




IS IT TIME TO IMPLEMENT A CORPORATE SECURITY PROGRAM?



HILLCREST
ADVISORY GROUP, LLC



www.HillcrestAdvisoryGroup.com
973.699.1099

About the Author:

Chris Lowery is the Managing Director of Hillcrest Advisory Group and is an accomplished leader with over 30 years of experience in global corporate security and compliance. With over 20 years specializing in the pharmaceutical industry, Chris is both a strategic business partner and tactical expert in global threat assessment and risk mapping, investigations, product protection, compliance, crisis management, intellectual property protection, fraud (internal/external), executive protection, due diligence, and physical security protection.

The Hillcrest Advisory Group partners with organizations to provide strategic business support to identify risk, build corporate security programs, develop and implement enterprise wide security solutions and strategies to promote corporate asset protection and compliance.

BUSINESS VALUE OF CORPORATE

In today's complex business environment, a growing company without a business-aligned corporate security program is leaving itself vulnerable to risks which, if left untreated, could result in the loss of company assets, lapses in business continuity, interruption of business growth, increased liability, and damage to a company's reputation. Unfortunately, the critical decision to implement a corporate security program is often made *after* a compliance oversight or loss has occurred. Senior management has the responsibility and obligation to address all risks which will ensure the safety and well being of its assets.

Key Risk Categories

COMPANY ASSETS

- People
- Property
- Products
- Information
- Reputation

Corporate Security, as a valued member of a leadership team, plays a critical role in systematically identifying and mitigating risks that could negatively impact a business. The engagement of an effective corporate security program addresses two primary risk categories:

1. **Asset Protection** - A holistic, proactive, disciplined, cost effective and measurable approach to the protection of assets.
2. **Compliance Support** - The implementation, monitoring, support and enforcement of policies, programs and practices to ensure adherence to state, federal and international regulations.

In addition to the traditional asset protection programs associated with security, senior management must recognize that there are dozens of international, federal and local regulations that dictate how companies – large, small, and all sizes in between – must operate. Regulations require programs to implement internal controls, engage in monitoring and support enforcement. Not recognizing the full obligation of these regulations can ultimately result in governmental sanctions, heavy fines, loss of business privileges, lawsuits and even criminal charges.

Careful consideration must be given to these obligations and the potential impact that non-compliance can have on business growth, reputation and shareholder value. A systematic approach must be coordinated carefully to assure that risk and control processes operate as intended.

Board Level Risks Identified

In a 2011 study completed by *The Security Executive Council*, global CEOs were asked to rank the top risks they anticipate their companies will be challenged with in the coming year. This chart illustrates Board Level Risks that were most commonly identified as having the greatest material impact on organizations – all of which require support from the security function.

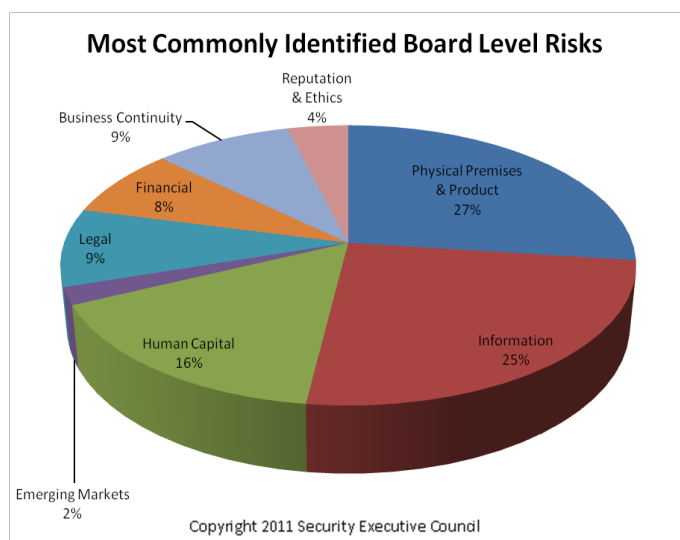


Figure A:

Corporate Security Sphere of Influence

A company's security risks will vary by industry, geography, size, business profile and many other factors. Some companies are more at risk than others; however, *no* company is completely immune to the loss of assets and compliance requirements.

The increasing number of threats to critical intellectual property, product integrity, fraudulent activity, theft, compliance standards, competitors, data and privacy demands, geopolitical unrest and the overall threat landscape of simply doing business are constantly evolving, forcing companies to realize the importance of security and the role it plays within a successful business.

Implementing a security program will prevent damage and loss of company assets. The choices made and subsequent actions (or lack thereof) regarding asset protection, business risk mitigation, security policies, and compliance can dramatically impact a company's bottom line.

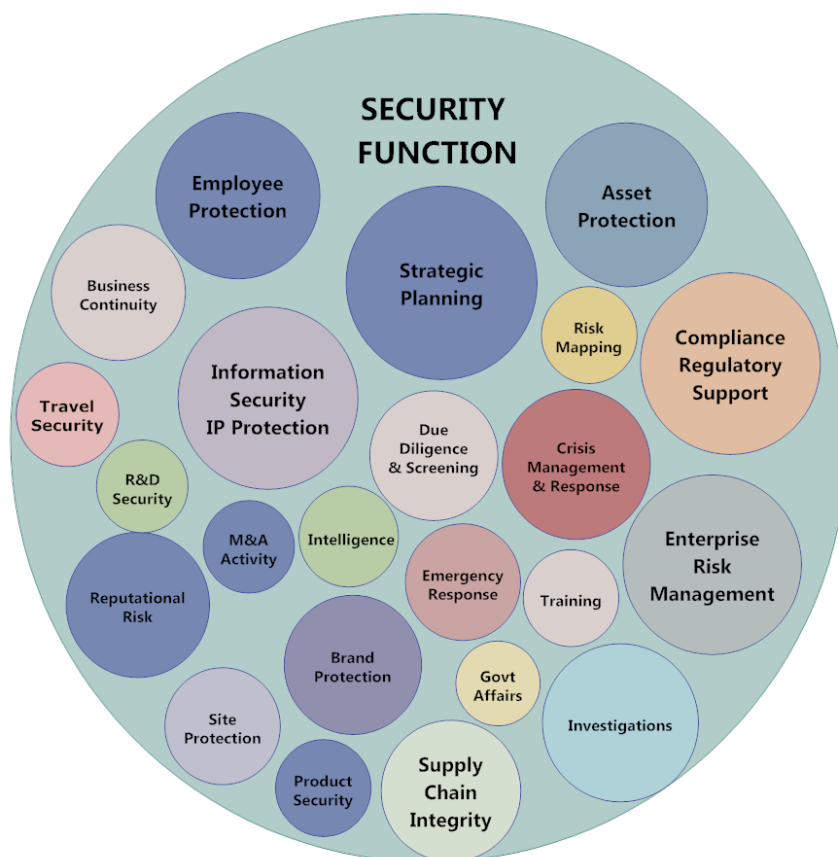


Figure B: Illustrates those areas in which a Corporate Security Program contributes. While direct ownership of each of these areas may not be appropriate for the business, Security plays a critical role in each of these areas.

The implementation of a Corporate Security Program will, at minimum, provide the following benefits:

- ⇒ **A proactive**, disciplined, visible and measurable approach to asset protection
- ⇒ **A consistent** method for identifying, ranking and addressing risks to assets
- ⇒ **Demonstrated compliance** with audit and regulatory requirements
- ⇒ **Improved resource utilization** and cost efficiencies by applying resources based on level of risk
- ⇒ **A central repository** of all security resources, risks, controls and policy related data

Program Implementation

The implementation of a *comprehensive* security program can be overwhelming, which is why a dedicated security executive, serving as a security Subject Matter Expert (SME), is paramount in properly aligning security strategy with the business. An effective security program is best accomplished through partnership across all functions and with board level support. This partnership and support will result in a uniquely tailored and unified business-based framework from which to assess risk, identify mitigation strategies, make sound business decisions, implement controls, and measure program effectiveness.

A typical implementation cycle of a holistic security program is an evolving process in which risks are identified and prioritized, options are presented with a cost benefit for each measure, and then approved by executive leadership.



Figure C: Illustrates the business aligned process of evaluating and implementing proposed security programs.

Senior Management's Obligation to Protect Assets



Senior management and the board of directors bear the direct responsibility and have the *obligation* to consider the “duty of care” of its employees and address all risks to promote the safety and well being of its assets. Companies that are unable to recognize these responsibilities and implement the appropriate steps to mitigate these risks have not heeded the warning of sound business practices. Failure to do so creates unnecessary risk to the business.

As companies grow, solutions to security issues are often implemented in a piecemeal fashion and handled by multiple business units. One of the worst decisions senior management can make is leaving security components and responsibilities divided amongst different functions, which almost always results in duplication of efforts, excess costs, ineffective and inconsistent measures, unidentified gaps and increased risks.

In addition, growing companies tend to focus most of their effort on increasing revenue, with little attention given to risk and protection of assets. In today's environment, risk is of *equal importance* to revenue growth and cost reductions. Simply put, the cost to the business to reactively respond to loss and/or compliance violations is far greater than the cost to proactively address these risks by implementing a corporate security program. The potential consequences are just too large to ignore.