Demonstrating Value > Building Influence >

The New Challenges of the CSO

By the Security Executive Council

The Chief Security Officer role has adopted new complexities in the face of seismic shifts in risk and business over the last few years. As organizations continue to define their new normal, CSOs will be challenged to re-examine their priorities and strategies for protecting people and assets in this new environment.

COVID-19

Businesses and communities continue to manage the reverberating impacts of the global pandemic.

The workplace has been redefined. While most employers have returned to at least a partially in-person workplace, telework and hybrid work are here to stay for many. A McKinsey survey of 278 executives in August 2020 found that respondents expected to reduce office space by 30 percent on average as they adopt more flexible and hybrid workspaces. Continuing to protect employees and secure company-issued devices as well as sensitive information and intellectual property in a hybrid environment will be an ongoing challenge for many CSOs.

In many organizations, the role of the security function expanded significantly. Symptom tracking, mask enforcement, expanded operations center functions such as COVID reporting and helplines, device delivery and retrieval to and from at-home employees, expanded intelligence tracking to advise on the closing and re-opening of facility sites – CSOs saw some or all of these come under their purview.

The Great Resignation

Millions lost jobs or were furloughed during COVID closures in 2020, and 4 million Americans quit their jobs in 2021. The recovery has lagged as workers transition to new fields, reconsider their options, and hold out for higher pay and better benefits.

For the CSO, this presents a twofold challenge. First, it’s harder to find strong team members.

There is more competition for qualified positions, and there are fewer takers for lower-wage jobs such as some contract security personnel.

Second, with increased job transition comes increased risk of information theft and fraud. Departing employees may take data with them, unwittingly or intentionally. The value of intellectual property may be seen as a bargaining chip in a new job search. And employees who are planning to leave are more likely to engage in theft and fraud before they make their exit.

Catastrophic Weather Events

The 2020 World Disaster Report by the International Federation of Red Cross and Red Crescent Societies found that extreme weather events have been increasing since the 1960s, and the increase has sped up since the 1990s. The UN Food and Agriculture Organization states that natural disasters are now happening three times more often than they were 50 years ago. The damage and cost of these events has increased as well. According to Munich RE, storms, floods, wildfires and earthquakes destroyed assets worth $280 billion in 2021 – over $100 billion more than in 2019 – and U.S. locations accounted for a high share of that loss. All of this emphasizes the criticality of the CSO's role in crisis management and business continuity.

Nation-state Attacks

According to a study by cyber security researchers at HP and criminologists at the University of Surrey, the number of Nation-state cyberattacks against businesses has risen since 2017, and a third of attacks from 2017-2020 targeted businesses. These findings are not exclusive to any given sector or size of business, though pharmaceutical companies did see more campaigns seeking to gain access to COVID-19 vaccine research. Digitization, distributed business models, and international business partnerships complicate this threat further.

CSOs with responsibility for cyber security must certainly recognize and deal with this threat, but CSOs whose role is predominantly corporate security must also examine their mitigation processes to ensure that attempts to steal intellectual property aren't also coming via physical access or human intelligence.

Social Activism

The 2020 Black Lives Matter protests constituted the largest protest movement in U.S. history and an unprecedented amount of property damage, but it wasn't the beginning of the trend. The Institute for Economics & Peace's 2020 Global Peace Index found that civil unrest had already doubled over the decade preceding 2020, and the Center of Strategic and International Studies found that the number of mass protests globally has increased by 11.5% per year, on average, since 2009.

The protests of 2020 also weren't the end. As this article is being written, the Ambassador Bridge between the United States and Canada is being reopened after being blocked for 7 days by Canadian anti-vaccine protesters, which cost about a billion Canadian dollars and harmed Canada's reputation as a reliable trading partner.

Strategies to Consider

There will be no one-size-fits-all solution to any of the risk issues presented by these new challenges. But as CSO grapple with them in their own organizations, with an eye to their available resources and corporate culture, here are a few recommendations that may be broadly helpful.

Consider new technologies. During the pandemic, many companies embraced speed, flexibility, and agility as the way forward. Continued increases in the use of artificial intelligence technology reflect that focus. Look for ways to leverage these trends for the good of the organization through the security function. (One place to start is our Digital Transformation Primer.) Now may be a good time to propose new or enhanced investments in intelligence resources for faster, better risk decision making.

Similarly, if your GSOC played a significant and successful role in pandemic response, look for ways to enhance its capability in ways that can present new opportunities for the business. For more information see our article GSOC: Business Drivers and Service Scope.

In light of increased fraud risk, upper management may also be more receptive to proactive insider threat mitigation techniques. For more on these, see the summary of our Security State of the Industry webinar on How Proactive Investigations Can Boost the Bottom Line.

Prioritize internal collaboration. A 2020 SEC poll found that in general, collaboration between corporate and cyber security had increased from the year prior. Hopefully that will serve as a foundation to look for new ways to partner with cyber security or information security to help secure sensitive data in a hybrid environment, and to protect information against insider risk.

Partnering with HR is a good idea as well as both functions work to better serve and validate employees in the new workplace.

The CSO can also look to other functions as he or she works to maximize the value of existing staff, given the hiring challenges of the Great Resignation. Working closely with other leaders can help pinpoint force multipliers and opportunities to use existing staff to address joint concerns.

Build and maintain community relationships. Focus on business continuity and crisis management planning. Reach out to shore up internal and public-private partnerships, update plans, engage in training, and set up tabletop exercises. Look at all the possibilities, from weather disasters to mass protests, and engage in positive relationship building among the people of your local community. For more, check out a recent faculty blog on collaborating to reduce the impact of activist events.

Visit the Security Executive Council web site to view more resources in the Demonstrating Value: Building Influence 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/