

Corporate Security Career > Career Development >

What Is Corporate Security?

Introduction

Businesses today operate within a more complex, sophisticated, and interconnected competitive universe than they did 20 or even 10 years ago. Success in this environment requires organizations to take smart risks – to expand into new territories, invest in innovations, and develop new partnerships. The corporate security function plays a critical role in enabling smart risk taking by providing risk intelligence and assuring the safety and security of the organization’s physical assets, people, and operations in every venture.

What This Guide Will Do

- Define corporate security as a function
- Describe the risks corporate security can manage
- Examine the value it can contribute to the organization
- Identify program options and common roles and responsibilities

What Is Corporate Security?

The corporate security function uses people, processes, and technology to protect the organization from negative events and situations. Corporate security identifies, monitors, and deters internal and external threats to an organization’s personnel, property, and assets and manages physical crises when they occur. It also assesses risks to the organization, communicates them to executives and management, and manages them appropriately.

It’s not uncommon for some of the corporate security function’s responsibilities to be shared with other departments. For instance, while risks to digital information and assets fall under the

corporate security umbrella in some organizations, they are frequently managed by separate but related cybersecurity or information security functions within a corporation. Similarly, while business continuity and resilience frequently fall under corporate security, they may in some organizations exist apart from, but in partnership with, the corporate security function.

Why Do Businesses Need Corporate Security?

In a global economy in which threats have become increasingly multifaceted and complex, corporate security is a critical function of business. Corporate security practitioners are skilled in employing technology, staff, and processes to deter and respond to the manifold hazards that put businesses at risk.

Corporate security monitors and mitigates risk across incidents from many domains. While the specific activities of corporate security will differ depending on the needs of the company, here are a few examples of the types of risks corporate security can manage.

Risks to people. Employees and executives require and deserve safe and secure workspaces. Corporate security can work with Human Resources to provide training and services that anticipate and deter incidents of workplace violence and can deploy staff and technology to keep unauthorized individuals off the corporate campus. They can develop mitigation controls for hazards of all types – from natural disasters to demonstrations and riots – and implement communication networks for employees and first responders. If such incidents do occur, corporate security can maintain communication with employees and staff to direct emergency response. Corporate security can provide personnel protection services, keeping at-risk employees safe at work, on the road, and often at home as well.

Risks to property and assets. Threats to company assets come in many forms and from many angles. Corporate security can employ loss prevention technology and processes to deter theft of assets from outside and inside the organization. They can monitor for and anticipate threats to valuable intellectual property as well. Corporate security can protect brick-and-mortar locations such as offices and manufacturing sites from malicious damage. They may also secure product and materials throughout the supply chain.

Risks to continuity. Corporate security keeps the business going when the unexpected occurs. They create, practice, and revise crisis management plans to ensure that there are redundant services available if something goes wrong. Corporate security runs regional or global operations centers from which they can monitor and respond to incidents, gather intelligence, and communicate with stakeholders. Security works with internal and external partners, including governments and emergency services, after an incident to determine what lessons can be learned and applied to the next crisis.

Other business risks. Corporate security often conducts risk assessments and risk analyses to understand the risks that could most impact business strategy and operations. From the results, security can develop the appropriate mitigation strategies. The documentation of policies and procedures that corporate security creates can protect businesses from litigation, and the function’s intelligence capabilities can help in mitigating reputational risk to the organization as well.

It's important to note that while it is corporate security’s role to identify risks and present the business with risk mitigation options, senior management and business unit leaders own the risk.

How Does Corporate Security Contribute to Business Value?

Corporate security enables businesses to do their business. It responds to changes in the company’s willingness to take risks, informs executives of the potential impact of risks, and ensures that higher-risk activities can be taken with as much security as possible by incorporating multiple layers of protection.

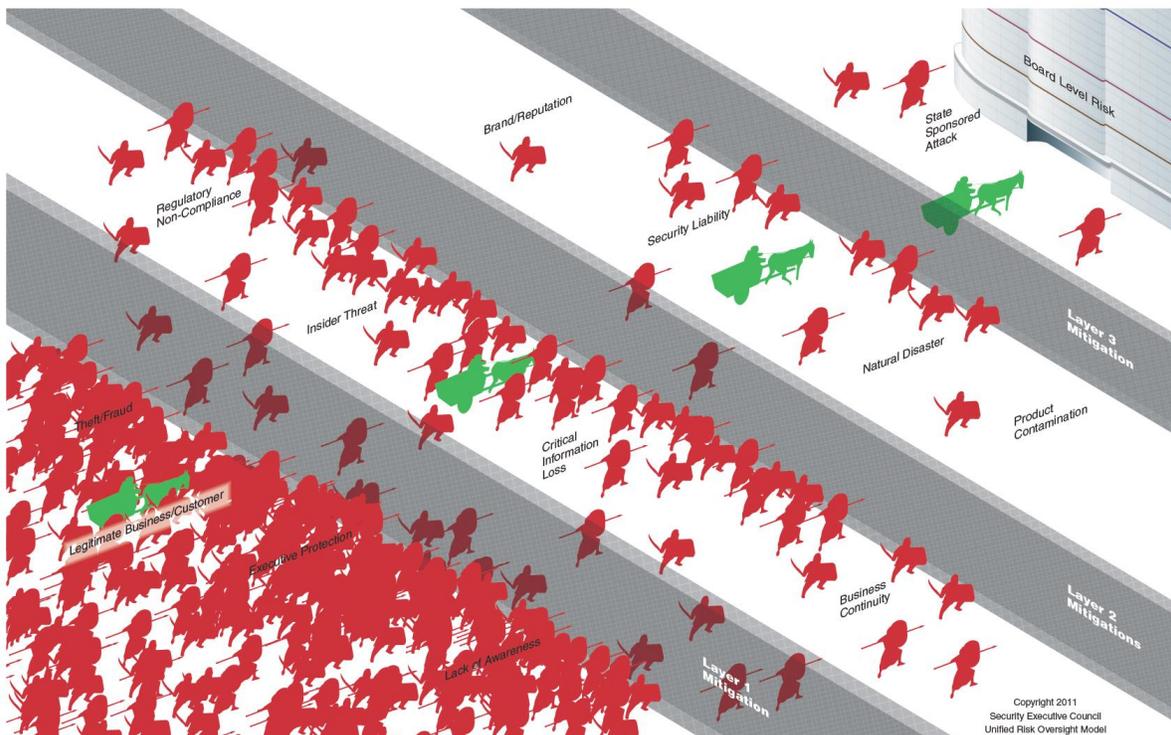
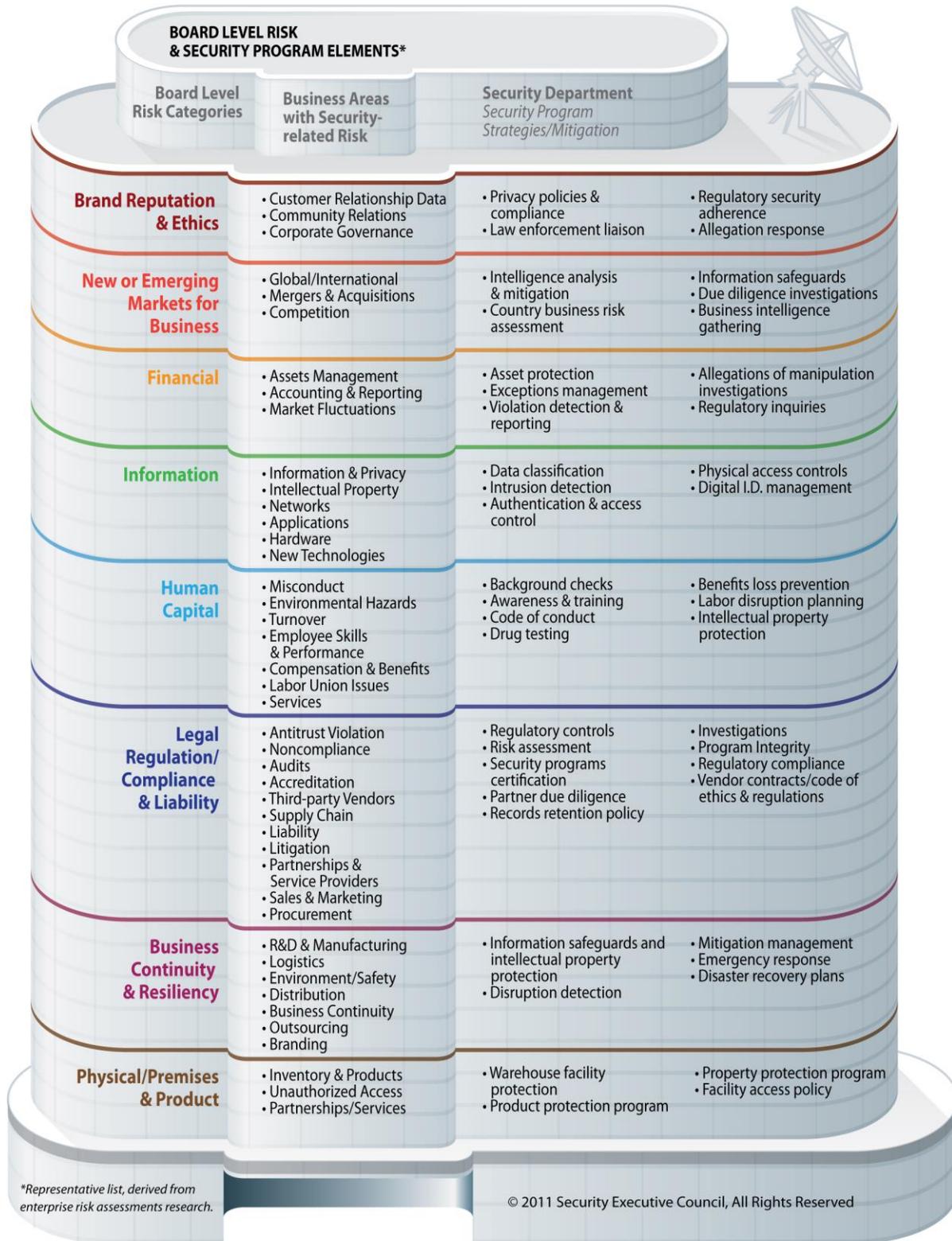


Figure 1: Each layer of security stops a large percentage of threats (or attackers). However, because businesses inevitably choose to accept some risk, residual risk will always exist.

The diagram below, based on Security Executive Council research, shows the many ways in which common corporate security programs and services interface with the broader categories of risk with which the corporate board is concerned.



In each of these board-level risk categories, corporate security can not only help the organization limit loss; it can contribute new value. Here are just a few examples.

- Corporate security investigations and due diligence can help the business reduce or prevent fraud and counterfeiting.
- In a time of high-profile, reputationally damaging security incidents, many companies have begun using strong corporate security as a differentiator in the competition for clients and customers.
- Proactive security programs can identify and deter threats before they can cause damage.
- Corporate security helps companies meet regulatory requirements, avoiding fees and fines.
- Corporate security's intelligence skills can help in assessing business transactions and vetting potential organizational partnerships.
- Many corporate security functions are running security operations centers in a way that can positively impact the organization in areas outside security's traditional purview, including quality control, HR, logistics, and more.
- Corporate security resilience programs allow companies to return to profitability quickly after a negative event.
- Corporate security technology may be used to assist other functions. For example, security cameras on a manufacturing floor may be configured to assist in quality control as well.

As several of these examples show, a strong collaborative relationship between corporate security and other functions will act as a force multiplier for organizational security and risk management and will maximize security's value contribution. Corporate security may participate in or spearhead a Unified Risk Oversight body that invites functions across the organization to share threat information and concerns as well as opportunities.

What Programs Does Corporate Security Oversee?

A corporate security function will determine which security programs to develop based on the risks that have been identified in a security risk assessment and the goals and priorities of the organization. However, there are a number of programs that are fairly common among corporate security functions across industries.

According to the Security Leadership Research Institute's 2021 Corporate Security Organizational Structure, Cost of Services and Staffing Benchmark, corporate security functions were most commonly accountable and responsible for the following programs and services:

- Asset Protection/Loss Prevention

- Awareness and Education
- Business Continuity/Resilience
- Emergency Response and Disaster Recovery
- Guard Service /Uniformed Officer
- Incident Reporting
- Investigations
- Law Enforcement Liaison
- Personnel Protection/Workplace Violence
- Physical Site Security Design and Systems Specifications
- Risk Assessments
- Security Related Regulations and Compliance Management
- Security/Business Command Center (GSOC)
- Travel Security

Other corporate security services may include:

- Event Security
- Executive Protection
- Intelligence
- Supply Chain Security
- Background Verification/Due Diligence/Pre-employment Screening

Note that not every corporate security function will have all of these programs.

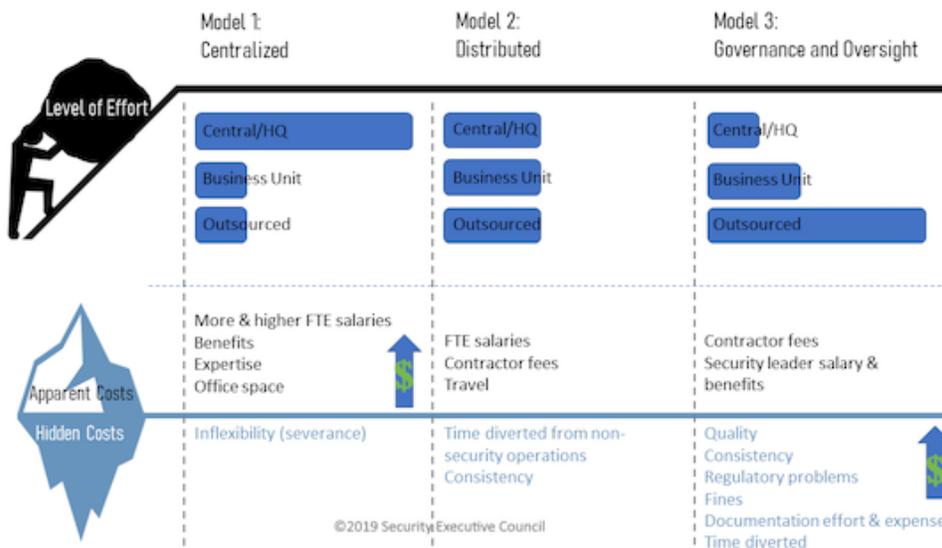
Where Does Corporate Security Fit Within the Organization?

Corporate security functions vary in size, structure, and placement within the organization.

There are three primary models of corporate security service delivery in organizations:

1. Centralized, in which security resides primarily in-house, with a large central staff and a corporate security leader over it.
2. Distributed, in which responsibility is spread out among central corporate security, business units and contractors. In some instances, the business units report to their local leadership with a dotted line to the senior corporate security leader, and in others they report directly to corporate security.
3. Governance and oversight, in which corporate security services are primarily outsourced and overseen by a single leader or minimal corporate security team.

Security Service Delivery Models



Apparent cost is only one factor in total cost of security.

Each model has a different impact on the following service level variables:

- Quality
- Consistency
- Regulatory compliance
- Documentation

The senior corporate security leader may have any one of a variety of titles: Chief Security Officer, Vice President of Security, Head of Global Security, or Director of Corporate Security, to name a few. He or she may report directly to the Chief Executive Officer or one or two levels below, and the reporting line may run through Corporate Security or Global Security or another department such as Finance, Facilities, Legal, Shared Services, Human Resources or Cyber Security.

Depending on the scope of the function and the service delivery model chosen, other corporate security team members may include a security director, security manager, regional security manager, site or business unit security manager, investigators, threat analysts, information security specialists, emergency preparedness manager, protective services and uniformed guard force staff.

Connect With Us

The SEC is the leading research and advisory firm focused on corporate security risk mitigation strategies and plans. We work with security leaders to transform security programs into more capable and valued centers of excellence.

[Contact us](#) to discuss how we can help your corporate security function become more effective and efficient.

Visit the Security Executive Council web site to view more 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/>