SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Leadership > Security as a Business >

What Does the Board and Senior Management Need to Know About Corporate Security?

The Evolution Has Started

By Kathleen Kotwica, EVP and Chief Knowledge Strategist, Security Executive Council

The Security Executive Council's subject matter experts, most former CSOs, have hundreds of collective years of experience in corporate security. They both brought value to their businesses through corporate security and raised corporate security to a level of high value in their organizations. Some presented to the Board of Directors; others influenced senior management, who then brought some issues to the Board. But many CSOs don't gain the traction they need to rise to that level of attention.

Why does corporate security frequently garner less attention from Boards and senior management than cyber security? A lot of it comes down to money – a severe information breach can cost a company much more than a single physical security event. But many small losses do add up. In its 2020 Report to the Nations, the ACFE estimates that organizations lose 5% of revenue to internal fraud each year, and fraud prevention and detection represents only one aspect of what corporate security is involved in.

Corporate security is about much more than protecting an organization from unauthorized physical access, and this may not be clear to some Boards and senior managers. We'd like to let senior management and the Board know a little more about the advantages of a high-functioning security organization and what it can bring to a company.

We asked our subject matter experts to share some lesser-known benefits of corporate security and some examples of ways in which corporate security can evolve (and has evolved, in many instances) beyond the typical expectations for the function. This list may be helpful to senior management who want to engage the Board's attention for the corporate security group, especially if they can also show how loss avoidance due to risk controls equals savings. It may also be helpful to CSOs who want to evolve their functions to an attention-getting level.

- Corporate security actively supports enterprise risk management strategy and helps the business meet its risk management agenda. Security can help shore up dangerous and costly vulnerabilities that, unmitigated, can come back to haunt the organization.
- Security is flexible and eager to meet the demands of the business.
- Security knows the importance of working as a team with other functions.
- Security partners with internal and external stakeholders after an incident to determine what lessons can be learned that can be applied to the next crisis. They advise on what tools and resources they are missing to properly plan, prepare and manage the next crisis.
- Security can meet the needs of the organization regarding emerging issues intelligence.
- Security can provide effective crisis plans that are founded on thoughtful creative planning, rigorous testing, and the ability to act swiftly and decisively when faced with limited and changing facts. They rely on solid communications tactics and strategies that reach all their internal and external stakeholders in a timely manner and well ahead of traditional and social media.
- Security monitors and mitigates across incidents from many domains, such as pandemics, climate change impacts, supply chain fragility, social unrest, workplace violence, travel safety, and labor shortage.
- More and more security organizations are increasing the bench strength of the security team with people who have non-security backgrounds, such as data analysts and technologists. A team with diverse skill sets can improve security's value and service offerings.
- Due to recent events, many security organizations have invested in frictionless access controls and security systems that integrate with other business unit platforms, such as visitor systems tied to pre-employment background investigation files for identifying red flag entries, and access controls that interface with HR systems for tracking building occupancy and attendance.
- Security is generally good at fact gathering and communicating in a crisis, and there is some movement to provide actionable intelligence to "see around corners." Security is well versed in how intelligence works, how to use it, and where to get it.

- Security operations centers (SOC or GSOCs) are becoming 24x7x365 in some companies, and corporate security is running them in a way that is ROI capable and significantly quantifiable. They have discovered new ways to use SOCs that can positively impact the organization in areas outside security's traditional purview, including quality control, HR, logistics, and more.
- Security is evolving to a more precise idea of all-hazards risk. Many are distributing responsibilities across their internal network.
- Some advanced Security teams are working on proactive loss recovery, which will save the company money.

Many thanks to the contributors to this article: George Campbell, SEC Emeritus Faculty; Francis D'Addario, SEC Emeritus Faculty; Bob Hayes, SEC Managing Director; and Dan Sauvageau, SEC Emeritus Faculty.

Click here for more information on what makes the SEC different.

Visit the Security Executive Council web site to view more resources in the Security Leadership : Security as a Business 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/

