Top Security Threats and Management Issues Facing Corporate America

2016 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 40 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.

Securitas Security Services USA, Inc. has completed its 2016 "Top Security Threats and Management Issues Facing Corporate America" survey. We are pleased to publish the findings of the survey in this report.

Over the years, this survey has become an industry standard and is often used by corporate security managers in numerous markets for security-related data when making decisions relative to security planning. I want to thank all of our respondents who participated, generating an excellent response rate from security executives in 39 states, Canada and Mexico. Your input is critical to our report and has revealed that the top five security threats for 2016 are as follows:

1. **Cyber/Communications Security: Internet/Intranet Security**
2. **Workplace Violence Prevention/Response**
3. **Active Shooter Threats**
4. **Business Continuity Planning/ Organizational Resilience**
5. **Cyber/Communications Security: Mobile Security**

It comes as no surprise that Cyber/Communications Security retained its #1 ranking from our three previous surveys, and Workplace Violence Prevention/Response rose in ranking to again be the #2 threat. What is surprising is that two threats never before listed in our survey—Active Shooter Threats and Cyber/Communications Security: Mobile Security—are #3 and #5, respectively. The high ranking of these new threats is undoubtedly an indicator of current events, both in the U.S. and globally.

The top security management challenges that were identified are: 1) Security Staffing Effectiveness: Training Effectiveness Methods, 2) Promoting Employee Awareness, and 3) Implementing Best Practices/Standards/Key Performance Indicators. An interesting observation about these rankings is that Budget/Maximizing ROI (ranked #1 in 2012 and #3 in 2014) dropped to 8th place in the 2016 survey.

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

We extend a special thanks to the security practitioners who contributed editorial commentary for this report, namely:

- **Tom Ridge**, Chairman, Ridge Global
- **Timothy Williams**, CPP, Chief Security Officer, Caterpillar Inc.
- **Charles Baley**, Chief Security Officer, Farmers Group, Inc.
- **Michael Howard**, Chief Security Officer, Microsoft Corporation
- **Gail Essen**, CPP, PSP, CEO, Professional Security Advisors
- **Richard Avery**, CPP, Northeast Region President, Securitas Security Services USA, Inc.

On behalf of the entire management team at Securitas USA, I hope you find the information contained in this report to be of value in assisting your organization to achieve its security objectives.

A Message From:

Don Walker, CPP

CHAIRMAN – SECURITAS SECURITY SERVICES USA, INC.

Thank you to our customers and friends for participating in the 2016 Securitas Top Security Threats Survey. Also, thank you to our guest authors who contributed their thoughts regarding current risks, threats or issues of concern to them and their organizations. We are grateful for their insights regarding strategy, use of technology, training and operating procedures. As risks change and new threats emerge, we hope you agree that the survey and the analysis of the data can be very useful tools in assisting organizations develop security prevention, detection, response and/or mitigation strategies and procedures.

One of the things that struck me in analyzing the data is that of the 29 threat categories, approximately one half can be caused or committed by insiders (current or former employees or trusted business partners/guests). Therefore, it is no surprise that Employee Selection/Screening and Rescreening always ranks in the top ten threats or issues concerning security executives. This year, we included "Insider Threats" as part of the overall category. Many of the incidents we see in the headlines are categorized as workplace violence, cyber-crimes, information compromise, identity theft or major frauds. Many of those incidents were, in fact, the direct result of a malicious insider or someone who circumvented adequate vetting.

Therefore, it may be useful for anyone concerned with the insider threat to refer to the "Common Sense Guide to Mitigating Insider Threats," published by Carnegie Mellon University's Software Engineering Institute. Many of the lessons learned in its case studies validate the need for a comprehensive physical security program working in concert with a proactive information security program. Our Pinkerton subsidiary and its partners are working closely with our customers to eliminate or mitigate the insider threat by using the data, strategies and tools addressed by the guest authors in this survey report.

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 life member of the International Security Management Association (ISMA), the Society of International Business Fellows (SIBF) and Leadership Nashville. He is a former 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 2016 "Top Security Threats and Management Issues Facing Corporate America" survey. This survey has become an industry standard and is often used by corporate security management in a wide range of industry sectors for security-related data when making decisions relative to security planning.

Securitas USA surveyed a wide range of security managers and directors from Fortune 1000 companies, facilities managers and others responsible for the safety and security of corporate America's people, property and information. The objective was to identify emerging trends related to perceived security threats, management challenges, and operational issues. This survey 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.

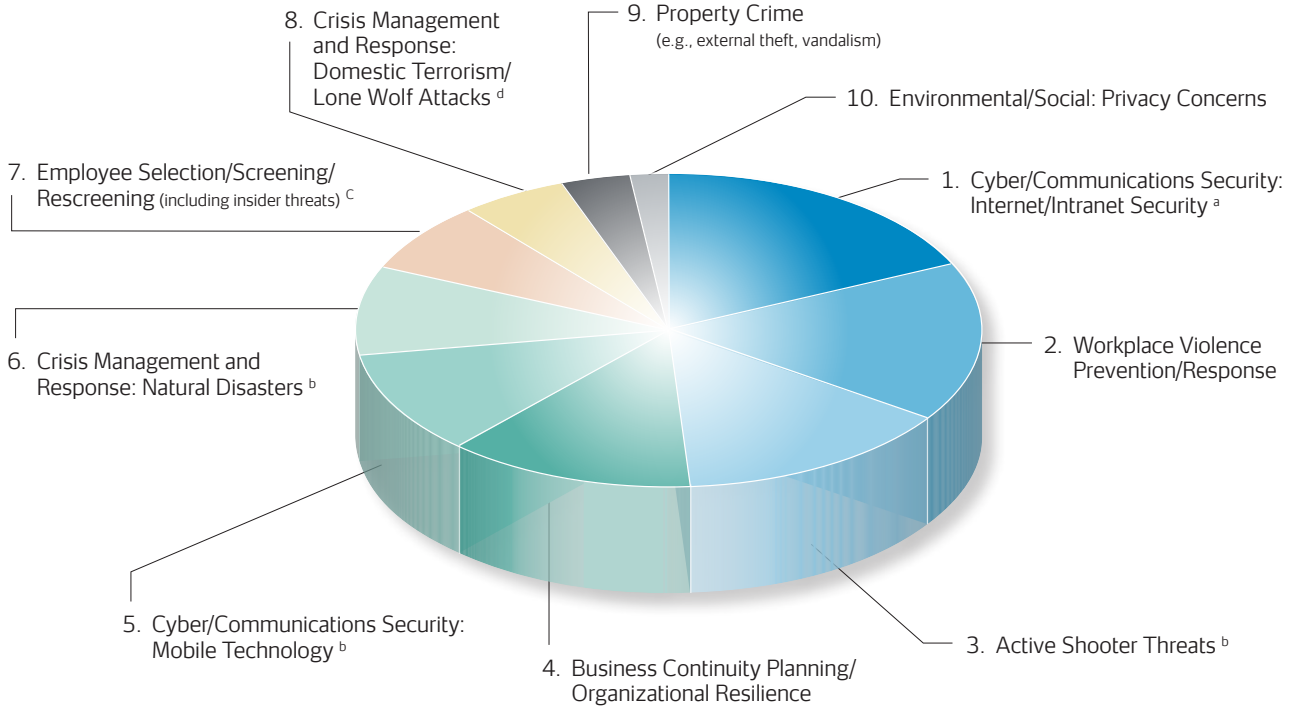
Today's Threat Environment

The study revealed the challenges of greatest concern to corporate security directors, in rank order (See Figure 1). The threat of Cyber/Communications Security: Internet/Intranet Security, formerly known as Cyber/Communications Security (e.g., internet/intranet security), remains the greatest security concern facing Fortune 1000 companies in 2016. Workplace Violence Prevention/Response moves back up to 2nd place in 2016 after holding this position from 2010-2012, and briefly moving to 3rd place in 2014. Active Shooter Threats, a new attribute in 2016, holds 3rd place, while Business Continuity Planning, including Organizational Resilience, falls 2 spots to 4th place after a 2nd place ranking in 2014.

A new breakout of Cyber/Communications Security, Mobile Technology, holds 5th place, while another new threat, Crisis Management and Response: Natural Disasters, holds 6th place. Newly-worded Employee Selection/Screening/Rescreening (including insider threats) moves down to the 7th spot in 2016, while it previously held 4th place from 2008-2014. Newly worded Domestic Terrorism/Lone Wolf Attacks maintains 8th place, a position it held in 2014, while Property Crime falls to the 9th place position in 2016 (from 6th place in 2014). Environmental/Social: Privacy Concerns falls to the 10th place position in 2016 (from 5th place in 2014).

Figure 1

2016 Top Security Threats



a. Prior to 2016, this attribute was known generally as: Cyber/Communications Security (e.g., internet/intranet security)
b. New attribute in 2016
c. Prior to 2016, this attribute was known generally as: Employee Selection/Screening
d. Prior to 2016, this attribute was known generally as: Crisis Management and Response: Domestic Terrorism

Professional Management Issues

A significant portion of the Securitas USA survey is devoted to identifying key management issues, as well as operational, staffing and budgetary issues facing corporate security executives. Figure 2 shows the operational issues of greatest concern revealed in 2016.

Figure 2

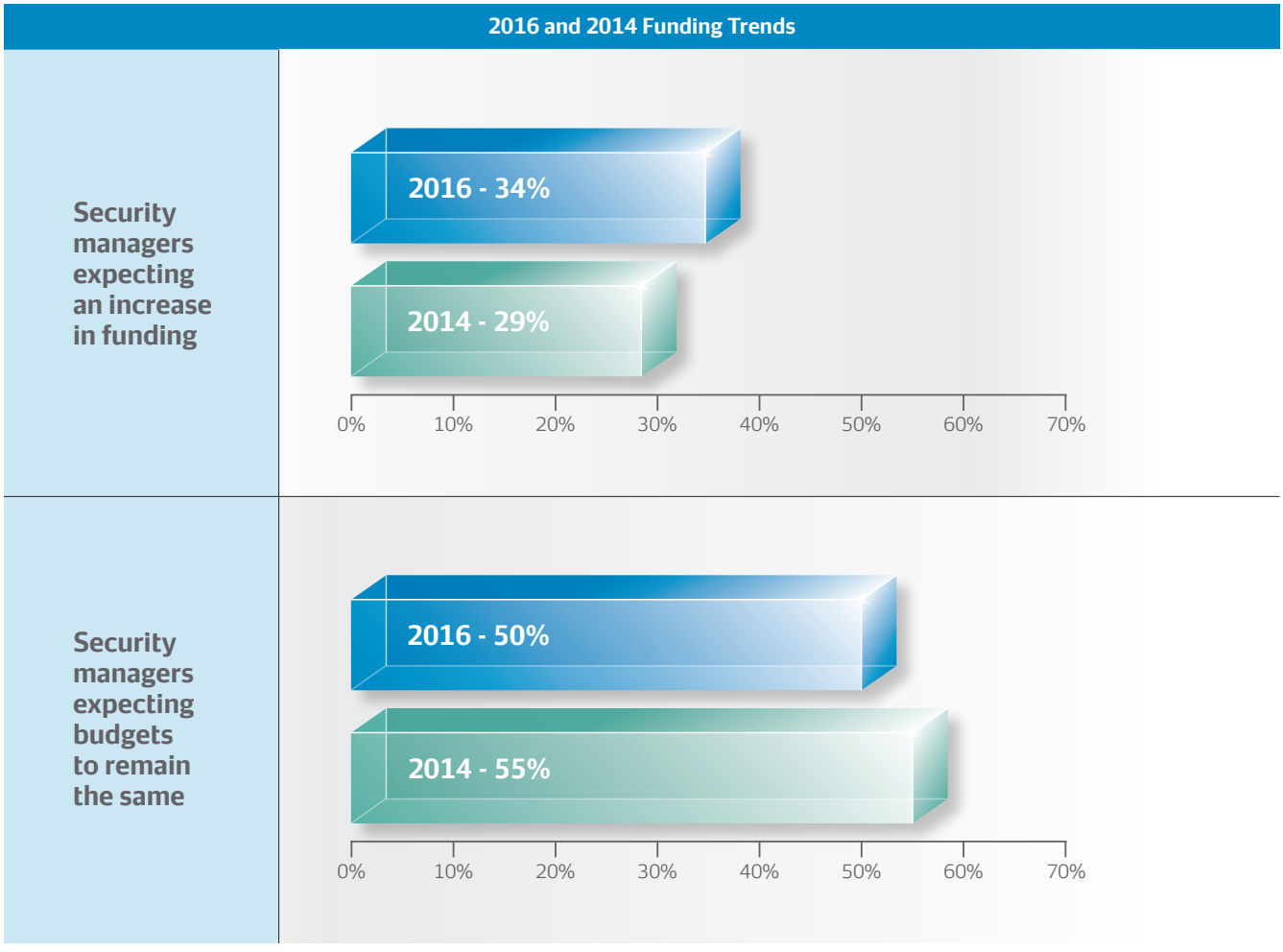
Operational Issues of Greatest Concern	
1	Security Staffing Effectiveness: Training Effectiveness/Methods
2	Promoting Employee Awareness
3	Implementing Best Practices/Standards/Key Performance Indicators
4	Strategic Planning
5 (Tie)	Staying Current With Technological Advances [a]
5 (Tie)	Threat Assessments
5 (Tie)	Regulatory Compliance Issues (state/federal legislation) [b]

a. Prior to 2016, this attribute was known generally as: Keeping up with Technological Advances
b. Prior to 2016, this attribute was known generally as: Regulatory/Compliance Issues (e.g., OSHA, C-TPAT, state, federal legislation, etc.)

Funding Trends

Over the next three to five years, the funding outlook for corporate security programs shows that 34% of security managers are expecting an increase in funding in 2016, compared to 29% in 2014. It further shows that 50% of security managers are expecting budgets to remain the same in 2016, compared to 55% in 2014.

Figure 3



To assess the relative level of concern held by security professionals, the Security Threats survey presented a list of 29 potential security threats developed by Securitas USA. These were refined from the 2014 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 2016 rankings are shown in Figure 4.

Figure 4

2016 Rank	Top Security Threats - Ranking	Average Importance Score
1	Cyber/Communications Security: Internet/Intranet Security [a]	4.17
2	Workplace Violence Prevention/Response	3.95
3	Active Shooter Threats [b]	3.94
4	Business Continuity Planning/Organizational Resilience	3.93
5	Cyber/Communications Security: Mobile Technology [b]	3.79
6	Crisis Management and Response: Natural Disasters [b]	3.68
7	Employee Selection/Screening/Rescreening (including insider threats) [c]	3.64
8	Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks [d]	3.56
9	Property Crime (e.g., external theft, vandalism)	3.53
10	Environmental/Social: Privacy Concerns	3.48
11	General Employee Theft	3.26
12	Identity Theft	3.24
13	Litigation: Inadequate Security	3.19
14	Unethical Business Conduct	3.17
15	Executive/Employee Protection (including travel security/airline safety) [e]	3.14
16	Litigation: Negligent Hiring/Supervision	3.07
17	Substance Abuse (drugs/alcohol in the workplace)	3.05
18	Fraud/White-Collar Crime	3.02
19	Organizational Espionage/Theft of Trade Secrets [f]	3.01
20	Intellectual Property/Brand Protection/Product Counterfeiting	2.98
21	Bombings/IEDs/Bomb Threats [g]	2.91
22	Crisis Management and Response: Political Unrest/Regional Instability/Public Demonstrations/Protests [h]	2.86
23	Environmental/Social: Robberies	2.85
24	Environmental/Social: Diseases/Viruses (e.g., Zika virus) [i]	2.83
25	Global Supply-Chain Security	2.81
26	Insurance/Workers' Compensation Fraud	2.75
27	Crisis Management and Response: International Terrorism	2.70
28	Labor Unrest	2.44
29	Crisis Management and Response: Kidnapping/Extortion	2.28

a. Prior to 2016, this attribute was known generally as: Cyber/Communications Security (e.g., internet/intranet security)
b. New attribute in 2016
c. Prior to 2016, this attribute was known generally as: Employee Selection/Screening
d. Prior to 2016, this attribute was known generally as: Crisis Management and Response: Domestic Terrorism
e. Prior to 2016, this attribute was known generally as: Executive Protection (including travel and security)
f. Prior to 2016, this attribute was known generally as: Business Espionage/Theft of Trade Secrets
g. Prior to 2016, this attribute was known generally as: Bombings/Bomb Threats
h. Prior to 2016, this attribute was known generally as: Crisis Management and Response: Political Unrest/Regional Instability/National Disasters (evacuation potential)
i. Prior to 2016, this attribute was known generally as: Environmental/Social: Pandemics (e.g., Ebola virus)

Cyber/Communications Security: Internet/Intranet Security is the foremost concern of corporate security directors, reflecting the country's high reliance on technology. This is the breakout of what was formerly known as Cyber/Communications Security (e.g., internet/intranet security), which held the position from 2010 through 2014. Workplace Violence Prevention/Response moves back up to the 2nd spot after holding this position from 2010 - 2012, and falling to the 3rd position in 2014. Active Shooter Threats, a new attribute, earned the 3rd spot while Business Continuity Planning/Organizational Resilience falls to the 4th spot after being in 2nd place in 2014. Cyber/Communications Security: Mobile Technology and Crisis Management and Response: Natural Disasters, both new attributes, earned the places of 5th and 6th, respectively.

Figure 5

Top Security Threats - Ranking 2000 - 2016*

Security Threats	2000	2001	2002	2003	2008	2010	2012	2014	**2016**
Cyber/Communications Security: Internet/Intranet Security [a]	2 (tie)	2	4	3	3	1	1	1	**1**
Workplace Violence Prevention/Response	1	1	1	1	1	2	2	3	**2**
Active Shooter Threats [b]	NA	NA	NA	NA	NA	NA	NA	NA	**3**
Business Continuity Planning/Organizational Resilience	2 (tie)	5	2	2	2	3	3	2	**4**
Cyber/Communications Security: Mobile Technology [b]	NA	NA	NA	NA	NA	NA	NA	NA	**5**
Crisis Management and Response: Natural Disasters [b]	NA	NA	NA	NA	NA	NA	NA	NA	**6**
Employee Selection/Screening/Rescreening (including insider threats) [c]	5	3	5	5	4	4	4	4	**7**
Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks [d]	16	17	3	4	7	12	15	8	**8**
Property Crime (e.g., external theft, vandalism)	12	10	9	12 (tie)	5 (tie)	7	5	6	**9**
Environmental/Social: Privacy Concerns	NA	NA	NA	NA	NA	NA	NA	5	**10**
General Employee Theft	6	6	8	7	5 (tie)	8	6	7	**11**
Identity Theft	NA	16	14 (tie)	10	12	11	10	9	**12**
Litigation: Inadequate Security	13 (tie)	13	11 (tie)	18	19 (tie)	16	9	13	**13**
Unethical Business Conduct	7	9	7	8	9	5	8	10	**14**
Executive/Employee Protection (including travel security/airline safety) [e]	NA	NA	NA	NA	22 (tie)	13	18	21	**15**
Litigation: Negligent Hiring/Supervision	13 (tie)	14	18	20	25	23	17	15 (tie)	**16**
Substance Abuse (drugs/alcohol in the workplace)	9	8	10	9	19 (tie)	17	13	15 (tie)	**17**
Fraud/White-Collar Crime	4	4	6	6	8	10	12	14	**18**
Organizational Espionage/Theft of Trade Secrets [f]	11	12	19	16	15 (tie)	15	16	17	**19**
Intellectual Property/Brand Protection/Product Counterfeiting	NA	NA	NA	NA	21	14	11	19	**20**
Bombings/IEDs/Bomb Threats [g]	NA	NA	NA	NA	14	24	19	24	**21**
Crisis Management and Response: Political Unrest/Regional Instability/ Public Demonstrations/Protests [h]	17	20	14 (tie)	11	10	6	7	12	**22**
Environmental/Social: Robberies	NA	NA	NA	NA	27 (tie)	19	14	18	**23**
Environmental/Social: Diseases/Viruses (e.g., Zika virus) [i]	NA	NA	NA	NA	17	18	22	11	**24**
Global Supply-Chain Security	19	18	22	21	27 (tie)	22	20	20	**25**
Insurance/Workers' Compensation Fraud	15	15	17	17	26	25	21	22	**26**
Crisis Management and Response: International Terrorism	NA	NA	NA	NA	NA	NA	NA	23	**27**
Labor Unrest	NA	NA	NA	NA	29	26	23	25	**28**
Crisis Management and Response: Kidnapping/Extortion	18	19	20	19	33	27	24	26	**29**

* Rankings for 2000-2016 do not include every threat option, as some were replaced by new options in more recent surveys
a. Prior to 2016, this attribute was known generally as: Cyber/Communications Security (e.g., internet/intranet security)
b. New attribute in 2016
c. Prior to 2016, this attribute was known generally as: Employee Selection/Screening
d. Prior to 2016, this attribute was known generally as: Crisis Management and Response: Domestic Terrorism
e. Prior to 2016, this attribute was known generally as: Executive Protection (including travel and security)
f. Prior to 2016, this attribute was known generally as: Business Espionage/Theft of Trade Secrets
g. Prior to 2016, this attribute was known generally as: Bombings/Bomb Threats
h. Prior to 2016, this attribute was known generally as: Crisis Management and Response: Political Unrest/Regional Instability/National Disasters (evacuation potential)
i. Prior to 2016, this attribute was known generally as: Environmental/Social: Pandemics (e.g., Ebola virus)

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 (25%); Finance and Insurance (12%); Utilities (10%); Healthcare and Social Assistance (10%); Real Estate, Rental and Leasing (9%); Transportation and Warehousing (6%); Information (6%); and Retail Trade (3%).

A. Manufacturing

The top three concerns among security directors at Fortune 1000 manufacturing companies in 2016 show similar results when compared to 2014. Cyber/Communications Security: Internet/Intranet Security is in 1st place, while Workplace Violence Prevention/Response maintains 2nd place. Business Continuity Planning/Organizational Resilience is tied for 3rd place with a new attribute, Cyber/Communications Security: Mobile Technology. Active Shooter Threats, and Crisis Management and Response: Natural Disasters, also new attributes in 2016, earned 5th and 6th place rankings.

Figure 6

Top Threats by Industry - Manufacturing

Total Respondents Rank 2016	Rank Within Industry 2016	Security Threats	Rank Within Industry 2014
1	1	Cyber/Communications Security: Internet/Intranet Security [a]	1
2	2	Workplace Violence Prevention/Response	2
4	3 (tie)	Business Continuity Planning/Organizational Resilience	3
5	3 (tie)	Cyber/Communications Security: Mobile Technology [b]	NA
3	5	Active Shooter Threats [b]	NA
6	6	Crisis Management and Response: Natural Disasters [b]	NA
7	7 (tie)	Employee Selection/Screening/Rescreening (including insider threats) [c]	4
19	7 (tie)	Organizational Espionage/Theft of Trade Secrets [d]	5
9	9	Property Crime (e.g., external theft, vandalism)	11
20	10	Intellectual Property/Brand Protection/Product Counterfeiting	7

a. Prior to 2016, this attribute was known generally as: Cyber/Communications Security (e.g., internet/intranet security)
b. New attribute in 2016
c. Prior to 2016, this attribute was known generally as: Employee Selection/Screening
d. Prior to 2016, this attribute was known generally as: Business Espionage/Theft of Trade Secrets

B. Finance and Insurance

The top security threat for 2016 in the Finance and Insurance industry is Cyber/Communications Security: Internet/Intranet Security, and remains unchanged compared to 2012. Workplace Violence Prevention/Response moves back up to 2nd place from 3rd place in 2014. Environmental/Social: Privacy Concerns moves up to a 3rd place tie with new attribute, Cyber/Communications Security: Mobile Technology, after it was tied for 4th place in 2014. Active Shooter Threats, another new attribute, earns a 5th place ranking, while Business Continuity Planning/Organizational Resilience falls from its 2014 2nd place ranking to 6th place.

Figure 7

Top Threats by Industry - Finance and Insurance

Total Respondents Rank 2016	Rank Within Industry 2016	Security Threats	Rank Within Industry 2014
1	1	Cyber/Communications Security: Internet/Intranet Security [a]	1
2	2	Workplace Violence Prevention/Response	3
5	3 (tie)	Cyber/Communications Security: Mobile Technology [b]	NA
10	3 (tie)	Environmental/Social: Privacy Concerns	4 (tie)
3	5	Active Shooter Threats [b]	NA
4	6	Business Continuity Planning/Organizational Resilience	2
18	7	Fraud/White-Collar Crime	6
7	8	Employee Selection/Screening/Rescreening (including insider threats) [c]	4 (tie)
12	9	Identity Theft	7
15	10	Executive/Employee Protection (including travel security/airline safety) [d]	10

a. Prior to 2016, this attribute was known generally as: Cyber/Communications Security (e.g., internet/intranet security)
b. New attribute in 2016
c. Prior to 2016, this attribute was known generally as: Employee Selection/Screening
d. Prior to 2016, this attribute was known generally as: Executive Protection (including travel and security)

C. Utilities

In 2016, Domestic Terrorism/Lone Wolf Attacks jumps to 1st place in 2016, up from 5th place in 2014. Cyber/Communications Security: Internet/Intranet Security falls to 2nd place in 2016 after being in first place for 2014 in the Utilities industry. Tied for 3rd place are two new attributes for 2016: Active Shooter Threats and Crisis Management and Response: Natural Disasters. Newly worded Employee Selection/Screening/Rescreening (including insider threats) falls two spots to 5th place in 2016, while Business Continuity Planning/Organizational Resilience drops to 6th place after being in 2nd place in 2014.

Figure 8

Top Threats by Industry - Utilities

Total Respondents Rank 2016	Rank Within Industry 2016	Security Threats	Rank Within Industry 2014
8	1	Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks [a]	5
1	2	Cyber/Communications Security: Internet/Intranet Security [b]	1
3	3 (tie)	Active Shooter Threats [c]	NA
6	3 (tie)	Crisis Management and Response: Natural Disasters [c]	NA
7	5	Employee Selection/Screening/Rescreening (including insider threats) [d]	3
4	6	Business Continuity Planning/Organizational Resilience	2
2	7	Workplace Violence Prevention/Response	4
5	8	Cyber/Communications Security: Mobile Technology [c]	NA
9	9 (tie)	Property Crime (e.g., external theft, vandalism)	7 (tie)
27	9 (tie)	Crisis Management and Response: International Terrorism	16

a. Prior to 2016, this attribute was known generally as: Crisis Management and Response: Domestic Terrorism
b. Prior to 2016, this attribute was known generally as: Cyber/Communications Security (e.g., internet/intranet security)
c. New attribute in 2016
d. Prior to 2016, this attribute was known generally as: Employee Selection/Screening

D. Healthcare and Social Assistance

Active Shooter threats, a new attribute in 2016, is the greatest concern of security threats in the Healthcare and Social Assistance industry. Environmental/Social: Privacy Concerns is the second greatest concern in 2016 after placing 5th for this industry in 2014. Workplace Violence Prevention/Response maintains its 3rd place position as Cyber/Communications Security: Internet/Intranet Security moves down to 4th place in 2016 from 1st place in 2014. Business Continuity Planning/Organizational Resilience moves down to 5th place after it previously held 2nd place in 2014.

Figure 9

Top Threats by Industry - Healthcare and Social Assistance

Total Respondents Rank 2016	Rank Within Industry 2016	Security Threats	Rank Within Industry 2014
3	1	Active Shooter Threats [a]	NA
10	2	Environmental/Social: Privacy Concerns	5
2	3	Workplace Violence Prevention/Response	3
1	4	Cyber/Communications Security: Internet/Intranet Security [b]	1
4	5	Business Continuity Planning/Organizational Resilience	2
5	6	Cyber/Communications Security: Mobile Technology [a]	NA
8	7 (tie)	Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks [c]	14
9	7 (tie)	Property Crime (e.g., external theft, vandalism)	11
6	9 (tie)	Crisis Management and Response: Natural Disasters [a]	NA
11	9 (tie)	General Employee Theft	12
12	9 (tie)	Identity Theft	13

a. New attribute in 2016
b. Prior to 2016, this attribute was known generally as: Cyber/Communications Security (e.g., internet/intranet security)
c. Prior to 2016, this attribute was known generally as: Crisis Management and Response: Domestic Terrorism

E. Real Estate, Rental and Leasing

For management security threats in the Real Estate, Rental and Leasing industry, Active Shooter Threats, a new attribute, earns a 1st place mention as Business Continuity Planning/Organizational Resilience maintains its 2014 ranking of 2nd place. Cyber/Communications Security: Internet/Intranet Security takes over the 3rd spot, up from 4th place in 2014. Workplace Violence Prevention/Response jumps to 4th place in 2016 from 10th place in 2014. Cyber/Communications Security: Mobile Technology, a new attribute, tied for 5th place along with Property Crime, Crisis Management and Response: Natural Disasters and Domestic Terrorism/Lone Wolf Attacks.

Figure 10

Top Threats by Industry - Real Estate, Rental and Leasing

Total Respondents Rank 2016	Rank Within Industry 2016	Security Threats	Rank Within Industry 2014
3	1	Active Shooter Threats [a]	NA
4	2	Business Continuity Planning/Organizational Resilience	2
1	3	Cyber/Communications Security: Internet/Intranet Security [b]	4
2	4	Workplace Violence Prevention/Response	10
5	5 (tie)	Cyber/Communications Security: Mobile Technology [a]	NA
6	5 (tie)	Crisis Management and Response: Natural Disasters [a]	NA
9	5 (tie)	Property Crime (e.g., external theft, vandalism)	1
8	5 (tie)	Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks [c]	7 (tie)
13	9	Litigation: Inadequate Security	6
22	10	Crisis Management and Response: Political Unrest/Regional Instability/ Public Demonstrations/Protests [d]	11

a. New attribute in 2016
b. Prior to 2016, this attribute was known generally as: Cyber/Communications Security (e.g., internet/intranet security)
c. Prior to 2016, this attribute was known generally as: Crisis Management and Response: Domestic Terrorism
d. Prior to 2016, this attribute was known generally as: Political Unrest/Regional Instability/National Disasters (evacuation potential)

F. Transportation and Warehousing

In the Transportation and Warehousing industry, Workplace Violence Prevention/Response moves up to 1st place after being tied for 5th place in 2014. Property Crime is the security threat of second greatest concern in 2016, moving down from 1st place in 2014. A four-way tie for 3rd place occurs with two new threats: Active Shooter Threats and Crisis Management and Response: Natural Disasters. Business Continuity Planning/Organizational Resilience, which moves up from an 8th place tie in 2014 and Domestic Terrorism/Lone Wolf Attacks up from a 16th place tie in 2014 complete this year's four-way tie.

Figure 11

Top Threats by Industry - Transportation and Warehousing

Total Respondents Rank 2016	Rank Within Industry 2016	Security Threats	Rank Within Industry 2014
2	1	Workplace Violence Prevention/Response	5 (tie)
9	2	Property Crime (e.g., external theft, vandalism)	1
3	3 (tie)	Active Shooter Threats [a]	NA
4	3 (tie)	Business Continuity Planning/Organizational Resilience	8 (tie)
6	3 (tie)	Crisis Management and Response: Natural Disasters [a]	NA
8	3 (tie)	Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks [b]	16 (tie)
11	7 (tie)	General Employee Theft	2
13	7 (tie)	Litigation: Inadequate Security	15
1	9 (tie)	Cyber/Communications Security: Internet/Intranet Security [c]	5 (tie)
7	9 (tie)	Employee Selection/Screening/Rescreening (including insider threats) [d]	3
16	9 (tie)	Litigation: Negligent Hiring/Supervision	12 (tie)

a. New attribute in 2016
b. Prior to 2016, this attribute was known generally as: Crisis Management and Response: Domestic Terrorism
c. Prior to 2016, this attribute was known generally as: Cyber/Communications Security (e.g., internet/intranet security)
d. Prior to 2016, this attribute was known generally as: Employee Selection/Screening

G. Information

Crisis Management and Response: Natural Disasters, a new attribute, and Intellectual Property/Brand Protection/Product Counterfeiting, up from 7th place in 2014, share the threat of greatest concern in the Information industry in 2016 by being tied for 1st place. Cyber/Communications Security: Internet/Intranet Security takes the 3rd place spot after it previously held 2nd place in 2014. Tied for 4th place are: Business Continuity Planning/Organizational Resilience, Employee Selection Screening/Rescreening (including insider threats), Environmental/Social: Privacy Concerns and Workplace Violence Prevention/Response.

Figure 12

Top Threats by Industry - Information

Total Respondents Rank 2016	Rank Within Industry 2016	Security Threats	Rank Within Industry 2014
6	1 (tie)	Crisis Management and Response: Natural Disasters [a]	NA
20	1 (tie)	Intellectual Property/Brand Protection/Product Counterfeiting	7
1	3	Cyber/Communications Security: Internet/Intranet Security [b]	2
2	4 (tie)	Workplace Violence Prevention/Response	4
4	4 (tie)	Business Continuity Planning/Organizational Resilience	1
7	4 (tie)	Employee Selection/Screening/Rescreening (including insider threats) [c]	5
10	4 (tie)	Environmental/Social: Privacy Concerns	3
5	8 (tie)	Cyber/Communications Security: Mobile Technology [a]	NA
14	8 (tie)	Unethical Business Conduct	12 (tie)
12	10 (tie)	Identity Theft	10
19	10 (tie)	Organizational Espionage/Theft of Trade Secrets [d]	8 (tie)

a. New attribute in 2016
b. Prior to 2016, this attribute was known generally as: Cyber/Communications Security (e.g., internet/intranet security)
c. Prior to 2016, this attribute was known generally as: Employee Selection/Screening
d. Prior to 2016, this attribute was known generally as: Business Espionage/Theft of Trade Secrets

H. Retail Trade

To Fortune 1000 retailers and related companies, Business Continuity Planning/Organizational Resilience and Cyber/Communications Security: Internet/Intranet Security are tied as the top security threats of greatest concern in 2016. The former was previously ranked 12th among the top threats with the industry in 2014, while the latter was tied for 2nd place in 2014. After being tied for 7th place in 2014, Property Crime (e.g., external theft, vandalism) shares 3rd place with Executive/Employee Protection (including travel security/airline safety) which was tied for 19th in 2014.

Figure 13

Top Threats by Industry - Retail Trade

Total Respondents Rank 2016	Rank Within Industry 2016	Security Threats	Rank Within Industry 2014
4	1 (tie)	Business Continuity Planning/Organizational Resilience	12
1	1 (tie)	Cyber/Communications Security: Internet/Intranet Security [a]	2 (tie)
9	3 (tie)	Property Crime (e.g., external theft, vandalism)	7 (tie)
15	3 (tie)	Executive/Employee Protection (including travel security/airline safety) [b]	19 (tie)
5	5 (tie)	Cyber/Communications Security: Mobile Technology [c]	NA
6	5 (tie)	Crisis Management and Response: Natural Disasters [c]	NA
11	5 (tie)	General Employee Theft	1
13	5 (tie)	Litigation: Inadequate Security	17 (tie)
7	9 (tie)	Employee Selection/Screening/Rescreening (including insider threats) [d]	4 (tie)
10	9 (tie)	Environmental/Social: Privacy Concerns	10
16	9 (tie)	Litigation: Negligent Hiring/Supervision	17 (tie)
24	9 (tie)	Environmental/Social: Diseases/Viruses (e.g., Zika virus) [e]	15 (tie)
25	9 (tie)	Global Supply-Chain Security	9
26	9 (tie)	Insurance/Workers' Compensation Fraud	15 (tie)

a. Prior to 2016, this attribute was known generally as: Cyber/Communications Security (e.g., internet/intranet security)
b. Prior to 2016, this attribute was known generally as: Executive Protection (including travel and security)
c. New attribute in 2016
d. Prior to 2016, this attribute was known generally as: Employee Selection/Screening
e. Prior to 2016, this attribute was known generally as: Environmental/Social: Pandemics (e.g., Ebola virus)

A list of 17 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).

Maintaining its trend from 2014, Security Staffing Effectiveness: Training Effectiveness/Methods holds the top position for 2016 security management issues. Promoting Employee Awareness is 2nd, Implementing Best Practices/Standards/Key Performance Indicators is 3rd, Strategic Planning is 4th, and tied for 5th place are: Staying Current with Technological Advances, Threat Assessments, and Regulatory/Compliance Issues (state/federal legislation). The top security management issues ranked 8th through 10th are: Budget/Maximizing Return on Investment, Adequate Staffing Levels and Maturity of Workforce.

Figure 14

2016 Rank	Management Issues	Average Importance Score
1	Security Staffing Effectiveness: Training Effectiveness/Methods	4.06
2	Promoting Employee Awareness	4.01
3	Implementing Best Practices/Standards/Key Performance Indicators	3.88
4	Strategic Planning	3.87
5 (tie)	Staying Current with Technological Advances [a]	3.85
5 (tie)	Threat Assessments	3.85
5 (tie)	Regulatory/Compliance Issues (state/federal legislation) [b]	3.85
8	Budget/Maximizing Return on Investment	3.77
9	Security Staffing Effectiveness: Adequate Staffing Levels	3.76
10	Security Staffing Effectiveness: Maturity of Workforce [c]	3.73
11 (tie)	Security Staffing Effectiveness: Selection and Hiring Methods	3.70
11 (tie)	Security Staffing Effectiveness: Security Officer Turnover/Retention [d]	3.70
13	Managing Remote Security Operations	3.43
14	Additional Security Responsibilities (aviation/compliance/ethics, etc.)	3.31
15	Career Development/Multiple Job Responsibilities	3.29
16	Security Staffing Effectiveness: Absenteeism	3.22
17	Global Supply-Chain Decisions	2.56

a. Prior to 2016, this attribute was known generally as: Keeping up with Technological Advances
b. Prior to 2016, this attribute was known generally as: Regulatory/Compliance Issues (e.g., OSHA, C-TPAT, state, federal legislation, etc.)
c. New attribute in 2016
d. Prior to 2016, this attribute was known generally as: Security Staffing Effectiveness: Security Officer Turnover


ECURITAS

Reporting Relationships

Corporate security reporting relationships are diverse and show little organizational consistency across the Fortune 1000 companies. The largest groups report to the Facilities area (21%). Operations (18%) and Administration (18%), CEO/President (11%), and Environmental/Health/Safety (10%) are the next most frequently mentioned areas.

Responses are summarized in Figure 15.

Figure 15

Organizational Area	2012	2014
Facilities	17%	**215**
Operations	17%	**18%**
Administration	11%	**18%**
Directly to the CEO/President	10%	**11%**
Environmental/Health/Safety	9%	**10%**
Legal	11%	**9%**
Human Resources	8%	**8%**
Risk Management	6%	**5%**
Finance	7%	**4%**
Audit	2%	**1%**
IT/MIS	2%	**1%**

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

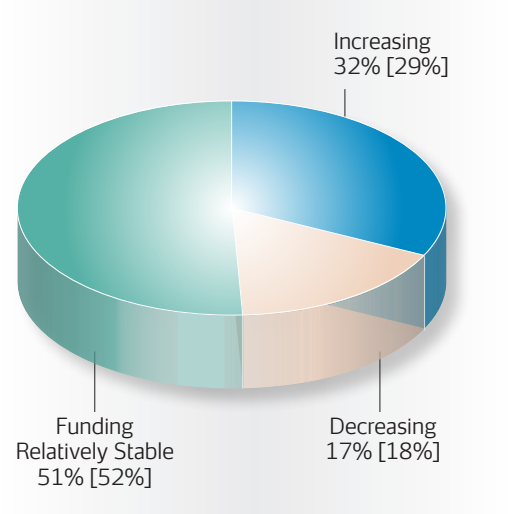
Budget and Funding

Funding Trends

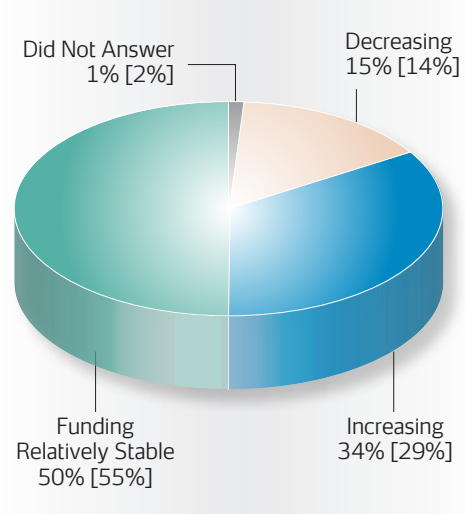
The funding outlook for corporate security programs over the next three to five years reflects that 34% of security managers are expecting an increase in funding in 2016. The percentage of security managers expecting budgets to remain the same is 50% in 2016, while the percentage of managers anticipating decreased funding is 15% in 2016.

Note: The percentages in the [brackets] are 2014 percentages.

Security Funding: Past 3 – 5 Years



Security Funding: Next 3 – 5 Years



A. Survey Methodology

For the 2016 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 963 security directors and other executives identified as having oversight of the corporate security function of these companies. The survey questionnaire was distributed in October 2016. Respondents were asked to complete and return the surveys via mail, fax or e-mail. This year respondents were offered the option to complete the survey online via a link and password provided in the cover letter. Results were compiled and analyzed in December 2016.

Reflected in this report are the responses taken from 151 returned surveys, which represented a 16% 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.

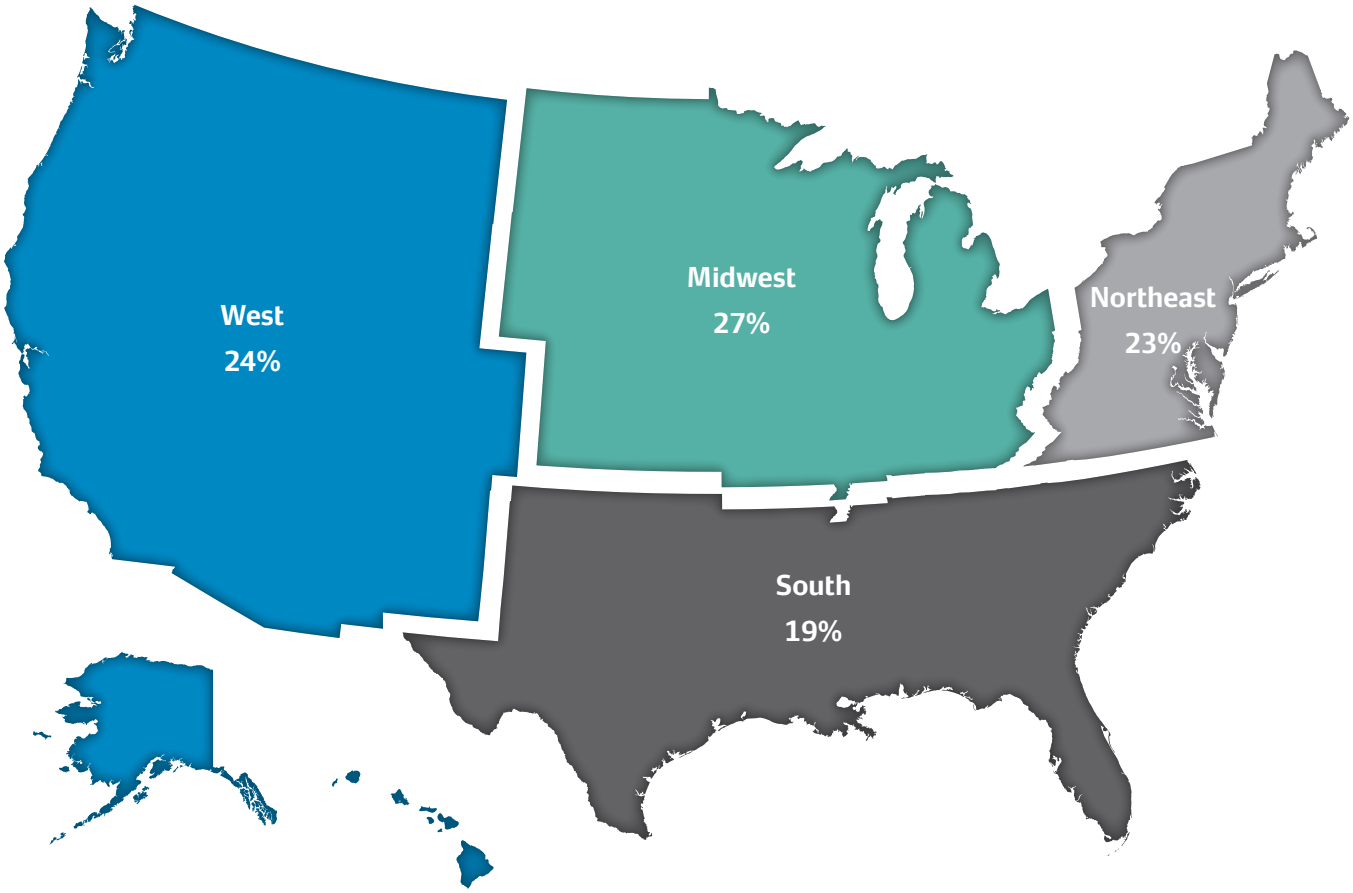
B. Respondent Distribution

Twenty specific industries were 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 was 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
Wholesale and Retail Trade	8
Health Care and Social Assistance	15
Arts, Entertainment and Recreation	8
Finance and Insurance	18
Real Estate, Rental and Leasing	14
Professional, Scientific and Technical Services	6
Educational Services	4
Transportation and Warehousing	9
Government and Law Enforcement	4
Manufacturing	38
Information Services	9
Other	3
TOTAL	**151**

C. Geographic Distribution

Responses from 38 states are represented in the survey results. For illustrative purposes, geographic distribution is grouped into four regions of the U.S. as shown below:



Regions Total - 93%

International Total (Canada and Mexico) - 7%

Total - 100%

Cybersecurity and the IoT Threat

TOM RIDGE

One need not have a top secret security clearance to understand that the civilized world is confronted with two permanent conditions. On a near-daily basis, headlines chronicle the scourge of global terrorism and the challenges of cybersecurity–or what I call the "Digital Forevermore."

But the physical and the digital domains do not operate independently. For security professionals, how we assess and organize for interwoven 21st Century risk will be critical to our ability to successfully thwart increasing threats and the actors behind them.

Physical Security Threats

In the physical domain, the list of cities recently victimized by terrorists continues to grow: Brussels, Paris, Nice, San Bernardino, Orlando, Berlin, and Istanbul, just to name a few. ISIS and like-minded extremists, as well as those either directed or inspired by them, have targeted stadiums, airports, and other "soft" infrastructure through bombings, mass shootings, and truck attacks.

What we have witnessed with our own eyes is reflected in hard data. The latest figures in the 2016 Global Terrorism Index reported a 650% increase of terror-related deaths across developed countries.

Atop this mountain of concerns are those driven by actors with whom you are all too familiar: thieves, nefarious insiders, and active shooters. For your security team, it is a never-ending list and monumental task. So we turn to technology for assistance. But it is not as easy as simply acquiring a new tool or system.

The IoT Threat and Cyber Connection

While ransomware, phishing scams and other threats garner the attention of the cybersecurity team, there are other digital threats that could impact more than just your networks – and it might come from a place you may not expect.

It is estimated that by 2020, between 50-75 billion devices will be connected to the internet via a myriad of devices and platforms. Smart phones, laptops, and tablets are just the tip of the iceberg.

In additional to putting massive amounts of customer data, intellectual property, and trade secrets at risk, the Internet of Everything (IoT) means that critical controls, access points, camera networks and environmental, health, safety (EHS) systems can be at potential risk as well.

This prompts key questions:

- Do your physical security, cyber, and EHS leaders discuss not only the safety and security benefits of cross-over technologies, but also how these connections might compromise enterprise security? In other words, does a technology you acquire to enhance physical security create a potential digital risk? And vice versa?
- How does your organization assess the impact of a system procurement or acquisition of new security (physical or cyber) and EHS technologies on your enterprise?
- Do your procurement processes and organizational structure support or inhibit collaboration?
- How might IoT-related gaps in your cyber insurance coverage leave you exposed?

At the end of the day, potential gaps that emerge between physical, cyber and EHS managers are not really about the technology connections, but human connections. And turf, bureaucracy, or budget issues will provide cover for no one if these vulnerabilities are exposed.

21st Century risk increasingly forces the recognition that enterprise security is a team sport. All of the players must understand roles and establish clear lines of responsibility–and must pay particular attention in areas of overlap.

For firms already integrating capabilities and effectively supporting cross-discipline governance and coordination, continue to lead the way. The rapidly expanding threat surface, however, suggests that a review is prudent as part of your security continuous improvement process.

Even when sophisticated programs and technologies are deployed to thwart them, our adversaries have learned to communicate and collaborate.

We must certainly do it within our organizations or they will get the best of us.

Tom Ridge, the first U.S. Secretary of Homeland Security and 43rd Governor of Pennsylvania, is Chairman of Ridge Global. Ridge Global works with Fortune 500 companies and leaders around the world to assess and reduce enterprise risk and to build more resilient organizations through innovative protection and response capabilities, cyber education and insurance solutions.

Learn more at ridgeglobal.com.

Cyber Security is Built on Relationships and Perseverance

TIM WILLIAMS, CPP

Timothy L. Williams, CPP, is the Chief Security Officer 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.

Most of us are not surprised that, for the fourth time 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 my organization, we defined several keys to successfully battle cybercrime. We relied on our team's expertise wherever possible, but we also recognized that partnerships with other companies and government groups were fundamental to staying ahead of this curve. Sharing what we learned is also crucial. Our lessons learned are many, and I would like to share a few with you in hopes of sparking additional ideas.

Combatting Cybercrime: Six Keys to Success

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. We built 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.

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 are evolving. Staying keenly aware of changing dynamics, the latest information from industry experts and emerging solutions are fundamental to being expert advisors to management.

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.

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.

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 my organization, 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.

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 can become 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 threating form.

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.

Workplace Violence Prevention/Response

CHARLES A. BALEY

Workplace violence continues to be one of the top security threats facing corporate America with an evolving scope of complexity toward defining, assessing, and mitigating the risk, and preparing for the most appropriate response. If we include active shooter threats and domestic terrorism incidents in our scope, we incorporate three of the top ten concerns for 2016.

According to the American National Standard (ANSI) "Workplace Violence Prevention and Intervention" (ASIS/ANSI WVPI.1-2011), workplace violence is viewed as "a spectrum of behaviors, including overt acts of violence, threats and other conduct that generates a reasonable concern for safety from violence, where a nexus exists between the behavior and the physical safety of employees and others (such as customers, clients and business associates), on-site or off-site, during activities related to the organization."

Similarly, the U.S. Occupational Safety and Health Administration (OSHA) defines workplace violence as "any act or threat of physical violence, harassment, intimidation, or other threatening disruptive behavior that occurs at the workplace." OSHA has also defined the standard model for classifying the types of workplace violence, commonly referred to as the OSHA four-type model, based upon the relationship between the perpetrator and the victim(s).

Effective prevention, intervention, mitigation and response strategies must also consider the key elements of motivation and opportunity.

"Type I" incidents include those in which no relationship exists between the perpetrator and the victim or target and the organization. The motivation is associated with the crime being committed (e.g., armed robbery).

"Type II" incidents include those in which a legitimate business relationship existed or currently exists between the perpetrator and the organization. The motivation is based in a dispute originating from that business relationship.

"Type III" incidents include those in which the perpetrator had or currently has some form of employment relationship with the organization. The motivation is a result of the employment relationship.

"Type IV" incidents include those in which the perpetrator is a current or former intimate partner of an employee. The motivation evolves from the personal relationship.

Terrorism and violent extremism have been associated with "Type I" incidents; however, given the fact that violent extremism is an ideologically-motivated violence assessed and addressed with specialized mitigation, preparation and response, a "Type V" incident has been suggested. "Type V" incidents would include "any unlawful act of force or violence, ideologically-motivated, and committed to coerce a government or civilians in support of political or social objectives." In recent years, we have experienced a growing number of incidents of ideologically-motivated violence which have most commonly occurred at business locations.

In order to optimize its effectiveness, a workplace violence program must be designed and maintained as a proactive and dynamic experiential process. Historically, prevention programs and training have focused on the warning signs and risk indicators of the Type I through IV typologies. Research has demonstrated that the suggested Type V category exhibits unique behavioral indicators that are not consistent with the conventional warning signs of workplace violence. These unique indicators include the eight signs of terrorism, and acute behavioral patterns that are linked to radicalization rather than single risk factors. By acknowledging the unique characteristics of ideologically-motivated violence, training, awareness and mitigation strategies can be implemented in an effective and timely manner.

In general, awareness and prevention training should educate employees on how to identify warning signs, how to report potential threats of violence, and how to respond when acts of violence occur. It's especially imperative that employees understand the connection between warning signs and violence, and how certain behavior patterns can lead to violent acts. A conscious, conditioned reflex to say something if you see, hear or perceive something is perhaps the single most effective component of our prevention strategies. Target hardening, training and practical exercises round out an effective program. Training effectiveness remains a top management issue for our industry.

Nonetheless, because no organization can prevent workplace violence entirely, it's essential to form a team of professionals who are dedicated to managing the workplace violence program. At a minimum, the composition of the team should include senior leadership, human resources, legal and security. The team would have responsibility to establish and implement strategies necessary to protect against, mitigate, respond to, and recover from threats, as well as continuously evaluating the overall effectiveness of the program and following new research and lessons learned, in order to make recommendations for program improvements.

The ability to sustain a workplace violence program is an ongoing process and it depends on all employees to make it successful. By promoting workplace violence prevention, coupled with encouraging employees to report warning signs, it is indeed possible to mitigate the risk of violent incidents from occurring.

Charles A. Baley
is the Chief Security Officer for Farmers Group, Inc. headquartered in Los Angeles, CA. He joined Farmers in 2006 and has over 40 years of experience in security/risk management and investigative services in both the public and private sectors. In his current role, Baley is responsible for all matters related to security governance, oversight and execution, including security crisis management, physical security systems, executive protection strategies, risk and threat assessments, internal investigations and strategic support services to legal, IT, human resources, regulatory and compliance divisions.

Baley earned his BA with Honors and Distinction in Criminal Justice from the University of Illinois and received his MBA from the University of Chicago. He has been a member of ASIS International since 1980 and currently serves in a volunteer leadership role as a Commissioner on the Standards and Guidelines Commission. He previously served as the Chairman of the Insurance Fraud Council. Additional professional affiliations include the High Technology Crime Investigation Association (HTCIA) where he previously served as the president of the Midwest Chapter, Association of Threat Assessment Professionals (ATAP), International Security Management Association (ISMA), and InfraGard where he currently serves on the LA Board of Directors.

Baley has also enjoyed teaching criminal justice related courses over the past 35 years at a variety of academies, colleges and universities and is currently an adjunct faculty member at California State University Fullerton, teaching Contemporary Issues in Corporate Security Management, Leadership, Embracing Change, and Strategic Thinking and Decision Making.

Addressing the Impact of Technology in the Security Industry

MICHAEL HOWARD

Michael Howard,
Chief Security Officer (CSO) for Microsoft Corporation, holds global responsibility for vital security functions, including operations, investigations, risk mitigation, crisis management, executive protection, security technology, strategy, intelligence, and employee awareness.

Howard led development of Microsoft's interconnected Global Security Operations Centers (GSOCs), which oversee Global Security monitoring and response, and have become well known in the security field as a leading model for conducting operations globally. Looking to the future, Mike is steering Microsoft Global Security in the transition to a Virtual Security Operations Center (VSOC), leveraging the mobility and the cloud.

The GSOCs, based in the United States and India, have become well known in the security field as a leading model for conducting operations globally.

As a security leader, Howard contributes to the field through key roles in numerous industry organizations: CSO Roundtable Advisory Board, Past President; International Security Management Association (ISMA), Past President; Security Industry Association (SIA), Board of Directors; and U.S. State Department Overseas Security Advisory Council (OSAC), Fostering Innovation Committee.

Howard spent 22 years with the Central Intelligence Agency, finishing as Chief of Station, the agency's highest field position. Mike also worked in the CIA's Office of Security and served on the security staff of the Director of Central Intelligence. He worked in the Counterterrorism Center, ran global programs, and served in assignments around the world. He was executive officer for the Office of Military Affairs and a special investigator for the Office of Inspector General.

Howard also served as a law enforcement officer with the Oakland, California, police in the late 1970s. He holds a BS in criminal justice administration from San Jose State University.

The world is a very different place now than when I first began my second career in 2002 in the private sector as CSO for the Microsoft Corporation. Today, cyber threats, workplace violence, and active shooters top the list of security concerns for corporations.

As CSO for Microsoft, my job is to manage the physical safety and security program of our global enterprise (190 countries, 850 physical buildings and over 200,000 workers). One of the success factors for any corporate security program is having a strong partnership between the physical and logical security teams. I've seen many CSOs struggle to develop or maintain a relationship with their cyber security counterparts. The world has too many dangers lurking in the shadows to let pride, fiefdoms, and stubbornness get in the way of a holistic security strategy of integrating physical and logical security. This does not mean a reorganization where the respective groups land in one organization. This may make sense in some companies; however, with the right relationships and partnership agreements (either with MOUs or policies), it is possible to have a robust physical and cyber security program reporting in different groups. At Microsoft, the office of the CISO is in the IT department and my physical security team resides in the Finance organization. I have a very strong relationship with Microsoft's CISO Bret Arsenault, and our company's security policies are governed by an internal group called the Information Risk Management Council (IRMC). This governance structure allows all business groups to know their security risks and provides a decision-making body to ensure alignment of risk prioritization and ownership.

When I first started at Microsoft, the physical security team was very disorganized and its reputation with employees and executives was more of a "guns, guards, and gates" organization. There was no strategic alignment of technology or a partnership with IT security. Over the last 14 years, I have pushed hard for my team to be at the forefront when it comes to a comprehensive program that is aligned with our company's goals to enable our business groups and employees to feel safe at work. Nothing can hurt productivity more than employees fearing to travel or to come to the office.

We had to change the mindset of executives and employees that the physical security team was more than a bunch of security guards checking locked doors and patrolling the campus. This required a comprehensive strategy involving the right leadership, functional teams, and technology. The first major strategic step we took in 2007 was creating three integrated centers known as Global Security Operations Centers (GSOC). They were strategically located around the world to cover the Americas, Europe/Middle-East/Africa, and Asia. The byproduct of a good strategy is that when your security team can avert threats or manage a crisis effectively, employees and executives see the value of security. They have an appreciation for what you do to keep them safe, and you are now looked upon as a trusted advisor and trusted leader. I'm very proud that my organization has evolved to the trusted advisor level.

The evolution of technology solutions and the cloud have helped us to be at the forefront for what I feel is the future of physical security. Close to 100% of our physical security technology is in the cloud and we're piloting cloud-based access control and digital video solutions. We see the value of artificial intelligence (AI), big data, robotics, and the power of the cloud that is moving our GSOCs to the Virtual Security Operations Centers (VSOC). The VSOC is an intelligence driven, operations led fusion center which focuses on mission critical issues. We are inverting the pyramid of traditional GSOC duties and pushing up to 90% of the data monitoring to the cloud. Using AI and the cloud, we'll be able to push the millions of incoming data to the cloud and automatically make sense of that data acting on mission critical functions. For example, we took an existing cloud monitoring service solution for data center servers and, through IT, built a tool that monitors 16 of our IP physical security enabled devices such as: digital cameras, video servers, duress alarms, sensors, emergency stations, etc. Now in real time, we can monitor the health of all our IP-enabled devices through a dashboard. We don't have to wait until something breaks as we can see heat maps, critical locations, and stack rank service requests based on risk. We not only have a greater visibility of our physical security technology eco-system, we're saving money as we can determine the replacement life-cycle of hardware not based on manufacturer's recommendations, but on real data of our technology eco-system.

This is the future and exciting times are ahead for our industry that will make the world a safer place. To keep up to date on our Microsoft Global Security efforts, please visit www.microsoft.com/globalsecurity

Promoting Employee Awareness

GAIL ESSEN, CPP, PSP

"Baseball is ninety percent mental and the other half physical." I agree with Yogi Berra and would say the same about security. A large part of the mental game in security is promoting employee awareness, which has ranked second as a management issue in the 2012, 2014, and 2016 studies.

Definition

For the purposes of this article, I define Promoting Security Awareness as *the continual improvement by all employees towards the demonstrated understanding of the company's deployed policies, procedures and countermeasures used to protect their assets*.

Start at the top

"The opportunity for fraud is generally created through the absence or weakness of internal controls." [1] The well-documented theft triangle lists "opportunity" as a cornerstone.

Establishing a resilient security culture starts with ownership and endorsement by the most senior leaders in the company. It's establishing tighter controls and eliminating easy opportunities. At a minimum, there should be financial support in programs, technology and experts. The investment becomes the proof statement that the company values safety and security. The leaders must also become walking billboards and incorporate the messaging into the annual investors report.

Leverage Self Interest

How do you achieve compliance? We are naturally programmed to protect ourselves. Abraham Maslow lists "security and safety" before "belongingness and love" in his "needs" hierarchy. If employees understand that the security culture exists to protect them and their jobs, they are more likely to participate.

Even the best consultants can't know the intricacies of your processes as well as the people who do the work. Comparing industry risk data with employee input for a given area or process helps to mitigate it and gives the employee a sense of involvement and importance. Promoting awareness builds a strong culture and has a positive impact because employees become the champions and gatekeepers.

Consistency

Security awareness must begin during the onboarding process and be repeated on a regular basis. If the employee is not part of the corporate security team, a refresher course should be part of the employee's regimen at least semi-annually, but quarterly is better. Completion of the courses could be incentive-based for teams and departments. Most people enjoy being part of a winning team, so posting results is a way to keep teams engaged and security at the forefront.

Return on Investment

Investing in a security awareness program yields a high rate of return. Every employee has the ability to identify, slow or stop a threat. Simply knowing there is a high focus on security will drive the bad actor to an easier target. Gaining access to intellectual property, financial data, or customer lists can have devastating consequences when the adversary uses the information to do harm. The return on the (comparably minimal) investment to create and maintain the security culture becomes high, when the inevitable "it" happens.

1. Walsh, T.J., CPP & Healy, R.J, CPP & Williams, T.L., CPP & Knoke, M.E, CPP (Comp.). (2012). Protection Of Assets, Security Management: Alexandria, VA: ASIS International

Gail Essen, CPP, PSP is the CEO of Professional Security Advisors, a consulting firm that provides support to regional, national and global clients. She is a 25 year veteran known for accelerating business development and process improvements. Her progressive growth and wide range of experience, including owning a WBE, MBE, DBE business, converged in her current role, where she established herself as a trusted business advisor.

Gail is board certified as a Certified Protection Professional (CPP) and as a Physical Security Professional (PSP). Gail is CVI (Chemical-Terrorism Vulnerability Information) certified.

Gail currently serves as a member of the Board of Directors for ASIS International. She is also a member of InfraGard, OSAC and IAHSS.

Contact Gail at: gail.essen@prosecurityadvisors.com and www.prosecurityadvisors.com

Richard K. Avery, CPP
brings forty years of demonstrated security and management expertise to his position of Northeast Region President, Securitas USA – an industry and market leader in this region of 14,000 employees. As a member of ASIS International for 36 years, Avery has been honored to serve as Chair of the Boston Chapter. Avery holds board certification as a Certified Protection Professional, the security profession's highest recognition of practitioners. He is a member of the Building Owners and Managers Association (BOMA), High Tech Crime Investigation Association (HTCIA), The International Association of Venue Managers (IAVM),Association of Threat Assessment Professionals (ATAP), FBI Boston Citizens' Academy and the National Fire Protection Association (NFPA). Avery has appeared on numerous occasions in both the print media and on broadcast news as a subject matter expert in the security profession.

Employee Selection/Screening/Insider Threat

RICHARD K. AVERY, CPP

Today's employers have increasing, unique challenges that were unheard of years ago in recruiting, background screening, hiring and managing employees. Limited, restricted and heightened regulated verification of employee applications, criminal records and references, as well as the approach to managing employees, all combine to make hiring decisions more critical, and much more risky, than ever before.

Because every organization's business model is different, your employee vetting and selection process will depend on the industry, company culture and job requirements. However, whether you are hiring an entry level employee or a C-suite executive, there are some best practices that will help to ensure a qualified hire.

- Have the applicant complete an actual job application. According to CareerBuilder, more than 25% of employers do not conduct background investigations, and its 2014 study found that 58% of hiring managers have discovered false statements on resumes. Having prospective employees complete an application ensures they are responsible both for the content and any discrepancies or misrepresentations. One in three applicants embellishes job titles, length of service, matching qualifications and/or experiences to the actual job for which they are applying.
- A thorough telephone screening interview, followed by in-person interviews with a human resources professional and someone from the department for which the applicant is applying, will go a long way in uncovering possible fabrications.
- A complete background check should include criminal records as permitted by law and traffic violations if the position calls for driving a company or personal vehicle for business. Special care is needed for individuals who will be responsible for working with children, in healthcare, or with the elderly. Education and address verification is critical, as well length of service and job title verification with former employers. Detailed backgrounds are usually best performed by a third party FCRA (Fair Credit Reporting Act) reporting agency specializing in backgrounds, both for legal reasons and to expedite the process through special databases and processes – ensuring a thorough, timely and legally sound result. Many states are passing laws prohibiting employers from asking candidates for their passwords to their private social media accounts. Nevertheless, much information can often be found simply by searching the internet. The Society for Human Resource Management (SHRM) states that 40% of employers surveyed said they used social media or online searches to screen job candidates in 2015, an increase from 33% in 2013. However, there are clear risks organizations must consider and address before social media checks are instituted, including standardization, opinions relative to candidate privacy, the accuracy and intent of information contained in social media profiles, and risks for potential discrimination claims in simply viewing social media profiles, as well as ever-increasing class action claims. Clearly, consultation with internal human resources and legal professionals should be sought to ensure consistency of approach and avoid any possibility of adverse impact.
- Remember – third party vendors should be subject to the same hiring standards as your own organization.

"Insider threats" are becoming more of a reality and a topic of discussion in the C-suite, as they tend to focus on the possibility of an employee acting out at a work location or other locations, bringing unwanted media scrutiny to the organization. Pre-employment background checks assist in mitigating risk in this regard, but it may be time to look forward and assess the insider risk of employees during the course of employment. Perhaps your employee was not a risk when hired, but what about the interim? Life events at home with spouse or children, finances, new politically radicalized views and, of course, workplace performance, can create tremendous stress upon an employee, who could then become a higher threat risk. Processes have been developed which allow an organization a dynamic versus a static or even periodic risk profile of employees.

Another danger of an insider threat is an employee approached by outsiders for critical information, unauthorized access, product information or even conducting terrorist activity. These situations are typically more difficult to uncover due to the employee's familiarity with internal processes and protocols, which can be used against an employer to enable prohibited or criminal activities. More and more organizations are forming Insider Threat Teams that establish policies and procedures to mitigate the opportunities for employers to be potential targets, and encourage individual involvement through employee awareness programs, including anonymous "hot lines" that highlight certain and extraordinary behaviors, job rotation, and management observation. In the end, while organizations are more often aware of the inherent risks and dangers of negligent hiring, we cannot lose focus on the real danger of negligent retention–policy violations must be handled in a consistent manner.

Securitas Security Services USA, Inc. is The Leader in Protective Services, serving a wide range of customers in a broad spectrum of industries and markets. As the U.S. division of an international organization with local focus, we offer comprehensive security solutions that leverage our 85,000 employees, knowledge, and technology to provide the protection necessary to meet each client's unique security requirements.

Our security solutions draw on The Six Pillars of Protective Services:

- *On-site Guarding*
- *Mobile Guarding*
- *Remote Guarding*
- *Electronic Security*
- *Fire and Safety*
- *Corporate Risk Management*

Securitas USA is committed to building long-lasting partnerships through a full understanding of its clients' security needs in order to provide superior service.

For more information, visit www.securitasinc.com

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

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

Securitas Security Services USA, Inc.
Nine Campus Drive
Parsippany, NJ 07054
www.securitasinc.com