Security’s Risk Mitigation Focus Creates a Management Risk-Nado!

By Mark McCourt, Publisher
S

ecurity 500 members are enabling enterprise missions through proactive risk and resilience programs built on strong customer service cultures. Transforming security into a service organization requires flexible strategy and brilliant execution in an ever turbulent and global Risk-Nado.

“Everyone has a plan ‘till they get punched in the mouth.”

Mike Tyson

While the economics have shifted for security organizations from an event response function to a risk management and enterprise resilience focused organization, the way forward is still being paved with innovative best practices, new ROI metrics and negotiating a dynamic threat matrix, all with a smile and a nod toward exemplary customer service and value. The vision for enterprise security has always been to protect brand, people, infrastructure and both physical and logical assets. To successfully get in front of and mitigate risks requires a visionary leader who gets the “business-side” with a highly dedicated and trained security team, all backed by C-Suite support.

“Security is about enabling a mission. Business leaders are able to take our tools and apply them to a variety of settings to create success. Our job is to create an environment of success for the enterprise. It is not what we do; rather, it is how we enable the enterprise to achieve its goals.”

Frank Taylor,
VP & CSO, General Electric

Reengineering any organization’s purpose creates challenges, the first of which is evaluating the type of leadership required to succeed. In many enterprises, security leadership changed to match new goals. Once that leader is selected, the culture and skill sets of the entire department evolve. Security 500 organizations have faced a dynamic, if not violent, transformation among its leadership during the past dozen years. Those who remained in place were strong leaders and leveraged their skills while also sharpening their business relationships and understanding; thereby enhancing their credibility. Those who were unable to meet the role’s new demands were displaced.

“We are not just there to break the glass in case of emergency.”

Mike Howard, CSO, Microsoft

Second, security’s focus on prevention and customer service demanded a new strategy for security operations. Identifying risks, threats and vulnerabilities for the purpose of mitigation so that they never come to be, requires seeing into the future as much as possible. Security is being directed to pull the lever back from event response and incident reporting to identifying threats and the enterprise’s vulnerabilities that would allow those threats to be realized. And by eliminating vulnerabilities, they significantly mitigate those threats and reduce risk.

“As we have seen in many cases it only takes one serious incident to give a brand a black eye leading to losses of millions of dollars in sales because persons do not want to frequent that brand any longer. No one can prevent crime and injuries, but it is important to provide reasonable care to mitigate the chances of serious incidents from occurring.”

Pat Murphy, Senior Director, Global Safety and Security Services, Marriott International Inc

The size and scope of risk management has outstripped manual processes to successfully identify, manage and support organizational goals. Automation is the critical piece of the puzzle. By leveraging technology through operations centers and mining big data, information is moving security in front of risk.

Perhaps this accounts for Workplace Violence being at the top of Security 500 organization’s critical issues? The statistics are measurable, the vulnerabilities are identifiable, and the process to mitigate the risk is known. Every CEO is right to ask that ensuring the safety and security of all stakeholders not be a far-off goal, but one that is achieved.

This drive to prevention is the big “aha” that security has always understood but the economics were against. No longer. The C-Suite gets that it is better for the brand, the business and the bottom line to focus on risk and resilience. And it’s the force behind the dynamic shift in organizational structures, leaders, metrics, technology and innovation in enterprise security programs. A Risk and Resilience strategy demands that enterprise security leaders not answer the question, “What is the best security program?” but rather, “What are the right security programs?”

“Security is a journey, not a destination. You are never finished. And being satisfied with a program now does not mean you will be satisfied with it tomorrow. The threats, attacks, types of attackers are always changing.”

Stephen Scharf, Senior Vice President and Global Chief Information Security Officer, Experian

Layering risk and resilience programs increases flexibility to identify risks or to mitigate threats that move through one vulnerability, then stopped by complimentary security measures. To succeed, Security 500 enterprises are strategic and focused on best practices that:
1) Develop situational awareness through intelligence gathering and analysis.
2) Create and execute enterprise risk management plans.
3) Implement and test resilience plans with stakeholders and public partners that include business continuity, disaster recovery and emergency management.
The economic benefit is security’s capacity to integrate with organizational goals and align with planning versus trying to provide security in hindsight. This mission ties directly to security’s service culture to protect stakeholders, while viewing them as their customers.

“The fascinating aspect is looking at critical risks that might arise today or in 50 years. We discuss risk as a concept beyond just the financial exposure. We look at emergency management holistically with a strong focus on risk management. What capabilities do we have and which do we need to identify and mitigate threats? How do we identify and eliminate our vulnerabilities? From supporting the community’s planned events to preparing for the unknown, our job is to both be ready today and to look ahead.”

Bijan Karimi,
Assistant Deputy Director,
City of San Francisco, Department of Emergency Management

Workforce Protection and travel management is an example of the perfect storm balancing risk and resilience management with a customer service culture. The trend toward “Big Data” includes fusing intelligence from multiple sources into a command or operations center (such as a GSOC) to both look to the future and identify risks that may impact a traveling employee. The ability to notify that employee and support their business travel needs and work goals supports the enterprise and the employee, and it exemplifies security’s value.

“My focus is to be an ambassador for security. It is very rewarding to be in the schools and talk with the students, teachers and parents. Being proactive identifies risks. Most rewarding is to go to work every day with tomorrow’s leaders and have a customer service mindset.”

Joseph Perchetti,
Supervisor of Security,
Radnor Public School District (PA)

This is one reason that security technology and integration, especially in Security Operations Centers, have increased dramatically among Security 500 member focus in two prior Security 500 surveys. Enterprises are leveraging technology to gather and analyze risk-related information such as political unrest, weather, natural disasters, terrorism, organized crime data and service disruptions such as power.

There is another reason that the enterprise risk program’s focus and purpose to mitigate risk by eliminating vulnerabilities through an ongoing security program. A significant component is communication with stakeholders, as security is everyone’s job. Communicating, educating and gaining buy-in from stakeholders to actively participate in their personal security as well as the protection of organizational assets (physical and logical) and infrastructure is a force multiplier. A recent example of a successful program includes the “See Something, Say Something” program from DHS and texting at NFL games.

“Our role is to protect people, places and products. We are aligned to the HR department because security is about people first and foremost. We developed a Command or Global Security Operations Center to proactively communicate with and protect our employees. It is important that they feel secure, especially as we expand to international markets.”

Timothy Caddigan,
Director, Corporate Security & Facilities, Altria Client Services

If and when creating situational awareness and eliminating identified risks fails, the third pillar of a successful program must be ready to kick into action. Enterprise Resilience includes business continuity, emergency management and disaster recovery to respond and recover from unanticipated events. These programs are designed to protect life, limit damage and restore normal operations as quickly as possible. First responders, public/private partnerships, mass notification and consistent training are staples of enterprise resilience best practices.

“The leadership of any enterprise is challenged to keep their eye on the security or emergency ‘ball’ and therefore must provide the resources and structure to allow for it take place on a continuous basis. Our president encourages the development of plans, testing communication systems and stress training to prepare and respond to events.”

Bob Harkins,
Associate Vice President for Campus Safety and Security,
The University of Texas at Austin

Among the key economic measures to support enterprise risk and resilience management programs are the cost/benefit analysis to evaluate the downtime cost of outages, lost customers/orders and post-event costs (e.g. insurance cost due to a higher risk portfolio), compared to the investment in best practices to identify and mitigate identified risks. Not every identified risk is mitigated. Risks forecast to have minimal impact are recognized, but not mitigated.

“Security contributes by translating a complicated set of practices and merging them into a set of businesses strategies. How much risk we accept and how much risk we choose to mitigate is translated into business proposals and decisions.”

Stephen Scharf,
Senior Vice President and Global Chief Information Security Officer, Experian

Security 500 member best practices and management excellence include:

1. Address risk first and foremost by using intelligence and analysis to create enterprise-wide situational awareness that identifies threats. Security mitigates risks by eliminating vulnerabilities and preparing for unforeseen events by having a robust resilience program.

2. Organizationally, security is enterprise-wide. Leading security programs eliminate silos by managing from a single, global or enterprise-wide office of the CSO combining corporate, physical, logical and cyber security programs within one organization to eliminate weak links.

3. Security leaders raise risk to their organization’s top line by working to support bottom-line goals and values. Focusing risk and resilience programs and spending on helping their enterprise achieve its mission exemplifies security’s contribution and economic value in identifiable and measurable ways.

4. Represent the enterprise’s brand and have a customer-centric service culture and outlook on security’s role of purpose.

5. Leverage technologies, especially Global Security Operations Centers, Cyber Security Operations Centers and guard tour technologies that complement or reduce manual labor, such as video surveillance. Big data analytics can be applied to create situational awareness

Radnor Public School District (PA)

November 2013 • SECURITY • SecurityMagazine.com
by identifying threats and eliminating vulnerabilities.  
6. Contribute to the organization’s overall vision and mission by enabling the organization to effectively and efficiently achieve its goals.  

While too many critical issues are mentioned in the annual survey for review, we analyze those most frequently noted as areas where budget and resources are being allocated for the coming year.

“CEOs should know about Security that they need an entity in the organization to think about risk and security full time. We learn from every crisis and get better as a result. We have warts, yes, but we work on removing those warts every day.”

Frank Taylor, Vice President and Chief Security Officer, The General Electric Company

2013 KEY TRENDS AND AREAS OF FOCUS:

1. Workplace Violence

Despite significant investment in both educational programs, zero tolerance policies and enhanced access technologies; workplace violence rose to the number one area of focus in 2013. The workplace violence statistics are numbing. OSHA reports that more than two million American workers are victims annually, most of whom work in healthcare. One respondent in healthcare noted that successful mitigation requires a constant security presence, which is costly: “Our officers perform an average of 110 one-on-one observations (stand-bys) every month, with 35 percent of those patients becoming unruly/combatative.” Yet, it was noted that this policy has prevented serious injury or legal action for more than 20 years.

The number of workplace homicides has declined from a high of 1,080 in 1994 to a low of 518 in 2010. In 2011, nearly one in five workplace fatalities was attributed to workplace violence (780 or 17 percent of all workplace fatalities). Of those fatalities, 36 percent of men were most likely to be killed by a robber, while 39 percent of women were most likely to be killed by a relative or domestic partner. Murder is the leading cause of death for women in the workplace.

The FBI has identified four types of workplace violence:
1. Violent acts by criminals with no connection to the workplace or the victim(s).
2. Violent acts against employees by customers, students, patients or others for whom the organization provides services.
3. Co-worker violence against another co-worker or co-workers.
4. Violence by a non-employee who has a relationship with an employee.

In this year’s Security 500 survey, definition number two – violent acts against employees by customers, students, patients or others for whom the organization provides services – received significant mention. While this has been a significant risk and issue in healthcare, it is also growing in other sectors. Managing the behavior of the very people or guests you are protecting is a growing challenge for security. Many organizations are investing limited security resources to respond to inappropriate or illegal activity by their own employees, students, patients, fans and hotel or mall retail guests. The liability for failing to do so is clear. Brad Reid, Senior Scholar, Dean Institute for Corporate Governance and Integrity, Lipscomb University, recently wrote on the Huffington Post:

While the terminology varies somewhat, businesses may anticipate three categories of individuals entering their premises: guests, invitees, and trespassers. A “guest” is one having a specifically addressed personal invitation to enter the property, such as a mayor invited to a grand opening. An “invitee” is an individual reasonably expected to enter the property, such as a customer or an employee, but who has not been personally invited like the guest. A “trespasser” is an unlawful intruder. In the absence of specific legislation or regulation, the common law doctrine of negligence applies to virtually all injuries that guests, invitees, or trespassers might receive at the hands of an outsider who enters the business premises. Strict liability may apply to a business engaged in intentional wrongdoing or conducting ultra-hazardous activities. Negligence law imposes a high duty of care by the business toward guests, reasonable care toward invitees, and low or no care toward adult trespassers.

He also pointed out a recent lawsuit where the workplace violence was perpetuated by customers and the liability of the business “must take appropriate measures to protect persons on the premises from foreseeable criminal acts of third parties.”

Communicating with stakeholders, identifying appropriate behavior and best practices and responding to these behavioral issues is an ongoing effort. Sports leagues, especially the NFL, have employed texting so that fans can alert security to inappropriate behavior by other fans. Perhaps what was once college students being stupid has become an incident, because not taking action now may result in later legal, brand reputation and operational expenses. As tolerance continues to move toward zero, enterprises will increasingly take action and report incidents. And the investment to manage this crowd or stakeholder control related risk will rise accordingly. According to Meagan Newman of law firm Seyfarth Shaw, “In all cases, it is less expensive to prevent an incident than it is to deal with the aftereffects.”

In addition to clear, zero tolerance policies against workplace violence, leading security enterprises are:
• Providing regular training
• Supporting victims of workplace and domestic violence
• Adopting and practicing consistent and fair discipline
• Fostering a climate of trust between employees and management
• Leveraging external resources to support the program and employees

2. Budgets

As enterprise security builds a strategic program including situational awareness, risk management and resilience, the requirements to successfully execute, hire, train and maintain a high level of awareness, proactive mitigation and preparedness stresses budgets.

In 2013, budgets across the Security 500 increased in nearly half of all organizations by an average of nine percent. More than 83 percent reported their budget increasing or remaining the same. Among the 17 percent with reduced budgets, the reduction was eight percent, on average. Compared with the 2012 survey, the overall results are best defined as flat.

In 2012, 57 percent reported increases, 27 percent remained the same and 16 percent reported decreases. In both cases, the increases and decreases averaged 9 percent.

Enterprise security leaders implementing single, enterprise-wide risk and resilience programs are taxed to justify all components of their ERM plan through implementation. At the core of this planning program are GSOCs, or global security...
operations centers. GSOCs are critical for the collection and analysis of risk and incident information, situational awareness for response and a communications hub to connect with first responders, law enforcement, stakeholders and the broader community. GSOCs deliver significant value by protecting physical assets including infrastructure and facilities for the aforementioned reasons of technology replicating humans, and the ability to collect risk and security information at the local level while monitoring and managing it at the GSOC.

"Our three Global Security Operations Centers allow us to see how events around the world are impacting our 700-plus Microsoft locations and to display the critical information we need to assess situations much faster."

Brian Tuskan, Microsoft

The ability to attract, train and retain qualified employees with unique skills is also a budgetary issue. As the job responsibilities and employees’ skill requirements increase, so do the salary and benefits. This issue is addressed as critical issue number seven in the Security 500 report.

Budget limitations are also an issue around stakeholder communications. The ability to create situational awareness and alert stakeholders to risks has the most value when you are able to alert them to the risks in a way that they can secure or protect themselves. After all, why have an expensive shark detection technology if you cannot alert swimmers that there are sharks? What is the point of effectively notifying them about sharks if they refuse to get out of the water?

Identifying the best ways to get the attention and appropriate stakeholder behavior pressures budgets. The funding to continually educate and remind people to be aware, protect themselves and take appropriate emergency action requires spending. These exercises, tests and drills tend to face budgetary scrutiny as time progresses without an event.

"Security can do whatever you want it to; it just comes at a cost. The correct answer is finding the money for service or cost centers that refresh the technology to consistently contribute to business goals. Our goal is patient security and service and our investments must support that."

Gordon Snow, Chief of Protective Services, The Cleveland Clinic

As C-Suite executives better understand risk mitigation’s value versus event response and/or experience, a security-related event whose impact is reduced or eliminated as a result of preparedness, budgets for stakeholder protection training should expand.

3. Cyber Crime

We are building our lives around our wired and wireless networks. The question is, are we ready to work together to defend them?

This headline appears on the FBI’s Cyber Crime homepage. Each day or minute, both cyber threats and cyber security solutions leap over one another in an endless game of checkers. As one CSO noted in the Security 500 survey, “The security and privacy of client data are and always have been our top priorities. Trust and confidence about the security of account information is the bedrock of our relationships with our clients.”

The most notable cyber crime of 2013 involved a cyber blitz when 2,904 ATMs were combined with an old-fashioned frat: on-the-street bank robbery. In New York City on February 19, thieves stole $45 million in a matter of hours. The criminals were sophisticated computer experts who hacked into and changed confidential banking information so that withdrawals would be approved.

While this single crime was highly publicized in the media, there are many cyber crimes that go unnoticed. The Internet Crime Complaint Center received more than 289,000 cyber crime complaints in 2012, including:

• Total complaints received: 289,874
• Complaints reporting loss: 114,908
• Total Loss: $525,441,110.00
• Median dollar loss for those reporting a loss: $600
• Average dollar loss overall: $1,813
• Average dollar loss for those reporting a loss: $4,573

The biggest data breach in 2013 (as of publication) was a break-in to computers of retail chains that included 7-Eleven and Carrefour. U.S. prosecutors indicted four Russians and a Ukrainian for the crime. The criminals led a “worldwide scheme that targeted major corporate networks, stole more than 160 million credit card numbers and resulted in hundreds of millions of dollars in losses,” said Paul Fishman, the U.S. attorney in New Jersey.

A recent HB Gary study warned that public companies should be concerned that cyber attacks can affect investor decisions and stock prices. For example:

• 67 percent of investors are likely to research whether a company has been fined or sanctioned for previous cyber security incidents.
• 69 percent are unlikely to invest in a company with a history of data breaches.
• 78 percent are unlikely to invest in a company with a history of one or more cyber attacks.
• 71 percent would be interested in reviewing a company’s cyber security history if it was included in regulatory filings.
• 66 percent of investors are more concerned about a company’s reaction to a cyber attack that the attack itself.
• Investors are twice as concerned about customer data (57 percent) versus theft of intellectual property (29 percent).
Edward Snowden’s leaking of National Security Agency documents and subsequent interview revealed that the NSA deliberately introduced flaws into cryptographic systems to ensure it could read encrypted traffic. By deliberately inserting vulnerabilities into cyber security product design, the NSA may have made every CSO’s job more difficult to mitigate cyber threats.

Cyber threats and crime are not under one broad definition. The term APT, for advanced persistent threat, is a good qualifier to identify the security challenge. The attack is advanced; meaning mitigation and defense may not be in place or may not exist. It is persistent, so if it doesn’t succeed now, it tries continuously to do so. Each sector of the Security 500 has their unique risks and areas of focus to protect information and prevent loss. Among those noted in the survey and briefly defined are:

SCADA: An acronym for supervisory control and data acquisition, a computer system for gathering and analyzing real-time data. SCADA systems are used to monitor and control a plant or equipment. A cyber attack could take control over these industrial systems and cause widespread damage.

Hactivism: Hacking for social or political causes by causing a denial of service attack or taking over a major media organization’s website and posting messages. A recent example is the Syrian Electronic Army’s attacks on the New York Times, Twitter and Huffington Post’s UK websites.

Identity Theft: The act of stealing another person’s identity to create fraudulent credit accounts or use their identity to illegally gain access to the actual person’s assets is a significant issue for sectors with significant financial or intellectual property entrusted to them. It is estimated that more than 9 million people have their identities stolen annually, and there are more than 10,000 active criminal identity theft rings in the U.S.

Consumerization of IT/BYOD: As stakeholders select the types of devices they want for both personal and business use, they bring risks such as viruses or bots to the enterprise network. Also they leave with potentially valuable intellectual property, data and other logical assets.

Social Engineering Hacking: Phishing and Pharming, Smishing and Vishing: The art of tricking the human or “human hacking” to get information. Phishing is a form of online identity theft that lures consumers into divulging their personal financial information to fraudulent websites, also known as spoofed websites. Pharming is similar to phishing but more sophisticated. Pharmers also send emails. The consumer, however, can be duped by the pharmer without even opening an email attachment. Smishing is an identity theft scheme that involves sending consumers text messages containing a link to a fraudulent website or a phone number in an attempt to collect personal information. Vishing involves the use of Voice over Internet Protocol (VoIP). Fraudsters use this technology to trick people into divulging their personal financial information through one of the most trusted forms of communication: the telephone.

Cloud Computing: Your data is on another organization’s system. If they are hacked, you are hacked. It is not about the cloud so much as about securing the data.

Incident Response: With cyber criminals successfully targeting organizations of all sizes across all industry sectors, organizations need to be prepared to respond to the inevitable data breach. Recommended reading includes 10 Steps to Planning an Effective Cyber Incident Response, Harvard Business Review, by Tucker Bailey and Josh Brandley, July 2013.

Insurance: With the probability that your enterprise will be successfully hacked, enterprises are buying off the risk with cyber insurance. Gone are the days of The Graduate being advised to pursue a career in “plastics.” Now is the day to whisper in your children’s ears: “cyber law.”

4. Physical Security

Your C-Suite might be tired of hearing copper wire theft stories, but the thieves are not tired of stealing it. The C-Suite does not like thinking that their employees may

**Where Security Lives:**

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>COO/Operations</td>
<td>17%</td>
</tr>
<tr>
<td>Risk/Legal/General Counsel</td>
<td>16%</td>
</tr>
<tr>
<td>CEO/President/Executive Management</td>
<td>15%</td>
</tr>
<tr>
<td>CFO/Finance</td>
<td>12%</td>
</tr>
<tr>
<td>Facilities</td>
<td>12%</td>
</tr>
<tr>
<td>CAO/Administration</td>
<td>11%</td>
</tr>
<tr>
<td>Human Resources</td>
<td>9%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
<tr>
<td>CIO/IT</td>
<td>3%</td>
</tr>
</tbody>
</table>

Security continues to move around in the enterprise as organizations both recognize its strategic value and seek the best cultural fit, while grappling with the myriad issues risk itself raises for any enterprise. From security’s goal to change personnel’s behavior (HR), manage complex regulatory issues (Legal), tackle the high growth issue of cyber crime (IT), recognize risk as a balance sheet item (Finance), understand its basic function (facilities or store operations) to showing a clear bottom line value (CEO); CSOs in similar sectors often encounter highly different cultures and organizational charts. As one CSO shared, “When a new CEO comes in and wants to make changes for the sake of change, Security appears like an easy place to do it.”
be the thieves, either. That is a metaphor for the challenge of keeping an enterprise's attention and interest in securing both their own and their employer's property as well as to participate in their own safety. Organizations are facing a number of ongoing and increasing physical security risks from both external and internal threats. Further, the need to identify and manage guests to reduce potential loss requires both technical and human vigilance.

"Our mission is to maintain a pleasant, family-oriented environment. Security is a critical element of the equation for a successful property. The mall environment is unique and lots can occur. First, we have a complex community with many tenants, people and events that include measurable risks. We identify both minimal and elevated risks, build security programs around them and measure our results. We have a very high success rate."

Dan Ryan, Senior Director, Corporate Security, General Growth Properties

Physical security includes protection from fire, natural disasters, burglary, theft, vandalism and terrorism. And the risk mitigation programs rely on the basics of guns, guards and gates, with a modern dash of security technology added in for flavor. The continued growth in security budgets demonstrates the recognition of risk and the necessity in mitigating it through investments in access control, surveillance and identity management technologies as well as security officers.

As General Growth Properties recognizes, their task is to create a secure and productive atmosphere, in their case, for consumers to spend money through best practices in visitor management, crowd control, asset protection, organized crime prevention, anti-vandalism programs and theft.

And in case you are not tired of insider copper wire theft stories, here is 2013’s winner. In a three-year criminal plan, 17 people, including 15 Long Island Rail Road employees, stole copper wire spools from a rail yard while on duty, sometimes while collecting overtime. They sold the copper to a local scrap metal company for pennies on the dollar and netted more than $250,000 before being arrested.

5. Technology Integration and Management

Security technology implementation, specifically to support physical security programs, is increasing. In addition to the increased budgets reported by Security 500 members, a recent study released by IMS stated:

If the security boom is over then it seems that end users haven’t got the message, with 45 percent claiming that their security budget had increased during 2012, according to an end-user survey conducted by IMS Research. In the survey of almost 200 representatives from end users of physical security equipment across North America, 44 percent also said that their annual budget exceeded $100,000. Another 20 percent exceeded $500,000 a year.

The revelation that information and cyber security technologies may deliberately have flaws and/or back doors may account, in part, for the uptick in IT security spending. As CRN.com’s Ken Presti reported, “Despite economic uncertainties sometimes impeding the broader market, increases in the number and complexity of threats faced by information technology is expected to drive IT security budgets higher in the coming year, according to a recent study conducted by 451 Research. We found that 45 percent of the respondents are expecting a budget increase for 2013, mostly in the 5- to 10-percent range,” said research director Daniel Kennedy. “Companies realize they need to respond to the problems that are out there. Only 8 percent of the individuals anticipated budget reductions.”

CSOs’ Top Areas of Responsibility

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigations</td>
<td>94%</td>
</tr>
<tr>
<td>Intellectual Property</td>
<td>90%</td>
</tr>
<tr>
<td>Emergency Management/Crisis Management</td>
<td>75%</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>71%</td>
</tr>
<tr>
<td>Corporate Security</td>
<td>64%</td>
</tr>
<tr>
<td>Risk Management</td>
<td>53%</td>
</tr>
<tr>
<td>Physical Security/Facilities</td>
<td>52%</td>
</tr>
<tr>
<td>Asset Protection/Loss Prevention</td>
<td>44%</td>
</tr>
<tr>
<td>Supply Chain/Vendor</td>
<td>40%</td>
</tr>
<tr>
<td>Brand/Product Protection</td>
<td>35%</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>30%</td>
</tr>
<tr>
<td>Cyber Security/IT Security</td>
<td>24%</td>
</tr>
<tr>
<td>Insurance</td>
<td>21%</td>
</tr>
<tr>
<td>Drug and Alcohol Testing</td>
<td>18%</td>
</tr>
<tr>
<td>Other</td>
<td>18%</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>16%</td>
</tr>
<tr>
<td>Workforce/Executive/Personnel Protection</td>
<td>9%</td>
</tr>
</tbody>
</table>
The technology investment is being driven by the core elements noted in this year’s Security 500 Summary: To gather intelligence, manage risk and ensure resilience. That cannot be done without situational awareness, which can only be created by applying technology.

The leading investment among Security 500 members is either an all-in GSOC or the components of the one through partnerships or subcontracting. GSOCs are critical for the collection and analysis of risk and incident information, situational awareness for response and a communications hub to connect with first responders, law enforcement, stakeholders and the broader community. GSOCs deliver significant value protecting physical assets, including infrastructure and facilities for technology that replicates humans and the ability to collect risk and security information at the local level while monitoring and managing it at the GSOC.

Big data analytics fuses both structured content such as report data and statistics, and unstructured content like email and social media, enabling effective risk management and incident response. Powerful command and control programs integrate many types of information, analyze it and quickly notify the appropriate responders.

By leveraging big data, enterprises can optimize their decision-making, interact with law enforcement and better protect people, infrastructure and property, thereby enabling and ensuring business.

Video networks are being employed to reduce man-hours or guard service costs, provide situational awareness and intelligence to first responders and for both compliance and evidentiary purpose to defend against lawsuits.

As security migrates from pure response to risk management and resilience, security enterprise executives will continue to adopt an “all hazards” strategy that demands continued investment in security technology. One survey respondent noted their “Extensive use of and investment in technology in lieu of personnel with highly effective results.”

6. Enterprise Resilience

Resilience management has expanded from the narrower “business continuity and disaster recovery” associated with IT data crashes. Today, the enterprise is viewed as an organism that faces myriad risks, including physical and logical, manmade and natural, external and insider. The scope of planning may be as local as the home office or as far reaching as the global supply chain.

“Our contribution to the city and community is planning, preparing people and organizations and creating a conduit and process for emergency management. The process of planning is more if not equally important to the actual plan.”

Bijan Karimi, Assistant Deputy Director, City of San Francisco, Department of Emergency Management

Fusing these disparate and siloed plans into an actionable enterprise resilience program may be an organization’s greatest challenge. Far from security’s role in event response, the new goals of identifying and mitigating risks opens the door to discussions of preparing for and preventing the highly likely to making crystal ball forecasts of the unforeseen.

Enterprise Resilience’s broad definition includes business continuity, emergency management and disaster recovery for both physical and logical infrastructure and workforce protection. Revenue continuity is at the heart of the organism to remain open or get back up and running ASAP. Budget is the brain balancing necessity against luxury. Justifying enterprise resilience plans and programs is a significant challenge. Estimates and actual costs often vary widely well after an event has occurred.

Enterprise resilience has become an “all hands on deck” exercise where social media has changed communications and altered our perceptions of first responders. The complexity of planning has increased as have the available resilience tools and resources. What is constant is leveraging technologies and best practices to continuously identify threats and vulnerabilities, update and test resilience plans and communicate and drill with stakeholders.

Perhaps the most important learning among leaders is that the planning experience is as important as the actual plan, because the interaction among your stakeholders through training programs and table top exercises creates relationships, identifies risks and reveals vulnerabilities. Creating the structure that facilitates the critical planning process to achieve successful execution is a vital discipline.

While planning exercises prepare enterprises for responding to and recovering from events, how those plans will actually perform are uncertain until battle tested.

7. Human Capital: Hiring/Training/Retention

“Security is becoming both an acceptable and desirable profession. And as security, especially information security in the media, gains coverage, it raises the career interest level. There are numerous opportunities for networking and career development in security today.”

Stephen Scharf, Senior Vice President and Global Chief Information Security Officer, Experian

New leadership across security organizations combined with a triangular focus on risk management and resilience, customer service culture and supporting organizational goals on a global or enterprise-wide scale requires hiring, training and retaining talent that will capably perform critical tasks. On the positive side, security is becoming a profession of choice for current study and those entering the labor force. This is a sea change, compared to the traditional second career for retired law enforcement or military members.

“The key to success in today’s challenging and changing security field is to never stop learning. While a degree can help you get your foot in the door or make the next step up the promotional ladder, continued training and education is critical to staying on top of today’s biggest security threats. No longer can you get by having just a general knowledge of the law. You have to be educated in the areas of terrorism, risk management, drug awareness, preventative safety measures, OSHA, ADA and emergency management, just to name a few. Regardless of our specialized area of security, constant training is vital. Professionals should continue to seek out opportunities to expand and update their knowledge.”

Jason Hudson, Santa Fe Station Casino & Hotel

As the role of security expands to manage additional functions, new geographies and address regulatory issues, the skill sets and
continued training of its personnel expand, as well. Perhaps one of the most difficult training exercises is to incorporate restraint into the program to avoid creating legal liabilities. This is particularly challenging for enterprises who are managing third-party security services relationships.

Beyond consistent management training, there is an ongoing need to hire, train, evaluate and appropriately manage enterprise security officers. As security enterprises work with external service partners to manage cost and deliver specific capabilities, they are challenged to craft a successful training program. And private officer jobs are forecast to continually grow this decade at an average of 15 percent. At issue is ensuring that security officers are both prepared as first responders in any emergency and excellent brand representatives in any encounter.

Shawn Reilly, former Chief of Police and Director of Security for the Greenville Health System, recently wrote in the article, “How to Train Your Security Training Program” (Security, September 2013), “The elements of the security training program remain the same no matter what size the department. The only change is the scope and manpower.”

He adopted and modified the United States Air Force training program strategy for any organization to leverage. He recommended: “Develop, manage and execute training programs, providing realistic and flexible training, producing a highly skilled, motivated force capable of carrying out all tasks and functions in support of (your security department’s) mission. These programs should provide the foundation for all security readiness.”

As accredited universities bring more formal curriculum and degree programs toward the private security management discipline and away from prior law enforcement or military training as the core educational history, the profession will continue to advance.

“There is no longer a time in any field that you can be a good leader and be deficient in any area. Great leaders are comfortable being uncomfortable. They must constantly listen, learn and grow. Leadership is never about any one person, it is about teams and having leaders in various functions, not just one.”

Gordon Snow, Chief of Protective Services, Cleveland Clinic

8. Emerging/Frontier Market Expansion

As organizations expand into new geographic expansions, the effort to support business operations by protecting people, assets and intellectual property requires security to expand, as well. Among the most cited changes impacting security organizations in emerging and frontier markets is political unrest. Political protests, such as the Arab Spring, bring both business disruptions and workforce protection risk issues to the forefront.

Being aware and prepared are the most reliable and best employed mitigation plans to manage risk. Security organizations are relying on GSOCs to gather intelligence and analyze threats so that proactive measures can be implemented.

They are also challenged by protecting intellectual property from fraud, counterfeiting and theft on a global scale as laws and protections are different and in some geographies that are neither illegal nor aggressively prosecuted. Creating public/private partnership and gaining law enforcement cooperation requires finding strong/connected local talent and appropriate due diligence.

Natural disasters or medical emergencies add complexity to global workforce protection as they are rarely foreseen. Those traveling or living abroad can become isolated. Leading organizations are proactively partnering with service companies that specialize in supporting internationally based employees with best practices and training prior to their travel or deployment, as well as providing them with emergency contact information and local resources.

“We have risk assessments and discuss the threats in great detail. The planning includes plugging vulnerabilities so the risks cannot reach the hotel and present reasonable mitigation plans. Terrorism, political unrest and natural disasters are always top of mind for the company. We have emergency plans in place to evacuate people and secure the properties.”

Pat Murphy, Senior Director, Global Safety and Security Services, Marriott International Inc

International regulations and compliance laws are another area of specialized expertise and focus for enterprise security to manage. While many compliance rules require traditional “red tape” processes, participation in compliance programs such as Nexus for personnel travel or CT-PAT for international shipping actually speed and secure business processes.
9. Supporting Organizational Goals

Interestingly, many Security 500 members take this for granted: “Of course, our purpose is to support organizational goals.” And they do so without measured thought. Yet, the thought deserves discussion as a key trend and objective.

“Security contributes by translating a complicated set of practices and merging them into a set of businesses and strategies. How much risk we accept and how much risk we choose to mitigate is translated into business proposals and decisions.”

Timothy Caddigan, Director, Corporate Security & Facilities, Altria Client Services

Security leadership and value is being tied directly to business unit and organizational goals as the best measure of its contribution. So directly tied, business unit leaders are paying for risk management and security as a direct service versus a “forced” overhead allocation. Further, these internal customers view security as a consultancy, and they are routinely seeking their advice to understand and manage risks and enabling them to reach their objectives. The transparency of this relationship allows the business unit to identify security’s value to achieving their goals, resulting in increased reliance, use and spending with security.

As organizations from businesses to hospitals and universities have become single, global entities, the recognition that security should also be a global enterprise with a consistent mission and leadership has evolved at the C-Suite level. A significant trend is the consolidation into a “first” global security organizations led by “first” global CSO offices.

The concept of security as an accelerator for reaching objectives and maximizing financial results is in full force at leading organizations. Top CSO recruits would have it no other way. The chosen enterprise security leader clearly views their role as an executive in the organization who contributes to its success by managing security and risk. They are neither law enforcement, nor security (of the guns, guards and gates era). 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.

One consequence is that budgets or funding cannot be guaranteed if either the perceived risk level declines or the contribution of security is not visible to its internal customer. There is now an increased understanding and appreciation of security’s value at the C-Suite level that is being met by business units having the option to utilize security as a service.

“Fidelity Investments includes many venture businesses outside the core responsibility of financial services, and includes hotel/lodging, exhibitions, commercial real estate, lumber and contractor supply (largest contractor supply company in the U.S.), oil and gas extraction, agriculture, biosciences. Being privately held, Corporate Security is responsible for supporting the needs/requests of each business line as well as the core financial services operation.”

John O’Connor, Fidelity Investments

An organization with a world-class security program has positive messaging from the C-Suite followed by positive feedback from business units. This creates continued positive messaging from the C-Suite. This momentum changing influence will greatly impact the security organization, positively or negatively, depending on security’s measurable and perceived value.

Business leaders delivering the most value to their organizations through security are doing so by focusing on areas that most directly and transparently support business goals. And in turn, the security organization is focusing its strategy, time and attention on those programs where funding will be available.

“Being told that we are seen as strongly integrated into the business’ mission is a great compliment. Security is a true profession and the landscape is changing. Security must be integrated into the core mission of the enterprise and receive a seat at the table.”

Mike Howard, CSO, Microsoft

10. Brand and Intellectual Property

The damage insider (Edward Snowden) or external (Efficient Services Escrow Group) actors can cause to an organization or community can be devastating. You are probably well aware of the impact Snowden’s actions have had on the NSA. You may be unaware that a cyber attack that stole millions from its accounts actually put the Efficient Services Escrow Group out of business. Brand or trademark dilution, counterfeiting and product diversion by dishonest employees or organized crime can disrupt a business and damage its image. Efforts to steal valuable intellectual property or counterfeit branded products are pervasive and often perpetrated by trusted business partners or employees.

A 2013 Symantec study identified that half of employees who left or lost their jobs in the last 12 months kept confidential corporate data, and 40 percent plan to use it in their new jobs. The results show that everyday employees’ attitudes and beliefs about intellectual property (IP) theft are at odds with the vast majority of company policies.

Employees not only think it is acceptable to take and use IP when they leave a company, but also believe their companies do not care. Only 47 percent say their organization takes action when employees take sensitive information contrary to company policy, and 68 percent say their organization does not take steps to ensure employees do not use confidential competitive information from third-parties. Organizations are failing to create an environment and culture that promotes employees’ responsibility and accountability in protecting IP.

On the counterfeiting side, Pfizer’s Viagra still seems to be the gold standard among counterfeiters. A study funded by Pfizer and authored by Dr. Irwin Goldstein identified that 77 percent of the Viagra they purchased from 22 online pharmacy sites was fake. That study snowballed the notion that online pharmacies are probably selling fake everything, not just Viagra, making them both dangerous and untrustworthy. Fake Viagra is found to be made with such ingredients as blue printer ink and sheetrock.

A study co-chaired by Jon Huntsman, former U.S. Ambassador to China, concluded that “the scale of international theft of American intellectual property, today, is unprecedented.” The study places the cost of more than $300 billion annually, more than all of the annual U.S. exports to Asia and equivalent to creating 2.1 million jobs.

Security traditionally got the tail end of an insider theft or counterfeiting operation, leaving them to the post-event investigation and report on what preventative steps might be implemented. The proactive risk and resilience focused security organization is working to identify these risks and eliminate the threat before an event damages the brand.