally invests in schools with security curriculums by donating equipment and resources that aid in the education of security professionals. Our ultimate goal is to help grow the new security generation.

ing of business processes (35 percent), and ability to influence (27 percent). Interestingly, knowledge of security and understanding of IT both come in at 18 percent. This list certainly paints a very different picture of the ideal CSO than one might have imagined even a few years ago.

3 Relationship Builder. Today's CSO isn't going to be chained the data center. In addition to building and motivating his own team of pros, he's going to be out on the front line. A successful CSO will spend a great deal of his time developing relationships and cultivating security champions to carry his message throughout the organization. In evidence, *CSO* Magazine asked respondents to rate such relationships. Obviously, direct reports (95 percent),

IT (92 percent) and IT executives (91 percent) rank high. But so do other groups including CEO/president (89 percent), line of business (86 percent), users (83 percent), CFO (81 percent), legal (76 percent) and board of directors (74 percent). This kind of interaction requires finesse on the part of the CSO. "The most successful CSO will know how to tailor his message and will adapt his style to specific audiences," says Boston, whether it's senior executives, line-of-business managers, techies or even users.

4 An Eye Toward Pervasive Security. "Security is much more successful when it starts at the top," says Danigelis. "That is, when the CEO is practicing it and living it." This commitment is communicated down the ranks by example. Still, the CSO must build the team, implement the processes and deploy the technologies that can help individuals make their own contributions to security. "It's everyone's responsibility to maintain security, because we all represent potential points of vulnerability," says Boston, which could be as simple as a weak password, an unattended laptop or an unlocked filing cabinet. Indeed, there are creative techniques to effect change. Boston says Cisco introduced a full-scale Corporate Security Programs Organization (CSPO) whose mission is to drive and reinforce behavioral change, thereby creating a pervasive security culture. The team evangelizes security through awareness training, internal promotions, cascading e-mail campaigns from the business executives to their teams, and weekly voicemails to senior executives. CSPO even uses a semi-annual Security Champion Awards system, whereby individuals who have gone above and beyond the call of duty are rewarded for their security efforts.

5 Dual Reporting Structure. The reporting structure for the security officer is often a topic of hot debate, with IT on one side and executive management on the other. The *CSO* Magazine survey respondents nearly split down the middle, with 59 percent reporting directly to security/IT management and 41 percent reporting to executive management. But the best-case reporting scenario, says Boston, is a combination of the two—that is, a direct link to the CEO and a pragmatic connection to operations. "When reporting solely to IT, all of a CSO's time could be consumed by operational issues," he explains. On the other extreme, reporting directly to the CEO doesn't work either, because there is always an opportunity to overturn security guidelines in favor of the bottom line. "A dual reporting structure is necessary to maintain independence," says Boston. "It's much like the auditing function," with its own set of checks and balances.

"That said, a CSO is still only as good as the team he builds," adds Boston. "A successful CSO will surround himself with great people – specialists within the team and champions throughout the company – that can round out the security function, execute on its implementation and enforcement, and evangelize its importance."

The Security Community Comes Together

As the CSO role continues to evolve, every security professional has a strong responsibility to the security community as a whole. Boston sees this as a win for everyone. "If the CSO is not out talking about security with others in the industry, he may become too narrow-minded when it comes to emerging threats and their defenses," he says. Boston is also quick to point out that "shared best practices in security serve us all very well, and our communal defense can only be improved through collaboration."

At Cisco, CSO John Stewart is an active spokesperson for the company, participating in organizations like ISSA. "He is able to use his hard-earned war stories to illustrate what could happen without proper defenses… and, of course, what can be done to defend against threats," explains Boston. "With folks like John out there paving the way, security talent just keeps getting better." ■