THE CONFERENCE BOARD

Corporate Security Measures and Practices

An Overview of Security Management Since 9/11

SPECIAL REPORT 05-01-SR

The Conference Board creates and disseminates knowledge about management and the marketplace to help businesses strengthen their performance and better serve society.

Working as a global, independent membership organization in the public interest, we conduct research, convene conferences, make forecasts, assess trends, publish information and analysis, and bring executives together to learn from one another.

Corporate Security Measures and Practices

An Overview of Security Management Since 9/11

by Thomas E. Cavanagh

contents

ABOUT THE **AUTHOR**

Thomas E. Cavanagh is a senior research associate in global corporate citizenship at The Conference Board. He was the author of *Corporate Security Management: Organization and Spending Since 9/11*, a study which received widespread media coverage in 2003. While at The Conference Board, he has also authored *Community Connections: Strategic Partnerships in the Digital Industries*, a study of corporate partnerships to over-come the "digital divide," and *Corporate Community Development: Meeting the Measurement Challenge*, a study of the returns on corporate investments in community economic development projects. He was the lead author of *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*.

ACKNOWLEDGMENTS

The author wishes to thank Mary Jacobson, Clayton Shedd, Ana Da Silva, and David Vidal of The Conference Board for organizing the senior executive roundtables held in 2004, and Nancy Wong, Richard Cooper, James Plehal and Marie Vachon of the U.S. Department of Homeland Security for participating in the roundtable sessions. We also wish to thank Meredith Whiting of The Conference Board for assisting with the research in 2003, and Ronald Berenbeim of The Conference Board for assisting with the drafting of this manuscript.

ABOUT THIS **REPORT**

This report was sponsored by the U.S. Department of Homeland Security. It summarizes information that was originally published in a series of reports released by The Conference Board in 2003 and 2004, as follows:

Corporate Security Management: Organization and Spending Since 9/11 (Research Report No. 1333). This study was sponsored by ASIS International, and reported the results of surveys of 199 security directors, 52 risk managers, and 80 IT security officers. Over 50 percent of each sample was derived from companies with $1 billion or more in annual sales.

Managing Corporate Security in Mid-Markets (Executive Action Report No. 67). This report presented more detailed information on mid-market companies from the research project described above.

Security in Mid-Market Companies: The View from the Top (Executive Action Report No. 102). This study was sponsored by the U.S. Department of Homeland Security. It reported the results of a survey of 96 senior managing executives (primarily CEO's, presidents, and chairmen) from mid-market companies, defined as companies with annual revenues between $20 million and $1 billion.

Security in Mid-Market Companies: Tackling the Challenge (Executive Action Report No. 119). This study was sponsored by the U.S. Department of Homeland Security. It summarized the discussion at senior executive roundtables that were convened in Atlanta and Cleveland in June, 2004.

Key Findings

Corporate security has become a high-profile issue since the events of September 11, 2001 exposed America's vulnerability to terrorist attack. Because over 80 percent of America's critical infrastructure is managed by the private sector, corporate security managers have an essential role to play in the protection of key industries and the people who work in them.

In the wake of September 11, many companies reviewed their security operations. The events of that day made clear that security was not merely a matter of protecting employees and facilities from physical harm. A terrorist attack on a major business district could disrupt operations, inhibit travel, snarl supply chains, and pose major strategic issues for the conduct and even the survival of a multinational business.

CEO's were often dismayed to discover that the security function was highly decentralized and widely dispersed through their companies' management structures, making accountability and coordination difficult. While there has been some movement toward greater coordination of the security function since 9/11, it remains decentralized in most companies.

Larger companies have been more successful than smaller companies in coping with the challenges posed by the new security environment. In general, smaller companies appear to be having difficulty finding the resources they need to upgrade their security operations.

Larger companies have been increasing their spending on security and adding to their security staff more rapidly than smaller companies, accentuating a gap in security readiness that was already present.

The findings presented in this report summarize the results of three separate research projects undertaken by The Conference Board since 2002:

- A survey of 199 security directors, 80 IT security officers, and 52 risk managers in late 2002 and early 2003, supplemented by four in-depth case studies, sponsored by ASIS International.
- A survey of 96 chief executives of mid-market companies in the spring of 2004, sponsored by the U.S. Department of Homeland Security.
- The discussion at two regional forums of mid-market corporate executives held in Atlanta and Cleveland in June, 2004, sponsored by the U.S. Department of Homeland Security.

Organization of the Security Function

- Despite having strategic implications for business management, security is still being treated as an operational concern by most companies in the United States. Centralization, coordination, and strategic management of the corporate security function are still relatively unusual.
- Security management tends to be decentralized in most large companies with responsibilities clustered into three distinct categories: (1) physical security (protection of personnel, goods, and facilities); (2) IT security (protection of data and communications); and (3) risk management (insurance and other financial issues).
- High-level reporting and accountability are still the exception rather than the rule, especially in larger companies, where silo problems are more deeply entrenched. Security responsibility is more streamlined and decentralized in smaller companies, where security executives are more likely to report to the top management.
- In terms of salary and executive level, IT security is the most prestigious security portfolio, although it is often simply an extension of the IT operation. Risk management is generally part of the financial management of the company. The position of security director is the lowest-ranking and tends to be focused on issues of physical protection. Most security executives serve below the vice presidential level and earn less than $150,000 per year. The traditional emphasis on physical protection is reflected in the recruitment of security directors from law enforcement and the military.

Defining Critical Industries

Following the usage of the U.S. Department of Homeland Security, critical industries are defined as the following: transportation; energy and utilities; financial services; media and telecommunications; information technology; and health-care. Remaining industries are classified as non-critical.

Spending Patterns

- Corporate security spending has clearly increased since 9/11, but the increases have been unevenly distributed. About half of companies report a permanent increase in the level of security spending, with companies in the critical industries leading the way.
- The median increase in total security spending in the year following 9/11 was only 4 percent, but this figure disguises a wide range, with 7 percent of companies stepping up their security spending by 50 percent or more. Larger, multinational companies reported larger increases than smaller, domestic companies. The median increase for companies with annual revenues over a billion dollars was 5.5 percent compared to 1.4 percent for firms with annual revenues below that level. However, smaller companies pay a larger share of their sales volume for security.
- Insurance and risk management was the area showing the most dramatic increase in spending, with a median increase of 33 percent in 2002. Fully one-fifth of companies report that their spending on insurance has at least doubled since 2001. The increase in insurance costs has been concentrated among companies in the critical industries.
- Companies in the Northeast Metro region reported bigger increases in spending on security and risk management than companies in the rest of the United States.

Preparedness and Business Continuity

- Smaller companies (less than 1000 FTE's) are less likely to have written security guidelines and procedures in place to handle security challenges.
- Smaller companies are less prepared for emergencies. Larger companies are more likely to have backup storage at an off-site location, conduct a risk assessment or audit of vulnerabilities, have security checkpoints, and regularly test their disaster recovery and business continuity plans.
- The risk of business interruption is greater for smaller companies because relatively few of them have established off-site emergency operations centers.

Patterns of Organization

Despite raised expectations and heightened visibility, corporate America is undergoing an evolution rather than a revolution in the management of security concerns.

The Conference Board studies found that security management tends to be decentralized in most large companies, with responsibilities clustered into three distinct silos:

- Physical security (protection of personnel, goods, and facilities)
- IT security (protection of data and communications)
- Risk management (insurance and other financial issues)

In smaller companies, security responsibilities tend to be more streamlined and centralized. Of course, smaller companies in general tend to resist the proliferation of silos that is so common in large multinational corporations, making for fewer layers of bureaucracy in other realms of management as well.

One consequence is that security executives are more likely to report to the top management of their companies in smaller firms. Looking only at companies with less than $500 million in revenues, 24 percent of security directors report directly to the CEO or COO. This figure drops to 18 percent in companies between a half-billion and a billion dollars in revenues, and 12 percent or less in companies with $1 billion or more in revenues.

The differences are even more dramatic with regard to the other two major security positions. Fully one-third of risk managers report to the top in companies with under $1 billion in revenues, compared to 14 percent in companies above that size. Almost half (48 percent) of IT security officers report to the CEO or COO in companies under the $1 billion mark. In companies with $1 billion to $5 billion in sales, 36 percent of IT security officers report to the top. However, none of the IT security officers interviewed report directly to the CEO or COO in companies above $5 billion in revenues.

More security executives report to the top in smaller companies

Percentage reporting to CEO or COO

	Percentage	Number of respondents
Security directors		
Under $500 million	24.1%	54
$500 million to $1 billion	18.2	33
$1 billion to $5 billion	8.8	57
Over $5 billion	11.8	51
Risk managers		
Under $1 billion	33.3%	24
Over $1 billion	14.3	28
IT security officers		
Under $1 billion	48.1%	27
$1 billion to $5 billion	36.0	25
Over $5 billion	0.0	28

Security Directors

Security has traditionally been associated with physical protection—"the guard at the gate"—in the lingo of the profession. This function remains the core responsibility of the senior executives who manage corporate security. These executives primarily come from a background in the "peacekeeping" professions, with 47 percent having police experience and one-third coming from the military. Some 15 percent have worked in the security industry for a vendor or consultant, and 12 percent have been employed in private investigation.

Most security directors come from a background in law enforcement or the military

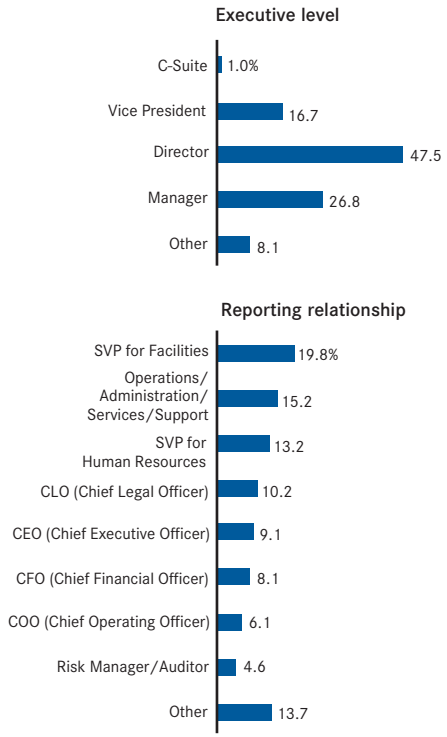
Number of respondents: 199

While important, strategic business management does not loom as large in the career paths of security directors. Just under one-fourth report diversified corporate management experience, while 11 percent have been involved in facilities management and 9 percent apiece in IT and risk management. As security issues "move up the food chain" in significance, senior management experience will probably become more important in the future as a qualification for the position of security director.

Given their importance in the current business environment, security directors occupy a surprisingly modest level in the corporate totem pole. Most security directors hold mid-level management positions that are deeply imbedded in the routine operations of their companies.

The vast majority of security directors hold a rank below the vice presidential level. Only 1 percent hold a title at the C-suite level and 17 percent are vice presidents. Almost half (48 percent) are directors and 27 percent are managers.

Profile of Security Directors



Number of respondents: 199

Reporting relationships are remarkably diverse. The most common pattern (20 percent) is for security directors to report to the SVP for Facilities, reflecting the profession's traditional emphasis on physical protection. Another 15 percent report to an executive with responsibility for operations, administration, services, or support, while 13 percent report to the SVP for Human Resources.

Most security directors do not report directly to the top management of their companies. Only 9 percent of security directors report to the CEO. Some 10 percent report to the Chief Legal Officer, presumably due to liability and compliance issues. Another 8 percent report to the CFO, and 6 percent report to the COO. C-suite access may become more common in the future as security concerns become more integrated into strategic management. But at present, a routine reporting relationship to the CEO or COO is still relatively unusual.

Risk Managers and IT Security Officers

The functions of risk management and protecting the IT system are handled in separate silos in most companies, distinct from each other and from the physical security function as well. Interestingly, both of these positions appear to enjoy more seniority and influence within the corporate structure than the security director position.

Risk managers serve at a considerably higher level than security directors. Some 8 percent hold the title of Chief Risk Officer or Chief Administrative Officer, placing them at the top management level. Fully 31 percent are vice presidents and 21 percent are directors, while 31 percent serve at the manager level.

The reporting relationships reflect this seniority. Among risk managers, 21 percent report to the CEO, and an identical percentage reports to the CFO. Another 15 percent report to an executive with financial responsibilities, indicating the preeminence of financial concerns in determining the accountability for the risk management portfolio.

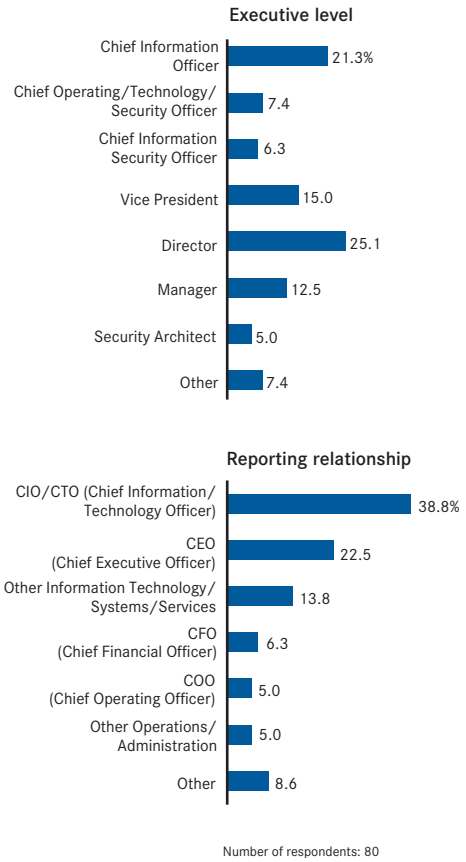
A less common pattern is for the risk manager to report to an executive with operational responsibilities in human resources (8 percent), or facilities, administration, or procurement (4 percent apiece). Only 4 percent of risk managers report to a Chief Security Officer, indicating that the risk manager position is defined primarily in terms of financial issues rather than security responsibilities.

IT security is the most prestigious of the three major security portfolios. Over one-third of the IT security officers surveyed serve at the senior management level. The Chief Information Officer is the IT security officer at 21 percent of the companies surveyed, meaning that security is part of that executive's responsibility as the company's senior IT official. Some 6 percent hold the title of Chief Information Security Officer and another 7 percent have a different C-level title.

Profile of Risk Managers

Number of respondents: 52

Profile of IT Security Officers



Number of respondents: 80

Fifteen percent of IT security officers are vice presidents, while one-quarter are directors and one-eighth are managers. Another 5 percent hold the title of Security Architect.

Over two-thirds of IT security officers report to C-level executives. Some 39 percent report to the Chief Information Officer or Chief Technology Officer, and 23 percent report directly to the CEO, while 6 percent report to the CFO and 5 percent to the COO. Another 14 percent report to an executive in information systems or services, meaning that about half of all IT security officers report through an IT silo. The high level of IT security officers reflects how critical IT systems have become to the management of a modern corporation.

Accountability is Widely Dispersed

Security responsibilities are widely dispersed in a typical company. Security executives were asked who had the ultimate responsibility for a variety of security-related functions. There are only three functions for which over half of all companies report the same pattern of accountability:

- IT security is the ultimate responsibility of a senior IT executive in two-thirds of companies.
- Insurance and risk management is the ultimate responsibility of the CFO in just over half of companies.
- Background investigations are the ultimate responsibility of the SVP for Human Resources in just over half of companies.

Security responsibilities are widely dispersed

Executive with ultimate responsibility for…	CIO/CTO/ SVP for IT	CFO	SVP for HR	CSO	SVP for Facilities	COO
IT security	67.3%					
Insurance/financial risk management		54.8%				
Background investigations			54.8%	14.2%		
Protecting employees			15.2	25.8	17.2%	
Protecting buildings and facilities			10.1	23.6	24.6	
Executive security			10.2	24.5	14.3	
Business recovery and continuity	13.1	18.2				19.2%
Biological/chemical/radiological hazards			9.6	18.1	18.6	
Emergency preparedness			11.1	17.6	17.6	
Protecting supply chain		11.3		10.8	15.4	10.3
Protecting distribution chain				13.3	14.9	10.8

Number of respondents: 199

For all other security-related functions, no more than one-quarter of companies report that ultimate responsibility is handled by any one executive. Three main clusters appear, however. The following responsibilities related to physical protection are usually accountable to the CSO, the SVP for Facilities, or the SVP for Human Resources:

- Protecting employees
- Protecting buildings and facilities
- Executive security
- Biological, chemical, and radiological hazards
- Emergency preparedness

Protecting the supply and distribution chains are usually the ultimate responsibility of the SVP for Facilities, the CSO, or the COO. Business recovery and continuity have a very distinctive pattern, with accountability assigned to the COO, CFO, or a senior IT executive.

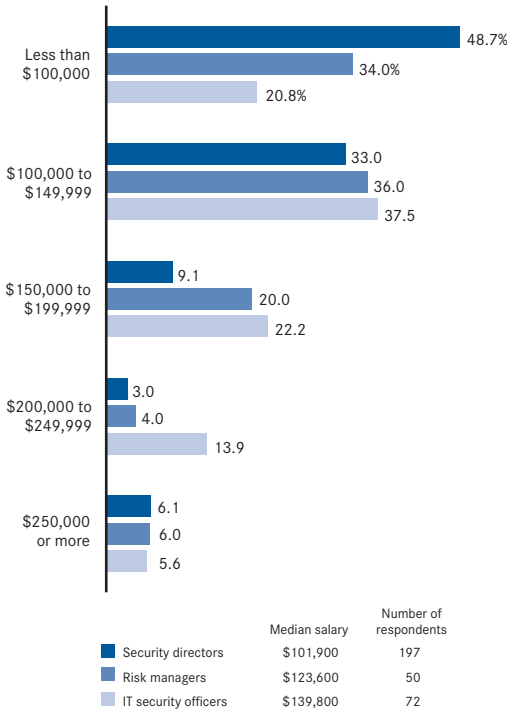
Salary Levels

Compared to the most senior management positions, security executives earn relatively modest salaries. The salary levels reflect the prestige and reporting relationships discussed earlier.

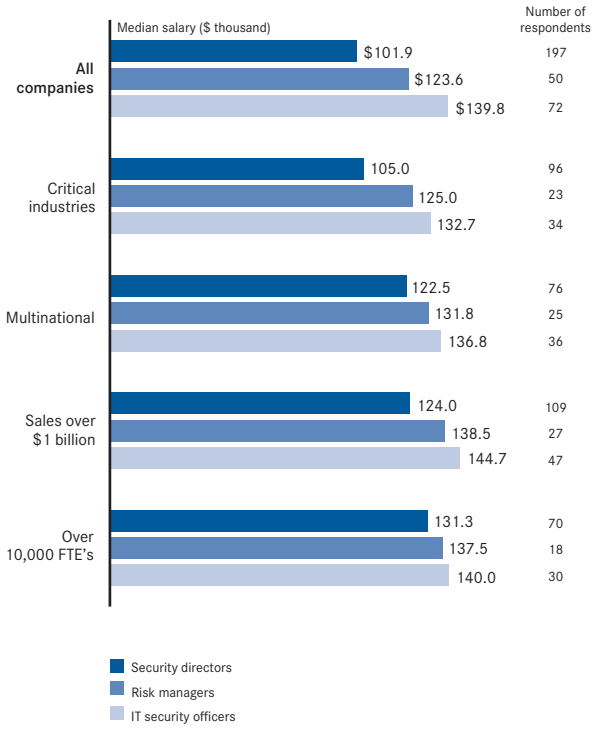
Data from The Conference Board's 2003 report on security spending showed that IT security officers are the best paid of the three security management positions, earning a median salary of $139,800 per year. Risk managers are second with a median salary of $123,600. The security directors bring up the rear, with a median salary of $101,900. Fully 20 percent of IT security officers make at least $200,000 a year, compared to 10 percent of risk managers and 9 percent of security directors.

Large multinational companies pay the highest salaries for security directors and risk managers. For example, the median salary for security directors in companies with at least $1 billion in sales is $124,000, well above the median of $101,900 for all companies. The median for risk managers in such companies is $138,500, again well above the overall median of $123,600. On the other hand, the difference in median salaries between IT security officers in these large companies and the overall median is less than $5,000 per year. It appears that salary levels in the IT security profession are driven less by the size of the company than by the expertise required to fill the position.

IT Security officers are the most highly paid security executives



Security directors and risk managers earn more at large multinationals



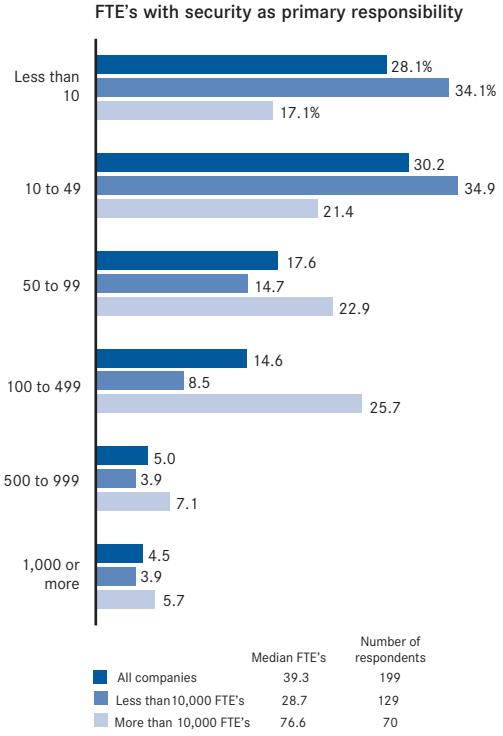
Salaries are lower in smaller companies

Annual salary of security director

Sales level	Less than $100,000	$100,000 to $149,000	$150,000 to $199,000	$200,000 or more	Number of respondents
Under $500 million	73.6%	20.8%	3.8%	1.9%	53
$500 million to $1 billion	70.6	26.5	2.9	0.0	34
$1 billion to $5 billion	42.1	42.1	8.8	7.1	57
Over $5 billion	17.6	41.2	17.6	23.6	51

The position of security director carries a much lower salary in smaller companies than in larger ones. In companies with less than $1 billion in annual sales, over 70 percent of security directors earn less than $100,000 a year, a relatively modest salary for a senior executive in a contemporary firm. Over half of all security directors make above $100,000 a year in companies with $1 billion or more in sales. In companies with over $5 billion in sales, 82 percent of security directors make over $100,000 per year, and almost one-quarter (24 percent) make over $200,000 per year.

Most companies employ less than 50 people for security



Staffing Levels

Security directors were asked how many FTE's their companies employ that have security as their primary responsibility. Among the 199 companies in the sample, the median number of security employees is 39.3. Of course, the number varies depending on the size of the company. For companies with under 10,000 total FTE's, the median security employment is 28.7 FTE's. For companies with 10,000 or more FTE's, the median security employment is 76.6 FTE's.

Just under half of all companies (47 percent) reported that they increased their security staffing level following 2001. Larger companies were more likely to increase security staff. Some 38 percent of companies with under $500 million in revenues said they increased their security FTE's after 2001. This proportion rises to 44 percent for companies between $500 million and $1 billion in sales; 52 percent between one and five billion dollars; and 55 percent with over $5 billion in sales.

Larger companies are expanding their security operations more rapidly

Percentage of companies increasing security FTEs since 2001

Sales level	Percentage	Number of respondents
Under $500 million	37.7%	53
$500 million to $1 billion	44.1	34
$1 billion to $5 billion	51.7	58
Over $5 billion	54.9	51

Note: "Don't know" eliminated.

Similarly, security staff has risen among 55 percent of companies with 10,000 or more total FTE's, compared to 46 percent of companies with 1,000 to 9,999 FTE's and only 32 percent of companies with a payroll below 1,000 FTE's.

When critical and non-critical industries are broken into specific industry segments, a wide disparity appears on this measure. Financial services companies were most likely to report an increase in security staffing (62 percent of companies), followed by companies in the "digital industries" (technology, media, and telecommunications) with 53 percent reporting an increase, energy and utilities (47 percent), healthcare (39 percent), retail and wholesale trade (33 percent), and manufacturing (31 percent).

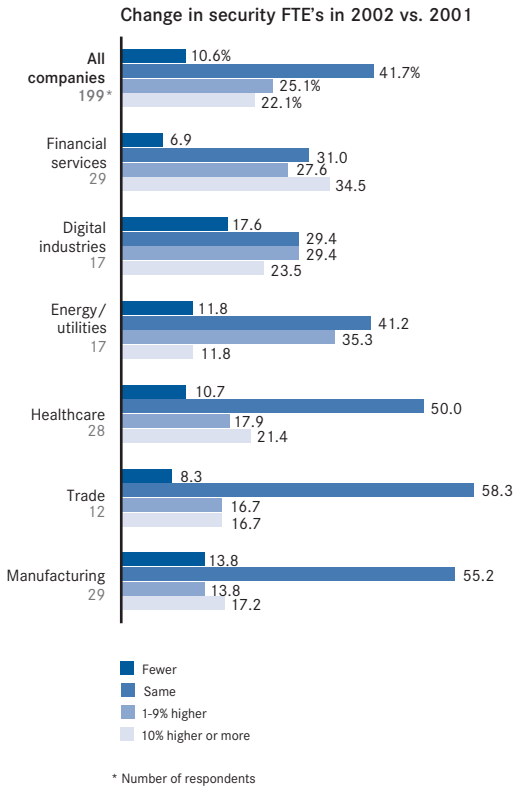
IT security is a relatively small share of security employment at most companies. Almost half of all companies (48 percent) employ fewer than 5 FTE's whose primary responsibility is IT security. However, companies in critical industries are much more likely to have a relatively large contingent of people dealing with IT security. Almost half of such companies (48 percent) have 10 or more FTE's working on security, compared to 31 percent of companies in non-critical industries.

Larger companies are increasing security staff more rapidly (2002 data)

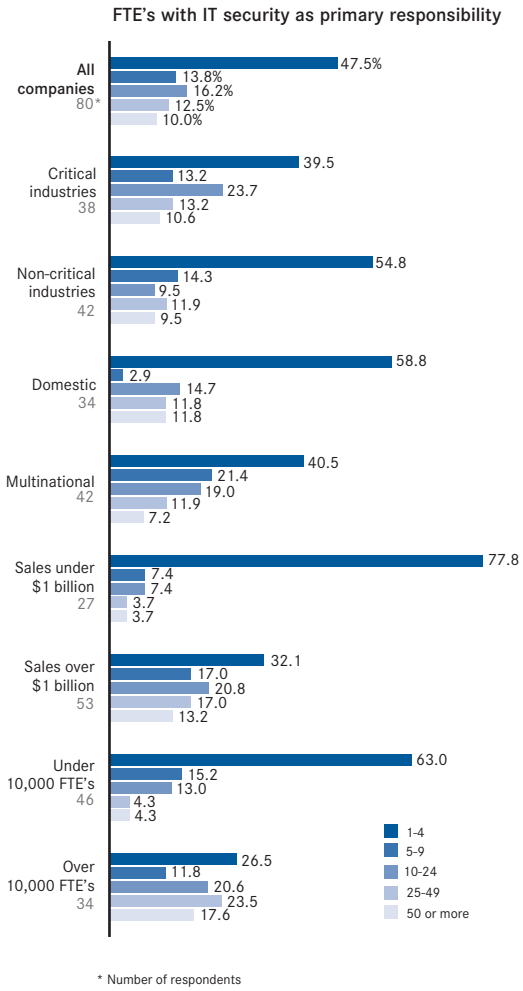
Change in security FTE's	Under 1,000 FTE's	1,000 to 9,999 FTE's	10,000 or more FTE's
Fewer than last year	7.1%	12.1%	10.1%
Same as last year	60.7	41.4	34.8
1% to 9% higher	25.0	25.3	26.1
10% or higher	7.1	21.2	29.0
Number of respondents	28	99	69

Note: "Don't know" eliminated.

Financial and technology companies are increasing security staff most rapidly



Companies in critical industries employ more people for IT security



Not surprisingly, larger companies have more staff devoted to IT security. Fully three-quarters (75 percent) of companies with $5 billion or more in sales have 10 or more IT security personnel, and 43 percent have 25 or more. Only one-quarter (24 percent) of companies between $1 billion and $5 billion in sales have 10 or more IT security staffers, while over half (52 percent) have fewer than five. Meanwhile, over three-quarters (78 percent) of companies with under $1 billion in sales have fewer than five IT security staffers. Similarly, 62 percent of companies with 10,000 or more total FTE's have 10 or more IT security personnel, compared to 22 percent of companies with a total payroll below that size.

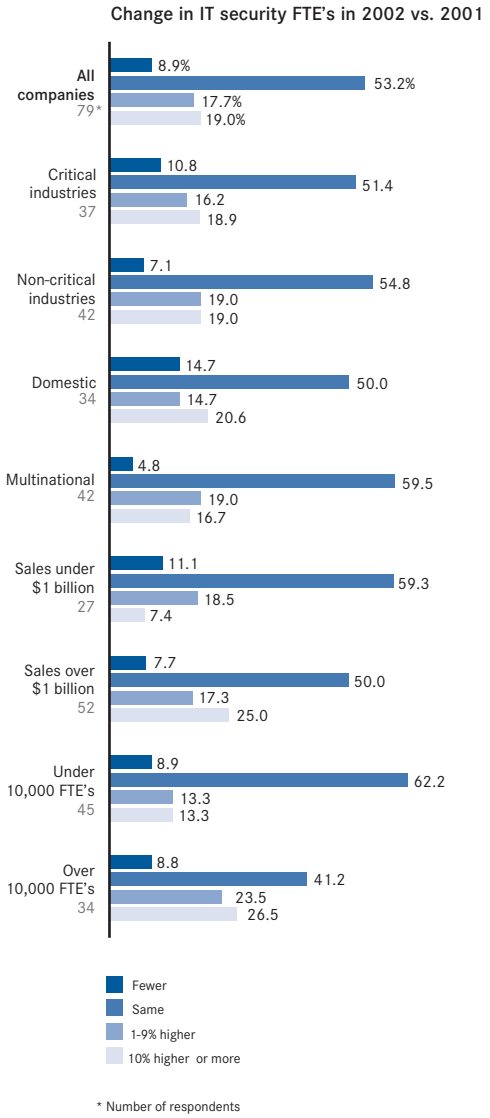
Most companies have a small IT security staff

IT security FTE's	Under $1 billion	$1 billion to $5 billion	Over $5 billion
1 to 4	77.8%	52.0%	14.3%
5 to 9	7.4	24.0	10.7
10 to 24	7.4	8.0	32.1
25 or more	3.7	16.0	42.8
Number of respondents	27	25	28

Note: "Don't know" eliminated.

Larger companies have increased their IT security staff most rapidly. While 42 percent of companies with $1 billion or more in sales increased their IT security staff since 2001, only 27 percent of companies below this sales level have done so. Similarly, half of companies with 10,000 or more FTE's have increased IT security staff, compared to 27 percent of companies below that level of employment.

Larger companies are increasing IT security staff most rapidly



* Number of respondents

Consolidation of Security Management

Following 9/11, expectations seemed to be that corporate America would move to centralize the security function under the control of a Chief Security Officer (CSO) reporting directly to the CEO. That does not appear to be the case.

The Chief Security Officer (CSO) position is intended to be analogous to that of a Chief Financial Officer (CFO) or Chief Information Officer (CIO). The CSO would coordinate all security responsibilities throughout the company and would be accountable to top management and the governing board. With a single person accountable for security responsibilities, the many silos involved in security operations could be better coordinated and information could be disseminated more effectively throughout the corporation.

The CSO concept hinges on the perceived need to integrate security concerns into corporate strategy. In theory, the position would give security issues a place at the table whenever high-level decisions are being made about location of facilities, supply chain sources, choice of corporate partners, and procedures to ensure the safety of a company's products and stakeholders. The CSO would concentrate on the "big picture," delegating routine oversight of physical security to managers at the operating level.

With regular access to the C suite, the CSO would be better able to redirect company policies quickly in response to an emergency or a perceived threat. Finally, the CSO would control the security budget for the corporation as a whole, so security spending could be managed more effectively.

Authority and Financial Resources

Looking their companies, security executives tend to be much more satisfied with their decision-making authority than with the financial resources under their control. Security executives were asked to agree or disagree with the statement: "I have the decision-making authority I need to deal with the security concerns that I am directly responsible for in my company" or an equivalent statement dealing with risk management or IT security concerns. Almost all security executives agreed with this statement; 51 percent of security directors, 35 percent of risk managers, and 43 percent of IT security officers agreed with it strongly.

However, there was much less agreement with the statement: "I have the financial resources I need to deal with the security concerns that I am directly responsible for in my company" or the equivalent for risk management or IT security. Only 26 percent of security directors, 19 percent of risk managers, and 14 percent of IT security directors agreed strongly that they had the financial resources they needed. Meanwhile, 27 percent of security directors, 25 percent of risk managers, and 35 percent of IT security officers disagreed with this statement.

Security executives in non-critical industries were the least satisfied with their control over financial resources. Fully one-third (33 percent) of security directors in non-critical industries disagreed that they had enough control over finances, compared to 21 percent of security directors in critical industries. The disparities were even greater for risk managers: 32 percent in non-critical industries disagreed, compared to 17 percent in critical industries. The dissatisfaction was most acute among IT security officers—almost half (45 percent) in non-critical industries disagreed that they had adequate financial resources, compared to 24 percent in critical industries.

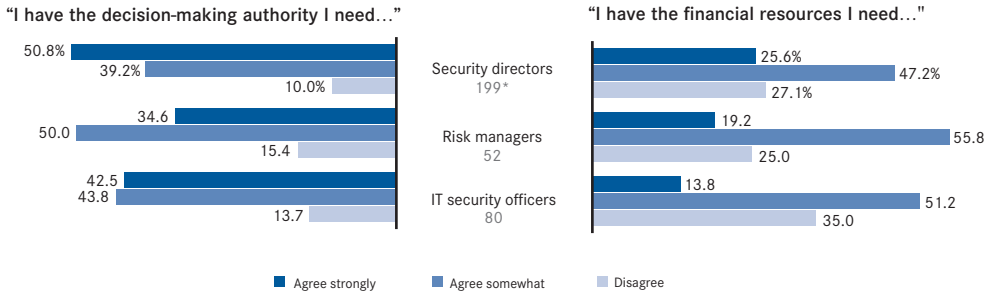
Apparently in critical industries, it is easier for security executives to make a business case for obtaining the financial resources they feel they need. In the non-critical industries, because security does not appear to be quite as integral to the business, it is more difficult for security executives to battle successfully for a share of the corporate budget.

"I have the financial resources I need to deal with security concerns that I am directly responsible for in my company."

Sales level	Agree strongly	Agree somewhat	Disagree	Number of respondents
Under $500 million	25.9%	38.9%	35.2%	54
$500 million to $1 billion	23.5	50.0	26.4	34
$1 billion to $5 billion	25.9	46.6	27.5	58
Over $5 billion	25.5	54.9	19.6	51

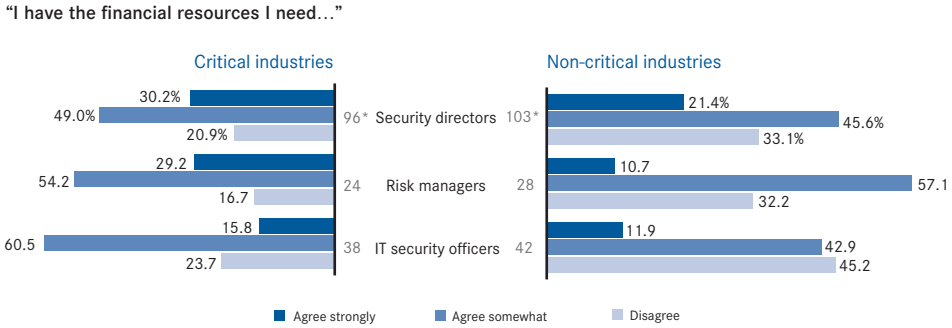
Security directors in smaller companies were also more likely to complain that their financial resources are inadequate. Looking at companies with less than $500 million in sales, over one-third (35 percent) of the security directors disagreed that they had the financial resources they need to deal with security concerns. This proportion drops to about one-quarter for companies between $500 million and $5 billion in revenues, and only 20 percent for companies with more than $5 billion in sales.

Security executives are more satisfied with their decision-making authority than with their financial resources



* Number of respondents

Security executives in non-critical industries are least satisfied with their control over financial resources



* Number of respondents

Changes in Accountability

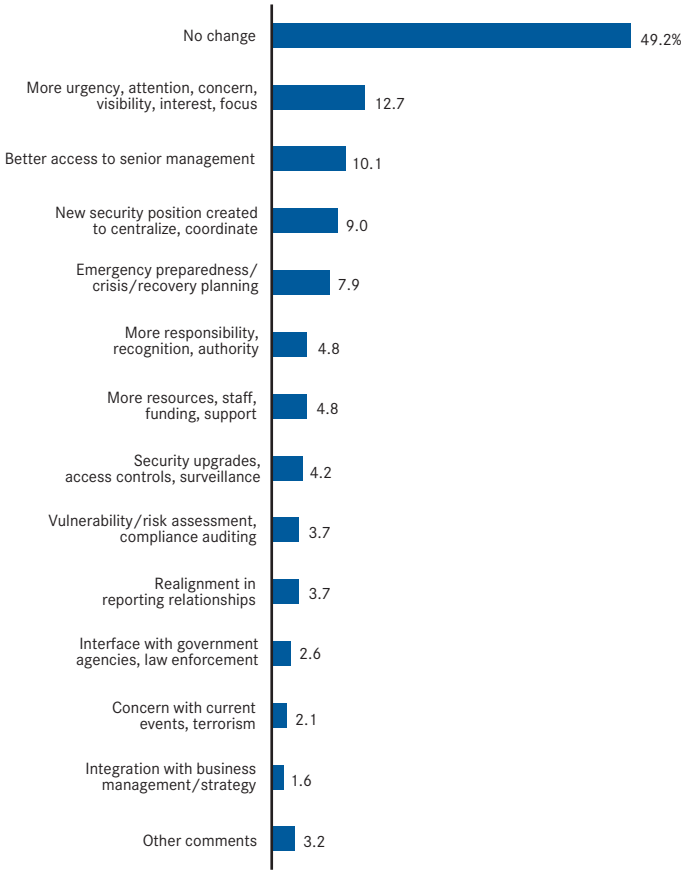
Security oversight was scattered prior to 9/11, so security issues had never been addressed holistically in most companies. Some companies have chosen to totally consolidate responsibility for security management, creating a new position of chief security officer who reports to top management and works closely with the corporate risk manager and IT director to align all aspects of security. Other companies vested the EH&S or risk management office with responsibility for security, or effected some combination of the two strategies. Security management has clearly gained stature and recognition as a vital business function.

When security directors were asked how the accountability for security issues had changed in their companies, just under half (49 percent) reported no change at all. Changes in corporate organization charts appeared to be relatively rare. Some 9 percent of companies have created a new executive position to centralize and coordinate security, and 4 percent have realigned their reporting relationships.

Most of the changes mentioned are subtle, and have to do with increased priority placed on security issues in their company's management. For example, 13 percent of security directors noted an increased urgency and visibility for security issues; 10 percent reported having better access to senior management; 5 percent enjoyed more recognition and authority; and 5 percent have received more resources. Other security directors found there was a new stress on procedures: 8 percent saw more emphasis on emergency preparedness and crisis management; 4 percent reported security upgrades; and 4 percent saw more concern with risk assessment and compliance auditing.

Most companies report no change in accountability for security since 9/11

"Since the events of September 11, 2001, how has the accountability for security issues in your company changed?"



Number of respondents: 189

Note: Summary coded from open-ended responses.

Crisis Management Teams

Many companies reexamined their security operations in the wake of 9/11. Most companies, however, have not made dramatic changes in the organization of their security operations as a result of these deliberations.

Formation of a security oversight and emergency-response team was one of the first actions taken by many of the companies interviewed. Including executives representing the security, EH&S, business continuity, communications, human resources, legal, insurance, and other relevant functions, these groups were generally charged with:

- reviewing existing security measures
- analyzing security risks
- aligning security policies and processes for all operations
- evaluating physical and IT security needs for the short and long term
- recommending changes in the corporate structure to strengthen emergency response capabilities
- recommending capital improvements to cope with the increased threat

These groups continue to function actively, driving integration of security throughout the corporation.

The following steps were generally taken to enhance physical security:

- strengthening facility perimeters
- increasing uniformed security protection
- installing or upgrading identification and surveillance systems
- limiting facility access
- increasing security training and drills
- hardening physical security

Many companies have established crisis operations centers to be activated during severe emergencies or potential crises and to serve as a clearinghouse for all aspects of emergency response.

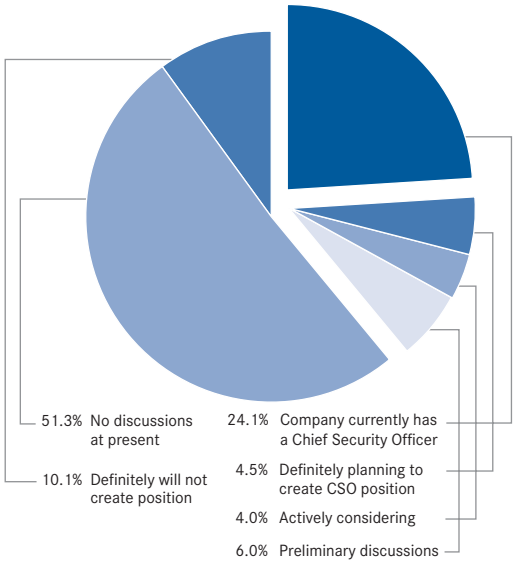
Creating the CSO Position

In the survey of security directors, 24 percent reported that their company currently has the position of CSO. (It should be noted, however, that none of the security directors surveyed had this exact title.)

Most of the companies without a CSO position do not appear to have much interest in creating one. As of 2003, only 5 percent of companies overall said they were definitely planning to create the position; 4 percent were actively considering the idea; and 6 percent were engaged in preliminary discussions. Over half of all companies (51 percent) were not discussing the idea at the time, and 10 percent had definitely decided not to create the position.

When asked which kinds of experience are most valued in a CSO, the protective services are still given pride of place. Security directors were asked to rank four kinds of experience on a scale of 1 to 4 in terms of their importance (1 being most important) as preparation for the CSO position. Military and police work finished first, with an average rank of 1.99, followed by strategic business management (2.37), finance and risk management (2.57), and information technology (3.07).

Most companies don't plan to have a Chief Security Officer



Number of respondents: 199

Companies in critical industries are more likely to have a CSO than those in non-critical industries (29 vs. 19 percent), suggesting that centralization of the security function is especially important in industries where security is most vital. Domestic companies are also more likely to have a CSO than multinationals (32 percent vs. 18 percent).

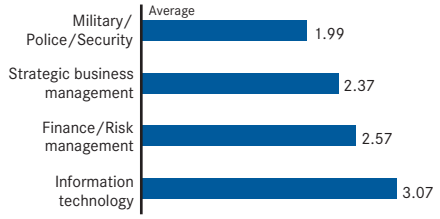
The position of Chief Security Officer (CSO) is much more common in smaller companies. While 41 percent of companies under $500 million in sales have a CSO, this proportion drops to 27 percent in companies between a half-billion and one billion dollars, 17 percent in companies between one and five billion dollars, and only 12 percent in companies over $5 billion in revenues.

The debate in the security profession over whether to create a CSO position appears to be having more of an impact on larger companies, however. Looking only at companies that do not have a CSO, over one-fifth of companies above the $1 billion in mark are considering creating the position of CSO, almost twice the 12 percent of companies below the $1 billion level that are considering the position.

Security operations are clearly more centralized in smaller companies. We believe this is probably because organizational silos and senior-level executive positions are more likely to proliferate in larger companies, making it more difficult to consolidate security authority behind a single individual in the person of a CSO. Of course, one could also argue that this proliferation is precisely why a CSO might be needed to bring order out of this potential for organizational chaos.

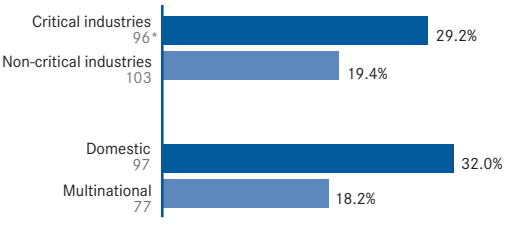
Protective service experience is most valued in a CSO

"Please rank the importance of each of the following kinds of experience as preparation for the position of Chief Security Officer, from 1 for most important to 4 for least important."



Number of respondents: 197

Companies in critical industries and domestic companies are most likely to have a CSO



* Number of respondents

CSOs are more common in smaller companies…

Percentage of companies with CSO

Sales level	Percentage	Number of respondents
Under $500 million	40.7%	54
$500 million to $1 billion	27.3	33
$1 billion to $5 billion	17.2	58
Over $5 billion	11.8	51

…but larger companies are more likely to be considering the CSO option

Percentage of companies discussing creation of CSO position

Sales level	Percentage	Number of respondents*
Under $500 million	12.5%	32
$500 million to $1 billion	12.0	25
$1 billion to $5 billion	24.9	48
Over $5 billion	20.0	45

* Asked only companies that do not currently have a CSO.

As one would expect, CSOs are more likely than other security directors to report to top management. A total of 43 percent report to a C-suite executive, compared to 27 percent of security directors in companies that had no interest in creating the CSO position. In companies that did not have a CSO but were considering creating the position, 43 percent report to a C-level executive, the same as in companies that already have a CSO. However, 28 percent of CSOs report to the very top level (CEO or COO), compared to only 11 percent of security directors in companies that are considering whether to create the CSO position.

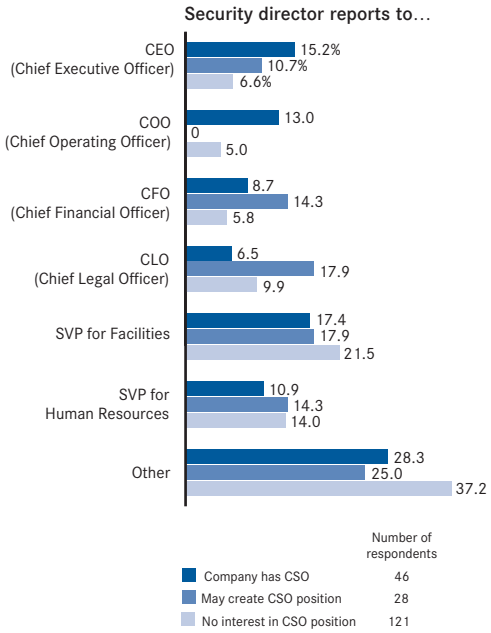
The pattern suggests that the decision to create a CSO is influenced by certain pre-existing patterns in security management. If a company's security director already reports directly to upper management, then the company is more likely to consider designating this executive as the CSO to reflect the importance of the responsibilities.

There is evidence that the CSO solution does indeed enhance the ability of security directors to implement policies within their companies. Almost three-quarters (72 percent) of CSOs agreed strongly that they had the decision-making authority they need, compared to 39 percent of security directors in companies that were considering appointing a CSO, and 45 percent in companies with no interest in the CSO position.

However, the major complaint of security executives concerns their lack of control over the purse strings, and having a CSO does not appear to ameliorate that concern. Regardless of where a company stands on the CSO issue, only about one-quarter of security directors agreed strongly that they have the financial resources they need.

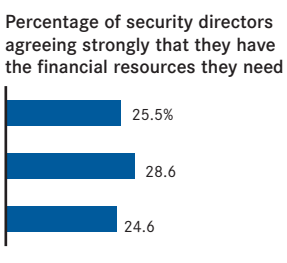
Even so, while CSOs may be just as dissatisfied with their financial clout as other security directors, they are increasing spending more rapidly. The median spending increase on security in the year after 9/11 in companies with a CSO was 5.3 percent, compared to 2.4 percent in companies with no interest in the CSO position. Spending increased most rapidly (6.7 percent) in companies that did not have a CSO but were thinking of creating the position.

CSOs are more likely to report to top management



CSOs are far more likely to have the authority they feel they need…

… but CSOs are no more likely to have the financial resources they feel they need



* Number of respondents

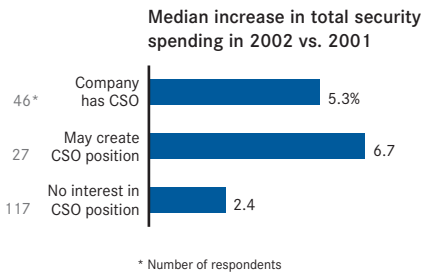
This pattern again suggests that as a company upgrades the priority it places on security, it is more likely to consider creating the position of CSO.

This point becomes even clearer if we look at the relationship between certain kinds of security sending increases and interest in creating the CSO position. Companies that were considering the creation of the position have specialized needs. They were twice as likely as other companies to report increases in spending on IT security (77 percent) or business recovery and continuity (59 percent).

We can refine this analysis even further by looking only at companies that did not have a CSO. Among the remaining companies, those that reported certain kinds of spending increases were also much more likely to report interest in the CSO position.

For example, among non-CSO companies that had increased spending on IT security, 32 percent were thinking of creating a CSO, compared to only 8 percent of non-CSO companies that had not increased IT spending. Among non-CSO companies that had increased spending on business recovery and continuity, 28 percent were discussing the CSO option, compared to 12 percent that had not increased such spending. Somewhat smaller disparities exist among non-CSO companies depending on whether or not they had increased spending on risk management (25 vs. 14 percent) or protecting buildings and facilities (22 vs. 14 percent).

Companies with CSOs are more likely to increase security spending



* Number of respondents

The conclusion seems inescapable: interest in creating a CSO is driven by a higher profile for security concerns within a company. As the security director becomes more accountable to the C-suite, and spending increases on specialized concerns like IT security and business recovery, senior management is more likely to consider the CSO option as a means to improve the coordination and effectiveness of security management.

Table 2

Companies discussing a CSO position have specialized spending needs…

Percentage of companies reporting increase in spending on…	Company has CSO	May create CSO position	No interest in CSO position
IT security	34.1%	77.3%	38.7%
Business recovery and continuity	28.2	59.1	34.3
Insurance/financial risk management	36.8	50.0	32.9
Protecting buildings and facilities	56.8	64.0	50.0
Executive security	14.3	22.7	18.3
Biological/chemical/ radiological hazards	16.7	21.7	23.4
Background investigations	22.0	25.0	25.2
Number of respondents	47	27	122

… compared to other companies without a CSO

If companies without a CSO are spending more on…	May create CSO position	Number of respondents
IT security	32.1%	53
Business recovery and continuity	27.7	47
Insurance/financial risk management	25.0	36
Protecting buildings and facilities	22.2	72
Executive security	20.0	25
Biological/chemical/radiological hazards	18.5	27
Background investigations	18.2	33

If companies without a CSO are spending the same or less on…	May create CSO position	Number of respondents
IT security	8.1%	62
Business recovery and continuity	12.2	74
Insurance/financial risk management	14.1	64
Protecting buildings and facilities	13.8	65
Executive security	16.0	106
Biological/chemical/radiological hazards	20.0	90
Background investigations	18.4	98

Spending
on Corporate Security

Except for risk management and insurance, corporate spending on security has increased only moderately since 9/11.

The heightened concern over corporate security since September 11, 2001 occurred in a difficult economic climate, which discouraged major new commitments of funds. Large-scale capital improvements that could not demonstrate an immediate return on investment were a particularly tough sell to management.

Thus, the perceived need to upgrade corporate security clashed with the perceived need to control expenses until the economy recovered. There have been sharp increases in spending on unavoidable costs involving insurance and risk management, but relatively modest increases in security spending overall. The biggest increases have been concentrated among large multi-nationals and companies in critical industries, which are perceived to have the highest exposure to risk.

Despite the centralization of security operations in smaller companies, they have more difficulty than larger companies finding the resources to meet their current security challenges. The gap in financial resources is having important implications for the restructuring of security operations since the terrorist attacks of September 11, 2001. Since that date, larger companies have been expanding their security operations more rapidly than smaller companies, making the existing gap in security capability that much larger.

Financial constraints impose more of a burden on smaller companies in terms of meeting their security needs. They pay much lower salaries to their security executives; pay a higher share of revenues for security expenditures; and are less likely to feel that their security spending is adequate. Smaller companies are also less prepared than larger companies to deal with IT disruptions that might necessitate activation of a disaster recovery or business continuity program.

Defining Security

In the surveys discussed in this report, the definition of "security" (with regard to spending and procedures) was left up to the respondent. It was clear from the pattern of answers received that security directors and senior managing executives define "security" primarily in terms of physical security, i.e. the protection of people, goods, and facilities. Except where otherwise indicated (as in the surveys of IT security officers and risk managers), the survey data should be interpreted in this light.

A Permanent Increase in Spending

Security spending jumped immediately after 9/11, as many companies tightened the security perimeter controlling access to their facilities. Among the most common changes were hiring additional guards and installing surveillance cameras, turnstiles, and other mechanisms at entry points. These upgrades were especially common in New York City (particularly Manhattan) and the Washington, D.C. area, the two regions attacked on 9/11 and considered most at risk of continued terrorist activity.

There was some uncertainty, however, as to whether the increases in spending were merely a temporary response to a time-bounded emergency or represented a more permanent increase in the level of security spending, with implications for corporate budgets going forward. The survey results indicate that for most companies, security spending has increased and the increase appears to be permanent.

Security directors were asked which of four statements came closest to describing their company's spending since 9/11. Roughly one-third of companies said that their spending was not affected in any significant way, leaving two-thirds reporting an increase. Some 13 percent reported a spike in spending, i.e., a temporary increase that was expected to recede in the future. Another one-third of companies said that spending hit a new, higher plateau after 9/11, but they did not expect additional increases in the future. Finally, 18 percent said that their spending on security would continue to increase for the next several years.

Adding together the last two categories, just over half (52 percent) of companies reported a permanent increase in their level of security spending following 9/11. However, there is a considerable difference between companies in critical and non-critical industries. In the critical industries, 56 percent of companies reported a permanent increase, vs. 39 percent not reporting a permanent increase. In the non-critical industries, the division is much more even: 48 percent reported a permanent increase, while 52 percent did not.

There are major differences among specific industries with regard to the trend in security spending. Over two-thirds (71 percent) of companies in the energy and utilities industry reported a permanent increase, followed by 62 percent of companies in the financial services industry. Smaller proportions of companies reported a permanent increase in security spending in the technology sector (47 percent), healthcare (46 percent), retail and wholesale trade (42 percent), and manufacturing (38 percent).

About half of companies report a permanent increase in security spending

Which of these statements comes closest to your view about your company's spending on security-related concerns since September 11, 2001?

	All companies	Critical industries	Non-critical industries
Our company's spending on security has not been affected in any significant way	32.2%	27.1%	36.9%
Our company's spending on security has increased on a temporary basis, but it will probably decline in the future	13.1	11.5	14.6
Our company's spending on security will continue at a higher level than it was prior to September 11, 2001, but we do not anticipate significant future increases in the level of security spending	33.7	43.8	24.3
Our company's spending on security will continue to increase every year for the next several years	18.1	12.5	23.3
None of the above	3.0	5.2	1.0
Number of respondents	199	96	103

Utilities and financial companies report a permanent increase in security spending

Which of these statements comes closest to your view about your company's spending on security-related concerns since September 11, 2001?

	Energy	Finance	Digital	Health	Trade	Manufacturing
Our company's spending on security has not been affected in any significant way	11.8%	27.6%	35.3%	28.6%	50.0%	41.4%
Our company's spending on security has increased on a temporary basis, but it will probably decline in the future	11.8	10.3	5.9	17.9	8.3	20.7
Our company's spending on security will continue at a higher level than it was prior to September 11, 2001, but we do not anticipate significant future increases in the level of security spending	58.8	51.7	35.3	32.1	25.0	24.1
Our company's spending on security will continue to increase every year for the next several years	11.8	10.3	11.8	14.3	16.7	13.8
None of the above	5.9	0.0	11.8	7.1	0.0	0.0
Number of respondents	17	29	17	28	12	29

A Modest Increase Overall

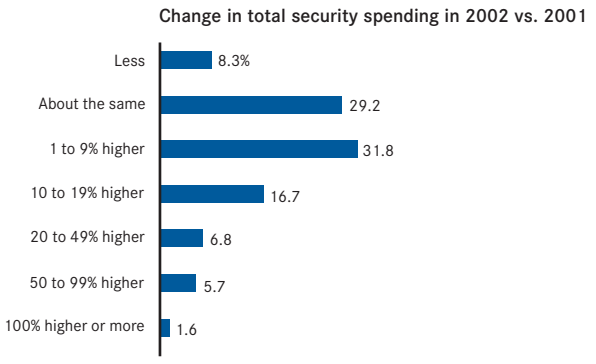
Although most security directors reported a permanent increase in spending, the size of the increase was not very large on the whole. The median increase across all companies in the year following 9/11 was only 4 percent, a relatively modest figure. However, this aggregate statistic fails to capture the wide range of change in security spending since 2001.

The companies cluster in three groups, each comprising approximately one-third of the sample.

- The first group reported no increase: 8 percent actually reported spending less in 2002 than in 2001, and 29 percent reported spending about the same on security.
- The second group of 32 percent reported moderate increases between 1 and 9 percent.
- The remaining companies (31 percent) reported increases of 10 percent or more. A small group of companies increased spending dramatically: 14 percent are spending at least 20 percent more on security per year, and 7 percent have stepped up their spending by 50 percent or more.

Larger multinational companies and firms in critical industries reported bigger increases in security spending than smaller domestic companies. The median increase for multinationals (defined as companies receiving 10 percent or more of their sales overseas) was 4.7 percent, vs. 3.6 percent for domestic companies.

Most companies report a modest increase in overall security spending



Median increase: 4%
Number of respondents: 192
Note: "Don't know" eliminated.

The median increase for companies with 10,000 or more employees was 5.4 percent, compared to 3 percent for companies below that staffing level.

For companies with sales over one billion dollars, the median increase was 5.5 percent, vs. 1.4 percent for companies below that level of sales. Under half (48 percent) of companies with less than $500 million in sales reported an increase in their security spending in 2002. This proportion rises to 61 percent among companies between a half-billion and one billion dollars in sales; 68 percent for companies between one and five billion dollars; and 71 percent for companies with annual revenues of $5 billion or more.

The level of increase was quite consistent throughout the critical industries, where the median increases for the four major industry groups cluster in the 4 to 5 percent range. In the non-critical sector, the median increase for manufacturing companies was 3.8 percent, compared to 1.3 percent in retail and wholesale trade.

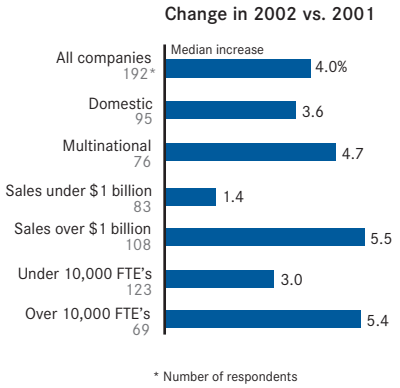
Larger companies are expanding their security operations more rapidly

Percentage of companies increasing total security spending in 2002

Sales level	Percentage	Number of respondents
Under $500 million	48.0%	50
$500 million to $1 billion	60.6	33
$1 billion to $5 billion	67.8	56
Over $5 billion	70.6	51

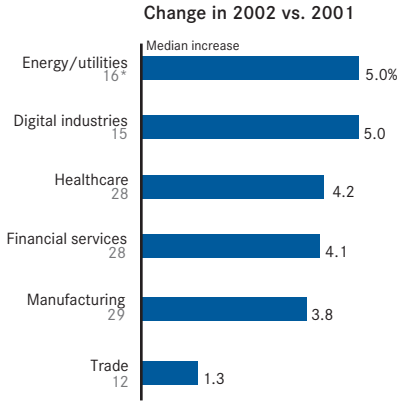
Note: "Don't know" eliminated.

Large multinationals report bigger increases in overall security spending



* Number of respondents

Most industries report a modest increase in security spending



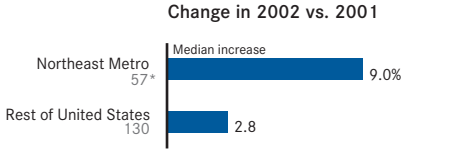
* Number of respondents

Security Spending in the Northeast

Geographic location is one of the strongest predictors of increased spending on corporate security. Companies were assigned to a region based on the location of their headquarters.

Security spending is increasing much more rapidly in the metropolitan Northeast, defined as a headquarters location in the Boston, New York, Philadelphia, or Washington metropolitan areas. In the Northeast Metro corridor, the median increase for total security spending in the year after 9/11 was 9 percent, compared to 2.8 percent in the rest of the country. Clearly, the direct experience with the terror attacks of 9/11 prompted a greater sense of urgency in the Northeast compared to the rest of the country.

Security spending is increasing most rapidly in Northeast Metro areas...



"Northeast Metro" is defined as companies having headquarters in the Boston, New York, Philadelphia, and Washington, DC metropolitan areas.

*Number of respondents

Smaller Companies Bear a Larger Burden

In purely dollar terms, security spending is not a major budget item for most companies. Security directors were asked to estimate the total spending on security by their companies in the United States. (A preliminary focus group determined that estimating security spending overseas would be extremely difficult and very inaccurate, so the study did not attempt to estimate security spending outside the country.)

The median security spending for all companies in 2002 was $4.4 million. Fifteen percent of all companies reported spending over $10 million a year on security, while 29 percent reported spending less than $1 million.

Companies with at least $5 billion in sales reported spending a median of $7.1 million a year on security, compared to a median of $5.3 million for companies between $1 billion and $5 billion sales, $3.5 million for companies between a half-billion and a billion in sales, and under $1 million for companies with less than $500 million in sales. Of the companies with over $5 billion in sales, 30 percent reported spending at least $10 million a year on security.

Larger companies spend more on security

Total spending on security	Under $500 million	$500 million–$1 billion	$1 billion–$5 billion	Over $5 billion	All companies
Less than $1 million	52.9%	37.5%	19.6%	10.0%	28.8%
$1 million to $9 million	45.1	50.0	66.1	60.0	56.0
$10 million or more	2.0	12.5	14.3	30.0	15.1
Median	<$1 million	$3.5 million	$5.3 million	$7.1 million	$4.4 million
Number of respondents	51	32	56	50	189

Note: "Don't know" eliminated.

Security spending is more of a burden for smaller companies

Security spending as a percentage of annual sales

Sales level	Less than 1%	1 to 1.9%	2 to 2.9%	3% or more	Number of respondents
Under $500 million	43.6%	38.5%	12.8%	5.1%	39
$500 million to $1 billion	51.9	25.9	7.4	14.8	27
$1 billion to $5 billion	76.1	15.2	6.5	2.2	46
Over $5 billion	71.1	20.0	6.7	2.2	45
All companies	62.7	24.1	8.2	5.0	157

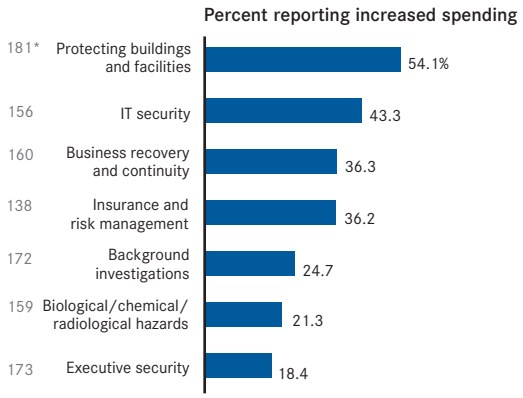
There was considerable variation among companies in the amount of security spending as a percentage of annual sales. While 63 percent reported spending less than one percent of sales on security, 5 percent of companies spent 3 percent or more of their sales on security.

One would of course expect security spending to be higher in dollar terms among the larger companies. And we have already seen that the recent increase in security spending was generally concentrated among larger companies. However, relative to the size of the company, the total cost of security appears to be more of a burden for smaller companies than for larger firms.

Security spending is more of a burden for smaller companies when expressed as a percentage of annual sales. Some 56 percent of companies with less than $500 million in sales spent 1 percent or more of their annual revenues on security. This proportion drops to 48 percent for companies between a half-billion dollars and one billion dollars in sales, and about one-quarter of firms with over one billion dollars in sales.

Security directors were asked to estimate the degree of change in spending in a variety of security categories. Over half of companies (54 percent) reported an increase in spending on protecting buildings and facilities. Spending on IT security was reported to be rising by 43 percent of companies, followed by business recovery and continuity (36 percent) and insurance and risk management (36 percent).

Most companies have increased spending on buildings and facilities



* Number of respondents

Note: "Don't know" eliminated.

The Cost of IT Security

Despite its importance, IT security is a relatively low-budget item in many companies. Over half of all companies in the sample of IT security officers (55 percent) reported spending less than $1 million per year on IT security, and this proportion rose to 89 percent in companies with under $1 billion in sales. Larger companies devote more resources to this line item. Among companies with $1 billion to $5 billion in sales, over one-third (35 percent) spent at least $1 million per year on IT security. Companies with over $5 billion in sales spent at much higher levels, with 44 percent spending $5 million or more on IT security per year.

Benchmarking is the most common means of determining spending on IT security, used by 40 percent of companies, but a close second is affordability: one-third of companies said they spent "as much as we can afford." Other common guidelines are recommendations from consultants (19 percent) and the cost of previous incidents (14 percent).

The median company spent 1.9 percent of its total IT budget on IT security. The median was considerably higher for companies in the critical industries (2.4 percent) than companies in the non-critical industries (1.6 percent).

As with security spending in general, IT security tends to be more of a burden for smaller companies. Among companies with under $1 billion in sales, 39 percent reported spending 5 percent or more of their IT budget on security compared to 14 percent of companies with over $1 billion in sales.

Most companies spend under $1 million a year on IT security

IT security spending	Under $1 billion	$1 billion–$5 billion	Over $5 billion	All companies
Less than $1 million	88.9%	65.2%	11.1%	54.5%
$1 million to $5 million	11.1	34.8	44.4	29.9
$5 million or more	0.0	0.0	44.4	15.6
Number of respondents	27	23	27	77

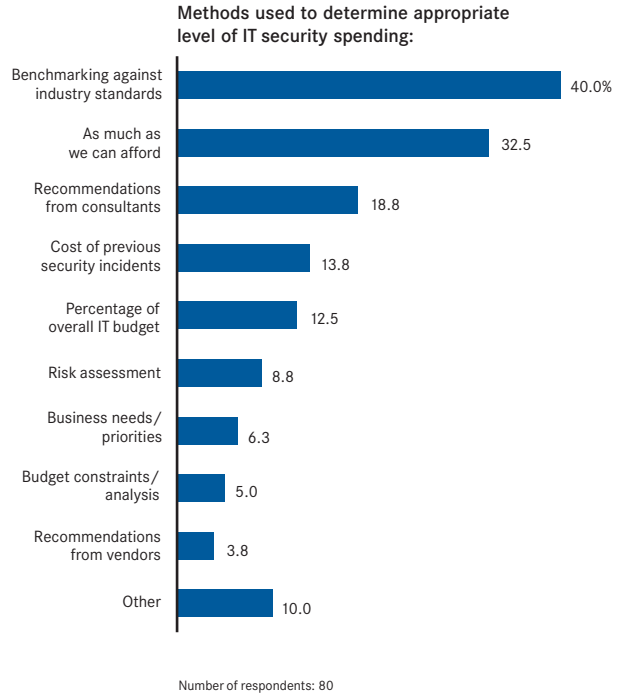
Note: "Don't know" eliminated.

Domestic companies also spent relatively more on security, with 35 percent spending at least 5 percent of their IT budget on security, compared to 13 percent of multinationals.

There is a wide disparity among companies in the rate of spending increase on IT security. The median increase in the year after 9/11 was only 1.9 percent, but this figure hides an enormous amount of variation. Almost half of all companies (47 percent) did not increase spending on IT security; on the other hand, 36 percent increased spending by 10 percent or more, and 21 percent increased it by at least 20 percent.

The increases are pronounced in the critical industries, where 28 percent of companies increased IT security spending by 20 percent or more, compared to 15 percent of companies in non-critical industries. Larger companies were also more likely to increase IT security spending: 31 percent of companies with 10,000 or more employees stepped up IT security spending by 20 percent or more compared to 14 percent of companies below that payroll level.

Benchmarking and affordability drive IT security spending



IT security is more of a burden for smaller domestic companies

IT security spending as percentage of IT budget

	Less than 1%	1% to 1.9%	2% to 4.9%	5% to 9.9%	10% or more	Median	Number of respondents
All companies	**28.0%**	**26.7%**	**22.7%**	**16.0%**	**6.7%**	1.9%	75
Critical	22.2	25.0	27.8	13.9	11.1	2.4	36
Non-critical	33.3	28.2	17.9	17.9	2.6	1.6	39
Domestic	23.5	17.6	23.5	23.5	11.8	3.2	34
Multinational	28.2	35.9	23.1	10.3	2.6	1.6	39
Under $1 billion sales	23.1	19.2	19.2	23.1	15.4	2.8	26
Over $1 billion sales	30.6	30.6	24.5	12.2	2.0	1.7	49
Under 10,000 FTE's	23.8	28.6	21.4	14.3	11.9	2.0	42
Over 10,000 FTE's	33.3	24.2	24.2	18.2	0.0	1.8	33

Note: "Don't know" eliminated.

IT security spending is increasing in critical industries

Change in 2002 vs. 2001

	Less	Same	1–9% higher	10–19% higher	20–49% higher	50% + higher	Median	Number of respondents
All companies	**7.9%**	**39.5%**	**17.1%**	**14.5%**	**10.5%**	**10.5%**	**1.9%**	**76**
Critical	8.3	36.1	16.7	11.1	13.9	13.9	4.2	36
Non-critical	7.5	42.5	17.5	17.5	7.5	7.5	0.7	40
Domestic	3.0	33.3	21.2	21.2	15.2	6.1	7.1	33
Multinational	12.5	42.5	12.5	10.0	7.5	15.0	0.0	40
Under $1 billion sales	3.7	40.7	22.2	22.2	0.0	11.1	3.3	27
Over $1 billion sales	10.2	38.8	14.3	10.2	16.3	10.2	1.4	49
Under 10,000 FTE's	4.5	45.4	18.2	18.2	4.5	9.1	0.6	44
Over 10,000 FTE's	12.5	31.3	15.6	9.4	18.8	12.5	5.0	32

Note: "Don't know" eliminated.

The Business Case for Security

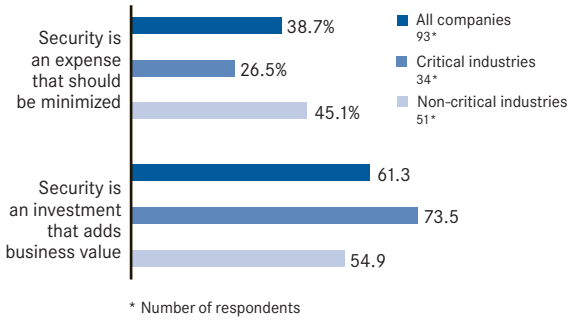
Security has a traditional disadvantage of being viewed primarily as a cost rather than as a source of business value to a company. Given that a direct link to the company's revenue generation is at the root of much corporate decision-making, the absence of any such link for security makes it a difficult sell to management. The notion of a "Triple Bottom Line," reflecting economic, social, and environmental impacts, could one day benefit thinking about corporate security in the way that it now guides thinking in citizenship and sustainability.

In order to determine whether chief executives in the mid-market sector believe in the business case for security, they were asked a forced-choice question: "Which of these statements comes closest to your views about spending on your company's security?"

- "Security is an expense that should be minimized."
- "Security is an investment that increases business value."

In the sample of chief executives, 61 percent endorsed the business case argument that security provides value for the firm that yields a positive return on investment, while 39 percent believed that security is simply a cost that should be minimized. The business case is even more strongly supported by executives in the so-called "critical industries" which are considered most vulnerable to terrorism and other security problems. Executives from companies in the critical industries endorsed the business case argument by almost a three-to-one margin (74 to 26 percent), while sentiment was much more evenly divided among executives in the non-critical industries (55 to 45 percent).

Critical industries accept the business case for security spending

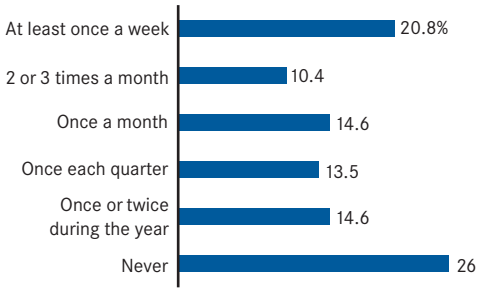


* Number of respondents

C-Suite Access and Security Spending

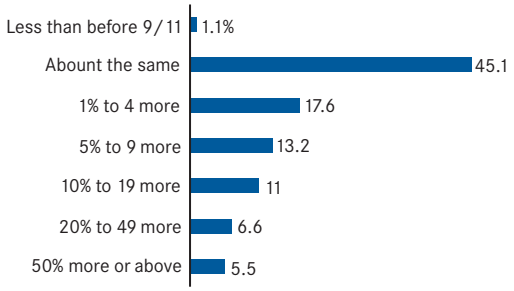
There is a wide variation in the degree of access to the C-suite that security directors enjoy. Some 21 percent of chief executives reported that they meet with their head of security at least weekly, and an additional 25 percent meet at least monthly. However, 28 percent meet with their security directors only a few times a year, and 26 percent reported that they have never met with the security chief at any time during the previous year.

During the past year, on average, how often have you met with the head of security for your company?



Number of respondents: 96

How much is your company currently spending on security on an annual basis compared to what it was spending on security prior to September 11, 2001?



Number of respondents: 91

Note: "Don't know" eliminated.

Belief in the business case (i.e., that security is a valuable investment as opposed to a cost center) strongly affects both security spending and the C-suite access enjoyed by security directors. Among the companies where the chief executive believes that security adds business value, two-thirds reported an increase in security spending since 9/11, while 61 percent of the companies run by executives who view security mainly as an expense reported no increase in spending.

The results are even more dramatic with regard to C-suite access. In companies run by executives who believe in the business case, 32 percent meet with their security directors once a week or more, and another 32 percent meet with their security directors at least once a month. On the other hand, in companies where the chief executive views security as an expense to be minimized, half of the security directors never met with their chief executive in the previous year.

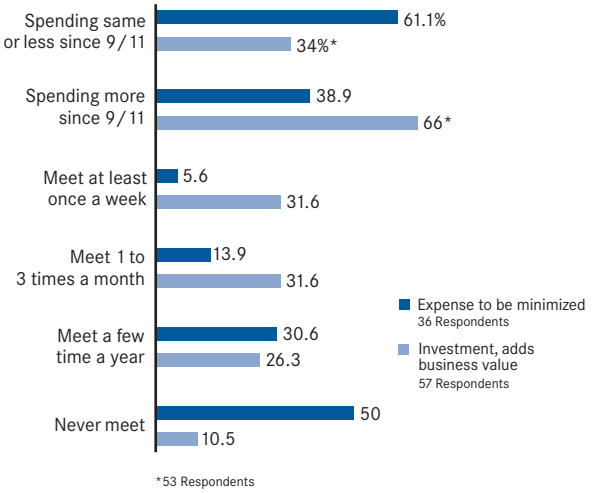
C-suite access has a direct impact on security spending. Three-quarters of the companies with weekly security meetings at the C-suite level reported an increase in security spending after 9/11, compared to only 30 percent of companies where the security director and chief executive never meet.

The size of the security spending increase is also related to the frequency of senior-level meetings. In companies with senior-level security meetings at least once a month, at least 30 percent reported an increase in spending of 10 percent or more, compared to 19 percent of companies with occasional senior-level meetings and only 9 percent of companies where the chief executive and security director never meet.

Clearly, one of the keys to effective security management is convincing the chief executive of the business case for security. The business case is the key to securing face time with senior executives and making the case for increasing security spending. This case appears to be easier to make for companies in the critical industries, where security may have a direct impact on corporate performance, and larger companies, which have more assets at risk.

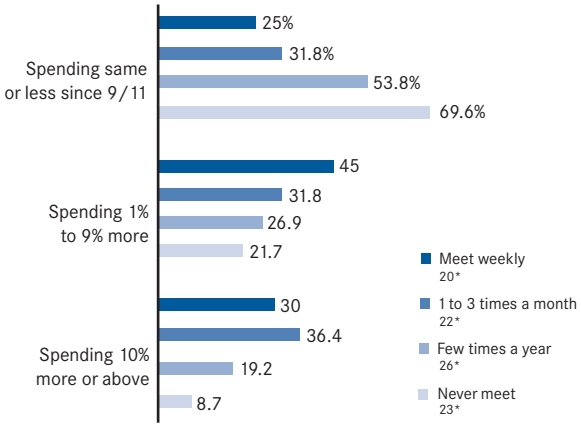
Absent an understanding of the value that security brings to the company, access to the top will be limited, because security will be viewed as a cost center that makes no contribution to the bottom line. In sum, articulating and championing the business case must be seen as an essential part of the role played by any corporate security director.

Belief in the business case enhances security spending and C-suite access



*53 Respondents

C-suite access boosts security spending

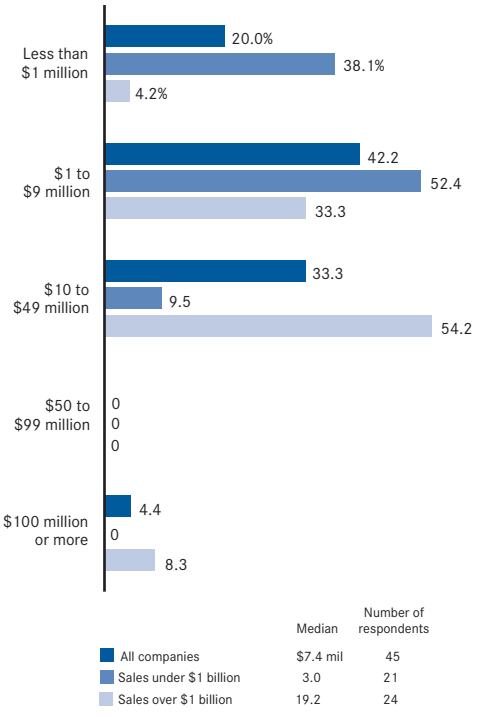


* Number of respondents

Risk Management
and Preparedness

The terrorism threat focused business' attention on areas of vulnerability not always considered prior to September 11. Many companies invested in risk analysis reviews, addressing every aspect of their operations from product security in manufacture and delivery to the location of IT operations to terrorism scenario planning and travel policies. For companies with hundreds and even thousands of installations, going beyond the immediate hardening processes to identify specific vulnerabilities at every facility was an enormous undertaking.

Most large companies spend at least $10 million per year on insurance and risk management



Note: "Don't know" eliminated.

Whether or not new risk management programs were considered necessary appears to depend largely on the company's type of business. After looking closely at their existing risk management programs, some firms felt that no new systems were necessary. Others have spent tens of millions of dollars to upgrade their risk management programs. Some had begun to plan for terrorism attacks long before 9/11. For example, several chemical companies were working as early as 1999 with the American Chemical Council and its Center for Chemical Process to develop what has become a highly respected vulnerability assessment technology for the industry.

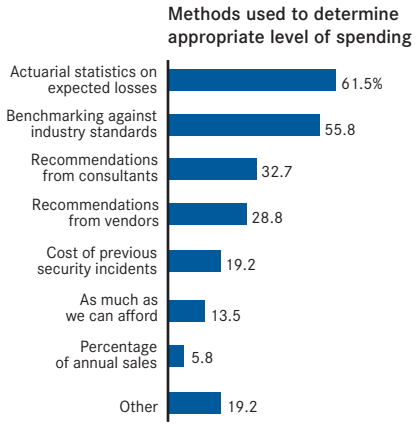
Risk Management as a Line Item

Insurance and risk management is one of the biggest single line items in a typical company's security-related spending. The median spending on insurance and risk management for all companies in the risk managers' sample was $7.4 million. The median spending was much higher for companies with more than $1 billion in sales ($19.2 million) than for companies below this sales level ($3 million). Indeed, 63 percent of companies above the billion-dollar level in sales pay at least $10 million per year for risk management, and 8 percent pay at least $100 million per year.

Actuarial data are employed by 62 percent of risk managers to gauge the appropriate level of spending. Other commonly employed tools are benchmarking against industry standards (56 percent) and recommendations from consultants (33 percent).

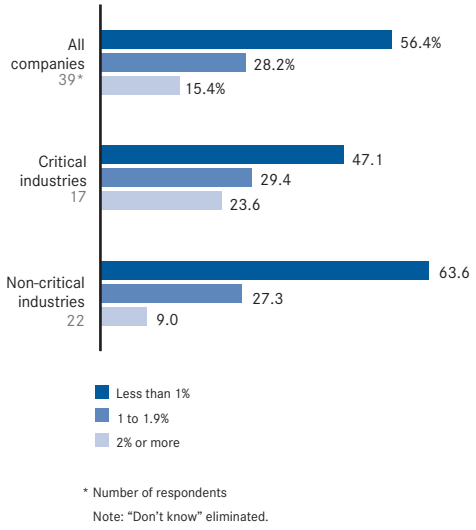
Companies in the critical industries spend a higher amount on risk management as a percentage of their annual sales. Over half (53 percent) of companies in critical industries spend 1 percent or more of their sales on risk management, compared to 36 percent of companies in non-critical industries.

Actuarial data are most common means of determining spending on risk management



Number of respondents: 52

Critical industries spend a higher percentage of their sales on risk management



* Number of respondents

Note: "Don't know" eliminated.

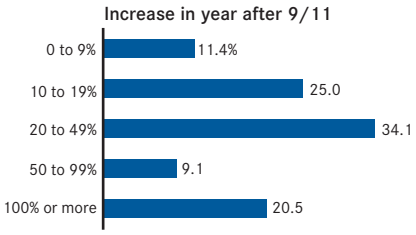
The Soaring Cost of Risk Management

Costs for insurance and risk management have been soaring because of the massive losses incurred on 9/11. To reflect the increased risk to corporate facilities and employees, insurers have dramatically raised premiums for certain kinds of coverage.

The Conference Board survey of corporate risk managers found a median increase of 33 percent in spending on insurance and risk management in the year after 9/11. Even this figure understates the severity of the costs borne by some companies. A remarkable 21 percent of risk managers reported that their costs had at least doubled from 2001 to 2002.

The increases in risk management costs were spread quite evenly across various sectors of the economy. The median increase for multinationals was 40.6 percent, compared to 26.4 percent for companies with a domestic focus.

Insurance and risk management costs are soaring



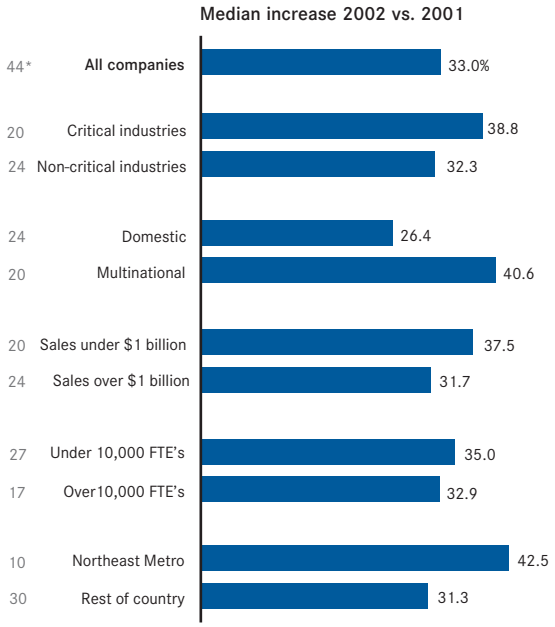
Median increase: 33%

Number of respondents: 44

Note: "Don't know" eliminated.

Geographic location is an important factor: the median increase in Northeast Metro areas was 42.5 percent, compared to 31.3 percent in the rest of the United States. Companies in critical industries reported a larger increase than those in non-critical industries (38.8 percent vs. 32.3 percent). Smaller companies reported larger increases in percentage terms than larger companies, but the differences were relatively minor.

Multinationals are bearing the largest increases in insurance and risk management costs



* Number of respondents

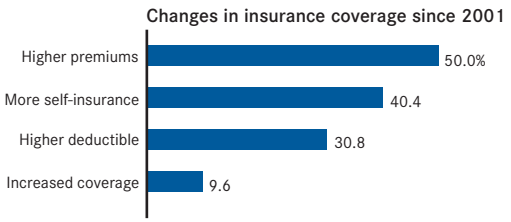
Changes in Insurance Coverage

Half of risk managers report paying higher insurance premiums since 2001, and 10 percent have increased their level of insurance coverage. The increase in insurance costs has prompted companies to assume more of the risk themselves to hold down their spending. For example, 40 percent of risk managers have increased their level of self-insurance, and 31 percent took policies with higher deductibles.

For categories of insurance that are most directly related to security threats, the biggest increases in insurance costs are being incurred by companies in critical industries, which are perceived to be most at risk. For example, the median increase in property insurance was 37.5 percent for companies in critical industries, vs. 22.1 percent in non-critical industries. For liability insurance, the median increase was 40.6 percent in critical industries compared to 13.6 percent in non-critical industries. Companies in critical industries face a median 23.8 percent rise in spending for medical insurance, vs. 9 percent for non-critical industries.

Large multinationals are facing the biggest increases in cost for property insurance. The median increase in property insurance spending for multinationals (39.3 percent) was double the rate for domestic companies (19 percent). Companies with over $1 billion in sales report a higher median increase than companies below that size (35 vs. 20 percent).

Companies bear more of the insurance risks themselves



Number of respondents: 52
Note: Multiple responses possible.

On the other hand, domestic companies face the biggest increases in costs for liability insurance and medical insurance. Health coverage is a particular problem for smaller domestic companies. The median increase in medical insurance spending was 15.7 percent for domestic companies, vs. 8.8 percent for multinationals. Companies with less than $1 billion in sales reported a much higher increase in medical costs (15.6 percent) than those over that level of sales (6.7 percent). The finding suggests that there are important economies of scale for securing cost-effective medical coverage for companies doing almost all of their business in the United States.

Business interruption coverage differs from the pattern for other security-related coverage. The median increase in both critical and non-critical sectors hovers around the 16.5 percent reported for companies overall. The key factor here appears to be the scale of the business. Multinationals reported much larger median increases in business interruption insurance costs than domestic companies (29 percent vs. 12.5 percent), and companies with 10,000 or more employees reported larger median increases than those with fewer employees (29 percent vs. 14.4 percent).

Critical industries face the biggest increases in security-related insurance costs

Median increase in 2002 vs. 2001	Property insurance	Liability insurance	Business interruption	Medical insurance
All companies	**28.1%**	**21.5%**	**16.5%**	**13.0%**
Critical industries	37.5	40.6	18.0	23.8
Non-critical industries	22.1	13.6	16.0	9.0
Domestic	19.0	27.5	12.5	15.7
Multinational	39.3	18.3	29.0	8.8
Sales under $1 billion	20.0	19.0	15.0	15.6
Sales over $1 billion	35.0	25.0	19.0	6.7
Under 10,000 FTE's	24.3	23.0	14.4	13.9
Over 10,000 FTE's	35.0	23.0	29.0	9.0

Note: "Don't know" eliminated.

Number of respondents				
All companies	40	40	38	29
Critical industries	18	18	17	12
Non-critical industries	22	22	21	17
Domestic	22	22	20	17
Multinational	18	18	18	12
Sales under $1 billion	19	19	17	16
Sales over $1 billion	21	21	21	13
Under 10,000 FTE's	25	26	24	22
Over 10,000 FTE's	15	14	14	7

Insuring Office Space

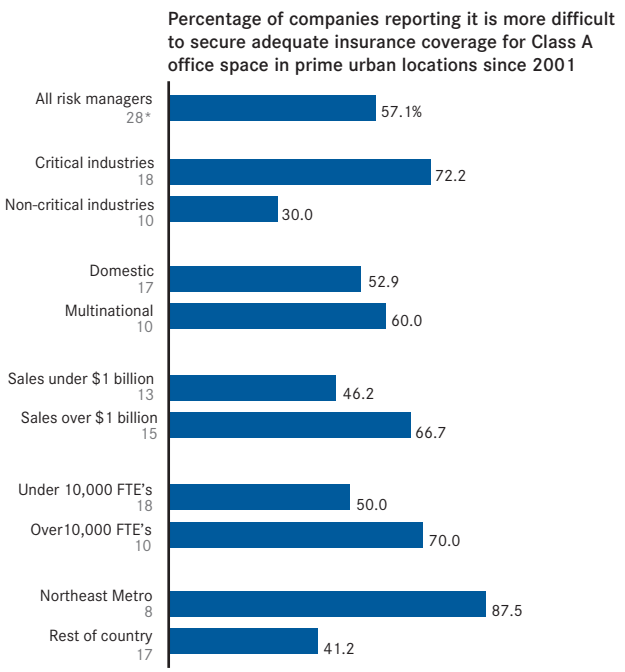
Concerns about terrorism have clearly influenced the ability of some companies to secure adequate insurance coverage since 9/11. Over half of all risk managers (57 percent) report that it is becoming more difficult to secure adequate insurance coverage for Class A office space in urban locations since 2001. (Note: this percentage excludes "don't know" responses and companies not having Class A office space in an urban location.)

This problem is most acute for companies with headquarters in the Northeast Metro region, where fully 88 percent reported increased difficulty in insuring Class A office space compared to 41 percent in the rest of the country. Companies in critical industries are much more likely to report difficulty (72 percent) than companies non-critical industries (30 percent).

Larger companies are also more likely to report a problem with office space insurance. Two-thirds of companies with $1 billion or more in sales reported that insurance for Class A urban properties is a problem, compared to 46 percent of companies below that sales level. Similarly, 70 percent of companies with 10,000 or more employees reported difficulty insuring such space compared to half of companies below that payroll level.

Direct coverage for terrorism is also becoming more difficult to secure. While 27 percent of companies have such coverage, 17 percent have been unable to renew it, and an additional 29 percent did not have it before or after 9/11. There seems to be considerable ambiguity with regard to this type of coverage: 6 percent of companies say it depends on circumstances, and 21 percent are not sure if they are covered.

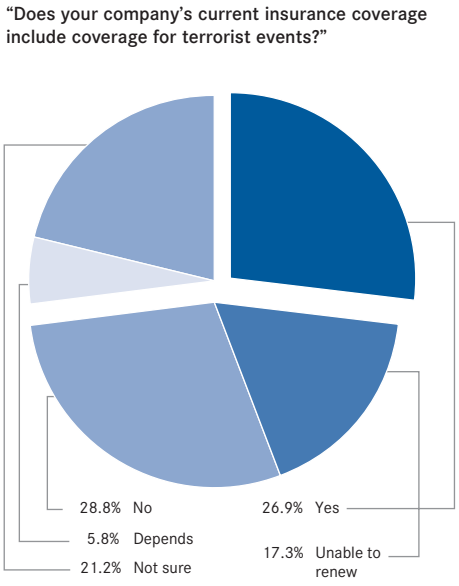
Class A office space is becoming more difficult to insure



* Number of respondents

Note: "Don't know" and "not applicable" eliminated.

Most companies lack coverage for terrorism



Number of respondents: 52

Terrorism, the Blackout, and Hurricane Isabel

Although there has not been a major terrorist incident on American soil since 9/11, there were two other events in 2003 that posed major security risks to companies: the widespread failure of the electric grid on August 14, and Hurricane Isabel in September. The study posed questions to determine the severity of the impact of each of these events.

Just under half of the companies reported that 9/11 had the most severe impact on their business, compared to 6 percent citing the blackout and 4 percent citing the hurricane. Forty percent said that none of these events had a severe impact on their business.

Which of these events had the most severe impact on the conduct of your company's business?

	All companies	Northeast Metro	Rest of U.S.A.
Terror attacks of September 11, 2001	49.5%	54.2%	44.9%
Electric blackout of August 14, 2003	6.3	12.5	4.3
Hurricane Isabel in September, 2003	4.2	12.5	1.4
None of these events had a severe impact on our company	40.0	20.8	47.8
Number of respondents	95	24	69

Which of the following problems were experienced by your company during and/or immediately after each of the following events?

All companies	Terror attacks 9/11/01	Electric blackout 8/14/03	Hurricane Isabel 9/18/03
Disruption of business travel	79.2%	20.8%	9.4%
Drop in revenues	46.9	12.5	6.3
Facility closed for business	15.6	15.6	5.2
Loss of electric power	1.0	21.9	8.3
Loss of telephone service	4.2	17.7	4.2
Loss of Internet access	4.2	16.7	4.2
Number of respondents	96	96	96
Northeast Metro			
Disruption of business travel	70.8%	29.2%	8.3%
Drop in revenues	45.8	16.7	16.7
Facility closed for business	41.7	37.5	12.5
Loss of electric power	0.0	33.3	25.0
Loss of telephone service	8.3	37.5	12.5
Loss of Internet access	8.3	37.5	12.5
Number of respondents	24	24	24
Rest of U.S.A.			
Disruption of business travel	81.2%	17.4%	8.7%
Drop in revenues	46.4	10.1	2.9
Facility closed for business	5.8	8.7	2.9
Loss of electric power	1.4	17.4	2.9
Loss of telephone service	1.4	10.1	1.4
Loss of Internet access	1.4	8.7	1.4
Number of respondents	69	69	69

Note: Multiple responses possible.

The Northeast Metro region had the most severe impact from all three events. While 48 percent of executives outside this region said that none of the three events had a severe impact, only 21 percent of those in the Northeast Metro region said the same.

However, what is most striking about 9/11 is its truly national impact. While 54 percent of Northeastern companies said the terror strikes had the most severe impact, 45 percent of executives in the rest of the country said the same thing.

The loss of life and physical damage caused by the terror strikes were traumatic and unprecedented. However, the key to understanding the economic cost of 9/11 is its extensive impact on the most fundamental business operations, which was truly nationwide in scope. Fully 79 percent of companies reported a disruption in business travel due to the terror attacks, and 47 percent reported a drop in revenues; it is very striking that there is no major regional disparity in this pattern.

The nationwide shutdown of the air transportation system for a week left many business travelers (and many senior executives) stranded. The interruption in financial trading, slowing in the supply chain, and catastrophic collapse of demand in Lower Manhattan exacted an economic toll as well, which rippled through the national economy.

In the nation as a whole, 16 percent of businesses reported that they closed as a result of the power outage, the same as during the terror attacks. In some respects, the blackout had a greater impact on company operations.

As a result of the blackout, 22 percent of companies lost electric power, 18 percent lost telephone service, and 17 percent lost Internet access; these percentages are all in the low single digits for the terror strikes. While the loss of these utility functions is clearly a nuisance, companies appear to rebound from such events without too much difficulty (assuming the outages are not long-lived).

Breaking down the data by region further highlights the unique severity of 9/11. In the Northeast Metro region, one-third of businesses lost electricity, Internet access, and phone service during the blackout; and substantial proportions (from 13 percent to one-quarter) report losing these services during Hurricane Isabel. By contrast, less than 10 percent of companies in the Northeast experienced these problems as a result of the terror attacks. Comparable percentages of Northeastern businesses closed both as a result of 9/11 and the blackout (42 percent vs. 38 percent).

The most significant differences are seen in the disruption of business travel (71 percent from 9/11 vs. 21 percent in the blackout) and a drop in revenues (47 percent vs. 13 percent). These problems account for the severity of the impact of the terror strikes. Chief executives consider these economic impacts even more important than the temporary loss of networked services in the conduct of company operations. Future assessment of corporate vulnerabilities should bear such findings in mind.

Smaller Companies are Less Prepared

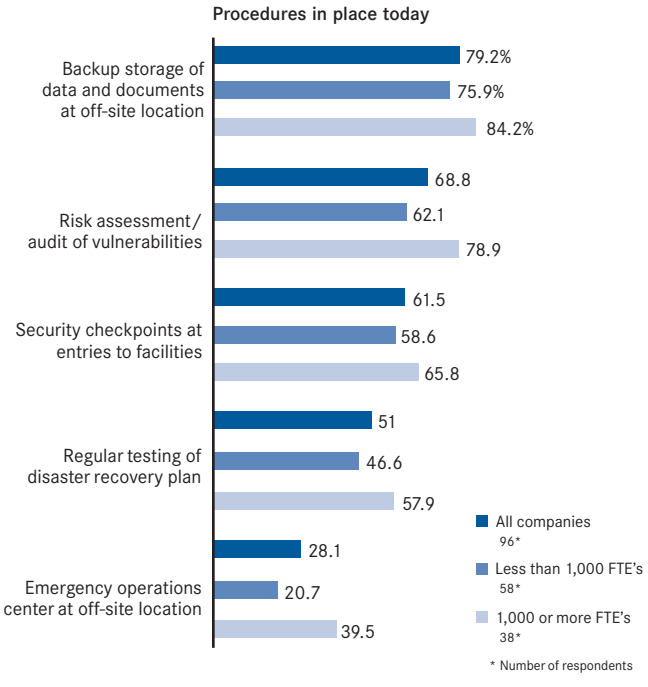
In order to gauge the level of preparedness among mid-market companies, a variety of questions were asked to ascertain the involvement of boards of directors in security policies and the level of preparedness for emergencies. In general, the smaller the company, the less likely the board is to establish written security guidelines, and the less likely the company has procedures in place to handle security challenges.

Looking at larger mid-market companies (with 1,000 or more FTE's), 71 percent have board-approved written guidelines on disaster recovery and business continuity, compared to 43 percent of smaller companies (with less than 1,000 FTE's). Half of the larger companies have written board policies on emergency preparedness, compared to 41 percent of the smaller companies. Interestingly, corporate boards are more involved in setting policy for crises than for routine (non-emergency) security procedures; only about one-third of mid-market companies, regardless of size, report that the board has approved written policies on routine security.

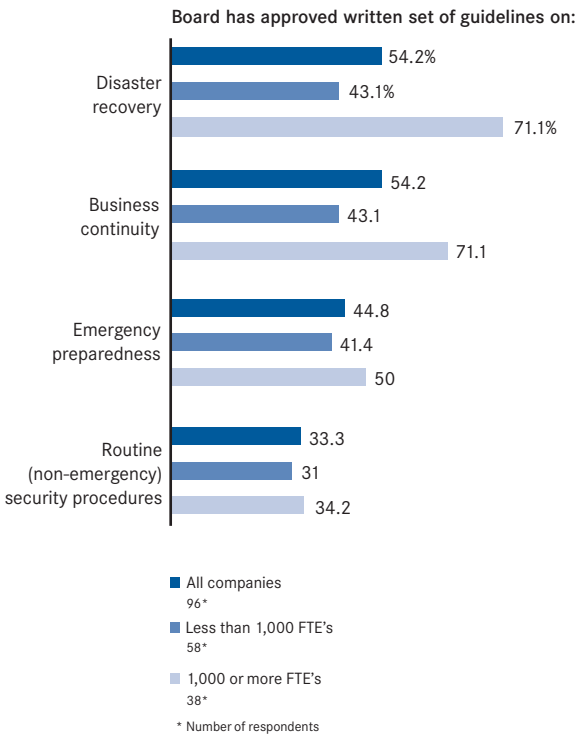
Similarly, smaller companies are less prepared for emergencies. Larger companies are more likely to have backup storage at an off-site location (84 percent, vs. 76 percent for smaller companies); conduct a risk assessment or audit of vulnerabilities (79 percent vs. 62 percent); and have security checkpoints (66 percent vs. 59 percent).

The biggest (and most alarming) gap is with regard to having an off-site emergency operations center: 40 percent of larger companies have established such a facility, compared to only 21 percent of smaller companies. This finding suggests that many smaller companies would have difficulty conducting their business in the event of a prolonged outage or closure at their primary facility. Given the vital role that smaller mid-market companies play in the economy, the economic impact could be quite severe indeed should another terrorist episode of the scale of 9/11 unfold in a heavily populated area.

Smaller companies are less prepared for emergencies



Smaller companies lack written policies approved by the board

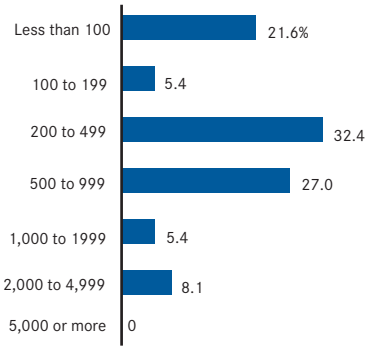


The Desirability of Dispersing Facilities

Risk managers were asked to estimate the maximum number of employees they consider prudent to locate in a single facility. The median was 425. Only 14 percent of risk managers consider it prudent to situate 1,000 or more employees at a single location. If companies were to act on these perceptions, the recent trend toward consolidation of facilities in downtown office towers and suburban office parks might give way to a desire to disperse employees and operations.

However, most companies do not report plans to disperse their facilities. Only 5 percent of security directors indicated that their companies are definitely planning to rent, buy, or construct additional facilities to disperse employees for security reasons, and 8 percent of companies are planning additional facilities to disperse operations. An additional 10 percent of companies are discussing the possibility of dispersing employees for security reasons, and another 15 percent are discussing whether to disperse operations. That leaves over-three quarters of companies that are not currently discussing the idea of dispersing facilities.

Maximum number of employees considered prudent to locate in a single facility

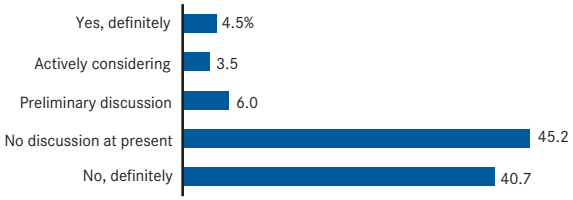


Median: 425
Number of respondents: 37
Note: "Don't know" eliminated.

Given the lack of interest in additional facilities, it is not surprising that very few companies are planning to spend much money on construction for security reasons during the next five years. Almost two-thirds of security directors (65 percent) expect to spend less than $1 million on security-related construction, and only 7 percent anticipate spending $10 million or more.

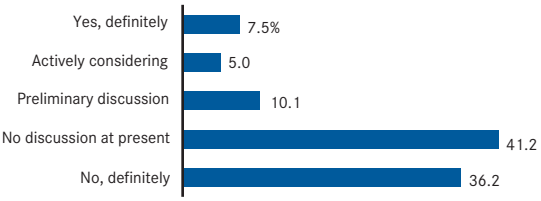
Most companies are not planning to disperse facilities for security reasons

Planning to rent, buy, or construct additional facilities in order to disperse *employees* for security reasons



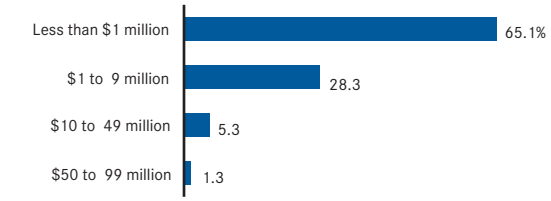
Number of respondents: 199

Planning to rent, buy, or construct additional facilities in order to disperse *operations* for security reasons



Number of respondents: 199

Estimated spending on construction for security reasons during next five years



Number of respondents: 152
Note: "Don't know" eliminated.

Disaster Recovery and Business Continuity

The constraints on financial resources limit the resilience of IT operations at smaller companies in the face of system disruptions. The Conference Board survey of IT security officers suggests that smaller companies are less prepared than larger companies to deal with disaster recovery and business continuity problems.

Three-quarters (74 percent) of companies with less than $1 billion in sales have a disaster recovery program in place, compared to 88 percent of companies between one and five billion dollars in sales, and 93 percent of companies above the $5 billion level in revenues. The difference in capability is even more apparent when one looks at whether a disaster recovery program has been tested and/or used in an emergency.

Smaller companies are less prepared for IT recovery and continuity

Disaster recovery program

Sales level	In place	Tested/ used	Number of respondents
Under $1 billion	74.1%	48.1%	27
$1 billion to $5 billion	88.0	64.0	25
Over $5 billion	92.9	78.6	28

Business continuity program

Sales level	In place	Tested/ used	Number of respondents
Under $1 billion	57.7%	30.8%	26
$1 billion to $5 billion	80.0	48.0	25
Over $5 billion	85.7	64.3	28

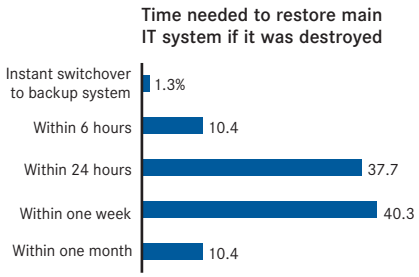
Less than half (48 percent) of companies under the $1 billion sales level have ever attempted to implement disaster recovery procedures, compared to 64 percent of companies between $1 billion and $5 billion in size, and 79 percent of companies with more than $5 billion in revenues.

The findings are quite stark with regard to business continuity. Some 58 percent of companies with less than $1 billion in sales have a business continuity program in place, a proportion that rises to 80 percent for companies between one and five billion dollars in revenues, and 86 percent for companies over $5 billion in size.

Less than one-third (31 percent) of companies with under $1 billion in sales have ever tested or used a business continuity program, compared to 48 percent of companies between $1 billion and $5 billion in sales, and 64 percent of companies above the $5 billion level.

Just under half of companies (49 percent) reported that they could restore their IT system within 24 hours of a disaster. Another 40 percent could restore their system within one week, leaving 10 percent who would need a full month to restore their IT system.

About half of companies could restore their IT system within 24 hours of a disaster



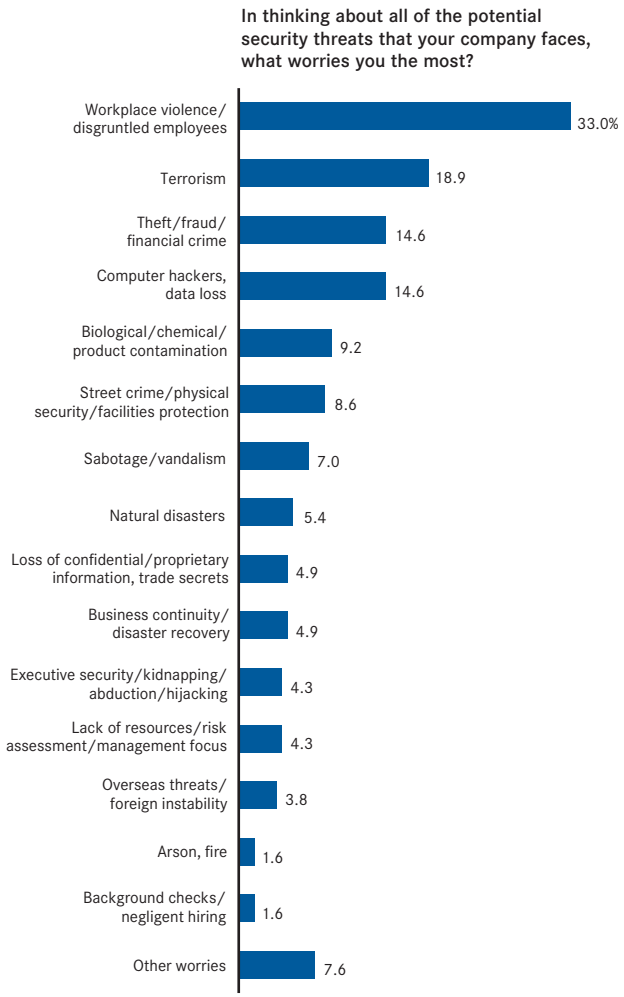
Number of respondents: 77

Note: "Don't know" eliminated.

What Security Executives Worry About

The sheer variety of threats faced by contemporary businesses presents a long list of contingencies for which security executives must be prepared. All three types of security executives (security directors, risk managers, and IT security officers) were asked an open-ended question to elicit what they are most worried about. Security directors are most concerned about the possibility of workplace violence, a worry voiced by one-third of the sample. Terrorism was the next most frequent mention (by 19 percent), followed by financial crime (15 percent) and computer hacking (15 percent).

Security directors worry most about workplace violence



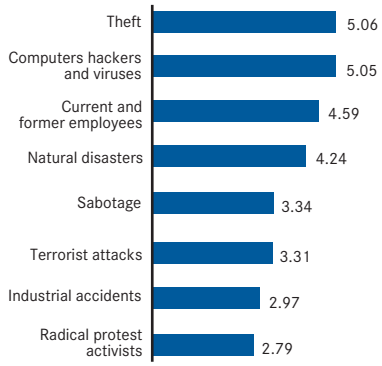
Number of respondents: 185

Note: Summary coded from open-ended responses.

A different question was posed to gauge the severity of different types of threats. Security directors were asked to rate the severity of threats to their companies on a 7-point scale, with 7 representing the most severe threat. The threats rated most highly on this scale are theft (averaging 5.06 on the 7-point scale) and computer hackers and viruses (5.05). These worries are followed by current and former employees (4.59) and natural disasters (4.24).

The relatively low rating for terrorism (3.31) on the scale question, compared to the open-ended question, suggests that most security directors believe the probability of a terrorist incident affecting their own company is relatively low. At the same time, the damage from such an incident could be quite severe if it were to occur.

Theft and computer hacking are the most direct threats



Number of respondents: 197

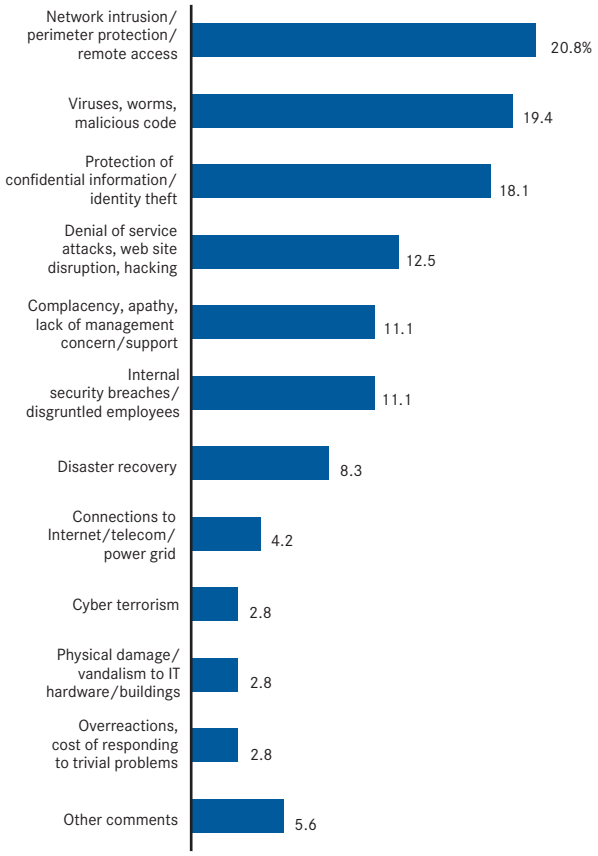
Threats to IT Security

IT security officers primarily focus on preserving the integrity of their networks and web sites. When responding to the open-ended question, the most common worry concerns network intrusion and perimeter protection, mentioned by 21 percent. Close behind are viruses and worms (cited by 19 percent), protecting confidential information (18 percent) and web site disruption (13 percent).

When presented with a 7-point scale to rate the severity of various IT threats, the most highly rated threat was viruses and worms (mean of 4.11, or about halfway, on a 7-point scale). This was followed by insider abuse of Internet access (3.59), laptop theft (2.94), theft of proprietary information (2.22), denial-of-service attacks (2.21), and firewall penetration (2.20) Most of the items received ratings near the bottom of the severity scale, suggesting that most IT security officers are fairly sanguine about their ability to protect their companies' systems.

Network intrusion is the biggest worry for IT security officers

In thinking about all of the potential IT security threats that your company faces, what worries you the most?



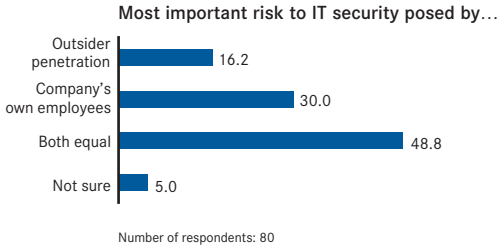
Number of respondents: 72

Note: Summary coded from open-ended responses.

When asked whether insiders or outsiders are the greatest threats to their IT systems, almost half of IT security officers (49 percent) rate both as equal threats, while 30 percent fear their own company's employees and only 16 percent worry most about outsiders.

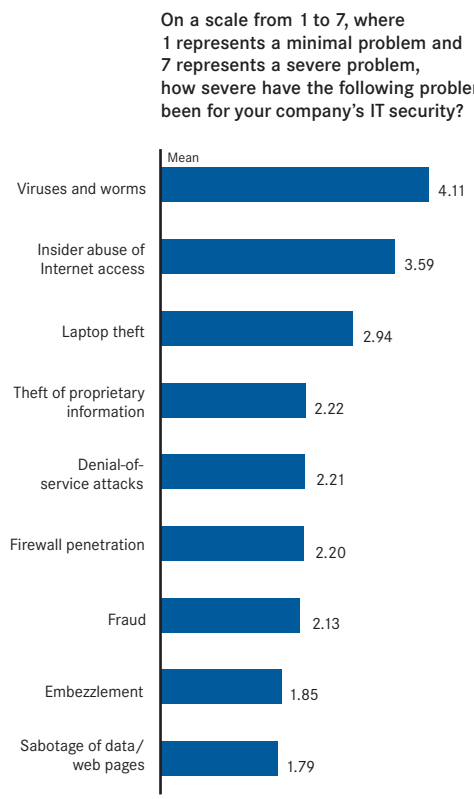
Risk managers have a somewhat different set of concerns. Perhaps because they deal with insurance issues, they seem much more attuned to the dangers posed by terrorism and emergency preparedness. In the open-ended question, terrorism is most often cited as the threat that worries risk managers the most (by 22 percent), followed by business interruption and disaster recovery (17 percent) and workplace violence (11 percent).

Insiders and outsiders are equally threatening to IT security



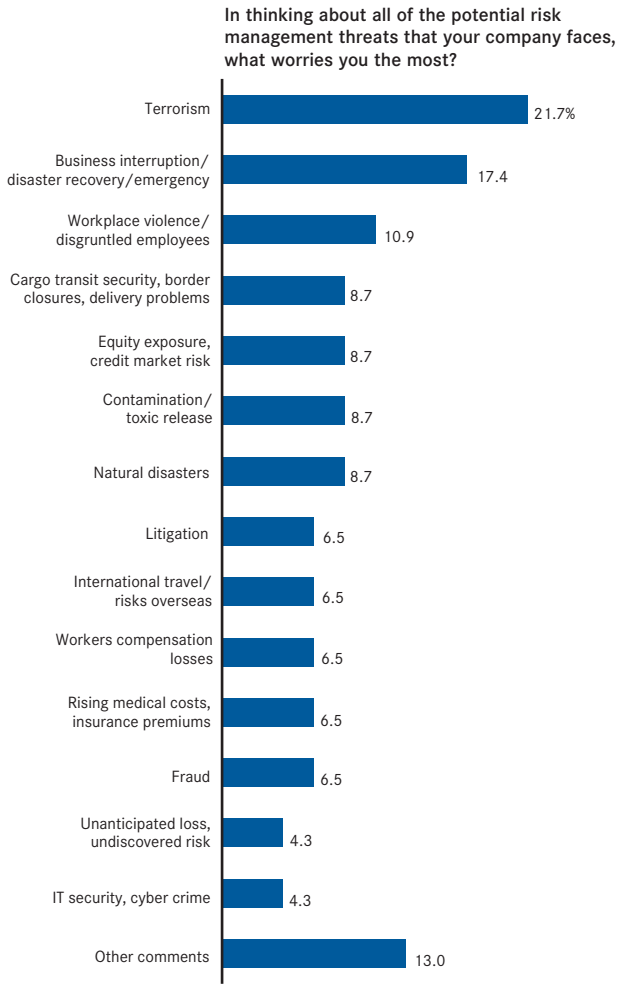
Number of respondents: 80

Viruses and worms are the most direct threats to IT security



Number of respondents: 80

Risk managers are most worried about terrorism and disaster recovery



Number of respondents: 46
Note: Summary coded from open-ended responses.

Vulnerability in the "Extended Enterprise"

Security is about interconnectedness. The connection points that pose the greatest risk for system failure are those holding the system together. Vulnerability assessments need to identify the critical nodes where systems are most prone to failure and where attackers can cause the greatest harm.

To be sure, companies in some industries are more highly interconnected than others and therefore share a vulnerability to service disruption, which can cascade through a system or network. Air travel, electric utilities, telecommunications, financial services, border crossings, and the Internet are potentially vulnerable to a widespread interruption of service resulting from intended or unintended causes. For executives in Cleveland, the experience of the 2003 Northeast electrical blackout which originated in their region was proof enough that interconnectedness was a powerful factor for security risk even when the cause was not intentional.

For these executives and others, the good news is that since 9/11, a great deal of progress has been made in terms of hardening and protecting key targets in critical industries. This good news is offset by a sobering realization, however; as the "A list" of targets becomes harder to attack, terrorists and hackers are likely to move down the list to "softer" targets of opportunity that may not be as thoroughly protected. There is clear evidence of this pattern in Asia and the Middle East in recent years; U.S. embassies and military bases have become better defended, so terrorists have increasingly targeted hotels, shopping centers, restaurants, and residential facilities. A similar pattern is a possibility that American companies need to be aware of.

"Soft" targets are often clustered together in a local business district or neighborhood. An approach that is gaining favor to protect such targets is to establish security buffer zones. A hardened perimeter is created that surrounds a business district or neighborhood. Entry through this perimeter is carefully monitored and controlled, but access to facilities within the perimeter is relatively unconstrained. This appears to be an effective strategy in terms of both cost and unobtrusiveness.

For mid-sized businesses, many executives believe the most important arena for security compliance may well be their participation in the supply chain for larger companies. Increasingly, major enterprises view their supply and distribution chains as a critical component of their own risk profiles. They analyze security not just within their own companies, but across the "extended enterprise," believing that the company's entire value chain must be protected as well. As a consequence, they are insisting that smaller companies meet certain baseline security standards as a price of doing business.

Standards imposed by major corporations, rather than those imposed by the government, may well turn out to be the most important incentive for smaller companies to upgrade their security operations. In some industries, these requirements will increasingly pose a barrier to new entrants. On the other hand, security best practices will be a potent selling point for innovative companies, especially those that do business with clients in the critical industries.

Many executives believe that given the role of mid-market companies as external providers to larger firms, outsourcing poses a particularly knotty set of security issues, because it may leave essential operations vulnerable, yet outside the direct control of a major company. The security risks related to outsourcing are especially acute in emerging or less developed economies, where such basic procedures as comprehensive background checks on employees may be difficult or impossible to perform due to deficient record-keeping. Nevertheless, the financial advantages of offshoring will make the practice increasingly common in order to meet competitive pressures. Security risks are being managed by more intensive due diligence in establishing foreign operations and negotiating business partnerships.

In the public sector, important relationships have been forged in recent years among first responders at the local level, and among the various federal, state, and local units involved in emergency management. The essential piece missing in the eyes of many mid-market business executives is liaison between the public and private sectors. Mid-market executives complain that the various government agencies are in close touch with one another but do a poor job of coordinating with smaller entities in the private sector. Many corporate managers feel they do not have a clear idea of who to contact in the event of an emergency, or how the emergency procedures would be implemented. This is an area where executives felt that greater communication is urgently needed.

Mid-Market Companies…

Tackling the Challenge

Given the acute challenges facing smaller businesses, there is widespread interest in how they are attempting to upgrade their security operations. There was extensive discussion about tackling the challenge of corporate security at the senior executive roundtables held in Atlanta and Cleveland in June, 2003. Among the many subjects discussed were the complex relationship between the government and the private sector, and the importance of framing the issue of security in language that resonates with business executives.

Regulatory Frameworks

Businesses in the mid-market sector tend to cast a wary eye on proposals for regulating their activities. Large companies may also squawk about the regulatory burden, but they generally can find the resources to monitor compliance and handle the paperwork required. For smaller companies, with a thinner staffing structure, the burden of poorly conceived and drafted regulations can seem overwhelming.

In contrast to enforcement by regulation, mid-market executives at the meetings said they would prefer a regime that emphasizes self-regulation and voluntary compliance. These executives recognize the need for security, and by and large, they want to "do the right thing" to safeguard their employees, their customers, and their communities. But they expressed nervousness that the heightened public awareness of security may lead to the imposition of a regulatory regime they would find burdensome. "Who do we listen to?" was a prominent question.

To be sure, some executives express an interest in "intelligent regulation" that would level the playing field for all companies in a given industry. There is also continuing concern about the perceived inadequacy of regulation regarding the electric grid. As a result of the widespread electric blackout of August 14, 2003, some executives expressed a fear that inadequate maintenance and haphazard load sharing could trigger additional problems in the future. The electric system is so vital to the conduct of business that some executives felt a national standard for utility performance may be preferable to the current patchwork system of oversight at the state and regional level.

This experience of business interdependence and vulnerability was cited as evidence that security should be seen as a systemic risk, and not just a localized or industry problem. And, if the conceptualization of security needs diverged between the public and the private sectors, so too would the prescriptions of each sector for action. This potential for public/private dissonance is a particular concern to mid-market entities, who see their roles as drivers of economic growth and who make decisions mostly for reasons of business "value."

The fragmentation of regulatory initiatives was an additional concern. Many federal and state agencies, some with missions (such as environmental protection) not specifically related to security, have begun issuing regulations with security implications. Keeping track of these many requirements is time-consuming and burdensome, especially for companies with operations in a number of different states that involve a variety of industries. According to some executives, a central clearinghouse to collect and analyze relevant federal and state security regulations would be a valuable service for companies lacking the resources to track these initiatives themselves. A significant obstacle to this approach is the fact that no one government agency (not even DHS) has the statutory authority to act in this capacity.

In the absence of such a public sector clearinghouse, other private sector efforts with a similar purpose have begun. Since 9/11, there has been a major move in the direction of industry standards and certification procedures for corporate security. In general, mid-market executives strongly prefer this approach for devising, adopting and implementing security guidelines. An executive from the food industry, for example, cited the many and sometimes contradictory regulations in his industry as something to avoid when designing a coherent security program.

Many trade associations have drafted or revised security standards to reflect the new environment. Trade association standards have the advantage of being tailored for specific industries, and they are widely disseminated, understood, and incorporated into company operating procedures. They become part of the common currency of practice for seasoned executives in a given industry. By becoming part of the culture of the industry, trade association standards ensure that security concerns are aligned with the company mission, rather than being seen as a burdensome cost center that detracts from the company mission.

Globalization is another factor impacting regulation. For example, ISO is currently undertaking an accelerated initiative to devise a uniform security standard for private corporations that could be implemented and assured through a certification process. As the preeminent body for devising worldwide industrial standards, ISO is thoroughly familiar to many executives, and the organization enjoys a good deal of credibility in the corporate community. For example, the ISO standards on quality assurance and environmental management have facilitated the efforts of many companies to implement procedures that improve their performance in these areas. A set of ISO guidelines on security can be expected to have a similar impact.

A representative from DHS noted that the regulatory process is too slow and cumbersome to keep pace with the constantly evolving nature of the terrorist threat. There is a serious danger that regulations will be drafted to "refight the last battle" rather than anticipate likely threats in the future. Such mandates would be a wasteful use of the scarce resources available for security spending in smaller companies. A consensus view was that it makes far more sense to allow companies to define the most appropriate means to meet the objective of security in their particular setting.

Coordination with Government Agencies

The September 11 experience has highlighted a dilemma for companies attempting to establish effective emergency response programs. One company identified more than 40 agencies charged with advising its business units about potential threats, sometimes asking for conflicting or inconsistent information. There is general agreement, especially among companies operating critical infrastructure or manufacturing volatile products, that coordination among the agencies themselves is crucial.

Another area of concern was how to address the conflict between withholding information for reasons of security and sharing it as a prerequisite to enjoying security that is effective. Thomas E. Cavanagh of The Conference Board reported on findings that effectiveness in sharing is only possible if the public sector can carve out a "zone of comfort" that allows sensitive information to be shared with the private sector in a non-adversarial setting. This suggests that an institutional framework is needed within which companies can discuss their problems candidly without fear of legal liability, litigation, or risks to customer privacy and intellectual property. Absent such a non-threatening and cooperative culture of public/private interaction, there may be a perverse incentive to hide problems from public view and which is harmful to security.

This phenomenon is well-documented in the annual IT security surveys produced by the Computer Security Institute and the Federal Bureau of Investigation. The surveys indicate that the majority of IT security lapses are never reported to the public or to the government for fear of adverse publicity, market response, or litigation. (See Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, "2004 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, 2004.)

Throughout the discussions with mid-market executives, representatives of DHS pointed out an undisputed finding that economic security was a matter of national security. Terrorists have a goal to shock entire economic systems and undermine confidence in the functioning of the society. They are not simply focused on harming people and property. The interdependence of national security, which is chiefly a governmental function, and economic security, which involves mostly private business and "critical" infrastructure, was a backdrop to a discussion on the language and communication of security and the "business case."

Communication and the Business Case

According to executives at The Conference Board meetings in Cleveland and Atlanta, generally speaking, business and government are not speaking the same language when it comes to homeland security. For mid-market managers concerned with everyday risks of doing business, the official terminology centering on the term "homeland security" seems remote and not actionable. The U.S. Department of Homeland Security is perceived as being primarily concerned with the threat of terrorism. To many smaller companies, especially outside the Northeast, terrorism per se does not appear to be as relevant a threat as other everyday risks of doing business, executives said. While government seems concerned with sources of external threats, security directors at such companies said they focus more on internal security concerns like disgruntled employees, workplace violence and other sources of internal instability.

Few if any executives were responsive to the term "homeland security," which some said was not a very meaningful construct or frame of reference for executives accustomed to the language of commerce. Executives said that phrases such as "risk management" and "business continuity" resonate much better with business people. These are functions that they recognize as being central to ongoing business operations. If the relevance of security to corporate management is going to increase, then concepts that fit with existing corporate missions and procedures will need to be used.

One example that executives cited was how the discipline of safety came to be a mainstream business concern. Today, safety is imbedded in any company that aspires to best practice levels of performance management. If security is going to arrive at a similar level of corporate operating recognition, then new ways of describing it may have to be formulated. In contrast, if there is no solution to this language barrier, it becomes much harder to buy the "business case" for security as a value-adding activity. Thus, the language of security and the perception of its value are interconnected.

Whatever the ultimate approach may be, mid-market executives agree with peers in other areas of business that defining the business case for security is the key factor in making security a higher priority for corporate managements. Articulating the business case requires a thorough appreciation of the relevance of security to corporate reputation and business opportunities. Determining the "return" on security investments also requires a framework to measure the value added to the company through such investments.

At present, mid-market executives say they find it difficult to analyze security spending in these terms. They lack the tools and staff resources to perform such an analysis. It is true that at least insurance is one realm in which security spending yields tangible financial results; many insurers will reduce premiums if a company can demonstrate that it has instituted procedures and dedicated capital to lowering risk exposure. But by and large, there is a lack of tools, metrics or staff resources to measure other aspects of security investment in an equally straightforward manner.

Ultimately, the value of security spending will be demonstrated to the extent that it becomes a proactive management tool, and not merely a reaction to incidents or disasters. Security managers tend to think of their jobs in terms of responding rather than initiating. Among executives at the security roundtables in Atlanta and Cleveland, there was a common sentiment that security's access to the "C-suite" was inadequate to these times and that a change of mindset would be a prerequisite to enhancing the priority accorded to security in corporate operations.

Appendix

About the Research

Security Directors Surveys

Senior security executives were interviewed online from October 2002 through February 2003. The study was sponsored by ASIS International. Separate questionnaires were developed for security directors, risk managers, and IT security officers, and were targeted at the senior executive responsible for each of those functions in a given company. The samples comprise 199 security directors, 52 risk managers, and 80 IT security officers.

Over 50 percent of each sample was derived from companies with $1 billion or more in annual sales, roughly the cutoff for inclusion in the Fortune 1000. In the sample of security directors, there are 110 companies above $1 billion in sales and 88 below. In the sample of risk managers, there are 28 companies above $1 billion in sales and 24 below. In the sample of IT security officers, there are 53 companies above $1 billion in sales and 27 below.

Following the usage of the U.S. Department of Homeland Security, critical industries are defined as the following: transportation; energy and utilities; financial services; media and telecommunications; information technology; and healthcare. Remaining industries are classified as non-critical. There are 96 companies from critical industries and 103 from non-critical industries in the sample of security directors. There are 24 companies from critical industries and 28 from non-critical industries in the sample of risk managers. There are 38 companies from critical industries in the sample of IT security officers, and 42 from non-critical industries.

Multinational companies are defined as companies that derive 10 percent or more of their sales from overseas. All other companies are defined as domestic. There are 77 multinational companies and 97 domestic companies in the sample of security directors. There are 25 multinational and 25 domestic companies in the sample of risk managers. There are 42 multinational and 34 domestic companies in the sample of IT security officers.

Respondent companies were classified into regions according to the ZIP code of their headquarters location. Companies in the Boston, New York, Philadelphia, and Washington metropolitan areas were classified as Northeast Metro; companies headquartered in the United States outside these areas are classified as "Rest of United States." Companies headquartered outside the United States were omitted from this particular classification. There are 57 Northeast Metro respondents in the sample of security directors, and 130 from the rest of the country. There are 12 Northeast Metro respondents in the sample of risk managers, and 35 in the rest of the country. There are 16 Northeast Metro respondents in the sample of IT security officers, and 62 in the rest of the country.

Chief Executives Survey

Senior managing executives from mid-market companies were interviewed online from May 18 to June 14, 2004. The sample was drawn from companies with annual revenues between $20 million and $1 billion. A total of 96 respondents participated.

The respondents have the following titles: 61 CEO; 31 President; 23 Chairman; 3 Managing Director; 2 COO; 1 Managing Partner. (Note that some respondents have more than one title.)

Annual revenues are as follows: 16 below $50 million; 23 from $50-99 million; 27 from $100-249 million; 12 from $250-499 million; 18 with $500 million or more.

Ownership structure is as follows: 33 privately held; 29 publicly traded; 11 non-profit; 9 family-owned; 7 employee-owned; 3 cooperative or credit union; 2 partnership; 2 other.

Employing the usage of the U.S. Department of Homeland Security, 35 companies are in critical industries (transportation; energy and utilities; financial services; media and telecommunications; information technology; and healthcare). There are 53 companies in non-critical industries, and 8 could not be classified.

Region is as follows: 24 in the Northeast Metro (defined as zip codes in the Boston, New York, Philadelphia, and Washington metropolitan areas); 6 in the remainder of the Northeast; 20 in the South; 28 in the Midwest; and 15 in the West. Three could not be classified by region.

RELATED PROGRAMS & SERVICES FROM THE CONFERENCE BOARD

Research Reports

Corporate Security Management: Organization and Spending Since 9/11
R-1333-03-RR, 2003

Executive Action Reports

Cops, Geeks, and Bean Counters: The Clashing Cultures of Corporate Security
Executive Action 115, 2004

The Mid-Market Company Series

Security in Mid-Market Companies: Tackling the Challenge
Executive Action 119, 2004

Security in Mid-Market Companies: The View from the Top
Executive Action 102, 2004

Managing Corporate Security in Mid-Markets
Executive Action 67, 2003

Learning and Networking Opportunities from The Conference Board

Council of Corporate Security Executives

The Council provides an exclusive forum for peer exchange of information and best practices on security management at the senior level in major corporations. For more information contact: Julie Crocker at Julie.crocker@conference-board.org

Research Director **David Vidal**

Publishing Director **Charles Mitchell**

Managing Editor **John Lumea**

Author **Thomas E. Cavanagh**

Design **Peter Drubin**

Production **Andrew Ashwell**

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

The Conference Board Europe
Chaussée de La Hulpe 130, box 11
B-1000 Brussels
Belgium
Tel 32 2 675 5405
Fax 32 2 675 0395
conference-board.org/europe.htm

The Conference Board Asia-Pacific
2502C Admiralty Centre, Tower 1
18 Harcourt Road
Hong Kong SAR
Tel 852 2804 1000
Fax 852 2869 1403

The Conference Board of Canada
255 Smyth Road
Ottawa, Ontario K1H 8M7
Canada
Tel 613 526 3280
Fax 613 526 4857
conferenceboard.ca