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

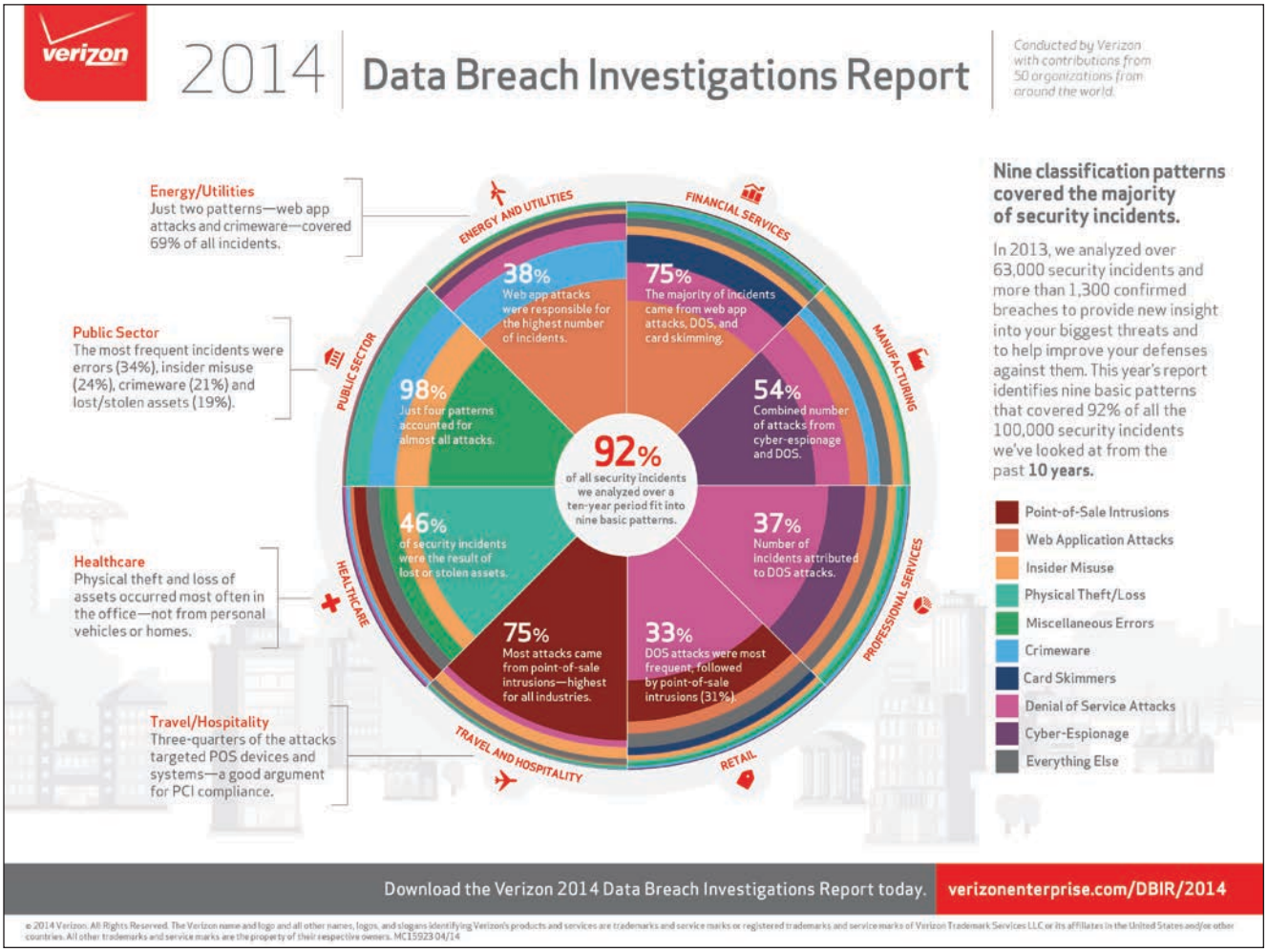
It is counterintuitive that cyber crime is the number one threat facing enterprise security leaders, because only 28 percent of those security leaders that rank it as their first concern in the Security 500 report have direct responsibility for it. Indeed, the number of incidents is growing rapidly in 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

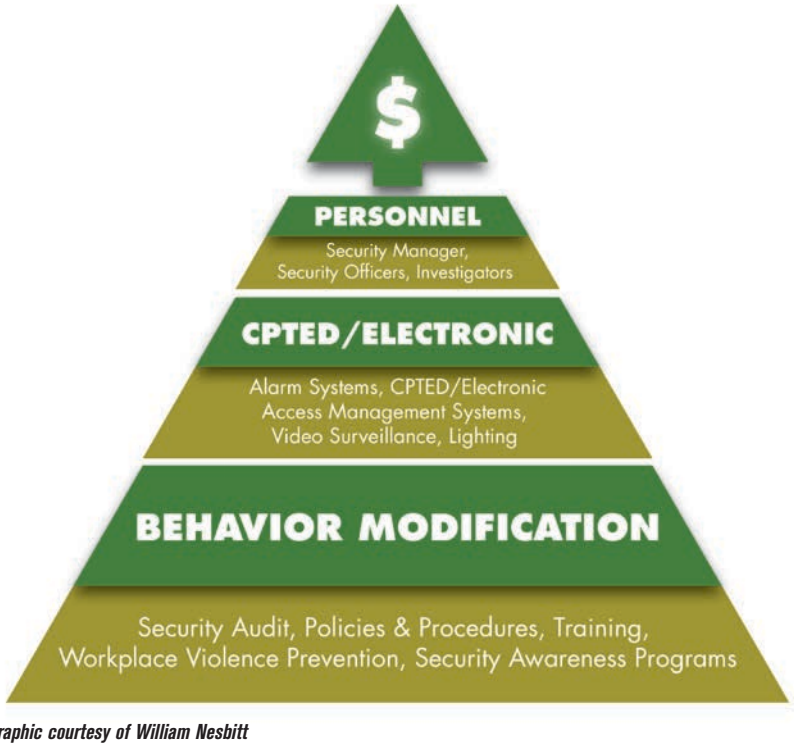
Technology integration and management appeared on the Security 500 horizon for the first time in 2012. It has remained front and center and has risen to the third-most mentioned issue this year. There are a number of factors at work here, primarily driven by risk management and security goals. And the 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.

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***



Graphic courtesy of William Nesbitt

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.

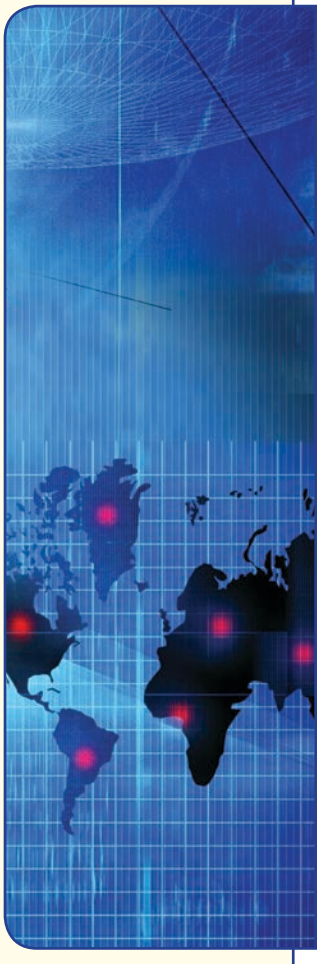
Where Security Lives

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:

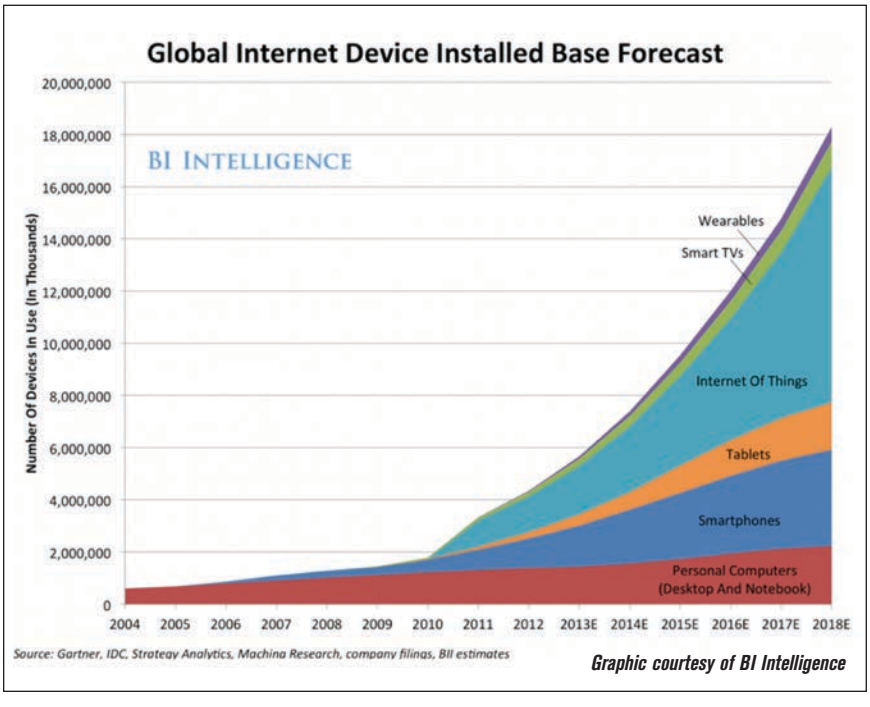
The increased role of Information Technology supporting the "security application" and moving security onto its network is driving the adoption of IP-based technologies at an ever faster pace. IT looks at technology on a "per se" basis, meaning "does this product do what it is supposed to do and solve 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.



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.

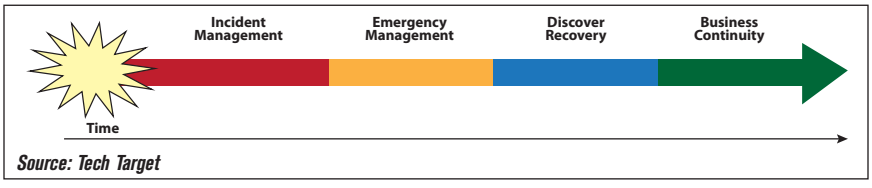
There are also compliance requirements placed on companies by their customers. More and more, security is participating in completing proposals, giving prospects tours of their security departments and engaging with customers.

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 coor-

dinated 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***

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.

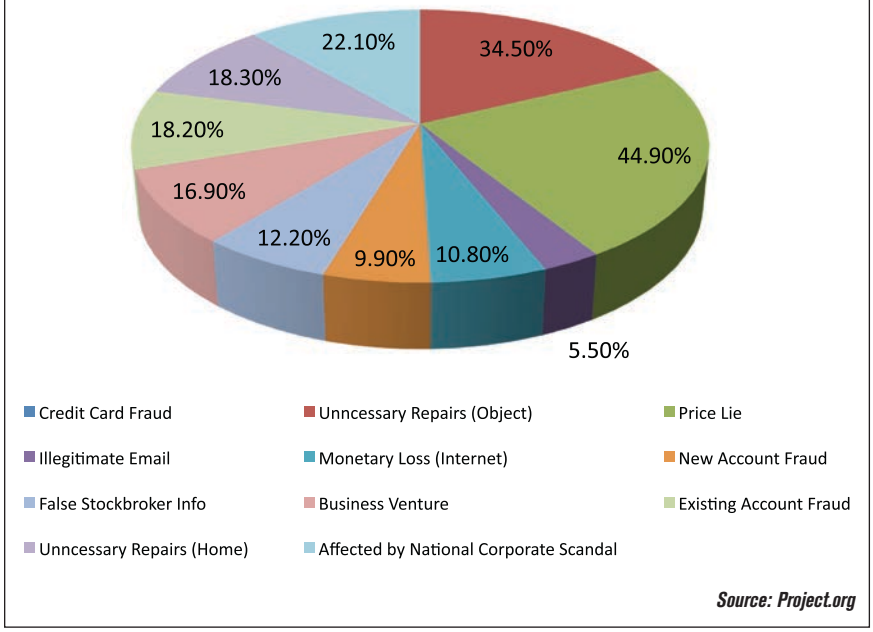
> "With retail stores, you are faced with some additional challenges like shoplifting and employee theft, return fraud, organized retail crime, online fraud and traditional robberies and burglaries. Getting merchandise from Point A to B has become much more complex."
> ***Jerry Blum, AutoZone***

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***



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.

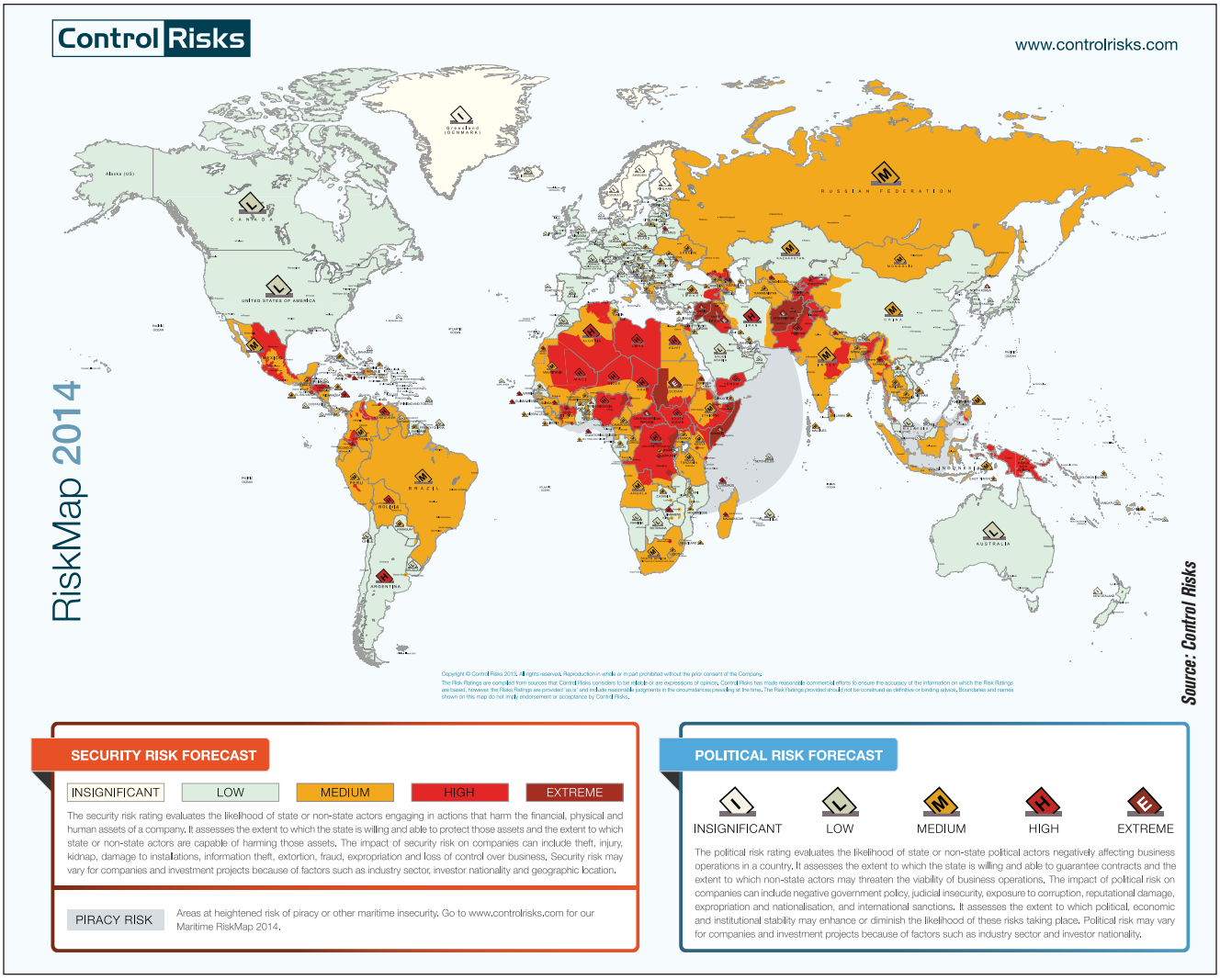
> "Companies looking for more security staff aren't going to find them – they're going to have to create them. We wanted to call attention to this security shortage because it's not a quick fix. This won't be solved in a year. It will be a four- to eight-year cycle in order to close that gap."
>
> ***John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



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 under-

standing 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 anti-corruption 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