Top Security Threats and Management Issues Facing Corporate America

2014 Survey of Fortune 1000 Companies

SECURITAS

80
2031

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.

We have completed the "2014 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 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 23% response rate from security executives in 38 states and Canada. Your input is critical to our report and it has revealed that the top five threats for 2014 are as follows:

1. Cyber/Communications Security

2. Workplace Violence

3. Business Continuity Planning

4. Employee Selection/Screening

5. Privacy Concerns

Cyber/Communications Security retained its #1 ranking from our previous survey. The next three threats also placed similarly to their rankings in the last survey, although there were some minor changes in position. An interesting development occurred with threat #5 — Privacy Concerns. This is a threat that has never appeared in our previous surveys, yet it achieved a Top 5 ranking this year.

The top security management challenges that were identified are: 1) Training Effectiveness/ Methods for Security Staffing Effectiveness, 2) Promoting Employee Awareness, and 3) Budget/Maximizing Return on Investment. 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 those security practitioners who contributed editorial comment for this issue, namely:

- Dave Tyson, CPP, CISSP, Senior Director, Global Information Security & Chief Information Security Officer, SC Johnson
- Brian J. Allen, Esq., CPP, CFE, CISM, Group Vice President & Chief Security Officer, Time Warner Cable Inc.
- Regis Becker, CPP, Chief Ethics and Compliance Officer, The Pennsylvania State University
- Terrance Gainer, Senior Advisor, Securitas Security Services USA, Inc.
- Jesse Berger, Vice President, Employment Screening Division, Pinkerton

Lastly, on a related note, Securitas USA is proud to be the exclusive sponsor of the ASIS Foundation's *Student Writing Competition*. In addition to a college scholarship, the winners received the opportunity to offer editorial comment on the Top Security Threats of 2014. We welcome the contributions of these outstanding students, Austin Bharadwaja and Robert Mavronicolas, to our report.

Don Walker, CPP

CHAIRMAN – SECURITAS SECURITY SERVICES USA, INC.

At Securitas and Pinkerton, we strive to constantly stay abreast of the current and evolving risks and threat levels faced by our clients around the globe. Most of the identified risks have remained constant for many years. What has changed is the degree of risk, the severity of the potential threats, the disregard for human life, the magnitude of the event, and the speed with which threat levels can change. The events of 9/11, the massive data breaches against organizations, and the terrorist activities in the Middle East and Africa demonstrate how quickly things can change and how threat levels need to be constantly evaluated.

Technology is speeding our communications, increasing our productivity, improving our quality of life, and making numerous other positive changes. At the same time, our increasingly hyper-connected environment is creating new security challenges, risks and threats. Cyberspace is used for a multitude of legitimate scientific, financial and business applications, in addition to social interaction. However, cyberspace and the rapid expansion of technology are being exploited and misused as tools for terrorist recruiting and communication; for enabling criminal enterprises and drug cartels to conduct their activity; for government sponsored hackers, individuals and enterprises to infiltrate and steal company and individual secrets; and for various other threats against organizations.

That's why our respondents again ranked Cyber/Communications Security as the number one threat, closely followed by Business Continuity and Organizational Resilience. We have asked our guest experts to comment on both Cyber Security and Organizational Resilience, as well as the need for adequate Employee Selection/Screening and Ethical Behavior to help prevent the insider threat or attack (such as the massive data theft by Edward Snowden).

We hope you find the Top Security Threats report to be a valuable tool for highlighting issues, trends and benchmarking with your peers. The report does not focus on specific countermeasures, as each organization is unique and may need to develop plans that are customized to each facility. However, there are numerous external resources available to assist organizations in developing programs to combat these and other security threats. One excellent resource is the suite of standards developed by ASIS International's Commission on Standards and Guidelines and approved by the American National Standards Institute. Current standards and guidelines include those that address Business Continuity, Organizational Resilience, Preemployment Background Screening, Workplace Violence Prevention and Intervention, and Physical Asset Protection. Visit www.asisonline.org/Standards-Guidelines/Pages/default.aspx for additional information.

As security threats of all types continue to increase on what seems to be a daily basis, it is incumbent upon all security practitioners to address these threats directly as they relate to each of our organizations. Only then will our workplaces, homes and communities continue to be safe from the host of security issues discussed in this 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 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 2014 "Top Security Threats and Management Challenges 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.

The 2014 survey drew 248 responses from corporate security directors and other executives with primary responsibility for their companies' security programs, yielding a 23% response rate.

Today's Threat Environment

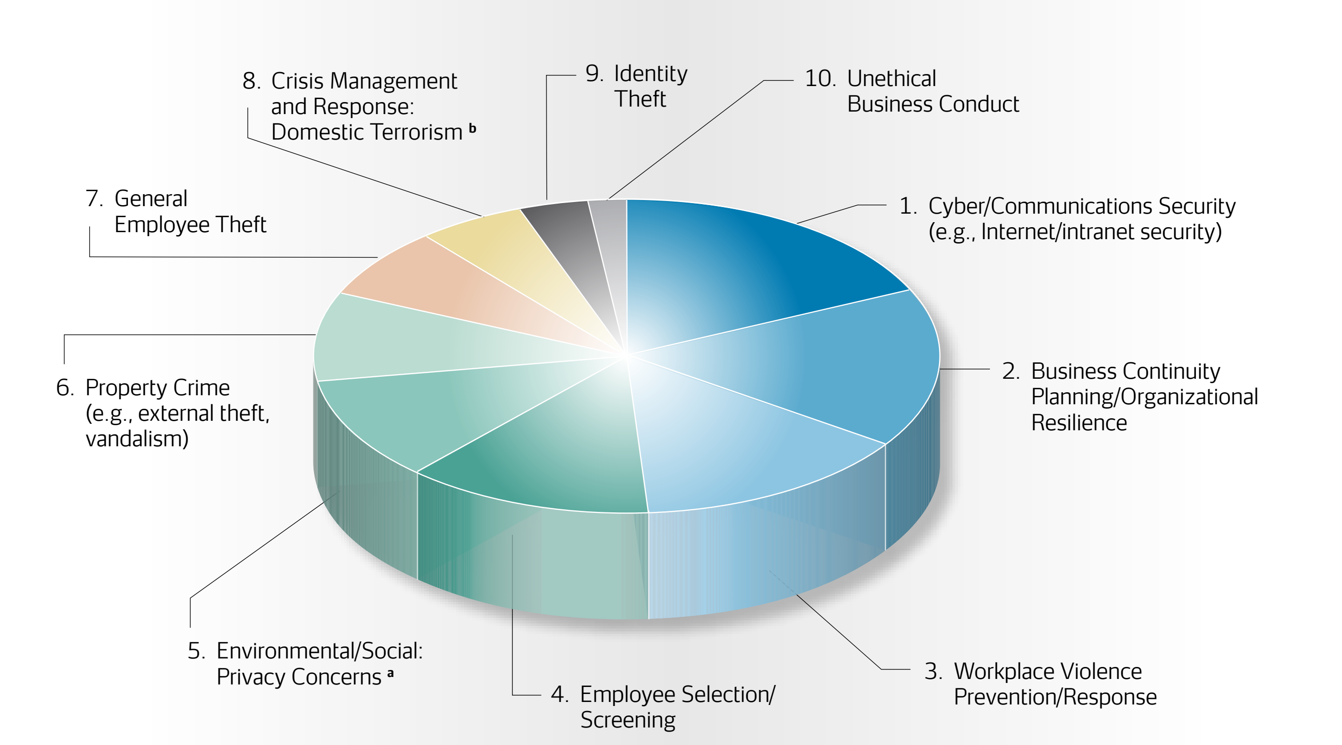
The study revealed the issues of greatest concern to corporate security directors, in rank order (See Figure 1).

The threat of Cyber/Communications Security remains the greatest security concern facing Fortune 1000 companies in 2014. Business Continuity Planning, including Organizational Resilience, moves up to 2nd place in 2014 after being in 3rd place since 2010. Workplace Violence held the number two spot since 2010 and falls to 3rd place in 2014, while Employee Selection/Screening remains in 4th place, holding this position since 2008.

Privacy Concerns, a new attribute in 2014, holds the 5th place position; Property Crime falls to 6th place in 2014 from 5th place in 2012; General Employee Theft falls to 7th place in 2014 from 6th place in 2012; Domestic Terrorism, a newly separated attribute in 2014, holds the 8th place position; Identity Theft moves up to 9th place in 2014 from 10th place in 2012; and Unethical Business Conduct falls to 10th place position in 2014 from 8th place in 2012.

Figure 1

2014 Top Security Threats



a. New attribute in 2014

b. Prior to 2014, this attribute was known generally as: Crisis Management and Response: 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 2014.

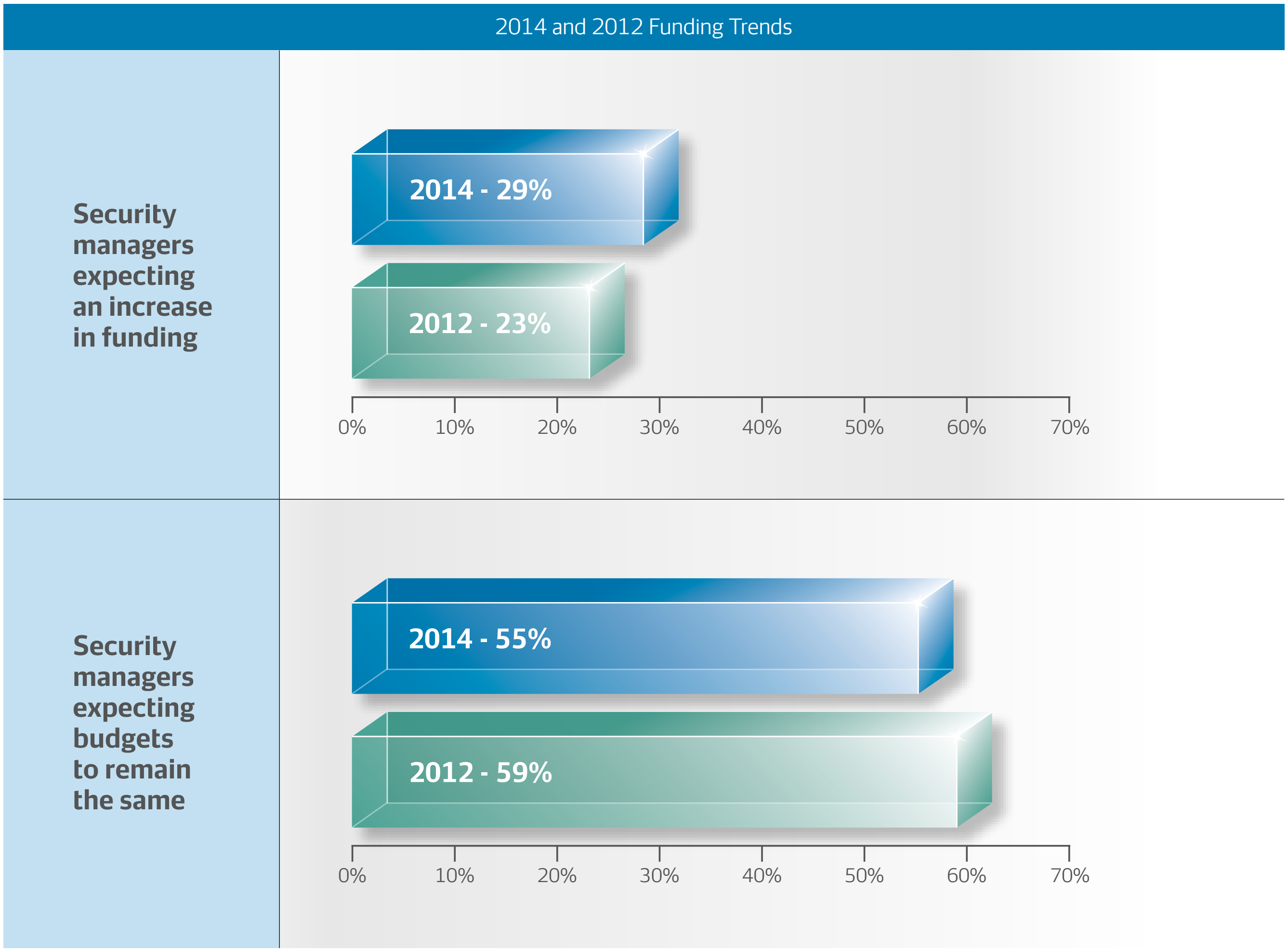
Figure 2

	Operational Issues of Greatest Concern
1	Security Staffing Effectiveness: Training Effectiveness/Methods
2	Promoting Employee Awareness
3	Budget/Maximizing Return On Investment
4	Regulatory/Compliance Issues (e.g., OSHA, C-TPAT, state/federal legislation, etc.)
5	Keeping Up With Technological Advances

Funding Trends

Over the next three to five years, the funding outlook for corporate security programs shows that 29% of security managers are expecting an increase in funding in 2014 compared to 23% in 2012. It further shows that 55% of security managers are expecting budgets to remain the same compared to 59% in 2012.

Figure 3



To assess the relative level of concern held by security professionals, the Security Threats survey presented a list of 26 potential security threats developed by Securitas USA. These were refined from the 2012 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 2014 rankings are shown in Figure 4.

Figure 4

2014 Rank	Top Security Threats - Ranking	Average Importance Score
1	Cyber/Communications Security (e.g., Internet/intranet security)	3.99
2	Business Continuity Planning/Organizational Resilience	3.86
3	Workplace Violence Prevention/Response	3.80
4	Employee Selection/Screening	3.70
5	Environmental/Social: Privacy Concerns [a]	3.48
6	Property Crime (e.g., external theft, vandalism)	3.44
7	General Employee Theft	3.22
8	Crisis Management and Response: Domestic Terrorism [b]	3.11
9	Identity Theft	3.10
10	Unethical Business Conduct	3.07
11	Environmental/Social: Pandemics (e.g., Ebola virus) [c]	3.05
12	Crisis Management and Response: Political Unrest/Regional Instability/National Disasters (evacuation potential)	3.04
13	Litigation: Inadequate Security	3.02
14	Fraud/White-Collar Crime	2.97
15 (tie)	Substance Abuse (drugs/alcohol in the workplace)	2.96
15 (tie)	Litigation: Negligent Hiring/Supervision	2.96
17	Business Espionage/Theft of Trade Secrets	2.95
18	Environmental/Social: Robberies	2.92
19	Intellectual Property/Brand Protection/Product Counterfeiting	2.89
20	Global Supply-Chain Security	2.85
21	Executive Protection (including travel security)	2.80
22	Insurance/Workers' Compensation Fraud	2.64
23	Crisis Management and Response: International Terrorism [b]	2.60
24	Bombings/Bomb Threats	2.54
25	Labor Unrest	2.42
26	Crisis Management and Response: Kidnapping/Extortion	2.31

a. New attribute in 2014
b. Prior to 2014, this attribute was known generally as: Crisis Management and Response: Terrorism
c. From 2008 through 2012, this attribute was known generally as: Environmental/Social: Pandemics

Cyber/Communications Security is the foremost concern of corporate security directors, reflecting the country's high reliance on technology. It has held this position since 2010. Business Continuity Planning/Organizational Resilience moves up to 2nd place from 3rd place in 2012, and Workplace Violence Prevention/Response is currently the third highest concern. Employee Selection remains in 4th place (where it has been since 2008). Privacy Concerns, a new attribute in 2014, holds the 5th place position, while Property Crime falls to 6th place in 2014 from 5th place in 2012. General Employee Theft falls to 7th place from 6th place. Domestic Terrorism, a newly separated attribute in 2014, holds the 8th place position.

Figure 5

Top Security Threats 1997 - 2014*

Security Threats	1997	1998	1999	2000	2001	2002	2003	2008	2010	2012	**2014**
Cyber/Communications Security (e.g., Internet/intranet security)	10	8	7	2 (tie)	2	4	3	3	1	1	**1**
Business Continuity Planning/Organizational Resilience	5	7	2	2 (tie)	5	2	2	2	3	3	**2**
Workplace Violence Prevention/Response	1	2	1	1	1	1	1	1	2	2	**3**
Employee Selection/Screening	4	4	4	5	3	5	5	4	4	4	**4**
Environmental/Social: Privacy Concerns [a]	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	**5**
Property Crime (e.g., external theft, vandalism)	12	10	10	12	10	9	12 (tie)	5 (tie)	7	5	**6**
General Employee Theft	2	1	6	6	6	8	7	5 (tie)	8	6	**7**
Crisis Management and Response: Domestic Terrorism [b]	15	17	14	16	17	3	4	7	12	15	**8**
Identity Theft	NA	NA	NA	NA	16	14 (tie)	10	12	11	10	**9**
Unethical Business Conduct	3	6	9	7	9	7	8	9	5	8	**10**
Environmental/Social: Pandemics (e.g., Ebola virus) [c]	NA	NA	NA	NA	NA	NA	NA	17	18	22	**11**
Crisis Management and Response: Political Unrest/Regional Instability/ National Disasters (evacuation potential)	NA	NA	19	17	20	14 (tie)	11	10	6	7	**12**
Litigation: Inadequate Security	13	13	13	13 (tie)	13	11 (tie)	18	19 (tie)	16	9	**13**
Fraud/White-Collar Crime	7	3	3	4	4	6	6	8	10	12	**14**
Substance Abuse (drugs/alcohol in the workplace)	9	11	8	9	8	10	9	19 (tie)	17	13	**15 (tie)**
Litigation: Negligent Hiring/Supervision	16	16	15	13 (tie)	14	18	20	25	23	17	**15 (tie)**
Business Espionage/Theft of Trade Secrets	NA	9	12	11	12	19	16	15 (tie)	15	16	**17**
Environmental/Social: Robberies	NA	NA	NA	NA	NA	NA	NA	27 (tie)	19	14	**18**
Intellectual Property/Brand Protection/ Product Counterfeiting	NA	NA	NA	NA	NA	NA	NA	21	14	11	**19**
Global Supply-Chain Security	NA	NA	17	19	18	22	21	27 (tie)	22	20	**20**
Executive Protection (including travel security)	NA	NA	NA	NA	NA	NA	NA	22 (tie)	13	18	**21**
Insurance/Workers' Compensation Fraud	17	19	16	15	15	17	17	26	25	21	**22**
Crisis Management and Response: International Terrorism [b]	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	**23**
Bombings/Bomb Threats	NA	NA	NA	NA	NA	NA	NA	14	24	19	**24**
Labor Unrest	NA	NA	NA	NA	NA	NA	NA	29	26	23	**25**
Crisis Management and Response: Kidnapping/Extortion	NA	NA	18	18	19	20	19	33	27	24	**26**

* Rankings for 1997-2012 do not include every threat option, as some were replaced by new options in more recent surveys

a. New attribute in 2014

b. Prior to 2014, this attribute was known generally as: Crisis Management and Response: Terrorism

c. From 2008 through 2012, this attribute was known generally as: Environmental/Social: Pandemics

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 (26%); Real Estate, Rental and Leasing (13%); Healthcare and Social Assistance (12%); Finance and Insurance (8%); Utilities (8%); 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 2014 remain unchanged compared to 2012. Cyber/Communications Security is 1st, Workplace Violence Prevention/Response is 2nd and Business Continuity Planning/Organizational Resilience is in 3rd place. Employee Selection/Screening moves up to 4th place from 6th place and Business Espionage/Theft of Trade Secrets moves up to 5th place from 6th place in 2012.

Figure 6

Top Threats by Industry - Manufacturing

Total Respondents Rank 2014	Rank Within Industry 2014	Security Threats	Rank Within Industry 2012
1	1	Cyber/Communications Security (e.g., Internet/intranet security)	1
3	2	Workplace Violence Prevention/Response	2
2	3	Business Continuity Planning/Organizational Resilience	3
4	4	Employee Selection/Screening	6 (tie)
17	5	Business Espionage/Theft of Trade Secrets	6 (tie)
20	6	Global Supply-Chain Security	5
19	7	Intellectual Property/Brand Protection/Product Counterfeiting	4
5	8	Environmental/Social: Privacy Concerns [a]	NA
7	9	General Employee Theft	8
10	10	Unethical Business Conduct	12

a. New attribute in 2014

B. Real Estate, Rental and Leasing

For management security threats in the Real Estate, Rental and Leasing industry, Property Crime remains in 1st place as the security threat of greatest concern in 2014. Business Continuity Planning/Organizational Resilience jumps from 8th place in 2012 to 2nd place in 2014. Robberies moves up to 3rd place in 2014 from 6th place in 2012. Cyber/Communications Security makes a jump to 4th place in 2014 from 11th place in 2012, while Privacy Concerns, a new attribute for 2014, comes in at 5th place. Inadequate Security moves up to 6th place in 2014 from 8th place in 2012. Domestic Terrorism, a newly separated attribute in 2014, ties 7th place with Employee Selection/Screening in 2014.

Figure 7

Top Threats by Industry - Real Estate, Rental and Leasing

Total Respondents Rank 2014	Rank Within Industry 2014	Security Threats	Rank Within Industry 2012
6	1	Property Crime (e.g., external theft, vandalism)	1
2	2	Business Continuity Planning/Organizational Resilience	8 (tie)
18	3	Environmental/Social: Robberies	6
1	4	Cyber/Communications Security (e.g., Internet/intranet security)	11
5	5	Environmental/Social: Privacy Concerns [a]	NA
13	6	Litigation: Inadequate Security	8 (tie)
8	7 (tie)	Crisis Management and Response: Domestic Terrorism [b]	NA
4	7 (tie)	Employee Selection/Screening	2
9	9	Identity Theft	7
3	10	Workplace Violence Prevention/Response	5

a. New attribute in 2014
b. Prior to 2014, this attribute was known generally as: Crisis Management and Response: Terrorism

C. Healthcare and Social Assistance

Cyber/Communications Security is the greatest concern of security threats in the Healthcare and Social Assistance industry, moving up to 1st place in 2014 from 2nd place in 2012. Business Continuity Planning/Organizational Resilience moves up to 2nd place in 2014 from 3rd place in 2012. Workplace Violence Prevention/Response falls from the 1st place position in 2012 to 3rd place in 2014, while Employee Selection/Screening remains in 4th place in 2014. Privacy Concerns, a new attribute in 2014, comes in at 5th place. Pandemics (e.g., Ebola virus), makes a major jump from 19th place in 2012 to 6th place in 2014. Crisis Management and Response ties 7th place in 2014 (rising from 9th place in 2012) with Business Espionage/Theft of Trade Secrets, which jumps from 18th place in 2012.

Figure 8

Top Threats by Industry - Healthcare and Social Assistance

Total Respondents Rank 2014	Rank Within Industry 2014	Security Threats	Rank Within Industry 2012
1	1	Cyber/Communications Security (e.g., Internet/intranet security)	2
2	2	Business Continuity Planning/Organizational Resilience	3
3	3	Workplace Violence Prevention/Response	1
4	4	Employee Selection/Screening	4
5	5	Environmental/Social: Privacy Concerns [a]	NA
11	6	Environmental/Social: Pandemics (e.g., Ebola virus) [b]	19
12	7 (tie)	Crisis Management and Response: Political Unrest/Regional Instability/National Disasters (evacuation potential)	9 (tie)
17	7 (tie)	Business Espionage/Theft of Trade Secrets	18
19	9 (tie)	Intellectual Property/Brand Protection/Product Counterfeiting	6
20	9 (tie)	Global Supply-Chain Security	11

a. New attribute in 2014
b. From 2008 through 2012, this attribute was known generally as: Environmental/Social: Pandemics

D. Finance and Insurance

The top security threat for 2014 in the Finance and Insurance industry is Cyber/Communications Security, and remains unchanged compared to 2012. Business Continuity Planning/Organizational Resilience moves up from 3rd place in 2012 to 2nd place in 2014. Workplace Violence Prevention/Response falls from 2nd place in 2012 to 3rd place in 2014. Employee Selection/Screening ties 4th place in 2014 (moving up from the 6th position in 2012) with Privacy Concerns, a new attribute in 2014.

Figure 9

Top Threats by Industry - Finance and Insurance

Total Respondents Rank 2014	Rank Within Industry 2014	Security Threats	Rank Within Industry 2012
1	1	Cyber/Communications Security (e.g., Internet/intranet security)	1
2	2	Business Continuity Planning/Organizational Resilience	3
3	3	Workplace Violence Prevention/Response	2
4	4 (tie)	Employee Selection/Screening	6 (tie)
5	4 (tie)	Environmental/Social: Privacy Concerns [a]	NA
14	6	Fraud/White-Collar Crime	4
9	7	Identity Theft	6 (tie)
8	8	Crisis Management and Response: Domestic Terrorism [b]	NA
10	9	Unethical Business Conduct	8
21	10	Executive Protection (including travel security)	5

a. New attribute in 2014
b. Prior to 2014, this attribute was known generally as: Crisis Management and Response: Terrorism

E. Utilities

In 2014, Cyber/Communications Security remains the security threat of greatest concern in the Utilities industry. Business Continuity Planning/Organizational Resilience remains in 2nd place, while Employee Selection/Screening moves up to 3rd place in 2014 from 8th place in 2012. Workplace Violence Prevention/Response falls to 4th place in 2014 from 3rd place in 2012. Domestic Terrorism, a newly separated attribute in 2014, holds the 5th place position in 2014. Privacy Concerns, a new attribute in 2014, comes in at 6th place. Substance Abuse ties 7th place in 2014 (making a jump from 11th place in 2012) with Property Crime, falling from the 5th place position in 2012.

Figure 10

Top Threats by Industry - Utilities

Total Respondents Rank 2014	Rank Within Industry 2014	Security Threats	Rank Within Industry 2012
1	1	Cyber/Communications Security (e.g., Internet/intranet security)	1
2	2	Business Continuity Planning/Organizational Resilience	2
4	3	Employee Selection/Screening	8
3	4	Workplace Violence Prevention/Response	3
8	5	Crisis Management and Response: Domestic Terrorism [b]	NA
5	6	Environmental/Social: Privacy Concerns [a]	NA
6	7 (tie)	Property Crime (e.g., external theft, vandalism)	5
15 (tie)	7 (tie)	Substance Abuse (drugs/alcohol in the workplace)	11 (tie)
9	9	Identity Theft	7
12	10 (tie)	Crisis Management and Response: Political Unrest/Regional Instability/National Disasters (evacuation potential)	10
7	10 (tie)	General Employee Theft	9
10	10 (tie)	Unethical Business Conduct	14 (tie)
11	10 (tie)	Environmental/Social: Pandemics (e.g., Ebola virus) [c]	21
14	10 (tie)	Fraud/White-Collar Crime	11 (tie)

a. New attribute in 2014
b. Prior to 2014, this attribute was known generally as: Crisis Management and Response: Terrorism
c. From 2008 through 2012, this attribute was known generally as: Environmental/Social: Pandemics

F. Transportation and Warehousing

In the Transportation and Warehousing industry, Property Crime is the security threat of greatest concern in 2014, moving up from 8th place in 2012. General Employee Theft moves up to 2nd place in 2014 from 7th place in 2012. Employee Selection/Screening moves up to 3rd place in 2014 from 5th place in 2012. Robberies makes a jump to 4th place in 2014 from 12th place in 2012. Cyber/Communications Security, Workplace Violence Prevention/Response and Global Supply-Chain Security all tie for 5th place in 2014.

Figure 11

Top Threats by Industry - Transportation and Warehousing

Total Respondents Rank 2014	Rank Within Industry 2014	Security Threats	Rank Within Industry 2012
6	1	Property Crime (e.g., external theft, vandalism)	8
7	2	General Employee Theft	7
4	3	Employee Selection/Screening	5 (tie)
18	4	Environmental/Social: Robberies	12 (tie)
1	5 (tie)	Cyber/Communications Security (e.g., Internet/intranet security)	9
3	5 (tie)	Workplace Violence Prevention/Response	4
20	5 (tie)	Global Supply-Chain Security	10 (tie)
2	8 (tie)	Business Continuity Planning/Organizational Resilience	2 (tie)
5	8 (tie)	Environmental/Social: Privacy Concerns [a]	NA
15 (tie)	10	Substance Abuse (drugs/alcohol in the workplace)	12 (tie)

a. New attribute in 2014

G. Information

Business Continuity Planning/Organizational Resilience moves up from 2nd place in 2012 to be the security threat of greatest concern in the Information industry in 2014. Cyber/Communications Security falls from 1st place in 2012 to 2nd place in 2014. Privacy Concerns, a new attribute in 2014, comes in at 3rd place. Workplace Violence Prevention/Response moves up from 6th place in 2012 to 4th place in 2014. Employee Selection/Screening remains the same at 5th place in 2014. Executive Protection jumps from 14th place in 2012 to 6th place in 2014.

Figure 12

Top Threats by Industry - Information

Total Respondents Rank 2014	Rank Within Industry 2014	Security Threats	Rank Within Industry 2012
2	1	Business Continuity Planning/Organizational Resilience	2 (tie)
1	2	Cyber/Communications Security (e.g., Internet/intranet security)	1
5	3	Environmental/Social: Privacy Concerns [a]	NA
3	4	Workplace Violence Prevention/Response	6
4	5	Employee Selection/Screening	5
21	6	Executive Protection (including travel security)	14
19	7	Intellectual Property/Brand Protection/Product Counterfeiting	7 (tie)
17	8 (tie)	Business Espionage/Theft of Trade Secrets	9
14	8 (tie)	Fraud/White-Collar Crime	2 (tie)
9	10	Identity Theft	4

a. New attribute in 2014

H. Retail Trade

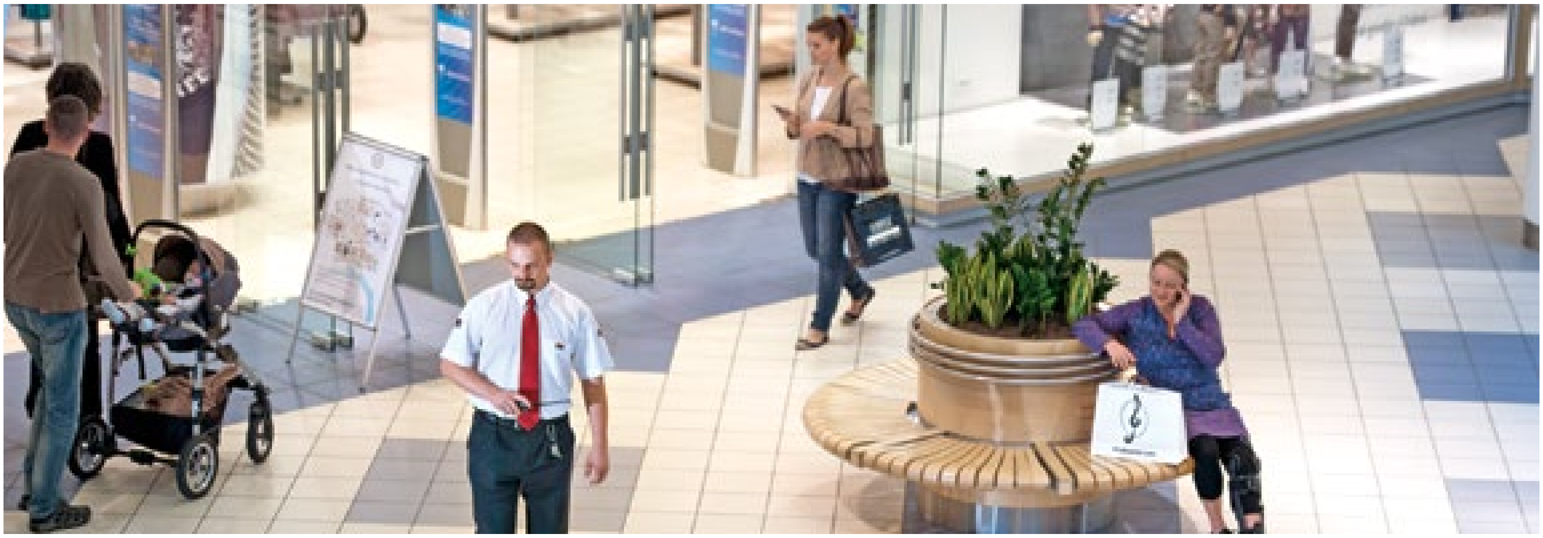
To Fortune 1000 retailers and related companies, General Employee Theft, which ranked 3rd in 2012, moves to 1st place as the security threat of greatest concern in 2014. Cyber/Communications Security ties 2nd place in 2014 (falling from 1st place in 2012) with Identity Theft, which moves up from 3rd place in 2012. Employee Selection/Screening makes a major jump from 17th place in 2012 and ties at 4th place in 2014 with Workplace Violence Prevention/Response, which moves up from 6th place in 2012. Robberies falls to 6th place in 2014 from 5th place in 2012. Fraud/White-Collar Crime ties 7th place in 2014 (making a jump from 11th place in 2012) with Property Crime, falling from the 2nd place position in 2012.

Figure 13

Top Threats by Industry - Retail Trade

Total Respondents Rank 2014	Rank Within Industry 2014	Security Threats	Rank Within Industry 2012
7	1	General Employee Theft	3 (tie)
1	2 (tie)	Cyber/Communications Security (e.g., Internet/intranet security)	1
9	2 (tie)	Identity Theft	3 (tie)
4	4 (tie)	Employee Selection/Screening	17 (tie)
3	4 (tie)	Workplace Violence Prevention/Response	6 (tie)
18	6	Environmental/Social: Robberies	5
14	7 (tie)	Fraud/White-Collar Crime	11 (tie)
6	7 (tie)	Property Crime (e.g., external theft, vandalism)	2
20	9	Global Supply-Chain Security	14
5	10	Environmental/Social: Privacy Concerns [a]	NA

[a] New attribute in 2014



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 challenges with regard to their anticipated impact on your company's security program during the next 12 months." Results are shown below (Figure 14).

Training Effectiveness/Methods for Security Staffing Effectiveness holds the top position for 2014 security management issues. Promoting Employee Awareness is 2nd, Budget/Maximizing Return On Investment is 3rd and Regulatory/Compliance Issues is 4th. Keeping Up With Technological Advances ranks 5th. The top security management challenges ranked 6th through 10th are: Threat Assessments, Strategic Planning, Implementing Best Practices/Standards/Key Performance Indicators, Adequate Staffing Levels and Selection and Hiring Methods for Security Staffing Effectiveness

Figure 14

2014 Rank	Management Issues	Average Importance Score
1	Security Staffing Effectiveness: Training Effectiveness/Methods	3.94
2	Promoting Employee Awareness	3.82
3	Budget/Maximizing Return On Investment	3.78
4	Regulatory/Compliance Issues (e.g., OSHA, C-TPAT, state/federal legislation, etc.)	3.73
5	Keeping Up With Technological Advances	3.71
6	Threat Assessments	3.69
7	Strategic Planning	3.67
8	Implementing Best Practices/Standards/Key Performance Indicators	3.63
9	Security Staffing Effectiveness: Adequate Staffing Levels	3.60
10	Security Staffing Effectiveness: Selection and Hiring Methods	3.57
11	Security Staffing Effectiveness: Security Officer Turnover	3.37
12	Managing Remote Security Operations	3.25
13	Additional Security Responsibilities (aviation/compliance/ethics, etc.)	3.16
14	Career Development	3.13
15	Security Staffing Effectiveness: Absenteeism	2.98
16	Global Supply-Chain Decisions	2.57

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 (17%) or Operations (17%). Administration (11%), Legal (11%) and CEO/President (10%), Environmental/ Health/Safety (9%) and Human Resources (8%), Finance (7%) and Risk Management (6%) are the next most frequently mentioned areas.

Responses are summarized in Figure 15.

Figure 15

Organizational Area	2012	2014
Facilities	16%	**17%**
Operations	13%	**17%**
Administration	16%	**11%**
Legal	9%	**11%**
Directly to the CEO/President	12%	**10%**
Environmental/Health/Safety	11%	**9%**
Human Resources	11%	**8%**
Finance	2%	**7%**
Risk Management	7%	**6%**
IT/MIS	2%	**2%**
Audit	2%	**2%**

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

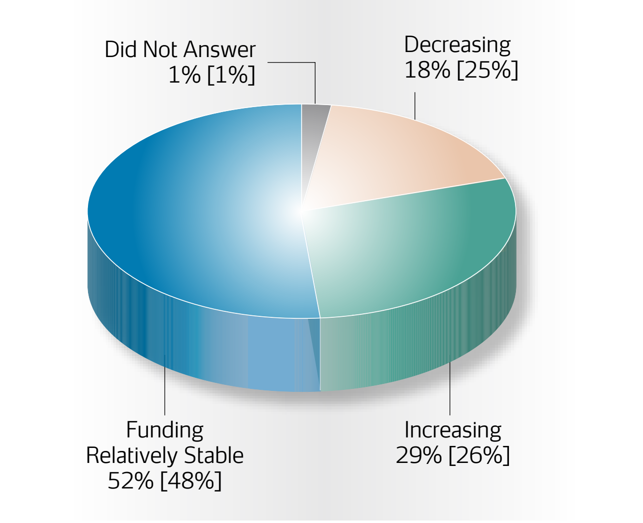
Budget and Funding

Funding Trends

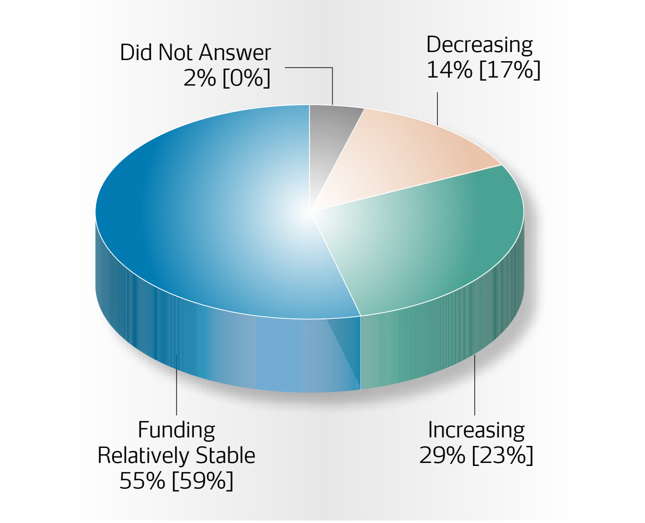
The funding outlook for corporate security programs over the next three to five years reflects that 29% of security managers are expecting an increase in funding in 2014. The percentage of security managers expecting budgets to remain the same is 55% in 2014, while the percentage of managers anticipating decreased funding is 14% in 2014.

Note: The percentages in the [brackets] are 2012 percentages.

Security Funding: Past 3 - 5 Years



Security Funding: Next 3 - 5 Years



A. Survey Methodology

For the "2014 Top Security Threats and Management Challenges Facing Corporate America" survey, 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 1,072 security directors and other executives identified as having oversight of the corporate security function of these companies. The survey questionnaire was distributed in November 2014. 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 January 2015.

Reflected in this report are the responses taken from 248 returned surveys, which represented a 23.1% 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.

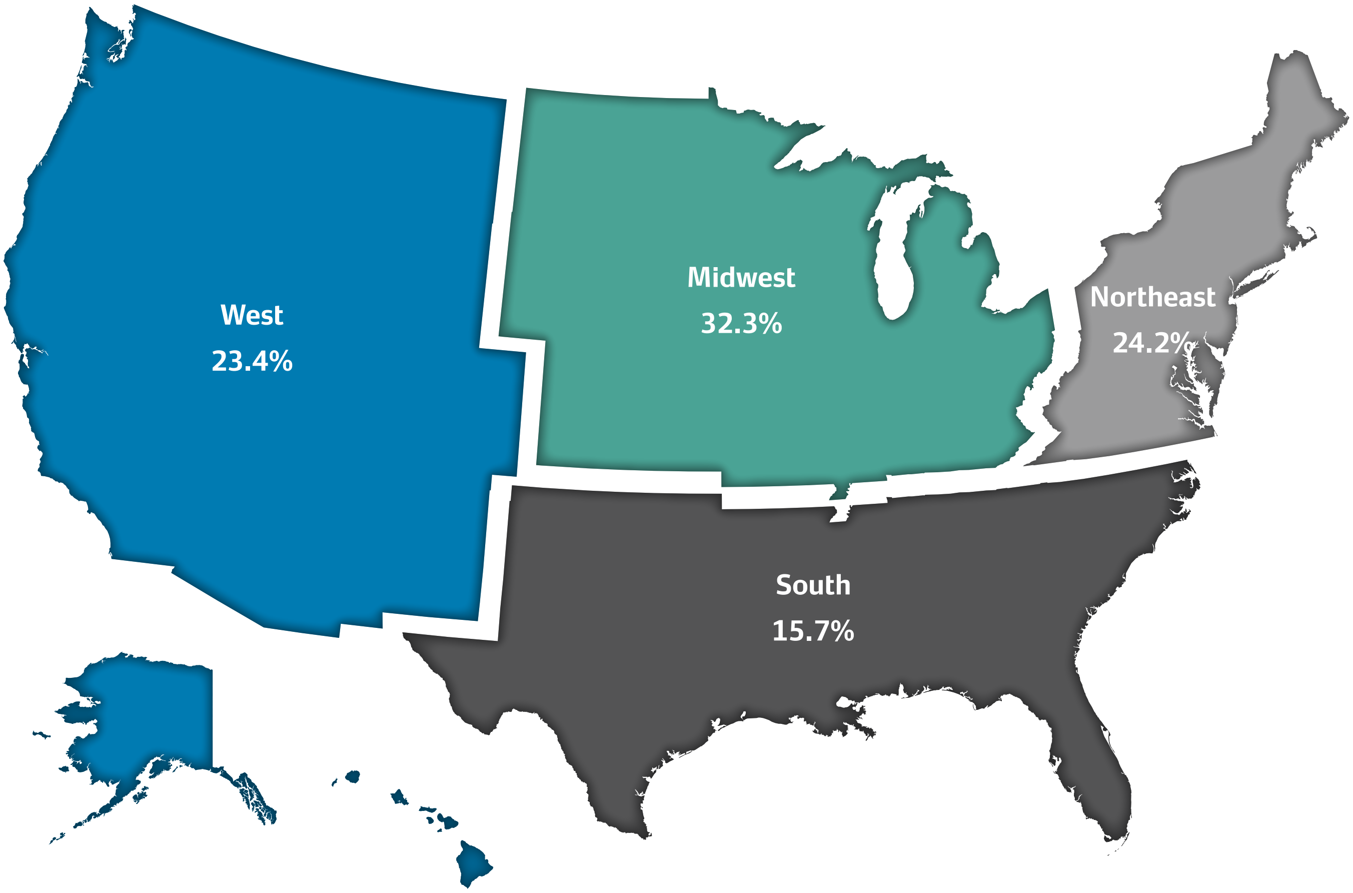
B. Respondent Distribution

Twenty-one specific industries 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	19
Construction	3
Wholesale Trade	3
Retail Trade	8
Healthcare and Social Assistance	30
Arts, Entertainment and Recreation	6
Finance and Insurance	20
Real Estate, Rental and Leasing	31
Professional, Scientific and Technical Services	10
Educational Services	19
Accommodation and Food Services	1
Transportation and Warehousing	14
Law Enforcement	5
Manufacturing	**65**
Food Manufacturing	11
Wood Product Manufacturing	5
Computer and Electronic Product Manufacturing	7
Electrical Equipment, Appliance and Component Manufacturing	7
Transportation Equipment Manufacturing	10
Miscellaneous Manufacturing	25
Information	**14**
Telecommunications	6
Other Information Services	8
Other	**4**
TOTAL	**248**

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 - 95.6%

International Total (Canada) - 4.4%

Total - 100%

2014 Top Information Security Threats

DAVE TYSON, CPP, CISSP

For many people, 2014 was considered the year of the computer breach; literally dozens of major breaches were publicly announced throughout the year. Moreover, 2015 is shaping up to be just as active, if not even more perilous, for companies in defending their intellectual property, customer (PII), healthcare (PHI) and other sensitive information.

There are Four Mega Trends for understanding the largest threats facing companies in 2015 and beyond.

1. The Pace of Technological Change Versus a Company's Understanding of the Risks of Using it

   On average, technology users carry 2.9 devices at all times, but given the millions of mobile apps available in the various on-line App stores, it is nearly impossible for the average person to understand how safe they are. Consumers also discard devices at a hastening rate, with over 220,000,000 tons of old computers and other technology devices being trashed in the United States each year. It makes one wonder if these devices have all had the data on them wiped and properly deleted.

2. The New Normal of Social Media

   Facebook uploads are 500 times more than the NY Stock Exchange and there are 350,000,000 Snapchat messages sent every day. While it's hard to know how much of this information puts people or companies at risk, it is certainly a growing area of exposure for businesses today.

3. The Interconnection Revolution – The Internet of Things

   Whether it's your car, your home electrical meter, or your refrigerator, the connecting of devices to the Internet will become the next great unknown: by 2020, it is estimated there will be 30,000,000,000 in-home IP connected devices.

4. The Gap Between the Skills of the Hackers and the Tools for Everyday People to Protect Themselves is Widening

   Over half of Internet traffic in 2014 was from 'bots,' or robot controlled computers that are programmed to attack and steal your computer; you could say the internet is in peril of becoming the new Wild West where safe places are rare and lawlessness is common.

All is not lost, though.

The good news is that companies can easily take real steps to protect themselves, and the best weapons they have are security aware employees. Good security fundamentals still matter in this day and age and proper technology risk assessments, trained information security personnel and clear, top down management prioritization for data protection can make a world of difference.

Most importantly, the question that must be asked going forward concerning technological risk is not IF you can do something, but SHOULD you do it, and do you fully appreciate the risks, both now and in the future, of how a technology will be used?

Dave Tyson, CPP, CISSP is an Enterprise Security Senior Executive with 30 years' experience in all facets of Enterprise Security.

Tyson is currently a Senior Director, Global Information Security & CISO for SC Johnson. Prior to that he lead security programs for PG&E, one of the largest power utilities in the U.S., was the Global Security operations lead for eBay, and the Chief Security Officer for the Host City of the 2010 Winter Olympics.

Tyson has a Master's Degree in Business Administration (MBA) specializing in Digital Technology Management, is a Certified Protection Professional (CPP) and Board Certified in Security Management, and is a Certified Information Systems Security Professional (CISSP).

Tyson is a frequent speaker at conferences and education events in North and South America, Asia and Europe. He has published dozens of articles in industry magazines and published the first book on Security Convergence via Butterworth Heinemann: *Security Convergence: Managing Enterprise Security Risk*.

Tyson is a member of the Board of Directors and 2015 President of ASIS International.

Business Continuity and Cybersecurity

BRIAN J. ALLEN, ESQ., CPP, CFE, CISM

Brian Allen, ESQ., CPP, CFE, CISM is the Chief Security Officer for Time Warner Cable located in New York, NY. He joined Time Warner Cable in January, 2002 and has over 20 years of experience in the security field. In his role as CSO, Brian is responsible for the global protection of Time Warner Cable's assets, and coordinates the company's crisis management and business continuity management program, including the coordination with federal and state emergency management organizations. Allen also manages cybersecurity policy for the company. He leads the security risk management program, which includes the company's Law Enforcement Response Center, the customer facing Enterprise Risk Operation Center, oversight of internal/external investigations and heads up the company's workplace violence program.

Allen earned his BS in Criminal Justice from Long Island University and received his Juris Doctor from Touro Law Center in New York. He is a member of the New York State Bar Association, a Certified Protection Professional with ASIS, a Certified Fraud Examiner with the ACFE and a Certified Information Security Manager with ISACA. Allen is also a member of the International Security Management Association and the Association of Threat Assessment Professionals.

Allen actively sits on the Board of Directors with the Domestic Violence Crisis Center in Connecticut, served on the Board of Directors of ASIS International from 2011-2013, and actively sits on the Board of Trustees of the ASIS International Foundation.

Today's environment of business risk exposure is a constantly shifting landscape. The changing data security threat scenarios brought about by technical advances like the "Internet of Things," and the potential for supply chain disruption based on threats to the automated systems that businesses depend on so indispensably to keep operations up and running, are only two of the many serious concerns to consider. It sometimes seems that Cybersecurity threats change every time you read a newspaper, and further, that the cyber threat profile has rapidly changed from a technology and data security issue to a business resiliency and risk management issue. As fast as this topic is moving, we have to ask – are business continuity and crisis management plans keeping pace?

The threats we are now seeing to organizational resiliency bring with them a need for more creative thinking from business leaders on how to anticipate the potential impacts to the business from a cyber-event. They also spotlight a necessity for closer engagement of technical responders and crisis planners with the business units to develop a business response to events that were once perceived as technical issues.

There are many questions that must be considered as drivers for developing comprehensive response programs and practices:

- How quickly should a validated cyber risk get escalated to a response team?
- Who is driving the response – the IT department or the business?
- What's the impact to the business?
- Is the impact a business issue or a technical problem and who's making the distinction?
- Does the business properly know the cyber risk and is it weighing in appropriately to prioritize the risks?
- Is the change in risk changing the engagement with the business or is the siloed approach to security, response and continuity still being maintained?

While discovering answers to these questions, the business continuity and crisis management programs can play a key role in bridging the gaps from an event being perceived as a pure technology problem, to identifying risks to operations brought about by the underlying technical incident and engaging with the business to develop a response to all types of crises.

The major hurdles can't be understated in this process, the primary one being that the cyber event is, by historical definition, a technology issue and a technology problem, which the potential impacts to the business are proving it is not. Moving the business into this space can feel like an overreach because, at the outset, the risk to operations is not fully understood by the business. However, to reach a higher level of organizational resilience, it's essential to break down these walls. Below are some best practices to engage the business in the changing cyber risk discussion using existing business continuity management program responsibilities.

- Hold small, tightly focused exercises for business functions exploring the potential business impacts of a cyber risk.
- Clearly identify escalation criteria that would bring the business into any cyber incident response plan.
- Provide risk governance guidance to the business based on a business impact analysis related to cyber threats.

Unethical Business Conduct

REGIS W. BECKER, CPP

Unethical business conduct is perennially one of the highest ranked threats to organizations. That should not be a surprise, as no asset is more valuable to any business or institution than its reputation, and no asset is more vulnerable. A century old firm with a history of satisfied customers, happy employees and enriched investors can be brought down by the unethical conduct of a single employee. Every employee carries the reputation of their employer with them each day. Every interaction the employee has with your constituents has an impact and leaves an impression, whether good or bad.

I remember some terrific advice I received many years ago as a young FBI Special Agent, and I paraphrase it here as follows — "Every meeting you have every day of your career as an Agent might be the only time the person you're dealing with comes in contact with the FBI in their entire life – always conduct yourself as a professional because you represent every FBI employee in every interaction you have!" That is a powerful message that obviously goes well beyond unethical behavior — but that advice alone can't prevent unethical business behavior and won't protect your organization.

Millions of words have been written about how to set up proper ethics and compliance controls in your company, so where do you begin, and how do you set the proper tone and reach your employees? Of course, the U.S. Federal Sentencing Guidelines model ethics and compliance program (www.ussc.gov/guidelines-manual/2012/2012-8b21) is a great place to start, but I would suggest a simpler way to think about the issue. I think ethics and compliance programs boil down to three principles: Infrastructure, Engagement and Consequences.

Infrastructure consists of the ethics and compliance policies, procedures, certifications, hotlines, promotions and the people who manage those programs in every organization. These things are often what come to mind when we think of ethics programs and they are very important, but they are really only the beginning.

Engagement on ethics and compliance matters is, in my view, the most important and impactful of the three principles. Engagement means that leadership includes ethical topics when addressing employees and the public. It means that management considers the ethical components in the decision-making process. It means that, just like safety, it is a frequent topic at staff meetings and in training sessions. In short, ethics and compliance should be part of the fabric of the organization.

Consequences means that ethical actions and decisions have real world ramifications, both good and bad. What kind of behavior gets rewarded in your organization? What gets punished? Are policies ignored if good business results are achieved? Who are the role models both in leadership and middle management? Who sets the tone? The organization that gets this right greatly reduces the risk of unethical business behavior.

Of course, it sounds simple when we list these principles in this fashion. The key is, as always, in execution; the leadership team that focuses on these three principles and drives them into the organization's DNA will rarely, if ever, suffer the ethical lapses we read about every day.

Regis W. Becker, CPP directs the Penn State University Office of Ethics and Compliance. In this role, he serves as Chief Ethics & Compliance Officer and oversees all compliance issues throughout the University. Regis is also charged with developing Penn State's first comprehensive program of institutional ethics.

Becker previously served as Chief Compliance Officer for PPG Industries, a global Fortune 250 company with headquarters in Pittsburgh, PA, and as Director of Corporate Security for Praxair, Inc.

He began his career in law enforcement serving as an Allegheny County, PA detective and as an FBI Special Agent. A 1978 graduate of Penn State with a bachelor's degree in law enforcement, Becker earned his Juris Doctorate from the Duquesne University School of Law and MBA from the Western Connecticut State University. He is admitted to practice law in Pennsylvania.

Becker was elected to two terms as a member of the Board of Directors of ASIS International from 1992-97. He served as President of ASIS International in 1996 and Chairman of the Board the following year.

Crisis Management and Response

TERRANCE W. GAINER

The Honorable Terrance W. Gainer is Senior Advisor to Securitas Security Services USA, Inc. He advises the company on a range of security and law enforcement-related matters following a noteworthy 47-year career in law enforcement at federal, state and local levels. Terry joined the Chicago Police Department in 1968 and served as a homicide detective for several years before attending law school and returning to the Chicago PD as Chief Legal Officer. He subsequently served for nearly 10 years as Director of the Illinois State Police. In 1998 Terry was named Executive Assistant Chief of the Metropolitan Police in Washington, DC, responsible for all operations, and was appointed Chief of the U.S. Capitol Police in 2002. Four years later, he became the 38th U.S. Senate Sergeant at Arms, the Senate's chief law enforcement and administrative officer.

The key to effective crisis management and response, a Top 10 threat as identified in Securitas USA's newest Top Security Threats survey, is anticipating and preparing for emergency situations before they occur. Too often, organizations make the mistake of waiting until a crisis occurs to consider the proper response. That results in almost no chance of minimizing damage – either to people and property or to the organization's image and reputation among stakeholders.

As part of a safety and emergency preparedness program, organizations need to identify and assess the full range of potential risks, then develop specific action plans to prevent, mitigate, respond and recover from them. Depending on the type of organization, that can involve significant, ongoing work, but the effort almost certainly will prove worthwhile. Let me offer a few guiding principles for successful crisis management learned during my 47 years of experience in law enforcement.

Plan for all hazards and risks, then you'll be able to adapt to whatever occurs.

As Sergeant at Arms for the U.S. Senate, I was involved in planning and directing response tactics for all types of security-related situations, including terrorist attacks. But we never anticipated the event that occurred on August 23, 2011, a day that a Senate session was scheduled. A 5.8 earthquake shook the Washington, DC area, damaging several monuments and buildings, including the U.S. Capitol. Because contingency plans were in place for managing other types of disasters – procedures for evacuating the building, sheltering in place, securing all exits, assessing damage, treating injuries and even holding the Senate session in another location, if necessary – many potential difficulties were averted.

Establish clear command and control, a practical communications system and remain flexible as the situation develops.

Thousands of people began arriving hours in advance of President Obama's first inaugural ceremony on January 20, 2009. Because of a delay in opening a main entrance to seating, a local police officer directed the people to line up in a nearby traffic tunnel that had been closed for the event. Officials were never notified that they were waiting there, and the calls, texts and tweets from stranded ticket holders went unanswered because no one at the Command Center was monitoring telephone and social media communications.

Consider the needs of all stakeholders who play a role in a crisis situation.

When a lone gunman entered Building 197 inside the headquarters of the Navy Sea Systems Command at the Washington Navy Yard on September 16, 2003, several people immediately called 9-1-1 to report the location of the shooter. However, police and first responders were delayed because they did not know the location of the building, did not have key cards to enter, and could not access the interior CCTV surveillance that would have helped them assess the situation. Careful planning can expedite the resolution of an emergency and reduce inaccurate media speculation about an event.

Regularly update and test crisis management plans, and continue training.

On September 19, 2014 an intruder jumped the fence on the Pennsylvania Avenue side of the White House and entered through the North Portico door. Although protocols call for an officer to stand outside of that door, no one was there. The intruder later was captured, but the situation points to the need for everyone to understand and strictly follow their organization's security policies, procedures and guidelines. Be sure everyone knows what to do in the event of an emergency.

Follow best practices and keep the post-crisis recovery in mind.

Recent confrontations between police and citizens in New York City and Ferguson, Missouri highlight both the value of technology and the need for all law enforcement agencies to review 'use of force' practices. In any crisis situation, it is important to document to the extent possible eyewitness reports, when and why decisions were made, and details of investigative actions.

Learn from your experiences and the actions of others in crisis management.

It's easy to identify mistakes and poor decisions in the aftermath of a crisis situation, but is equally important to consider the appropriate actions – those who successfully diffused a confrontation, prevented property damage and injuries, or saved lives. Incidents will occur in every organization; the goal is to prevent them from escalating to crises.

Employee Selection and Screening

JESSE BERGER

Unsurprisingly, the threats of cyber security (#1) and workplace violence (#3) remain uppermost for organizations polled in the most recent "Top Security Threats and Management Issues Facing Corporate America" survey. While there are a multitude of ways to protect your organization from these security challenges in 2015, a comprehensive employment screening and selection program, the #4 top security concern, remains a critical first step.

Addressing Workplace Violence

Workplace violence remains a growing concern for employers in recent years. In maintaining a safe workplace, an employment screening program can help identify potentially harmful, dangerous or violent individuals from ever entering your employee pool in the first place.

The most commonly considered employment screening tool is a comprehensive criminal background check, which can identify the potential for violent patterns of behavior. A candidate with a long list of violent crimes, such as assault or battery, might not be an ideal employee for most employers.

Another tool for employers is a reference check, which can help reveal undesirable patterns of behavior in candidates. Detailed reference checks can uncover a termination from a previous job due to a physical altercation or a repeated history of acting out or becoming argumentative with peers or upper management. These types of behavioral issues can sometimes be prevented from happening at your business by conducting reference checks so you know exactly who you are hiring.

Reducing Internal Data Breaches

Similarly, a comprehensive employment screening plan can help weed out individuals who have been investigated for cyber crimes or may have a propensity to engage in a potential data breach. Employment screening can help reduce the risk of internal data breaches in virtually every industry, but for those operating in a highly regulated field, such as financial services, a screening program is imperative.

In addition to running background or reference checks as mentioned above, a civil investigation can help identify potential character concerns for new applicants. Perhaps an applicant has a history of civil charges or history of theft. You may also consider launching a digital investigation to comb social networks and media sources for any undesirable patterns of behavior or insight into an applicant's character.

Furthermore, a psychometric assessment can shed light on a potential employee's character. If a person appears to have questionable integrity or could be interpreted as untrustworthy, it may be cause for concern.

While employment screening programs can be time and labor intensive, the list of reasons and benefits to engage in a proper screening process far outweigh the costs. Employment screening can help prevent loss of property and theft, and keep your employees safe from a potentially violent or deceptive individual.

Security incidents like a workplace violence situation or even an internal data breach remain two top concerns among security industry professionals, and with good reason. While it is impossible to prevent every potential risk or security challenge from arising, a thorough employment screening process will help reduce the risk of an incident from occurring in the first place. Organizations are only as good as the people they employ, and a comprehensive screening process will help ensure the highest caliber workforce.

Jesse Berger
is the Vice President of Pinkerton's Employment Screening Division, where he oversees all functions and operations of the domestic market. Berger has 20 years of business ownership and progressive management experience. In 2010, Berger sold his company, Navicus, to Pinkerton. Berger was CEO and Chairman of Navicus, a national provider of employment screening and talent management software services. Under his leadership, revenue more than quadrupled and the company grew rapidly from a small regional operation to a national player serving organizations with as many as 100,000 employees. Navicus was recognized by Inc. magazine as one of the fastest growing companies in America for four consecutive years. Berger was an integral part in building a company with a strong reputation which was recognized as a leading innovator in integrated talent management solutions and electronic employee life cycle transaction management.

Berger received his Juris Doctorate from the Shepard Broad Law Center at Nova Southeastern University and graduated with a BS in Finance from The American University in Washington, DC.

Cyber Crime

ROBERT MAVRONICOLAS

Robert Mavronicolas is a winner of the ASIS Foundation's 2014 Student Writing Competition.

He is a final-year student at the University of Portsmouth's Institute of Criminal Justice Studies in the United Kingdom and currently studying towards a Master's degree in Security Management. Born and raised in South Africa, Robert emigrated to the UK at the start of the financial depression where he comfortably settled in the private security work sector. Having a background in education and training, he currently works in London as a security consultant and operations manager where he brings the same enthusiasm and energy to his discipline as he does outside of work in his academic studies and family life. He also holds a BA (Hons) degree from the University of Cape Town as well as a PgCert in Security Management from Loughborough University.

When it comes to top security threats and management issues that will have the greatest impact on corporate industry and continue to challenge the security landscape well into the foreseeable future, cybercrime consistently ranks at the top of the charts.

With new technology come new risks, and reading the security landscape requires security professionals to keep their ears to the ground. The most recent trends, identified by the Freedonia Group industry report and discussed by Securitas USA experts in 2014, point towards white collar crime – such as embezzlement, industrial espionage and computer crimes. The experts agree that this is one of the biggest reasons for the sudden market increase for security consulting.

However, it is cybercrime which is crippling businesses and costing the most in lost revenue. PwC estimates that cybercrime is costing the global economy $445 billion a year. But just in 2015 alone, as we have more recently become aware, cybercrime is also reaching the upper echelons of national security. South Africa's intelligence community is reeling from the news of the "spy cables" leaks. But South Africa is not alone in protecting its cyberterritory. The British Prime Minister, David Cameron, in a January 2015 public address, pledged to introduce legislation allowing eavesdropping on suspected terrorist communications. This is subject to Home Secretary approval and a Conservative Party win in the next general election.

The unpredictability of the changing security landscape, particularly when it comes to cybercrime, is what forces security experts to expect the unexpected. By developing security strategies which will enable security professionals and companies alike to prepare for the unpredictability of these security threats, lessons can crucially be shared and hopefully also foster new ideas in driving forward successful security management.

Key recommendations may include:

Updating security policies.
Simply because an organization has set security policies in place does not necessarily make those policies fit for their intended purpose. Since the nature of each type of security threat is different from one another, security risk experts need to modify the use of the existing security risk templates in order to increase their chances of being able to mitigate the identified threats.

Effectively mitigating network breaches and system vulnerabilities.
Security teams can do this by continuously upgrading their anti-virus, anti-span, anti-spyware and anti-phishing software. In addition, by creating early warning signals, cyber security managers can predict the approach of a critical threshold. In the process of doing so, business organizations and their security management teams can reduce attack risk and drive the related critical threshold to a much higher point.

Lastly, successful security management strategy ideally means ensuring every employee within an organization is on board. Only then can security experts be better prepared for the unexpected.

The Importance of the Hiring Process

AUSTIN BHARADWAJA

Adequate employee selection and screening is vital to any organization. A former manager and mentor of mine once told me, "Austin, it all starts with the hiring." As a security professional involved heavily in the screening and selection of new candidates, I know this reasoning to be fact.

As security professionals, we need to strive for the most stringent hiring practices. This will help to bolster the image of our industry and succeed in what always should be our #1 goal: protecting our client's people, property and assets. When we hire a security officer, in many cases, we are also hiring an individual who will have the keys to our customer's facility. We want to ensure this individual is of sound character and mind and exhibits a high degree of professionalism.

A top notch hiring process should always begin with a formal face-to-face interview. On the spot hiring of security officers/guards is all too common in our industry. When this occurs, it eliminates the value that time can have on objective reasoning and allows our emotions to make hiring decisions. Candidates should always be administered a complete drug test and be subjected to a thorough background investigation. Applications should examine all pertinent aspects of the individual's character such as work history, references, military history, criminal history, credit history, etc. One negative aspect of a person's history should also not be a deciding factor in hiring; a 'big picture' concept of an applicant should always be applied. Most active shooter incidents are conducted by individuals with no prior arrests or convictions for violent crimes. Essentially, we should hesitate to jump to conclusions about an individual, despite what the history might state on paper and strive to focus on the complete package of the applicant.

These reasons are also why psychological testing is typically conducted on applicants, especially those guarding top secret installations and those required to carry firearms. Additional screening may also be helpful for armed security officers.

I have heard some managers state, "We are only as good as the people who report to us." I could not disagree more. Your impact should be more profound than that. You are as good as the people who you choose to recruit, under the circumstances in which you choose to recruit them, utilizing the resources you and your organization choose to invest in the screening and selection process of candidates. Therefore, you as security professionals involved in hiring can make the difference with how our industry is viewed and, more importantly, the organization you work so strenuously to successfully represent. You can make the difference.

Austin Bharadwaja is a winner of the ASIS Foundation's 2014 Student Writing Competition.

He has been employed by a large security services provider since 2011. He is currently a relationship manager for the company's Northern Nevada branch, and has served in this capacity for the past three years. Prior to his current position, he worked as a security officer in a healthcare facility. Before entering the security profession, he served in the U.S. Army Reserves from 2007-2011 while attending school at Montana State University, where he majored in Political Science. He also participated in the school's Army ROTC program where he utilized their scholarship opportunities to finance his education. Austin is currently a member of the ASIS International Northern Nevada Chapter. Additionally, he sits on the Northern Nevada Security Directors Committee. He has over six years of management experience and is responsible for managing security operations within his branch, including the screening, selection and hiring of all new employees. Austin is currently a student in the University of Nevada, Reno's Executive MBA program with a projected August 2015 graduation.

A Valuable Partner in Security

As an industry leader, we have firsthand experience with worldwide security trends and have developed protocols for a variety of scenarios. A company of our size offers a comprehensive approach — we can provide a full range of services that leverage our officers and technology for a complete and flexible security plan to meet all of your security requirements. Securitas USA is committed to forming a mutually beneficial partnership and fully understanding its clients' security needs in order to provide the highest possible level of service.

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

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