2014 SECURITY 500®

THE PREDICTIVE REVOLUTION

By Mark McCourt, Publisher

> In 1963 David Ogilvy, the father of Madison Avenue and author of a classic business book, "Confessions of an Advertising Man," wrote: "An advertisement is like a radar sweep, constantly hunting new prospects as they come into the market. Get good radar, and keep it sweeping." Half a century later advertisers are at last taking him at his word. Behavioural profiling has gone viral across the internet, enabling firms to reach users with specific messages based on their location, interests, browsing history and demographic group. Ads can now follow users from site to site: a customer who looks online for flights to Frankfurt will be inundated with German holiday offers. Conversant, a digital-marketing firm uses an algorithm to deliver around 800,000 variations of an ad to its big clients' prospective customers to make it as irresistible as possible. Kraft, a food company, monitors online opinions on its brands in an office which it calls "the looking glass."
>
> ***The Economist, Little Brother, September 2014***

As you read through this year's Security 500 Report and the advertisements surrounding it, you may not realize how much marketing's mission is intertwined with security's. Perhaps a digital marketing conference would be as valuable to you as attending a security industry event because the era of collecting, analyzing and interpreting information to identify risks and predict threats has arrived. Scorned for its use by three-letter government agencies, the results are clear. It works. The Predictive Revolution is the culmination of a three-stage evolution in risk and security practices.

First was the Responsive Era, which defines most of enterprise security's history. Similar to the show "Law and Order" where each episode begins with a dead body, security waited for the phone to ring alerting them to an event requiring response and an investigation to complete. Doors were not locked, and when property was stolen, the police were called to take a report and perhaps investigate. Post 9/11, the bar was raised by insurers, corporate leadership and stakeholders, who demanded and funded bigger and better security programs. Thus, the familiar "guns, guards and gates" and "second career cops" definitions waned. The enterprise security profession gained momentum.

"RISK" became centric to the security's mission and management role. The Preventive Era emerged. By identifying foreseeable risks, security organizations could take preventive action to eliminate vulnerabilities and thwart potential threats. Predictive Security evolved to identifying risks to prevent events from occurring and effectively responding to unforeseen events that occur.

For example, we learned that by not locking our doors the property in our homes would be stolen, and we responded. From experience we could predict this outcome. We learned to lock our doors. But we did not know which homes would be robbed, or when or by whom.

Locking our doors is preventive.

Now, the Predictive Revolution is here. Like marketers who leverage technology to gather information and intelligence to predict future buying behavior, physical, cyber and intelligence security operations centers (SOCs) work to predict and thwart events that would negatively impact business continuity, infrastructure and stakeholders.

> "Any successful organization needs to advance in all three domains of people, process and technology. But it starts with good people to advance the latter."
>
> ***Rich Mason, Honeywell***

As I have written before, it's all about: "Getting the right information to the right people at the right time to make the right decision to predict an event that will happen and prevent it from happening or to respond effectively to an event thereby stopping a disaster from becoming a catastrophe." Now, "predict an event that will happen" has been added to the statement.

The people, processes and technology needed to be predictive are sweeping across the Security 500, bringing with them broad operational and bottom-line benefits. Now security organizations are more able to predict who is likely to take property and when and calculate risk. By being predictive, threats can be acted upon and mitigated before their negative impact occurs.

Neither criminal actors nor consumers realize how closely their online behavior can be tracked, analyzed and spun into actionable intelligence. Nor does Mother Nature.

It's predictable then, that the Predictive Era is having a significant effect on security organizations. The mission, organizational chart, talent requirements and activities of the predictive organization are forcing a dramatic change in their risk strategies and execution.

What is clear is that the drive to become predictive will continue, and the stresses it will place on risk and security organizations during this transition are significant. Here are some key areas that face change as a result:

Leadership: It must be more intertwined with the businesses culture and its goals to build the right programs that deliver measureable benefits. C-Suite and Board support are required.

Human Capital: A major challenge is trying to hire people who may not yet exist. The new breed of security officer is more likely to wield an algorithm than a gun. HR's engagement in talent management is necessary.

Communication: Gathering, processing and returning information to avoid high probability threats can cement an enterprise security department's future as either a clairvoyant or a Chicken Little. Once a threat is identified, having a mitigation plan in place with a high likelihood of success is important.

Budget: "Doing more with less" is a common theme among organizations' changing practices to focus on technology resources and human capital to leverage them, while maintaining a constant risk posture during the transition.

Technology: Perhaps it goes without saying, but a significant investment in new and different technologies and a change from prior technology strategies is happening.

Having expert team members in this discipline and internal relationships (especially with IT) is important for success.

> "We are involved in company, not merely security decisions which means there are no surprises. That is the critical difference that enables success."
>
> ***Steve Baker, State Street Corporation***

The security profession has never been more dynamic than it is today. Just look around the world and it is clear that from physical to intellectual to logical property, it might all be stolen and sold, in the click of a mouse. Hostilities around the world, in our schools and at our workplaces continue to escalate and demand action. Natural disasters, pandemics and extreme weather, combined with globalization require travel support, emergency medical resources and constant vigilance. Thus, it is the ones and zeroes that will tell us in greater quantity and quality what is happening, what will happen and what to do next. Strong business leadership driving organizational alignment with enterprise goals is making the Predictive Era a reality among Security 500 members.

2014 KEY TRENDS AND AREAS OF FOCUS:

1. Cyber Crime

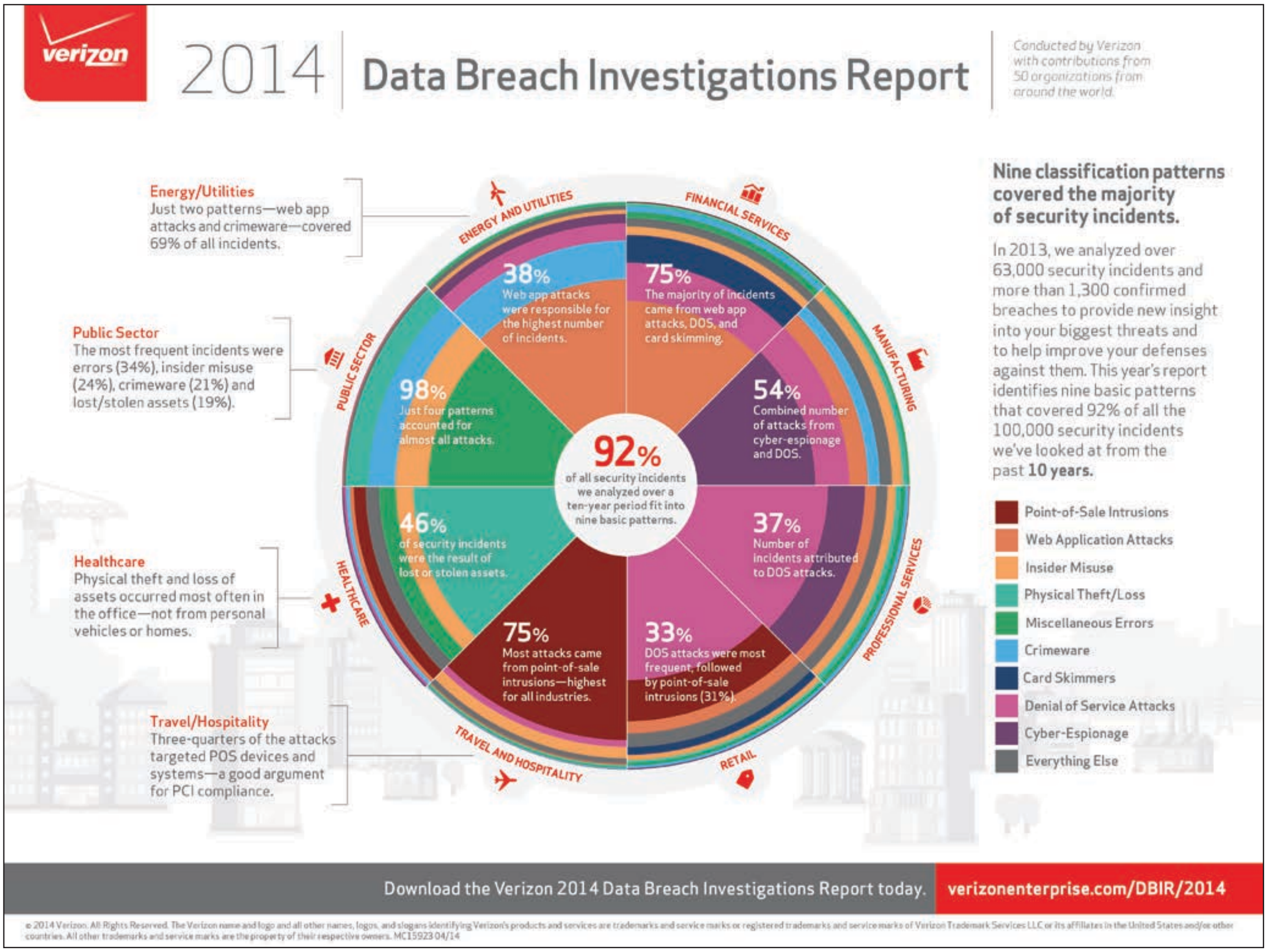
It is counterintuitive that cyber crime is the number one threat facing enterprise security leaders, because only 28 percent of those security leaders that rank it as their first concern in the Security 500 report have direct responsibility for it. Indeed, the number of incidents is growing rapidly in scope and quantity. The Target case study with no CSO or CISO in position was an easy, um, target (sorry) for cyber criminals. But Target is not unique in neither understanding nor preparing well against cyber threats as Home Depot, JP Morgan Chase and numerous other enterprises proved.

The cost, brand damage and, in the Target case, CEO's career have appropriately risen to the top of C-Suite issues and discussion. Cyber is finally getting the organizational attention deserved to do what security does best: Evaluate the risks and craft a plan to eliminate vulnerabilities, mitigate risks and prepare for resilience in response to an incident.

The two key casualties at Target were the CIO and the CEO. But IT's role and expertise is not in securing. It is in enabling. Organizing the business to address the cyber threat as a business risk and staffing to successfully remove the threat are the best practices for securing the business.

Steven Chabinsky hit the organizational nail on the CEO's head in a recent Cyber Tactics column for this publication, when he wrote:

> *Unfortunately, the pervasive attitude that cybersecurity is an IT problem rather than a C-Suite whole-of-enterprise concern likely stems from the top. As the National Association of Corporate Directors recently observed, a lack of cyber expertise on corporate boards presents a real and urgent threat to oversight. Inexplicably though, the NACD also found that "a demand for IT experience generally has not surfaced*



in director recruitment." That needs to change. Simply put, thinking of cybersecurity as an IT issue is similar to believing that a company's entire workforce, from the CEO down, is just one big HR issue.

And the *13th Annual EY Global Fraud Survey: Overcoming Compliance Fatigue: Reinforcing the Commitment to Ethical Growth* showed that 48 percent of CEOs considered cyber crime as "low risk to their business." As you know, they are flat out wrong.

The *2014 Verizon Data Breach Investigations Report* shows that every Security 500 sector is targeted and victimized by cyber crime. At the same time, they are able to classify the nine most used threats indicating that defending against known threats will work against cyber.

> "Initially, we were like a hockey goalie facing the net instead of watching the threat. By turning around, we get to work on knowing the opponent, understanding their moves. We are able to balance security against threats. Our defenders become collectors of information and intelligence to build a defensive strategy and optimize response. Learning as much as possible about the adversary's tactics and techniques gives us an edge in discovering and stopping attackers."
>
> ***Gary Gagnon, MITRE***

And, yes there is clear evidence that cyber crime is a business, not an IT, problem. As *Business Week* reported, customers will stop shopping and take their banking business elsewhere. The report recognized that 71 percent of customers will switch banks due to fraud. Also, it notes, retailers experience a significant drop in brand perception after a data breach. As reported in the 2013 Security 500, a study by HB Gary found that 78 percent of investors are unlikely to invest in a company with a history of cyber attacks.

Skating on the other side of the ice is privacy. Marketers are leaning heavily on the customer information that can be gathered from online and offline behavior. But Security can learn a thing or two about intelligence and information gathering from marketing programs. A recent report in *The Economist* titled: "Stalkers, Inc." states that surveillance is the advertising industry's new business model, noting the average person is being observed by 1,300 marketers each time they click on a website. But once you turn that hockey goalie around, you go from defense to offense inviting new threats.

What responsibility does enterprise security have for the privacy of its brand and leaders? For example, the BuyPartisan App reveals the political leanings of company board members and executives when a product barcode is scanned. Yes, it just got harder to sell soap.

It is important to track the fallout from the Catsouras (U.S.) and Costeja (Europe) privacy decisions facing what content can stay and what must be removed from websites and search engines. Contrary to popular belief, a recent Boston Consulting Group study found that younger consumers are as concerned about their privacy as older generations.

Thus, an increasingly used mitigation strategy is buying cyber insurance to protect businesses against the financial risks in the connected world. Including both liabilities and the actual cost of crime, insurance policies (and their premiums) will be on the rise as board risk committees consider both the cyber threats against legal, personal and brand exposure.

The PwC *2014 Global Economic Crime Survey* reported that 24 percent of companies have been a victim of cybercrime. PwC theorized the number as higher, since many organizations either don't report or don't know that they are victims. As a result, PwC anticipates a steady increase in cyber insurance coverage by companies seeking to mitigate financial risks related to cyber crimes.

2. Workplace Violence

As the NFL spins out of control over the recent Adrian Petersen, Ray Rice and Greg Hardy incidents, you may wonder what it has to do with your enterprise. First, it is a case study in crisis management as the lack of preparation and resilience within the NFL regarding workplace violence issues (and/or domestic abuse). Second, it documents the observation of Michael Chertoff, former Director of Homeland Security, that once a crisis occurs in an enterprise, the ability of the CEO to manage and execute their business agenda becomes impossible. And workplace violence is prevalent across all sectors, especially in healthcare.

> "It's a horrible response. The NFL has essentially re-victimized the victims by trying to smooth it over and not expressly giving their apologies to the victims. The whole incident was a debacle, in how the NFL handled it. It's just getting worse and worse and worse in their handling of it and understanding the cycles of violence."
>
> ***Raquel Singh,***
> ***Voices of Women Organizing Project***

And domestic abuse has an economic impact on businesses because women are the most frequent victims, often missing work and being terminated because while there are policies against workplace violence, there are frequently no policies for the victims of that violence.

> "Workplace violence is at the forefront of our security concerns right now. We provide personal safety training and conflict resolution training for our employees, because they deal with a lot of confrontational situations on a daily basis. Their ability to negotiate through some real difficult situations minimizes the amount of risk to them and the amount of risk to us as first responders."
>
> ***Kirk Simmons,***
> ***Hennepin County, Minnesota***

For a statistical look at the problem, the World Health Organization gives a global view in their recent study, the *World Health Organization's Key Facts (2013)*:

- Violence against women – particularly intimate partner violence and sexual violence against women – are major public health problems and violations of women's human rights.
- Recent global prevalence figures indicate that 35 percent of women worldwide have experienced either intimate partner violence or non-partner sexual violence in their lifetime.
- On average, 30 percent of women who have been in a relationship report that they have experienced some form of physical or sexual violence by their partner.
- Globally, as many as 38 percent of murders of women are committed by an intimate partner.
- Violence can result in physical, mental, sexual, reproductive health and other health problems, and may increase vulnerability to HIV.
- Risk factors for being a perpetrator include low education, exposure to child maltreatment or witnessing violence in the family, harmful use of alcohol, attitudes accepting of violence and gender inequality.
- Risk factors for being a victim of intimate partner and sexual violence include low education, witnessing violence between parents, exposure to abuse during childhood and attitudes accepting violence and gender inequality.
- In high-income settings, school-based programs to prevent relationship violence among young people (or dating violence) are supported by some evidence of effectiveness.

- In low-income settings, other primary prevention strategies, such as microfinance combined with gender equality training and community-based initiatives that address gender inequality and communication and relationship skills, hold promise.
- Situations of conflict, post conflict and displacement may exacerbate existing violence and present new forms of violence against women.

> "For workplace violence threats, we've really strived for open lines of communication with our employees so we can hopefully anticipate and avoid any situation on the front end. We provide continual awareness messaging to them and reinforce that if you see something or hear something, please say something."
>
> ***Jerry Blum, AutoZone***

William Nesbitt from Security Management Services International offers the hierarchy below to reduce both workplace violence incidence and the program's cost.

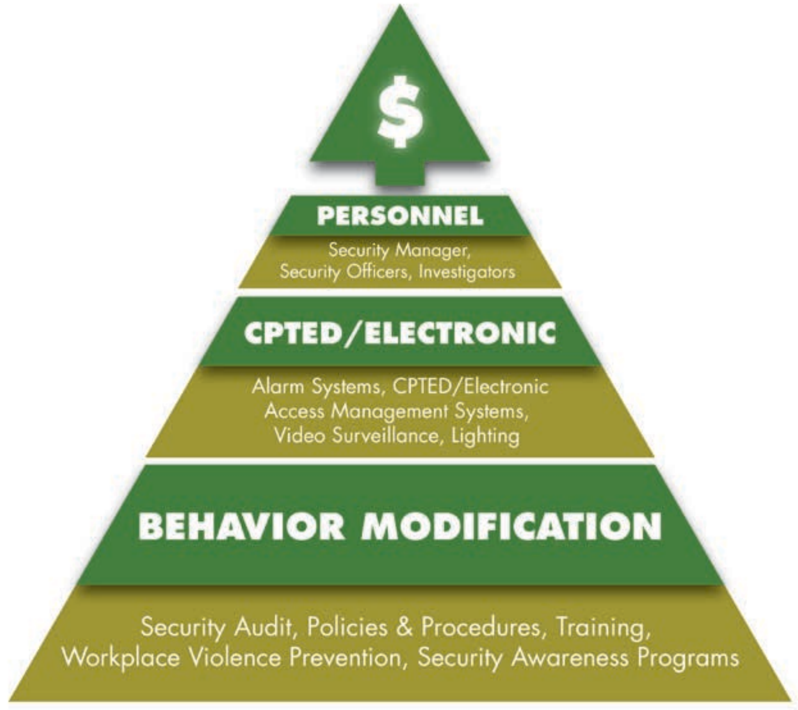
Note how education, listening, talking with employees and watching for concerning behaviors are highly effective practices for identifying threatening behavior and diffusing potentially violent situations. The ability to identify escalating behavior to predict violent acts by integrating training, technology and observation will increase prevention.

> "We recognized early on at our large facilities, those with over 200 people, that these organizations become organisms with changes in culture and behavior; incidents increase. Understanding how behavior will change helps us prepare for, predict and prevent incidents."
>
> ***George Booth, eBay***

While the situation in the NFL may not be directly applicable to all enterprises, the awareness and discussion it created allows the opportunity to scrutinize and update current policies and programs.

3. Technology Integration and Management

Technology integration and management appeared on the Security 500 horizon for the first time in 2012. It has remained front and center and has risen to the third-most mentioned issue this year. There are a number of factors at work here, primarily driven by risk management and security goals. And the investment and growth is significant. Simply, the security's role is too wide to rely solely on manpower. And the technology infrastructure, especially by leveraging the corporate network, has opened a new industry of automated solutions to support and enhance the mission.


$
PERSONNEL
Security Manager, Security Officers, Investigators
CPTED/ELECTRONIC
Alarm Systems, CPTED/Electronic Access Management Systems, Video Surveillance, Lighting
BEHAVIOR MODIFICATION
Security Audit, Policies & Procedures, Training, Workplace Violence Prevention, Security Awareness Programs

Graphic courtesy of William Nesbitt

The Physical Security Market by System and Services Report by Markets and Markets projects the global market for access control, IP video surveillance management software, locks, PSIM, perimeter intrusion detection, system integration, and designing and consulting will reach $88 billion by 2019. That is a considerable jump from a market currently estimated at about half that size, but not unrealistic.

Similarly, the investment in cybersecurity products and services will continue to grow. TechNavio's analysts forecast the global cyber security market will grow at 11.81 percent annually through 2018. Forecast at $67 billion by Gartner Group in 2013, that number would push the combined total of cyber and physical security spending more than $110 billion.

All totaled, physical and cyber security technology spending is big and will get bigger, worldwide through 2018.

> "We are making a concerted effort to support logical security by leveraging our intelligence and social media monitoring programs to help them protect against the threats. A second initiative is to speed identity management. And Big Data is on our roadmap. We ask 'What don't we know?' and 'How can technology help fill in the blanks?'"
>
> ***George Booth, eBay***

Here are several key factors at play in this year's Security 500 findings:

The movement toward preventive and predictive security programs:

The security mission has migrated from responding to preventing, and is moving toward predicting. Having situational awareness to identify and mitigate threats requires information. And security technology has become very good at collecting, analyzing and presenting many data points into actionable information. Thus, as long as technology supports and enhances security's mission as directed by the C-Suite, technology investment will continue to accelerate.

Tracking social media, big data and data mining are all critical to capture, analyze and act on information for the purpose of predicting events and protecting against negative events.

Where Security Lives

Security 500 Members report into or are within these departments:

COO/Operations	**22.50%**
Facilities	**17.00%**
CEO/President/Executive Management/Board/Board Committee	**16.50%**
CAO/Administration	**12.00%**
Human Resources	**11.00%**
CFO/Finance	**11.00%**
Risk/Legal	**6.00%**
Information Technology	**4.00%**

CSOs' Top Areas of Responsibility

Investigations	**97%**
Workplace Violence Prevention/Active Shooter Prevention	**97%**
Terrorism/Bomb Threats	**94%**
Physical/Assets/Facilities (Proprietary Property Not for Resale)	**91%**
Security Technology & Integration	**84%**
Weather/Natural Disasters	**83%**
Workforce/Executive/Personnel Protection/Travel Support	**80%**
Contract Management (Guards, Technology Integrators, Contract Employees)	**80%**
Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	**80%**
Risk Management Planning	**76%**
Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	**70%**
Fire	**67%**
Loss Prevention/Asset Protection of Goods for Resale	**66%**
Regulatory Compliance	**65%**
Brand Protection/Intellectual Property/Product Protection/Counterfeiting/Fraud Protection	**54%**
Political Unrest	**54%**
Global Security Operations Center Management	**52%**
International Workforce Protection and Support	**52%**
Business Expansion Support	**47%**
Supply Chain/Product Diversion/Logistics/Distribution	**32%**
Emerging/Frontier Market Expansion	**29%**
Drug and Alcohol Testing	**29%**
Cyber/Information Technology	**28%**
Insurance	**15%**

The demand for more data and analytics of EVERYTHING will continue to rise among security organizations. Security programs will rely heavily on gathering and analyzing information from the Internet of Things.

Improved cost/benefit of technology beyond security only applications:

The improvements in security technology are bringing important information through analytics, friendlier user interfaces, better price/performance and applications beyond security. The ability to apply technology for constant operations (versus only emergencies/events) is powerful. One example is using access control/ID systems and reporting to negotiate and reduce insurance rates, which are typically set by insurer estimates. Those bottom line savings impress the C-suite, offset costs and expand security's contribution.

Migrating physical security onto the network:

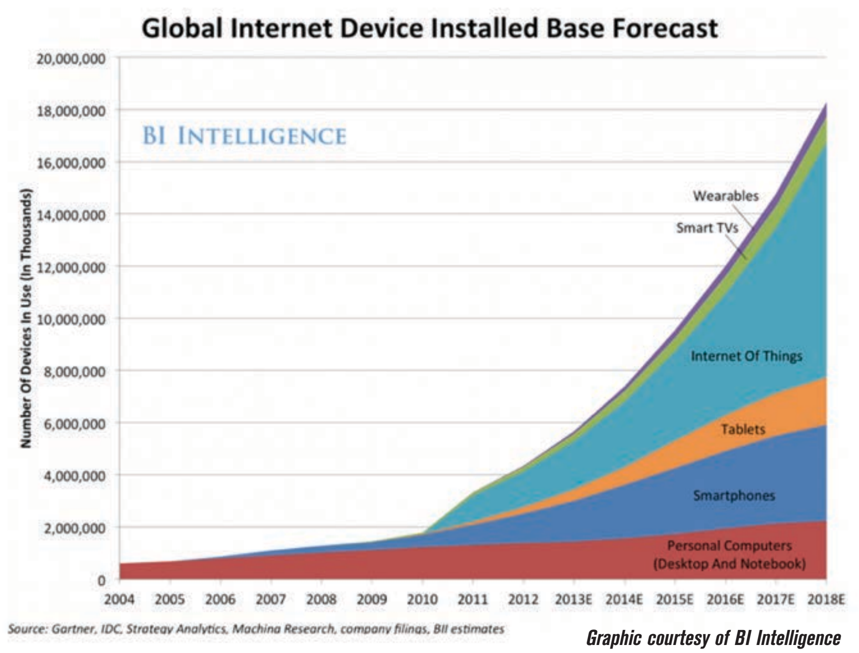
The increased role of Information Technology supporting the "security application" and moving security onto its network is driving the adoption of IP-based technologies at an ever faster pace. IT looks at technology on a "per se" basis, meaning "does this product do what it is supposed to do and solve the problem?" As a result, their participation in the acquisition and adoption of security technology products brings both immediacy and criticism to the procurement process. But the outcome is that IT is used to spending on IT and has no issue doing so for security or other internal customers to improve processes and better manage information.

Cloud Based-Solutions, Big Data and the Internet of Things:

If you use Google Maps then you may have experienced watching the roadway on the screen turn from green to yellow to red, indicating traffic has slowed and then stopped. How does that happen? There are a lot of Google users on that road, and their devices are transmitting their current position, direction and speed. As those devices slow from 50 miles per hour to 35 to 20, then the roadway colors change. That is big data, and it provides useful information, in this case, for security to help employees with travel.

> "More things are connecting to the Internet than people – last year there were more than 5 billion cellphones, 2 billion broadband connections and 1 billion people who are on Facebook and Twitter. By 2020, there will be 50 billion devices that will be connected to some network."
>
> ***Jeanne Beliveau Dunn, Cisco***

The impact of social media is already significant and will continue to grow as a first alarm for security operations centers. The opportunity to monitor social media posts, as events that may impact your organization and its people occur, is a powerful resilience tool. The vast amount of information wearable and cloud connected devices will generate will enable security organizations to better identify risks, manages events and increase resilience.



Source: Gartner, IDC, Strategy Analytics, Machina Research, company filings, BII estimates

Graphic courtesy of BI Intelligence

> "We want to be on the cutting edge of school policing by finding new and innovative ways to keep kids safe."
>
> ***Hector Rodriquez, Santa Ana Unified School District***

4. Budgets

Budget vs. 2013

	Total
Increased	65%
Stayed the Same	21%
Decreased	15%

Ultimately, value is driving budgets in 2014. Security organizations that have become trusted advisors for managing risk and enabling businesses to succeed are gaining credibility and a strong internal brand. The result is stronger financial support. In 2014, 65 percent of Security 500 members reported their budgets increased over the prior year. And that is the highest percentage of members reporting an increase in the history of the Security 500 benchmark survey.

> "Our executive leaders have consistently given us the support and opportunity to prove that security can and should bring value to the bottom line. By aligning with the long-term company and department strategy, we deliver meaningful results, and we get support."
>
> ***Vance Toler, Southwest Airlines***

The average increase was 8 percent (versus 9 percent in 2013). This is a strong jump over 2013 when 47 percent reported increased budgets. Fifteen percent reported their budgets were decreased. This is a slight improvement over the prior year survey, with 17 percent reporting reduced budgets. Those reporting a budget decrease experienced an 8 percent cut.

And fewer organizations were stagnant. Only 20 percent reported having the same budget, a significant drop from the prior year's 35 percent. Combined, 85 percent reported their budget increasing or remaining the same (versus 83 percent in 2013).

As the security profession has matured, business-minded executives have brought strong leadership and organizational skills to their enterprises. Successful leaders consider themselves a key part of the company's management team with responsibility to understand and contribute to business goals.

> "Working for a conglomerate means you will never get bored, as the environment is so diverse. Risk management is an iterative, dynamic negotiation. It requires good relationship management, marketing, and a good awareness of business objectives and risk tolerances and is a perfect function by which to explore all of the other key functions in a global business."
>
> ***Rich Mason, Honeywell***

Underlying the business goals in many sectors are compliance costs to ensure business continuity. Many sectors including connected commerce, healthcare, finance, higher education and energy, face myriad physical and cyber security requirements from government regulations. New regulations require new spending, changes to business processes, and training.

> "It is my job to understand our security costs better than they do (i.e. financial management). That allows us to gain credibility and make the business case."
>
> ***Stephen D. Baker, State Street Corporation***

There is a cost to ensuring compliance that is only overshadowed by the fear of the cost of not being compliant. In connected commerce and retail, the cost and sophistication to be PCI DSS compliance is significant. However, failure to meet PCI DSS compliance can be catastrophic. Target is facing a class action lawsuit, government fines, reduced sales volume and significant brand damage. Thus, the cost of compliance and related security budgets are being driven higher across this and other sectors.

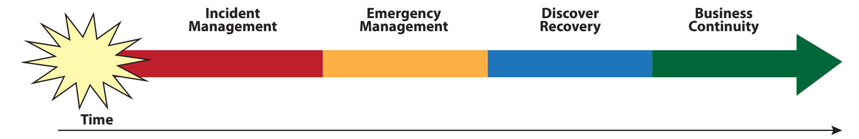
There are also compliance requirements placed on companies by their customers. More and more, security is participating in completing proposals, giving prospects tours of their security departments and engaging with customers.

Budgets are also getting support because the enterprises are not only experience security's competent work, but getting feedback in metrics and measures. Last year's Security 500 keynote theme, "Time to Play Money Ball" has borne out.

By having a strong grasp of the mission and directly showing both support for and contribution to top and bottom line goals, security is gaining additional funding by making its customers successful.

5. Business Resilience

Security magazine defines enterprise resilience to integrate business continuity, emergency management and disaster recovery. It is accepted that no matter how much preemptive work is done, events will occur. And managing in a crisis, limiting the damage and getting the enterprise's operations back up and running normally is important. From local offices impacted by weather to the global supply chain disrupted by political unrest, the expanse of issues is wide and growing for security programs to plan and prepare.



Source: Tech Target

> "It goes to the fact that every employee at every level of the enterprise takes responsibility for ensuring MITRE's security and the security of the information with which we are entrusted. It's a core part of our culture."
>
> ***Gary Gagnon, MITRE***

We have witnessed a long, slow cycle over the past century of self-reliance by stakeholders shifting to a heavy reliance on emergency responders. Currently, the integration of emergency responders and stakeholders toward risk and resilience is being employed. This integration makes resilience planning an "all hands on deck" process and the notion of the first responder has changed. Those for whom resilience programs are meant to secure are actively participating in their own safety. Across all sectors, from K-12 students rehearsing lockdowns to fans texting about other unruly fans at sporting events, no one is excluded from planning and participating in resilience.

And technology is playing an increasingly important role allowing communications through social media and mass notification systems to accelerate both the inbound fusion and outbound distribution of information. Pervasive information allows stakeholders to no longer just be bystanders, but to be actors supporting resilience programs.

While the mass participation of stakeholders and their personal technology is increasing the speed of detection and diagnosis, there is still the issue of appropriate response. Someone has to have authority and expertise to correctly respond and ensure that an event is not improperly managed or worse, that a disaster becomes a catastrophe.

Knowing both the authority (e.g. corporate security, fire department, cyber SOC, etc.) and the individual(s) is the result of strong rehearsal, typically table top exercises and communication. Getting to know one another prior to an emergency is as important as the actual plan.

> "We built a challenged security culture where security is everyone's responsibility – enlisting our 40,000 employees to be on the lookout."
>
> ***Greg Halvacs, Cardinal Health***

Response activities typically include evacuating the affected area, searching for those that need to be rescued, assessing the breadth and depth of the emergency and working to contain damage and restore operations. These activities are directed at maintaining life and regaining the emotional well-being of the impacted community.

The lack of leadership and communication during a disaster in a timely manner often leads to significant communication and operational problems beyond just the actual incident. Brand image, public relations, revenue and profit loss, legal liabilities and CEO firings are more often the outcome of poor enterprise resilience programs. Examples include Katrina in New Orleans, Virginia Tech, BP and Target, where the lack of a coordinated and timely response led to significant damages beyond the initial incident.

6. Physical Security, Crime and Asset Protection

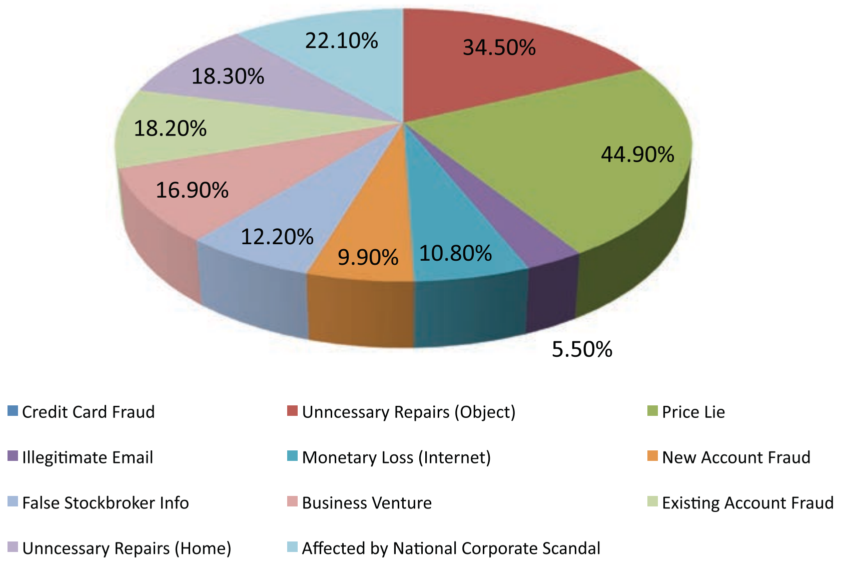
The FBI's *Crime in the United States* report for 2013 identified 7,252,652 property related crimes including larceny, robbery and burglary, totaling $15.5 billion in losses.

Enterprises (non-residential) from businesses to public schools get their fair share. Incidence of crimes in non-residential sites:

- Robbery 27.3%
- Burglary 25.5%
- Larceny 15.0% (estimated)

> "We spend a lot of times securing our parking lots. . .your Average Joe burglar has changed to where they don't spend their time robbing houses. They rob cars."
> ***Jim Sawyer, Seattle Children's Hospital***

Percentage of All White Collar Crime



Source: Project.org

Statistics are not available, but logically the dollar value of commercial enterprise asset theft has a higher dollar value than residential. Also, motor vehicle statistics include all losses and are not identified by victim (personal or commercial) in the FBI statistics.

In the retail sector, loss prevention issues continue to impact businesses despite increased investments in technology, training and tactics. The National Association of Shoplifting Prevention notes:

- More than $13 billion worth of goods are stolen from retailers each year. That's more than $35 million per day.
- There are approximately 27 million shoplifters (or 1 in 11 people) in the U.S. today. More than 10 million people have been caught shoplifting in the last five years.

> "With retail stores, you are faced with some additional challenges like shoplifting and employee theft, return fraud, organized retail crime, online fraud and traditional robberies and burglaries. Getting merchandise from Point A to B has become much more complex."
> ***Jerry Blum, AutoZone***

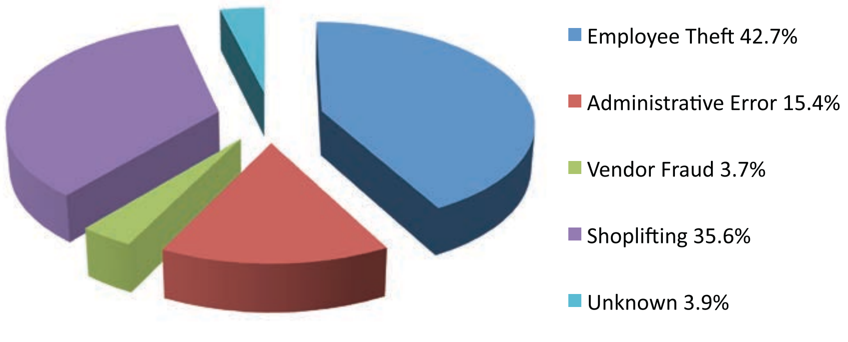
While shoplifting shrink is a major drain on retailer profits, product diversion within supply chains is also a significant challenge. Diversion criminals are typically more professional than shoplifters including members of organized crime. The typical theft is larger in both dollar value and potential brand damage. In addition to the monetary losses, failing to deliver for supply chain partners expecting deliveries to conduct business can cause the loss of business contracts. Resold products that are damaged or altered may lead to significant brand, warranty and financial losses.

Insider crime, including both physical assets and white collar theft and fraud, were noted as major areas of risk that Security 500 members are targeting to increase controls, improve audits and identify inappropriate activities that typically lead to a loss.

Corruption is also a concern as the incidence has doubled over the past two years to 16 percent, according to a report from the *EY Global Fraud Survey*. More than 40 percent of the CEOs surveyed believe that corruption and bribery are widespread within their countries. And 11 percent of the CEOs surveyed considered misstating financial performance to be a justifiable action. Only 6 percent of the overall respondents considered doing so justifiable.

> "Our security team has the opportunity to effectively and positively impact more than 1.8 million employees servicing 70 million customers around the world every single day. One of my main motivations is to ensure that our customers come into our restaurants and feel safe and secure and enjoy their meal. We have a very strong supply chain, and we have worked hard to protect our food from the farm to the fork."
> ***Dennis Quiles, McDonald's***

Sources of Inventory Shrinkage



Source: advantagepolygraphservices.com

Going the Extra Mile

Jerry Blum

Director of Security Services, AutoZone, Inc.

In more than 5,300 AutoZone stores in the U.S., Puerto Rico, Mexico and Brazil, the number one job for AutoZoners is to provide "Wow! Customer Service." And AutoZone's security focus is no different, says Jerry Blum, Director of Security Services for AutoZone. The security team's focus is on more than just customers. There are vendors, employees and other business partners, too.

To secure a business partner's needs, Blum's team will work with them to protect theft-prone products while still keeping them available to the customer with anti-theft devices or placing the merchandise in a well-monitored section of the store.

"The potential for risks like workplace violence incidents or data breaches, are not just limited to retail, but with retail stores, you face additional challenges like shoplifting and, of course, employee theft, return fraud, organized retail crime, online fraud, and traditional burglaries and robberies," Blum says. "We deal with store operations, legal, finance, HR, merchandising and the supply chain; it's just an environment where hard work and cooperation really pays off."

Blum wears many hats within the corporation, including overseeing management, operation and maintenance of all security-related equipment; business continuity and disaster recovery; security officers; corporate investigations; international due diligence; and services, including executive protection.

He has to be mindful of unique business and security challenges for AutoZone's international locations as well, advising senior management on international security issues and monitoring domestic and international travel for employees. With stores in Puerto Rico, Mexico and Brazil, as well as the U.S., he says: "We face issues of importing and the supply chain concerns – getting merchandise from point A to point B – have become much more complex. Mexico and Brazil both have some unique challenges. Each country has unique requirements, and the coordination with local authorities in the presentation of cases has presented some challenges." To address some of these concerns, Blum and his team work with the Retail Industry Leaders Association (RILA), Overseas Security Advisory Council (OSAC) and ASIS International for intelligence gathering and information sharing with other retailers, and AutoZone has a security team in Mexico that Blum describes as robust and in-tune with local issues.

Open lines of communication with employees and stakeholders is one of the keys to Blum's workplace violence mitigation strategy, including awareness campaigns and a workplace violence hotline where AutoZoners can leave confidential concerns before an incident takes place.

"As far as the C-Suite is concerned, I think they would consider our security team unobtrusive, yet highly responsive to their needs. We are engaged in all aspects of the business, and we don't impede anybody in providing great customer service," he says. In fact, AutoZone's Store Support Center's Alarm Services Group recently received one of the company's highest internal awards – the Extra Miler – which is presented to an individual or group of employees who demonstrate outstanding performance. The team earned it by implementing a new program in which some members worked three weeks straight without a day off, Blum says, to ensure that the program was implemented effectively and best served the company's purposes.

In return for their dutiful service, Blum and other AutoZone leaders work to invest back into their teams.

"We have a training department here that has a library that everyone has access to, and much of those materials are around leadership, management, effective communications and presentation skills, we expose our teams to these on a regular basis," he says. "To be a leader in this organization, you have to be committed to building a diverse and high-performance team, and we've been very successful in that. If we have an individual who is lacking in a certain area, we identify that area, address it with them, and purposefully focus on developing that necessary skill."

Within loss prevention measures and even supply chain security, crisis management is key. Blum is also responsible for emergency preparedness training, which includes tabletop exercises with every department, but the structure of the company helps as well: "We have a pretty flat structure, which allows us to be nimble and make decisions quickly and on our own. AutoZone really empowers its people. We train them to make the right decisions. We allow them to make decisions, and we support them.

"Our managers know that I'm available to them at any time and they can come to me for advice. Likewise, I know that my VP is available, and I can consult with her whenever I need," he adds.

Prior to joining AutoZone, Blum served 27 years with the Memphis Police Department, where he retired as a Deputy Chief. He has earned numerous awards, including the Memphis Police Department Medal of Valor. SECURITY

SECURITY SCORECARD
- Annual Revenue: $9.8 billion
- Security Budget: $28 million

CRITICAL ISSUES
- Cybersecurity
- Workplace Violence
- Asset Protection/Theft

SECURITY MISSION
- Insurance
- Fire
- Supply Chain
- Regulatory Compliance
- Supporting Business Growth
- Drug Testing
- "Customer Facing" Posture
- Business Resiliency

Protecting the Last Mile

Gregory L. Halvacs

SVP, Chief Security Officer Global Security, Flight Operations, Global Real Estate, Cardinal Health Inc.

CardinalHealth

The nature of providing health care services is changing, particularly as the focus shifts from hospital-based care to providing care in more cost-effective settings. The introduction of the Affordable Care Act and other key drivers are making it increasing important for health care providers, and their supply companies, to reduce costs for customers and patients, says Greg Halvacs, the Chief Security Officer and Senior Vice President for Global Security, Flight Operations and Global Real Estate at Cardinal Health, a health care services company based in Dublin, Ohio.

"The Cardinal Health tagline is 'Essential to Care,' reinforcing that we not only provide medical products and pharmaceuticals that are essential to the delivery of health care, but we also provide a broad array of products and solutions that improve the quality and cost effectiveness of care," he says.

Some of those initiatives that Halvacs provides through security include sharing contract services from national vendors for security equipment, access control and background checks. The Cardinal Health sales team also presents the company's 8,000 independent retail customers with options for continuing education classes in security solutions, which could focus on robbery prevention, risk mitigation, store security and personnel safety, for example.

"We work across the whole organization, whether it's HR, quality, legal, operations, communications, or mergers and acquisitions," he says. "We partner with them. We make sure we're at the table, and that we remain proactive. When we identify potential security issues, we sit down with leadership and educate them on what we want to do and how we want to go about doing it. I think it's very high-level and has built a lot of credibility throughout the years in the organization at all levels."

Halvacs' security team develops metrics and in-house case studies to help sell their case to the C-Suite, as well as to educate different business units about emerging risks.

> **"We have disaster preparedness plans in place to ensure that all of our customers can always receive the medical and pharmaceutical supplies their patients need."**

But it's not just the C-Suite that is being educated about security measures – Cardinal Health's security team recruits its 40,000 employees to be on the lookout: "We are building a culture where security is everyone's responsibility. We constantly get reports from the field, reporting suspicious activity."

A part of that effort's success is Cardinal Health and the security team's commitment to hiring the very best security talent. The enterprise's background check and drug testing program was recently centralized under one individual, and the company switched methods from urine analysis to hair testing to mitigate the possibility of cheating on drug tests. Halvacs can also depend on security and compliance coordinators at each of Cardinal Health's 400 global locations to implement policy processes across the enterprise, including a company-wide technology upgrade on security systems three years ago.

As a supply chain-based enterprise, Cardinal Health has to protect products "to the last mile," Halvacs says. "Our drivers deliver products to thousands of points of care every day. Because of the levels of products we carry, sometimes they're targeted for theft, so we're always looking at how to prevent theft within the supply chain, especially on the last mile – the last point to the customer, whether it's a chain pharmacy or an independent retailer or hospital."

To best mitigate the risk to the last mile, Halvacs and his team use CAP Index ratings and predictability modeling, as well as extensive awareness training of driver surroundings, including if they're being followed.

Halvacs says that the strength and reliability of Cardinal Health's supply chain services are perhaps most evident when disasters – like tsunamis, floods, tornadoes or hurricanes – strike. "We have disaster preparedness plans in place to ensure that all of our customers – particularly hospitals and retail pharmacies – can always receive the medical and pharmaceutical products their patients need, even in times of disaster. Through our global command center, we track the T-minus schedules for hurricanes, and our regional teams assist with monitoring weather and wild fires. We make sure that our four distribution centers are fully stocked, so we have the capability and agility to respond throughout our network."SECURITY

SECURITY SCORECARD

- Annual Revenue: $91 billion
- Security Budget: Confidential

CRITICAL ISSUES

- Asset Protection/Theft
- Crisis Management
- Fraud/IP Theft: External, Partner and Insider Threats

SECURITY MISSION

- Insurance
- Cybersecurity
- Fire
- Supply Chain
- Regulatory Compliance
- Supporting Business Growth
- Drug Testing
- Risk Management Planning

Unique-ness

Gary Gagnon

Senior Vice President and Chief Security Officer, MITRE Corporation

MITRE

Many organizations protect their cyber infrastructure by looking inward, focusing on their own networks and systems. They dedicate themselves to reducing the attack surface, assessing their vulnerabilities, and conducting system patching – all to continuously monitor their own networks.

To Gary Gagnon, senior vice president and chief security officer of the MITRE Corporation, this defense posture makes about as much sense as having Tuuka Rask turn his back on the opposing team during the Stanley Cup playoffs. Rask, the star goaltender for the Boston Bruins, doesn't fend off slapshots by staring at his own goal's crossbar or checking the durability of the net. He focuses on his opponents, watching as their playbook unfolds, identifying their weaknesses and signaling to his teammates for backup.

Gagnon thinks this strategy can be just as effective in protecting cyber assets. "Initially, we were like a hockey goalie facing the net instead of watching the threat. By turning around, we get to work on knowing the opponent, understanding their moves. We are able to balance security against threats. Our defenders become collectors of information and intelligence to build a defensive strategy and optimize response," he explains. "Learning as much as possible about the adversary's tactics and techniques gives us an edge in discovering and stopping attackers."

As the director of cybersecurity at MITRE, Gagnon plays a key role in guiding the defense of some of the nation's most critical cyber assets – those of the Federal Aviation Administration, the Department of Defense, and the Department of Homeland Security. He has unique insights into his client base, having held leadership positions in solving information security issues for the U.S. Army, U.S. Navy, and National Security Agency.

MITRE is a not-for-profit organization that operates federally funded research and development centers (FFRDCs). Government agencies establish FFRDCs to address specific, long-term needs that can't be met by in-house staff or traditional contractor resources. In this capacity MITRE plays a unique role as a trusted adviser to both military and civilian government agencies.

For Gagnon, earning and preserving that trust means never recommending any cybersecurity capability or approach to a sponsor that hasn't first been tested on MITRE's own computer networks and systems.

"We realized that we needed to run our network security solutions here to understand and prove them out before taking them to our government sponsor customers," says Gagnon. "That way, we practice what we preach and we preach, what we practice."

MITRE's approach to cyber defense is based on the "kill-chain" framework, originally developed by Lockheed Martin. The kill-chain depicts the phases of a cyber attack, comprised of a series of steps that an adversary might take to compromise, control and exploit a target.

By better understanding adversaries – their tendencies, techniques, tools and intentions – organizations can bolster their threat-based defenses and improve their chances of preventing, detecting and mitigating cyber intrusions.

"MITRE adopted the ideas, practiced them, added to them, and started talking about them, and promoting them with our sponsors," says Gagnon.

In fact, MITRE offers many ways to help sponsors adopt this more proactive stance. For instance, it helps diverse stakeholders create partnerships for sharing detailed cyber threat information, which can then be used to improve the defense capabilities of each individual member. Partnerships also give members tools and strategies they might not otherwise have access to.

In keeping with his commitment to "practice what we preach," Gagnon test ran this integrated approach to intelligence- and resource-sharing at MITRE before bringing it to clients. One of his first moves as CSO was combining MITRE's physical and information security divisions, a departure from industry standard. "These functions cannot and do not operate independently," he says. "They're all part of a security ecosystem."

This security ecosystem consists of a highly capable and motivated team. MITRE relies on an all-inclusive approach, in which every security team member can manage, rather than just route, an issue or inquiry through to resolution. "We work as risk management advisers for the organization," notes Gagnon. "Our value is rooted in continuous improvement, sharing what we learn and changing thinking about security to a threat-based defense model."

To share information across an entire community, there needs to be a common language and Gagnon has led MITRE's efforts to establish and communicate software industry security data standards to fortify vendor products against vulnerabilities.

To fully understand the critical needs of his sponsors, Gagnon focuses on customer engagement. "At MITRE, we view security as a team sport and operate as a team," he says. "It's the only way to gain adoption across our various organizational departments, understanding client issues and demonstrating due diligence to ensure success." SECURITY

SECURITY SCORECARD

- Annual Revenue: $1.7 Billion
- Security Budget: Confidential

CRITICAL ISSUES

- Brand Protection/Intellectual Property/Product Protection/Counterfeiting/Fraud Protection
- Business Expansion Support

SECURITY MISSION

- Asset Protection/Theft
- Enterprise Resilience
- Fraud/IP Theft: External, Partner and Insider Threats
- Regulatory Compliance
- Risk Management Planning
- Supporting Business Growth
- Supply Chain
- Technology Integration and Management
- Workplace Violence

Ambassador for the County

Kirk D. Simmons

Security Manager, Hennepin County

"Being a government organization that services every facet of the public, there is a whole host of different scenarios that take place on a daily basis," says Kirk Simmons, Security Manager for Hennepin County in Minnesota. "There are occasions where people are getting their kids taken away from them or they're being told they need to pay a lot of money in taxes. So, for them, it's not a really pleasant experience all the time. So, as the security department, we want to ensure that employees and the people utilizing our services can do so in a safe manner. We're there to protect them and make sure they do what they need to do and get home safely."

Hennepin County has more than 100 buildings in its system, including libraries, service centers ("A one-stop government shop" that include vital records, taxpayer services, DMV, passports, etc.), health services, courthouses, and other government facilities and offices. For the past eight years, Simmons has been the Security Manager for the County, and he has seen the security department grow from a necessary evil to a legitimate partner in the local government.

"When I first started with security in Hennepin County, people just came into work for a bad day, and that was pretty much it," he says. "Nobody really understood what it meant to formulate a mission and establish long-term goals, and work towards those goals, adjusting them along the way to make sure they met with where the country was going."

Simmons, who earned a Master of Arts degree in Organizational Leadership from Bellevue University (Nebraska), aimed to change that mentality to a proactive security strategy. For example, he is boosting his staff's potential by exposing them to a variety of organizational leadership and security material, which they discuss on a regular basis.

"We set aside time to discuss these principles, and we use them when we plan out our mission for the next three- or four-year period to establish guidelines for where we need to go and where we should be from a professionalism standpoint. We also look at our training components to make sure that they're applicable to what we're currently responsible for.

> **"I don't view ourselves in a security organization as a 'necessary evil,' but more of a real partner in being able to help deliver those services."**

"People are becoming more familiar with my expectations, and I'm feeling that they're growing beyond that now, taking the initiative to know what our overall security mission is and being able to articulate that with our training."

Security employees have a minimum of first responder training, and they provide services above and beyond the typical call of duty, including escorting litigants to and from their vehicles if requested, security planning for events and ID badging responsibilities.

Hennepin County security training extends beyond the department also, as workplace violence is one of the main risks facing Simmons' team today. They provide basic personal safety training and conflict resolution training for employees, especially for those who deal with confrontational situations daily.

"It seems to be inbred in the culture these days that if people don't get what they want, they have a tendency to lash out physically," Simmons says. "It's in our best interest to make sure that all the employees know as much about these solutions as possible. These educational tools help them negotiate through some of the really difficult situations, so they minimize the amount of risk to them and the amount of risk to us as first responders."

Departments in Hennepin County are run almost as their own independent business units, and security training requirements are at the discretion of each department head. Some have more participation than others (service center employees, for example, are well-versed in de-escalation methodology now), but employees are able to access training on their own, if they prefer, through the County's training website.

"I feel as though it's a good idea to get as many frontline staff members to these training sessions as possible – it will help them be able to do their jobs better, so customer service rankings will reflect more positive experiences, and employees will be able to work in a safer environment."

"I don't view ourselves in a security organization as a 'necessary evil,' but more of a real partner in being able to help deliver those services to the residents of the county and to the employees. When people walk in to work or to get their services, if they see a security officer standing there, they feel safe. We're there to be ambassadors for the county – giving directions, providing services – simple as that."

Before joining Hennepin County's security team, Simmons was the Corporate Loss Prevention Manager for Musicland Stores Corporation. He has also served both reserve and regular in the United States Marine Corps as a Military Policeman. *Security* thanks him for his service. SECURITY

SECURITY SCORECARD

- Annual Revenue: $1.9 billion
- Security Budget: $5.6 million

CRITICAL ISSUES

- Workplace Violence
- Service Coordination
- Resource Allocation

SECURITY MISSION

- Insurance
- Cybersecurity
- Fire
- Supply Chain
- Supporting Business Growth
- Risk Management Planning
- Asset Protection/Theft
- Terrorism

Learning Self-Reliance from Isolation

Alexander S. Ubiadas, Jr.

Emergency Management Staff Officer
Board of Water Supply, City and County of Honolulu

BOARD OF WATER SUPPLY
CITY AND COUNTY OF HONOLULU

As Hurricane Iselle barreled down on the island of Oahu in early August, Alexander Ubiadas was prepared. He had already invested in ruggedized security equipment at isolated facilities, built long-term recovery plans and worked with his staff to get facilities as ready as possible for the storm. Because while people might survive for a while without electricity, they truly need safe, clean water, no matter the weather.

Ubiadas is the Emergency Management Staff Officer for the City and County of Honolulu's Board of Water Supply, where he and his team are responsible for protecting the clean water infrastructure for the entire Island of Oahu, which includes thousands of miles of pipeline, thousands of assets, more than 300 facilities, 600-plus employees and hundreds of daily visitors. In order to secure this infrastructure, Ubiadas relies on advance information and threat awareness, because often help is thousands of miles away.

"We have to be very self-reliant, especially here in Hawaii, and we're able to do that because our water sources are here, and this tropical environment allows for recharging of the aquifers," Ubiadas says. "It's a noble cause doing security in such an isolated area because I can't rely on someone next door. I can't rely on anyone other than who I've got. … If there's a catastrophic incident, we have agreements that we can use, but it's going to take them a while to get here. The longer it takes for either an investigation to happen or for some kind of response team to arrive, the longer people have to wait for restoration of water services or, just at the very least, where we can guarantee the quality of the water that's being provided."

And while Ubiadas might not be able to prevent natural disasters, he and his team can work to mitigate other threats. He works with neighborhood watch groups and local security associations to stay tuned in to what's happening on the island and what trends to watch for, in addition to internal security measures and awareness programs.

> **"It's a noble cause doing security in such an isolated area because I can't rely on someone next door."**

Board of Water Supply personnel in the field are taught what constitutes suspicious behavior and how to report it. In-house and contracted security officers patrol the facilities and areas regularly. Deterrents include signage, random anti-terrorism measures, decoy police cars and cameras, and electronic security measures. Chain link fences are being replaced by expanded metal fences with razor-wire at the top to help further discourage intruders.

"We'll provide personal protection for employees going into high-threat or very secluded areas where we have many of our facilities, where there might not be anyone around if they call for help. We also give employees resources, such as referrals to self-defense classes, if they're truly concerned about their safety," he says.

"A lot of our work is done behind the scenes, and that can lead to some people not seeing the value of security, because we try to conceal it when we use anti-terrorism measures, trying to prevent incidents, and so it doesn't affect operations, cause panic or delays."

In order to sell security as more than just an insurance policy, Ubiadas and his team work up case studies from other municipalities to share with city officials, or build metrics on investigation close rates, or reductions in intrusions after changing the fencing (a 99- to 100-percent reduction so far, Ubiadas reports) or other security measures.

"Once we successfully sell the security brand, people are very appreciative; they like the concept of what we're doing, and they want us to do more. They look to us as subject matter experts, and they recognize that we have the knowledge, experience and capability that we can provide on an as-needed basis if something arises," he says. "They recognize that they can call us for personal security advice instead of the police. They start to understand our mission as a security and emergency management resource, and then they start to change their direction and have a more positive attitude toward us.

"The key is in giving them the 'What's in it for me,'" Ubiadas adds. "That's what gets them on board to help us all succeed."

Prior to joining the Honolulu Board of Water Supply, Ubiadas was a full-time emergency manager with the Hawaii Air National Guard and served in several positions, including being deployed in support of Operations Iraqi and Enduring Freedom. *Security* magazine thanks him for his service. He is married and has one son, and in his free time, he can be found practicing his marksmanship or spending time with family. SECURITY

SECURITY SCORECARD

- Annual Revenue: $186 million
- Security Budget: $1 million

CRITICAL ISSUES

- Physical Security
- Cybersecurity
- Insider Threats

SECURITY MISSION

- Insurance
- Fire
- Supply Chain
- Regulatory Compliance
- Supporting Business Growth
- Drug Testing
- "Customer Facing" Posture
- Risk Management Planning

The Ultimate Security Strategy – Embracing Authentic Customer Service

Jim Sawyer

Director of Security Services, Seattle Children's Hospital

Seattle Children's
HOSPITAL • RESEARCH • FOUNDATION

Jim Sawyer has a lot of "friends for life" at work. Some of the "friends" Sawyer has made were at one time hostile, angry and frustrated clients, people tested by enormous stress levels.

Jim Sawyer is Security Director for Seattle Children's Hospital, a 250-bed children's hospital in the Laurelhurst neighborhood of Seattle, which is currently ranked as one of the top 10 children's hospitals in America by *U.S. News & World Report.*

Sawyer and his team work every day in the hospital's open environment to diffuse and support many hostile and angry parents who are frustrated by life's recent events. Those frustrations include but are not limited to money challenges, debt, bankruptcy, family strife and having a sick child.

Sawyer has many methods that helps him "make friends" and to diffuse many hostile situations. "Our security team uses a term called 'restatement for clarification,' which is paraphrasing," Sawyer explains. "We listen to people's complaints and restate what they've told us. Some people are stunned that they are being listened to versus having summary judgements made about them. By listening, we have the opportunity to build true rapport and have a 'friend for life.' Many of our new-found 'friends' were people who were initially hostile, if not threatening."

Workplace violence is a recognized hazard in the healthcare industry. It can affect and involve workers, clients, customers and visitors. It ranges from threats and verbal abuse to physical assaults and even homicide. In 2010, the Bureau of Labor Statistics (BLS) data reported healthcare and social assistance workers were the victims of approximately 11,370 assaults by persons – a greater than 13-percent increase over the number of such assaults reported in 2009. Almost 19 percent of these assaults occurred in nursing and residential care facilities alone.

Sawyer says that this is his greatest security challenge, and he trains his staff to deescalate as much as possible. "A lot of clients in hospitals aren't exactly refined, sensitive intellectuals. But if their child is sick, they are totally focused on their child, and we want to support them during that difficult time. I hear a lot of security organizations stress, 'We have zero tolerance.' Well, that's nonsense. It's a reactionary term. For healthcare, that's toxic. You don't want that. And we tolerate a lot, which we should. We get spit on, sworn at, cursed at with some frequency. And that's because people are under stress. What we want is 'zero incidents.' You don't want anything bad to happen. And that's how you have to build your program on a 'zero incidents philosophy.'"

His staff of 75 proprietary security officers is trained in customer service while quickly taking a thorough assessment of the client and the situation. "Our security officers are more about supporting people in crisis and treating people well than being an enforcer," Sawyer explains. "If someone asks for help, we never turn them down. And the same time, with a smile on our faces, we're doing a quick risk assessment to determine what, if any threat, they are to our hospital, patients and staff."

"You have one shot to make a good first impression, and we work very hard on that," Sawyer adds. "We issue 1,500 photo ID badges every day. We greet people at the hospital entrance, and we authenticate whether they belong here. And then if they are lost, we will walk them to their destination. We don't want to become an Orwellian nightmare for somebody. But when they walk into the entrance of the hospital, they will find us."

An additional area where Sawyer and his team have focused attention is the hospital parking lots. "We spend a lot of time on parking lots, because parking lots are inherently unsafe for many reasons. They are convergent zones for bad things like domestic violence and assault. In addition, your Average Joe burglar has changed to where they don't spend their time robbing houses. They smash and grab cars. Our outside presence pays off."

Sawyer examines security incidents on a monthly basis and assesses the success of the situation based on the resolution, with the goal always being a non-violent resolution. "We are fairly self critical and for a reason. Too many organizations drink their own Kool-Aid, so to speak, and never examine their practices and behaviors. That is all things wrong. Organizations need to ask 'Are we a just culture?' and 'Do we make mistakes that anger people?'"

The hospital emergency room continues to be a challenge at Seattle Children's, as it is with most hospitals. "People are in crisis," he says. "Often, people come in, and they think their child is much worse than they are. We also see more cases of self-injurious children. Twenty-five years ago, I would see maybe one child a month come in who was self-injurious. Now we sometimes see five to 10 a day. That is quite a concern."

The bottom line with his security strategy and risk mitigation, Sawyer says, is customer service. "It sounds basic, but if you're working with the public, train your staff to make good first impressions, to deescalate a situation, to read body language, to read verbal and non-verbal cues and ultimately to treat people right. If you can do that, you can move mountains." SECURITY

SECURITY SCORECARD

- Annual Revenue: $1.665 Billion
- Security Budget: $3 Million

CRITICAL ISSUES

- Workplace Violence
- Staffing and Training
- Patient Behavioral Health and Violence

SECURITY MISSION

- Active Shooter
- Drug and Alcohol Testing
- Enterprise Resilience
- Physical/Assets/Facilities
- Regulatory Compliance
- Security Technology and Integration
- Weather/Natural Disasters

Life Happens Here

John Dailey

Chief of Police,
Duke University
and Duke University
Hospital

Duke
UNIVERSITY

And Duke's security team assures it. "Thinking about the higher education and healthcare facilities at Duke, it is amazing what occurs on a given day. Students learn something that will change their life. Another person's life will be saved at the hospital. A researcher will make a discovery that changes quality of life for others. There may be a wedding in the chapel. There is a high likelihood Duke will compete for or win a national sports championship. And we have celebrity speakers and lecturers visiting frequently. This is a very rewarding, exciting and dynamic environment," Chief Dailey explains.

The security team at Duke is all about higher education above the surface, and they work to keep law enforcement below the surface. "We continue to focus on customer service for all the stakeholders on our campus. Duke is consistently named a top 10 institution and high quality service is expected from every department, especially security. The mission is a successful and positive experience for every person that visits Duke."

Duke ensures that their team members are highly trained in necessary law enforcement and emergency management skills. At the same time they focus heavily on emotional capabilities. "We emphasize empathy so our officers see things the way the student, patient or victim sees them. We look hard at emotional intelligence during hiring and promotions. We work to hire the people who fit into the culture and are able to manage the environment. This can be very challenging, and we discuss it all the time," Dailey says.

At the same time, the regulatory landscape in higher education is evolving. The Clery Act is being expanded to record additional crimes. Dailey works closely with IAHSS for the Duke University Hospital and is working towards accreditation for their police department.

Security's mission is to help create an environment for world class education, research, healthcare and entertainment. Simply stated, without a secure environment, Duke cannot be Duke. And Dailey recognized early that a secure environment could not be created alone.

> **"Security is in front of every college leader today."**

"We partner with the Office of Information Technology and are developing comprehensive technical security plans. There are now templates across similar facilities. For example, our data centers, and physical plant (critical dependency facilities) have one level of security. Residence Halls have another," explains Dailey.

Human resources provides background screening and intervention to stay in front of potentially threatening behavior. "We work to educate others to recognize and report concerning behavior. We have three teams of highly skilled, cross-functional professionals that comprise our Behavioral Assessment Teams that work with students, employees and patients, as required. And the Environmental, Health and Safety department manages fire protection, but we are the first responders. Hence we coordinate and drill closely to be prepared," he adds.

Students are engaged in their own safety, as well, as additional federal regulations are making safety programs mandatory on college campuses. During the first week all new students are required to attend a security session and to attend follow up programs held by peers including resident advisors, student groups and graduate students.

Dailey's team also offers prevention awareness programs that students and employees may attend based on personal interest. Among the most popular are active shooter and the Citizen's Police Academy which receives six times the applicants as there are seats available.

Chief Dailey joined the Duke Police department as an officer after six years in the U.S. Army. He moved into a management role at Duke, was recruited to North Carolina State as Assistant Police Chief and then returned to Duke as the Chief in 2009.

"This is a fast changing and highly dynamic profession. Security is in front of every college leader today. We get tremendous support from leadership with both vocal and financial recognition. We meet with student and employee groups and ask how they feel about their safety and get ideas. We listen well and are highly responsive. That makes a big difference," says Dailey.

At the heart of Duke's program are the highly dedicated professionals who are passionate about service and very connected to the culture and helping it achieve its goals. "We work at it every day," adds Dailey. "When we have a day without fear or incidents, we allow Duke to do what makes Duke great. That is the expectation. That is the mission." SECURITY

SECURITY SCORECARD

- Annual Revenue: $4 Billion
- Security Budget: $12 Million

CRITICAL ISSUES

- Workplace Violence
- Security Technology and Integration
- Affordable Care Act

SECURITY MISSION

- Active Shooter
- Asset Protection/Theft
- Behavioral Health and Violence
- Enterprise Resilience
- Fan Violence
- Loss Prevention/ Asset Protection of Goods for Resale
- Player Misconduct
- Risk Management Planning
- Sexual Assault
- Weather

"Hope" is Not a Plan

Hector Rodriguez, Ed.D.

Chief of Police, Santa Ana Unified School District Police Department

Chief Hector Rodriguez believes so much in the Santa Ana Unified School District (SAUSD) and the safety of the children who attend SAUSD schools that he sends his own children to school there.

"We are protecting very valuable assets – children," he says, "so one of the things that I did was enroll my sons in the school district. This a very challenged district with its share of community issues and under-resourced agencies, yet I brought my two boys here to make the point that we trust our officers with the most valuable things that parents have."

The Santa Ana Unified School District Police Department is a school district in Orange County, California, that serves the city of Santa Ana. Although its geographic size is only 26 square miles, it is the sixth largest school district in the State of California with approximately 58,000 students.

Chief Rodriguez has worked to not just teach his 26 officers (eight of whom are school resource officers) about safety; he has taught prevention and intervention strategies as a means of addressing school security problems.

He understands a police agency's constantly evolving role in the community. He has more than 26 years of law enforcement experience, 23 of which have been in the area of school policing. Prior to his selection as Chief, he was a member of the Los Angeles School Police Department (LASPD) for more than 22 years, with his most recent assignment as Deputy Chief of Field Operations; a command of approximately two-thirds of the 360 sworn officers.

Other assignments included overseeing the LASPD's Communication Center, as well as canine operations, firearms training, motors and the technology unit. In addition, Chief Rodriguez also has significant operational experience at the executive level of police administration including internal investigations, audits and strategic planning. He also served as a full-time, as well as a line reserve police officer with the Los Angeles Police Department (LAPD). He holds master's and doctorate degrees in Education from the University of Southern California.

"We are working at creating the safest possible campuses," he says. "We are not focusing solely on enforcement, but also on prevention and intervention. We realize that we help shape our kids' views about police officers and government in general, based on our contacts with them. We strive to engineer trust and build collaboration. We are very well prepared to respond to active shooter events, but more importantly, we want to ensure as much as possible that we get to the child before he or she gets to that point of wanting to cause harm."

"Our schools are not violent, but we recognize that some of our schools are located in socio-economically challenged areas with a higher rate of crime issues. Occasionally, some of these issues will spill on to our campuses," he adds. "So our officers need to know what's going on in the neighborhoods."

One area of attention in the media, with regards to school security, is arming school resource officers. SAUSD's school resource officers are armed. "It's an unfortunate necessity. They have to protect the students and themselves. There's no question. You cannot have a police officer on a campus that is not armed. We hope that they don't have to use their weapon, but hope is not a plan. We are not arming teachers, though; teachers are there to teach and protect our children, but they don't have the same mindset or level of training that we do with regards to the use of a firearm as a defensive tool."

Armed or not armed, Chief Rodriguez says, is not the focus. Instead, it's training his staff to be completely engaged on campus to build trust. "The more trust that students have in our officers, the more information they will receive about gangs, theft and at-risk students who can cause problems."

He aligns his outreach efforts with the goal of closing the achievement gap within the district, helping to push higher graduation rates and getting more kids to attend college. "If you approach the problem from that perspective, you are solving a lot of community crime issues," he says. He does so by sending his staff to training beyond tactical mandates and giving them classes on understanding the development of the teenage brain. "A teenager does not have fully developed rational thought processes," he adds. "Our officers need to understand this in order to better engage young adults who are still developing as human beings."

Another type of training is how to address runaways from a counseling perspective and to give parents resources that can impact the quality of life on campus. He stresses: "We have a daily opportunity to impact a young person's life. I talk about that every day. If we do our job right, we will have an impact on the community crime rate because our kids will graduate."

All of his officers will receive EMT training this year, further perpetuating the idea that they are there to help and support students and not necessarily be just an enforcer. While he has support from parents and the school board, he does admit that there's a challenge to measure prevention. "If there's no crime, people assume that you don't need the resources that you are asking for. But that's when you really need them because you are making a difference." SECURITY

SECURITY SCORECARD

- Annual Operating Revenue: $505 Million
- Security Budget: $7.2 Million

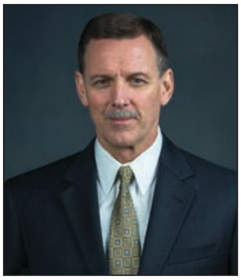
CRITICAL ISSUES

- Increase in Crimes
- Providing Relevant Threat Assessment Training to Officers and Changing the Mindset from Reactive to Preventative/Predictive
- Civil Activism/Demonstrations

SECURITY MISSION

- Active Shooter
- Asset Protection/Theft
- Contract Management (Guards, Technology Integrators, Contract Employees)
- Enterprise Resilience
- Investigations
- Security Technology and Integration
- Terrorism
- Workplace Violence

Common Ground in Different Perceptions of Security



Vance Toler

Director of
Corporate Security,
Southwest Airlines

"At the heart of our mission at Southwest Airlines is an unrelenting dedication to deliver the highest quality of customer service in the industry. After all, we're in the service and hospitality industry. Our purpose is to connect people to what's important to them in their daily lives. In order for the security team to make a meaningful contribution to the success of the company, we can't deviate from those core beliefs." This is the mission statement of Vance Toler, the Director of Corporate Security for Southwest Airlines.

Toler, who has been with the company for nearly 20 years, refuses for security to be a roadblock to Southwest's growth or to hinder its excellent customer service for more than 100 million passengers who fly Southwest annually. Having the reputation of being a department of denial can be "a common albatross hung around security's neck," he says. And he and his team work hard to avoid that reputation in the enterprise.

"One of the most important attributes of a successful security organization is you have to be first and foremost viewed as a trusted business partner. We have achieved that over a period of time by consistently demonstrating that we know our business; we know the company's direction; we know each business unit's operation. You can't make recommendations for security programs or provide council or guidance that has any value unless you understand not only what problem needs to be solved, but how it fits within that organization."

"We align our goals to the company's," Toler says. "And then at the end of the day, we have to deliver meaningful and measurable results and produce effective security strategies. We have to walk the walk and talk the talk. For security organizations to demonstrate true value, you also have to be proactive.

"Proactivity comes in many forms," he continues, "whether it's getting out in front of your employees and developing meaningful education and awareness programs, or developing risk assessment protocol and processes aimed at mitigating known or evolving threats across the system, or partnering with leaders and employees to solve unique problems. You have to achieve those things before you'll be looked at as anything more than a reactionary department."

As Southwest Airlines expands to international service, especially, proactive security strategies are key to assuring the business, Toler says. New routes to the Caribbean and Mexico bring opportunities for business expansion, as well as some additional risk, but the prospect is not an unwelcome one for Toler.

"We focus our resources on areas we determine pose the greatest potential for loss, or brand impact. Right now, international security is top on our list, which includes developing an effective travel risk management program for our employees who are going to these new international destinations. We're learning along the way, and it's obviously exciting from an operational standpoint, a revenue standpoint, and, believe it or not, a security standpoint."

One key is to keep stringent security, often put in place in an effort to stamp out risk, from bogging down agile business practices: "Anyone – any security leader or security department – can stop theft," Toler says. "But if we shut down the operation to do so, obviously that approach is ineffective and unreasonable. So we do our best avoid the strategy of 'no.' We approach the table with the attitude of how can we make this happen within the organization's business units' needs, and develop an effective and sustainable solution that will still address the threat or risk. It has to be a balance. Departments lose credibility when they don't keep that balanced approach in mind."

Safety is the airline's number-one priority, and Southwest looks at risk management as an enterprise-wide initiative, so assessments are coordinated with other business units. Under Toler's leadership, security at Southwest Airlines has positioned itself as a collaborator and an enabler of business, not a blocker, which in turn has opened many doors for the security team to succeed.

"Everyone at the table has a different perspective of security and risk, and they often apply a different level of importance to what you're recommending based on how they perceive the risk. If the objective is perceived as unnecessary, it will be viewed as having high risk, low returns. Others who perceive it to be needed will view it to have both high returns and lower risk. We have to understand what is being asked, and when possible, try to meet in the middle.

"I think our biggest contribution, of which there are many from my great team, is day in and day out coming in with the approach of 'We are here to help,' to enable the operation to move forward while mitigating the identified risk."

Toler joined Southwest Airlines in 1995 as a Fraud Investigator to create and implement the Finance Investigation unit. He lives in Keller, Texas, with his wife, Debbie, and daughter, Sydney. SECURITY

SECURITY SCORECARD

- Annual Revenue: $17.7 billion
- Security Budget: $3.5 million

CRITICAL ISSUES

- Enterprise Risk Management Enhancement
- Employee Travel/Kidnapping & Ransom
- Maintaining Awareness

SECURITY MISSION

- Insurance
- Cybersecurity
- Fire
- Supply Chain
- Supporting Business Growth
- Asset Protection/Theft
- Enterprise Resilience

From Farm to Fork

Dennis Quiles, CPP

Director of Global Security, McDonald's Corporation

Since 1955 McDonald's has been proud to serve the world some of its favorite food. Along the way, McDonald's not only lived through history, but created it: from drive-thru restaurants, to Chicken McNuggets, to college credits from Hamburger University and much more.

Dennis Quiles, a U.S. Army veteran, is Director of Global Security at McDonald's Corporation, where he has served for the last 18 years. A 34-year veteran of the protection business, Quiles is an acknowledged professional in physical security, hospitality, corporate security and casino surveillance.

"We deliver leadership and safety and security solutions to our global partners while supporting the organization's strategic business plans. We uphold our core business values and protect our most valuable assets which are our customers, people, products and brand," he explains. Most McDonald's restaurants are individually owned and operated so Quiles and his team serve as a resource and work to convey security best practices to franchisee- and company-owned restaurant managers across the globe.

Quiles' role also involves functions for physical security for the corporate and regional offices and supporting a team of security managers around the world. The department's success is due to the undivided collaboration of the Home Office Global Safety and Security Team: Jim McHenry, Director of Global Safety; Filippo Marino, Director of Intelligence and Executive Protection; Cory Keith, Meetings and Events Security Manager; and the strategic direction of the Global Safety and Security Vice President, Michael Peaster.

"The global security managers do the same type of work for their restaurants at the regional or country level that we do here," Quiles says, "they protect the employees, the brand and the business."

His relationship with the McDonald's C-Suite is "a procession of trust and mutual cooperation," he says. "We are viewed as business partners because we influence and provide support to the organization including supporting the organization's business plans and goals. We actively collaborate with McDonald's intelligence managed by Senior Intelligence Manager, Ryan Long. Ryan's team provides us with actionable intelligence to work with management to ensure that they are well informed. Some of the information is comprised of global safety and security related trends and issues that may impact the system and business strategies going forward."

Quiles' peers share a "mutual perception; they look at McDonald's Security as collaborators," he says. "We work with industry subject matter experts and federal and local agencies to enable mutual cooperation and to develop sustainable networks. The focus of McDonald's Security is to provide restaurant staff with tools that help them understand the safety and security guidelines developed to provide a safe and secure working environment."

Global Security's proficiency becomes evident through several initiatives including McDonald's worldwide scorecard, owner/operator and customer comments and industry surveys. "The data is very helpful," Quiles says, "and of course, we are always reviewing our practices to improve the system, and I wouldn't have it any other way because the information provides us the opportunity to enhance our services and see how everyone is looking at us rather than just looking in the mirror."

McDonald's operations management is most proud of its food, so Quiles and team contribute to keeping the supply chain safe and effective. "We strive to work with suppliers, owner/operators and crew who tirelessly work around the clock to ensure that we provide fresh and safe products for our customers. That's our goal. We have a very strong supply chain, and we have worked hard to protect our food from the farm to the fork."

Quiles is quick to appreciate the opportunities that he's been given to succeed so he works to mentor and support future security professionals. "First, we make sure that the candidate can do the job. We don't hire based on the fact that someone likes the person," he says. "It is because that person holds the management and technical skills and has what it takes to manage the position. Then we mentor by discussing development opportunities for future growth. We also help our global security managers with their development programs and talent management when appropriate. We pride ourselves in providing assistance. On many occasions it's about what the person's experience would bring that will enhance the system. We hire the individual that is prepared to meet the challenge, has the right attitude, skills and personality for the job."

"I have truly enjoyed my role over the past 18 years," Quiles adds, "in part because of the opportunity to work with so many diverse cultures and the development opportunities that have arisen from operating in 119 countries. McDonald's Global Safety and Security professionals have the opportunity to effectively and positively impact the system and the 70 million customers around the world that choose McDonald's every single day. One of our department's main objectives is to ensure that when our customers come into our restaurants they feel safe and secure. Our company's goal is to ensure McDonald's remains a place that you can bring your family to have a comfortable and enjoyable dining experience." SECURITY

SECURITY SCORECARD

- Annual Revenue: $26 Billion
- Security Budget: Variable

CRITICAL ISSUES

- Customer and Crew Safety
- Cybersecurity
- Food Defense
- Civil Activism/Demonstrations

SECURITY MISSION

- Asset Protection/Theft
- Brand Protection/Fraud/IP Theft: External, Partner and Insider Threats
- Enterprise Resilience
- Political Unrest/Activism
- Risk Management Planning
- Supply Chain
- Terrorism
- Workplace Violence

Securing Other People's Money

Stephen D. Baker

Vice President and Deputy CSO, State Street Corporation

All $27,430,000,000,000 of it. That is $27 "Trillion" with a capital "T" of other people's money under custody at State Street Corporation. Most of their customers, actually, are other financial institutions as well as institutional investors, and their brand and business relies on the continuous vigilance of their executive leaders including Steve Baker, Vice President and Deputy CSO.

"State Street, which is the second oldest bank in the United States, was founded in 1792 and has a great foundation enabling us to look at risk profiles and support the business by addressing threats. Our bank's strong focus on satisfying customers and investors, as well as protecting our reputation, has strongly integrated security into the business," says Baker. "We are a leading trust bank, so the big bucket we manage as a business is risk."

Global Security's mission is to safeguard our people, property, information, reputation and ensure the continuity of business operations. Security does this through the continuous implementation and improvement of security programs and safety measures. Security's participation on key committees such as Operational Risk, Country Risk and Vendor Risk committees, along with a reporting line to the Chief Legal Officer who serves on the Executive Management Committee, gives the State Street Security staff a very relevant place of responsibility. In addition Baker's role on the Corporate Incident Response team eliminates information gaps and keeps his team ahead of the curve.

"I consider myself a business person first, with an expertise in security. Banking regulations can have some advantage for a security function to have direct view of expectations and demands on security. It enables us to influence and control the security-related risk management agenda," he says.

Cybersecurity, political unrest/travel safety and terrorism/shareholder activism are some of the biggest risk issues and are heavily intertwined. "Our big 'risk' focus is the protection of our critical infrastructure. State Street is designated as a Systematically Important Financial Institution (SIFI) in the U.S. and globally because of its size, complexity, interconnectedness and the lack of readily available substitutes for the financial infrastructure it provides." states Baker.

> **"It is my job to understand our security costs better than my bosses do."**

State Street Global Security is highly regarded by all of its stakeholders. The security team works closely with senior business executives. "By being integrated into the business, we understand the goals prior to planning. Reaching across the organization and working with the other business units is a favorite aspect of my job," he says.

The financial services sector has its unique challenges and opportunities. Banking laws require banks to have a CSO. Jack Eckenrode is the bank's Senior Vice President and Chief Security Officer. Security is required to develop a security program and present it to the Board of Directors for approval. That approval provides support for the programs implementation. The Global Security function also provides significant support to the Legal team through litigation support activities and to the Compliance group through its assistance with due diligence and investigations pertaining to global money laundering laws; Foreign Corrupt Practices Act violations; and employee ethics infractions. Security is a separate global division and has centers of excellence to maximize its effectiveness and efficiency. "By reporting to a member of the management committee, we have visibility into long-term plans and initiatives. This allows us to identify risks and present those risks and solutions early to the business people who own them. The result is that the bank makes the right decision as an entity. Security is neither dictating a policy nor being dictated to when it comes to risk management," Baker says.

The security team has worked to measure all aspects of their value and cost matrix. One initiative separated constant RFP costs,

SECURITY SCORECARD

- Annual Revenue: $9.8 Billion
- Security Budget: $29 Million

CRITICAL ISSUES

- Cybersecurity
- Political Unrest/Activism
- Terrorism
- Safeguarding State Street's people, property, information, reputation and the continuity of business operations worldwide through the implementation and improvement of security programs and safety measures.

SECURITY MISSION

- Asset Protection/Theft
- Brand Protection/Intellectual Property/Product Protection/Counterfeiting/Fraud Protection
- Business Expansion Support
- Enterprise Resilience
- Fraud/IP Theft: External, Partner and Insider Threats
- Employee Travel/Kidnapping & Ransom
- Fire
- Insurance
- Regulatory Compliance
- Risk Management Planning Supporting Business Growth
- Supply Chain
- Technology Integration and Management
- Weather
- Workplace Violence

such as hourly contract officers and equipment costs from variable costs including sick leave and vacation. By separating these items they are more able to predict expenses and budget across the organization.

A second initiative to improve security without increasing costs was the move from four leased office buildings to one bank-owned building. While the direct cost of security increased, they were able to document that the indirect costs funded by the bank at the leased buildings met or exceeded these direct costs. Thus, the cost transfer was equal. "This is a financial services company, and our bosses understand financials! It is my job to understand our security costs better than they do. That allows us to gain credibility and make the business case," says Baker.

Security contributes to the direct bottom line results as well. By capturing actual entry and exit data through the access control system at their buildings, the bank was able to do occupancy modeling for the global real estate department, provide actual use and incident reports for insurance quotes and leverage travel information for employee tax issues. "We are able to reduce cost, increase efficiency and gain internal customer satisfaction as a result," he notes.

Security conducts internal evaluations and surveys that result in security team members being highly regarded and valued. The key to success is ensuring prospective hires are a strong cultural fit with more of a business risk focus and less of an enforcement mentality. Second, training is critical. "We require our employees to identify training needs and complete these programs. We also have a flexible structure that allows volunteering, pursuing certifications, association involvement and participating on mentoring teams, on bank time," says Baker. "And we lead by example. Everyone participates in these programs from the top on down to our interns."

Security's engagement in the business from inception to delivery ensures that State Street has solid enterprise risk management planning. "We are involved in company, not merely security decisions, which means there are no surprises. That is the critical difference that enables success. The many inbound calls we receive for advice points to our value across the company.

"By satisfying customers, regulators and providing a safe workplace for employees and visitors, Security will continue to be a viable entity by being engaged in the business and supporting the company's goals. We are expected to be the experts and are often asked, 'how do we get this done?'" concludes Baker. "We work each day to reduce risk, win customers over, meet regulatory requirements and support the business while safeguarding our people, all with management support! I love my job!" SECURITY

Changing the Weather

Rich Mason

VP, Honeywell Global Security, Honeywell

Honeywell

Honeywell is a Fortune 100 diversified technology and manufacturing leader, serving customers worldwide with aerospace products and services; control technologies for buildings, homes and industry; turbochargers; and performance materials. With such diversity of opportunity at Honeywell, having the right controls and security in place is critical to long-term success.

Rich Mason, VP of Honeywell Global Security, sees beyond the sheer size and challenges of managing security operations at a large diversified company and has embraced and capitalized upon Honeywell's unique security challenges and business opportunities. "Working for Honeywell means you will never get bored, as the environment is so diverse," Mason says. "Risk management is an iterative, dynamic negotiation. It requires good relationship management, marketing and a good awareness of business objectives and risk tolerances and is a perfect function by which to explore all of the other key functions in a global business."

"What makes this job interesting is that we're very diverse in terms of our risk tolerance," Mason adds. "I have to deal with different ends of the spectrum: one that wants flexibility and another that is grounded in significant regulatory requirements, like Defense, that aren't willing to go as fast or aggressive. We don't have a 'one size fits all' approach. Security is very much a dialogue. Our security team consists of businesspeople, consultants and advocates. That's what makes us unique and successful."

Honeywell is also a Six Sigma enterprise, a set of techniques and tools for process improvement developed by Motorola in 1986. Six Sigma seeks to improve the quality of process outputs by identifying and removing the causes of defects (errors) and minimizing variability in manufacturing and business processes. Each Six Sigma project carried out within an organization follows a defined sequence of steps and has quantified value targets, for example, reducing costs. That process helps security's role at Honeywell, Mason says, because defects – with security, it's risk– is managed very carefully. "We look for repeatable process, and we try to eliminate defects and waste," Mason says. "I am constantly tracking failure modes and working on solutions to ensure those issues don't arise again. Through our leadership we've built an environment that is continuously improving. We're not comfortable just reporting the weather; we're actively changing it."

However, the challenge with managing risk with a Six Sigma environment, Mason says, is the risk to become complacent. "One campaign for us right now is resilience. I think too many security organizations are getting caught in the trap of saying compliance is good enough to manage risk. Some will say: 'If I'm ISO certified and if I have my government certification, I'm secure.' And I like to push back on folks and say that's minimum security. Let's not confuse that with resilience. Resilience is this concept of no matter what gets thrown at us we can minimize the impact, we can get up quickly, we can learn from it and we can continuously improve. The only way to do that is when security is integrated, when it is built in, not bolted on."

Mason's professional background is both physical and cybersecurity, with previous security positions before being named Honeywell's first Chief Information Security Officer for the Aerospace division, and then taking on the CSO role.

His cyber background has proven useful in his CSO role at Honeywell as he has responsibility over cyber, physical and industrial security, which covers managing employee and facility government clearances. A CSO for each of Honeywell's major lines of businesses report to him. Mason reports to Honeywell's General Counsel.

Honeywell has developed Security Centers of Excellence where all standard work, such as training, managing employees' clearances, facility clearances, lining up audits and pre-audits and inspections, gets managed. "It also trains our security team on being better business people. I think that's what is changing in the security environment. It is taking pure play security folks and up-armoring them with marketing skills, with procurement skills and engineering skills, and overall, creating well-rounded business professionals."

Overall, security's mission is "about people," Mason adds. "Any successful organization needs to advance in all three domains of people, process and technology. But it starts with good people to advance the latter. At Honeywell people are our ultimate differentiator. We have skilled, motivated people that embrace change and are constantly looking for ways to improve and increase their productivity through new tools and standardized work. That's what makes us valuable partners to the Leadership team," says Mason.

At the end of the day, what also defines Mason's success, he says is "doing meaningful work. Protecting Honeywell and national security interests in the chemical, aerospace, defense, process control, manufacturing and technology sectors are very rewarding." SECURITY

SECURITY SCORECARD

- Annual Revenue: $39 Billion
- Security Budget: Confidential

CRITICAL ISSUES

- High Growth Regions
- Cyber Resiliency
- Governance Risk and Compliance

SECURITY MISSION

- Asset Protection/Theft
- Business Expansion Support
- Cybersecurity
- Drug and Alcohol Testing
- Employee Travel
- Enterprise Resilience
- Loss Prevention/
  Asset Protection of goods for resale
- Risk Management Planning
- Supply Chain
- Supporting Business Growth
- Terrorism
- Weather
- Workplace Violence

Securing the enterprise's physical assets and supply chain is a major part of the job, perhaps somewhat taken for granted or overlooked at the C-Suite. As Dennis Quiles of McDonald's notes, integrating asset protection programs with the company mission can be achieved.

7. Human Capital: Hiring, Training and Retention

> "To be a leader in this organization, you've got to be committed to building a diverse and high-performing team."
>
> ***Jerry Blum, AutoZone***

The acceleration of an effort to defend against cyber crimes, integrate new technologies and support organizational goals is demanding a new set of skills, culture, people and on-going training programs. Many CSOs have said, "It's not about guns, guards and gates, anymore." Actually, it's not about people that use guns, guards and gates anymore. The gates are still there; the people are being changed.

> "Companies looking for more security staff aren't going to find them – they're going to have to create them. We wanted to call attention to this security shortage because it's not a quick fix. This won't be solved in a year. It will be a four- to eight-year cycle in order to close that gap."
>
> ***John Stewart, Cisco***

The level of executive management and organizational leadership skills, having a strong cultural fit and immersing in the business vision and goals of their organization are a critical first step for CSO success. The next step is to build an organization of deputies and specialists that internalize the same values and goals to build security's internal brand as a professional and proactive organization.

> "At Honeywell we have skilled, motivated people who embrace the vision of integration as an enabler, standard work and Six Sigma as a defect reducer, commoditization as a value creator, security as a competitive advantage builder, intelligence as a risk manager, data as a predictor, and relationship management as the glue that holds it all together."
>
> ***Rich Mason, Honeywell***

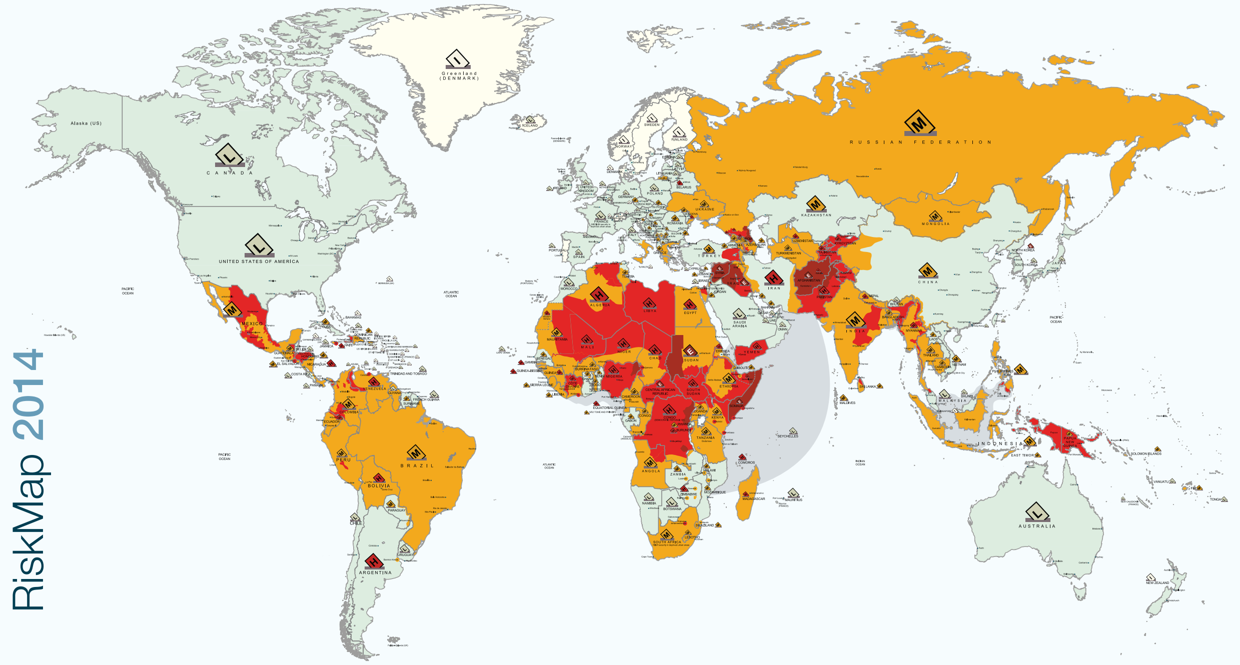
Finding, training, motivating and retaining qualified people that meet the organizational culture and want to be a part of a successful team for the long-term career is a great challenge. International sourcing is particularly difficult due to the sticker shock associated with compensation levels.

There is an ongoing reliance on human

Control Risks

www.controlrisks.com

RiskMap 2014



Copyright © Control Risks 2013. All rights reserved. Reproduction in whole or in part prohibited without the prior consent of the Company.

The Risk Ratings are compiled from sources that Control Risks considers to be reliable or are expressions of opinion. Control Risks has made reasonable commercial efforts to ensure the accuracy of the information on which the Risk Ratings are based, however, the Risks Ratings are provided 'as is' and include reasonable judgments in the circumstances prevailing at the time. The Risk Ratings provided should not be construed as definitive or binding advice. Boundaries and names shown on this map do not imply endorsement or acceptance by Control Risks.

Source: Control Risks

SECURITY RISK FORECAST

INSIGNIFICANT	LOW	MEDIUM	HIGH	EXTREME

The security risk rating evaluates the likelihood of state or non-state actors engaging in actions that harm the financial, physical and human assets of a company. It assesses the extent to which the state is willing and able to protect those assets and the extent to which state or non-state actors are capable of harming those assets. The impact of security risk on companies can include theft, injury, kidnap, damage to installations, information theft, extortion, fraud, expropriation and loss of control over business. Security risk may vary for companies and investment projects because of factors such as industry sector, investor nationality and geographic location.

PIRACY RISK — Areas at heightened risk of piracy or other maritime insecurity. Go to www.controlrisks.com for our Maritime RiskMap 2014.

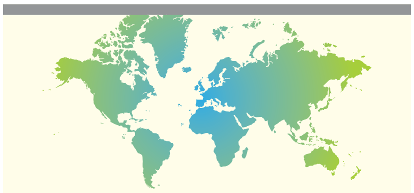
POLITICAL RISK FORECAST

I	L	M	H	E
INSIGNIFICANT	LOW	MEDIUM	HIGH	EXTREME

The political risk rating evaluates the likelihood of state or non-state political actors negatively affecting business operations in a country. It assesses the extent to which the state is willing and able to guarantee contracts and the extent to which non-state actors may threaten the viability of business operations. The impact of political risk on companies can include negative government policy, judicial insecurity, exposure to corruption, reputational damage, expropriation and nationalisation, and international sanctions. It assesses the extent to which political, economic and institutional stability may enhance or diminish the likelihood of these risks taking place. Political risk may vary for companies and investment projects because of factors such as industry sector and investor nationality.

resources to identify, train and develop leading talent within security organizations enabling security to become more effective and valuable to its stakeholders. Human capital management is now critical for any CSO to remain ahead of the curve and succeed.

8. Business Expansion



Geographic Security Responsibility

(Among Those With Locations):

	Total
North America	98%
Australia	74%
Europe	72%
South America	72%
Asia	71%
Africa	63%

The push to emerging and frontier markets was a consistent critical issue among Security 500 members in the first years of the survey. This category has matured to encompass supporting business expansion enterprise wide. International locations, no matter how unique or challenging, have become part of the new normal. The integration of security into business expansion goals and planning has enabled security to research and identify risks, assign specialists to support expansions and in turn, stay ahead of business unit requirements.

> "One of the most important attributes of a successful security organization is you have to be first and foremost viewed as a trusted business partner."
>
> *Vance Toler, Southwest*

This question was changed from the prior years to ask part one: "In which regions does your organization have business operations?" and part two: "Do you provide security services in this region?" As a result, the answers compared to prior years are not comparable but are more accurate. For example, among the enterprises with business operations in Europe, 72 percent provide security services for those operations.

At the top of the list for business expansion is reputational risk. New markets involve new cultures, stakeholders and expectations. Gregg Anderson, a director at Crowe Horwath LLP in Chicago noted in *Insurance Business* magazine, "It's not just looking at the return on investment."

The movement toward a single global office of the CSO enabling a consistent mission and leadership to support the global enterprise has led to our consolidating emerging markets, frontier markets and business growth into one trend this year, business expansion. Having a single optic for planning risk management, policies, technology integration, threat analysis and employee support is becoming a best practice.

The concept of security as an accelerator for reaching objectives and maximizing financial results is being noticed and appreciated by internal business leader customers. CSOs clearly view their role as an executive who contributes to organizational success by managing security and risk. Equally important, they work in organizations where the C-Suite understands the economic value added and does not view security as a narrow, technical function.

9. Workforce, Executive and Travel Protection

Both keeping the workforce secure, informing them they are secure and having them participate in their own security by educating and changing their behavior is an art and a science. Travel is stressful to many people when it goes off without complications. Delays, health issues, fear or being victimized do not only impact that individual and their productivity; but clearly have implications for the brand, employees and other ecosystem partners.

While coordinating safe passage and 24/7 support for stakeholders has been a role for some security organizations historically. It became mainstream after Hurricane Katrina and the drive for international growth during the 2009 deep recession in the U.S. and Europe. It continues to be a growing service as new technologies and services become available (as noted in the big data section). Attitude, technology, intelligence, communication and collaboration are the key elements to successful travel support programs. This year, 80 percent of Security 500 members report responsibility for workforce, executive and travel protection.

The global economy is not only impacting business people who work in or travel internationally. Universities, hospitals, volunteer and religious organizations are expanding to international destinations at an increasing pace. Cleveland Clinic has opened a medical center in Saudi Arabia; The Church of Latter Day Saints has missionaries traveling around the world, constantly. Carnegie Mellon, Duke and Johns Hopkins all have campuses in China. And volunteers are at risk, as recently witnessed, from terrorist beheadings to Ebola outbreaks.

> "Our security officers are more about supporting people in crisis and treating people well than being an enforcer."
>
> *Jim Sawyer, Seattle Children's Hospital*

Attitude: If security officers were given an accurate title on their badges, it would read "Director of First Impressions" directly relating to the importance of how attitude and demeanor impact either a prospective customer or criminal's behavior.

Concierge programs, including hiring hospitality majors and training them in security and safety, have come into popularity. The C-Suite likes the brand image and they tend to have higher employee retention rates and are ultimately are less costly over time than traditional hourly guard services.

What is clear is that these "Directors of First Impressions" are critical for the security brand and reflect strongly on the CSO and security operations.

Technology: Travel tracking and support solutions enable enterprises to keep in touch with their stakeholders. Should an event disrupt that traveler's plans, such as a natural disaster or personal health issue, the plans are already in place to know, notify, support and take action on that person's behalf. This technology is being utilized for everything from weather to political unrest to both reassure stakeholders prior to their business travel to supporting them during impactful events. The importance of the reassurance is that it strengthens both security's and the overall enterprise's brand in the mind of the stakeholder.

Intelligence: There is a lot of information available today. Bringing it into an Intelligence Operations Center for analysis, discussion and appropriate action is a critical step in successfully implementing the travel support program. Collecting all Twitter mentions of your company alone may or may not be useful. But understanding the trend lines and themes within those messages is valuable to gain situational awareness more quickly. Having smart, intellectually curious team members who can connect the dots and translate information into intelligence is a significant part of the predictive movement across leading security organizations.

> "Doing 'meaningful work' is a success criterion. Protecting Honeywell and national security interests in the chemical, aerospace, defense, process control, manufacturing and technology sectors is very rewarding for me."
>
> ***Rich Mason, Honeywell***

Communication: Engaging stakeholders in their own safety through education, behavioral modification, policies and support resources (technical and human) play a core role in workforce protection. Individuals that work against their own wellbeing make security's job difficult and expensive. Thus policies, their purpose and the tools to participate appropriately are required. Approved hotel lists for corporate travel are one example where risks are identified in a certain geography and reduced by selecting pre-screened properties.

Collaboration: Especially for international travel support, having feet on the ground relationships with local knowledge is vital. It is a best practice to engage local law enforcement in areas where enterprises have physical and human capital investments. In addition, providers of guard, travel and medical services are routinely engaged as a risk mitigation component of international business planning. Their institutional knowledge, experience and relationships are critical at times of increased risk or crisis.

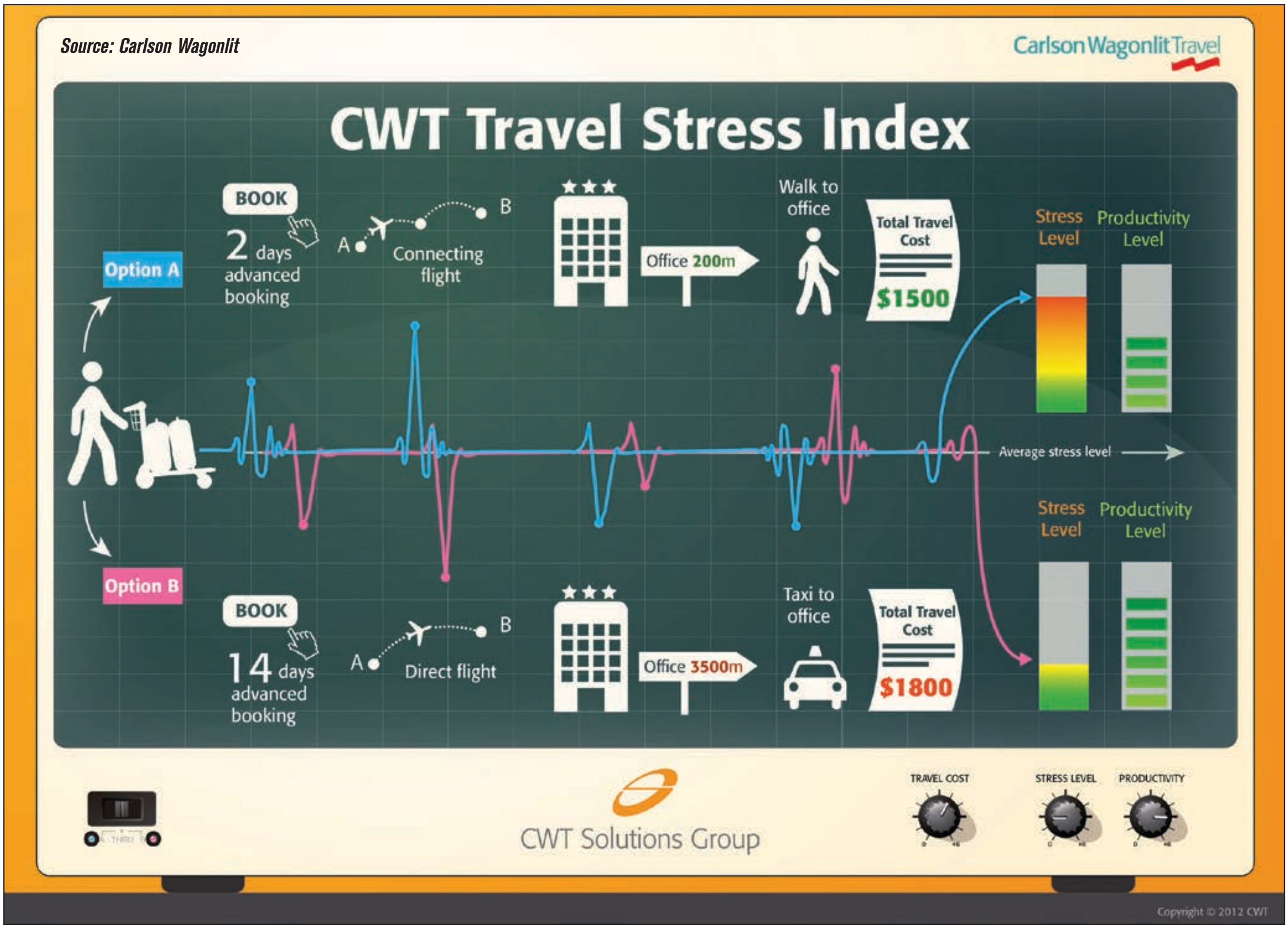
10. Regulatory Compliance

Understanding, funding and managing regulatory compliance within your specific Security 500 sector is now anticipated and expected by the C-Suite from its security leaders. Brian Loughman, the EY Americas Leader for Fraud Investigation & Dispute Services (FIDS), identified six key themes for regulatory compliance:

1. Dealing with reputational harm and the business risk associated with cyber-crime will become part of a General Counsel's responsibility set.
2. Balancing significant growth opportunities in Africa with perceived corruption risk.
3. The impact of regulation will be felt stronger than ever by the financial services industry.
4. FCPA compliance will remain a top priority for life sciences companies operating in emerging markets.
5. Anti-money laundering and corruption programs to face greater scrutiny.
6. The opportunity to leverage "Big Data" in the context of compliance and anticorruption will allow companies to ask new questions.

The study also warns of "regulatory compliance fatigue" having a negative impact on enterprises that are not up to the task of maintaining their programs as consistently and constantly as required. Enterprise leaders should also focus on the right program to meet the threat, which might mean doing more than the minimum. SECURITY

Source: Carlson Wagonlit



Copyright © 2012 CWT

2014 SECURITY 500

2014 RANKINGS

Agriculture/Farming/Food Manufacturing

Rank	Company Name	Security 500 Member	Title	City	State
1	Archer Daniels Midland	Jeffrey Larner	Vice President of Global Security	Decatur	IL
2	General Mills, Inc.	Christoph J. Welsh	Director of Global Security	Minneapolis	MN
3	McDonald's Corporation	Michael Peaster	Vice President of Global Safety and Security	Oak Brook	IL
4	Perdue Farms	Kort Dickson	Director of Corporate Security	Salisbury	MD
5	McCormick & Company, Inc.*	Bryan Fort	Director of Corporate Security	Sparks	MD
6	Pepsico, Inc.*	David Carpenter	Vice President of Security	Purchase	NY
7	Farmer John Meats	Robert L. Jones	Vice President of Human Resources	Vernon	CA
8	Hershey's*	Matthew F. Ryan	Director of Corporate Security Worldwide	Hershey	PA
9	Kellogg Company*	Scott Lindahl	Chief Security Officer	Battle Creek	MI
10	Kraft Foods Global, Inc.*	Ruben Chacon, CISSP, CISM	Senior Manager of GIS and ITOPS Security for America, Spain	Northfield	IL
11	Land O'Lakes, Inc.*	Dan Taussig	Director of Global Security	Arden Hills	MN
12	Agrium*	Leslie O'Donoghue	Executive Vice President of Corporate Development and Strategy; Chief Risk Officer	Calgary	AB
13	Syngenta Corporation*	C. David Gelly	Director of Corporate Security	Winston-Salem	NC
14	The Scotts Company*	Lenny Hall	Global Security Manager; Chief Security Officer	Marysville	OH
	LISTED ALPHABETICALLY				
	Mars, Incorporated	Scott W. Sheafe	Global Security Director	McLean	VA
	Monsanto Company	Peter Sullivan	Director of Global Security	St. Louis	MO

Business Services/Consulting

Rank	Company Name	Security 500 Member	Title	City	State
1	ADP	Roland Cloutier	Chief Security Officer	Roseland	NJ
2	EY (formerly Ernst & Young)	John Imhoff	Director of Global Security	Washington	DC
3	Deloitte	Ted Almay	Global Chief Security Officer	Raleigh	NC
4	Iron Mountain Incorporated	Jack Faer	Chief Security Officer	Boston	MA
5	CACI International, Inc.	Jeffrey J. Berkin	Senior Vice President; Chief Security Officer	Fairfax	VA
6	Hogan Lovells	Jeff Lolley	Head of Global Information Security	Washington	DC
7	InfoMart	Robbie Bible	Chief Information Officer	Marietta	GA
8	ADT Security Services*	Ed McDonough	Chief Security Officer	Boca Raton	FL
9	SAIC (Science Applications International Corporation)*	Stephen T. Colo	Senior Vice President; Chief Security Officer	McLean	VA
10	KPMG*	Charlie Steadman	Executive Director of Firmwide Security	New York	NY
11	PricewaterhouseCoopers*	Preston Jennings	Chief Information Security Officer	New York	NY
12	Brink's Incorporated*	Phillip Henning	Director of Physical Security and Global Security	Richmond	VA
	LISTED ALPHABETICALLY				
	Accenture	Timothy Weir	Managing Director of Global Asset Protection	Chicago	IL
	Experian	Stephen Scharf	Chief Information Security Officer	Costa Mesa	CA
	Marchex	Greg Nelson	Director of Security	Seattle	WA

*Estimated

Agriculture/Farming/Food Manufacturing

CRITICAL ISSUES:

Cybersecurity
Budget/Funding
Political Unrest/Activism
Technology Integration and Management
Supply Chain
Asset Protection/Theft
Regulatory Compliance

BUDGET VS. 2013:	
Increased	43%
Decreased	57%

SECURITY REPORTS TO:	
Human Resources	50%
Chief Risk or Legal Officer/ Risk/Legal/General Counsel	33%
COO/Operations	17%

GEOGRAPHIC RESPONSIBILITY:	
Africa	83%
Asia	83%
North America	83%
Australia	67%
Europe	67%
South America	67%

ORGANIZATIONAL RESPONSIBILITIES:

Brand Protection/Intellectual Property/ Product Protection/Counterfeiting/Fraud Protection	100%	Security Technology and Integration	83%	Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	33%
Investigations	100%	Terrorism	83%	Drug and Alcohol Testing	33%
Political Unrest	100%	Global Security Operations Center Management	67%	Emerging/Frontier Market Expansion	33%
Workplace Violence	100%	Weather/Natural Disasters	67%	Regulatory Compliance	33%
Workforce/Executive/Personnel Protection/Travel Support	100%	Business Expansion Support	50%	Supply Chain	33%
Contract Management (Guards, Technology Integrators, Contract Employees)	83%	Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	50%	Fire	17%
Employee Travel/Kidnapping & Ransom	83%	Loss Prevention/Asset Protection	50%		
Physical/Assets/Facilities (Proprietary Property Not for Resale)	83%	Risk Management Planning	50%		

Business Services/Consulting

CRITICAL ISSUES:

Cybersecurity
Political Unrest/Activism
Terrorism
Technology Integration and Management
Regulatory Compliance
Supporting Business Growth

BUDGET VS. 2013:	
Increased	56%
Stayed the Same	33%
Decreased	11%

SECURITY REPORTS TO:	
Chief Risk or Legal Officer/Risk/Legal/ General Counsel	33%
CEO/President/Executive Director	23%
CFO/Finance	22%
CIO/Information Technology	22%

GEOGRAPHIC RESPONSIBILITY:	
North America	100%
Asia	67%
Europe	67%
South America	67%
Africa	56%
Australia	56%

ORGANIZATIONAL RESPONSIBILITIES:

Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	89%	Brand Protection/Intellectual Property/ Product Protection/Counterfeiting/Fraud Protection	67%	Emerging/Frontier Market Expansion	44%
Investigations	89%	Business Expansion Support	67%	Regulatory Compliance	44%
Physical/Assets/Facilities (Proprietary Property Not for Resale)	89%	Global Security Operations Center Management	67%	Fire	33%
Security Technology & Integration	89%	International Workforce Protection and Support	67%	Political Unrest	33%
Contract Management (Guards, Technology Integrators, Contract Employees)	78%	Terrorism/Bomb Threats	67%	Drug and Alcohol Testing	22%
Cyber/Information Technology	78%	Workforce/Executive/Personnel Protection/Travel Support	67%	Loss Prevention/ Asset Protection of Goods for Resale	22%
Risk Management Planning	78%	Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	56%	Insurance	11%
Workplace Violence Prevention/ Active Shooter Prevention	78%	Weather/Natural Disasters	56%	Supply Chain/Product Diversion/Logistics/ Distribution	11%

Some charts may not equal 100% due to rounding.

Construction/Real Estate Development

CRITICAL ISSUES:

Enterprise Resilience
Major Incidents
Technology Integration and Management
Affordable Care Act

BUDGET VS. 2013:	
Increased	100%

SECURITY REPORTS TO:	
COO/Operations	100%

GEOGRAPHIC RESPONSIBILITY:	
North America	100%

ORGANIZATIONAL RESPONSIBILITIES:	
Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	100%
Contract Management (Guards, Technology Integrators, Contract Employees)	100%
Investigations	100%
Physical/Assets/Facilities (Proprietary Property Not for Resale)	100%
Security Technology & Integration	100%
Terrorism/Bomb Threats	100%
Weather/Natural Disasters	100%
Workplace Violence Prevention/ Active Shooter Prevention	100%

Diversified

CRITICAL ISSUES:

Enterprise Resilience
Political Unrest/Activism
Workplace Violence
Cybersecurity
Budget/Funding

BUDGET VS. 2013:	
Increased	67%
Decreased	33%

SECURITY REPORTS TO:	
CAO/Administration	67%
CEO/President/Executive Director	33%

GEOGRAPHIC RESPONSIBILITY:	
North America	100%
Europe	67%
Asia	33%

ORGANIZATIONAL RESPONSIBILITIES:

Brand Protection/Intellectual Property/ Product Protection/Counterfeiting/Fraud Protection	100%	Loss Prevention/Asset Protection of Goods for Resale	100%	Workplace Violence Prevention/ Active Shooter Prevention	100%
Business Expansion Support	100%	Physical/Assets/Facilities (Proprietary Property Not for Resale)	100%	Workforce/Executive/ Personnel Protection/Travel Support	100%
Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	100%	Regulatory Compliance	100%	Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	67%
Contract Management (Guards, Technology Integrators, Contract Employees)	100%	Risk Management Planning	100%	Fire	67%
Cyber/Information Technology	100%	Security Technology & Integration	100%	Political Unrest	67%
Global Security Operations Center Management	100%	Supply Chain/Product Diversion/Logistics/ Distribution	100%	Drug and Alcohol Testing	33%
International Workforce Protection and Support	100%	Terrorism/Bomb Threats	100%	Emerging/Frontier Market Expansion	33%
Investigations	100%	Weather/Natural Disasters	100%	Insurance	33%

Some charts may not equal 100% due to rounding.

Education (K-12)

CRITICAL ISSUES:

Cybersecurity
Staffing and Training
Asset Protection/Theft
Active Shooter
Budget/Funding

SECTOR SPECIFIC METRICS:	
Security Budget/K-12 Student	$1.70

BUDGET VS. 2013:	
Increased	36%
Stayed the Same	55%
Decreased	9%

SECURITY REPORTS TO:	
COO/Operations	45%
Board or Board Committee	9%
CFO/Finance	9%
Facilities	9%
GM/Business Unit	9%
Other	19%

GEOGRAPHIC RESPONSIBILITY:	
North America	100%

ORGANIZATIONAL RESPONSIBILITIES:

Investigations	100%	Loss Prevention/ Asset Protection of Goods for Resale	73%	Drug and Alcohol Testing	36%
Terrorism/Bomb Threats	100%	Physical/Assets/Facilities (Proprietary Property Not for Resale)	73%	Brand Protection/Intellectual Property/ Product Protection/Counterfeiting/Fraud Protection	27%
Workplace Violence Prevention/Active Shooter Prevention	100%	Security Technology & Integration	73%	Global Security Operations Center Management	18%
Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	91%	Workforce/Executive/Personnel Protection/ Travel Support	73%	Supply Chain/Product Diversion/ Logistics/Distribution	18%
Weather/Natural Disasters	91%	Regulatory Compliance	64%	Emerging/Frontier Market Expansion	9%
Fire	82%	Contract Management (Guards, Technology Integrators, Contract Employees)	55%	Insurance	9%
Risk Management Planning	82%	Cyber/Information Technology	45%		
Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	73%	Political Unrest	45%		

Education (University)

CRITICAL ISSUES:

Budget/Funding
Technology Integration and Management
Workplace Violence
Sexual Assault
Active Shooter

BUDGET VS. 2013:	
Increased	93%
Stayed the Same	7%

SECURITY REPORTS TO:	
COO/Operations	21%
Facilities	14%
CAO/Administration	7%
CEO/President/Executive Director	7%
CFO/Finance	7%
CIO/Information Technology	7%
Other	37%

GEOGRAPHIC RESPONSIBILITY:	
North America	71%
Asia	14%
Africa	7%
Australia	7%
Europe	7%
South America	7%

ORGANIZATIONAL RESPONSIBILITIES:

Terrorism/Bomb Threats	100%	Regulatory Compliance	79%	Cyber/Information Technology	29%
Weather/Natural Disasters	100%	Contract Management (Guards, Technology Integrators, Contract Employees)	71%	Brand Protection/Intellectual Property/ Product Protection/Counterfeiting/Fraud Protection	21%
Workplace Violence Prevention/ Active Shooter Prevention	100%	Security Technology & Integration	71%	Insurance	21%
Fire	93%	Workforce/Executive/Personnel Protection/ Travel Support	71%	Business Expansion Support	7%
Investigations	93%	Loss Prevention/Asset Protection of Goods for Resale	57%	Emerging/Frontier Market Expansion	7%
Risk Management Planning	86%	Political Unrest	57%	Supply Chain/Product Diversion/Logistics/Distribution	7%
Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	79%	Drug and Alcohol Testing	36%	Other	14%
Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	79%	Global Security Operations Center Management	36%		
Physical/Assets/Facilities (Proprietary Property Not for Resale)	79%	International Workforce Protection and Support	36%		

Some charts may not equal 100% due to rounding.

Energy and Utilities

CRITICAL ISSUES:

Cybersecurity
Budget/Funding
Supporting Business Growth
Enterprise Resilience
Workplace Violence
Employee Travel/Kidnapping & Ransom

BUDGET VS. 2013:	
Increased	43%
Decreased	57%

SECURITY REPORTS TO:	
COO/Operations	43%
Chief Risk or Legal Officer/Risk/Legal/ General Counsel	29%
CEO/President/Executive Director	14%
Human Resources	14%

GEOGRAPHIC RESPONSIBILITY:	
North America	100%
Asia	29%
Australia	29%
Africa	14%
Europe	14%
South America	14%

ORGANIZATIONAL RESPONSIBILITIES:

Contract Management (Guards, Technology Integrators, Contract Employees)	100%	Risk Management Planning	86%	Loss Prevention/Asset Protection of Goods for Resale	57%
Investigations	100%	Workplace Violence Prevention/ Active Shooter Prevention	86%	Cyber/Information Technology	43%
Physical/Assets/Facilities (Proprietary Property Not for Resale)	100%	Workforce/Executive/Personnel Protection/ Travel Support	86%	Global Security Operations Center Management	43%
Security Technology & Integration	100%	Business Expansion Support	71%	Supply Chain/Product Diversion/Logistics/ Distribution	43%
Terrorism/Bomb Threats	100%	Fire	71%	Emerging/Frontier Market Expansion	29%
Brand Protection/Intellectual Property/Product Protection/Counterfeiting/Fraud Protection	86%	Weather/Natural Disasters	71%	Political Unrest	29%
Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	86%	Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	57%		
Regulatory Compliance	86%	International Workforce Protection and Support	57%		

Finance/Banking/Insurance

CRITICAL ISSUES:

Workplace Violence
Budget/Funding
Cybersecurity
Technology Integration and Management
Regulatory Compliance
Political Unrest/Activism
Fraud/IP Theft:
External, Partner and Insider Threats
Supporting Business Growth

SECURITY REPORTS TO:	
CAO/Administration	26%
Facilities	16%
Human Resources	16%
CFO/Finance	11%
Chief Risk or Legal Officer/Risk/ Legal/General Counsel	11%
COO/Operations	5%
Other	15%

BUDGET VS. 2013:	
Increased	53%
Stayed the Same	26%
Decreased	21%

GEOGRAPHIC RESPONSIBILITY:	
North America	100%
Asia	47%
Europe	42%
South America	32%
Africa	16%
Australia	16%

ORGANIZATIONAL RESPONSIBILITIES:

Contract Management (Guards, Technology Integrators, Contract Employees)	100%	Weather/Natural Disasters	84%	Business Expansion Support	63%
Investigations	100%	Global Security Operations Center Management	79%	International Workforce Protection and Support	63%
Physical/Assets/Facilities (Proprietary Property Not for Resale)	100%	Risk Management Planning	79%	Emerging/Frontier Market Expansion	42%
Terrorism/Bomb Threats	100%	Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	74%	Loss Prevention/ Asset Protection of Goods for Resale	37%
Workplace Violence Prevention/Active Shooter Prevention	100%	Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	74%	Cyber/Information Technology	21%
Workforce/Executive/Personnel Protection/ Travel Support	100%	Political Unrest	74%	Drug and Alcohol Testing	21%
Fire	89%	Regulatory Compliance	74%	Insurance	16%
Security Technology & Integration	89%	Brand Protection/Intellectual Property/ Product Protection/Counterfeiting/Fraud Protection	63%	Supply Chain/Product Diversion/Logistics/ Distribution	5%

Some charts may not equal 100% due to rounding.

Government (Federal, State and Local)

CRITICAL ISSUES:

Workplace Violence
Insider Threats
Technology Integration and Management
Budget/Funding
Supporting Business Growth

BUDGET VS. 2013:

Increased	50%
Stayed the Same	37%
Decreased	13%

GEOGRAPHIC RESPONSIBILITY:

North America	100%

SECURITY REPORTS TO:

CAO/Administration	25%
COO/Operations	13%
Facilities	13%
Chief Risk or Legal Officer/Risk/Legal/ General Counsel	13%
Other	36%

ORGANIZATIONAL RESPONSIBILITIES:

Physical/Assets/Facilities (Proprietary Property Not for Resale)	100%	Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	63%	Brand Protection/Intellectual Property/Product Protection/Counterfeiting/Fraud Protection	13%
Investigations	88%	Fire	63%	Business Expansion Support	13%
Terrorism/Bomb Threats	88%	Political Unrest	63%	Cyber/Information Technology	13%
Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	75%	Loss Prevention/ Asset Protection of Goods for Resale	50%	Drug and Alcohol Testing	13%
Contract Management (Guards, Technology Integrators, Contract Employees)	75%	Regulatory Compliance	50%	Insurance	13%
Security Technology & Integration	75%	Risk Management Planning	50%	International Workforce Protection and Support	13%
Weather/Natural Disasters	75%	Workforce/Executive/ Personnel Protection/Travel Support	38%	Supply Chain/Product Diversion/Logistics/ Distribution	13%
Workplace Violence Prevention/ Active Shooter Prevention	75%	Global Security Operations Center Management	25%		

Healthcare/Hospital/Medical Center

CRITICAL ISSUES:

Workplace Violence
Budget/Funding
Technology Integration and Management
Active Shooter
Staffing and Training
Patient Behavioral Health and Violence
Asset Protection/Theft

SECTOR SPECIFIC METRICS:

Security Budget/Hospital Bed	$260.71

BUDGET VS. 2013:

Increased	76%
Stayed the Same	14%
Decreased	10%

GEOGRAPHIC RESPONSIBILITY:

North America	76%
Asia	8%
Europe	3%
South America	3%

SECURITY REPORTS TO:

COO/Operations	22%
Facilities	19%
CEO/President/Executive Director	14%
Human Resources	11%
CAO/Administration	5%
CFO/Finance	3%
CIO/Information Technology	3%
Other	23%

ORGANIZATIONAL RESPONSIBILITIES:

Investigations	97%	Regulatory Compliance	78%	Brand Protection/Intellectual Property/ Product Protection/Counterfeiting/Fraud Protection	38%
Terrorism/Bomb Threats	97%	Weather/Natural Disasters	78%	Supply Chain/Product Diversion/Logistics/ Distribution	35%
Workplace Violence Prevention/ Active Shooter Prevention	97%	Risk Management Planning	76%	Drug and Alcohol Testing	32%
Physical/Assets/Facilities (Proprietary Property Not for Resale)	92%	Contract Management (Guards, Technology Integrators, Contract Employees)	73%	International Workforce Protection and Support	32%
Security Technology & Integration	89%	Fire	73%	Global Security Operations Center Management	30%
Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	84%	Workforce/Executive/Personnel Protection/Travel Support	73%	Emerging/Frontier Market Expansion	19%
Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	84%	Business Expansion Support	46%	Insurance	16%
Loss Prevention/Asset Protection of Goods for Resale	78%	Political Unrest	43%	Cyber/Information Technology	14%

Some charts may not equal 100% due to rounding.

Hospitality/Casino

CRITICAL ISSUES:

Staffing and Training
Budget/Funding
Enterprise Resilience
Supporting Business Growth

SECTOR SPECIFIC METRICS:	
Security Budget/Hotel Key	$1,044.49

BUDGET VS. 2013:	
Increased	67%
Decreased	33%

SECURITY REPORTS TO:	
GM/Business Unit	67%
COO/Operations	33%

GEOGRAPHIC RESPONSIBILITY:	
North America	100%

ORGANIZATIONAL RESPONSIBILITIES:			
Fire	100%	Be or Become “Customer Facing” (Meet With and Enhance Security for Customers)	67%
Investigations	100%	Brand Protection/Intellectual Property/Product Protection/Counterfeiting/Fraud Protection	67%
Loss Prevention/Asset Protection of Goods for Resale	100%	Business Expansion Support	67%
Physical/Assets/Facilities (Proprietary Property Not for Resale)	100%	Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	67%
Risk Management Planning	100%	Insurance	67%
Terrorism/Bomb Threats	100%	Regulatory Compliance	67%
Weather/Natural Disasters	100%	Contract Management (Guards, Technology Integrators, Contract Employees)	33%
Workplace Violence Prevention/Active Shooter Prevention	100%	Drug and Alcohol Testing	33%
Workforce/Executive/Personnel Protection/Travel Support	100%	Political Unrest	33%

Industrial/Manufacturing

CRITICAL ISSUES:

Cybersecurity
Workplace Violence
Supporting Business Growth
Budget/Funding
Terrorism
Supply Chain

BUDGET VS. 2013:	
Increased	48%
Stayed the Same	33%
Decreased	19%

SECURITY REPORTS TO:	
Human Resources	25%
Chief Risk or Legal Officer/Risk/Legal/ General Counsel	25%
CFO/Finance	10%
COO/Operations	5%
Facilities	5%
CIO/Information Technology	5%
Other	25%

GEOGRAPHIC RESPONSIBILITY:	
North America	100%
Europe	85%
Asia	75%
South America	70%
Australia	55%
Africa	30%

ORGANIZATIONAL RESPONSIBILITIES:					
Investigations	100%	Global Security Operations Center Management	85%	Business Expansion Support	60%
Workplace Violence Prevention/Active Shooter Prevention	100%	Loss Prevention/ Asset Protection of Goods for Resale	85%	Supply Chain/Product Diversion/Logistics/ Distribution	60%
Workforce/Executive/Personnel Protection/Travel Support	100%	Risk Management Planning	85%	Emerging/Frontier Market Expansion	45%
International Workforce Protection and Support	95%	Security Technology & Integration	80%	Regulatory Compliance	45%
Physical/Assets/Facilities (Proprietary Property Not for Resale)	95%	Weather/Natural Disasters	80%	Fire	40%
Terrorism/Bomb Threats	95%	Brand Protection/Intellectual Property/Product Protection/Counterfeiting/Fraud Protection	75%	Drug and Alcohol Testing	30%
Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	90%	Political Unrest	75%	Cyber/Information Technology	20%
Contract Management (Guards, Technology Integrators, Contract Employees)	85%	Be or Become “Customer Facing” (Meet With and Enhance Security for Customers)	70%	Insurance	10%

Some charts may not equal 100% due to rounding.

Information Technology/Communications/Media

CRITICAL ISSUES:

Workplace Violence
Employee Travel/Kidnapping & Ransom
Cybersecurity
Political Instability

BUDGET VS. 2013:	
Increased	80%
Stayed the Same	10%
Decreased	10%

SECURITY REPORTS TO:	
Chief Risk or Legal Officer/Risk/Legal/ General Counsel	40%
Facilities	20%
CAO/Administration	10%
CFO/Finance	10%
Human Resources	10%
Other	10%

GEOGRAPHIC RESPONSIBILITY:	
North America	100%
Asia	90%
Europe	90%
Australia	80%
South America	70%
Africa	60%

ORGANIZATIONAL RESPONSIBILITIES:

Investigations	100%	Terrorism/Bomb Threats	90%	Regulatory Compliance	60%
Security Technology & Integration	100%	Weather/Natural Disasters	90%	Supply Chain/Product Diversion/Logistics/ Distribution	60%
Workplace Violence Prevention/Active Shooter Prevention	100%	Workforce/Executive/Personnel Protection/Travel Support	90%	Loss Prevention/ Asset Protection of Goods for Resale	50%
Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	90%	Business Expansion Support	80%	Cyber/Information Technology	40%
Contract Management (Guards, Technology Integrators, Contract Employees)	90%	Emerging/Frontier Market Expansion	70%	Risk Management Planning	40%
Global Security Operations Center Management	90%	Brand Protection/Intellectual Property/Product Protection/Counterfeiting/Fraud Protection	60%	Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	30%
International Workforce Protection and Support	90%	Fire	60%	Drug and Alcohol Testing	20%
Physical/Assets/Facilities (Proprietary Property Not for Resale)	90%	Political Unrest	60%	Insurance	20%

Ports/Terminals

CRITICAL ISSUES:

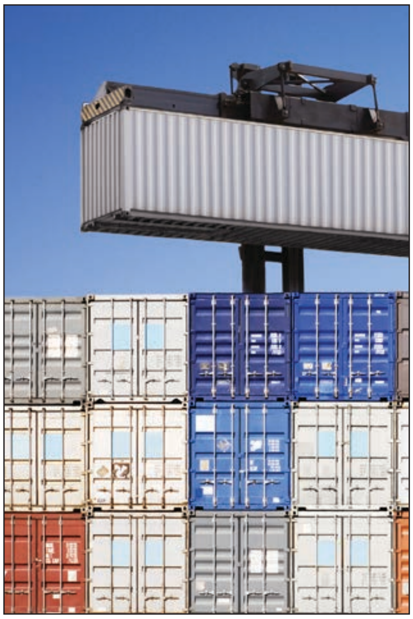
Weather
TWIC Compliance
Technology Integration and Management

BUDGET VS. 2013:	
Increased	65%
Stayed the Same	25%
Increased	10%

SECURITY REPORTS TO:	
CEO/President/Executive Management	100%

GEOGRAPHIC RESPONSIBILITY:	
North America	100%

ORGANIZATIONAL RESPONSIBILITIES:	
Brand/Product Protection	100%
Business Continuity	100%
Corporate Security	100%
Cyber/Information Technology	100%
Disaster Recovery	100%
Investigations	100%
Physical Security/Facilities	100%
Regulatory Compliance	100%
Supply Chain/Vendor	100%



Some charts may not equal 100% due to rounding.

Retail (Connected Commerce)

CRITICAL ISSUES:

Cybersecurity
Loss Prevention (Retail)
Organized Retail Crime
Workplace Violence
Political Instability

BUDGET VS. 2013:	
Increased	50%
Stayed the Same	17%
Decreased	33%

SECURITY REPORTS TO:	
CFO/Finance	50%
Chief Risk or Legal Officer/Risk/Legal/ General Counsel	33%
COO/Operations	17%

GEOGRAPHIC RESPONSIBILITY:	
North America	83%
Europe	42%
Asia	33%
South America	33%
Africa	17%
Australia	17%

ORGANIZATIONAL RESPONSIBILITIES:

Investigations	100%	Weather/Natural Disasters	83%	Emerging/Frontier Market Expansion	50%
Workplace Violence Prevention/ Active Shooter Prevention	100%	Risk Management Planning	75%	Global Security Operations Center Management	50%
Brand Protection/Intellectual Property/ Product Protection/Counterfeiting/Fraud Protection	92%	Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	67%	Business Expansion Support	42%
Contract Management (Guards, Technology Integrators, Contract Employees)	92%	Fire	67%	Regulatory Compliance	33%
Loss Prevention/ Asset Protection of Goods for Resale	92%	International Workforce Protection and Support	67%	Cyber/Information Technology	17%
Security Technology & Integration	92%	Workforce/Executive/Personnel Protection/ Travel Support	67%	Drug and Alcohol Testing	17%
Physical/Assets/Facilities (Proprietary Property Not for Resale)	83%	Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	58%	Insurance	17%
Terrorism/Bomb Threats	83%	Supply Chain/Product Diversion/Logistics/ Distribution	58%	Political Unrest	8%

Spectator Sports (Arenas/Facilities/Teams/Venues)

CRITICAL ISSUES:

Terrorism
Fan Violence
Player Misconduct
Weather

BUDGET VS. 2013:	
Increased	100%

GEOGRAPHIC RESPONSIBILITY:	
North America	84%
Asia	8%
Europe	8%

SECURITY REPORTS TO:	
Facilities	17%
CAO/Administration	8%
CEO/President/Executive Director	8%
CFO/Finance	8%
COO/Operations	8%
CIO/Information Technology	8%
Chief Risk or Legal Officer/Risk/Legal/ General Counsel	8%
Other	35%

ORGANIZATIONAL RESPONSIBILITIES:

Terrorism/Bomb Threats	100%	Risk Management Planning	83%	International Workforce Protection and Support	42%
Weather/Natural Disasters	100%	Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	75%	Cyber/Information Technology	33%
Workplace Violence Prevention/Active Shooter Prevention	100%	Workforce/Executive/Personnel Protection/Travel Support	75%	Global Security Operations Center Management	33%
Investigations	92%	Contract Management (Guards, Technology Integrators, Contract Employees)	67%	Brand Protection/Intellectual Property/Product Protection/Counterfeiting/Fraud Protection	25%
Physical/Assets/Facilities (Proprietary Property Not for Resale)	92%	Loss Prevention/Asset Protection of Goods for Resale	67%	Business Expansion Support	17%
Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	83%	Political Unrest	67%	Insurance	17%
Fire	83%	Security Technology & Integration	67%	Emerging/Frontier Market Expansion	8%
Regulatory Compliance	83%	Drug and Alcohol Testing	42%	Supply Chain/Product Diversion/Logistics/ Distribution	8%

Some charts may not equal 100% due to rounding.

Transportation/Logistics/Supply Chain/Distribution/Warehousing

CRITICAL ISSUES:

Workplace Violence
Supply Chain
Technology Integration and Management
Maintaining Awareness
Budget/Funding

BUDGET VS. 2013:	
Increased	75%
Stayed the Same	13%
Decreased	12%

SECURITY REPORTS TO:	
CEO/President/Executive Director	25%
COO/Operations	25%
Chief Risk or Legal Officer/Risk/Legal/ General Counsel	13%
Other	37%

GEOGRAPHIC RESPONSIBILITY:	
North America	100%
Asia	50%
Europe	25%
South America	13%

ORGANIZATIONAL RESPONSIBILITIES:					
Business Resilience (Business Continuity, Emergency Management & Disaster Recovery)	100%	Global Security Operations Center Management	88%	Political Unrest	63%
Contract Management (Guards, Technology Integrators, Contract Employees)	100%	Loss Prevention/Asset Protection of Goods for Resale	88%	Supply Chain/Product Diversion/Logistics/ Distribution	63%
Investigations	100%	Physical/Assets/Facilities (Proprietary Property Not for Resale)	88%	Cyber/Information Technology	50%
Terrorism/Bomb Threats	100%	Risk Management Planning	88%	Drug and Alcohol Testing	50%
Workplace Violence Prevention/Active Shooter Prevention	100%	Security Technology & Integration	88%	International Workforce Protection and Support	50%
Be or Become "Customer Facing" (Meet With and Enhance Security for Customers)	88%	Weather/Natural Disasters	88%	Emerging/Frontier Market Expansion	38%
Brand Protection/Intellectual Property/ Product Protection/Counterfeiting/Fraud Protection	88%	Workforce/Executive/Personnel Protection/ Travel Support	88%	Fire	38%
Business Expansion Support	88%	Regulatory Compliance	75%	Insurance	13%

2014 Security 500 Methodology

THE SECURITY 500 Benchmarking Survey is based on information from several sources:

- Data supplied directly by participating enterprises
- Data obtained through public resources/ records

The Security 500 tracks 18 vertical markets and collects unique data where appropriate (such as the number of unique facilities in healthcare) and applies this data to key metrics. The key metrics collected this year include but is not limited to:

- Security Spending/Person
- Security Spending/Revenue
- Security Employees/Officer

"Person" is focused on the type of person the security budget is intended to protect. Examples include employees, citizens, students and patients. There is a series of general questions that all participants completed along with unique questions within each sector.

The 2014 Security 500 Survey includes the following:

- Sectors were measured and evaluated on metrics among peer organizations.
- The data requested and metrics used to benchmark within each sector were based on the input of our advisors.

The purpose of the Security 500 is to create a reliable database to measure your organization versus others and create a benchmarking program among security organizations. The results will enable you to answer the question, "Where Do I Stand?" as a basis of an ongoing peer review process. Due to the greater accuracy of the information provided by security executives compared to that of estimations, completed entries were given greater weight in the rankings than the estimations. Additionally, the sector in which a company is ranked is based on self-reported information. For example, one clothing retailer may select "Retail" and another clothing manufacturer may select "Manufacturing/Industrial" as their sectors.

The 500 enterprises and security leaders listed in this report are among the biggest and best security organizations in the world. All of them have been included in the 2014 Security 500 Report based on security metrics for their individual sectors, however, security leaders were given the option this year in the Security 500 Survey to be either listed by rank or alphabetically. This serves to provide these security organizations the recognition they deserve as members of this prestigious list without disclosing their position within the market.

Based on continued feedback and the goal of creating a valuable resource for our participants and industry, the Security 500 is spread across 18 different sectors. We recognize that as a result of continued unprecedented economic changes some organizations and their security leaders may no longer be in place. The listings are based on the information available at the time of publication. Each participating organization will receive their confidential report by November 30, 2014. For additional information, please e-mail to: S500Questions@bnpmedia.com

Security thanks all of the participants in the Security 500 Report – without their assistance and insight, this valuable resource would not be possible. SECURITY

Some charts may not equal 100% due to rounding.

Construction/Real Estate Development

Rank	Company Name	Security 500 Member	Title	City	State
1	General Growth Properties	Dan Ryan	Senior Corporate Security Director	Chicago	IL
2	AECOM*	Dennis Clark	Vice President; Chief Security Officer	Los Angeles	CA
3	Chicago Bridge & Iron (CB&I)*	Richard A. Fisher	Vice President of Global Corporate Security	The Woodlands	TX
4	Empire State Building*	Donald P. O'Donnell	Director of Security	New York	NY
5	Forest City Enterprises*	Vince Hill	Vice President of Loss Prevention	Cleveland	OH
6	Colliers International*	Terry De Niro	Director of Security	Sacramento	CA
7	GWL Realty Advisors Inc.*	Ernie Eves	Manager of Security and Life Safety	Edmonton	AB
8	Jones Lang LaSalle*	John Friedlander	Director of Security	Chicago	IL
9	Boston Properties*	Alan Snow	Director of Safety and Security	Boston	MA
10	Simon Property Group*	Vincent Cascella	Director of Corporate Security Operations	Indianapolis	IN
11	Servest UK*	Michael Lamoureaux	Managing Director	London	
12	Macerich*	Chris Woiwode	Vice President of Security	Santa Monica	CA
13	Pulte Group*	Gary Haire	Director of Corporate Security	Bloomfield Hills	MI

Diversified

Rank	Company Name	Security 500 Member	Title	City	State
1	Cox Enterprises	Duane Ritter	Vice President of Corporate Security	Atlanta	GA
2	The MITRE Corporation	Gary J. Gagnon	Senior Vice President; Chief Security Officer	McLean	VA
3	Charles River Laboratories	Stephen Morrill	Corporate Vice President of Global Security	Wilmington	MA
4	Loews Corporation*	Jerry Meade	Corporate Director of Security	New York	NY
5	Toyota Tsusho America, Inc.*	Matthew Nunn	Corporate Security Manager	Georgetown	KY
6	Williams Companies*	Bruce List	Director of Security	Houston	TX
	LISTED ALPHABETICALLY				
	Safelite AutoGlass	David Riber	Director of Corporate Security	Columbus	OH

Education (K-12)

Rank	Company Name	Security 500 Member	Title	City	State
1	Los Angeles School Police Department	Steven Zipperman	Chief of Police	Los Angeles	CA
2	Montgomery County Public Schools	Robert B. Hellmuth	Director of the Department of School Safety and Security	Rockville	MD
3	Clark County School District Police	James R. Ketsaa	Chief of Police	Henderson	NV
4	Cleveland Metropolitan School District Division of Safety and Security	Lester Fultz	Chief of Security	Cleveland	OH
5	Santa Ana School Police Department	Hector Rodriguez	Chief of Police	Santa Ana	CA
6	Littleton Public Schools	Guy Grace	Manager of Security and Emergency Planning	Littleton	CO
7	Frederick County Public Schools	Clifton V. Cornwell	Supervisor of Security and Emergency Management	Frederick	MD
8	McCracken County Public Schools	Larry Zacheretti	Director	Paducah	KY
9	Oswego City School District	John C. Anderson V	Director of School Security and Safety	Oswego	NY
10	Radnor Township School District	Joe Perchetti	Supervisor of Security	Wayne	PA
11	Whitfield County Public Schools	Mike Ewton	Chief Officer of Operations	Dalton	GA
12	Broward County School District*	Jerry Graziose	Director of Safety Department	Oakland Park	FL
13	Fairfax County Public Schools*	Frederick E. Ellis	Director of Office of Safety and Security	Falls Church	VA

*Estimated

Education (University)

Rank	Company Name	Security 500 Member	Title	City	State
1	University of Pennsylvania Division of Public Safety	Maureen S. Rush, M.S., CPP	Vice President for Public Safety; Superintendent of Penn Police	Philadelphia	PA
2	New York University Department of Public Safety	Randy Stephan	Vice President of Global Security	New York	NY
3	University of Chicago	Marlon C. Lynch	Associate Vice President for Safety, Security and Civic Affairs; Chief of Police	Chicago	IL
4	University of Florida	Linda Stump	Chief of Police	Gainesville	FL
5	Duke University	John H. Dailey	Chief of Police	Durham	NC
6	University of South Carolina, Columbia	Chris Wuchenich	Associate Vice President for Law Enforcement and Safety	Columbia	SC
7	Johns Hopkins University*	Edmund Skrodzki	Executive Director	Baltimore	MD
8	The University of Texas at Austin*	Gerald Robert (Bob) Harkins	Associate Vice President for Campus Safety and Security	Austin	TX
9	The Ohio State University*	Vernon Baisden	Assistant Vice President for Public Safety	Columbus	OH
10	Michigan State University*	James Dunlap	Director of Public Safety; Police Chief	East Lansing	MI
11	Texas A&M*	J. Michael Ragan	Chief of Police	College Station	TX
12	High Point University	Jeff Karpovich	Security Director	High Point	NC
13	University of La Verne	Stan Skipworth	Senior Director of Campus Safety	La Verne	CA
14	West Virginia University Police Department	Bob Roberts	Chief of Police and Emergency Management	Morgantown	WV
15	Medical College of Wisconsin	David Feller	Director of Public Safety	Milwaukee	WI
16	Longwood University Police Department	Robert R. Beach	Chief of Police; Director of Public Safety	Farmville	VA
17	Bluegrass Community and Technical College	Todd Gray	Operational Manager for Security and Safety	Lexington	KY
18	Carson-Newman University	James A. Hodges	Director of Safety and Security	Jefferson City	TN
	LISTED ALPHABETICALLY				
	Drexel University	Domenic Ceccanecchio	Vice President of Public Safety	Philadelphia	PA
	Norwich University	Michael P. Abraham	Chief of Security	Northfield	VT
	Yosemite Community College District	Becky Crow	Director of Campus Safety	Modesto	CA

Energy and Utilities

Rank	Company Name	Security 500 Member	Title	City	State
1	Baker Hughes, Inc.	Michael Couzens	Vice President; Chief Security Officer	Houston	TX
2	Chesapeake Energy Corporation	Tony Blasier	Vice President; Chief Security Officer	Oklahoma City	OK
3	Consumers Energy	John G. Russell	CEO	Jackson	MI
4	San Antonio Water System	Joshua Dean	Director of Security	San Antonio	TX
5	Honolulu Board of Water Supply	Alexander S. Ubiadas, Jr.	Emergency Management Officer	Honolulu	HI
6	Exxon Mobil Corporation*	Chad Stevens	Global Operations Manager of Security	Houston	TX
7	Shell Oil Company*	Terry Whitley	Senior Security Manager	Houston	TX
8	Chevron Corporation*	Wesley Lohec	Vice President of Health, Environment and Safety	San Ramon	CA
9	Duke Energy*	Darren Myers	Managing Director of Enterprise Protective Services	Charlotte	NC
10	Pioneer Natural Resources*	Butch Brazell	Director of Global Security	Irving	TX
11	American Electric Power*	Stanley Partlow	Director of BL Transportation Services and Security	Columbus	OH
12	FirstEnergy Corperation*	James Whitley Jr.	Executive Director	Akron	OH
13	Florida Power & Light Company*	James Burke	Director of Security	Juno Beach	FL
14	Hess Corporation*	Elizabeth L. Cheney	Global Vice President of Environment, Health, Safety and Social Responsibility	New York	NY
15	Tennessee Valley Authority*	David G. Jolley	Vice President of Security and Emergency Management	Knoxville	TN
16	Xcel Energy*	Rick Benolken	Manager of Safety and Training	Minneapolis	MN
17	Southern California Edison*	Dana Kracke	Vice President of Safety, Security and Compliance	Rosemead	CA
18	Entergy Corporation*	Chris Peters	Vice President of NERC Compliance and Critical Infrastructure Protection	The Woodlands	TX
19	DTE Energy*	Michael Lynch	Chief Security Officer	Detroit	MI

*Estimated

Energy and Utilities - continued

Rank	Company Name	Security 500 Member	Title	City	State
20	Kinder Morgan Energy Partners, LP*	Dwain Jones	Corporate Director of Security	Houston	TX
21	Spectra Energy*	Michael Frankovich	Director of Security	Houston	TX
22	Memphis Light Gas and Water*	LaShell Vaughn	Vice President; Chief Technology Officer	Memphis	TN
23	BC Hydro*	Doug Powell	Manager of SMI Security, Privacy and Safety	Burnaby	BC
24	Helmerich & Payne*	Matthew White	Global Security Manager	Houston	TX
25	PG&E*	Anil Suri	Vice President; Chief Risk and Audit Officer	San Francisco	CA
26	Hunt Consolidated, Inc.*	James Savage	Senior Vice President of Global Security	Dallas	TX
27	JEA*	William Bland, CPP	Security Manager	Jacksonville	FL
28	Portland General Electric Company*	Joseph L. Goodale	Security Manager	Portland	OR
29	Sabine Pass LNG/Cheniere Energy, Inc.*	Bruce Graham	Manager of Security and Emergency Response	Cameron	LA
30	Manitoba Hydro*	Chris McColm	Chief Security Officer	Winnipeg	MB
31	Vectren Corporation*	Janell Ellis	Manager of Corporate Security	Evansville	IN
32	El Paso Water Utilities*	Al Heredia	Chief Security Officer; Emergency Response Coordinator	El Paso	TX
	LISTED ALPHABETICALLY				
	Birmingham Water Works	Scott Starkey	Security Manager	Birmingham	AL
	Exelon Corp.	F. Edward Goetz	Vice President of Corporate and Information Security Services	Chicago	IL
	NV Energy	Bruce Barnes	Manager of Infrastructure Security	Las Vegas	NV
	Peabody Energy	Andrew Cobb	Director of Global Security	St. Louis	MO
	Rio Tinto	David Gracey	Global Head of Security	Montreal	QC

Finance/Banking/Insurance

Rank	Company Name	Security 500 Member	Title	City	State
1	Fidelity Security Services (FSSI)	Dan Sauvageau	Chief Security Officer	Boston	MA
2	Prudential Financial	Lori Hennon Bell	Chief Security Officer	Newark	NJ
3	State Street Corporation	Jack C. Eckenrode	Senior Vice President; Chief Security Officer	Boston	MA
4	State Farm Insurance	Dan Consalvo	Director Corporate Security	Bloomington	IL
5	Capital One	Timothy T. Janes, CPP, CFE	Managing Vice President; Chief Security Officer	McLean	VA
6	E*TRADE Financial	Russell Ross	Vice President of Corporate Security	Menlo Park	CA
7	Nationwide Mutual Insurance Company	Jay C. Beighley CPP	Associate Vice President of Corporate Security	Columbus	OH
8	WellPoint, Inc.	Greg Wurm	Director of Domestic Security Operations	Indianapolis	IN
9	CNA Financial	William Phillips	Chief Security and Safety Officer	Chicago	IL
10	MasterCard	Richard Gunthner	Senior Vice President; Head of Global Corporate Security Group	Purchase	NY
11	Blue Cross Blue Shield of Florida	Harold Grimsley, CPP	Senior Director of Corporate Security	Jacksonville	FL
12	Aflac	Scott Shaw	Senior Manager of Security	Columbus	GA
13	Thrivent Financial	Mark Theisen	Director of Corporate Security and Business Resilience	Appleton	WI
14	People's United Bank	Richard Sardellitti	Security and Investigations Agent	Danvers	MA
15	Insurance Corporation of British Columbia	Bill Anderson	Manager of Corporate Security	North Vancouver	MB
16	Burke and Herbert Bank	Lester J. Bain CSO, CFE	Director of Security; BSA Compliance Officer	Alexandria	VA
17	American International Group*	Steven Tursi	Vice President; Chief Security Officer	New York	NY
18	Wells Fargo & Company*	Michael Bacon	Executive Vice President; Chief Security Officer	San Francisco	CA
19	Fannie Mae*	Patrick Williams	Director of Corporate Security and Resiliency	Washington	DC
20	Morgan Stanley*	Neil Vetrano	Vice President of Corporate Security and Investigations	New York	NY
21	Kaiser Permanente*	Phil Hoffman	Director of Security Services	Oakland	CA
22	New York Life Insurance*	Leonard Mackesy	Chief Security Officer	New York	NY
23	Freddie Mac*	Henry Thomas	Director of Corporate Security	McLean	VA
24	TD Bank*	Gerry Bianchi	Vice President; Senior Manager of Physical Security	Mount Laurel	NJ
25	Aetna*	David Gionfriddo	Director of Corporate Security	Hartford	CT
26	Allstate*	Jeffrey Wright	Vice President; Chief Information Security Officer	Northbrook	IL
27	Progressive*	Paul Beckwith	Chief Security Officer	Mayfield Village	OH

*Estimated

Finance/Banking/Insurance - continued

Rank	Company Name	Security 500 Member	Title	City	State
28	Comerica Bank*	Herbert Kaltz	Vice President; Corporate Security Manager	San Jose	CA
29	CIBC World Markets*	Ted Samul	Manager of Corporate Security	New York	NY
30	Edward D. Jones & Company, LP*	Roland Corvington	Director of Global Security Services	St. Louis	MO
31	Amerisourcebergen Corp.*	Chris Zimmerman	Vice President of Corporate Security and Regulation	Valley Forge	PA
32	New York Stock Exchange*	Brian Gimlett	Chief Security Officer	New York	NY
	LISTED ALPHABETICALLY				
	Automobile Club of Southern California	Jason H. Cook	Manager of Security, Business Continuity and Emergency Services	Costa Mesa	CA
	Bank of New Hampshire	Shaun Sanborn	Senior Vice President; Security Administrator	Laconia	NH
	Blue Shield of California	Cary Takagawa	Senior Manager of Corporate Security and Safety	San Francisco	CA
	Goldman Sachs	Ken Damstron	Global Head of Safety and Security	New York	NY
	LPL Financial	Kevin Cliff	Director of Global Corporate Security	Concord	NC
	Visa, Inc.	Don Hill	Head of Global Security and Safety	Foster City	CA
	Western Union Financial Services	Phil Hopkins	Vice President of Global Security	Englewood	CO

Government (Federal, State, and Local)

Rank	Company Name	Security 500 Member	Title	City	State
1	New York City, N.Y.*	Joseph F. Bruno	Commissioner of the Office of Emergency Management	Brooklyn	NY
2	New Jersey Office of Homeland Security and Preparedness*	Edward Dickson	Director	Hamilton	NJ
3	California Emergency Management Agency*	Mark Ghilarducci	Director of the California Governor's Office of Emergency Services	Mather	CA
4	Illinois Emergency Management Agency*	Jonathon Monken	Director	Springfield	IL
5	Virginia*	Brian Moran	Secretary of the Department of Public Safety and Homeland Security	Richmond	VA
6	Los Angeles*	James Featherstone	General Manager	Los Angeles	CA
7	Chicago*	Gary Schenkel	Executive Director of the Office of Emergency Management	Chicago	IL
8	Philadelphia*	Samantha Phillips	Managing Director for the Office of Emergency Management	Philadelphia	PA
9	Florida*	Bryan Koon	Director of Emergency Management	Tallahassee	FL
10	Dallas*	Dean Sydlowski	Director of Corporate Security	Edmonton	AB
11	Boston*	Rene Fielding	Director of the Office of Emergency Management	Boston	MA
12	San Francisco*	Bijam Karimi	Director of Emergency Management	San Francisco	CA
13	Houston*	Carl Matejka	Coordinator for the Office of Emergency Management	Houston	TX
14	Toronto*	Dwaine Nichol, CPP	Director of Corporate Security	Toronto	ON
15	Hennepin County	Kirk D. Simmons	Security Manager	Minneapolis	MN
16	Clark County	Theodore Hooper	Assistant Manager	Las Vegas	NV
17	Ventura County	Rosalind Harris	Security Manager	Thousand Oaks	CA
18	Department of State*	Gregory B. Starr	Assistant Secretary for Diplomatic Security	Washington	DC
19	Phoenix*	Robert Hughes	Manager	Phoenix	AZ
20	Ontario Ministry of Finance	Brian Wood, PSP, ABCP	Coordinator of Security Services and Emergency Management	Oshawa	PE
21	Phoenix Water Services Department	John Culwell	Security Supervisor	Phoenix	AZ
22	Austin*	Otis Latin, Sr.	Homeland Security and Emergency Management Director	Austin	TX
23	Federal Reserve Board*	Michell Clark	Director	Washington	DC
24	New York City Environmental Protection	Kevin T. McBride	Deputy Commissioner	Flushing	NY
25	Edmonton	Dean Sydlowski	Director of Corporate Security	Edmonton	BC
26	Pollard Banknote Ltd.	Eric Hrycyk	Director of Corporate Security	Winnipeg	NB
27	Columbus*	Miki Calero	Chief Security Officer	Columbus	OH

*Estimated

Healthcare/Hospital/Medical Centers

Rank	Company Name	Security 500 Member	Title	City	State
1	HCA - Hospital Corporation of America	Tim Portale	Chief Safety and Security Officer	Nashville	TN
2	Cleveland Clinic	Gordon M. Snow	Chief of Protective Services	Cleveland	OH
3	Tenet Healthcare*	Britt T. Reynolds	President of Hospital Operations	Dallas	TX
4	Carolinas HealthCare System	John Knox	Executive Vice President; Chief Administrative Officer	Charlotte	NC
5	Massachusetts General Hospital*	Bonnie Michelman	Director of Police, Security and Outside Services	Boston	MA
6	New York-Presbyterian Hospital	Jeffrey Bokser	Vice President of Safety, Security and Emergency Services	New York	NY
7	Fraser Health	Jeffery Young	Executive Director of Integrated Protection Services	Surrey	MB
8	Cardinal Health	Greg Halvacs	Senior Vice President; Chief Security Officer	Dublin	OH
9	Hospital of the University of Pennsylvania	Maureen S. Rush, M.S., CPP	Vice President for Public Safety; Superintendent of Penn Police	Philadelphia	PA
10	Dallas County Hospital District	Kenneth Cheatle	Chief of Police	Dallas	TX
11	University of California-Irvine Health System	Scott Martin	Director of Security and Parking	Orange	CA
12	The University of Texas MD Anderson Cancer Center and UT-Health	William Adcox	Chief of Police	Houston	TX
13	Seattle Children's Hospital	Jim Sawyer	Director of Security Services	Seattle	WA
14	Aurora Health Care	Mike Cummings, CPP	Senior Vice President of Security Loss Prevention	Milwaukee	WI
15	Brigham & Women's Hospital*	Robert Chicarello, CPP	Director of Security and Parking	Boston	MA
16	Duke University	John H. Dailey	Chief of Police	Durham	NC
17	Medical City Dallas*	Leonard Sullivan	Director of Security	Dallas	TX
18	Ohio State University Wexner Medical Center	Michael Mandelkorn	Director of Security	Columbus	OH
19	Greenville Health System Law Enforcement Services	Joseph V. Bellino, CHPA	Chief of Police; Director of Security	Greenville	SC
20	University Health Network	Todd Milne	Senior Manager	Toronto	PE
21	Metropolitan Hospital Center	Anthony S. Notaroberta	Senior Associate Director	New York	NY
22	Boston Children's Hospital	Robert Ryan, CPP, CHPA	Security Director	Boston	MA
23	Dana-Farber Cancer Institute	Ralph Nerette	Security Director	Boston	MA
24	Saint Francis Hospital and Medical Center	Jack Mayoros	Director of Security	Hartford	CT
25	Baystate Medical Center	Thomas F. Lynch	Dierctor of Security	Springfield	MA
26	HealthEast Care System	Kathryn Correia	President; CEO	St. Paul	MN
27	Parkview Health	Thomas Rhoades	Director of Police and Public Safety	Fort Wayne	IN
28	Lancaster General Hospital	Daniel Ford	Director Security and Safety	Lancaster	PA
29	University of Chicago Medical Center	Marlon C. Lynch	Associate Vice President for Safety, Security and Civic Affairs; Chief of Police	Chicago	IL
30	Community Health Systems*	Gordon Carlisle	Vice President of Facilities Management	Franklin	TN
31	Baltimore Washington Medical Center	Karen Olscamp	President	Glen Burnie	MD
32	Antelope Valley Hospital	Timothy Lidberg	Director of Safety and Security	Lancaster	CA
33	Mayo Clinic Health System - Eau Claire	Drew Neckar, CPP, CHPA	Regional Director	Eau Claire	WI
34	The University of Texas Medical Branch at Galveston	Thomas E. Engells	Chief of Police	Galveston	TX
35	Van Andel Institute	Jana Hall	Chief Operating Officer	Grand Rapids	MI
36	Indiana University Health North Hospital	Garry Kimble	Chief of Police and Protective Services	Carmel	IN
37	King's Daughters Medical Center	Scott Hill	Director of Environmental Safety; Chief Security Officer	Ashland	KY
38	West Virginia University Police Department	Bob Roberts	Chief of Police and Emergency Management	Morgantown	WV
39	Anderson Hospital	Paul J. Head	Security Manager	Maryville	IL
40	Atlantic Health System*	Alan J. Robinson	Director of Protection Security Services and Emergency Management	Morristown	NJ
41	Advocate BroMenn Medical Center*	Peter Fee	Manager of Public Safety	Normal	IL
42	Ascension Health*	Patricia Maryland	President of Healthcare Operations; Chief Operating Officer	St. Louis	MO
43	Catholic Health Initiatives*	Phillip L. Foster	Senior Vice President; Chief Risk Officer	Englewood	CO
44	Trinitas Regional Medical Center	John Dougherty	Director of Security	Elizabeth	NJ

*Estimated

Healthcare/Hospital/Medical Centers - continued

Rank	Company Name	Security 500 Member	Title	City	State
45	Cedars-Sinai Hospital*	Corey Hart	Manager of Safety and Security	Los Angeles	CA
46	Henry Ford Health System*	Kevin Robinson	Security Manager	Detroit	MI
47	Shands HealthCare*	Steve Truluck	Director of Safety, Security and Transportation	Gainesville	FL
48	Children's Healthcare of Atlanta*	Josh Bornstein	Director of Safety and Security	Atlanta	GA
49	Cadence Health*	George DiLeonardi	System Director of Safety and Security	Winfield	IL
50	The Methodist Hospital - TMC*	Geoffrey Povinelli	Director of Security Services	Houston	TX
51	Cincinnati Children's Hosptial Medical Center*	Myron Love	Manager of Protective Services	Cincinnati	OH
52	Parkland Health and Hospital System*	Kenneth Cheatle	Chief of Police	Dallas	TX
53	Cook Childrens Healthcare System*	David B. Hollar	Director of Security	Fort Worth	TX
54	MetroHealth Systems*	Deborah Bonzak	Director of Protective Services	Cleveland	OH
55	Providence Health and Services*	Michael Boyd	Chief Information Security Officer	Renton	WA
56	Harlan Laboratories*	Ted Wasky	Global Chief of Security and Safety	Indianapolis	IN
57	Good Samaritan Health System*	Lawrence Phillips	Director of Security and Emergency Preparedness	Lebanon	PA
58	Holy Cross Hospital*	Michael Paseltiner	Director, Information Services	Fort Lauderdale	FL
59	Blessing Hospital*	John Bozarth	Administrative Director	Quincy	IL
60	Indiana University Health West Hospital*	Kurt Oosterlinck	Director of Security	Avon	IN
61	Specialty Hospital of Washington-Hadley*	Melvin Stewart	Security Manager	Washington	DC
62	Coler Goldwater Specialty Hospital and Nursing Facility*	Vito Aleo	Director of Hospital Police	Roosevelt Island	NY
63	Children's Hospital of Philadelphia*	Michael Brooke	Director of Security, Parking and Transportation	Philadelphia	PA
64	St. John's Lutheran Ministries*	Tom McKenna	Director of Facility Services; Security Resident Manager	Billings	MT
65	Hoag Memorial Hospital Presbyterian*	Edward Aguilar	Manager of Security and Emergency Management	Newport Beach	CA
66	Jersey Shore University Medical Center*	Douglas Campbell	Senior Manager for Risk and Security	Neptune	NJ
67	Memorial Medical Center*	Ed Curtis	CEO; President	Springfield	IL
68	Specialty Hospital of Washington-Hadley*	Melvin Stewart	Security Manager	Washington	DC
	LISTED ALPHABETICALLY				
	Advocate Illinois Masonic Medical Center	A.L. Matthews	Public Safety Manager	Chicago	IL
	Lancaster Regional Medical Center	Jeffrey Hatfield	Director of Security	Lancaster	PA
	Lexington Medical Center	Joel B. Huggins	Director of Public Safety	West Columbia	SC
	Mercy Health - Muskegon	James Roberge	Senior Director of Facilities	Muskegon	MI
	Nationwide Children's Hospital	Daniel Yaross	Director of Security	Columbus	OH
	Shawnee Mission Medical Center	Charles Murray	Director of Security	Shawnee Mission	KS
	Tanner Health System	Gary L. Thomas	Associate Administrator for Campus and Support Services	Carrollton	GA
	Yosemite Community College District	Becky Crow	Director of Campus Safety	Modesto	CA

Hospitality/Casino

Rank	Company Name	Security 500 Member	Title	City	State
1	Marriott International, Inc.	Hector Mastrapa	Vice President of Global Safety and Security, Americas	Bethesda	MD
2	The Walt Disney Company	Ron Iden	Senior Vice President; Chief Security Officer	Burbank	CA
3	MGM Resorts International	Tom Lozich	Executive Director of Corporate Security and Surveillance	Las Vegas	NV
4	Hilton Hotels*	John Beers	Director of Safety and Security	McLean	VA
5	Hyatt Global*	Mark Sanna	Global Head of Security; Corporate Vice President	Chicago	IL
6	Royal Caribbean Cruises Ltd.*	Gary Bald	Senior Vice President; Chief Security Officer	Houston	TX
7	Caesars*	Tim Donovan	Executive Vice President; General Counsel	Las Vegas	NV
8	Starwood Hotels*	Paul Frederick	Vice President of Global Security and Safety	Stamford	CT
9	Wynn/Encore Las Vegas*	Stephanie Wallace	Director of Surveillance	Las Vegas	NV
10	Las Vegas Sands*	Brian Nagel	Senior Vice President; Chief Security Officer	Las Vegas	NV

*Estimated

Hospitality/Casino - continued

Rank	Company Name	Security 500 Member	Title	City	State
11	Augustine Casino	Karen Shinham	Director of Security	Coachella	CA
12	Casino Aztar*	Derek Boss	Director of Security	Evansville	IN
13	Gold River Casino & Casino Oklahoma	Ellery Crossman	Director of Security	Anadarko	OK
14	La Cantera Hill Country Resort	Shaun Burdick	Director of Security	San Antonio	TX
15	Boyd Gaming Corporation*	Stan Smith	Vice President of Emergency Management	Las Vegas	NV

Industrial/Manufacturing

Rank	Company Name	Security 500 Member	Title	City	State
1	Honeywell	Rich Mason	Vice President of Honeywell Global Security	Morristown	NJ
2	General Electric Company*	Art Cummings	Chief Security Officer	Fairfield	CT
3	Caterpillar, Inc.*	Timothy L. Wiliams	Director of Global Security	Peoria	IL
4	General Motors Corporation*	Coover Chinoy	Director of Enterprise Security	Detroit	MI
5	Johnson & Johnson*	Kevin Donovan	Director Enterprise Security	New Brunswick	NJ
6	United Technologies Corporation*	Lee Warren	Chief Security Officer	Hartford	CT
7	Ford Motor Company*	Chris Hager	Director of Corporate Security and Fire	Dearborn	MI
8	Procter & Gamble*	Jonathan Blumberg	Director of Global Security	Cincinnati	OH
9	ConocoPhillips	Jim Snyder	Chief Security Officer	Houston	TX
10	Pfizer*	Rod McLeod	Director of Global Security	New York	NY
11	Northrup Grumman*	Christina Morris	Chief Security Officer	Millersville	MD
12	Lockheed Martin Corporation*	Robert E. Trono	Chief Security Officer	Bethesda	MD
13	Johnson Controls, Inc.*	Bob Soderberg	Vice President of Enterprise Security; Chief Security Officer	Glendale	WI
14	Novartis International*	Andrew Jackson	Head of Global Corporate Security and Aviation	Emeryville	CA
15	Huntsman Corporation*	Ron Gerrard	Vice President of Environmental, Health and Safety; Corporate Sustainability Officer	Salt Lake City	UT
16	Abbott Laboratories*	Robert Graves	Director of Global Security	Abbott Park	IL
17	TE Connectivity Ltd.	John E. Turey	Senior Director of Enterprise Risk Management and Security	Berwyn	PA
18	Texas Instruments Incorporated*	Brian Wrozek	Director of Worldwide Security	Dallas	TX
19	Altria	Timothy J. Caddigan	Director of Corporate Security and Facilities	Richmond	VA
20	Bechtel*	Tom Depenbrock	Senior Security Manager	San Francisco	CA
21	Amgen*	Wayne Williams	Director of Corporate Security	Thousand Oaks	CA
22	Linde North America	Jim Sonntag	Security Manager, Region Americas	Stewartsville	NJ
23	Cummins, Inc.*	William Martin	Global Director of Security	Columbus	IL
24	Goodyear Tire & Rubber Company*	Mike Hunstman	Chief of Police	Akron	OH
25	Fluor Corporation*	Garry Flowers	Executive Vice President of Project Support Services	Irving	TX
26	LyondellBasell*	Sam Smolik	Vice President of Health, Safety and Environment	Houston	TX
27	Agilent Technologies	Barry Gentry	Director of Security	Loveland	CO
28	Sony Computer Entertainment America*	Pete Kutch	Director of Corporate Safety and Security	Foster City	CA
29	MWV (formerly MeadWestvaco)*	Robert Feeser	Executive Vice President of Global Operations	Richmond	VA
30	Emerson Electric*	Tony Vermillion	Vice President of Global Security	St. Louis	MO
31	Ecolab*	Hasana Sisco	Vice President of Global Safety, Health and Environment	St. Paul	MN
32	Ingersoll Rand*	Kelly Richard	Director of Global Security	Davidson	NC
33	Beckman Coulter, Inc.*	Jeff Linton	Senior Vice President; General Counsel	Chaska	MN
34	Eastman Chemical Company*	David A. Golden	Vice President	Kingsport	TN
35	Deere & Company	Jeffrey Chisholm	Director of Enterprise Security and Preparedness	Moline	IL
36	Bristol-Myers Squibb*	Amy Lyons	Vice President of Corporate Security	New York	NY
37	Actavis/Watson Pharmaceuticals	Paul Bisaro	Chairman; Executive Director	Parsippany	NJ
38	Rockwell Collins	Michael J. Sullivan	Director of Security	Cedar Rapids	IA
39	Reynolds American, Inc.	Stephen A. Grimaldi	Director of Corporate Security	Winston-Salem	NC

*Estimated

Industrial/Manufacturing - continued

Rank	Company Name	Security 500 Member	Title	City	State
40	Hospira	Dan Colin	Director of Global Security and Privacy Officer	Lake Forest	IL
41	Emergent BioSolutions	Mark Alley	Senior Director of Global Protective Services and Public Affairs	Lansing	MI
42	General Dynamics Corporation*	Raymond H. Musser, CPP	Director of Security	Falls Church	VA
43	DuPont*	Donald Ostmann	Director of Security, North America	Wilmington	DE
44	Dow Corning*	Kevin Kendrick	Corporate Vice President of Global Security	Midland	MI
45	Boston Scientific*	Mark Darmiento	Director of Global Security	Marlborough	MA
46	Kohler Company	Patrick McCarthy	Director of Global Security	Kohler	WI
47	Herman Miller, Inc.	Dan Wilkins	Security Manager	Zeeland	MI
48	Colgate-Palmolive*	Lori Michelin	Vice President of Global Sustainability and Environmental, Health and Safety	New York	NY
49	Mattel*	Brian Blome	Vice President of Global Security and Investigations	El Segundo	CA
50	Carestream Health, Inc.	Thomas J. Rohr Sr., CPP	Director of Worldwide Corporate Security	Rochester	NY
51	The Dow Chemical Company*	Timothy J. Scott	Chief Security Officer; Corporate Director of Emergency Services and Security	Midland	MI
52	Weyerhaeuser Company*	Sara Kendall	Vice President of Corporate Affairs and Sustainability	Federal Way	WA
53	Westinghouse Electric Company*	Russ Cline	Director of Global Security	Madison	PA
54	International Paper*	Donald Macdonald	Director of Corporate Security	Memphis	TN
55	Harlan Laboratories	Ted Wasky	Global Director of Security and Safety	Indianapolis	IN
56	Amway*	Terry Celori	Manager of Enterprise Protection Services	Ada	MI
57	Watson Pharmaceuticals*	Gary D. Stewart	Director of Security	Corona	CA
58	Biogen Idec	Daniel Biran	Vice President of Global Security	Cambridge	MA
59	Bose*	Michael Phillips	Director of Global Security	Framingham	MA
60	W.L. Gore & Associates, Inc.*	Ken Ford, CPP	Global Security Leader	Newark	DE
61	Sanofi*	David Kent	Vice President of Security	Bridgewater	NJ
62	Logitech*	Scott Sidlow	Senior Manager for Environmental, Health and Safety; Security	Newark	CA
63	Textron Systems Corporation*	E. Robert Lupone	Executive Vice President; General Counsel and Secretary	Wilmington	MA
64	Dixie Brands, Inc.*	Sy Alli	Director of Corporate Security		
65	Autodesk, Inc.*	Dave Ego	Senior Manager of Global Safety and Security/CREFTS	San Rafael	CA
66	Infinera*	Dennis Hawker	Global Security Manager	Sunnyvale	CA
67	Vishay Siliconix*	Mansour Farahmand	Security Manager	Santa Clara	CA
68	Palantir*	Geoff Belknap	Director of Global Security	Palo Alto	CA
69	Weatherford International*	Andrew Baer	Director of Global Security	Dublin	
	LISTED ALPHABETICALLY				
	Briggs & Stratton Corp.	Dave Droster	Director	Wauwatosa	WI
	Kimberly Clark Corporation	James T. Murphy	Vice President of Global Security	Irving	TX
	Merck	Grant Ashley	Vice President of Global Security and Aviation	Whitehouse Station	NJ
	Navistar	Jeff Medek	Director of Global Security	Lisle	IL
	PING, Inc.	Doyle Parker	Director of Security and Telecommunications	Phoenix	AZ
	Raytheon	Dan Schlehr	Vice President of Global Security Services	Waltham	MA
	Teradyne, Inc.	Katherine L. Collins	Global Manager of Corporate Security	North Reading	MA
	The Boeing Company	Dave Komendat	Vice President; Chief Security Officer	Chicago	IL

*Estimated

Information Technology/Communications/Media

Rank	Company Name	Security 500 Member	Title	City	State
1	Dell, Inc.	John E. McClurg	Vice President; Chief Security Officer	Austin	TX
2	Microsoft Corporation	Mike Howard	Chief Security Officer	Redmond	WA
3	Verizon Communications*	Michael Mason	Chief Security Officer	Basking Ridge	NJ
4	Viacom, Inc.	John Honovic, CPP	Vice President of Security and Business Continuity	New York	NY
5	International Business Machines Corp.*	Joe Morton	Chief Security Officer	Armonk	NY
6	Google*	Eran Feigenbaum	Enterprise Director of Security	Mountain View	CA
7	Oracle Corporation*	Mary Ann Davidson	Chief Security Officer	Redwood City	CA
8	EMC Corporation*	Dave Martin	Chief Security Officer	Hopkinton	MA
9	Apple*	David Rice	Director of Global Security	Cupertino	CA
10	Juniper Networks, Inc.	Doyle B. Minnis, CPP	Senior Director of Safety and Security	Sunnyvale	CA
11	Symantec Corporation*	Chris Berg	Senior Director of Corporate Security and Safety	Mountain View	CA
12	VMware	Joseph Brown	Director of Global Security and Safety	Palo Alto	CA
13	Yahoo*	Greg Jodry	Director of Corporate Security and Safety	Sunnyvale	CA
14	Hitachi Data Systems	Michael Clements	Director of Global Protective Services	Santa Clara	CA
15	Intuit, Inc.	Thomas Hale	Director of Corporate Security	Mountain View	CA
16	NVIDIA Corporation	Jensen Huang	Chief Security Officer; Head of Global Protective Services	Santa Clara	CA
17	AT&T*	Ed Amoroso	Chief Security Officer; Senior Vice Presidnet	Dallas	TX
18	McAfee, Inc.*	Brent Conran	Chief Security Officer	Santa Clara	CA
19	Citrix Systems, Inc.*	Michael John	Director of Safety and Security	Santa Clara	CA
20	Facebook, Inc.*	John Sullivan	Chief Security Officer	Menlo Park	CA
21	Intel*	David Hoffman	Director of Security Policy; Global Privacy Officer	Santa Clara	CA
22	Sprint Nextel*	Perry Siplan	Chief Security Officer	Overland Park	KS
23	Progress Software	Richard King	Director of Corporate Security	Bedford	MA
24	Sony Pictures Entertainment*	Stevan Bernard	Executive Vice President	Culver City	CA
25	T-Mobile USA*	William Boni	Vice President; Chief Information Security Officer	Bellevue	WA
26	salesforce.com*	Patrick Heim	Senior Vice President; Chief Trust Officer	San Francisco	CA
27	Time Warner*	Raymond Drayton	Director of Corporate Security	New York	NY
28	DreamWorks Animation SKG*	Matthew Bogaard	Head of Corporate Security	Glendale	CA
29	Turner Broadcasting System, Inc.*	Bart Szafnicki	Vice President of Corporate Security	Atlanta	GA
30	Paramount Pictures*	Scott LaChasse	Vice President of Security and Emergency Services	Los Angeles (Hollywood)	CA
31	Vantiv*	Kim Jones	Chief Security Officer	Cincinnati	OH
32	AMC Networks*	Bruce Turtell	Director of Safety and Security	New York	NY
33	Sybase*	Larry Eade	Senior Director of Corporate Security	Dublin	CA
34	Pandora*	Gary Backus	Manager of Safety and Security	Oakland	CA
35	CBS*	Tom Cruthers	Senior Vice President of Corporate Services; Chief Security Officer	New York	NY
36	Twitter*	Greg Acton	Head of Safety and Security	San Francisco	CA
37	McGraw Hill Financial*	Robert Pritchard	Vice President; Chief Security Officer	New York	NY
38	Fox Entertainment Group*	Richard Culver	Vice President of Security, Environmental Health and Safety	Los Angeles	CA
39	EDM Americas, Inc.	Aaron Pappa	Senior Director of IT Infrastructure	Scranton	PA
	LISTED ALPHABETICALLY				
	Adobe Systems	Brad Arkin	Vice President; Chief Security Officer	San Jose	CA
	CISCO	David Walters	Director of Global Safety and Security	San Jose	CA
	Comcast Corporation	Mark Farrell	Chief Security Officer	Philadelphia	PA
	Frontier Communications	Lynne Monaco	Corporate Director of Safety and Security	Rochester	NY
	Nielsen	Robert Messemer	Chief Security Officer	Schaumburg	IL

*Estimated

Ports/Terminals (Sea, Land, Air)

Rank	Company Name	Security 500 Member	Title	City	State
1	Port of Long Beach	Randy Parsons	Director of Security	Los Angeles	CA
2	Massachusetts Port Authority*	Joe Lawless	Director of Maritime Security; Chief of Massport Police	Baltimore	MD
3	The Port Authority of New York and New Jersey	Joseph Dunne	Chief Security Officer	New York	NY
4	Port of Beaumont	Stephen Davis	Chief of Police	Beaumont	TX
5	Chicago O'Hare International Airport*	Richard A. Fisher, CPP, CFE	Federal Director of Security	Chicago	IL
6	Los Angeles World Airports*	Patrick Gannon	Director for Homeland Security and Public Safety	Los Angeles	CA
7	Hartsfield-Jackson Atlanta International Airport*	Balram Bheodari	Aviation Deputy General Manager	Atlanta	GA
8	Port of Los Angeles	Ronald Boyd	Chief of Port Police and Security	Los Angeles	CA
9	Port of Houston Authority*	Mark Smith	Chief of Police	Houston	TX
10	San Francisco Airport*	John Garrity	Commander	San Francisco	CA
11	Miami International Airport*	Lauren Stover	Assistant Aviation Director of Public Safety and Security	Miami	FL
12	Dallas-Fort Worth Airport*	Alan Black	Vice President of Operations	DFW Airport	TX
13	GA Port Authority*	John Trent	Senior Director of Strategic Operations and Safety	Savannah	GA
14	Virginia Port Authority	Colonel Michael L. Brewer	Chief of Police	Front Royal	VA
15	Austin Bergstorm International Airport*	Denise Hatch	Security Manager	Austin	TX
16	Port of Corpus Christie*	H. Archambo	Chief of Port Police and Security	Corpus Christie	TX
17	Port of Greater Baton Rouge*	Cortney White	Director of Engineering and Security	Port Allen	LA
18	Port of San Francisco*	Ken Tashian	Program Manager for Homeland Security	San Francisco	CA
19	Port of Savannah	Thomas Tickner	District Commander	Savannah	GA

Retail/Connected Commerce

Rank	Company Name	Security 500 Member	Title	City	State
1	eBay	George Booth	Senior Director	San Jose	CA
2	Limited Brands	John Talamo	Vice President of Loss Prevention and Safety Services	Columbus	OH
3	AMAZON	George Stathakopoulos	Vice President of Information Security	Seattle	WA
4	Wal-Mart Stores, Inc.*	Kenneth Senser	Senior Vice President	Bentonville	AR
5	CVS Caremark Corporation*	Kenneth P. Mortensen, Esq., CIPP/US, CIPP/G, CIPM	Vice President; Assistant General Counsel; Chief Privacy Officer	Woonsocket	RI
6	Starbucks Coffee Company*	Jack Sullivan	Vice President of Global Safety and Security	Seattle	WA
7	AutoZone, Inc.	Libby Rabun	Vice President of Loss Prevention	Memphis	TN
8	Costco*	Larry Mongague	Director of Security	Issaquah	WA
9	The Kroger Co.*	Karl Langhorst	Director of Loss Prevention	Cincinnati	OH
10	Lowe's Companies, Inc.*	Claude Verville	Vice President of Loss Prevention, Safety and Hazmat	Mooresville	NC
11	Target Corporation*	Brad Maiorino	Chief Information Security Officer	Minneapolis	MN
12	Safeway*	Kathleen Smith	Corporate Vice President of Loss Prevention	Pleasanton	CA
13	Kohl's Corporation*	Randy Meadows	Senior Vice President of Loss Prevention	Menomonee Falls	WI
14	Brinker International	Wyman Roberts	CEO	Dallas	TX
15	Best Buy*	Erik Buttlar	Senior Director of Asset Protection	Richfield	MN
16	Walgreens*	Tim Belka	Senior Director of Global Security	Springfield Township	IL
17	ARAMARK*	Jay Hess	Global Security Director	Philadelphia	PA
18	Dave & Buster's, Inc.	James Brussow	Director of Security	Dallas	TX
19	Big Y Foods, Inc.	Mark Gaudette	Director of Loss Prevention	Springfield	MA
20	Jack in the Box*	Gene W. James, CPP	Director of Asset Protection	San Diego	CA
21	Sports Authority*	John Clark	Director of Corporate Asset Protection	Englewood	CA
22	Domino's Pizza, Inc.	Van Carney	National Director of Safety and Loss Prevention	Ann Arbor	MI
23	Tween Brands - Justice and Brothers Stores	Robert LaCommare, CFI	Associate Vice President of Loss Prevention and Risk Management	New Albany	OH
24	Art Van Furniture	Michael F. Case	Director of Loss Prevention	Warren	MI
25	Cabela's*	David O'Brian	Director of Corporate Asset Protection	Sidney	NE

*Estimated

Retail/Connected Commerce - continued

Rank	Company Name	Security 500 Member	Title	City	State
26	Ann, Inc.*	Maurice Cloutier	Vice President of Corporate Loss Prevention	New York	NY
27	Dressbarn	Brian Bazer	Assistant Vice President of Asset Protection and Risk Management	Mahwah	NJ
28	Gap, Inc.*	Marjorie Jackson	Director of Global Corporate Security	San Francisco	CA
29	Ascena Retail Group, Inc.	Eric Pidgeon	Director of Loss Prevention - Global Supply Chain	Pataskala	OH
30	Raley's*	Jack Leidecker	Director of IT Security	West Sacramento	CA
31	Quiksilver*	Kevin Hatcher	Director of Security	Huntington Beach	CA
32	Overwaitea Food Group*	Keith Colonval	Director of Resource Protection	Vancouver	BC
33	Wendy's*	Chris Manning	Director of Loss Prevention and Security	Dublin	OH
34	Things Remembered	James Baumgart	Senior Manager of Loss Prevention	Heighland Heights	OH
35	Under Armour*	Frederick H. Bealefeld III	Chief Security Officer	Baltimore	MD
36	Express, Inc.*	Joe Reisinger	Vice President of Brand Security	Columbus	OH
	LISTED ALPHABETICALLY				
	Nutrisystem, Inc.	Bill Durso	Senior Director of Security, Facilities and Office Services	Fort Washington	PA
	Ralph Lauren Corporation	Shawn Segers	Senior Director of Corporate Security	New York	NY

Spectator Sports (Arenas/Stadiums/Venues)

Rank	Company Name	Security 500 Member	Title	City	State
1	MetLife Stadium	Daniel DeLorenzi	Director of Security	East Rutherford	NJ
2	FedEx Field*	Chris Bloyer	Vice President of Operations	Landover	MD
3	Arrowhead Stadium*	Brian Schaeffer	Manager of Security	Kansas City	MO
4	Cowboy Stadium*	Jeff Stroud	General Manager	Arlington	TX
5	Yankee Stadium*	Todd Letcher	Executive Director	New York	NY
6	SMG, Mercedes Benz Superdome*	Donald Paisant	Chief of Public Safety	Foster City	CA
7	Staples Center*	Lee Zeidman	President	Framingham	MA
8	The Rose Bowl*	George Cunningham	Chief Operations Officer	Pasadena	CA
9	Sun-Life Stadium*	Todd Boyan	Senior Vice President of Operations	Miami Gardens	FL
10	Gillette Stadium*	Kelly Way	Director of Operations	Foxboro	MA
11	Busch Stadium	Joe Abernathy	Vice President of Stadium Operations	St. Louis	MO
12	Comcast Spectacor, Wells Fargo Center*	Mike Hasson	Vice President of Security and Services	Philadelphia	PA
13	University of Phoenix Stadium*	Joe Coomer	Director of Security and Services	Glendale	AZ
14	San Diego Padres at Petco Park*	John Leas	Executive Director	San Diego	CA

Spectator Sports (Leagues/Teams/Events)

Rank	Company Name	Security 500 Member	Title	City	State
1	National Football League	Jeffrey Miller	Vice President; Chief Security Officer	New York	NY
2	FIFA*	Ralph Mutschke	Head of Security	Zurich	Switzerland
3	Major League Baseball*	Dan Mullin	Senior Vice President of the Department of Investigations	New York	NY
4	National Hockey League	Dennis Cunningham	Vice President of Security	New York	NY
5	NASCAR*	Mike Lentz	Senior Director	Daytona	FL
6	National Basketball Association	Richard W. Buchanan	Executive Vice President and General Counsel; Chief Compliance Officer	New York	NY
7	U.S. Tennis Open	Michael Rodriguez	Director of Security	New York	NY
8	Ironman World Championship*	John Bertsch	Director of Public Safety and Emergency Management	Kailua-Kona	HI

*Estimated

Transportation/Logistics/Supply Chain/Distribution

Rank	Company Name	Security 500 Member	Title	City	State
1	YRC Worldwide, Inc.	Wayne "Butch" Day	Chief Security Officer	Overland Park	KS
2	Schneider National, Inc.	Walt Fountain	Director of Safety and Enterprise Security	Green Bay	WI
3	Ryder System, Inc.	William Anderson	Group Director of Global Security	Miami	FL
4	McKesson*	Robert Pocica	Senior Vice President; Chief Security Officer	San Francisco	CA
5	Jacobson Companies	Christopher Steinour	Security Manager	Clive	IA
6	Ingram Micro*	Bob Burbach	Vice President of Global Security	Santa Ana	CA
7	United Airlines*	Michael J. Quiello	Vice President of Corporate Safety	Chicago	IL
8	Con-way Freight*	Curtis J. Shewchuk	Chief Security Officer	Ann Arbor	MI
9	Union Pacific*	Robert Morrison	Chief of Police	North Lake (Omaha)	NE
10	Southwest Airlines	Vance Toler	Director of Corporate Security	Dallas	TX
11	Sound Transit	Kenneth Cummins	Chief Security Officer	Seattle	WA
12	Thermo Fisher Scientific*	John F. Mitchell	Director of Corporate Security	Pittsburgh	PA
13	FedEx Ground*	Paul Stritmatter	Managing Director for PPS	Pittsburgh	PA
14	American Airlines *	John Caldwell	Senior Manager - Corporate Security	Fort Worth	TX
15	US Airways, Inc.*	Paul Morell	Vice President of Safety, Security and Environmental Programs	Phoenix	AZ
16	The Jones Group*	Bryan Gilligan	Vice President of Facilities	Lawrenceburg	TN
	LISTED ALPHABETICALLY				
	Associated Grocers of NE, Inc.	Alan Cote	Loss Prevention Manager	Pembroke	NH
	Cargill	Claude Nebel	Vice President of Global Security; Chief Security Officer	Wayzata	MN
	Ferguson Enterprises, Inc.	Raymond C. Ferrara	Director of Security and Business Continuity	Newport News	VA
	Walker SCM, LLC	Derreck Brown	Corporate Security Manager	Valley Stream	NY
	WW Grainger	Keith Blakemore	Director of Corporate Security	Lake Forest	IL

*Estimated