The Forces of Change

By Bob Hayes, Kathleen Kotwica and Marleah Blades, Contributing Writers

Security is changing. The various shifts underway right now involve more than just convergence, biometrics and Sarbanes-Oxley. Security is changing in ways that will transform what "security" encompasses, how it's accomplished, and its role and significance in the organization. In order to meet the rapidly evolving requirements of successfully protecting the business, security professionals must recognize and understand the forces that are driving these changes.

The Security Executive Council (SEC), an international professional membership organization for leading senior security executives, has been following a number of trends that are affecting its membership and the security industry at large. These trends have been recognized by members themselves as well as SEC faculty and staff. The council has asked subject matter experts to substantiate and comment on the most significant trends it has observed, and, in partnership with Security Magazine, it has created a list of the forces having the most significant impact on the direction of security today.

The forces discussed in this article are highlights of the complete list of Forces of Change the SEC has identified. The council plans to develop a tool to assist in tracking the strength and significance of these trends. Using this list as a resource, security professionals can prepare themselves and their programs to meet the present and coming challenges.

1) Globalization and Economic Risks
2) Continuing Reactions to Enron, 9/11 and Katrina
3) Expansion of Security into New Areas
4) Security-Related Legislation, Regulations, Voluntary Compliance Guidelines, and Standards
5) Businesses' Rapid Adoption of New Technology
6) Transnational Crime
7) The Changing Workforce
8) Public/Private Partnerships

1. GLOBALIZATION AND ECONOMIC RISKS

The United States has ranked in the top 10 most globalized countries in the A.T. Kearney/Foreign Policy Globalization Index for the past four years. (The index ranks countries based on indicators such as trade, foreign direct investment, participation in international organizations, travel, and Internet usage, according to Foreign Policy Magazine.) U.S. businesses continue to cross borders to build international sales and services and to cut costs; the federal government continues to create and alter economic and political relationships with other countries; and technology gives us nearly unfettered access to the societies and products of our international neighbors. All these factors combine to introduce new — or if not new, elevated — threats of which security must be aware.

Globalization and economic strain can lead to angry incidents.

• *Espionage and Theft of Intellectual Property*

"The economic viability of our country is absolutely tied to the national security of our country," said Lynn Mattice, Chairman Emeritus of the National Intellectual Property Law Institute and Chairman of the Board of Advisors for the Security Executive Council. Globalization has both enabled and compelled companies to import the best international talent and resources available. While leveraging competencies around the world is undoubtedly the trend for success going forward, unintended consequences are beginning to appear. The increased foreign exposure and access to valuable trade secrets, technologies and new innovations—specifically, to the core strategic intellectual property of the company—have raised the level of economic risk. Other countries recognize the leading position of U.S. corporations in technology markets and will steal to compete. The business landscape is now the world instead of a single country. The intelligence services of foreign governments sponsor and direct the priorities of commercial entities. This undoubtedly unfairly tips the scale and disadvantages corporate America. Also, unaudited and blurred global supply chains, which are more pervasive today, may illegally and unintentionally bolster, for example, foreign military programs. The confluence of these trends portends increased potential risk to competitive advantage, profitability, and, in some circumstances, our national security. "Companies must consider holistic enterprise-wide approaches to detect anomalous behaviors and potentially damaging activities undertaken by the new breeds of very talented but 'globalized' employees. Simply building higher security walls around the 'crown jewels' isn't an effective enough protection strategy anymore," said Kevin Favreau, Deputy Assistant Director, Counterintelligence Division, FBI.

• *Economic Turmoil*

In a global economy, economic and political turmoil in one region often has significant lasting effects on other regions across

the globe. Economic erosion can lead to political and social unrest, which can result in backlash against wealthier nations and international financial organizations. While the economy and political arena have quickly become more globalized even in small countries, culture and religion have remained the same in many regions. "It is these strains between globalization of the world's economic and financial systems and the other building blocks of a society that have created the tensions

Financial and terrorist forces brought in an increased sense of urgency.

that the security industry must face," said Delos Smith, president and chief economist of Delos Smith & Associates and former senior business analyst for the Conference Board. "These changes have created a lot of tension and anger, and that anger can be manifested in very destructive incidents. But for the security world to be successful, they need to know about culture and religion, which play extremely powerful roles in a society."

• ***Offshore Outsourcing***

The globalization of business has resulted in a new organizational structure for many U.S. companies. In years past, most or all company functions were performed in-house, with the corporate executives at the top tier overseeing all activities directly. Now, many companies outsource or contract many if not most corporate functions to other organizations, often abroad. This offshore outsourcing presents a number of security issues. Vetting of contractors and their employees is difficult in some countries, where laws and traditions sometimes limit the availability of background information. Espionage and fraud may be easier to perpetrate in such environments. Logistical problems and cultural concerns may impact the level of physical security available in outsourced locations. And risk management is complicated when company executives have no direct oversight over outsourced functions. Consider the toy companies that lost Christmas sales last year because their Chinese partners used lead paint in their products. A company's offshore partner may be directly responsible for an error, but, said Dick Lefler, Security Executive Council Emeritus Faculty and former vice president for worldwide security at American Express, "it's not the partner's brand and reputation that's on the line—you're the one that pays for it."

• ***Global Universities***

Increasing numbers of U.S. universities are opening campuses abroad to further diversify their student bodies and to offer students broader international experience while attracting highly qualified non-American applicants. If international locations are not developed with security in mind, they could become easy targets for international theft of U.S. research and development discoveries.

2. CONTINUING REACTIONS TO ENRON, 9/11 AND KATRINA

Three major events of the last decade have reshaped security: 9/11, the Enron scandal, and the devastation of Hurricane Katrina. Collectively, these events have repositioned risk as a Board-level concern, because, according to Dick Lefler, they have proved that "the implication of a risk goes far beyond the individual business unit. A risk could cost you lots of money in legal, brand, and reputational issues, which one single business unit couldn't comprehend. So boards are looking to understand risk in a holistic way."

• ***Enron***

The Sarbanes-Oxley Act, developed in response to the financial debacle at Enron Corporation and other high-profile accounting failures, drastically increased the level of required reporting and auditing to which the financial procedures and processes of public companies must be submitted. It also placed the responsibility for inaccuracies directly on the shoulders of C-level executives, stipulating criminal penalties with fines of up to $5 million and up to 20 years in prison for intentional violations. Of course, this makes compliance a top priority for publicly traded companies. SOx also requires executives to vouch for the security of internal controls, including IT systems.

• ***9/11***

The terrorist attacks of September 11, 2001 transfigured security in more ways than this small space will allow us to discuss. One of the most significant impacts was the increased urgency with which corporate executives began to view security and emergency response planning. In many organizations this resulted in increased funding and support for security initiatives, though sometimes only temporarily. September 11 also set into motion an unprecedented push for security-related laws, regulations and guidelines, both broad-based and industry-specific.

• ***Hurricane Katrina***

Nearly four years after 9/11, Hurricane Katrina once again put businesses to the test. R. David Paulison, the administrator of the Federal Emergency Management Agency, has said that Hurricane Katrina changed the face of emergency management. According to FDIC estimates, the storm's economic impact outweighed that of Hurricane Andrew and 9/11, and the toll it took on some businesses refocused nationwide attention on business continuity, emergency response and disaster recovery planning. Corporate executives recognized that the risk exposures in such a significant event extended well beyond loss of power, impacting brand reputation, employee safety, insurance costs and physical property.

• ***Continuing Motivation***

Natural and man-made crises continue to make regular headlines, both in the U.S. and abroad -- Societe Generale Bank's loss of 4.8 billion euros through rogue trading, the shooting at Northern Illinois University, the U.S. subprime disaster. All of these examples further push risk into the C suite. "You'll begin to see the elevation of the risk management position," said Lefler, "and you'll see the security manager position become a subset of the risk management approach. Operational risk management teams are being built with a risk management officer as the lead position, with the CSO acting as one part of the team."

3. EXPANSION OF SECURITY INTO NEW AREAS

In the past half decade, the changing threat and technology landscapes have pressed security into areas and industries it has never before been involved in.

• ***Broadening Applications***

Not long ago, few people had heard of "agroterrorism." Now it has its own international symposium, which is in its third year. While the food industry has always been security conscious, farmers and ranchers are entering into new territory in learning to participate in the protection of the food supply. Cities and towns are mounting cameras on their streets and in their trains and busses, water treatment facilities are under increased pressure to be secure — even libraries must take new measures to monitor and protect sensitive information.

• ***Depth of Influence***

Some of security's new territory extends to the desk of the CEO. Brand and reputational issues have earned a place in the security or risk management portfolio, and corporate executives in many organizations are showing increased willingness to support security in the protection of the company image.

• ***Changing Channels***

As security branches out into markets in which it previously had limited impact, the buying channels for security technology are shifting. Major security companies no longer hold a monopoly on security-related equipment. New industries are able to turn to familiar names within their own markets to meet some of their technology needs. In addition, groups besides security are using technology traditionally identified as security-related for non-security purposes — cameras for quality control, or to study buying habits in retail stores, for instance. These uses provide opportunities for efficiency but also open the company up to duplication of efforts and even abuse.

4. SECURITY-RELATED LEGISLATION, REGULATIONS, VOLUNTARY COMPLIANCE GUIDELINES, AND STANDARDS

In the past several years, world events and national scandals have led to the development of a flood of laws and standards that include security requirements. "Regulatory requirements have begun to force the security professional to become a risk assessor, a risk manager and mitigator," said Lou Magnotti, chief information security officer for the U.S. House of Representatives. However, compliance with all the relevant laws, regulations, guidelines and standards is an immense challenge for companies and for security executives.

• ***Laws and Regulations***

Most security professionals are unaware of the number of federal and state mandates that include security requirements that may impact their organizations. The Security Executive Council has been compiling a database — the first of its kind — and it currently includes 35 U.S. federal legislative actions (including executive orders and statutes) and 46 U.S. federal regulations. This current list is still far from complete. Even if corporate executives are equally unaware of all the applicable laws, they will turn to security when they're slapped with fines and penalties for noncompliance. Some security professionals are turning to best practices to gain compliance with a variety of rules at once. But the preponderance of laws and regulations is also increasing the importance of cross-departmental oversight, since many rules apply to several different functions.

• ***Standards and Guidelines***

In part to avoid further federal and state oversight, trade groups and associations in all industries have stepped up the development of voluntary guidelines and standards. Government entities may also issue guidelines where regulation would be unfeasible for an entire industry or where strict regulation could impose an unbalanced business or economic risk. Several years ago, security standards were exceedingly difficult to come by, and this lack was a source of constant chagrin in the industry. Now, eight security organizations alone are developing standards — and that doesn't include industry-specific trade associations outside security. The Security Executive Council's list of guidelines now stands at 44.

5. BUSINESSES' RAPID ADOPTION OF NEW TECHNOLOGY

Businesses and their employees today want data not just quickly, but immediately, from anywhere. Data storage and computing power continue to come in ever-smaller packages; data transfer through the Internet is increasingly faster, mobile and user-driven; and businesses are picking up on all these advances to enhance the productivity of their workforce. Faced with this barrage of new technology, security finds itself racing to secure new devices and implement new protection measures.

• ***Enterprise 2.0***

Enterprises are adopting Web 2.0 applications — that is, services like del.icio.us, MySpace, YouTube, and Wikipedia, which use the Web as their platform and incorporate content provided by users and other Web sites in increasing numbers to improve communication and workflow within their businesses and to improve relationships with clients. A December 2006 Forrester survey of 119 CIOs at mid-size and larger companies showed that 89 percent of the respondents had adopted at least one of six Web 2.0 tools (blogs, wikis, podcasts, RSS, social networking, and content tagging) and 35 percent were using all six. Because Web 2.0 applications are interactive, more data is exchanged than in traditional Web transactions, and the client computer plays a bigger role, opening up more vulnerabilities. Insiders using these services may also create risks.

• ***Mobile Devices***

Businesses rely on PDAs and smartphones to keep their traveling sales staffs and executives available at all times. Research in Motion, the maker of the

Web 2.0 and mobile devices have wide security impact.

BlackBerry, reported recently that it will reach 14 million BlackBerry subscribers by March 1, and there are new models of other brands of smartphones and mobile devices being released every month. AT&T even announced plans in January to begin marketing the Apple iPhone to businesses. These devices, as well as USB jump drives and consumer technologies like MP3 players, camera phones, and digital cameras all have the capacity to transmit and store potentially sensitive corporate data, leaving security profes-

sionals with an ever-evolving challenge. "We can't concentrate only on securing the endpoint; we have to manage the data," said David Meunier, vice president of information risk management & CISO for Masterlink Corp. "We need to focus on controlling the data coming into and leaving our environment."

• ***IP's Impact on Traditional Security***

Convergence, convergence, convergence. The digitization of security technology and its ability to transmit security data and commands across networks have revolutionized security. IP cameras can be controlled over the network, and their images can be accessed remotely through a PC. Physical and logical access control can be integrated for new ID/database efficiencies. IP security technology can provide long-term cost savings and recast the security labor landscape. Convergence of technology has also increased the need for either converged security management or heightened cooperation between the IT security and corporate security departments.

6. TRANSNATIONAL CRIME

Crimes in which the criminal is in one country and the victim in another continue to play a major role in both corporate security and national security. Detecting, combating and prosecuting such crimes present a maze of challenges for public and private security organizations.

• ***E-Crime***

Domestic e-crime, such as identity or credit card fraud, is hard enough to discover and prosecute. But transnational individuals and groups are now leveraging the boom of information technology to launch attacks at U.S. citizens and businesses from abroad. Criminals in countries like China, India and Russia are being hired to hack into the networks of U.S. organizations to glean valuable information for foreign entities. Unfortunately, says Ed McGarrell, director and professor in the School of Criminal Justice at Michigan State University, with transnational e-crime, legal action is extremely difficult. "If a citizen in Omaha is victimized by an organized crime group operating from the Ukraine with the information sold to a South American crime group, who has jurisdiction?"

Technology, among other forces, helps criminals leap borders to reach victims.

• ***Counterfeiting***

"In this global age the key threats to businesses are not likely to be the lone offender breaking into the warehouse but the criminal organization producing a faulty replica product and selling it under the company's brand," said McGarrell. International counterfeiting operations have become focal issues for the U.S. government and entities like Interpol. The International Herald Tribune reported last year that the Department of Homeland Security made 14,000 seizures of counterfeit goods worth a total of $155 million between October 2005 and September 2006, and U.S. authorities believe portions of the $500 billion global trade in counterfeit goods go to fund terrorism.

• ***Money Laundering***

International money laundering as a source of funding for terrorist activities is such a major concern for the U.S. government that it is the focus of the USA Patriot Act, which is intended to strengthen U.S. measures to prevent, detect, and prosecute such activities. The requirements found within the act apply not only to banks, but to securities broker dealers, money services businesses, operators of credit card systems, the insurance industry, and casinos, among others. Security professionals have traditionally seen no need to develop relationships with the treasurer, comptroller or CFO, but this element of transnational crime has some opening up dialogs with their financial department peers.

7) THE CHANGING WORKFORCE

As technology continues to advance and Generation Y and the Millennials flow into the business world, employers are seeing significant changes in their workforces and are working to accommodate these and deal with the threats they introduce.

• ***Degradation of the Honesty Pool***

Statistics from the Society for Human Resource Management and numerous private screening firms show that nearly half of job applicants make misrepresentations of some sort on their resumes or job applications, and clearly the problem doesn't end with entry-level positions. Bausch and Lomb CEO Ronald Zarella; Sandra Baldwin, the first female president of the U.S. Olympic Committee; David Edmundson, former CEO of Radio Shack; Kenneth Lonchar, former CFO of Veritas Software — all outed for falsifying information about their backgrounds. There even exists a Web site called www.fakeresume.com, which offers tips on falsifying information safely and claims that 70 percent of college graduates lie on their resumes. Background screening is not just a Human Resources issue; it's a security concern.

A changing workforce is pressuring security in new and complex ways.

• ***Insider Threat***

In the past decade, physical security has become effective enough to mitigate a very large amount of outside risk. One unintended result of this success is the pushing of threats inside the organization. The advancement of information technology has added new dimensions to the insider threat as well. The 2006 E-Crime Watch Survey by the U.S. Secret Service, SEI CERT Program, and CSO Magazine found that one third of e-crimes in which the perpetrator could be identified were committed by insiders. In both the physical and cyber sense, insiders know where to find the valuable assets and often have access to them or know how to gain access. Also, said David Meunier, "the more advanced we get in technology, the more we provide people the opportunity to cross line that they normally wouldn't." Crimes that used to require risk of public exposure, like fraud, stealing trade secrets, sabotage or pedophilia, can now be committed quickly, anonymously, and even conveniently.

• ***Work at Home Trend***

Telecommuting has become popular

for many companies, large and small, because networking technology and cell phones allow employees to work from home with most, if not all, of the resources of the office, often at a cost savings. Sun Microsystems has maintained a flexible workplace —that is, with some employees working in offices, some at home, and some doing both as needed — for around 10 years, and the program has saved the company hundreds of millions of dollars in real estate costs alone, according to Leslie Lambert, vice president of information technology at Sun Microsystems, Inc. In addition, she said, "we've been able to measure a greater than 33 percent productivity increase, and the flexible work environment is our number-one employee retention item." While Sun has a strong, proprietary access and authentication system protecting their network in this environment, many organizations that allow telecommuting don't have adequate measures in place. In fact, some have nothing stronger than password protection for remote access, leaving their networks easy prey to hackers. "A lot of companies are also going to third-party telecommuting centers. You have to secure these as well, because the third party may just set up a small network that's not really secure, so you may log in and leave half your data on that computer, or you may not close out your session so someone else can log on and still be connected or see what you've downloaded," said Lou Magnotti.

8) PUBLIC/PRIVATE PARTNERSHIPS

The new complexities of business and security have made it more difficult for corporations to track and respond to the myriad threats against them, and it's similarly more difficult for public agencies to monitor crime and national security threats when much of the danger lies in the business realm. Partnerships with public entities are becoming even more valuable in the globalized, high-tech business environment, where both public and private organizations have limited resources. The following two organizations have become or are becoming valuable resources for private and public security.

- ***The FBI Domain Program***

The goal of the FBI's Domain Program is to work with other public entities and private business to identify critical assets and the threats they face, collaboratively reconcile their vulnerabilities, and determine how best to protect them. "The program is really about enhancing public-private-sector communication opportunities and developing actionable information that prospers and protects the country. For starters, we intend to develop a more comprehensive awareness and understanding of the threat landscape across the country, including merging an assessment of national security and criminal bad actors with an inventory of critical entities such as people, places and things, potentially at risk. The program seeks to position and effectively engage the limited resources of the FBI in hot spots and against issues where vulnerabilities and threats intersect across the country, and then, ideally, provide relevant feedback to affected stakeholders that impacts sound risk management decision making," explained Tom Mahlik, Chief of the Counterintelligence Strategy and Domain Section at FBI. "After 9/11, the Bureau realized that we needed to further localize our efforts, while at the same time continuing to build a more detailed understanding of the national threat picture. We have since focused 56 FBI field divisions on identifying critical equities and threats in their domain—their backyard—and we asked them to partner up with other government agencies, corporate America and universities as part of the process. New confidences, trust and balanced expectations are being achieved on a daily basis. The preliminary responses and results have been higher levels of awareness and diligence in the private sector. Clearly, our goal in the longer run is to be more interactive, proactive and preventive in our efforts to protect the country," added Mahlik. The Counterintelligence-centric initiatives in the Bureau's Domain program fall into three areas:

- *Business Alliance.* Meeting with businesses to educate them on the threats and help them identify, audit and protect their IP, trade secrets and proprietary data.
- *Academic Alliance.* Made up of the National Security Higher Education Advisory Board (NSHEAB) and the College and University Security Effort (CAUSE) establishes a dialogue with academic institutions to increase awareness of threat and national security issues.
- *Counterintelligence Working Groups.* The National Counterintelligence Working Group and Regional Counterintelligence Working Group establish strategic interagency partnerships.

- ***The Overseas Security Advisory Council (OSAC)***

The Overseas Security Advisory Council (OSAC) is a Federal Advisory Committee created in the late 1980s to promote security cooperation between American business interests worldwide and the U.S. Department of State. OSAC currently works with more than 3,500 U.S. companies, educational institutions, religious and non-governmental organizations. Like the Domain Program, OSAC emphasizes information exchange and offers educational tools to private sector entities worldwide.

The world is changing, and security must change along with it. All security professionals should be watching these forces of change to see how they're impacting their organizations and to determine what to do about those impacts. They should also be looking out for other trends and factors of growing importance. The Security Executive Council is developing tools to help security professionals track these and other forces and see how their significance changes over time. No other organization has created a list of change indicators specific to the security industry. This is a continuing process, and the council continues to seek input on new and growing trends. If you're seeing strong trends or change indicators in your business, let us know by e-mailing mblades@secleader.com. Keep an eye on www.securityexecutivecouncil.com for updates and to monitor the forces of change for your organization. SECURITY

About the Authors

Bob Hayes is managing director of the Security Executive Council, a cross-industry professional organization of security executives devoted to advancing strategic security practices. He is responsible for program vision, identification of member needs, and the creation and execution of programs and tools to help security executives effectively lead and manage the security function at their organizations. Kathleen Kotwica is vice president research and product development for the Security Executive Council. Her responsibilities include determining member solutions and tools, product development and launch and analysis/research. Marleah Blades is Senior Editor for the Security Executive Council, where her responsibilities include writing and polishing the council's industry articles and columns as well as many member resources.