

2003 Competitiveness and Security Survey

Table of Contents

Creating a Business Case for Security	1
Survey Summary	2
Security and Business	3
New Security Initiatives	4
Risk Assessments: Frequency and Influence	5
Private Sector Responsibility	6
Expectations of New Regulations	6
Survey Methodology	7
Contact Information	8

*** Creating a Business Case for Corporate Security ***

Security depends as much on private sector initiatives as on public sector leadership.

The private sector is vital to securing the homeland precisely because the vast majority of economic assets and infrastructure are owned and operated by companies.

Creating a business case for security is both the critical challenge and opportunity.

The risks of mass disruption terrorism have been recognized for decades by many distinguished commissions and studies. Yet security against terror attacks was never embedded in the private sector because there was no business case for doing so. Like quality two decades ago, security was seen as a sunk cost and productivity-drain rather than a requisite for business continuity and competitiveness.

The 2003 Competitiveness and Security survey of senior business executives reflects a sea change in attitude from only one year ago.

In the September 2002 survey, nine of out ten business executives did not see their companies at risk from terrorist attacks. Less than 40 percent had addressed vulnerabilities in their information, telecommunications, electric power or supply chains. Most saw no possibility for a positive return on investment.

Key findings from the 2003 survey:

- Most business leaders now see security as a top or high priority.
- Risk management assessments are being conducted frequently.
- Connections to critical infrastructure are becoming a focus for risk management.
- Corporate leaders see opportunities for positive returns on security investments.
- Business leaders believe that the private sector should take the lead in setting security standards.
- The majority of executives believe that the public and private sectors share equal responsibility for homeland security.

Business leaders are unsure as to what constitutes best practice in security.

Although businesses are paying more attention to security, executives are unsure about whether their new standards and procedures constitute best practice. Among those who have adopted new security standards in the past twelve months, less than 40 percent believe the standards represent best practice.

Conclusion: Business attitudes toward security have changed profoundly over the past year. The time is right to identify and institutionalize best practices that create and reinforce a business case for security.

Survey Summary

Businesses executives rank security as a top or high priority.

- Eighty-six percent of the companies say security is a high or top priority.
- Sixty-five percent of companies have adopted new standards for security over the past 12 months.

Corporate leaders see opportunities for positive returns on security investments.

- Seventy-one percent believe security spending would be offset by gains in business continuity, productivity or competitiveness.

Companies are conducting more vulnerability assessments in new areas of risk management.

- Eighty-three percent of companies have conducted risk management assessments over the past 12 months in at least two of the following areas: physical security, IT security, and/or financial management.
- Seventy-one percent of companies have conducted comprehensive security assessments of electronic communications; 68 percent for financial assets; 58 percent for telecommunications and electric power connections.

Business leaders believe the private sector should take the lead in setting security standards for U.S. business.

- Nearly two-thirds of respondents believe the private sector should take the lead in setting security standards.
- Fifty-seven percent believe that the public and private sectors share equally in security responsibility—with an additional 23 percent believing that the responsibility lies mostly or entirely with the private sector.

Companies appear unsure as to what constitutes best practices.

- About a third of executives believe that their companies' security procedures would be candidates for best practice. Twenty-five percent aren't sure—and 37 percent believe that their security procedures probably did not represent best practice.

Supply chain and transportation security remain relatively lower priorities for businesses.

- Less than half conducted comprehensive risk assessments within their supply chain and for transportation and shipping procedures.

Key Findings

One clear trend in this year's results is that businesses are beginning to act on security concerns where last year they were reviewing their procedures and options. Their perspectives on vulnerability have broadened considerably with risk management assessments extending to critical infrastructure such as information technologies, telecommunications, electric power and financial services. Corporate security is no longer viewed as a matter of guards, gates and guns, but of interconnectivity and interdependence of networks.

Senior executives also appear to be questioning the conventional wisdom that security is inevitably a sunk cost. The results indicate that businesses are beginning to see a business case for security, anticipating a potential for positive returns on investments. There is a historical parallel with the quality movement. In the early 1980s, American business wrongly thought of quality as an added expense and a luxury, rather than a core business process with the potential to reduce cycle time and create competitive advantage.

Yet, this year's results also highlight that few are sure about how to integrate security effectively into their operations. This should not be surprising. The intellectual framework for quality management grew up over a period of decades after World War II and only institutionalized with the creation of the Baldrige Award in 1988. But, 9/11 was only a moment in time—and there is no accepted business model for integrated security management. The need to identify and institutionalize a set of best practices—security processes that create positive returns on investment—remains largely unmet.

Companies remain concerned about the potential for regulation in homeland security rather than cooperation. It may not be entirely coincidental that the area in which the public sector has taken the most hands-on role—transportation security—is the area in which the private sector has been the least pro-active. The private sector expects to be an equal partner in securing the homeland—and the process of sorting out roles and responsibilities has only just begun.

Security and Business

Companies Rank Security as a Top or High Priority

Although 70 percent of companies in the 2002 survey had reviewed or discussed security policies after September 11th, only 53 percent had actually changed them. In the intervening year, however, there appears to have been a sea change in business attitudes. In 2003, nearly nine out of 10 (88 percent) companies report that security is a top or high priority.

The responses vary significantly by geography. Companies in the Midwest and West are more likely to view security as a “low” priority than those in the South or Northeast. Specifically, 14 percent of companies in the Midwest and 16 percent of companies in the West rated security as a low priority versus just 5 percent in the East and 9 percent of companies in the South.

Similarly, the results vary by sales volume. Companies with sales in the \$50-\$70 million range are most likely to view security as a low priority (18 percent) while just 11 percent of companies with \$70-\$100 million volume and 10 percent of companies with \$100-\$200 million or \$200-\$500 million worth of sales place security as a low priority. No companies with \$500 million to \$1 billion in sales fail to prioritize security.

Security Is Considered Good for Business

Companies are beginning to see security as an investment rather than a sunk cost. In last year’s survey, just 24 percent of companies believed that changes in security could improve their long-term productivity versus 69 percent that did not. In the 2003 survey, by contrast, opinions have completely flip-flopped; 71 percent of companies now believe that increased security spending will improve long-term productivity—with security costs offset by gains in business continuity, productivity or competitiveness—versus only 26 percent that disagree.

Companies that believe security is a top or high priority (83 percent and 69 percent, respectively) and companies that have conducted security assessments in the past 6 months (78 percent) hold this belief most strongly.

Companies with less awareness of or attention to security are less likely to believe there is a positive return from security investment. For instance, just 62 percent of companies that have conducted security assessments in the last 12 months and 50 percent that have done so in the last 2 years believe security initiatives will create positive returns. These findings indicate that companies that have studied security more closely and recently have discovered it is a good investment.

Figure 1: Priority of Company Security

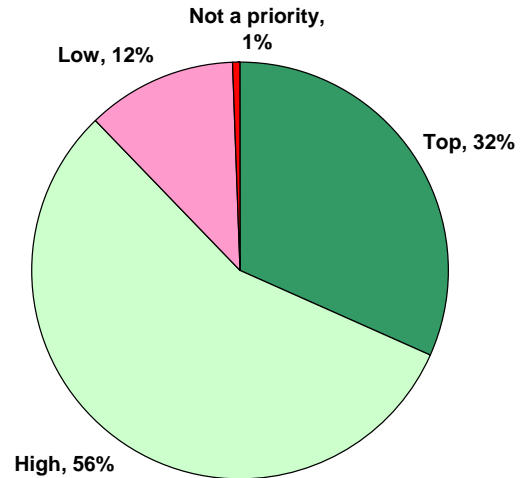
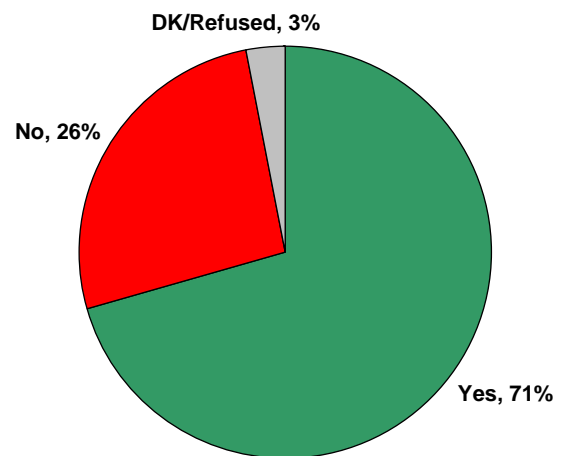


Figure 2: Is There a Positive Return on Investment for Security?



New Security Initiatives

Security Initiatives Are Implemented Corporate-wide

Over seven in ten (71 percent) companies report that security initiatives are being implemented at the corporate level. Companies that regard security as a top or high priority are far more likely to adopt corporate-wide initiatives (79 percent and 70 percent, respectively) compared to companies that assign low priority to security (56 percent).

Another significant factor is the timing of the last risk management assessment. Eight in ten (81 percent) companies that conducted risk management assessments within the past 6 months have implemented security on a corporate-wide basis. By contrast, only 64 percent of companies that conducted risk assessments in the past 12 months implemented corporate-wide policies and only 50 percent of companies whose last risk assessment occurred within the past 2 years have done so.

Nearly three quarters (74 percent) of the companies that have implemented security on a corporate-wide basis believe there will be a positive return on investment.

More Companies Are Adopting New Security Standards

Almost two out of three companies (65 percent) report that they have adopted new standards for security within the past 12 months. Not surprisingly, companies that consider security to be a top or high priority are the most likely to have adopted new security standards (74 percent and 65 percent, respectively).

Nevertheless, companies are divided on the effectiveness of their security standards. Among all respondents, about a third of companies—34 percent—believe that their security procedures would be candidates for best practice. One in four (25 percent) are uncertain, and 37 percent believe their company's security procedures would not constitute best practices.

Figure 3: From What Level Has Your Security Initiative Implementation Been Flowing?

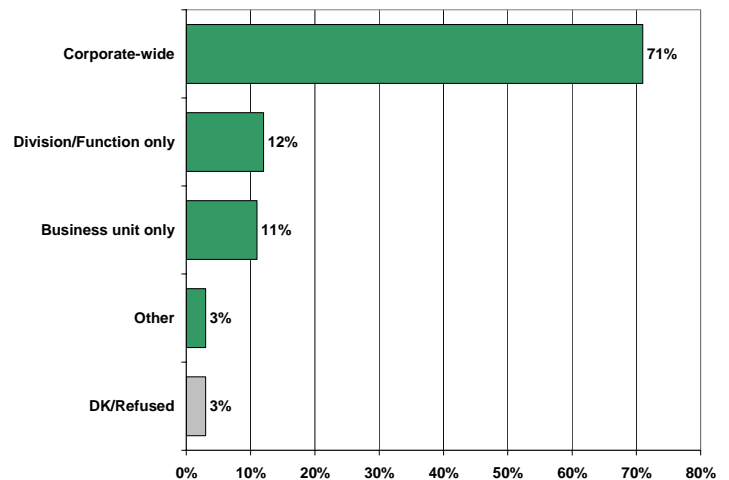
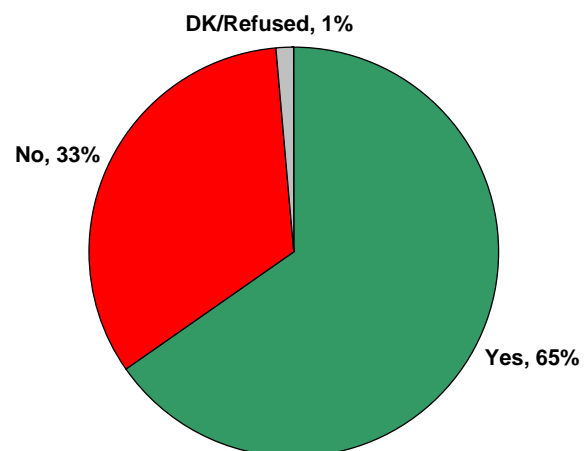


Figure 4: Have You Adopted New Security Standards in Past 12 Months?



Risk Assessments: Frequency & Influence

Corporate Risk Assessments Are Increasing in Frequency and Scope

In September 2002, just 58 percent of companies reported having conducted vulnerability assessments. In the year since, 83 percent of companies performed risk management assessments in at least two of the following areas: physical security, IT security or financial management. The majority (56 percent) of companies have performed such assessments in the last 6 months.

Compared to last year's survey, it is clear that companies are taking a much closer look at connections to critical infrastructure. Last year, the major focus was on physical assets and employee security. The percentage of companies that had examined the vulnerability of their infrastructure connections was relatively low.

This year, the percentage of companies performing a comprehensive security assessment increased dramatically in many categories. While physical assets and IT are the areas most likely to have received scrutiny (75 percent and 71 percent, respectively), companies are turning their attention to the security of financial assets (68 percent), fixed assets /inventory (60 percent), electric power (58 percent) and telecommunications (58 percent). The percentage of companies that have examined their supply chain and transportation security, however, remains relatively low.

Figure 5: Date of Last Company Security Assessment

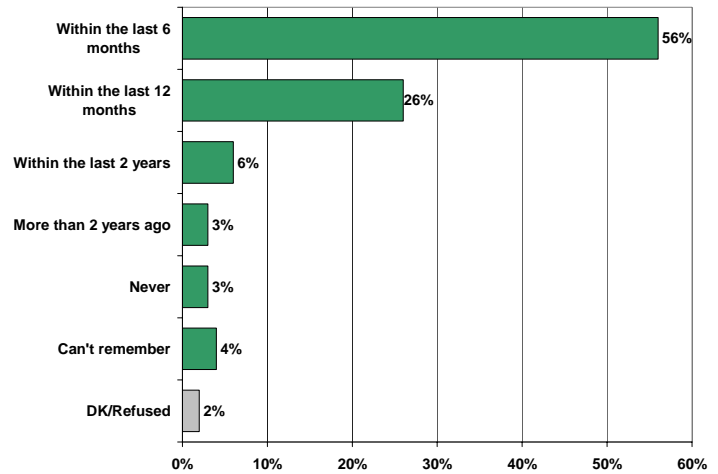


Figure 6: 2002-2003 Comparison of Risk Assessments

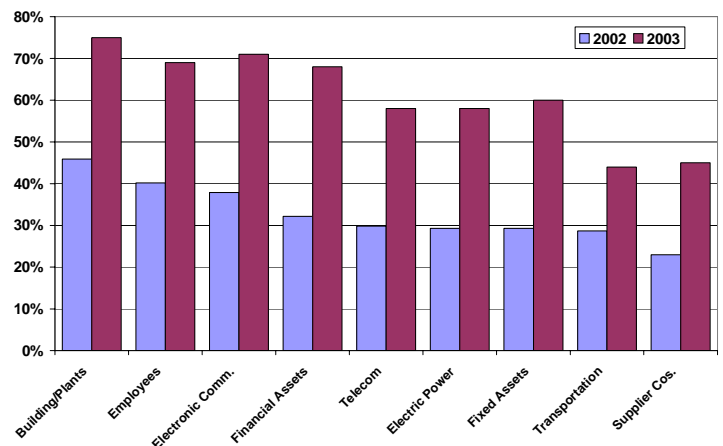
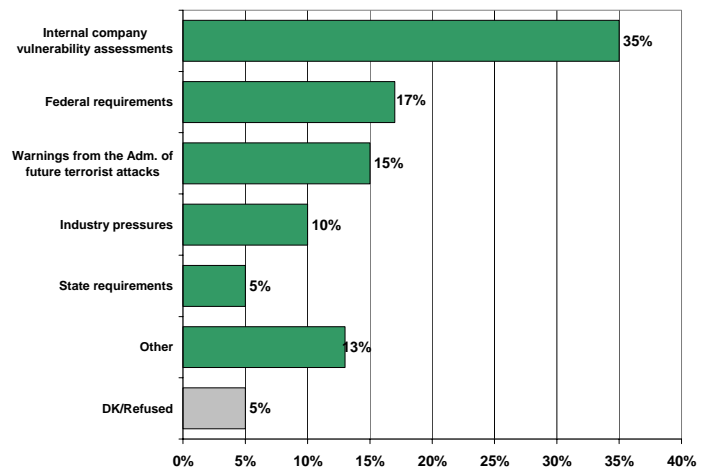


Figure 7: Key Factors Influencing Security Initiatives



Security Initiatives Have Been Most Influenced by Internal Vulnerability Assessments

A plurality of companies (35 percent) have implemented new security initiatives primarily as a result of internal company vulnerability assessments, 17 percent because of federal requirements, and 15 percent as a result of administration warnings.

Private Sector Responsibility

Executives Believe the Private Sector Should Take the Lead in Setting Security Standards

More than three in five business executives—62 percent—believe the private sector should take the lead in setting new standards for security. Strong supporters of a pro-active private sector include companies in the \$1 billion plus sales range (71 percent) and those companies that believe new federal regulations are likely (71 percent).

Respondents Believe Private and Public Sectors Should Share Responsibility Equally

Almost six in ten (57 percent) respondents believe that the public and private sectors should share responsibility for security equally. Just about two in ten (23 percent) feel security should be exclusively or primarily a private sector responsibility, and only 13 percent think that it is mostly or exclusively a public sector responsibility.

Expectation of New Regulations

A Majority Believe that New Homeland Security Regulations Are in the Offing

A majority of business executives (52 percent) believe that federal or state regulations are likely to be passed in the next 12 months.

Companies that do not believe new regulations will be passed also tend to view security as a low priority (59 percent) and are more likely to implement security at the business unit level (59 percent). Many of the respondents who do not believe new regulations are coming fall in the \$50-\$70 million (43 percent) and \$70-\$100 million (48 percent) annual sales ranges.

Figure 8: Should the Private Sector Take the Lead in Setting Security Standards?

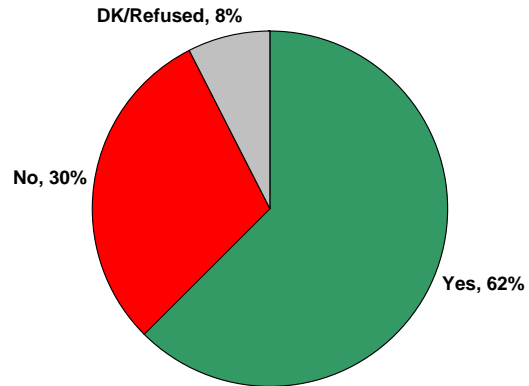


Figure 9: What is the Right Mix of Security

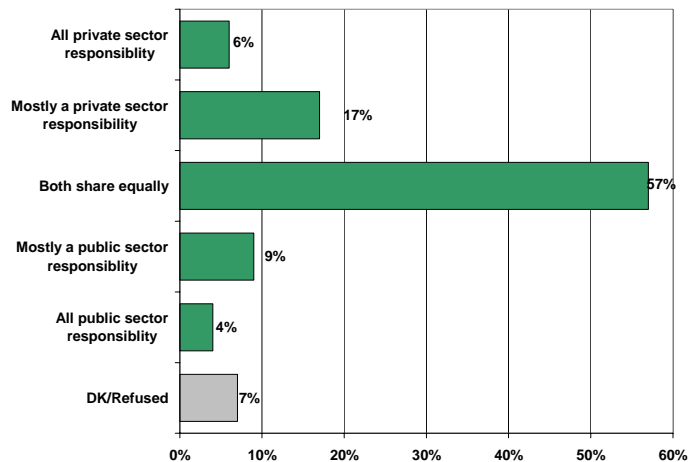
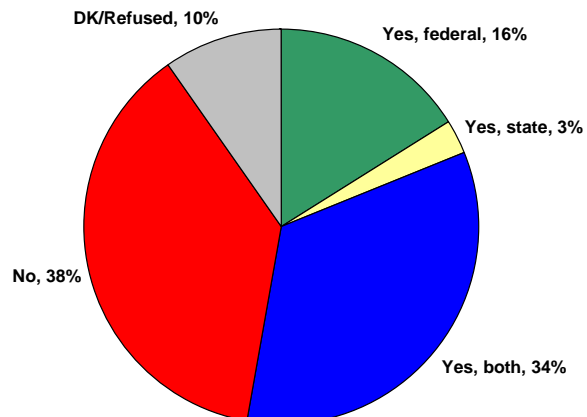


Figure 10: Do You Believe New Security Regulations Will Be Passed in the Next 12 Months?



Survey Methodology

Respondent Type

- The study has a total sample size of n=317 business executives (Chairman, President, CXO, EVP) from U.S. companies with a minimum of \$50 million in annual sales volume. Actual sales volume averaged over \$200 million.
- The study has a margin of error of 5.6% at the 95% confidence level.
- Respondents for this study were screened in order to ensure that they are at least somewhat familiar with the general elements of security at their company, including strategies, procedures, and responsibilities.

Data Collection

- The survey contains 35 questions, which took approximately 15 minutes to complete.
- Surveys were collected via telephone and the Internet.
- Sample for the study was purchased by WRS from InfoUSA.
- Specific job titles and company sales volume requirements were selected before purchasing the sample.
- All of the data were collected between September 22 and October 1, 2003.

Analysis of Data

- Due to rounding errors, certain sub-sample questions provide totals that may not sum exactly to 100%.

Figure 11: Annual Revenues

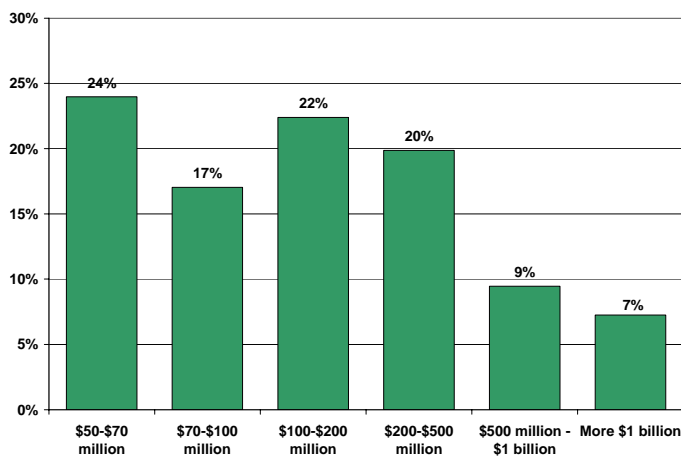
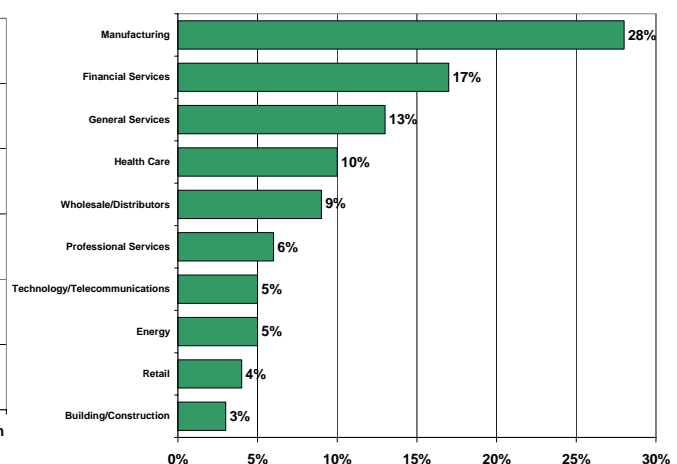


Figure 12: Industries



*** Contact Information ***



The **Council on Competitiveness** is a nonpartisan, nonprofit organization of CEOs, university presidents, and labor leaders committed to promoting U.S. economic growth, success in global markets, and a rising standard of living for all Americans.

Enriched by this unique convergence of talent, perspective and influence, the Council is strategically poised to shape economic agendas—on regional, national, and world stages—that anticipate and respond to the demands of a competitive environment for global trade and commerce.

Contact: Debra van Opstal, Sr. Vice President

1500 K Street, NW, Suite 850

Washington, DC 20005

202-969-3382

www.compete.org



- **Global Perspective**
- **Innovative Research**
- **Superior Results**

Wilson Research Strategies (WRS) is a leading research firm that empowers clients by providing knowledge, understanding, and insight into their most complex issues. WRS specializes in assessing the views of high-level, hard-to-reach audiences in the business, technology, entertainment, academic and political worlds. Over the past 5 years, WRS has conducted over 1,500 studies for U.S and foreign governments, influential associations, and over 100 of the current Fortune 500 corporations.

Contact: Jim Adams, President and COO

8484 Westpark Dr., Suite 800

McLean, VA 22102

703-744-7990

www.w-r-s.com

This report can be downloaded at either website. A customized report and analysis can be developed. For more information, contact Jim Adams.