Demonstrating Value > Communicating Value >

A Brief Introduction to the Value of Corporate Security for Non-Security Professionals

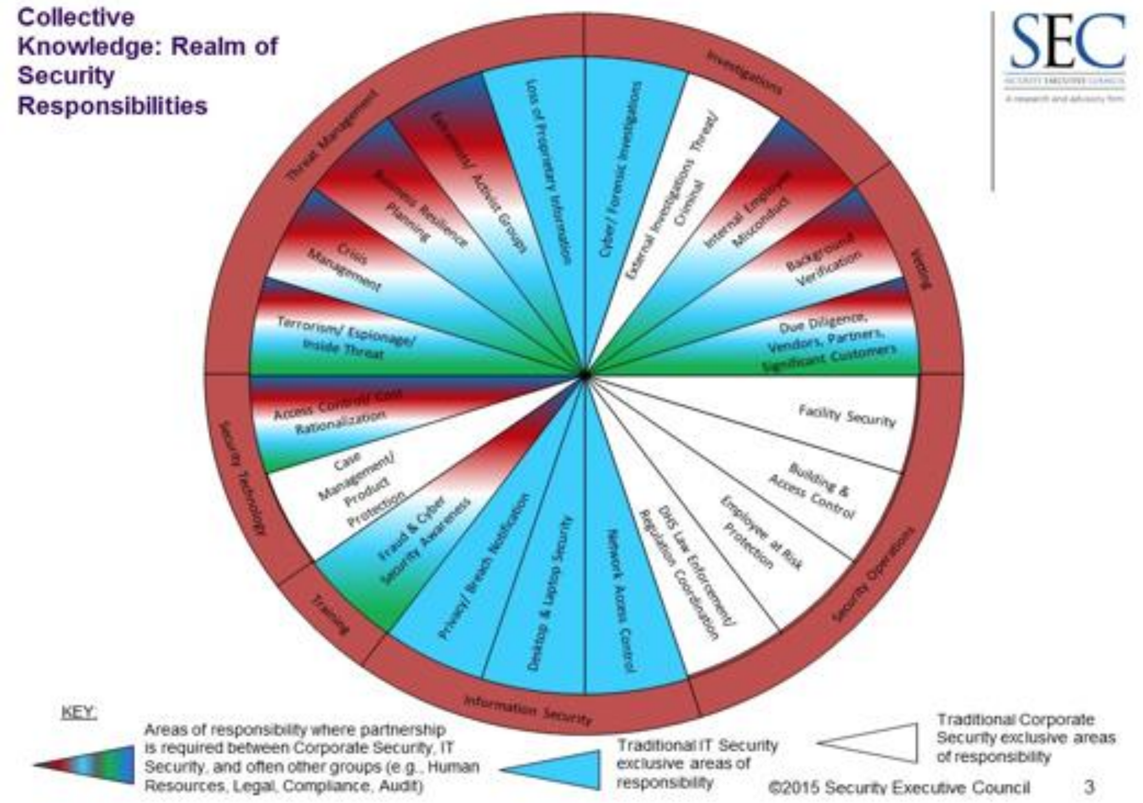
Created by Bob Hayes, Managing Director; and Kathleen Kotwica, Ph.D., EVP and Chief Knowledge Strategist, Security Executive Council

Have you ever wondered how companies prevent or respond to issues that could result in injured or killed employees, damaged or lost assets, law suits, regulatory fines, or loss of important corporate information? Most Fortune 500 companies have experienced these types of incidents, and many have established a corporate security department to minimize the impact and losses they bring.

Business activities that managers have overseen for years have recently become more complex and potentially damaging. Examples include:

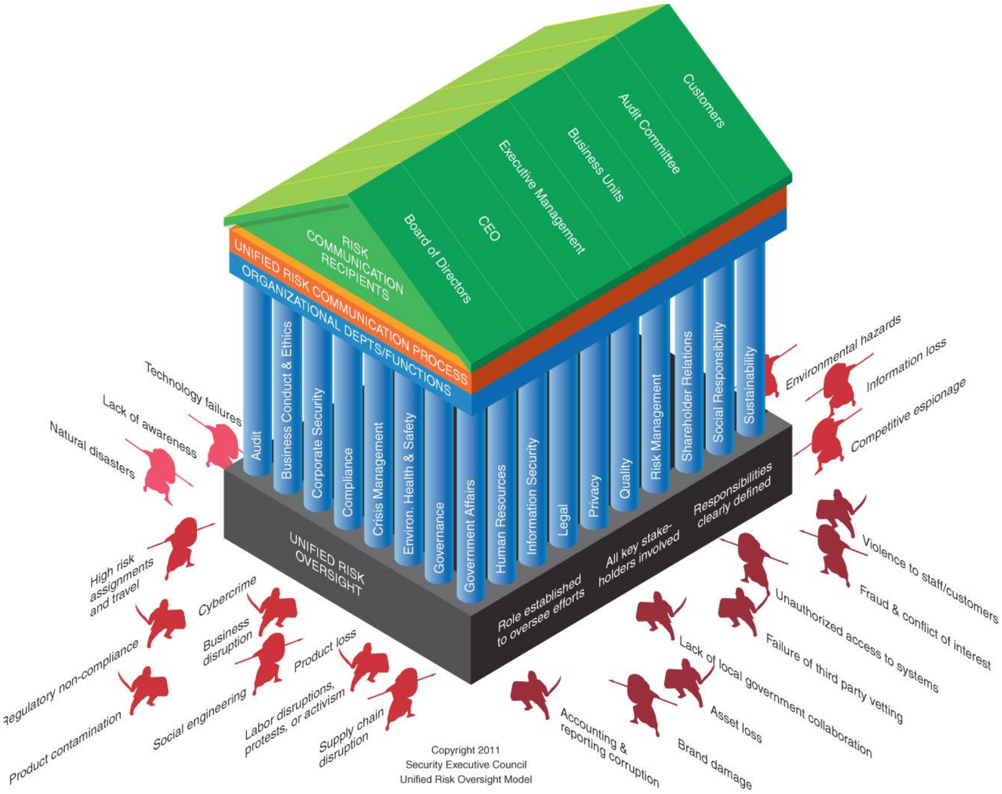
- Employee disagreements with other employees or managers.
- Corporate travel to new countries to buy materials or negotiate sales.
- Potential theft of new innovations, secrets to operating success or customer lists.
- More widespread and onerous government regulations and requirements. These may carry significant penalties for things such as failing to protect employees, products, property and computer systems that take significant time and resources and can result in unwanted costs and publicity.

Depending on the company size and industry, corporate security can mean different things to different organizations. The Security Leadership Research Institute research has identified 20 different responsibilities that fall under a corporate security department.


Collective Knowledge: Realm of Security Responsibilities
SEC
Security Executive Council
A research and advisory firm
Threat Management
Investigations
Vetting
Security Operations
Information Security
Training
Security Technology
Loss of Proprietary Information
Cyber/ Forensic Investigations
External Investigations Threat/ Criminal
Internal Employee Misconduct
Background Verification
Due Diligence, Vendors, Partners, Significant Customers
Facility Security
Building & Access Control
Employee at Risk Protection
DHS Law Enforcement/ Regulation Coordination
Network Access Control
Desktop & Laptop Security
Privacy/ Breach Notification
Fraud & Cyber Security Awareness
Case Management/ Product Protection
Access Control/ Cost Rationalization
Terrorism/ Espionage/ Inside Threat
Crisis Management
Business Resilience Planning
Extremist/ Activist Groups
KEY:
Areas of responsibility where partnership is required between Corporate Security, IT Security, and often other groups (e.g., Human Resources, Legal, Compliance, Audit)
Traditional IT Security exclusive areas of responsibility
Traditional Corporate Security exclusive areas of responsibility
©2015 Security Executive Council
3

Some companies have elevated the security manager position to the executive level by creating a Chief Security Officer (CSO) position. While a typical Chief Security Officer position does not exist in corporate America, there are areas of security that different CSOs at different companies will be responsible for depending on the industry or sector and what risks/threats are perceived to be important to address.

It is essential that the CSO works closely with other C-level functions and leaders, such as HR, Legal, IT, Finance, and individual business units. This has recently become more critical than ever to help effectively reduce security risks to the organization. The diagram below creates a visualization of Unified Risk Oversight (URO), where all the company organizations and leaders work in concert to reduce or eliminate security risks and residual risk—the risk that remains after efforts to mitigate the risk have been made.



Copyright 2011
Security Executive Council
Unified Risk Oversight Model

The foundational elements of a corporate security program are listed and defined in The Manager's Handbook for Business Security. This publication was created at the urging of the Federal Government to provide a resource to help businesses combat the types of losses or damages discussed previously. The 15 elements developed and agreed upon by numerous Fortune 500 CSOs are:

- Risk Assessment and Mitigation
- Strategic Security Planning
- Marketing the Security Program to the Business
- Organizational Models for the Security Department
- Regulations, Guidelines, and Standards
- Physical Security and First Response
- Security Training and Education
- Communication and Awareness Programs
- Safe and Secure Workplaces
- Business Conduct and Ethics
- Business Resiliency
- Securing the Supply Chain
- Measures and Metrics
- Continuous Learning: Addressing Risk with After-Action Reviews

Additional research has identified five key elements in corporate security success that need to be taken into consideration and managed when implementing or upgrading a program.

- Corporate level/organizational readiness for Security – the company's view of what security means to them and its purpose in light of business goals.
- Security leadership capability – the right fit for current expectations but also a vision of what could be.
- Security department maturity status - knowing where security programs are currently helps to develop a roadmap to a desired end state.
- Corporate culture – understand the corporate culture and tailor strategies and tactics within that framework.
- Regulatory requirements – what is required for a particular company or industry.

Once a corporate security function is in place, the real work begins in identifying vendors and service providers, managing information based on risks, and recruiting experienced and talented people. Finally, the best security departments work with executive management to add more value to the business; enable the business to operate where and how they need to; and provide employees a resource for their safety and security concerns.

Visit the Security Executive Council website for other resources in the Demonstrating Value: Communicating Value 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 here: https://www.securityexecutivecouncil.com/