THE CONFERENCE BOARD

ExecutiveAction

No. 115 September 2004

Trends in Corporate Security . . .

Cops, Geeks, and Bean Counters: The Clashing Cultures of Corporate Security

by Thomas E. Cavanagh, Senior Research Associate, The Conference Board

In most companies, the security function is divided into three distinct worlds: physical security, IT security, and risk management—the realms of "cops, geeks, and bean counters." Bridging this clash of cultures and creating a common frame of reference is essential if companies are to manage their total security needs in an effective manner.

As corporations attempt to upgrade security, they often find that coordination and control are difficult to achieve. Accountability is dispersed, with key decisions often made by middle managers. The security function itself is generally scattered into three distinct silos:

- Physical security (protection of people, goods and facilities)
- IT security (protection of data and communications)
- Risk management (protection of finances)

These three silos are separated not just by their distinct locations on the organizational chart, but by a clash of cultures as well:

- Physical security specialists are usually recruited from law enforcement and the military, where they are trained to respect an authoritarian command structure;
- IT security is part of the world of high technology, where innovation is admired and a libertarian value system often prevails;
- Risk managers are integral to the world of corporate finance, where the primary objectives are to maximize returns, minimize costs, and avoid losses.

It is hard to image three more disparate cultures. Each has its own educational and career path, its own jargon, and its own distinctive worldview. Simply getting them to communicate with one another (without a translator!) can be difficult. In a nutshell, corporate security exists in three different worlds: the realms of "cops, geeks, and bean counters." To effectively manage their total security needs, companies must bridge this clash of cultures and create a common frame of reference for the function.

The Clash of Cultures

Security experts often believe that isolating people, facilities, and information is a key procedure to ensure protection.. Walling off assets produces silos on the organization chart and it also produces a culture in which vital information may be hoarded rather than shared. As the Federal 9/11 Commission report has found, the consequences of organizational silos and information hoarding within the government can be dire indeed.

Similar problems often bedevil the private sector. Personnel trained in physical security often find the IT world a mystery. They don't understand the jargon and may be intimidated by the technical expertise needed to become recognized as a Certified Information Systems Security Professional (CISSP), the standard credential in the field.

The "geek" culture often values an ethic of sharing and freedom. Open-source code, wireless networking, and laptop portability may serve the convenience and enhance the productivity of computer professionals, but these features may be seen by "cops" as posing unacceptable risks of penetration into the heart of a company's data system.

The classic bureaucratic response to an insistence on unwanted procedures is passive resistance. Rules may be posted, but if rank-and-file employees don't accept their legitimacy, they simply won't follow them. To the "cops," who are used to a command-and-control model of institutional governance, these aspects of corporate culture often prove maddening. But the "cops" may not be flexible or sophisticated enough to engage in the persuasion necessary to inculcate a security-conscious culture among IT employees.

The "bean counters" bring a financial perspective to bear on security policy-making that often frustrates the physical and IT security managers. Risk managers can be important allies of security executives by quantifying the potential costs of risky behaviors or the lack of security procedures. But the flip side of their focus on spreadsheets is the asymmetry of financial calculations in the security field.

Simply put, it is much easier to measure the costs of investing in security than to quantify the benefits. The costs are tangible and immediate; the benefits are hypothetical, even if the risks are real. With sufficient skill in modeling, the benefits can be approximated in a probabilistic sense. But they can never be measured with certainty, and they are ultimately speculative and subject to judgment and persuasion. An overly rigid insistence on achieving precision in estimation can undermine the need for effectiveness in security by establishing criteria for security investments that can never be met.

Physical security professionals are trained to think in terms of prevention rather than return on investment. Thus, they can easily find themselves inadvertently presenting their recommendations as items that impact the cost side of the ledger without sufficient documentation of the potential benefits. Training the "cops" to think in terms of hurdle rates and other investment criteria often requires a major effort at retraining.

In the IT field, the major appeal to the company's financial decision-makers is the key role played by a firm's IT system in ensuring business continuity. If a company loses its e-mail or telephone access, or if a web site or electronic order system or automated logistics network goes down, the company for all practical purposes ceases to function. The results of a prolonged outage can be catastrophic. This is a powerful argument. But integrating the IT professionals' concerns with those from other operating divisions may prove difficult, unless and until an emergency actually occurs—at which point it may be too late to salvage the company's operations.

Defending Assets as the Common Core of Security

Despite their differences, there are some underlying commonalities to the security function in physical protection, IT, and risk management. In fact, the presence of such commonalities only underscores the depth of the cultural differences that flourish in the institutional cultures of many large companies.

At its core, security is about defending assets. These assets may be people; they may be products; they may be facilities; they may be supply chains or transportation systems; they may be proprietary customer data or intellectual property; they may be financial assets; they may be as tangible as cargo containers and their contents or as intangible as brands and bits and bytes.

Assets must be protected from destruction; they must also be protected from corruption and degradation. Protecting assets means protecting the integrity of assets from outside tampering or compromise. The premise is that assets should not be altered without the knowledge and permission of their owners; they must be protected from contamination or theft.

Protecting assets means establishing a perimeter around those assets, which is then defended. Entry through the perimeter is tightly controlled and requires permission. Determining screening procedures—the rules for allowing or disallowing entry—and enforcing those rules effectively, is the core of the job of the security professional.

The basic concepts hold true regardless of whether it is physical or IT security. It is, perhaps, easier to visualize safeguarding physical territory, but the exact same concepts apply to the world of IT. Just as the "guard at the gate" tries to stop intruders from entering a building, a computer firewall is designed to repel viruses, worms, and hackers from infiltrating an IT system.

Both physical and data security systems must have a means for authenticating the identity of potential entrants seeking access through the perimeter. One must also guard against theft. Breaking into a facility and stealing goods or equipment is the first danger that comes to mind. But theft of digital information can have grave consequences: customer identities, marketing databases, intellectual property, and financial records can be hijacked without adequate controls. Risk managers must ensure that their companies' systems can guard against fraud or incompetence, either of which can leave the firm exposed to unacceptable levels of financial risk.

The security process in all three realms shares an additional commonality: as the level of threat increases, so must the level of response necessary to counter the threat. Thus, security is a dynamic process, a sort of chess game in which the malefactors are constantly probing for weakness and the guardians must adjust their defenses accordingly. The ratcheting up of threat and response makes the entire process of security akin to hitting a moving target. The guardians can never let down their guard.

The Challenge of Coordination

The three silos enjoy widely differing levels of prestige and authority within a typical company.

- Physical security is the least potent, often lodged in middle management and reporting to operations managers at the business unit or facility level.
- Risk management is generally handled by actuaries who report through the chain of command to the CFO. Their key role in budgeting, accounting, and assessment of liability gives the risk managers a significant degree of influence in corporate strategy.
- IT security is vital to business continuity because IT has become so central to managing the day-to-day operations of the global corporation.

Exhibit 1

More In Common Than They Think

(*Whether they realize it or not, all three silos involved in the security function deal with analogous issues*)

Security Issue	The Silos		
	Physical Security "*Cops*"	*IT Security* "*Geeks*"	*Risk Assessment* "*Bean Counters*"
Assessment	Audits of vulnerabilities with regard to penetration of buildings, supply chains, or transportation systems	Use of "benign" hackers to determine where IT networks can be penetrated	Quantitative modeling to estimate exposure to financial risk under a variety of scenarios
Prevention	Hardening of physical facilities; use of gates, turnstiles, and other entry barriers	Maintaining firewalls; installing antivirus software	Establishing strict accounting controls
Detection	Guards or electronic devices to monitor and detect intruders	IT alerts when unauthorized uses or denial-of-service attacks are underway	Quantitative models to determine when exposure to financial or insurance risks has reached an unacceptable level
Response	Sending police, firefighters, and emergency medical personnel; evacuation of facilities	Shutdown and rebooting of computer systems	Launching investigations; use of financial hedges; closing out unprofitable trading positions
Recovery	Cleanup, repair, and reopening of damaged facilities	Switch to backup IT system; retrieval of data from offsite storage	Reversion to an acceptable profile of financial risk

In the immediate aftermath of 9/11, many companies expressed interest in creating the position of Chief Security Officer (CSO). The CSO would be a senior executive, analogous to a Chief Financial Officer (CFO) or Chief Information Officer (CIO), tasked with managing and devising strategy for the overall security posture throughout the company.

To date, most firms have stopped short of this end point. It is much more common for companies to establish a coordinating committee, drawn from all relevant silos, to deal with emergency response and business continuity. While these coordinating committees often owe their initiation to the need to manage a specific crisis, companies are increasingly viewing them as an essential tool for maintaining preparedness on an ongoing basis.

A carefully thought-out emergency response plan can make the key actors throughout the firm conversant with their responsibilities before an emergency occurs. Drills and tabletop exercises can identify potential problems and fine tune the procedures needed to ensure a timely and effective response in an actual emergency.

The strength of the coordinating committee model is its flexibility and adaptability, because various segments of the company can be consulted and engaged as needed. However, the ad hoc nature of the model can also limit its effectiveness as a preparedness tool. In the absence of an emergency, it may be difficult to obtain buy-in for the decisions that are reached. In fact, it may prove difficult to make clear decisions at all, because a need for consensus may reduce the range of the group's authority to the lowest common denominator. If the group cannot allocate resources or change company policy, its effectiveness and impact may be severely constrained.

Security as Risk Management

What the coordinating committee model lacks is a clear set of priorities for determining security policy. The discipline of risk management can provide a coherent intellectual framework for analyzing security needs and integrating the various strands of security management inside the corporation. Risk management affords a rigorous methodology for determining the likelihood of an adverse event, the value of the assets at risk, and an estimate of how much investment is appropriate to manage the resultant financial exposure.

The practice of risk management can be very helpful in crossing the cultural divide. It establishes a common set of concepts that can be applied to physical or virtual security. It provides tools that are relevant to the protection of both tangible and intangible assets. Most importantly, risk management relates security to financial management, enabling executives to measure the business value of security spending in relation to its benefits.

The most straightforward way to gauge the return on security investments is through their efficacy in reducing insurance premiums. Insurers will generally roll back premiums in recognition of security procedures that clearly reduce risk. In this way, the market creates incentives for companies to make their operations safer, and in turn reduces the exposure of insurers to the possibility of a catastrophic loss. The accelerating trend towards security standards and industry certification, such as the NFPA (National Fire Protection Association) 1600 Preparedness Standard, and the emerging ISO guidelines on security, should make this process increasingly routine.

However, risk is reflected in many aspects of corporate operations:

- Non-compliance poses risks in terms of legal liability and reputation;
- Loss of data can threaten privacy and shatter the trust of customers;
- Theft of intellectual property can eliminate a company's competitive edge in the marketplace, and undermine the value of its research and development spending;
- An industrial accident can destroy a company's standing as an employer of choice, and jeopardize its license to operate.

A peculiarity of risk management as a financial discipline is that it often defines returns as the avoidance of loss rather than the accrual of profit. This makes it difficult to relate the management of security risk to the central mission of a profit-making company. Absent a business model that relates security to profit, the security function can become vulnerable to cost-cutting pressures within the firm, especially when business is slow.

Yet the avoidance of loss can be measured, or at least estimated in probability terms. This discipline can be employed to assess which vulnerabilities are most in need of mitigation, and to set priorities for spending and changes in procedure.

"Don't Tell Me No, Tell Me How"

Protecting the perimeter may be the core of the security function. But security proves its value by going beyond the realm of defense and becoming a strategic asset in the management of the firm. Security isn't just about preventing loss; it is about enabling managers to take advantage of opportunities without undue risk. Increasingly, the message from the C-suite to the security director is: "Don't tell me no, tell me how."

The traditional career path of physical security professionals, with its emphasis on the peacekeeping professions (police and the military) has limitations when it comes to the depth and range of experience necessary to manage overall security risk. Often, the authoritarian mindset, necessary for success in the peacekeeping professions, may not be effective in implementing security policies across corporate silos. In a bureaucratic business environment, where command authority may be lacking and resources may not be sufficient, security executives must develop higher-order skills of persuasion to obtain buy-in and convince their managerial peers and their firm's employees that adherence to security procedures is truly in their own best interest.

Nor are the IT professionals ideally positioned to coordinate security across the company. They have traditionally been in charge of business continuity because of the central role of IT in daily operations. But their focus on technical issues of data management and their unfamiliarity with physical security requirements gives them an incomplete picture. IT security is increasingly seen as an unavoidable investment because of the perception of increased threat, but quantifying its benefits has been almost as elusive as measuring it in the field of physical security.

Risk management may be the function that comes the closest to integrating the many elements of corporate security in a comprehensive framework. It touches on both physical and data security; it is plugged directly into the financial management of the firm; and it can generate a powerful business case to ensure compliance and implementation of security initiatives.

Yet risk management is generally an analytic function rather than a command function. Risk managers can crunch the numbers and determine the risks associated with various company policies. But their direct sphere of decision making is usually limited to matters such as insurance and financial hedging. Security procedures must usually be enforced by someone else.

Getting "cops, geeks, and bean counters" to see their responsibilities in the same way may be a difficult sell. But the clash of cultures is detracting from the ability of many companies to integrate their security operations. Recognizing the commonalities that underlie their responsibilities, and making these silos conversant with one another, are just the first steps to making security an integral part of the company mission.

About the Author

Thomas E. Cavanagh is a Senior Research Associate in Global Corporate Citizenship at The Conference Board. In the past few years, he has conducted extensive research on corporate security issues. He was the lead author of *Corporate Security Management: Organization and Spending Since 9/11; After September 11th: The Challenge Facing American Business;* and of The Conference Board's series of Executive Action Reports on *Corporate Security in a Time of Crisis*. While at The Conference Board, he has also authored *Community Connections: Strategic Partnerships in the Digital Industries,* and *Corporate Community Development: Meeting the Measurement Challenge.* He is currently directing a major project on measuring the effectiveness of corporate citizenship programs.

Learning Opportunities from The Conference Board

The 2004 Corporate Security, Business Continuity & Crisis Management Conference:
Strategies to Protect Core Assets: Human, Financial, Reputational, Physical & Technological
November 10-12, 2004 – New York, NY
www.conference-board.org/security.htm

The Conference Board, Inc., 845 Third Avenue, New York, NY 10022-6679
Tel 212 759 0900 Fax 212 980 7014 www.conference-board.org