SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

How Business and Risk Drivers Impact Mitigation Strategy

Marleah Blades, Bob Hayes and
Kathleen Kotwica Ph.D.

Originally Published in Security Magazine

December 2012

How Business and Risk Drivers Impact Mitigation Strategy

As business changes, so does – or so should – security. The direction of business can have significant consequences for security, both internally – in terms of influence, funding and organizational structure – and externally – in new threats, new risk, new mitigation requirements.

Are you watching business trends and thinking about how they should impact security and your strategies to mitigate risk?

A study of business outlook reports and interviews with experts from the Security Executive Council and the University of South Carolina's Darla Moore School of Business have led us to several broad business trends that will have consequences for businesses risk and security functions in the near term. First we'll lay out the research on the trends themselves, and then we'll share some thoughts on their impacts on the security function.

The world economy will grow slowly, with emerging economies outpacing developed ones

Businesses across the globe – from the multinational to the mom and pop – should recognize after these past three years how much the world economy can impact their profitability. The U.S. banking crisis and the global recession have made risk a common language on the tongues of C-level executives and the general public. And as the U.S. struggles toward recovery and the European Union works to resolve its continuing debt crisis, economists offer little comfort for the near term.

While forecast percentages vary, economic outlooks from the World Bank, the Conference Board, Moody's and Deloitte, among others, predict continued slow growth in the global economy. According to the *Conference Board's Global Economic Outlook 2012*, "At 3 percent, on average (between 2012 and 2025), global growth will still be somewhat higher than the period 1980-1995 but between half and a full percentage point below the growth rate from 1995-2008."

Emerging market economies such as China, India and Brazil, however, will outpace developed ones. A Euromonitor International special report released in May found that "Between 2000 and 2012 real GDP from emerging market economies will have grown by a forecast average of 105 percent, while the real output of developed economies will have grown by just 20.2 percent." Moody's downgraded its growth forecast for emerging markets in August, but the new prediction of 5.2-percent growth through 2012 still outstrips the 2.8-percent growth forecast for the G20.

In Deloitte's Global Economic Outlook report from Q1 2011, Senior Economist Dr. Elisabeth Denison wrote, "With the maturing of emerging nations, financial power and consumption is increasingly shifting from West to East – or more accurately from aging industrial nations to emerging industrial powers in Asia, South America and Africa. These economies are morphing from being the world's workbench to being its sales booth."

The business landscape will be increasingly global

The rebalancing of world economies is one of many factors that will continue to draw businesses of all types and sizes into a more global landscape – through overseas expansion, offshore outsourcing, engaging global competitors and cross-border M&A.

The upward trends in offshoring and offshore outsourcing were established more than a decade ago, but the U.S. recession beginning in 2009 threw them into high gear. A 2012 study by the Offshoring Research Network (ORN) of Duke's Fuqua School of Business found that globally, 80 percent of large companies, 58 percent of midsize companies and 23 percent of small companies are doing some offshoring, and one-quarter of midsize companies and 35 percent of small companies are considering it for the future.

This is no surprise to Richard Lefler, former VP & CSO of American Express. "In a global competitive environment," he says, "if you don't produce your goods and services at a lower cost, if you don't constantly innovate to offer new products and if you don't effectively make your organization smaller in terms of general administration costs, then you're at a competitive disadvantage." In fact, in the ORN study, 72 percent of survey respondents

listed labor cost savings as one of the three most important drivers leading to overseas outsourcing.

The Hackett Group, Inc., a global strategic business advisory firm, has reported that the labor cost gap is closing between the United States and some other emerging economies, but new research from that firm forecasts that corporations in the U.S. and Europe will move an additional 750,000 jobs in IT, finance and other business services to India and other low-cost geographies by 2016.

Meanwhile, companies from the emerging economies that have grown during the U.S. and Eurozone recessions have continued to engage in cross-border investment and M&A. According to the U.S. Bureau of Economic Analysis, while foreign direct investment in the United States is down from its 2008 high (due to concerns about the volatility of U.S. economy), in 2011 it remained more than $143 billion higher than in 2002.

Even small organizations that don't outsource overseas or take direct foreign investment would do well to look at themselves in a global context, says Francis D'Addario, former security and risk executive for Starbucks Coffee, Hardees Food Systems and The Southland Corporation. "Even if you don't think you're global, your supply chain is," he says, and if that global supply chain is interrupted, the impact is no less real.

Add a maturing Internet infrastructure into the mix of world economies and globalization, and it can even be argued that the "small business," as it's traditionally understood, no longer exists. Dirk Brown, Director of the Faber Entrepreneurship Center at the University of South Carolina's Darla Moore School of Business, says, "If you're a flower shop in Columbia, South Carolina, you're no longer just competing with the flower shop down the road. You're competing with 1-800-Flowers – or you're partnering with them. So the way you do business, even small business, has to be considered on a national and international scale. Your business model has to shift to comprehend the global landscape."

As the Internet continues to grow and transform, the demand for and the value of information will continue their sharp rise

A joint study was published by the Pew Research Center and Elon University on March 23. It reported that by 2016, there will be 10 billion mobile Internet devices in use globally and smartphone traffic will have grown to 50 times its current size. The study also stated that Android users have been downloading apps at a rate of 1 billion a month.

A few months after the Pew study's release, Ofcam, the independent competition authority for the UK communications industries, said in its ninth annual communications market report that more than four in 10 smartphone users say their phone is more important for accessing the Internet than any other device.

Users of mobile technology expect information to be available anytime, anywhere and this expectation is driving the use of personal cloud services, according to Forrester Consulting. The firm has reported that approximately 58 percent of personal cloud users with smartphones access their cloud environments daily or hourly.

Customers and employees are demanding of businesses the same level of accessibility they enjoy in their personal lives, and companies are taking note, according to a Gartner report released in February. Personal mobile devices are now commonly used in enterprises, the report says, and "Management tools will need to encompass the cloud storage and sync services that users need."

CompTIA conducted a survey earlier this year that found that more than eight in 10 companies are using some form of cloud technology, and almost 25 percent of respondents said that cloud components made up between 30 percent and 50 percent of their overall IT architecture. John Naughton wrote in *The Guardian*on July 21, "providers of cloud computing will inherit the Earth, because all mobile devices are essentially windows on to the cloud. So, clearly, the future's mobile."

In their rush to stay abreast of consumers' push for on-demand information, companies continue to engage in social networking for internal and external influence. The 2011 Harvard Business Review Analytics Services report *The New Conversation: Taking Social Media from Talk to Action* found that 58 percent of companies had become "engaged in social networks like Facebook, microblogs like Twitter, and sharing multimedia on platforms such as YouTube." The report further stated that many of these organizations hadn't yet figured out how to use these media to their full advantage.

One might think that as information becomes more ubiquitous, it also becomes cheaper. But information worth protecting – trade secrets and other intellectual property – has in fact become many businesses' most valuable asset, according to USC's Brown. "In 1975, less than 20 percent of the value of the S&P 500 was in intangible assets. By 1990 it was half. Now, 80 percent of the S&P 500's value is in intangible assets."

"You're also seeing both developed and emerging global economies trying aggressively to secure intellectual property rights," he continues, noting that patent filings in China are rising more quickly than filings in the United States. "The world as a whole is racing to protect intangible assets because they realize how much value they hold."

These three broad trends are changing business, and as business changes, so does business risk. The risk-related consequences of these drivers are wide-ranging and deeply interconnected, and while they'll impact each company and security function differently, none will be left unaffected.

Faster, Cheaper, Smaller

One of the most significant effects of both the economic slowdown and the globalization of business has been and will continue to be the adoption of leaner methods of business operation, which spawn further impacts of their own.

The outsourcing trend is one of these results, and it's one that risk managers will have to consider very carefully. As we've seen, companies

tend to move processes to third parties (domestic and overseas) to save money, and as the economy continues on a slow growth path and global competition heats up, companies will continue to use this option for organizational savings. Unless they do so carefully, however, they will open up new vulnerabilities.

"Outsourcing creates an extended definition of 'insider,'" says George Campbell, former CSO of Fidelity Investments and author of *Measures & Metrics in Corporate Security*. "Outsourced employees can't do their job unless they have access to customer information and proprietary information. Where is security when it comes to selection of these providers and oversight of the risk associated with them?" Risk-cognizant organizations include background investigation and performance requirements in their contracts, but even then, someone must be responsible for ensuring these requirements are being met. "Security has an obligation in this extended business model to be part of the risk assessment process and part of the plans process," Campbell concludes. If companies do not heed the importance of risk oversight of third parties, their cost savings may come at the price of major breaches and reputational disaster.

As lean processes create new business risk, they also create risk for the security function specifically. "Faster, cheaper and smaller is the way the business is going, so there's a tremendous amount of pressure on security executives to figure out how to help their organizations grow business faster, how to reduce operating costs and how to have smaller organizations and be more effective," says Lefler. In some cases risk and security leaders are being asked to find the best ways to move their functions in this direction, but in others, the decisions are being made for them. Solutions to these requirements will differ. One small-scale option will be to replace guard cost, which tends to appreciate over time, with technology, which is capital investment that is depreciated over time. But most functions will be asked to do more than that.

According to Campbell, "We are seeing more security executives who are aligning themselves with business processes around total quality

management, operational excellence and Six Sigma, driving defects out of business processes and increasing quality. They're adopting these practices that have been in place in manufacturing for many years and forcing their functions into thinking much more critically about how they manage their processes and how they directly contribute to business performance and customer service."

Alignment for some security leaders means running a lean staff and using contract staff to fill gaps, says Mark Lex, who spent 15 years as the top security executive for several Fortune 500 organizations. "Some really smart people use a flex team model because it provides just in time service, and, if you've had budget erosion, it's a lot easier to have an invoice come to a field site for services provided than to have internal charge-backs when you have internal staffing."

The lean model means every business decision will need to be business-aligned and justified through verifiable metrics. The pressure placed on executives to show profit in a slow but globally competitive economy will trickle down to security just as it will to other functions. Measurable, aligned lean operation, according to D'Addario, will be "the price of admission."

"We're already seeing organizations after the 2008 downturn become more nimble," he says. "Leaders operating in the new parameters are finding that they have to do this. Security is increasingly becoming a notional shared service at the enterprise level. Silos are crumbling because they're too expensive for upkeep and there's no accountability.

"The net capability argument for stakeholders has to be there. I think we're going to see analysis ad nauseum until stakeholders are persuaded that organizations are as thin as they can be, capable, meeting the risks they say they might meet in their 10-K and doing it persuasively. Everybody knows they're having X incidents per Y employees, but they haven't shown how what they've done impacts the total cost and P&L for the organization."

As security functions continue to go lean, some will also have to adjust to less external support from municipal and state police forces, which are cutting back drastically due to the economic conditions.

Scrutinized or Overlooked?

In the last decade, the language of risk became common in the C-suite and the supermarket aisle. Businesses and the public talk, and worry, about security, and the recession of 2008 added new definitions of risk to the average vocabulary.

The public's economy-driven interest in risk has played a role in legislators' increased activity on corporate risk issues, such as the new SEC compliance requirements. In business, the uptick in risk interest has led and will continue to lead senior management to scrutinize the corporate security function and expect far more in terms of results and efficiency than it has in the past – another push for alignment, metrics and lean operations.

However, increased scrutiny only comes in organizations where the security function and the security leader are considered players in business risk management. In many organizations that's not the case – instead, risk experts who have come up through security have allowed themselves to be sidelined by lack of business skills, protection of silos and unwillingness to collaborate. This means that risk decisions are often being made either 1) by the wrong people or 2) by the right people without the benefit of informed advice.

"Think about who's involved in corporate governance and enterprise risk management. You'll find information security there, but too often we don't see corporate security mentioned – not as a full participant in that process," Campbell says. "Security managers need to ask themselves why that's the case. What can they do to better align themselves with the business model and with the corporate governance model? Because without that, the full scope of security risk is not going to be effectively understood in that organization."

When corporate security experts are left out of risk and governance decisions, businesses will continue to protect against yesterday's threats

rather than skillfully looking ahead to determine and manage the risks of tomorrow. They may also fail to make fully informed decisions about how to manage risks they do recognize.

Global Relevance and Risk

A broader view of current and future risk will be crucial for organizations that operate in a global environment.

As organizations move portions of their operations abroad, they must ensure not only that these decisions benefit the bottom line but that they do not result in unacceptable risk. Companies must also be sure to provide culturally relevant leadership and risk management for those operations, says D'Addario.

"When we came up with exception-based reporting for Starbucks – so we could identify someone who was not ringing sales properly or committing fraud – we had 99 percent accuracy for exception detection with 92 percent of cases contributing results," he says. "We could measure sales increases in millions of dollars when action was taken. Our philosophy was to trust partners, and this tool helped us hold people accountable within that guideline. The approach was tested and proven around the globe.

"When we introduced this process to our Asia Pacific markets, some leaders thought the solution may not be culturally relevant. It wouldn't be effective or culturally appropriate to highlight the failings of a single person on the team. So in these locations, instead of advising an individual that he or she has voids out of bounds by 8 percent over everyone else in the store, we advise the whole team they have voids that are out of bounds by 8 percent. The team can resolve an anomaly or problem relevantly when informed by the data," says D'Addario. "You can take the objectives of security and make them relevant to employees and management locally. If you're not allowing local input, you're missing opportunities in that local community." Piloting processes and measuring for success or failure gains buy-in, improvement opportunities and incremental contribution appreciation.

Organizations that don't have locations abroad but that do have at least one offshore supplier must also monitor and plan for broader risk impacts. As D'Addario points out, last year's tsunami in Japan is one of several high-profile crises that negatively affected multiple industries across the globe because of its impact on a supply chain that knows few borders. The risk of natural disasters, political unrest, crime or terrorism must be monitored not only in an organization's home country but in any region that could disrupt supply chain capabilities.

Compliance in a global economy is another area in which organizations will need to broaden their view of risk. As foreign direct investment increases, Brazilian, Chinese, Indian and Russian (BRIC) leadership may become more directly involved in the management of Western companies, Lefler notes. "A Chinese company buying a large U.S. company might have a different approach to exposure to Foreign Corrupt Practices Act violations. And the business practices of companies from BRIC nations, for example, may differ strongly in managing areas impacting on CSOs and security directors," he says.

Broader monitoring of risk must itself be done carefully and judiciously, explains Lex. Companies will be tempted to attempt to use every bit of information available, and a social, kinetic Internet provides a lot of information. Not all is worth monitoring. "An example would be security using social media for investigation," says Lex. "It takes a lot of time to follow every lead in that environment, and overlap is created all the time. You need to figure out what information you need and find it out quickly." Security professionals who are not discerning in their search for information will end up suffering from what social scientist Manuel Castells described as "informed bewilderment."

Under-Protected Intangible Assets

The demand for leaner operation including flex teams, the globalization of the marketplace and the consumer demand for information ubiquity – all of these lead businesses to the sensible conclusion that they must leverage the newest information technology, including cloud architecture, in order to compete. However, says USC's Brown, sometimes consumer and employee behavior and expectations move more quickly than the

technology that underpins them. Says Brown, “We as consumers have an assumption that the commercial transactions we make are secure, and we become very trusting of the Internet. But I think at some point we’ll have some huge fiascos because the underlying infrastructure is struggling to catch up.”

“If you – as a company, a consumer or a public agency – want the ability to have information on demand via any technology or medium, I would ask you, At what cost?” says Lefler. “The more you seek ubiquity, the greater your risk of someone else gaining that information.” Lefler continues that the potential for large-scale fraud increases dramatically when organizations consolidate information in the interest of accessibility. Companies recognize that breaches of customer information are bad for business, but it appears in many cases that recognition is purely theoretical.

Further, as we’ve seen, intellectual property (IP) is now among organizations’ most valuable assets. That’s why IP is under attack. In a July report, Dell Secureworks’ director of malware research, Joe Stewart, reported that the Counter Threat Unit had discovered 200 different families of custom malware used to spy and steal IP, with hundreds of attackers in just two groups out of Shanghai and Beijing.

Lefler points to the Flame and Stuxnet attacks as indicators of the future for the public and private sectors. “Those represented sovereign state attacks against another country. But the degree of sophistication of those attacks foreseeably exists with non-state actors – criminals, terrorist groups, and competitors as well. Sure, it’s against the law – a lot of things are, but that doesn’t mean they’re not going to happen. We already have people attacking companies to steal financial information and credit card information. As the technology matures and becomes more implementable by more people, more will be compromised.”

Brown argues that organizations must develop and implement intellectual property management strategies in order to protect against a threat that grows as business globalizes and technology matures: “IP strategy often is relegated to legal counsel, but IP strategy instead needs to be a more important part of your overarching operating plan. The global business

landscape has to be adopted into strategic planning more aggressively than it has been."

More and more companies are seeing themselves transforming into global, lean, connected organizations. The risks we've identified here are part of that. Risk professionals must appreciate the interconnections between changes in business and their security program strategies; they should strive to reach out to their organizational leadership to work together to understand the risks that may impact business goals as they move into this landscape. They must also remain cognizant of the organization's risk appetite and understand that as business changes, so must security.

"Companies that understand how to run in this new worldwide economy, including interfacing with global businesses, leveraging a mature Internet infrastructure and leveraging their core intangible assets, will be the winners," says Brown. "Worldwide we're sharing the risk more than we used to. The companies doing well are those that embrace that and manage the additional risk while leveraging their advantages."

This article was previously published in the print edition as "How Will Business and Risk Drivers Impact Your Mitigation Strategy."

Marleah Blades is former senior editor for the Security Executive Council, an innovative problem-solving research and services organization. The Council works with Tier 1 Security Leaders™ to reduce risk and add to corporate profitability in the process. To learn about becoming involved, e-mail contact@secleader.com or visit www.securityexecutivecouncil.com/sm. You can also follow the Council on Facebook and Twitter.

Bob Hayes is Managing Director of the Security Executive Council. He has more than 25 years of experience in security, including eight years as the CSO at Georgia Pacific and nine years as security operations manager at 3M. The Council works with Tier 1 Security Leaders™ to reduce risk and add to corporate profitability in the process. To learn about becoming involved, visit www.securityexecutivecouncil.com/?sourceCode=secmag.

Kathleen Kotwica, Ph.D., is EVP and chief knowledge strategist for the Security Executive Council (SEC). She develops strategies and processes to identify, store, understand, build upon, and disseminate the Council's Collective Knowledge™ and insights.. To learn about becoming involved, or to offer comments or questions about Next Generation Security leadership, e-mail contact@secleader.com or visit www.securityexecutivecouncil.com/sm.

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com