TOP SECURITY THREATS

AND MANAGEMENT ISSUES FACING CORPORATE AMERICA

2019 SURVEY OF FORTUNE 1000 COMPANIES


SECURITAS

Content

A MESSAGE FROM

Bill Barthelemy

CHIEF OPERATING OFFICER – SECURITAS SECURITY SERVICES USA, INC.

Securitas Security Services USA, Inc. has completed its 2019 "Top Security Threats and Management Issues Facing Corporate America" survey. We are pleased to publish the findings of the survey in this report.

BIO

William Barthelemy
Chief Operating Officer
Securitas Security Services USA, Inc.

Bill brings over 30 years of industry experience to the organization. With a Criminology Degree from Indiana University of PA, Bill began his career as an Investigator and transitioned into the Security Division after two years. Over the years he has served clients, employees and the company across a wide range of Securitas roles, including Scheduling Manager, Operations Manager, Branch Manager, Regional Operations Director and Region President. Bill brings an avid client service focus to the management team. He is an active member of the American Society of Industrial Security (ASIS), as well as the National Association of Chiefs of Police.

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 our respondents who participated, generating an excellent response rate from security executives in 32 states, Canada and Mexico.

YOUR INPUT IS CRITICAL TO OUR REPORT AND HAS IDENTIFIED THE TOP FIVE SECURITY THREATS FOR 2018 AS FOLLOWS:

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

TOP FIVE SECURITY THREATS FOR 2018

1. CYBER/COMMUNICATIONS SECURITY: INTERNET/INTRANET SECURITY
2. ACTIVE SHOOTER OR ACTIVE ASSAULT/ ASSAILANT THREATS
3. WORKPLACE VIOLENCE PREVENTION/RESPONSE
4. BUSINESS CONTINUITY PLANNING/ ORGANIZATIONAL RESILIENCE
5. CYBER/COMMUNICATIONS SECURITY: MOBILE TECHNOLOGY

THE TOP THREE SECURITY MANAGEMENT CHALLENGES THAT WERE IDENTIFIED ARE:

1. Security Staffing Effectiveness: Training Effectiveness/Methods
2. Security Staffing Effectiveness: Adequate Staffing Levels
3. Promoting Employee Awareness

As you will read, the survey results also outline the top security threats in various vertical markets as reported by security executives. Additionally, information is provided 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:

Randy Atlas, Ph.D., CPP, FAIA
Atlas Safety & Security Design, Inc.
"Designing Safe Schools in Dangerous Times"

Konrad Motyka
Executive Director for Campus Safety and Emergency Management
Mercy College
"Stopping Active Shooters: Bystanders Cannot Merely Stand By"

Dwayne Gulsby, CPP
Central Atlantic Region President
Securitas Security Services USA, Inc.
"Active Shooter Threats: Taking Action Before the Violence Starts"

Michael Ainslie, CPP, PSP, PCI
Head of Global Security
Allegis Group, Inc.
"Hostile Terminations: Blending Security with Empathy"

Sandra Cowie, CPP
Director of Global Security & Business Continuity
Principal Financial Group
"Recovery from an Active Shooter Event: A Business Continuity Perspective"

William J. Powers III, CPP
Director of Facilities
The Sterling and Francine Clark Art Institute
"Business Continuity Plan: Beyond the Basics"

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 particular security objectives.

A MESSAGE FROM

Tony Sabatino

EXECUTIVE VICE PRESIDENT – SECURITAS SECURITY SERVICES USA, INC.

We are thankful to our clients and colleagues for participating in our biennial Securitas Top Security Threats Survey.

BIO

TONY SABATINO
Executive Vice President
Securitas North American Division

Tony joined the company in 1991 as a Management Trainee after graduating from Wagner College with a degree in Economics and Business Administration.

He has held increasingly responsible positions within the company, including Business Development Manager, Branch Manager, Vice President-Operations, Area Vice President and Region President-Pacific Region. His career has provided the opportunity to work in several locations across the U.S., including New Jersey, Texas, New York, and California, each of which has given him a different perspective on current security concerns.

Tony has significant experience securing critical infrastructure sites for government and commercial clients including petro-chemical, hospital, maritime/port, aviation, utility (including electric transmission, water, gas, and solar), and mass gathering events.

By maintaining close ties with clients and employees in the front lines, Tony stays abreast of threats, emerging trends, and related concerns.

WE ALSO APPRECIATE the contributions of our guest editorial writers who shared their thoughts regarding current risks, threats or issues of concern to them and their organizations, which include:

- Active shooter threats and response
- Hostile employee terminations
- Business continuity planning
- Security measures at educational institutions

It is no surprise that "Cyber/Communications Security" has retained its #1 ranking from our four previous surveys, as well as "Workplace Violence Prevention/ Response" continuing to be the #2 threat. Although many workplace violence incidents, such as active assaults, are relatively low-probability, they are consistently high-impact. Planning for such incidents must be systematic and thoroughly reflect the most

current best practices. It is also important to note that, of the 27 identified threat categories, 21 can be caused or committed by insiders—an even higher count than our previous survey.

NOTABLE OBSERVATIONS OF THE SURVEY RESULTS CONCERNING MANAGEMENT CHALLENGES INCLUDE THE FOLLOWING:

- "Security Staffing Effectiveness: Adequate Staffing Levels" rose from 9th to 2nd place and "Security Officer Turnover/Retention" moved from 11th to 4th place.
- "Budget/Maximizing ROI" moved from 8th to 4th place, reflecting increasing pressure to justify or contain security program costs.
- Conversely, two challenges moved significantly downward. "Implementing Best Practices/Standards/Key Performance Indicators" dropped from 3rd to 12th place, and "Staying Current with Technological Advances" dropped from 5th to 10th place.

As security risks continue to change and new threats emerge, we hope you agree that the survey and analysis of the data can be very useful tools to assist your organization in developing security prevention, detection, response and/or mitigation strategies and procedures. Additional available resources include the standards and guidelines developed by ASIS International, which is accredited by the American National Standards Institute (ANSI) for this purpose.

THE ASIS/ANSI ACCREDITED STANDARDS INCLUDE:

- Workplace Violence Prevention and Intervention
- Risk Assessment
- Physical Asset Protection
- Supply Chain Risk Management

Securitas USA recognizes the many challenges faced by our clients and the security community at-large in developing programs designed to mitigate the threats identified in this report, as well as other threats unique to each organization. We stand prepared to collaboratively work with you in assisting with these endeavors.

Introduction

Securitas Security Services USA, Inc. has completed the "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 Fortune 1000 security managers and directors, 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 2018–2019 survey drew 142 responses, yielding a 12% response rate.

TODAY'S THREAT ENVIRONMENT

The study identified the challenges of greatest concern to corporate security directors in rank order (See Figure 1). The threat of Cyber/Communications Security: Internet/Intranet Security remains the greatest security concern.

The newly worded Active Shooter or Active Assault/Assailant Threats (formerly known as Active Shooter Threats) moves up to 2nd place after a 3rd place ranking in 2016. Workplace Violence Prevention/Response moves down to 3rd place after a 2nd place ranking in 2016, while Business Continuity Planning/ Organizational Resilience maintains its 4th place ranking.

Cyber/Communications Security: Mobile Technology continues in 5th place, while Employee Selection/Screening/ Rescreening (including Insider Threats) moves up to the 6th spot from the 7th spot in 2016. Crisis Management and Response: Natural Disasters moves one spot down to 7th place after holding 6th place in 2016. Property Crime (e.g., External Theft, Vandalism) moves up one spot to 8th place after placing 9th in 2016. Litigation: Inadequate Security is 9th after ranking 13th overall in 2016, while Crisis Management Response: Domestic Terrorism/Lone Wolf Attacks drops down two spots to 10th place after being ranked 8th in 2016.

PROFESSIONAL MANAGEMENT ISSUES

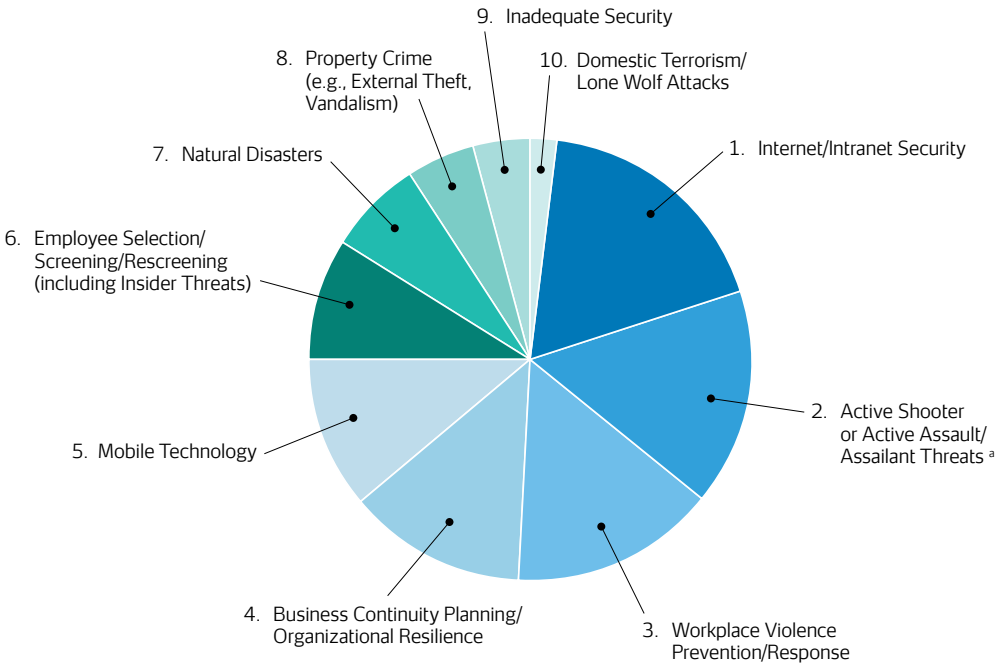
A significant portion of the Securitas USA survey is devoted to identifying key management issues, as well as operational, staffing and budgetary issues facing corporate security executives. Figure 2 shows the operational issues of greatest concern in 2018.

FUNDING TRENDS

Over the next three to five years, the funding outlook in Figure 3 for corporate security programs shows that 36% of security managers are expecting an increase in annual funding compared to 34% in 2016. It further shows that 51% of security managers are expecting budgets to remain the same in 2019 compared to 50% in 2016.

FIGURE 1

2018 TOP SECURITY THREATS



a. Prior to 2018, this attribute was known generally as: Active Shooter Threats

FIGURE 2

MANAGEMENT CHALLENGES/ OPERATIONAL ISSUES OF GREATEST CONCERN

1	Security Staffing Effectiveness: Training Effectiveness/Methods
2	Security Staffing Effectiveness: Adequate Staffing Levels
3	Promoting Employee Awareness
4 (TIE)	Budget/Maximizing Return on Investment
4 (TIE)	Security Staffing Effectiveness: Security Officer Turnover/Retention
6	Security Staffing Effectiveness: Maturity of Workforce

FIGURE 3

2018 AND 2016 FUNDING TRENDS

Security managers expecting an increase in funding

2018 **36%**

2016 **34%**

Security managers expecting budgets to remain the same

2018 **51%**

2016 **50%**

Top Security Threats

To assess security professionals' relative level of concern, the Security Threats survey presented a list of 27 potential security threats developed by Securitas USA. These were refined from the 2016 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 they feel will be most important to their company during the next 12 months." The 2018 rankings are shown in Figure 4.

FIGURE 4

2018 RANK	TOP SECURITY THREATS - RANKING	AVERAGE IMPORTANCE SCORE
1	Cyber/Communications Security: Internet/Intranet Security	4.39
2	Active Shooter or Active Assault/Assailant Threats [a]	4.23
3	Workplace Violence Prevention/Response	4.13
4	Business Continuity Planning/Organizational Resilience	4.03
5	Cyber/Communications Security: Mobile Technology	3.94
6	Employee Selection/Screening/Rescreening (including Insider Threats)	3.87
7	Crisis Management and Response: Natural Disasters	3.71
8	Property Crime (e.g., External Theft, Vandalism)	3.68
9	Litigation: Inadequate Security	3.61
10	Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks	3.57
11	Social Media [b]	3.49
12	Identity Theft	3.34
13	General Employee Theft	3.32
14	Unethical Business Conduct	3.31
15	Litigation: Negligent Hiring/Supervision	3.23
16	Executive/Employee Protection (including Travel Security/Airline Safety)	3.18
17	Organizational Espionage/Theft of Trade Secrets	3.14
18	Substance Abuse (Drugs/Alcohol in the Workplace)	3.11
19	Intellectual Property/Brand Protection/Product Counterfeiting	3.08
20	Bombings/IEDs/Bomb Threats	3.05
21	Fraud/White-Collar Crime	3.04
22	Crisis Management and Response: Political Unrest/Regional Instability/Public Demonstrations/Protests	2.92
23	Global Supply Chain Security	2.89
24	Insurance/Workers' Compensation Fraud	2.77
25	Crisis Management and Response: International Terrorism	2.72
26	Labor Unrest	2.55
27	Crisis Management and Response: Kidnapping/Extortion	2.48

a. Prior to 2018, this attribute was known generally as: Active Shooter Threats
b. A new threat added to the 2018 survey

Cyber/Communications Security: Internet/Intranet Security is the foremost concern of corporate security directors, reflecting the country's high reliance on technology; this position has been held since 2010. Active Shooter Threats moves up to 2nd place after a 3rd place ranking in 2016. Workplace Violence moves down to the 3rd spot after placing 2nd in 2016. Business Continuity Planning /Organizational Resilience maintains the 4th spot, while Cyber/Communications Security: Mobile Technology maintains its 5th place ranking.

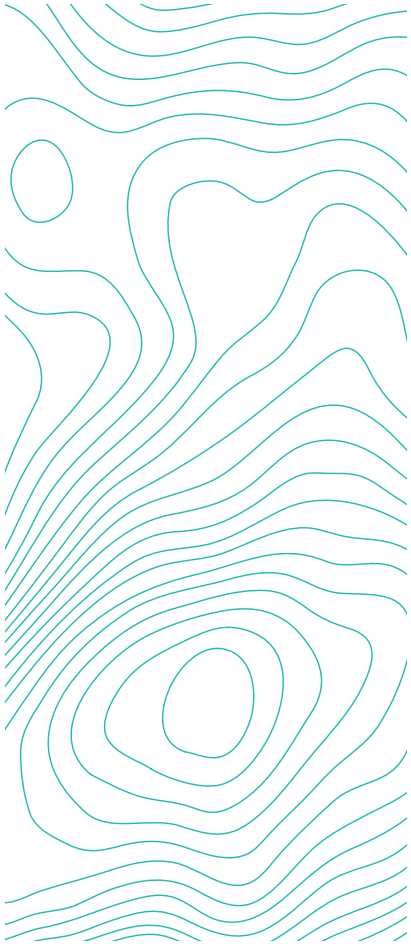


FIGURE 5

TOP SECURITY THREATS: RANKING 2001 – 2018

SECURITY THREATS	2001	2002	2003	2008	2010	2012	2014	2016	2018
Cyber/Communications Security: Internet/Intranet Security	2	4	3	3	1	1	1	1	1
Active Shooter or Active Assault/Assailant Threats [a]	NA	NA	NA	NA	NA	NA	NA	3	2
Workplace Violence Prevention/Response	1	1	1	1	2	2	3	2	3
Business Continuity Planning/Organizational Resilience	5	2	2	2	3	3	2	4	4
Cyber/Communications Security: Mobile Technology	NA	NA	NA	NA	NA	NA	NA	5	5
Employee Selection/Screening/Rescreening (including Insider Threats)	3	5	5	4	4	4	4	7	6
Crisis Management and Response: Natural Disasters	NA	NA	NA	NA	NA	NA	NA	6	7
Property Crime (e.g., External Theft, Vandalism)	10	9	12 (tie)	5 (tie)	7	5	6	9	8
Litigation: Inadequate Security	13	11 (tie)	18	19 (tie)	16	9	13	13	9
Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks	17	3	4	7	12	15	8	8	10
Social Media [b]	NA	NA	NA	NA	NA	NA	NA	NA	11
Identity Theft	16	14 (tie)	10	12	11	10	9	12	12
General Employee Theft	6	8	7	5 (tie)	8	6	7	11	13
Unethical Business Conduct	9	7	8	9	5	8	10	14	14
Litigation: Negligent Hiring/Supervision	14	18	20	25	23	17	15 (tie)	16	15
Executive/Employee Protection (including Travel Security/Airline Safety)	NA	NA	NA	22 (tie)	13	18	21	15	16
Organizational Espionage/Theft of Trade Secrets	12	19	16	15 (tie)	15	16	17	19	17
Substance Abuse (Drugs/Alcohol in the Workplace)	8	10	9	19 (tie)	17	13	15 (tie)	17	18
Intellectual Property/Brand Protection/Product Counterfeiting	NA	NA	NA	21	14	11	19	20	19
Bombings/IEDs/Bomb Threats	NA	NA	NA	14	24	19	24	21	20
Fraud/White-Collar Crime	4	6	6	8	10	12	14	18	21
Crisis Management and Response: Political Unrest/Regional Instability/ Public Demonstrations/Protests	20	14 (tie)	11	10	6	7	12	22	22
Global Supply Chain Security	18	22	21	27 (tie)	22	20	20	25	23
Insurance/Workers' Compensation Fraud	15	17	17	26	25	21	22	26	24
Crisis Management and Response: International Terrorism	NA	NA	NA	NA	NA	NA	23	27	25
Labor Unrest	NA	NA	NA	29	26	23	25	28	26
Crisis Management and Response: Kidnapping/Extortion	19	20	19	33	27	24	26	29	27

a. Prior to 2018, this attribute was known generally as: Active Shooter Threats
b. A new threat added to the 2018 survey

Threat Rankings Within Market Sectors

Securitas USA also sought to determine if security executives in various markets placed different emphasis on certain threats. The survey responses for the seven largest aggregate market 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/Logistics (31%); Finance and Insurance (11%); Healthcare and Social Assistance/Biotech and Pharmaceuticals (9%); High Tech, Commercial and Residential Real Estate and Utilities/Telecommunications (7%); and Education (6%).

MANUFACTURING/ LOGISTICS

The top concerns among security directors at Manufacturing/Logistics companies (a newly combined market) in 2018 are Internet/Intranet Security in 1st place, with the newly worded Active Shooter or Active Assault/Assailant Threats in 2nd place. Workplace Violence Prevention/ Response remains in 3rd place, while Business Continuity Planning/Organizational Resilience is in 4th. Mobile Technology rounds out the top five, with Employee Selection/Screening/Rescreening (including Insider Threats) in 6th place.

FINANCE AND INSURANCE

The top security threat in the Finance and Insurance market is Business Continuity Planning/Organizational Resilience, which moved to the top threat after placing 6th in 2016. Employee Selection/Screening/ Rescreening (including Insider Threats) is in 2nd place after an 8th place ranking in 2016, followed by a two-way tie for 3rd place with Internet/Intranet Security and Workplace Violence Prevention/Response; both categories were ranked 1st and 2nd, respectively, in 2016. The newly worded Active Shooter or Active Assault/Assailant Threats maintains 5th place and is joined by Natural Disasters in a two-way tie; Natural Disasters was previously ranked 13th in 2016.

FIGURE 6

TOP THREATS BY MARKET – MANUFACTURING/LOGISTICS

TOTAL RESPONDENTS RANK 2018	RANK WITHIN MARKET 2018	SECURITY THREATS	RANK WITHIN INDUSTRY 2016
1	1	Cyber/Communications Security: Internet/Intranet Security	NA
2	2	Active Shooter or Active Assault/Assailant Threats [a]	NA
3	3	Workplace Violence Prevention/Response	NA
4	4	Business Continuity Planning/Organizational Resilience	NA
5	5	Cyber/Communications Security: Mobile Technology	NA
6	6	Employee Selection/Screening/Rescreening (including Insider Threats)	NA
8	7 (tie)	Property Crime (e.g., External Theft, Vandalism)	NA
13	7 (tie)	General Employee Theft	NA
17	9	Organizational Espionage/Theft of Trade Secrets	NA
9	10 (tie)	Litigation: Inadequate Security	14
16	10 (tie)	Executive/Employee Protection (including Travel Security/Airline Safety)	NA

a. Prior to 2018, this attribute was known generally as: Active Shooter Threats

FIGURE 7

TOP THREATS BY MARKET – FINANCE AND INSURANCE

TOTAL RESPONDENTS RANK 2018	RANK WITHIN MARKET 2018	SECURITY THREATS	RANK WITHIN INDUSTRY 2016
4	1	Business Continuity Planning/Organizational Resilience	6
6	2	Employee Selection/Screening/Rescreening (including Insider Threats)	8
1	3 (tie)	Cyber/Communications Security: Internet/Intranet Security	1
3	3 (tie)	Workplace Violence Prevention/Response	2
2	5 (tie)	Active Shooter or Active Assault/Assailant Threats [a]	5
7	5 (tie)	Crisis Management and Response: Natural Disasters	13
5	7 (tie)	Cyber/Communications Security: Mobile Technology	3 (tie)
12	7 (tie)	Identity Theft	9
9	9 (tie)	Litigation: Inadequate Security	14
11	9 (tie)	Social Media [b]	3 (tie)

a. Prior to 2018, this attribute was known generally as: Active Shooter Threats
b. A new threat added to the 2018 survey

HEALTH CARE AND SOCIAL ASSISTANCE/BIOTECH AND PHARMACEUTICALS

The top concerns among security directors at Healthcare and Social Assistance/Biotech and Pharmaceutical companies (a newly combined market) are Internet/Intranet Security in 1st place, followed by Workplace Violence Prevention/Response in 2nd place. Business Continuity Planning/Organizational Resilience and Employee Selection/Screening/Rescreening (including Insider Threats) are tied for 3rd place, while Natural Disasters is ranked 5th.

FIGURE 8

TOP THREATS BY MARKET – HEALTHCARE AND SOCIAL ASSISTANCE/BIOTECH AND PHARMACEUTICALS

TOTAL RESPONDENTS RANK 2018	RANK WITHIN MARKET 2018	SECURITY THREATS	RANK WITHIN INDUSTRY 2016
1	1	Cyber/Communications Security: Internet/Intranet Security	NA
3	2	Workplace Violence Prevention/Response	NA
4	3 (tie)	Business Continuity Planning/Organizational Resilience	NA
6	3 (tie)	Employee Selection/Screening/Rescreening (including Insider Threats)	NA
7	5	Crisis Management and Response: Natural Disasters	NA
2	6	Active Shooter or Active Assault/Assailant Threats [a]	NA
5	7	Cyber/Communications Security: Mobile Technology	NA
11	8	Social Media [b]	NA
19	9	Intellectual Property/Brand Protection/Product Counterfeiting	NA
10	10 (tie)	Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks	NA
16	10 (tie)	Executive/Employee Protection (including Travel Security/Airline Safety)	NA

a. Prior to 2018, this attribute was known generally as: Active Shooter Threats
b. A new threat added to the 2018 survey

HIGH TECH

The top concerns among security directors at High Tech companies (a new market) are Internet/Intranet Security in 1st place, with Mobile Technology in 2nd place. The newly worded Active Shooter or Active Assault/Assailant and Threats and Workplace Violence Prevention/Response are tied for 3rd place, while Natural Disasters, Organizational Espionage/Theft of Trade Secrets and Intellectual Property/Brand Protection/Product Counterfeiting are tied for 5th place.

FIGURE 9

TOP THREATS BY MARKET – HIGH TECH

TOTAL RESPONDENTS RANK 2018	RANK WITHIN MARKET 2018	SECURITY THREATS	RANK WITHIN INDUSTRY 2016
1	1	Cyber/Communications Security: Internet/Intranet Security	NA
5	2	Cyber/Communications Security: Mobile Technology	NA
2	3 (tie)	Active Shooter or Active Assault/Assailant Threats [a]	NA
3	3 (tie)	Workplace Violence Prevention/Response	NA
7	5 (tie)	Crisis Management and Response: Natural Disasters	NA
17	5 (tie)	Organizational Espionage/Theft of Trade Secrets	NA
19	5 (tie)	Intellectual Property/Brand Protection/Product Counterfeiting	NA
4	8	Business Continuity Planning/Organizational Resilience	NA
6	9	Employee Selection/Screening/Rescreening (including Insider Threats)	NA
8	10 (tie)	Property Crime (e.g., External Theft, Vandalism)	NA
14	10 (tie)	Unethical Business Conduct	NA

a. Prior to 2018, this attribute was known generally as: Active Shooter Threats

COMMERCIAL AND RESIDENTIAL REAL ESTATE

In the Commercial Real Estate market, security directors propel Natural Disasters to a 1st place ranking after being tied for 5th place in 2016. The newly worded Active Shooter or Active Assault/Assailant Threats moves down one position to a 2nd place ranking. Internet/Intranet Security is in 3rd place, while Business Continuity Planning/Organizational Resilience, Property Crime (e.g., External Theft, Vandalism) and Inadequate Security are tied for 4th place.

FIGURE 10

TOP THREATS BY MARKET – COMMERCIAL AND RESIDENTIAL REAL ESTATE

TOTAL RESPONDENTS RANK 2018	RANK WITHIN MARKET 2018	SECURITY THREATS	RANK WITHIN INDUSTRY 2016
7	1	Crisis Management and Response: Natural Disasters	5 (tie)
2	2	Active Shooter or Active Assault/Assailant Threats [a]	1
1	3	Cyber/Communications Security: Internet/Intranet Security	3
4	4 (tie)	Business Continuity Planning/Organizational Resilience	2
8	4 (tie)	Property Crime (e.g., External Theft, Vandalism)	5 (tie)
9	4 (tie)	Litigation: Inadequate Security	9
6	7 (tie)	Employee Selection/Screening/Rescreening (including Insider Threats)	10 (tie)
12	7 (tie)	Identity Theft	16 (tie)
3	9 (tie)	Workplace Violence Prevention/Response	4
10	9 (tie)	Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks	5 (tie)

a. Prior to 2018, this attribute was known generally as: Active Shooter Threats

UTILITIES/ TELECOMMUNICATIONS

The top concerns among security directors at Utilities/ Communication companies (a newly combined market) are Internet/Intranet Security and the newly worded Active Shooter or Active Assault/Assailant Threats, which are tied for 1st place, while Business Continuity Planning/Organizational Resilience is ranked 3rd. Mobile Technology and Employee Selection Screening/Rescreening (including Insider Threats) are tied for 4th place, while Workplace Violence Prevention/ Response holds a 6th place ranking.

FIGURE 11

TOP THREATS BY MARKET – UTILITIES/TELECOMMUNICATIONS

TOTAL RESPONDENTS RANK 2018	RANK WITHIN MARKET 2018	SECURITY THREATS	RANK WITHIN INDUSTRY 2016
1	1 (tie)	Cyber/Communications Security: Internet/Intranet Security	NA
2	1 (tie)	Active Shooter or Active Assault/Assailant Threats [a]	NA
4	3	Business Continuity Planning/Organizational Resilience	NA
5	4 (tie)	Cyber/Communications Security: Mobile Technology	NA
6	4 (tie)	Employee Selection/Screening/Rescreening (including Insider Threats)	NA
3	6	Workplace Violence Prevention/Response	NA
11	7	Social Media [b]	NA
10	8 (tie)	Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks	NA
20	8 (tie)	Bombings/IEDs/Bomb Threats	NA
9	10	Litigation: Inadequate Security	NA

a. Prior to 2018, this attribute was known generally as: Active Shooter Threats
b. A new threat added to the 2018 survey

EDUCATION

In the Education market, the newly worded Active Shooter or Active Assault/Assailant Threats is ranked in 1st place after being tied for 2nd place in 2016. Property Crime moves to 2nd place after previously placing 5th and is joined by Domestic Terrorism/Lone Wolf Attacks, which was tied for 5th place in 2016. Internet/Intranet Security falls from 1st place and is joined in a four-way tie with Workplace Violence Prevention/Response, the newly added Social Media, and Bombings/IEDs/Bomb Threats for a 4th place ranking. Substance Abuse (Drugs/Alcohol in the Workplace) jumps from an 11th place ranking in 2016 to 8th place in 2018.

FIGURE 12

TOP THREATS BY MARKET – EDUCATION

TOTAL RESPONDENTS RANK 2018	RANK WITHIN MARKET 2018	SECURITY THREATS	RANK WITHIN INDUSTRY 2016
2	1	Active Shooter or Active Assault/Assailant Threats [a]	2 (tie)
8	2 (tie)	Property Crime (e.g., External Theft, Vandalism)	5 (tie)
10	2 (tie)	Crisis Management and Response: Domestic Terrorism/Lone Wolf Attacks	5 (tie)
1	4 (tie)	Cyber/Communications Security: Internet/Intranet Security	1
3	4 (tie)	Workplace Violence Prevention/Response	2 (tie)
11	4 (tie)	Social Media [b]	5 (tie)
20	4 (tie)	Bombings/IEDs/Bomb Threats	17 (tie)
18	8	Substance Abuse (Drugs/Alcohol in the Workplace)	11 (tie)
4	9 (tie)	Business Continuity Planning/Organizational Resilience	11 (tie)
7	9 (tie)	Crisis Management and Response: Natural Disasters	5 (tie)
9	9 (tie)	Litigation: Inadequate Security	17 (tie)

a. Prior to 2018, this attribute was known generally as: Active Shooter Threats
b. A new threat added to the 2018 survey

Security Management Challenges

A list of 17 security management topics was provided 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 graphically (Figure 13).

Maintaining its trend from 2016, Security Staffing Effectiveness: Training Effectiveness/Methods holds the top position for 2018 security management challenges. Security Staffing Effectiveness: Adequate Staffing Levels jumps to 2nd place after placing 9th in 2016. Promoting Employee Awareness moves one spot down to 3rd in 2016. Budget/Maximizing Return on Investment and Security Staffing Effectiveness: Security Officer Turnover/Retention are tied for 4th place after placing 8th and 11th, respectively, in 2016. Security Staffing Effectiveness: Maturity of Workforce is ranked 6th after a 10th place ranking in 2016, while Threat Assessments is ranked 7th after being tied for 5th place in 2016. The top security management challenges ranked 8th through 10th are: Security Staffing Effectiveness: Selection and Hiring Methods, Strategic Planning and Staying Current with Technological Advances.

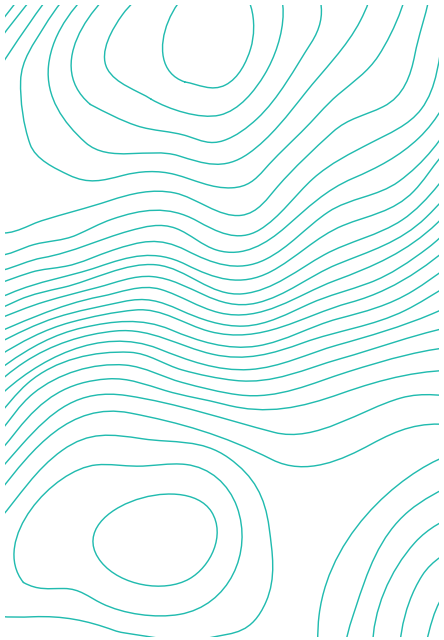


FIGURE 13

2018 RANK	MANAGEMENT CHALLENGES	AVERAGE IMPORTANCE SCORE
1	Security Staffing Effectiveness: Training Effectiveness/Methods	4.17
2	Security Staffing Effectiveness: Adequate Staffing Levels	4.09
3	Promoting Employee Awareness	4.02
4 (tie)	Budget/Maximizing Return on Investment	3.99
4 (tie)	Security Staffing Effectiveness: Security Officer Turnover/Retention	3.99
6	Security Staffing Effectiveness: Maturity of Workforce	3.96
7	Threat Assessments	3.94
8	Security Staffing Effectiveness: Selection and Hiring Methods	3.90
9	Strategic Planning	3.87
10	Staying Current with Technological Advances	3.85
11	Regulatory/Compliance Issues (State/Federal Legislation)	3.80
12	Implementing Best Practices/Standards/Key Performance Indicators	3.78
13	Additional Security Responsibilities (Aviation/Compliance/Ethics, etc.)	3.58
14	Career Development/Multiple Job Responsibilities	3.52
15	Security Staffing Effectiveness: Absenteeism	3.46
16	Managing Remote Security Operations	3.40
17	Global Supply Chain Decisions	2.77

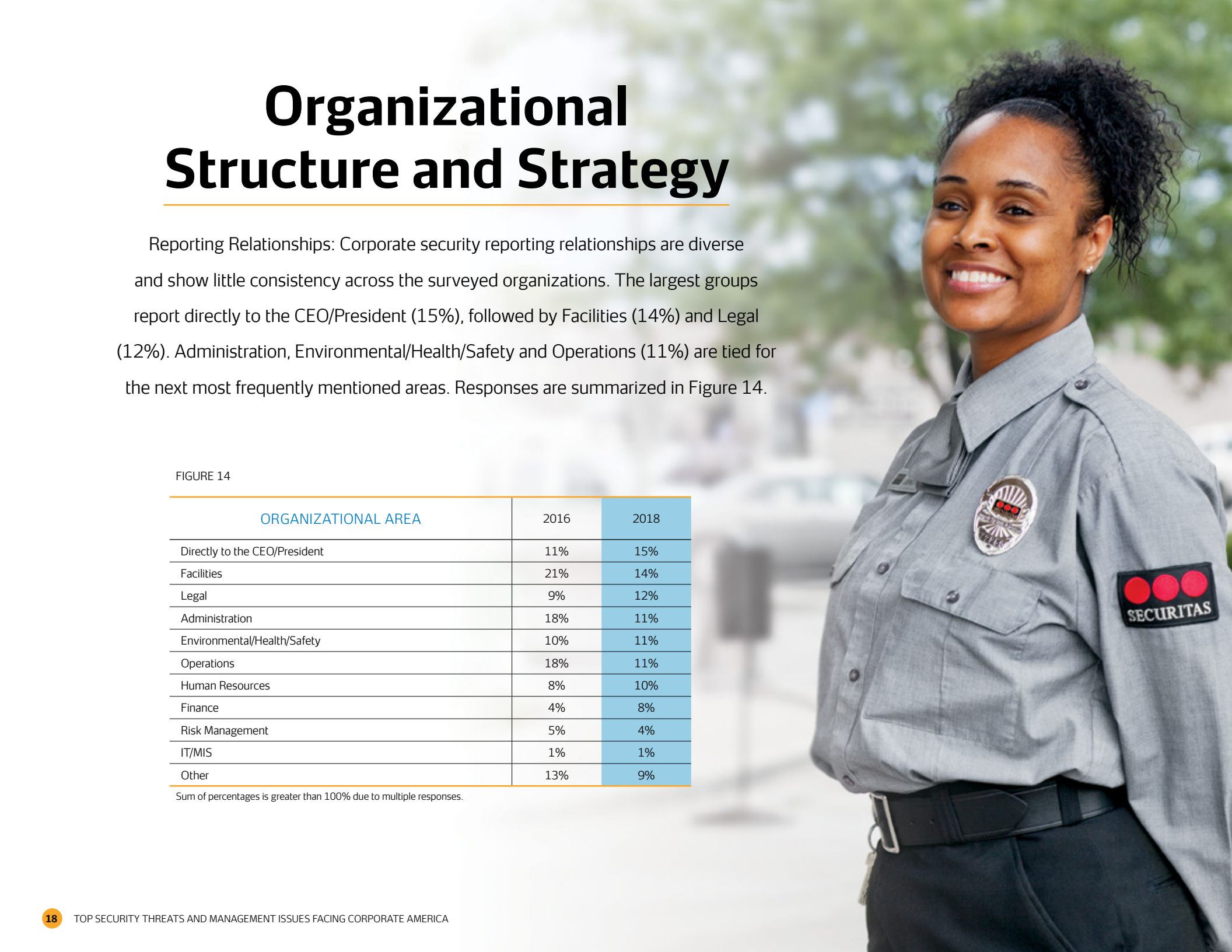
Organizational Structure and Strategy

Reporting Relationships: Corporate security reporting relationships are diverse and show little consistency across the surveyed organizations. The largest groups report directly to the CEO/President (15%), followed by Facilities (14%) and Legal (12%). Administration, Environmental/Health/Safety and Operations (11%) are tied for the next most frequently mentioned areas. Responses are summarized in Figure 14.

FIGURE 14

ORGANIZATIONAL AREA	2016	2018
Directly to the CEO/President	11%	15%
Facilities	21%	14%
Legal	9%	12%
Administration	18%	11%
Environmental/Health/Safety	10%	11%
Operations	18%	11%
Human Resources	8%	10%
Finance	4%	8%
Risk Management	5%	4%
IT/MIS	1%	1%
Other	13%	9%

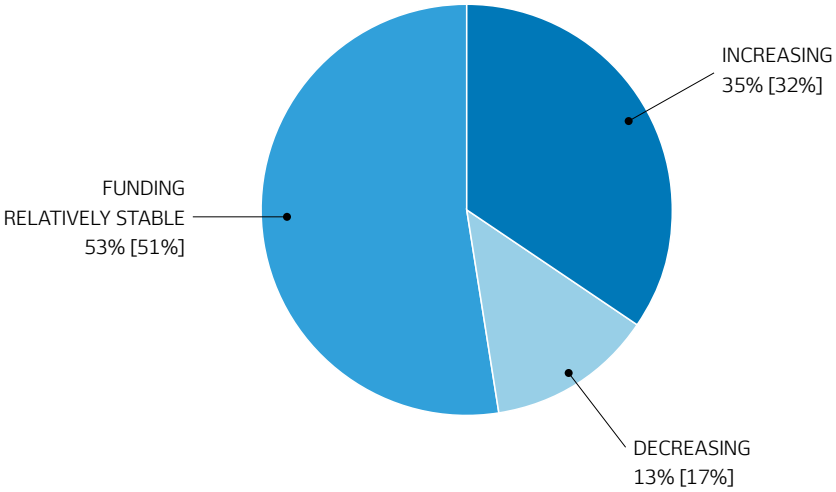
Sum of percentages is greater than 100% due to multiple responses.



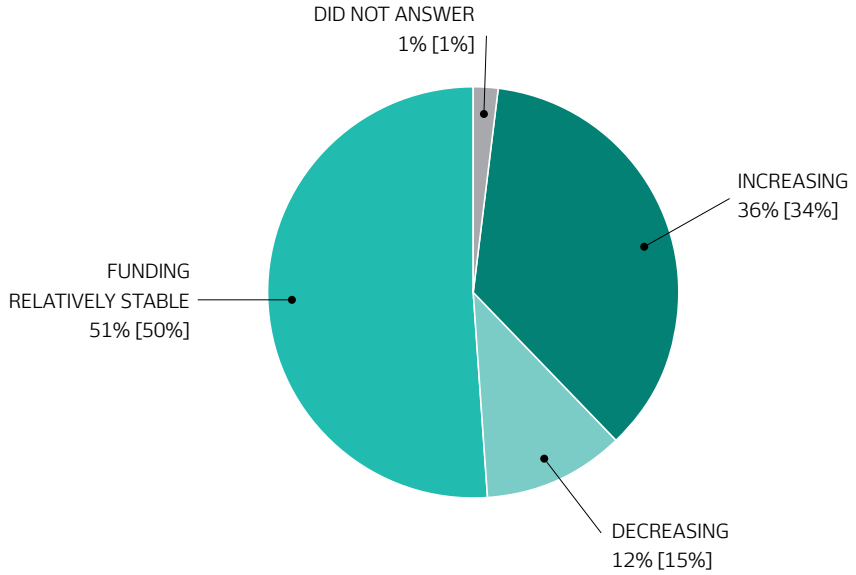
Budget and Funding

Funding Trends: The funding outlook for corporate security programs over the next three to five years reflects that 36% of security managers are expecting an increase in funding in 2019. The percentage of security managers expecting budgets to remain the same is 51%, while the percentage of managers anticipating decreased funding is 12%.

SECURITY FUNDING: PAST 3 – 5 YEARS



SECURITY FUNDING: NEXT 3 – 5 YEARS



NOTE: *The percentages in the [brackets] are 2016 percentages.*

Methodology and Sample Distribution

SURVEY METHODOLOGY

For this most current "Top Security Threats and Management Challenges" 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 sent via mail and email to 1,187 security directors and other executives identified as having oversight of the corporate security function at these organizations. The survey questionnaire was distributed in October 2018. Respondents were asked to complete and return the surveys via mail, fax or e-mail. Respondents were offered the option of completing the survey online via a link and password provided in the cover letter. Results were compiled and analyzed in January 2019. This report shows the responses of 142 returned surveys, which represented a 12% 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.

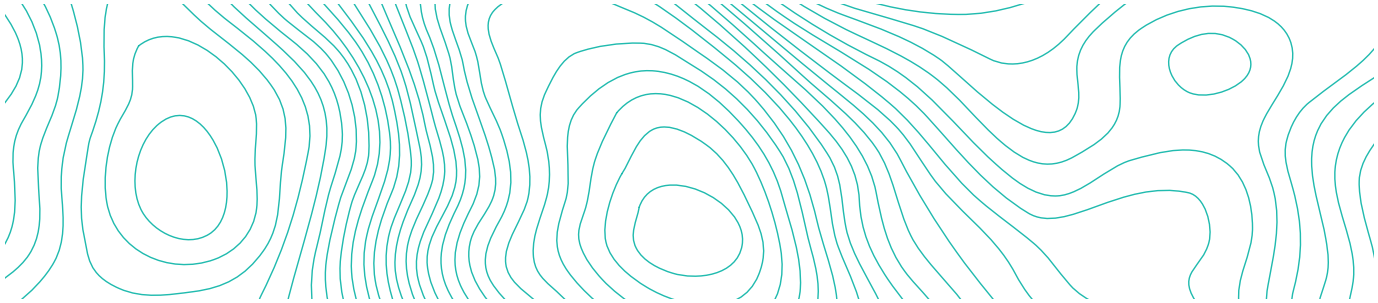
RESPONDENT DISTRIBUTION

Thirteen specific markets were represented in the returned surveys; smaller groups were aggregated into broader categories to permit analysis of the results by market sector. Segmentation of the total sample should be considered in the context of the Fortune 1000 companies in 2018, which does not represent every market and was more densely populated by those most heavily weighted here. Respondents selected their primary market affiliation from a predefined list as shown.

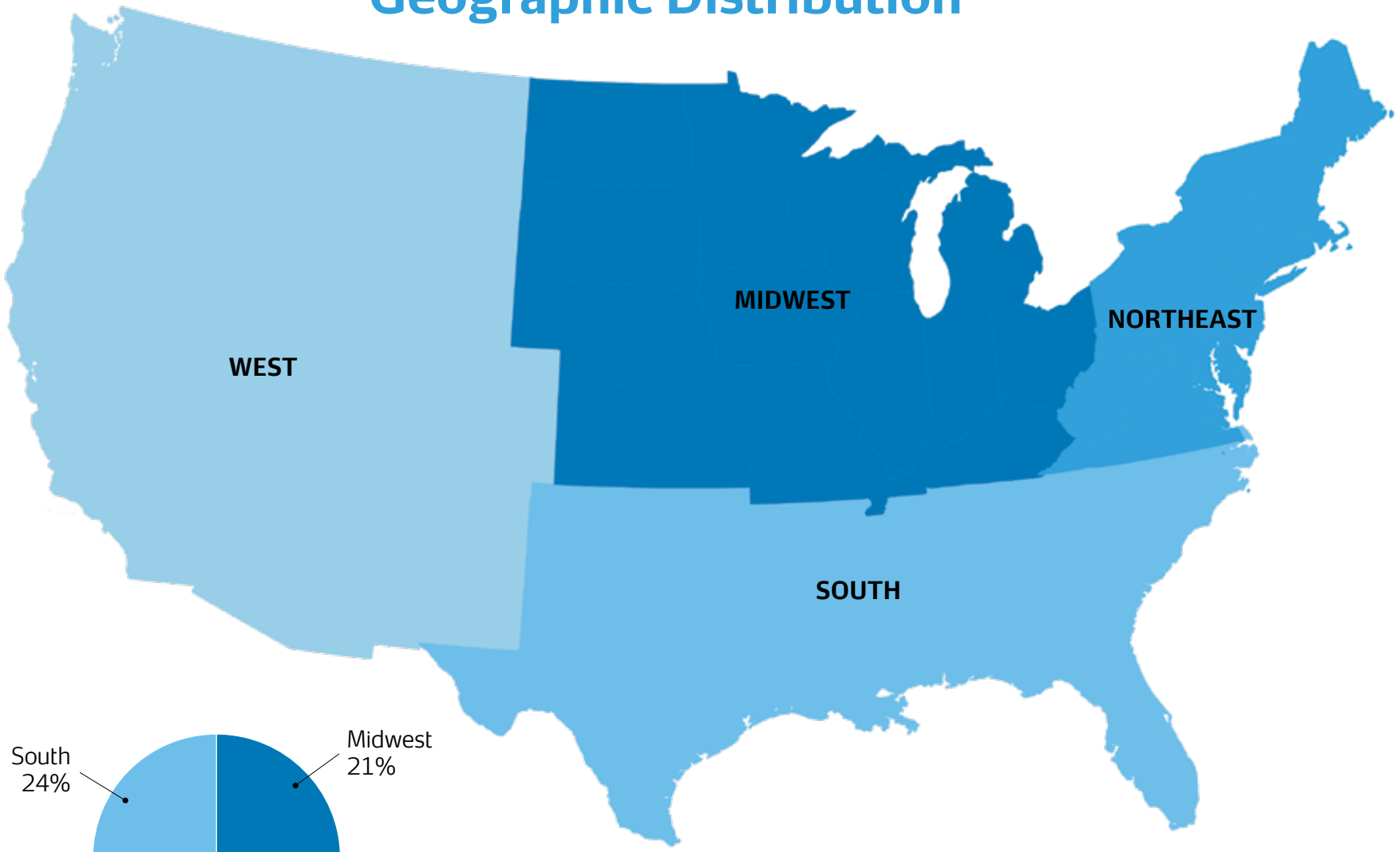
GEOGRAPHIC DISTRIBUTION

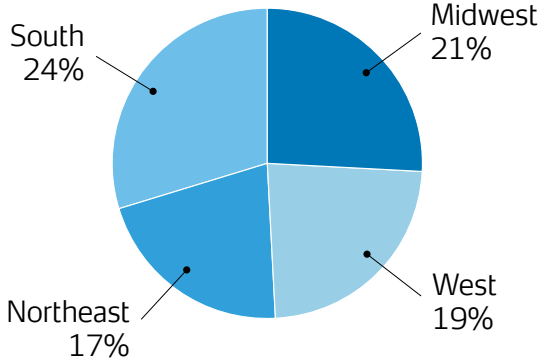
Responses from 32 states are represented in the survey results. For illustrative purposes, geographic distribution is grouped into four regions of the U.S. as shown in the map on the following page.

MARKET CLASSIFICATION MAIN/SUB-MARKET	TOTAL RESPONDENTS
Utilities/Telecommunications	10
Petrochemical/Oil and Gas	3
Retail	7
Healthcare and Social Assistance/Biotech and Pharmaceuticals	13
Arts, Entertainment and Recreation	2
Finance and Insurance	16
Commercial and Residential Real Estate	10
Professional, Scientific and Technical Services	5
Education	9
Hospitality and Food Services	4
Manufacturing/Logistics	44
High Tech	10
Government	3
Other/No Response	**6**
TOTAL	**142**



Geographic Distribution





Regions Total = 81%
International Total (Canada & Mexico) = 3%
Declined to Answer = 16%
Total = 100%

STOPPING ACTIVE SHOOTERS: BYSTANDERS CANNOT MERELY STAND BY

Konrad Motyka

ACTIVE SHOOTER STUDIES have consistently shown that when bystanders take decisive action, casualties are contained. This editorial provides notable examples, quantified evidence and expert opinions to enhance corporate security directors' efforts in training their employees to take such decisive action.

The Federal Bureau of Investigation (FBI) defines an active shooter as one or more individuals actively engaged in killing or attempting to kill people in a populated area. In 2017, the FBI reported 30 separate active shooting incidents in the United States. [1] Up to that point, it was the single largest number recorded during a one-year period. These incidents occurred in settings ranging from an outdoor music concert (Las Vegas, Nevada) where 58 were killed and 489 wounded, to a house of worship (Sutherland Springs, Texas) where 26 were killed and 20 wounded. There is no accurate predictor of where these incidents will occur. Mass casualty incidents have also occurred in academic settings, office parks, health care facilities, shopping malls, and private businesses.

Although an FBI study of *Pre-Attack Behaviors of Active Shooters in the United States between 2000 and 2013* showed that specific victims only were targeted in 27% of all incidents, the vast majority of victims simply happened to be in the wrong place at the wrong time. [2] Setting aside situations where specific victims were individually selected based on some form of acquaintance with the shooter, random victims were killed or injured either because the shooter did not care who got in his way (95% of active shooters are male) or because the shooter was trying to increase the body count to the highest possible level. These facts lead to an inescapable conclusion: in confronting an active shooter or shooters, inaction is no substitute for action.

The current prescription being advanced by professional law enforcement tactical instructors in most parts of the country is to RUN, HIDE, or FIGHT! The New York City Police Department has a slightly modified protocol called AVOID, BARRICADE, or CONFRONT (ABC). Both protocols recommend taking affirmative action to avoid becoming a helpless victim, thus increasing one's chances for survival.

The most common question audiences ask of instructors who teach RUN, HIDE, or FIGHT is: "Which do I do–Run, Hide, or Fight?" People want certainty; they want to be able to follow a formula for success to reduce the stress and panic of having to make a "life in the balance" decision in a moment of extreme danger. Unfortunately, each critical situation will be different–there is no one formula to apply that will always be successful. The key lies in decisive action, flexibility and adaptability.

I recently taught an Active Shooter class where, after covering some of the basics, I posited a situation where gunfire was heard in one part of the building and grew closer to our classroom. I asked the class, "What would you do?" Half the class would have exited through the far classroom door and headed to the emergency exit, while the other half would have locked the door, covered the door aperture, turned out the lights, silenced their cellphones, and piled furniture and

lockers in front of the door. I told the class that although removing themselves from danger was the preferred option, both options were correct. Both halves of the class were right because they refused to make themselves helpless prey for the theoretical shooter.

Another FBI study, *Active Shooter Incidents in the United States in 2016 and 2017*, noted that in ten of the incidents studied, the shooter was engaged either by armed or unarmed citizens. In eight of the ten incidents, decisive action by the citizens either prevented further casualties or stopped the shooter outright before he could inflict any harm. [1]

At the Jason Aldean concert in Las Vegas, the casualty count was incredibly high, and would have been higher still if many personnel trained as first responders had not been among the audience members. Even while under fire, they transported casualties out of the kill zone, comforted the wounded, and applied improvised tourniquets. [3]

In 2015, a middle school in Alabama received considerable media interest for asking students to bring canned goods that could be used to throw at an armed intruder as part of the last resort FIGHT recommendation. [4] Since then, reports of schools stockpiling hockey pucks and lacrosse balls have surfaced. After an initial burst of interest, those items are likely to end up gathering dust in a custodian's closet. It would be far better to focus on everyday materials that are readily at hand.

In the classroom cited earlier, I asked the students to take stock of what they might be able to use as a last resort. Answers ranged from staplers, to iPads, to those ubiquitous, BPA-free, partially filled stainless steel water bottles. Again, all those answers were correct. Anything that would distract an adversary or possibly inflict an injury could be useful, particularly when hurled en masse by everyone in the room. It goes without saying that by themselves, throwing objects would not be sufficient. At some point, it would become necessary to physically restrain or incapacitate the shooter. In this situation as well, everyday objects such as chairs and fire extinguishers can be useful.

The overall goal in preaching decisiveness and flexibility as a response to these harrowing situations is to prevent individuals from thinking of themselves as victims or potential victims. It is helpful for individuals to plan potential situations beforehand and create a mental "muscle memory" for what they might do in a life-threatening situation. While this may not be an enjoyable exercise, it is a sad fact that it is necessary in a world where the number of mass casualty incidents, if not necessarily their overall casualty levels, is increasing both exponentially and globally.

1. www.fbi.gov/file-repository/active-shooter-incidents-us-2016-2017.pdf/
2. www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/
3. Fink, Sheri. "After the Las Vegas Shooting, Concertgoers Became Medics." New York Times October 15, 2017
4. www.cnn.com/2015/01/13/living/feat-students-canned-goods-stop-school-shooters/

BIO

KONRAD MOTYKA

Konrad Motyka is the Executive Director for Campus Safety and Emergency Management for Mercy College. He joined the FBI in 1988 and was assigned to the New York Office. He has worked in counterintelligence, narcotics, and organized crime. From 1990 to 2001 he was a member of the New York Office SWAT Team, including being one of two Section Leaders. Motyka supervised the New York Office's Asian Organized Crime and Narcotics Unit from 2002 to 2008.

A two-term president of the FBI Agents' Association, Motyka retired from the FBI at the end of 2013. He is a recipient of the FBI Shield of Bravery and the Spanish White Cross of Police Merit. Motyka earned his B.A. degree from Columbia University and is a veteran of the United States Marine Corps.

ACTIVE SHOOTER THREATS: TAKING ACTION BEFORE THE VIOLENCE STARTS

Dwayne Gulsby, CPP

IT IS HARD TO IMAGINE, but prior to 2016, Active Shooter Threats did not even make the list of our Top Security Threats. Times have changed and preparing a well-designed plan and early detection of persons of concern are essential to avoid and respond to such tragic incidents.

Violence can be placed into one of two silos: planned or impulsive. Planned violence is premeditated and serves a level of purpose for those who plan and conduct violent attacks. Impulsive violence, on the other hand, is emotional and impromptu. These two types of violence are very different. According to the FBI, clinical and forensic data on adult and adolescent mass murder reveals that virtually all these acts are planned, rather than impulsive, violence. Planned violence usually involves an unresolved real or perceived grievance and a rationale of a violent resolution that eventually moves from thought to research, planning and preparation.

Whether an individual has actually conveyed a threat should not be a driving factor in the decision to conduct an investigation. In fact, for a person who truly intends to do harm, making a direct threat would be a disadvantage. Doing so naturally causes a logical and foreseeable chain of events to begin, including an investigation, increased vigilance, and target hardening, each presenting obstacles to the would-be offender.

One significant element that should be part of an organizational culture is to have employees feel a positive emotional connection to their environment and the workplace. This connection is cultivated by a climate of safety and respect, wherein people feel joined with the organization and believe that others in that environment know and care for them. It fosters a culture of shared responsibility. Employees are more likely to report their concerns when they believe all information is valued and that coming forward will be free of repercussions. Gut feelings about inappropriate conduct or comments are worth reporting, and someone trained to understand targeted violence can evaluate the information. An employee may have one small piece of information which, in turn, is used to complete the larger picture. Without such information, threat managers may not be able to accurately assess a situation.

When a person of concern has been brought to the attention of stakeholders, it is essential to engage as early as possible in the assessment and management process. By the time crisis-stage management is reached, potential solutions run the risk of being "knee jerk" rather than measured and thought out. By engaging in the assessment and management process as soon as a person of concern is identified, threat managers are more likely to succeed in preventing a violent outcome. Steering a person in a different direction early on may mean aiding someone who needs help before that person concludes violence is necessary.

Threat managers cannot predict the future. A targeted violence event cannot be anticipated, but active shooter attacks can be better understood, planned for and sometimes prevented. Cultivating a culture of shared responsibility and identification and investigation of persons of interest are of significant value. Falling victim to an active shooter attack is, from a statistical standpoint, highly unlikely. If one does occur, it becomes a life-or-death situation for all involved. While this is a low-risk event, it is of extremely high consequence for those involved, and understanding and preparing for such attacks will unquestionably save lives.

BIO

DWAYNE GULSBY, CPP

Dwayne Gulsby began his career with Securitas USA in 1992 on a part-time basis until he received his honorable discharge from the U.S. Marine Corps in 1994. He previously held the position of Vice President of Sales for the Mid-Atlantic Region as well as Business Development Manager and Operations Manager in the Virginia area. Gulsby was consistently successful in providing leadership to the business development and operational efforts year over year and, in January 2009, was appointed President of Securitas Canada Limited, managing the guarding operations across the country. In 2013 Gulsby was appointed President of the Central Atlantic Region, responsible for all facets of operations covering nine states and the District of Columbia.

He has been a guest speaker at various industry-related functions and has been interviewed by multiple media outlets. He has over 20 years of industry related experience and his progressive growth and solid leadership skills have positioned him as an industry expert.

BUSINESS CONTINUITY PLAN: BEYOND THE BASICS

William J. Powers III

IT IS IMPERATIVE THAT ORGANIZATIONS have a well-written All-Hazard Emergency Response Plan (ERP) in conjunction with an Incident Action Plan (IAP). This document includes a business continuity plan which helps the organization to maintain operations if possible. More than 40% of organizations are forced to close after a major incident. The plan is a living document that should be regularly reviewed and updated, as the process is dynamic and ever-evolving.

A comprehensive security analysis should be performed to help identify any potential risks. A strategy to mitigate such risks should then be developed. Scenario-based thinking will help to prepare and understand the challenges in managing the risks, and allows open-minded thinking to ask questions, such as "If this happens, what can be done?" Training must regularly occur and be consistent and in the right setting. Responders are often placed in difficult situations because the proper training has not been conducted. On-duty responders need training for everyone's safety.

The four phases of emergency management are preparedness, response, recovery and mitigation—they are the basis for the ERP.* The goal is to end the incident as quickly as possible. The IAP summarizes incident response tasks and instructs personnel on mitigating potential damage. The Incident Response section prepares individual responders by assigning role-specific tasks. The Incident Closure and Debrief sections direct responders on aiding business recovery. Each response follows a step-by-step process—governed by the Incident Command System (ICS)—that will guide responders from incident preparation through incident closure.

A business continuity plan should clearly state in writing the essential functions and goals of the organization. The document should identify and prioritize the systems and protocols to be sustained and provide the necessary information for their maintenance. The ERP and IAP form the framework of incident response. Life safety will always be the highest priority. As the incident concludes, the next important step is to normalize business operations as soon as practical. More than 40% of organizations do not survive a disaster for various reasons.

Businesses having a plan to move forward after a critical event will have a better chance of staying open versus a business with no plan. During an emergency is not the time to determine what can be done and whom to contact. In the planning stages, it is easier to think more clearly and establish contracts and billing rates with vendors, contractors and others if the incident involves more than a single facility.

Community and Regional Resilience Institute (CARRI) is a concept of emergency management that FEMA initiated, and which differs slightly from Incident Command. The entire community is involved in the plan, and the decisions are made by consensus regarding the plan elements. In 2011, this concept was tested in the U.S. through several pilot programs across the country. This process requires resources and support from all local community agencies. The concept of this plan is relativity simple; however, it does become complex as to who has the decision-making authority in the community and how resources are allocated. There are many political governing bodies in this process—all with an interest in seeing it succeed—from the President through the cabinet. The government has made grants available to municipalities. The concept is who is better-equipped to make decisions for the people most impacted. Everyone is familiar with both the process and the local agencies.

The more communities are involved and acquaint themselves with the local agencies, the better and stronger the community becomes. It is similar to community policing—knowledgeable community residents are more willing to share information with law enforcement.

Through Presidential Policy Directive 21 (PPD-21), enacted in February 2013, the National Infrastructure Protection Plan (NIPP) aligns with PPD-8, which addresses national preparedness. These directives help align communications with federal, state, local, tribal, and private sector groups to engage in emergency preparedness. With better communications, everyone working towards common goals, and understanding the fragile nature of critical infrastructure, people are more open to sharing when an incident occurs. The success of this integrated approach depends on leveraging the full spectrum of capabilities, knowledge and experience across the critical infrastructure, community and associated stakeholders. This requires efficient sharing of actionable and relevant information among partners to build situational awareness and enable effective, risk-informed decision-making.

* FEMA: https://training.fema.gov/emiweb/downloads/is10_unit3.doc

BIO

WILLIAM J. POWERS III

William J. Powers is the Director of Facilities at The Sterling and Francine Clark Art Institute in Williamstown, MA. Powers oversees the Facilities, Maintenance and Security Departments of the Clark Art. Powers has over 30 years of experience in cultural property protection, starting at the Berkshire Museum in 1981 and coming to the Clark Art Institute in 1995. In addition to being a member of the Board of Directors for International Foundation for Cultural Property Protection (IFCPP), Powers is the Sergeant at Arms for the IFCPP, as well as a Self-Defense and Use of Force expert. He is a certified instructor through the IFCPP and frequently lectures on cultural property protection at cultural facilities and colleges. He was one of the first IFCPP members to host a Regional CIPS Certification Workshop, and continues to contribute valuable assistance to the Foundation. Along with working with the IFCPP, he serves on the awards committee and is an active member on the Cultural Properties Council for ASIS.

Powers has a Master's Degree in Administration of Justice and Security. Powers also serves as a Captain with the Berkshire County Sheriff's Department, Uniform Branch, since 1995. He holds a 6th Degree Black Belt in martial arts and a Master Level Teaching Certificate. He is an active member of several national associations, including ASIS International, the American Association of Museums, the National Fire Protection Association, the New England Museum Association, the Association for Facilities Engineering, and the Museum Association Security Committee.

DESIGNING SAFE SCHOOLS IN DANGEROUS TIMES

Randall Atlas, Ph.D., CPP, FAIA

DESIGNING SAFE SCHOOLS is the responsibility of every community, while day-to-day operations are primarily the responsibility of teachers, school administrators, and school security/law enforcement officers. Before the first student walks the halls, however, an architect designs the school, creating subsequent relationships of people and their buildings.

The success or failure of each school is predisposed to the integration of security and crime prevention through environmental design (CPTED) during the design process and budget limitations. The basic CPTED premise is that the effective use and design of the built environment can reduce the opportunity and fear of crime and result, in this case, in improvement in the quality of the educational experience. Designing the next generation of schools for the effective use of space with CPTED features will substantially reduce the opportunity and fear of crime.

CPTED applies to both new and existing schools and is based on the concepts of natural surveillance, natural access control, territoriality, management and maintenance, and legitimate activity support. If a school layout seems unsafe, adopting a few CPTED fundamentals may help make it significantly safer.

CPTED elements that can have the most impact on school security include:

- Providing for limited and controlled entrances.
- Security layering and zoning.
- Staff training and operational strategies for protecting the building and its users.
- Perimeter boundary definition.
- Reducing conflicting user traffic patterns.
- Securing the classrooms with improved door hardware.
- Having spaces for sheltering in place in the event of an active shooter situation.

School administrators and architects cannot select appropriate countermeasures unless clear objectives are identified. The threats to a school are either external (from outside influences and persons) or internal (from students, faculty, staff, and workplace violence). CPTED can make a direct impact on reducing external threats through use of the concepts mentioned above. The internal threats can be primarily deterred through policy, procedure and management techniques, as opposed to physical design. When a school has multiple entrances and ground floor windows, for example, the threat and vulnerability levels increase greatly, and make the facility much more difficult for the protection of people, property and information.

Safe school design involves four key areas that should include CPTED security layering/defensible space planning practices.

- Site design includes features of landscaping, exterior pedestrian routes, vehicular routes and parking, and recreational areas.
- Building design features include building organization, exterior covered corridors, points of entry, enclosed exterior spaces, ancillary buildings, walls, windows, doors, roofs and lighting.

- Interior spaces include features of lobby and reception areas, corridors, rest rooms, stairs and stairwells, cafeterias, auditoriums, gyms, libraries and media centers, classrooms, locker rooms, labs, shops, music and computer rooms, and administrative areas.
- Systems and equipment include features such as alarms and surveillance systems, fire control, HVAC and mechanical equipment, vending machines, duress alarms, elevators, telephone and visitor identification systems.

A single point of entry is the new standard of care where possible. Depending on the size of the school, a single point of entry is preferred for maximum utilization of weapons screening, staffing and labor efficiency, and visitor entry. Weapons detectors can be integrated within an entry way, but with that comes the responsibility of pat downs, package screening, and video recording to prevent frivolous claims of inappropriate searches. Access to areas from main entryways should be carefully planned and not obscured. Main entryways should be obvious and designed with CPTED in mind. Treatments of secondary entries are just as important as primary entries.

Changes in fire code now make fire alarm pull stations optional. Classroom locks for schools must comply with fire and accessibility codes. While locks can prevent a hostage situation by using the door barricade devices, they can prevent quick response by police and EMS. Codes now allow school faculty/ administration three minutes to verify a fire condition, and either shut down the alarm or allow the alarm to activate, thereby evacuating the school. This was one of the lessons learned from the Stoneman Douglas shootings after the shooter's weapon discharged smoke and activated the fire alarm system, thereby creating confusion about whether to evacuate or shelter in place.

Summary: Many schools in the U.S. have an inviting and open campus style, with multiple buildings, entrances and exits; large windows; and many opportunities for hiding or privacy. These design configurations are not conducive to many current requirements that need to encompass security needs. Incorporating the principles of CPTED in the design and remodeling of schools can contribute to the overall safety of the school, while reducing the target hardening and fortressing effects of a "old school" bunker mentality. Security technologies such as cameras, sensors, weapons screening, etc. can contribute to overall school security, but not in all situations. Schools must not undervalue the importance of good maintenance, construction, and design; and a fair and equal management style of school operations. Creating a secure and safe educational environment is all about planning, but each school has unique needs. Best practices begin with a security threat and vulnerability assessment, which identifies the security functional requirements and design basis for each unique school environment.

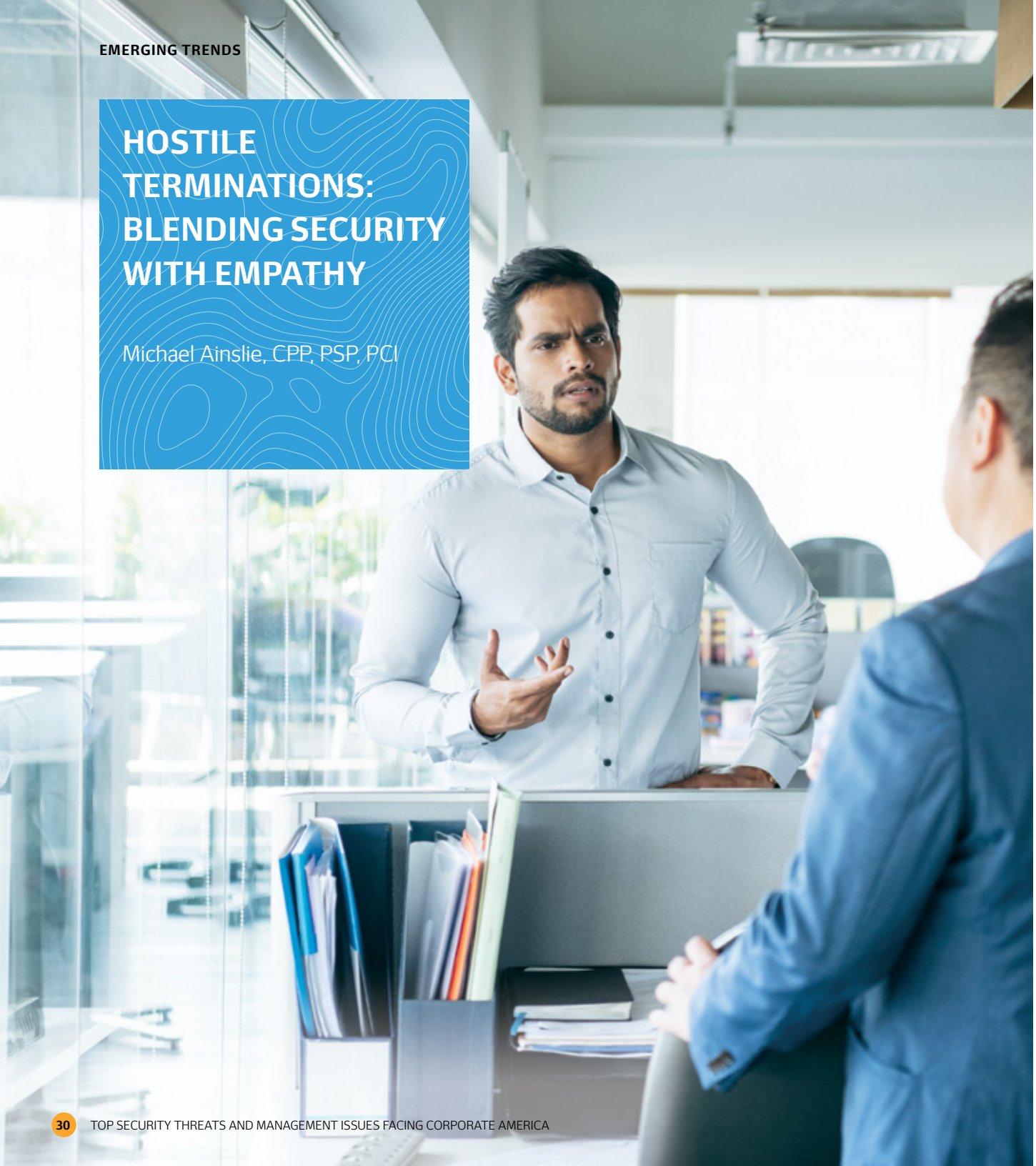
BIO

RANDALL ATLAS, PH.D., CPP, FAIA

Randall Atlas is America's only architect/ criminologist. Atlas received his Doctorate of Criminology from Florida State University, a Master's in Architecture from the University of Illinois, and a Bachelor of Criminal Justice degree from the University of South Florida. Atlas is president of Atlas Safety & Security Design, Inc., based in Fort Lauderdale, Florida. He is a registered architect in Florida, nationally accredited with the National Council Architectural Registration Board (NCAR.B), and is a Fellow with the American Institute of Architects. Atlas is a Certified Protection Professional (CPP), a past chairman of the ASIS Security Architecture and Engineering Council, and an appointed member of the National Fire Protection Association (NFPA) Premises Security Committee. Atlas is a professor at Florida Atlantic University, where he teaches a CPTED course online for the schools of Architecture and Criminal Justice. He is a member of the Florida Design Out Crime network, the International CPTED Association, a member of the International Society of Crime Prevention Practitioners and the International Association of Counterterrorism and Security Professionals. Atlas is a nationally recognized trainer and author on Crime Prevention Through Environmental Design. Atlas authored the book 21st *Century Security and CPTED* in 2008, and the 2nd Edition in 2013. Atlas has conducted risk vulnerability assessment security surveys for a variety of school environments throughout the United States, including Harvard, Ohio State, and Georgetown universities.

HOSTILE TERMINATIONS: BLENDING SECURITY WITH EMPATHY

Michael Ainslie, CPP, PSP, PCI



HOSTILE TERMINATIONS—a termination in which an employee could potentially pose an elevated risk to the company, its employees or the company's assets—are often the last opportunity to prevent our next workplace violence threat. Security and human resources (HR) have numerous procedures, policies and processes that guide functions including onboarding, adverse actions, terminations, and more. Security and HR typically work hand in hand for these events, with each understanding the concern of the other, while both work to ensure processes are followed step-by-step. While this approach works very well for routine actions, it does not necessarily provide the best outcome for a hostile termination.

When an employee is terminated, the company is potentially depriving the individual of income needed to support a lifestyle or family as well as potentially shattering dreams and a sense of accomplishment. Therefore, each termination should be evaluated to determine the emotional state of the employee and, to the degree possible, the extent of the threat posed by the terminated employee to the organization and its employees. Once a termination is determined to be an elevated risk to the organization, its employees or assets, it should be considered a hostile termination and handled according to its own process—one driven by understanding, compassion, flexibility and strategy.

During my 33 years in the security industry, I have learned that what you normally receive or experience from an employee is reflective of the overall person's character. Simply put, if the employee's life at work is a train wreck, then life outside of work is usually the same. As a rule, we are not terminating our top performers or most "put together"

employees. This is important to remember because it is not another termination—it is someone who probably really needs the job, is perhaps experiencing financial troubles or extreme personal problems, and is potentially on the verge of breaking down. The individual may also seek to blame someone else for any personal problems and what has gone wrong in his/her life. Therefore, security needs to take the lead in overseeing the hostile termination process—to ensure concerns and issues are addressed and resolved in a timely and compassionate manner, thus preventing unnecessary escalation of conflicts.

Security needs to place itself in the terminated employee's position. What will be the biggest concerns and issues and, more importantly, how do we resolve them? The immediate issue will usually be financial regarding how many future paychecks the employee will receive.

I have seen a variety of ways to handle this and will relay some of my experiences. An employee was abruptly terminated on a Friday for being very verbally abusive. This continued throughout the termination process but, by Monday afternoon, we had managed to calm the situation. On Wednesday, the situation again exploded to include an enhancement of the security posture at the offices, all because the employee was not paid on time. The terminated employee was to be mailed a hard copy check, which would be received on Friday versus the usual Wednesday direct deposit against which checks had already been written, thus further aggravating the individual's financial situation. We have since been able to ensure that, for future hostile terminations, the employee will be provided the severance check in a timely manner. For hostile terminations of employees who would normally be paid a larger lump sum we have had much success instead, paying the employee over several pay periods, contingent on no contact with the organization other than designated representatives.

Assigning a senior designated representative for the terminated employee provides a single point of contact for the various post-employment activities that will need to take place. These activities include but are not limited to shipping of personal items, return of corporate assets, W-2s, insurance, and 401(k)s. For the 401(k), we provide a real phone number so that the employee can contact our provider and reach a representative who will provide needed assistance versus getting lost and frustrated in a maze of online navigation or being placed on hold. The role of the senior designated representative is to ensure that issues are addressed and resolved in a timely manner, to include cutting through red tape when necessary. On rare occasions, a member of the CSO's staff serves in this capacity if necessary.

Hostile terminations are, in fact, still a process—one that starts from a point of empathy, compassion and understanding for the people involved. From that position, security is part of the solution in making the best of a bad situation and protecting the organization, its employees and assets from the next potential workplace violence threat.

BIO

MICHAEL AINSLIE, CPP, PSP, PCI

Since January 2017, Michael Ainslie has been the Head of Global Security for Allegis Group, Inc., where he works with key stakeholders within Allegis Group and its operating companies to develop, direct and coordinate activities relating to the protection, safeguarding and security of company employees, contractors and invitees, as well as other company assets across a global enterprise of over 550 locations.

Prior to joining the Allegis Group team, Ainslie worked and lived in multiple countries as a U.S. Federal Law Enforcement Officer and Senior Security Officer for nearly 28 years with the U.S. Central Intelligence Agency. He also worked with Honeywell International as a Senior Security Consultant, working closely with Fortune 500 companies to improve their security posture, both domestically and globally, through implementation of innovative, effective and non-invasive placement of people, processes and technology. He is a recognized expert in security and holds ASIS International certifications of Certified Protection Professional (CPP), Physical Security Professional (PSP) and Professional Certified Investigator (PCI). He is an active member of ASIS as well as the ASIS Utilities Security Council, where he serves as Secretary. Ainslie is also a member of the U.S. State Department Overseas Security Advisory Council (OSAC).

RECOVERY FROM AN ACTIVE SHOOTER EVENT: A BUSINESS CONTINUITY PERSPECTIVE

Sandra Cowie, CPP

AN ACTIVE SHOOTER EVENT can leave an everlasting imprint on organizations and the lives impacted by such a tragedy. In considering this topic, I thought, "What is different about business recovery from an active shooter event than other events impacting business operations?" I believe the first sentence above strikes at the core of that question.

The business continuity discipline is foundationally-based on an all-hazards approach and how organizations should prepare, respond and recover from those hazards. The maturity of the industry took us away from having a specific plan for the hundreds (or more) of different situations that might affect our ability to do business and instead focused on the fundamental elements of the impacts to an organization, regardless of the incident, i.e., the all-hazards approach. We quickly found the issues we needed to address were consistent, no matter the cause. We may have to deal with the loss of people, property or technology. From a strategic perspective, we need to plan for reputational, legal, regulatory and political risk. So, are there unique considerations in the "prepare, respond, recover" continuum that are different for an active shooter event?

Preparation is certainly a critical element to mitigating this risk, perhaps even more so than other hazards we face. A comprehensive workplace violence program addressing the many dynamics of this risk is essential. Others in this series are focusing on that important component as well as response, which in most cases will be mere minutes (with an average of 3-4 minutes) before the incident ends. So—back to recovery. Exercising your plans are key to not only developing muscle memory of your response teams as they work to address issues, but they

also raise issues that may be unique to a specific type of incident. Let's look at what we might face in the recovery phase of a workplace violence incident.

People: There will definitely be people impacted. Lives may be lost. Employees may be unable to return to work due to the emotional trauma of such an event. Fear is likely something you will be facing, whether your employees were directly in the area of the incident or not.

Property: While physical damage to your property is likely to be minimal, access to your property will certainly be an issue as your place of business becomes a crime scene.

Technology and infrastructure: Depending on the level of physical impact to your property and your contingency plans for back up, this area is likely to have the least impact in such an event. It is likely your systems and infrastructure will be available to conduct your business. What about the strategic risks to your organization?

Reputation: It will most definitely be at risk. You will be scrutinized on your security and workplace violence programs. Most importantly, you will be judged by your compassion as a company in dealing with the aftermath of the event. How did you treat your employees? What support did you provide them? How did you treat the families of the impacted employees? Does it reflect your brand? Does it demonstrate what you say you are and believe to your customers? Does your response show you care?

Legal: The prevention and response of your plan will be challenged. Did you have the right security controls in place? Was everything working as it should? Did you provide the proper training and take the appropriate actions?

Regulatory: In the U.S., OSHA is the overarching regulatory body that requires employers to provide a safe and secure work environment, including specifically addressing the risk of workplace violence. Other countries have similar laws. Does your program pass the test? There are also an increasing number of industry standards and guidelines on workplace violence, including those from ASIS and NFPA. Do your programs align with these industry best practices?

Political: Initial reaction might be that there would be limited impact in the political arena, but such an incident may put you in the spotlight regarding your position on weapons, the right to bear arms, our mental health system and the availability of care—a challenging environment when your customers likely have very diverse positions on these issues.

With this brief analysis exercise, we can see that the foundational elements of recovery and the issues we need to address remain critical and consistent in a workplace violence incident, as they do for other types of incidents. The biggest difference may take us back to the beginning of our discussion on this topic. The impact of such an event can leave an everlasting imprint on your organization and the lives of your employees Your recovery won't be just about returning to your facility and patching bullet holes—it will be a long process of compassion and healing.

BIO

SANDRA COWIE, CPP

Sandra Cowie is the Director of Global Security and Business Continuity for Principal Financial Group. Her responsibilities encompass site and personnel security/safety and business continuity globally for the company, including investigations, access control, physical security planning, executive protection, intelligence, emergency management and two emergency response centers. Cowie began her career at Principal in the Retirement and Income Solutions division, managing pension plans and funds and leading teams who managed plans and funds. She has been in security management since 1993.

With education and experience focused in management, finance and security, she has over 35 years' experience in those areas. She is Board Certified in Security Management and has advanced training in several security specialty areas. Active and recognized in the security industry, she has served in various leadership roles for ASIS International, including the Board of Directors, and currently serves as the Chair of the ASIS Foundation Board. Cowie is a member of ISMA, the CSO Roundtable, and serves at the request of the Secretary of State on the Executive Working Group as the first female private sector co-chair of the Overseas Security Advisory Council, addressing security issues of U.S. companies doing business globally. An advocate for public private partnerships, she was a founding member of Safeguard Iowa Partnership, serving on the board and several leadership positions.

Securitas Security Services USA, Inc. is *The Leader in Protective Services*, serving a wide range of clients 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 118,000 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 & 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 securitasinc.com