Corporate Security Career > Career Development >

Why the CSO is the Hardest Job in the Company – Part I

Created by the Security Executive Council

Being a Chief Security Officer has never been easy, but in recent years external and organizational changes have combined to make the CSO role much more complex.

External Challenges

Threats are coming after businesses from more directions and in more consequential ways.

1. We may once have believed that only government agencies were at risk of international espionage. Not so today. **Nation states are boldly and increasingly targeting private industry,** stealing intellectual property from commercial organizations and academic institutions. Individuals from China, Russia, and Iran have been indicted for such activities against U.S. businesses and entities. Cybercrime is the means we see most publicized in recent years, but that doesn't mean the ends aren't being carried out in other ways. Human intelligence is still the cheapest way to compromise an individual or company, but the near-exclusive emphasis on cyber security makes other types of protections a harder sell to management.

2. **Social activists** use social media to increase their bandwidth with supporters, quickly drawing unprecedented numbers of participants in protests and other activities that could impact security at company sites. One SEC client was targeted by activists who arranged protests at 500 different company sites across the globe on a single day.

3. Because of the **digitization of business,** access to one site potentially opens up access to the entire company. We need to rethink where we are vulnerable. Are all sites secured with equal diligence? What about partner or contract organizations that have access to company information? The FBI has reported instances of Chinese operatives targeting U.S. law firms with little or no security to access client information. The need to partner here—with the CISO, supply chain partners, and other functions—is critical.

4. **Social media gives angry customers a powerful weapon to inflict brand damage.** For example, last year United Airlines stock dropped $1.4 billion within 24 hours after a video began circulating of a UA passenger being dragged screaming off of an overbooked flight. Had security adopted and trained employees on a better protocol and procedure for managing unruly passengers, would this incident have been as damaging as it was for the brand?

Organizational Challenges

The structure of companies has changed, as has their reach and the nature of doing business in a connected world.

a. **Organizations are more complex.** More companies do business worldwide, sometimes with their own competitors. For example, a company's joint-venture manufacturing agreement in China may open up a new sales market, but it may also open the door to intellectual property theft.

b. Underinformed management often prioritizes the **security incident of the moment**—the one that gets the most news coverage—over legitimate and assessed threats against their specific organization. When executive demand and support shifts like this, CSOs are pulled constantly in new directions while security operational risk is routinely under considered.

c. **Many companies are simply not ready to accept or implement advanced security strategies**—whether because they still think of security as only "guns, gates and guards" or because they undervalue or misunderstand risk management. They may demand mitigation for certain high-profile threats but withhold support for necessary but time-consuming security basics, such as an enterprise security risk assessment. Recent Security Executive Council research has found that 23-24% of Fortune 500 companies don't even have a readily identifiable head of security. (For more about program maturity and what the SEC calls "organizational readiness for security," visit https://www.securityexecutivecouncil.com/spotlight/?sid=31210)

d. Organizations are exploring different **service delivery models**, which changes the effectiveness and structure of security programs. Many companies outsource elements of security; some maintain only a single security leader to write policy and contracts and outsource all the rest; and some rely primarily on business units to manage their own security services internally. The goal is to keep headcount to a minimum to save money, but these strategies often end up costing more and impeding the CSO's ability to identify threats and vulnerabilities to manage risk.

e. **Security solutions often require the knowledge and action of employees.** Access control doesn't work if employees allow "piggybacking". Workplace violence prevention programs don't work if employees don't report aggressive behavior. Network security is compromised if employees don't recognize and delete or report phishing emails. The security function must be adept at mobilizing the entire organization, not just its staff or department heads.

f. Because of the increase in threat vectors and organizational complexity, **every business function is involved in risk management now, but they may not know it.** A cooperative corporate culture or an existing framework for regular interdepartmental communication would make it easier for a security leader to remedy this—but many companies lack both.

g. **CSOs have little upward mobility within an organization.** Because of this, if they wish to advance their skills or their career, their most likely choice is to move to another company.

How to Succeed in the Hardest Job

Given these challenges, how is one to succeed in the CSO role? We have seen many security leaders find success by pursuing some or all of the following.

a. **Balance security knowhow with business knowhow.** CSOs come from a variety of backgrounds, and where they come from often determines which problem-solving tools they favor. Businesspeople may turn to administrative solutions, and former police or military may turn to criminal justice solutions—but in neither case is the favored tool alone enough to solve the problem. Seek out training or mentors who can help you learn the other side.

b. **Change the executive perception.** It's up to you to show them the value-adding potential of a well-designed and supported security program. Most executives know a lot about business risk, but many know little about the management of security risk. They may not realize the potential damage of security-related operational risk. They may think money solves security incidents, when in reality it can only reduce the odds of an event. Learn to evaluate other executives' perceptions of risk and security and learn to communicate your value story in a way that resonates with them.

c. **Develop an executive presence.** This goes hand in hand with changing the executive perception. The security leader's communications throughout the company should be clear, pointed, and professional. Develop your public speaking and presentation skills. Learn to speak the language of the business.

d. **Be a team player.** Executive management will prize your enthusiasm and aptitude for being a team player. So much of security – and good business – now requires active partnerships with other executives and functions that you can't very well succeed without this. Initiate regular communication with other business leaders. Learn their functions and seek out ways in which security can help them do their jobs more effectively. They can be your eyes and ears across the organization, and working with them can help you reduce redundancies and find opportunities to consolidate efforts.

Security Executive Council research has shown that the CSO who excels in today's complex environment is one who can incorporate elements from six areas of knowledge into his or her job performance: executive leadership, business knowledge, IT/information security, organizational knowledge, skills common to military and law enforcement, and emerging issue awareness. (For more, visit https://www.securityexecutivecouncil.com/spotlight/?sid=30239). The future is today. All of these elements impact the CSO's success. What will you do to develop them?

Be on the lookout for Part II on this topic, where we share the stories of security leaders who have pursued these tactics to their benefit and the benefit of their organizations.

Visit the Security Executive Council website for other resources in the Corporate Security Career: Career Development series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more**.**

Contact us at: contact@secleader.com

Website: https://www.securityexecutivecouncil.com/