Top Security Threats and Management Issues Facing Corporate America

2012 Survey of Fortune 1000 Companies

SECURITAS

A Message From:

Bill Barthelemy

CHIEF OPERATING OFFICER - SECURITAS SECURITY SERVICES USA, INC.

William Barthelemy, the Chief Operating Officer of Securitas Security Services USA, Inc. brings nearly 35 years of industry experience to the organization. With a Criminology degree from Indiana University of PA, he began his career as an investigator, moving to the Security Division after two years. He has worked in many field capacities including Scheduling, Operations Manager, Branch Manager, Regional Operations Director and Region President. He brings further client service focus to the management team, and he is an active member of ASIS International, as well as the National Association of Chiefs of Police.

We have completed the "2012 Top Security Threats and Management Issues Facing Corporate America" survey and, on behalf of the Securitas USA management team, we are pleased to publish the results.

This survey has become an industry standard and is often used by corporate personnel and educational institutions for security-related data when making decisions relative to security planning. I want to thank all of our respondents who participated, generating a 25.5% response rate from security executives in 42 states. Your input is critical to our report and it has revealed that the top four threats remain unchanged from 2010 as follows:

1. **Cyber/Communications Security**
2. **Workplace Violence**
3. **Business Continuity Planning**
4. **Employee Selection/Screening**

The top security management challenges that were identified are: 1) Budget/Maximizing Return on Investment; 2) Promoting Employee Awareness; and Security Staffing Effectiveness.

As you will read, the survey results also outline the top security threats as reported by various vertical markets. Additionally, it provides information on the reporting relationships of those participating in the survey as well as projected future budget and funding for security departments.

A special thanks to all those who contributed editorial comment for this issue, namely:

- Tim Williams, CPP,
  Director, Information Risk and Enterprise Security, Caterpillar, Inc.
- Robert Dodge, CPP,
  Pinkerton Senior Vice President, International
- Vincent MacNeill, CPP,
  Vice President, Program Development, Securitas Critical Infrastructure Services
- Bruce Wimmer, CPP,
  Pinkerton Director of Global Consulting
- Mark Geraci, CPP, CFE,
  Vice President and Chief Security Officer, Purdue Pharma L.P.

Don Walker, CPP

CHAIRMAN - SECURITAS SECURITY SERVICES USA, INC.

Depending on the country of publication, newspaper headlines are filled with articles that highlight risks and threats. Whether it is a story of gang violence, riots, corruption, thefts, natural disasters, terrorist attacks, government financial instability or the senseless killing of young people and need for gun control, the story leads to the same conclusion. We live in a world of numerous risks and changing levels of threats. At Securitas and Pinkerton, we are constantly staying abreast of the risk trends and threat levels around the globe. Part of our data collection and monitoring of risks is to survey our clients to determine the top security threats and management issues facing corporate America. This year and for the past ten years, the top three issues are the same. The only thing that has changed is the priority ranking. This year, as in the last report in 2010, Cyber/Communications Security is number one, immediately followed by Workplace Violence Prevention/Response and Business Continuity Planning/Organizational Resilience.

Since our corporate and daily lives depend on wired and wireless networks, it is logical that criminals, terrorists and foreign governments would exploit any areas of weakness to commit social media fraud, extort favors or money, steal sensitive data or commit espionage. In fact, FBI Director Robert Mueller has stated that "computer intrusions and network attacks are the greatest cyber threat to our (USA) national security." Whether the attacks are by a foreign government, a competitor, a terrorist or a criminal, they can wreak havoc on a person, an organization or government. Given the fact the FBI found over two million cases of embedded malicious software in 2012, it is easy to see why Cyber/Communications Security is again number one. The second highest priority threat was again reported as Workplace Violence which, according to the U.S. Department of Labor, is the second leading cause of deaths and injuries in the workplace. It is not only a U.S. or American issue, as the EU-OSHA has identified "violence, bullying and harassment as increasingly common features of the European workplace." Any discussion of workplace violence also includes healthcare facilities and school attacks, which occurred all too frequently in the U.S., Germany and France, as well as other countries. These attacks have led to an increase in awareness and preparedness to prevent such future crimes. For example, the U.S. Department of Homeland Security's awareness programs regarding "the active shooter" and the video "Run, Hide, Fight" help keep the issue in the forefront of security planning.

Business continuity and organizational resilience are more than the ability of an organization to adapt and even continue to function after a disastrous event. From hurricanes and other natural disasters, to major accidents, to criminal and terrorist attacks, organizations of all types and sizes are focusing on the issue of resilience. ASIS International has published several Standards and Guidelines regarding resilience of an organization and its supply chain in order to assist in the planning, prevention, protection, response and recovery after an incident. Because the stakes are so high and organizations are constantly adapting to new circumstances, it is easy to see why Business Continuity is in the top three concerns.

With the continued pressure on the recovery of our global economy, together with corporate emphasis on cost control and profit improvement, it's not surprising that security management is very concerned about budgets/maximizing return on investment for the protection of the organization, its people and assets.

Don W. Walker, CPP, is Chairman of Securitas Security Services USA, Inc. He is an internationally recognized expert in the security field, with an extensive background in all areas of security.

The Securitas Group acquired Pinkerton's Inc. in 1999. Walker joined Pinkerton in 1991, when it acquired Business Risks International (BRI), a security consulting and investigations company with global operations. After joining Pinkerton, he held various management positions, including Chairman, CEO, President, Executive Vice President of the Americas and Executive Vice President of International Operations.

Walker is a co-founder of the ASIS International CSO Roundtable, a member of the International Security Management Association (ISMA), the Society of International Business Fellows (SIBF) and Leadership Nashville. He is a member of the Board of Directors of the Ripon Society and a member of the National Law Enforcement Museum's Chief Security Officer Leadership Committee. He is past president of ASIS International, former treasurer of the International Association of Credit Card Investigators and a member of the original Bank Administration Institute Security Committee. He has served on numerous civic task forces, commissions and committees. Walker is a Certified Protection Professional. He received his Bachelor's degree from the University of Louisville and his Juris Doctorate from the Nashville School of Law.

Securitas Security Services USA, Inc. has completed the 2012 "Top Security Threats and Management Issues Facing Corporate America" survey. This survey has become an industry standard and is often used by corporate personnel and educational institutions for security-related data when making decisions relative to security planning.

Securitas USA surveyed a wide range of security managers and directors, facilities managers and others responsible for the safety and security of corporate America's people, property and information from Fortune 1000 companies. The objective was to identify emerging trends related to perceived security threats, management issues and operational issues. This has created a reliable, data-driven tool for security professionals to apply as they define priorities and strategies, develop business plans, create budgets and set management agendas.

The 2012 survey drew 297 responses from corporate security directors and other executives with primary responsibility for their companies' security programs, yielding a 25.5% response rate.

Today's Threat Environment

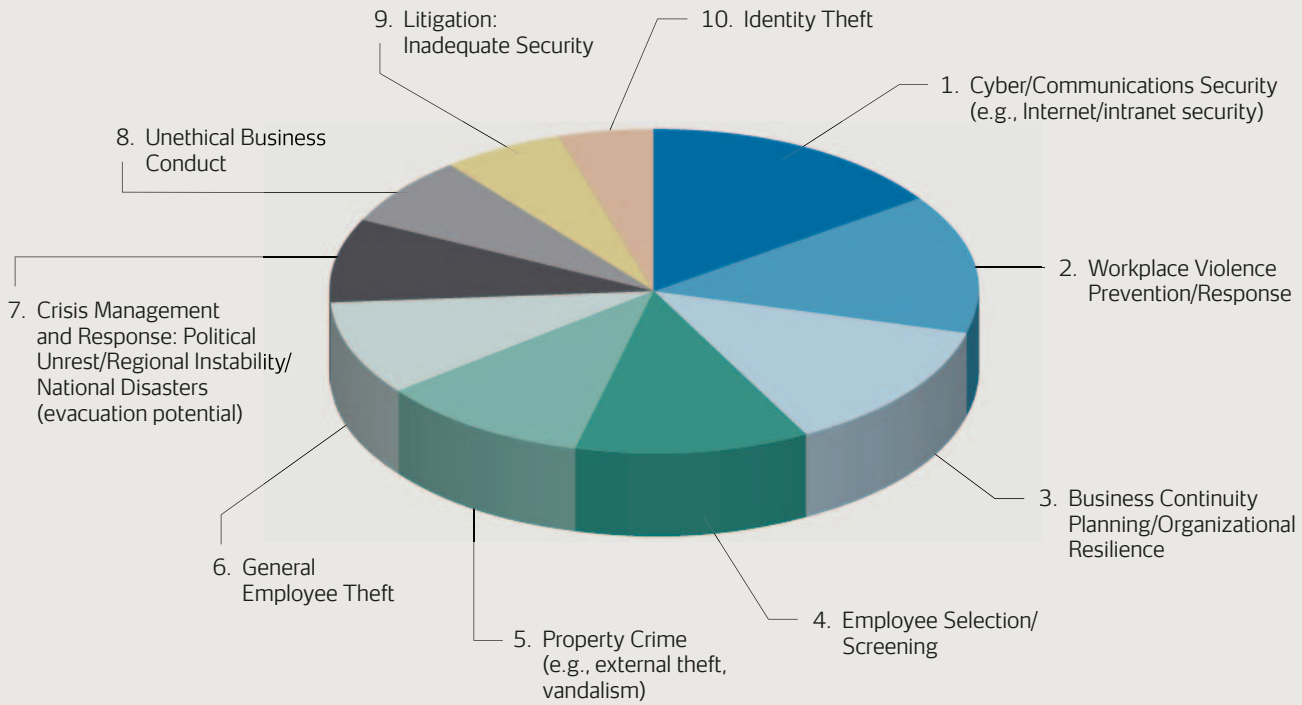
The study revealed the issues of greatest concern to corporate security directors, in rank order (see *Figure 1*).

The 2012 top four security threats remained unchanged from 2010. The threat of Cyber/Communications Security remained the greatest security concern facing Fortune 1000 companies in 2012. Workplace Violence held the number one spot from 1999 to 2008, but dropped to 2nd place in 2010 and remained there in 2012. Business Continuity Planning, including Organizational Resilience, remained in 3rd place while Employee Selection/Screening remained in 4th place.

Property Crime moved up to 5th place from 7th place, General Employee Theft moved up to 6th place from 8th place and Political Unrest/Regional Instability/National Disasters fell to 7th from 6th place. Unethical Business Conduct fell from 5th to 8th place in 2012, while Litigation: Inadequate Security and Identity Theft both moved up into the top 10.

Figure 1

2012 Top Security Threats



Professional Management Issues

A significant portion of the Securitas USA survey was devoted to identifying key management issues, as well as operational, staffing and budgetary issues facing corporate security executives. The operational issues of greatest concern revealed in 2012 are shown in Figure 2.

Figure 2

Operational Issues of Greatest Concern	
1	Budget/Maximizing Return On Investment
2	Promoting Employee Awareness
3	Security Staffing Effectiveness: Training Effectiveness/Methods
4	Implementing Best Practices/Standards/Key Performance Indicators
5	Threat Assessments

Funding Trends

The funding outlook for corporate security programs over the next three to five years changed slightly from the 2010 estimates, with 23% of security managers expecting an increase in funding compared to 27% in 2010; 59% compared to 55% in 2010 expected budgets to remain the same.

Figure 3

Top Security Threats

To assess the relative level of concern held by security professionals, the Security Threats survey presented a list of 24 potential security threats developed by Securitas USA. These were refined from the 2010 survey to be representative of today's concerns.

Respondents were asked to "Rate between 5 (most important) and 1 (least important) the following security threats or concerns you feel will be most important to your company during the next 12 months." The 2012 rankings are shown in Figure 4.

Figure 4

2012 Rank	Top Security Threats - Ranking	Average Importance Score
1	Cyber/Communications Security (e.g., Internet/intranet security)[a]	4.00
2	Workplace Violence Prevention/Response	3.92
3	Business Continuity Planning/Organizational Resilience	3.86
4	Employee Selection/Screening	3.70
5	Property Crime (e.g., external theft, vandalism)	3.57
6	General Employee Theft	3.50
7	Crisis Management and Response: Political Unrest/Regional Instability/ National Disasters (evacuation potential)	3.43
8	Unethical Business Conduct	3.30
9	Litigation: Inadequate Security	3.29
10	Identity Theft	3.26
11	Intellectual Property/Brand Protection/Product Counterfeiting	3.24
12	Fraud/White-Collar Crime	3.23
13	Substance Abuse (drugs/alcohol in the workplace)	3.19
14	Environmental/Social: Robberies	3.14
15	Crisis Management and Response: Terrorism	3.13
16	Business Espionage/Theft of Trade Secrets	3.12
17	Litigation: Negligent Hiring/Supervision	3.09
18	Executive Protection (including travel security)[b]	3.05
19	Bombings/Bomb Threats	2.95
20	Global Supply-Chain Security	2.92
21	Insurance/Workers' Compensation Fraud	2.85
22	Environmental/Social: Pandemic	2.81
23	Labor Unrest	2.54
24	Crisis Management and Response: Kidnapping/Extortion	2.47

a. Prior to 2012, this attribute was Internet/Intranet Security (including e-mail/e-commerce).
b. Prior to 2012, this attribute was two separate attributes: Executive Protection and Travel Security.

Cyber/Communications Security is identified as the foremost concern of corporate security directors, reflecting the country's high reliance on technology. This threat replaced Workplace Violence Prevention/ Response in 2010, which had been the number one concern from 1999 to 2008 and is currently the second highest concern. Business Continuity Planning/ Organizational Resilience remained in 3rd place (where it was in 2010) and Employee Selection remained in 4th place (where it has been since 2008). Property Crime moved up to 5th place from 7th place while General Employee Theft moved up to 6th place from 8th place.

Figure 5

Top Security Threats 1997 - 2012*										
Security Threats	2012	2010	2008	2003	2002	2001	2000	1999	1998	1997
Cyber/Communications Security (e.g., Internet/intranet security)[a]	1	1	3	3	4	2	2 (tie)	7	8	10
Workplace Violence Prevention/Response	2	2	1	1	1	1	1	1	2	1
Business Continuity Planning/Organizational Resilience	3	3	2	2	2	5	2 (tie)	2	7	5
Employee Selection/Screening	4	4	4	5	5	3	5	4	4	4
Property Crime (e.g., external theft, vandalism)	5	7	5 (tie)	12 (tie)	9	10	12	10	10	12
General Employee Theft	6	8	5 (tie)	7	8	6	6	6	1	2
Crisis Management and Response: Political Unrest/Regional Instability/National Disasters (evacuation potential)	7	6	10	11	14 (tie)	20	17	19	NA	NA
Unethical Business Conduct	8	5	9	8	7	9	7	9	6	3
Litigation: Inadequate Security	9	16	19 (tie)	18	11 (tie)	13	13 (tie)	13	13	13
Identity Theft	10	11	12	10	14 (tie)	16	NA	NA	NA	NA
Intellectual Property/Brand Protection/ Product Counterfeiting	11	14	21	NA	NA	NA	NA	NA	NA	NA
Fraud/White-Collar Crime	12	10	8	6	6	4	4	3	3	7
Substance Abuse (drugs/alcohol in the workplace)	13	17	19 (tie)	9	10	8	9	8	11	9
Environmental/Social: Robberies	14	19	27 (tie)	NA	NA	NA	NA	NA	NA	NA
Crisis Management and Response: Terrorism	15	12	7	4	3	17	16	14	17	15
Business Espionage/Theft of Trade Secrets	16	15	15 (tie)	16	19	12	11	12	9	NA
Litigation: Negligent Hiring/Supervision	17	23	25	20	18	14	13 (tie)	15	16	16
Executive Protection (including travel security)[b]	18	13	22 (tie)	NA	NA	NA	NA	NA	NA	NA
Bombings/Bomb Threats	19	24	14	NA	NA	NA	NA	NA	NA	NA
Global Supply-Chain Security	20	22	27 (tie)	21	22	18	19	17	NA	NA
Insurance/Workers' Compensation Fraud	21	25	26	17	17	15	15	16	19	17
Environmental/Social: Pandemic	22	18	17	NA	NA	NA	NA	NA	NA	NA
Labor Unrest	23	26	29	NA	NA	NA	NA	NA	NA	NA
Crisis Management and Response: Kidnapping/Extortion	24	27	33	19	20	19	18	18	NA	NA

* Rankings for 1997 – 2010 do not include every threat, as some were replaced by new options in more recent surveys.
a. Prior to 2012, this attribute was Internet/Intranet Security (including e-mail/e-commerce).
b. Prior to 2012, this attribute was two separate attributes: Executive Protection and Travel Security.

Threat Rankings Within Industry Sectors

Securitas USA also sought to determine if security executives in certain industries placed different emphasis on certain threats. The survey responses for the eight largest aggregate industry groups were examined separately in comparison with the overall sample results.

The largest groups and their proportion to the entire sample are as follows: Manufacturing (30%), Finance and Insurance (12%), Healthcare (8%), Transportation and Warehousing (8%), Rental and Leasing (8%), Information (5%), Utilities (5%), and Real Estate and Retail Trade (3%).

A. Manufacturing

The top 3 concerns among security directors at Fortune 1000 manufacturing companies in 2012 remained unchanged compared to 2010. Cyber/Communications Security was 1st, Workplace Violence Prevention/Response was 2nd and Business Continuity Planning/Organizational Resilience was 3rd place. Intellectual Property/Brand Protection/Product Counterfeiting moved up to 4th place from 7th place and Global Supply-Chain Security remained at 5th place in 2012.

Figure 6

Top Threats by Industry - Manufacturing			
Total Respondents Rank 2012	Rank Within Industry 2012	Security Threats	Rank Within Industry 2010
1	1	Cyber/Communications Security (e.g., Internet/intranet security)[a]	1
2	2	Workplace Violence Prevention/Response	2
3	3	Business Continuity Planning/Organizational Resilience	3
11	4	Intellectual Property/Brand Protection/Product Counterfeiting	7
20	5	Global Supply-Chain Security	5
16	6 (tie)	Business Espionage/Theft of Trade Secrets	4
4	6 (tie)	Employee Selection/Screening	9
6	8	General Employee Theft	12
7	9	Crisis Management and Response: Political Unrest/ Regional Instability/National Disaster (evacuation potential)	13
13	10 (tie)	Substance Abuse (drugs/alcohol in the workplace)	15
5	10 (tie)	Property Crime (e.g., external theft, vandalism)	14

a. Prior to 2012, this attribute was Internet/Intranet Security (including e-mail/e-commerce).

B. Finance and Insurance

The top security threat for 2012 in the Finance and Insurance industry was Cyber/Communications Security, moving up from 2nd place in 2010. Workplace Violence Prevention/Response dropped from 1st place in 2010 to 2nd place in 2012. Business Continuity Planning/Organizational Resilience remained in 3rd place. Fraud/White-Collar Crime moved into 4th place from 6th place and Executive Protection dropped to 5th place from 4th place in 2012.

Figure 7

Top Threats by Industry - Finance and Insurance			
Total Respondents Rank 2012	Rank Within Industry 2012	Security Threats	Rank Within Industry 2010
1	1	Cyber/Communications Security (e.g., Internet/intranet security)[a]	2
2	2	Workplace Violence Prevention/Response	1
3	3	Business Continuity Planning/Organizational Resilience	3
12	4	Fraud/White-Collar Crime	6
18	5	Executive Protection (including travel security)[b]	4
10	6 (tie)	Identity Theft	7
4	6 (tie)	Employee Selection/Screening	10
8	8	Unethical Business Conduct	9
11	9	Intellectual Property/Brand Protection/Product Counterfeiting	11
7	10	Crisis Management and Response: Political Unrest/ Regional Instability/National Disasters (evacuation potential)	5

a. Prior to 2012, this attribute was Internet/Intranet Security (including e-mail/e-commerce).
b. Prior to 2012, this attribute was two separate attributes: Executive Protection and Travel Security.

C. Utilities

In 2012, Cyber/Communications Security was the security threat of greatest concern in the Utilities industry. Business Continuity Planning/Organizational Resilience remained in 2nd place while Workplace Violence Prevention/Response dropped to 3rd place. Bombings/Bomb Threats moved to 4th place in 2012 from 12th place in 2010. Property Crime moved up to 5th place from 6th place while Terrorism dropped to 6th place from 5th place. Identity Theft made a major jump from 19th place to 7th place in 2012.

Figure 8

Top Threats by Industry - Utilities			
Total Respondents Rank 2012	Rank Within Industry 2012	Security Threats	Rank Within Industry 2010
1	1	Cyber/Communications Security (e.g., Internet/intranet security)[a]	1
3	2	Business Continuity Planning/Organizational Resilience	2 (tie)
2	3	Workplace Violence Prevention/Response	2 (tie)
19	4	Bombings/Bomb Threats	12
5	5	Property Crime (e.g., external theft, vandalism)	6
15	6	Crisis Management and Response: Terrorism	5
10	7	Identity Theft	19 (tie)
4	8	Employee Selection/Screening	4
6	9	General Employee Theft	7 (tie)
7	10	Crisis Management and Response: Political Unrest/ Regional Instability/National Disasters (evacuation potential)	7 (tie)

a. Prior to 2012, this attribute was Internet/Intranet Security (including e-mail/e-commerce).
b. Prior to 2012, this attribute was two separate attributes: Executive Protection and Travel Security.

D. Retail Trade

To Fortune 1000 retailers and related companies, Cyber/Communications Security, which ranked 6th in 2010, moved to 1st place as the security threat of greatest concern in 2012. Property Crime moved up from 6th place to 2nd place in 2012. General Employee Theft dropped from 2nd to 3rd position and Identity Theft moved up to a 3rd place tie from 9th place.

Figure 9

Top Threats by Industry - Retail Trade			
Total Respondents Rank 2012	Rank Within Industry 2012	Security Threats	Rank Within Industry 2010
1	1	Cyber/Communications Security (e.g., Internet/intranet security)[a]	6 (tie)
5	2	Property Crime (e.g., external theft, vandalism)	6 (tie)
6	3 (tie)	General Employee Theft	2
10	3 (tie)	Identity Theft	9
14	5	Environmental/Social: Robberies	1
2	6 (tie)	Workplace Violence Prevention/Response	3
8	6 (tie)	Unethical Business Conduct	4
23	6 (tie)	Labor Unrest	27 (tie)
7	9 (tie)	Crisis Management and Response: Political Unrest/ Regional Instability/National Disasters (evacuation potential)	10 (tie)
3	9 (tie)	Business Continuity Planning/Organizational Resilience	12

a. Prior to 2012, this attribute was Internet/Intranet Security (including e-mail/e-commerce).

E. Information

Cyber/Communications Security continues to be the security threat of greatest concern in the Information industry in 2012. Business Continuity Planning/Organizational Resilience remained in 2nd position, tied with Fraud/White Collar Crime, which moved up to 2nd position from 7th position. Identity Theft moved up to 4th place in 2012 from 8th place in 2010 and Employee Selection/Screening moved from 10th place in 2010 to 5th place in 2012.

Figure 10

Top Threats by Industry - Information			
Total Respondents Rank 2012	Rank Within Industry 2012	Security Threats	Rank Within Industry 2010
1	1	Cyber/Communications Security (e.g., Internet/intranet security)[a]	1
3	2 (tie)	Business Continuity Planning/Organizational Resilience	2
12	2 (tie)	Fraud/White-Collar Crime	7
10	4	Identity Theft	8
4	5	Employee Selection/Screening	10 (tie)
2	6	Workplace Violence Prevention/Response	5
11	7 (tie)	Intellectual Property/Brand Protection/Product Counterfeiting	9
5	7 (tie)	Property Crime (e.g., external theft, vandalism)	20
16	9	Business Espionage/Theft of Trade Secrets	3
8	10	Unethical Business Conduct	6

a. Prior to 2012, this attribute was Internet/Intranet Security (including e-mail/e-commerce).


11:23 AM
we engage globally
engaging with people
and issues locally,
nationally and
internationally

F. Healthcare and Social Assistance

Workplace Violence Prevention/Response and Cyber/Communications Security continue to be the security threats of greatest concern in the Healthcare and Social Assistance industry in 2012. Both held their positions with Workplace Violence Prevention/Response as the number one concern and Cyber/Communications Security as the number two concern. Business Continuity Planning/Organizational Resilience moved up to 3rd place from 12th place. Employee Selection/Screening moved up from 5th to 4th place, while General Employee Theft remained in 5th place.

Figure 11

Top Threats by Industry - Healthcare and Social Assistance			
Total Respondents Rank 2012	Rank Within Industry 2012	Security Threats	Rank Within Industry 2010
2	1	Workplace Violence Prevention/Response	1
1	2	Cyber/Communications Security (e.g., Internet/intranet security)[a]	2
3	3	Business Continuity Planning/Organizational Resilience	12 (tie)
4	4	Employee Selection/Screening	5 (tie)
6	5	General Employee Theft	5 (tie)
11	6	Intellectual Property/Brand Protection/Product Counterfeiting	24
5	7	Property Crime (e.g., external theft, vandalism)	7
13	8	Substance Abuse (drugs/alcohol in the workplace)	10
7	9 (tie)	Crisis Management and Response: Political Unrest/ Regional Instability/National Disasters (evacuation potential)	17 (tie)
14	9 (tie)	Environmental/Social: Robberies	11

a. Prior to 2012, this attribute was Internet/Intranet Security (including e-mail/e-commerce).

G. Real Estate, Rental and Leasing

For management security threats in the Real Estate, Rental and Leasing industry, Property Crime moved from 2nd place in 2010 to 1st place as the security threat of greatest concern in 2012. Employee Screening/Selection moved into 2nd place from 7th place. Litigation: Negligent Hiring/Supervision moved up to 3rd place from 11th place and tied with General Employee Theft, which moved up from 15th place. Workplace Violence Prevention/Response dropped from 1st place in 2010 to 5th place in 2012.

Figure 12

Top Threats by Industry - Real Estate, Rental and Leasing			
Total Respondents Rank 2012	Rank Within Industry 2012	Security Threats	Rank Within Industry 2010
5	1	Property Crime (e.g., external theft, vandalism)	2 (tie)
4	2	Employee Selection/Screening	7 (tie)
17	3 (tie)	Litigation: Negligent Hiring/Supervision	11 (tie)
6	3 (tie)	General Employee Theft	15 (tie)
2	5	Workplace Violence Prevention/Response	1
14	6	Environmental/Social: Robberies	2 (tie)
10	7	Identity Theft	14
3	8 (tie)	Business Continuity Planning/Organizational Resilience	6
7	8 (tie)	Crisis Management and Response: Political Unrest/ Regional Instability/National Disasters (evacuation potential)	11 (tie)
9	8 (tie)	Litigation: Inadequate Security	15 (tie)

a. Prior to 2012, this attribute was Internet/Intranet Security (including e-mail/e-commerce).

H. Transportation and Warehousing

In the Transportation and Warehousing industry, Terrorism was the security threat of greatest concern. Business Continuity Planning/Organizational Resilience and Bombings/Bomb Threats were tied for 2nd position. Workplace Violence Prevention/Response remained in 4th position.

Figure 13

Top Threats by Industry - Transportation and Warehousing			
Total Respondents Rank 2012	Rank Within Industry 2012	Security Threats	Rank Within Industry 2010
15	1	Crisis Management and Response: Terrorism	7 (tie)
3	2 (tie)	Business Continuity Planning/Organizational Resilience	2 (tie)
19	2 (tie)	Bombings/Bomb Threats	16
2	4	Workplace Violence Prevention/Response	4
4	5 (tie)	Employee Selection/Screening	5 (tie)
7	5 (tie)	Crisis Management and Response: Political Unrest/ Regional Instability/National Disasters (evacuation potential)	9 (tie)
6	7	General Employee Theft	13 (tie)
5	8	Property Crime (e.g., external theft, vandalism)	1
1	9	Cyber/Communications Security (e.g., Internet/intranet security)[a]	2 (tie)
9	10 (tie)	Litigation: Inadequate Security	7 (tie)
20	10 (tie)	Global Supply-Chain Security	9 (tie)

a. Prior to 2012, this attribute was Internet/Intranet Security (including e-mail/e-commerce).

A list of 16 security management topics was shown with the following instruction: "Rate between 5 (most important) and 1 (least important) the following security management issues with regard to their anticipated impact on your company's security program during the next 12 months." Results are shown graphically (Figure 14).

Budget/Maximizing Return On Investment held the top position for 2012 security management issues. Promoting Employee Awareness was 2nd, Training Effectiveness/Methods was 3rd and Implementing Best Practices/Standards/Key Performance Indicators was 4th. Threat Assessments ranked 5th. The top security management issues ranked 6th through 10th: Keeping Up With Technological Advances, Adequate Security Staffing, Selection and Hiring Methods for Security Staffing, Strategic Planning and Regulatory/Compliance Issues.

Figure 14

2012 Rank	Management Issues	Average Importance Score
1	Budget/Maximizing Return On Investment	3.91
2	Promoting Employee Awareness	3.90
3	Security Staffing Effectiveness: Training Effectiveness/Methods	3.86
4	Implementing Best Practices/Standards/Key Performance Indicators	3.77
5	Threat Assessments	3.72
6	Keeping Up With Technological Advances	3.69
7	Security Staffing Effectiveness: Adequate Staffing Levels	3.67
8	Security Staffing Effectiveness: Selection and Hiring Methods	3.66
9	Strategic Planning	3.63
10	Regulatory/Compliance Issues (e.g., OSHA, C-TPAT, state/federal legislation, etc.)	3.58
11	Managing Remote Security Operations	3.35
12	Security Staffing Effectiveness: Security Officer Turnover	3.34
13	Additional Security Responsibilities (aviation/compliance/ethics, etc.)	3.20
14	Career Development	3.18
15	Security Staffing Effectiveness: Absenteeism	3.08
16	Global Supply Chain Decisions	2.74

Reporting Relationships

Corporate security reporting relationships were diverse and showed little organizational consistency across the Fortune 1000. The largest groups (16%) report to the Facilities area or Administration. Operations (13%), CEO/President (12%), Human Resources (11%), Environmental/ Health/Safety (11%), Legal (9%) and Risk Management (7%) were the next most frequently mentioned areas.

Responses are summarized in Figure 15.

Figure 15

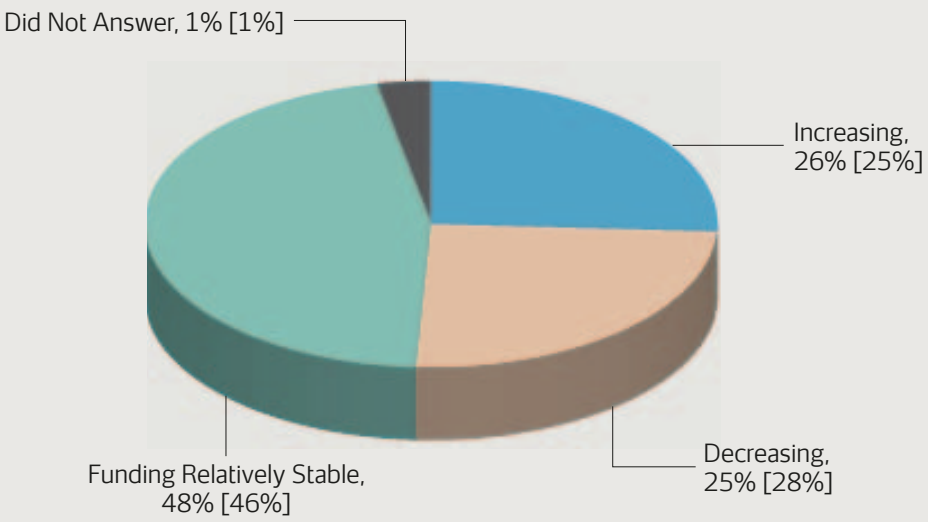
Organizational Area	2012	2010
Administration	16%	12%
Facilities	16%	19%
Operations	13%	10%
Directly to the CEO/President	12%	12%
Human Resources	11%	10%
Environmental/Health/Safety	11%	7%
Legal	9%	12%
Risk Management	7%	6%
Audit	2%	2%
Finance	2%	7%
IT/MIS	2%	2%
Did not answer	1%	1%

Sum of percentages is greater than 100% due to multiple responses.

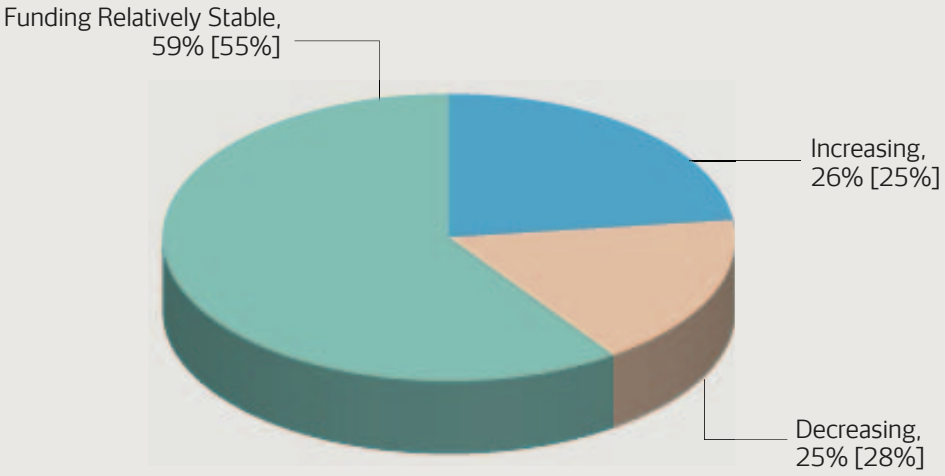
Funding Trends

The funding outlook for corporate security programs over the next three to five years showed some slight change from the 2010 estimates, with 23% of security managers expecting an increase in funding, down from 27% in 2010. The percentage of security managers expecting budgets to remain the same was 59% in 2012, up slightly compared to 55% in 2010. The percentage of managers anticipating decreased funding was 17%, compared to 16% in the previous survey.
Note: The percents in the [brackets] below are 2010 percentages.

Security Funding: Past 3 - 5 Years



Security Funding: Next 3 - 5 Years



A. Survey Methodology

For the 2012 survey "Top Security Threats and Management Issues Facing Corporate America," Securitas USA identified corporate security professionals at Fortune 1000 headquarters locations and compiled a proprietary database of these contacts. Sparks Research, a national marketing research firm, coordinated the research. The survey package included a four-page survey questionnaire, cover letter and postage-paid return envelope. This package was mailed to 1,165 security directors and other executives identified as having oversight of the corporate security function of these companies. The survey questionnaire was distributed in December 2012. Respondents were asked to complete and return the surveys via mail, fax or e-mail. This year respondents were offered an additional option to complete the survey online via a link and password provided in the cover letter. Results were compiled and analyzed in January 2013.

Reflected in this report are the responses taken from 297 returned surveys, which represent a 25.5% response rate. Previous years' results were based on a similar methodology. As in past years, the survey questionnaire was modified slightly to address current issues and to improve its reliability, yet the overall survey has remained largely consistent.

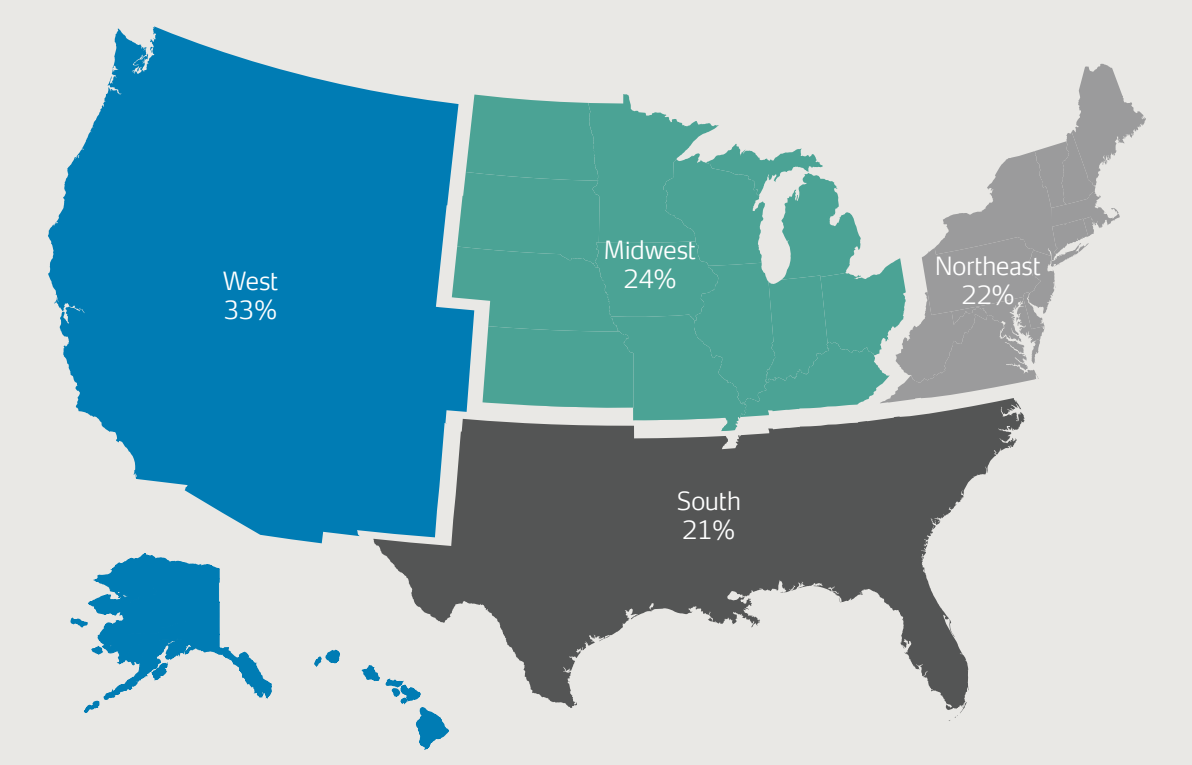
B. Respondent Distribution

Twenty-one specific industries are represented in the returned surveys; smaller industry groups were aggregated into broader categories to permit analysis of the results by industry sector. Segmentation of the total sample should be considered in the context of the Fortune 1000, which does not represent every industry and is more densely populated by the industries most heavily weighted here. Respondents selected their primary industry affiliation from a predefined list shown below.

Industry Classification Main/Sub-Industry	Total Respondents
Utilities	15
Construction	2
Wholesale Trade	4
Retail Trade	8
Healthcare and Social Assistance	23
Arts, Entertainment and Recreation	21
Finance and Insurance	35
Real Estate, Rental and Leasing	23
Professional, Scientific and Technical Services	16
Educational Services	10
Accommodation and Food Services	2
Transportation and Warehousing	24
Law Enforcement	6
Manufacturing	**90**
Food Manufacturing	18
Wood Product Manufacturing	4
Computer and Electronic Product Manufacturing	9
Electrical Equipment, Appliance and Component Manufacturing	10
Transportation Equipment Manufacturing	15
Miscellaneous Manufacturing	34
Information	**14**
Telecommunications	8
Other Information Services	6
Other	**4**
TOTAL	**297**

C. Geographic Distribution

Responses from 42 states were represented in the survey results. For illustrative purposes, geographic distribution is grouped into four regions of the U.S. as shown in the following chart:




SECURITAS
Security for your industry
About Securitas USA
Welcome to SecuritasVision

Cyber Security is Built on Relationships and Relentlessness

TIM WILLIAMS, CPP

Most of us are not surprised that, for the second year in a row, cybercrime ranks number one on Securitas USA's survey of "Top Security Threats and Management Issues Facing Corporate America." We might want it to be a blip on the security screen (pun intended), but we know that cyber security will remain a priority—an increasingly challenging one.

When the physical and cyber security teams converged at Caterpillar in late 2011, we defined several keys to successfully battling cybercrime. We rely on our team's expertise wherever possible, but we also recognize that partnerships with other companies and government groups are fundamental to staying ahead of this curve. Sharing what we learn is also crucial. Our lessons learned are many, and I would like to share a few with you in hopes of sparking additional ideas.

Combating Cybercrime: Six Keys to Success

1. **Prevention cannot be our sole passion.** No firewall can be built high enough, no anti-virus software updated quickly enough and no one piece of technology sophisticated enough to prevent all breaches. At Caterpillar, we build employee awareness about behaviors that can help prevent data loss, but we stress professional detection and response. Attacks will occur; knowing when and mitigating damage are today's necessities.

2. **Solutions will come from companies that do not currently exist.** Staying "in the loop" has taken on heightened meaning. Companies offering the best cyber security solutions may not exist for three to five years. Staying keenly aware of changing dynamics, the latest information from industry experts and emerging solutions are fundamental to being expert advisors to management.

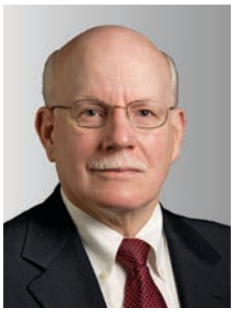
3. **An "intelligence-driven" process delivers better results.** Understanding who is coming after you, how and, if possible, when are the building blocks of cyber security. Government/private cooperation is vital but may not develop quickly enough to be effective in the corporate landscape. What we can do is create industry "safe harbors" for exchanging attack methodologies and other information without extending the liability of our firms.

4. **Expect the unexpected.** Have "intelligence" but also be prepared for anything. More time, research and "at the speed of the web" communications are often necessary to determine the next attack vectors. It's important to put in writing your strategy for detection and response, and act on it accordingly.

5. **Converging security organizations can eliminate redundancies and reflect interdependencies.** Anything attached to an IP address poses a risk to the entire infrastructure, including video cameras and access control. At Caterpillar, we are fortunate that our relationship with Securitas keeps our physical security attributes top-notch and helps to ensure that our converged solutions are properly designed, managed and maintained.

6. **Link security investments to strategy.** Having a carefully considered, clearly articulated, board-level strategy is essential to cyber security. What starts with a logical, contemporary risk assessment then becomes a clear delineation for levels of security applied to various areas and functions based on risk. Aligning risks to business drivers (the cash registers, so to speak) will become your business case for additional spending if an attack comes out of nowhere or morphs into a new, more threatening form.

At Caterpillar, the last two years have proven that managing risks today requires a clear vision and an agile team. Building relationships and keeping the keys to success top of mind are helping us suspect, detect and respond to cyber threats. Remaining relentless will assure we stay there.



Timothy L. Williams, CPP, is the Director of Information Risk and Enterprise Security for Caterpillar Inc. Williams is charged with the continued growth of global security for the enterprise.

Prior to joining Caterpillar in December 2006, Williams was the Chief Security Officer for Nortel. He also served as Vice President, Business Ethics. Prior to joining Nortel in 1987, Williams was Director of Corporate Security Services of Boise Cascade Corporation and an International Security Coordinator for Procter & Gamble.

Williams has conducted significant research into fraud and related ethics issues and has written extensively on these subjects for *Internal Auditor, Security Management Magazine* and *Security Journal*. He twice received the *Outstanding Contributor Award* from *Internal Auditing Magazine* and the Institute of Internal Auditing, and is co-author of the book *Fraud: Bringing Light to the Dark Side of Business*. He previously served as the Managing Editor of the *Protection of Assets Manual* and *Protection of Assets Bulletin*. Williams has been quoted in the *Wall Street Journal, New York Times, Globe & Mail* and *Financial Times*, among other publications.

Williams holds a MBA degree from the University of Toronto and a BS degree from the University of Cincinnati. He is a member of the Information Security and Audit Association and the Information Systems Security Association. He served as President of ASIS International in 2008.

Robert Dodge, CPP, is the Sr. Vice President - International for Pinkerton and has been involved in security, investigations and security consulting for 20 years. He also served honorably in the U. S. Navy. His investigation experience includes stints with a multinational high tech corporation as a corporate investigator. He also worked for a private investigation firm providing investigation and security consulting services on a global level to corporate clientele based in Silicon Valley. His security experience includes working with the Securitas Group as a Vice President in Northern California. In his current role as Senior Vice President, Dodge is responsible for managing all of Pinkerton's international offices and operations. He has operated on security and investigative projects in more than 60 countries. He has special expertise in corporate investigations and risk/vulnerability/threat assessments. Dodge has been designated a Certified Protection Professional (CPP).

He is an active member of ASIS International, Chief Special Agent Association, FBI Infragard Program, U.S. Secret Service, Electronic Crimes Task Force, California Association of Licensed Investigators and Intelnet.

Dodge is a constituent with the State Department Overseas Security Advisory Council and the FBI'S Domestic Security Advisory Council.

Dodge also serves on the ASIS International committee for the development of International risk assessment guidelines and standards.

Unethical Business Conduct

A 21st Century International Business Reality

ROBERT DODGE, CPP

Unethical Business Conduct has ranked among the "Top Ten Security Threats and Management Issues Facing Corporate America" every year since 1997. Everywhere we turn, there are stories of unethical personal and business conduct appearing in the media. It is no surprise that corporate America continues to be concerned about this subject, especially in the global arena.

Unethical business conduct can negatively impact an organization by damaging credibility, brand and reputation, as well as potentially causing significant loss of customers and business failure.

Unethical business conduct comes in many forms:

- **Financial misconduct** – to include bribery, fraud, tax evasion and price fixing
- **Mistreating employees** – abuse of workers (especially in the global supply chain), child labor, sweat shops, and illegal practices
- **Misrepresentation** – to include false marketing, falsified data on corporate reports, conflicts of interest and lying for financial gain

The importance of international business ethics and conduct has been rising steadily alongside the themes of globalization, virtualization and the rapid technology changes occurring within the global business landscape, and the dynamic shift of organizations' workforce compositions in many of these emerging global markets. The primary problem of unethical international business conduct is that many of the people, cultures and nations where U.S. companies do business embrace entirely different standards of both ethics and conduct than in the U.S.

A primary challenge for U.S. organizations doing business internationally is in the area of standards for employment practices, as they are inconsistent at best from one country to the next in many of the emerging markets. As a result, outside of the organizations' own decisions to enforce infractions of unethical business conduct, often no legal or governmental response is available in these markets to employers.

Let's also look at bribery as an example of unethical business conduct. This is one of the most difficult areas with which to deal on a global basis. The U.S. has aggressively adopted the provisions and enforcement of the Foreign Corrupt Practices Act (FCPA) to crack down on U.S. organizations and their employees who engage in, for example, illegitimate bribing to gain business from foreign governments. However, there are as many different views internationally on bribery as there are different cultures. Some see bribery as expected within their culture, while others view it as a very minor issue not worthy of prosecution. This can potentially lead to unethical business conduct along with a lack of available governmental and legal enforcement remedies.

Steps that businesses can take to help prevent unethical business conduct include:

- **Proper hiring** – study employees' values to ensure they match the company's values.
- **Code of conduct** – provide employees with a framework of what the company expects from them.
- **Lead by example** – ethical and proper business conduct needs to start at the top of the organization and permeate all levels of management.
- **Limit the opportunity** – have strong security controls, processes and procedures in place that minimize opportunities for unethical business conduct.
- **Employee appreciation** – loyal employees are less likely to participate in unethical business conduct.
- **Trust but verify** – Audits and compliance checks of business processes should be a standard operating practice, especially in international operations.

The bottom line is that good ethical business conduct helps to drive long-term shareholder value as well as brand and reputation. It is in the best interest of U.S. organizations to actively monitor themselves and strive for high integrity outcomes in both their external and internal dealings.

Business Continuity Planning

VINCENT MACNEILL, CPP

Two closely-related measures of the strength of any organization are its resiliency (its ability to return to normal operations after a disruptive event) and its business continuity (its ability to continue essential business operations despite that event). Resilience and continuity are also important to each division within an organization, and particularly so to its security operations. The last year has seen some challenges, but also two strategically important advances, in business continuity planning.

Initially, continuity plans mainly involved response to enterprise-specific property issues: if there's an explosion, how fast can we get the facility up and running again? What'll we do if our IT system crashes? Those concerns are still valid, but other issues are now moving to the front burner: interdependencies, personnel, supply chains and standards.

Business operations are dependent on external critical infrastructure, and business continuity plans must address those dependencies. Hurricane Sandy forcefully reminded us of the fragility of our infrastructures, with cascading failures such as power outages lasting longer because transportation gridlock delayed hundreds of responding bucket trucks. While many businesses suffered directly from physical damage, far more were impacted indirectly by critical infrastructure disruption.

Business operations are dependent on workers—hence the power of strikes. But workforces can be interrupted for other reasons. Workers show up at the office or plant only if they're both able and willing. Disasters can disrupt both ability and willingness, particularly if loyalty to the job conflicts with concern about families. A 2010 Columbia University study involving 1,100 emergency services personnel predicted that in the event of an influenza pandemic, only 49% of them would continue to work; specifically: 53% of police and fire personnel, 50% of paramedics, 43% of hospital workers, and 37% of corrections personnel. Emergency responders are highly dedicated: if 50% of them are staying home, what will other public and private workers do?

All businesses are dependent on goods and services provided by their suppliers and vendors, and need to supply their own goods and services to their customers. Supply chain disruptions on either end can put an organization out of business. In 2012, the White House issued a National Strategy for Global Supply Chain Security. President Obama summarized: "Disruptions to supply chains caused by natural disasters … and from criminal and terrorist networks … can adversely affect global economic growth and productivity.… We will … [foster] a resilient system that can absorb and recover rapidly from unanticipated disruptions." International treaties, congressional legislation, and proposed federal regulations will clarify how the strategy will be implemented, and how businesses will be affected. However, securing the supply chain would significantly protect business continuity.

Of even greater significance, in 2012 ISO 22301 and 22313 were issued to define business continuity management system requirements and provide guidance for such systems. With ISO certification as a primary demonstration of a company's resilience, expect the race to get certified, and to select suppliers and vendors who are also certified, to define and energize business continuity planning globally.

Vincent MacNeill, CPP, is the Securitas USA Vice President, Program Development for Critical Infrastructure Division. A 29 year Securitas USA veteran, MacNeill has been Area Vice President for Louisiana, Mississippi and Oklahoma, and Regional Manager for the South Central and Mid-Atlantic States.

Bruce Wimmer, CPP, is the Director of Global Consulting for Pinkerton. He is responsible for providing guidance and risk assessment assistance for Pinkerton and Securitas offices around the globe. He has more than 40 years of experience in law enforcement (nearly 22 years in the U.S. Air Force, mostly as a Special Agent in the Office of Special Investigations where he specialized in counter-espionage) and as a manager in Pinkerton offices in Taiwan, the People's Republic of China, Hong Kong SAR. He has lived and worked in a number of different countries in Europe, Asia and Latin America. As a Pinkerton manager, he has been a company focal point for helping organizations design programs to counter business spying. He also leads the Pinkerton Supply Chain Security Division. He is a Certified Protection Professional and has spoken multiple times about business espionage at the annual ASIS Seminar and Exhibits. He has assisted the American Water Works and U.S. Customs and Border Protection in developing risk assessment methodologies.

Business Espionage

BRUCE WIMMER, CPP

Sometimes survey results are interesting because they reveal as much about our lack of understanding of a particular threat, as with our insightful perception of other threats. While it is no surprise that Cyber Security is the number one perceived threat in this latest survey, what should be a surprise is that, with Cyber Security at #1, Business Espionage is down at #16.

Experts in government and the private sector agree that the main objective with business related cyber penetrations is the desire to get sensitive business information. Chip Tsantes of Ernst & Young advised that many of the cyber-attacks are designed to steal intellectual property. Ilias Chantzos of Arbor Network, testifying to a House of Lords EU Subcommittee, said, "Cyber-attacks are more focused now on stealing information than denial of service" or other crimes.

In March of 2013, the White House released its "Administrative Strategy on Mitigating the Theft of U.S. Trade Secrets." That report noted that 26 U.S. government agencies and 21 private sector organizations had worked together and determined that the main focus for addressing economic collection and industrial espionage was the threat from cyberspace. Again, cyber threats were directly linked to business/industrial espionage. In reality, cyber security compromises might often be better defined as a method or tool used to conduct business espionage.

Perhaps the reason for the strange cyber security/business espionage dichotomy might lie in what the *New York Times* reported in an analysis several years ago. The *New York Times* concluded that business espionage is one of the most under reported security threats facing companies and one of the main reasons is that it is one of the least understood threats that organizations face. The past two survey results tend to indicate that is still true.

While cyber security should undoubtedly be at the top of threats we face in business, if cyber security is #1, business espionage should probably be very closely linked to that threat, especially in terms of the potential consequences and risk to the business enterprise. Organizations should endeavor to have a better understanding of the business espionage threat, especially as it relates to the cyber security threat.

Employee Selection/Screening

MARK GERACI, CPP, CFE

It is not surprising that Employee Selection/Screening was identified as the #4 threat in the most recent "Top Security Threats and Management Issues Facing Corporate America" survey.

Resume fraud occurs at every level of any organization, including in the C-suite. Senior executives at well-known organizations such as Yahoo, RadioShack, and Bausch & Lomb, as well as academic institutions such as MIT and Notre Dame, have all experienced the embarrassment caused by resume fraud. Although hard to measure, the financial impact has been estimated by the Association of Certified Fraud Examiners in its 2002 study as being "$600 billion annually, or about $4,500 per employee." Other startling statistics include the following: a report that 70% of college students said they lied on their resume; according to SHRM (Society for Human Resource Management), 61% of its members said they "often" or "sometimes" find resume inaccuracies when vetting prospective hires; according to the FBI, approximately half a million people in the United States falsely claim to have college degrees; according to the website www.fakeresume.com, 80% of all resumes are misleading and 20% state fraudulent degrees. All of these examples and many more instances of resume fraud present a very serious security threat.

What appear to be the most common resume lies often include exaggerating education or the fabrication of degrees, falsifying credentials, omitting past employment, enhancing job titles and responsibilities, and lying about reasons for leaving a previous job. Moreover, applicants misrepresent military records, such as what occurred at Fox News when a consultant who was hired claimed to be a former Special Forces Lieutenant Colonel and war hero. Ultimately, it was learned that his military background consisted only of approximately 40 days of basic training. While the majority of organizations performs background checks on potential employees, these processes can vary greatly, with some organizations simply contacting references provided by the applicant to others hiring investigators to check every detail of the individual's resume. Some experts believe that the prevalence of resume fraud actually increases when the economy worsens. However, this type of fraud always seems to be present, regardless of economic conditions.

For these very reasons, ASIS International's Commission on Standards and Guidelines published a Pre-employment Background Screening Guideline in 2009. The Guideline is quite comprehensive and can serve as an excellent tool for use by any security or human resource professional in building a strong employee selection and screening process. The Guideline provides information concerning legal issues and the legal landscape affecting the pre-employment background screening process, the methods of structuring a pre-employment background screening program, and a number of ways to verify important items such as education, criminal history, credit reports, etc.

Although time consuming and costly, it is far better to pay now than to pay later by simply taking reasonable steps to appropriately screen those who enter our work force. As it is often said—"our employees are our greatest asset." At the very least, we should know they are who they say they are.

F. Mark Geraci, CPP, CFE, is the Vice President and Chief Security Officer of Purdue Pharma L.P. Geraci received an MBA from New York Institute of Technology; a BS Degree in Accounting from The State University of New York (ESC) at Stony Brook; and a BAA Degree in Criminal Justice from Florida Atlantic University, Boca Raton, FL.

In 1978 Geraci joined the New York State Attorney General's office as a special investigator. He joined Bristol-Myers Squibb Company as a Staff Assistant (Special Projects Group) in 1982, and held increasingly responsible positions of Manager of Investigations, Director, Corporate Security and, Senior Director – Corporate Security.

Geraci has been a representative to the U.S. Department of State, Overseas Security Advisory Council, since 1987. He is a member of ASIS International and served on the ASIS Board of Directors from 1993-1998; President of ASIS in 1998; and Chairman of the Board in 1999. He was the Chairman of the ASIS White Collar Crime Committee from 1990-1992. He is Chairman of the ASIS Commission on Standards and Guidelines and is a member of the ASIS CSO Roundtable. He is a member of ISMA (International Security Management Association), admitted as a Certified Fraud Examiner (CFE) by the Association of Certified Fraud Examiners, a Certified Protection Professional (CPP), and a Yale-Stimson Fellow with the University's Center for International and Area Studies.

Securitas Security Services USA is the most locally-focused security company in the United States, with over 450 local branch managers and nearly 100,000 security officers who provide unmatched security solutions to meet the specific needs of thousands of businesses. Internationally, the Securitas Group has approximately 300,000 employees worldwide, with established operations in more than 50 countries. We are committed to providng focused, responsive service at the local and international levels.

Securitas USA's services include on-site and remote guarding services, mobile patrols and inspections, access control, concierge and receptionist services, security console operators, alarm response, and specialized client requested services. Securitas USA is a leading security company that works with more than 80 percent of the Fortune 1000 companies and has annual revenues in excess of $3 billion.

For more information about Securitas USA, visit www.securitasinc.com

Top Security Threats and Management Issues Facing Corporate America Editorial Staff:
Don Walker, CPP; Lynne Glovka; Bernard Greenawalt, CPP; Jim McNulty

For additional copies of this publication, contact Lynne.Glovka@securitasinc.com

Securitas Security Services USA, Inc.
Two Campus Drive
Parsippany, NJ 07054
877-281-5543
www.securitasinc.com