The Time is Now: Making Information Security Strategic to Business Innovation

Recommendations from Global 1000 Executives

Report based on discussions with the "Security for Business Innovation Council"

Anish Bhimani, Managing Director, IT Risk Management, JP Morgan Chase
Bill Boni, Corporate Vice President, Information Security and Protection, Motorola
Dave Cullinane, Vice President and Chief Information Security Officer, eBay Marketplaces
Roland Cloutier, Vice President, Chief Security Officer, EMC Corporation
Dr. Paul Dorey, Vice President, Digital Security and Chief Information Security Officer, BP
Renee Guttmann, Vice President, Information Security & Privacy, Time Warner
David Kent, Vice President, Security, Genzyme
Dr. Claudia Natanson, Chief Information Security Officer, Diageo
Craig Shumard, Chief Information Security Officer, Cigna Corporation
Andreas Wuchner, Head IT Risk Management, Security & Compliance, Novartis

An industry initiative sponsored by: RSA, The Security Division of EMC

Table of Contents

Executive Summary

A broader definition of innovation has taken hold in the executive suite, and security is front and center in this evolution. In a world where employees, customers, partners and even competitors around the globe can be collaborators in the business innovation process, security strategies and practices now have the power to make or break major business goals. These include top CEO agenda items such as product quality, time to market, customer loyalty, company reputation and shareholder value.

Most security practitioners see this as a turning point. They envision a well-defined security road map tied to business innovation and corporate strategy. They strive to create a universal understanding that security investments have a direct line to business priorities, and that building security into business innovation processes drives bottom-line results. Unfortunately, most admit that the realization of this vision is still a long way off, and that the journey is fraught with obstacles.

Why is this the case, and how can we accelerate this transformation?

At RSA, these are the questions we posed to ourselves, and to ten respected security leaders from around the world. Their answers were insightful, and the lessons learned and innovative solutions they shared with us began to illuminate a way forward. In the end, they identified seven strategies that are critical to making information security strategic to business innovation. Their recommendations can be applied to any type of organization regardless of the size of its security team or budget, from large enterprises to small and mid-sized companies.

Why an industry initiative on information security's role in business innovation?

Business innovation is now a top-level concern at most enterprises, driven by the fiercely competitive global business environment. Viewed more broadly than it has been in the past, innovation is no longer seen as inventing products in a lab, but as an overarching, multi-disciplinary, cross-functional effort to create new value.

Today, business innovation means extending beyond the enterprise – open collaboration, direct interaction with customers, tighter integration with partners, and incorporating external talent and resources. Enterprises increasingly use information technology to power their innovation efforts while facing mounting regulation and escalating threats to information. Without the right security strategy, business innovation could easily be stifled or put the organization at great risk.

Yet, information security is typically not considered strategic to business innovation. When entering new markets, building new channels, creating new sourcing models, or delivering new products, the security team often gets brought in at the tail end of the process to "bolt-on" the controls. In some cases, the security team is not engaged in the process at all. But given the current and future challenges confronting the enterprise, shouldn't information security be a full partner at the innovation table?

Business Innovation Defined

Enterprise strategies to enter new markets, launch new products or services, create new business models, establish new channels or partnerships, or achieve operational transformation.

At RSA, we think so. In fact, we believe the time is ripe for a new approach to security. While most security professionals fully recognize the need to better align security with the business, many are still struggling to translate this understanding into concrete plans of action. They know where they need to go, but are unsure how to get there. This is why RSA is working with some of the top security leaders in the world to drive an industry conversation to identify a way forward. We will be sponsoring research and reports throughout the year that explore this topic, and invite you to join the conversation. Come to the "Security for Innovation" web site and read and comment on our initiatives, and contribute your own ideas. Together we can accelerate this necessary transformation in the industry.

The “Security for Business Innovation Council”

RSA has convened a group of ten of the top minds in information security worldwide. The “Security for Business Innovation Council” is made up of successful security executives from Global 1000 enterprises in a variety of industries. These companies must comply with global regulations, are very protective of their intellectual property, and care deeply about their reputation with customers and business partners. All recognize that to be competitive, information security needs to be part of their business innovation process.

Members of the council all stress that their respective companies are not perfect when it comes to their approach to information security, as they still have many challenges. But it is clear that their security programs represent some of the most advanced in the world. They were built by forward-thinking security executives working with other leaders across their organizations, with innovation-enabling strategies in mind. Their programs are not just narrowly defined as “information security” programs but also include elements of privacy, information risk management, compliance, quality control, business continuity and/or disaster recovery.

We are conducting a series of in-depth interviews with the members of this Council and are publishing their ideas in a number of reports to be released over the coming months. This first report is an overview of the current situation and impact on the business. It begins to put forth a vision for the future, including initial recommendations for how security teams can become full partners in the business innovation process. It also makes some predictions for how the role of information security will evolve and covers suggestions for how security vendors can play a part in this transformation.

For some security professionals, this first report will validate what they have already begun to put in place. For others, it will provide structure for their own strategies or it will lay out substantive steps to take. Subsequent reports will explore topics in more depth, such as building expertise in information risk management.

State of Affairs

Council members realize the reality at many other organizations is quite different than their own. When asked why information security isn't strategic to business innovation, they offered various reasons. All agree that while some of the responsibility comes from the business side of the equation, security professionals themselves are also to blame.

The reasons vary widely across companies and industries. For example, some vertical industries don't have a high standard of care. The size of the company may be so small that they're willing to risk it all. Given the nature of some businesses, they may not have any significant intellectual property. Some companies don't have a high level of connectivity, and may not work much with third parties. Others may have limited regulatory obligations for privacy and security.

Even if companies do face regulations, the hype around compliance has died down, so many take it less seriously – the "fear of God" has worn off. Some simply deny the risks or take chances. They may not grasp the value of their digital assets. Perhaps they have never suffered a breach or don't know they have. With breaches in the news on a daily basis, a kind of numbness has taken hold.

Company culture is also an important factor affecting attitudes about security. Perception plays a huge role: the security team is commonly perceived as "the people who say 'no.'" And many security practitioners do focus on the downside, perhaps as a natural outgrowth of constantly analyzing what could go wrong. Security practitioners also often have difficulties communicating risks in terms the business understands. In part this is because they often don't have a business background, but rather come from law enforcement, intelligence, or have grown up through technical positions.

Many security programs are relatively new, so the team may have been too busy laying the foundation and responding to incidents to be proactive. Another common problem is being overly focused on compliance. Many security programs were conceived in the heyday of compliance, so audits may still be dictating security priorities rather than business strategies.

"At most companies today, security projects are being driven by compliance and audit, so what a surprise that they don't have alignment with the business! Security practitioners are not working on business problems; they're working on regulatory issues."

"Typically, in most global organizations, security is viewed at best, as a necessary evil and more commonly as a necessary friction. This derives from security's primary focus on attempting to constrain behavior to prevent negative events. Although well-intentioned, the inevitable result is that security practitioners are not viewed as enablers of innovation but people preventing the business from doing what it needs to do."

BILL BONI, CORPORATE VICE PRESIDENT, INFORMATION SECURITY AND PROTECTION, MOTOROLA

"Today's organizations have to and often want to embrace changing technologies, so it's all about chasing and securing a moving target. If security is flying blind then security will often be perceived as an overhead."

CLAUDIA NATANSON, CHIEF INFORMATION SECURITY OFFICER, DIAGEO

The Impact on Business

When information security risks are not appropriately evaluated as part of the business innovation process, what does this mean to the business? The Council described a range of outcomes. Sometimes companies take too many risks with potentially devastating consequences. Security breaches have already tarnished many brands and even ruined businesses. On the other hand, when security concerns are considered in a vacuum and not weighed against potential reward, companies are held back. Often, lack of security planning creates unnecessarily high costs and project delays.

There have been some high-profile examples of the ramifications of introducing new products and services without properly assessing security and privacy risks. Facebook was criticized for introducing Beacon technology before carefully considering the customer privacy implications. This generated a lot of negative publicity and overshadowed the delivery of a new innovative service. Another example is the Apple iPhone. Less than a month after it was introduced, the iPhone was hacked: people were able to unlock the phone from the designated network providers. This security mis-step not only spurred negative publicity, but it also generated significant contractual problems and revenue losses.

> "If security is not part of innovation, it's going to cost you. There are certain things you can neglect, but the majority you cannot ignore. Sooner or later it will hit you. And the later you put security and compliance into projects, the more it will cost, because it just adds complexity."
>
> ANDREAS WUCHNER, HEAD IT RISK MANAGEMENT, SECURITY & COMPLIANCE, NOVARTIS

Many business innovation initiatives today involve new technologies like Web 2.0 and sourcing models like crowd sourcing. In this environment, there is great potential for enterprises to lose control of customer information and intellectual property. They risk regulatory fines or having their designs ripped off and copied. But if security practitioners focus too much on the risks, their companies could miss out on the benefits of new technologies and sourcing models. Take the example of handheld electronic mail devices. When this technology was first introduced, many security practitioners would simply not allow them to be used because they represented a new risk. But eventually security was overruled because the business benefits of ubiquitous connectivity, mobile access and continuous communications were valued more than the security concerns.

Business process outsourcing is another area where some companies move full steam ahead with "eyes wide shut," not fully considering the risks. These projects often involve giving access to highly sensitive data. A breach may go beyond a loss of reputation and involve customer or shareholder lawsuits. On the other hand, some companies are missing out on the benefits of outsourcing. They shy away from certain geographies because they misunderstand the risks or focus on the wrong threats. So risks have to be carefully weighed, but so do opportunities.

"I think results at many organizations fall short of what is achievable because security takes a risk-averse approach to projects and doesn't focus on opportunity."

BILL BONI, CORPORATE VICE PRESIDENT, INFORMATION SECURITY AND PROTECTION, MOTOROLA

The timing of this evaluation is critical. Generally, it costs far less to "build security in" than it does to "bolt it on" at the end. During any kind of innovation project, whether it's building a customer web site, moving data processing offshore, or introducing a new service, security issues will inevitably come up. When security gets called in late, it means delays and significant costs. There will be hard dollar costs associated with remediating any problems. Remediation might tie up staff for weeks or months, which creates opportunity costs. By the final phases of a project, flexibility is lost, certain options for security will simply no longer be available, and the remaining options can often be the most costly. Delays translate into other costs, like revising marketing campaigns or launch plans. Soft costs include the loss of goodwill. And then there is the competitive risk. The reality is that a company that has not had a delay is going to get ahead of you.

Recommendations

When information security is not strategic to the business innovation process, organizations take great risks or miss out on great opportunities. Project costs rise. Time to market is decreased. And ultimately, companies lose their competitive edge.

There is much to be gained by building an innovation-enabling security program. In initial discussions with Council members about what security professionals can do to make this happen, a number of excellent recommendations arose. Following is a brief summary of seven of them. We'll look at some of these in more detail in subsequent reports, and look forward to hearing from you about your own experiences and ideas.

Recommendations for making security more strategic to business innovation

1. Have the right mindset
2. Know the business and speak business
3. Recognize and seize opportunities to add value
4. Build relationships and win influence
5. Become a risk-versus-reward expert
6. Build repeatable processes
7. Make time for strategic thinking

1 Have the right mindset

"There is a whole different way of looking on security today. It's about not saying no. "No" doesn't need to be in the vocabulary at all. It's about, tell me what is it that you want to do and let's see what the best way is while making sure that we're protecting the reputation of the organization."

CLAUDIA NATANSON, CHIEF INFORMATION SECURITY OFFICER, DIAGEO

It is absolutely essential to start with the right mindset. As a security practitioner, your mission is not to say "no," but rather "how." When the business has its next big idea, don't say "You can't do that, it's not secure." Instead say "Okay, this is how security can help make it happen. These are the risks we'd face and this is what we could do to manage those risks."

"Be prepared to challenge your own assumptions, things that are apparently in the holy writ of security professionals. If you're not prepared to challenge your assumptions, then how can you expect to challenge others?"

PAUL DOREY, VICE PRESIDENT DIGITAL SECURITY AND CHIEF INFORMATION SECURITY OFFICER, BP

Your job is to support and protect the business. Be a trusted partner to the business innovators. Allow them to ride the edge without putting the company at risk. And be an innovator yourself. Constantly strive to improve the security program. Find new ways to better meet the needs of the business, to increase efficiencies, to decrease costs, and to create value.

Keep in mind that security is not compliance. If you've fallen into the compliance trap, try to get out of only responding to audits and instead, switch the *focus* to supporting business initiatives. Take a look at the big critical initiatives for your firm. Think about how you will support them. How will you help make them happen? Securely, but also, faster, better, cheaper? See the bigger picture: the risk *and* the reward.

"First, 'Do no harm': meaning before you propose a control, before you impose a "deny" before you prevent something, make sure that the harm isn't going to outweigh the benefit."

BILL BONI, CORPORATE VICE PRESIDENT, INFORMATION SECURITY AND PROTECTION, MOTOROLA

"I get quite annoyed when security people talk about 'them' not understanding security. But whose job is it to make someone understand? Not the recipient but the communicator. So, 'them' not understanding security is our failure."

PAUL DOREY, VICE PRESIDENT DIGITAL SECURITY AND CHIEF INFORMATION SECURITY OFFICER, BP

2 Know the business and speak business

To be a key player in business innovation, you must know the business inside and out. Know the vertical industry that your organization is in. Know the business environment, the issues, the competition, the market and the customers. Gain a detailed understanding of the business objectives, strategies and performance plans. What are the quarterly and yearly sales targets? Where will the growth come from? Where will the profit come from? Focus your security efforts where they will get the most return. Read the business strategies. Go to strategy meetings. Talk to the business people about their goals. Figure out the risk implications and determine how you will help manage those risks.

Hone your consultative business skills. You'll need to be good at working with people, communicating, and actively listening. You'll need the ability to be empathetic and to compromise. All of these skills will help you to be a trusted business partner. Speak the language of business. Don't use technical jargon. Transform your vocabulary. Instead of using the words, "information security," call it, "information risk management." Business leaders don't talk about information security. They talk about risk. It's what they understand; they make risk decisions everyday.

Look at it from their perspective, and frame security in a business context. Why should security be part of the business innovation model? Convey benefits such as faster time to market, more options for off-shoring, better integration of identities to decrease time to use, reduction in external asset costs, and decreases in the time it takes to deliver a product securely to market. All of these can be tied back to security. And as much as possible, have really good numbers to back up your statements. Be able to quantify how the security program can deliver value, reduce costs or improve efficiencies.

Run the security program like a business. Understand your customers' requirements and deliver services to meet them. Track your progress using metrics that are relevant to the business. Simplify. Make it easy for business people to get it. Be equipped to convey your message in an "elevator pitch." Practice delivering it so concisely that someone can understand it in ten minutes or less. Develop tools like simple one-page score cards for assessing risk; evaluations that can be completed in minutes. Slim down your rule books and policies. Use internal marketing campaigns to help the business and development teams get interested and on board. For example, Council members shared the names for their own internal branding campaigns such as: "Security in our DNA" and "Secure from the Start." Develop your own marketing skills, or consider bringing a marketing professional onto your extended team.

"A shorthand course on how to survive as a CISO in the 21st century would be focused on what's important to that organization. What's the lifeblood of the organization? Intellectual property? Cash flow? If it's a governmental agency, it's the public's trust. Focus on what puts the important things at risk."

BILL BONI, CORPORATE VICE PRESIDENT, INFORMATION SECURITY AND PROTECTION, MOTOROLA

"Part of the challenge is that it's extremely difficult to quantify things from a financial standpoint. It's difficult to say, for example, every application that goes through the systems development lifecycle and gets all of the security sign offs has a certain percent less flaws or we've had 'x' amount of less problems as far as downtime, or whatever the case may be. Those are really difficult statistics to get. Yet, those are the things that the business is looking for."

CRAIG SHUMARD, CHIEF INFORMATION SECURITY OFFICER, CIGNA CORPORATION

"Be active in the business discussions. So when they're opening a new business line, doing an M&A, starting a new initiative, you can see the potential risk implications of that and what investments might be needed to protect your assets. It's that ability to see things at the 50,000-foot level."

DAVE CULLINANE, VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, eBAY MARKETPLACES

"Security to me is a product. Market it like a product. Sell it like a product. Deliver it like a product. Build a supply chain for it. If you can bring yourself to understand that, then you will be able innovate to make your product better and to be more appealing to your end users.'

CLAUDIA NATANSON, CHIEF INFORMATION SECURITY OFFICER, DIAGEO

"If you are doing your job, you shouldn't even sound like a security person. The business doesn't care how many viruses you stopped. They don't care how many cases you wrote. 'How are you helping me meet my business objectives?'"

DAVID KENT, VICE PRESIDENT, SECURITY, GENZYME

"Get ahead of the business. Understand where they want to go. Figure out what the business inhibitors are from a security perspective. What would scare them or stop them from doing that business? And come up with services that allow them to go where they want to go."

ROLAND CLOUTIER, VICE PRESIDENT, CHIEF SECURITY OFFICER, EMC CORPORATION

3 Recognize and seize opportunities to add value

"Business process innovation today means offshoring, nearshoring, partnering. It's a requirement now to be able to innovate the way you deliver services through a lower cost model. This inherently involves giving people external to your organization access to your internal systems. You have to drive security as part of that process."

ROLAND CLOUTIER, VICE PRESIDENT, CHIEF SECURITY OFFICER, EMC CORPORATION

If ever information security had an opportunity to shine, it's now. Current business innovation projects have an inherent need for advanced information security. These projects fall into two broad categories. One is technology-driven innovation to achieve a range of goals. Examples are: Mobility – to increase workforce productivity and deliver new services to customers; VoIP – to decrease communication costs; Virtualization – to decrease datacenter costs; Web 2.0 applications – to speed collaboration and deliver customized content; and Virtual worlds – to find new ways of reaching customers. These new platforms for sharing or processing information require fast and accurate ways to identify users and manage their access, as well as unobtrusive methods of protecting the integrity and confidentiality of data.

The other broad category is sourcing and globalization. R&D and product development are now in-sourced, outsourced, crowd-sourced, and/or open-sourced. Companies go wherever they must to get the lowest cost or the best talent and resources. They also combine talent and resources in joint-venture partnerships. Business processes, in every functional area from HR to IT and finance, are moving off-shore or near-shore. Maximizing the value of third-party relationships has become a core competency and the truly competitive companies will master it.

These kinds of initiatives demand sharing intellectual property, infrastructure and ideas, while at the same time safeguarding trademarks, copyrights, and patents. When customer data or sensitive financial data is exchanged, confidentiality and privacy protections are paramount. How do you allow open, free yet secure communications between these partners and also have it be seamless to the end user? Security can solve these issues and can add value in managing identities, delivering faster integration with partners, and providing efficient on-boarding and off-boarding.

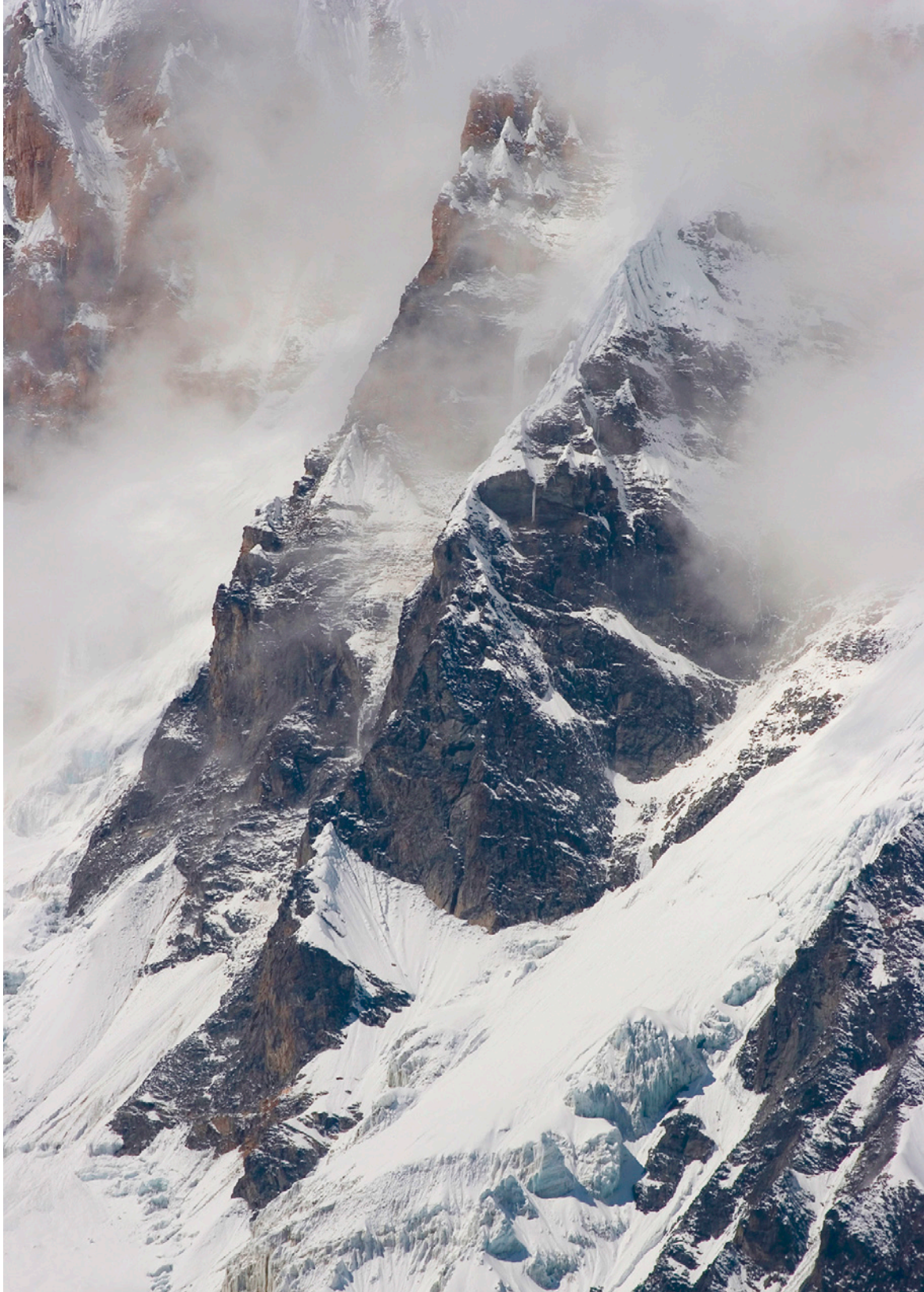
"The whole aspect of pushing things into a global workforce is having a huge impact on the business, and it's one of the things that people look to security for answers for."

DAVE CULLINANE, VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, eBAY MARKETPLACES

"Any initiatives that are aiming at the heart of technology, that are technology intensive, like the move to online channels and mobile devices, security should be square in the middle of these and involved very early on in the process."

"With globalization, there is an inherent need to manage identities. People are moving around and you have to keep track of them. They may be employed in the U.S. but working in Japan or on a project in Europe. Then add outsourcing and mergers and acquisitions. You've got to integrate all these groups. You need to give them crucial access and still let them continue to work in an effective way."

ANDREAS WUCHNER, HEAD IT RISK MANAGEMENT, SECURITY & COMPLIANCE, NOVARTIS



4 Build relationships and win influence

"Get out in front of the people, the sales people, the engineers, let them ask questions and drive your message home. People will get security. Get across how it affects their jobs, them personally. Like having the stuff they've been working on for years stolen. But it's very difficult to do that unless you're out there meeting them face to face."

ROLAND CLOUTIER, VICE PRESIDENT, CHIEF SECURITY OFFICER, EMC CORPORATION

It's one thing to have great innovation-enabling security strategies in mind, but converting your plans into action requires building relationships and having organizational influence. To really become part of your company's business innovation process, to be there at the table for new initiatives and add significant value, you have to win over a lot of people.

Beyond general support for the security mandate, executive management can help champion security's role in specific projects. Good allies can be found throughout the executive ranks, even in relatively unexpected places. Look for projects where you can deliver value for a specific executive, for example, the head of human resources. Often, security can add tremendous value to enterprise-wide projects involving the management of employees, contractors, and outside talent. Security can help manage a global workforce by increasing efficiencies in onboarding and offboarding and complying with worldwide privacy regulations.

But, executive leadership is only one facet. You need to build relationships at all levels and be able to convince the key people who are driving the business that you can contribute. Once they are convinced, you can gain the kind of access and involvement you need. Then you'll be in a position to really apply programs, systems, and services that drive value. Understand the organization well enough to know where you can leverage influence. Know who to convince in order to sway others.

A great tool to use to focus your efforts is a chart showing people's power and influence versus their support for security. Identify the key people in the organization. Some will be senior managers, while others could be influential individuals. Actually go through an exercise and plot them on the chart, with the vertical axis representing organizational influence and the horizontal reflecting support for security. People that end up in the top right hand corner are already strong supporters of security, and very high influencers in the organization. These are important relationships to safeguard. For influencers who are not currently strong supporters, define a strategy to convert them to the top right quadrant. Other key players may be supporters who currently don't have much power and influence, but are rising stars. Develop those relationships so that as their organizational influence rises, their support for security also grows. Maintain this matrix to keep track of your progress.

Relationship-building requires face-to-face interaction. This is the case for all of your stakeholders. Meet with business people in person as often as possible. Make it a point to go and have lunch with them often and talk about business. Posters, PowerPoint and online training can help convince end-users to uphold security policies and procedures, but face-to-face meetings can really help deliver your message. It personalizes your message and helps make it relevant. It also requires transparency. To be trusted by the business, you'll need to explain why certain controls must be put into place. You cannot just hide behind a veil of "top secret" or "classified," with no explanation.

"It's not technical expertise. It's understanding the organization. It's building the right relationships and ultimately, producing excellent work. In the end, dependable, excellent work validates why you were in there in the first place."

DAVID KENT, VICE PRESIDENT, SECURITY, GENZYME

5 Become a risk-versus-reward expert

"Value creation in the 21st century in many industries is largely about creating new experience and new content that is increasingly derived from digital sources and supported by digital forms, so the issue becomes, how do we measure and aggregate those up into opportunity and risk?"

BILL BONI, CORPORATE VICE PRESIDENT, INFORMATION SECURITY AND PROTECTION, MOTOROLA

The objective is to support the business in its endeavors to do new things, which inherently means taking new risks. To help your business get where it wants to go without jeopardizing the organization along the way, you'll need to be very good at weighing the risks versus the rewards. If you want to be at the table with the innovators, remember to keep the reward side in mind. It's a balance.

"Find out how the company measures risk in terms of high, medium, low and use that yardstick to create your own grid. Don't create your own "nomenclature." Understand how the business already defines risk and just plug into that. Position yourself as really lock step in place with the business, so that you get invited to the table."

Now the difficulty comes in actually making the risk-reward calculations. It's not easy. Unfortunately, information risk management as a discipline is still in the early stages. Really good statistics or the "actuarial" for security breaches simply don't exist yet. So it's hard to answer the questions "What negative events could happen?," "How likely are they?," "How much would we stand to lose if they occurred?," "How much would it cost to mitigate those risks?," and "How does this compare to the rewards?"

Some argue that it may not be possible to come up with standardized data when risk-reward calculations are so dependent on the company, its specific goals, and its taste for risk. A few standardized methodologies for assessing risks do exist, but even then, most formalized information risk management standards today don't adequately cover the reward side. The standards can help get you started, but ultimately you'll need to adapt any standard that you use to your company and the particular project. It comes down to developing an exceptional ability to make judgment calls. Get as much quantitative data as possible, but be able to make a qualitative decision.

Understand that you cannot mitigate all risks; there are some which the company will have to choose to accept and manage. For example, under the current global regulatory regime, some laws actually compete with one another so it may be impossible to comply with all of them. Or it may simply be cost prohibitive to implement certain controls. You can use benchmarking to validate your posture in determining a reasonable standard of care. What is required is a well-thought-out, well-documented process that demonstrates how risk decisions were reasonably made.

Gain a good understanding of the company's tolerance for risk and who can assume what level of risk within the organization. Create a risk assumption model for information risk management and get input and agreement from the business and executive leadership. This will help you to work with the business by guiding decision making about risk taking. Keep in mind the fundamental decision-making point, which some industries refer to as license to operate (LTO). If your activity breaches this, then you're bound to have your right to trade in a particular domain destroyed. There are some things that are just considered unacceptable. You wouldn't accept a probability measure of completely going out of business.

Find out how the business measures risk, what terms they use and what exactly these terms mean. Know what risks the business is concerned about. If your company is a public company, read the risk reports that are filed with the SEC. Once you understand how the business defines the risks, use the same definitions to discuss risks to information.

In explaining the risks to the business, effectively quantify how much of a risk something is and how much your controls are going to cost in order to mitigate that risk. Go ahead and use "headlines" or examples of breaches that have occurred at other companies, but make them relevant. Don't just use them to create vague fear, uncertainty and doubt. Try to come up with some numbers. How much would a customer information breach cost your company? What would the direct remediation costs be? What would the legal costs be? How many customers might you lose? What's the cost of a lost customer? Work with the business, finance and others in coming up with these numbers. Get them actively involved and providing input into the estimates.

It's also important to follow up with the business. For example, if you have presented a list of risks, once you put in place the necessary controls – new technologies or procedures, etc. – go back to the business to show what has been done to mitigate those risks.

"Find a way into the conversation. Go to the right meetings. Get on the right team. No one's going to invite you to these things; you've got to do it yourself."

DAVID KENT, VICE PRESIDENT, SECURITY, GENZYME

6 Build repeatable processes

Get security built into existing corporate systems for proposing, reviewing and approving business initiatives. Focus on creating fast and flexible processes that help to accelerate, not hold up, projects. Make your processes consistent across projects so that people learn how it works. Keep in mind that the objective is to get security "built in" to initiatives, not "tacked on', so you have to get in early.

It's pretty much a given that every project will entail collecting, handling, processing, and/or exchanging information. Often it's customer data, financial data, or intellectual property and involves third parties across the globe. The risks to that information require careful and deliberate consideration. If this starts early enough in the process, the enterprise will ultimately get better risk decisions, much lower costs and faster time-to-market.

"Create an architectural framework for the developers to plug into. Provide them with a platform that they can get secure services from. It makes their lives easier and it makes it cheaper and faster to create new applications."

DAVE CULLINANE, VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, eBAY MARKETPLACES

The right point of engagement will depend on the project. For some projects, it might not make sense for security to be at the table when the fundamental business decisions, like what new markets to enter or what new products to build, are being made. But, security would add value to decisions about whether or where to outsource certain data processing operations. And security must be engaged for service provider evaluations as part of the due diligence. For any project, once the technology component of the strategy kicks in, security should be there. For example, at the start of a new application design when the team is thinking about the end user environment and how the information will be accessed, security needs to have a voice.

Once you create sufficient awareness and credibility, the business will think about information risks from the start and invite security to join in the discussions early because they've seen excellent results when they do. Before you get to this point, you may have to figure out ways to "crash the party." Don't wait to get invited. Sometimes, you might even get people asking, "What the heck are you doing at this meeting?" Do your homework so that you know enough about the project to have a credible answer to this question. Be able to articulate how you are going to add value. Furthermore, it's paramount to have advocates around the table who will back you up. Before the meeting, meet one-on-one with some of the people who will be attending. Learn their perspective on how to make the project succeed and share your ideas for how you will be able to help.

"It's asking a lot to get every one of thousands of developers or engineers to think about security. So get it in embedded in the project life cycle. Do risk reviews as part of the evolution that 'say before you do this, you have to meet the following steps.'"

"When you're not involved early on, it's going to cost more money. It could potentially either delay a project or even stop a project. And it just puts a lot of angst in the process, and that's not a good thing. If you do things the right way, and have security built into the process that really enables the business to be innovative and move faster."

CRAIG SHUMARD, CHIEF INFORMATION SECURITY OFFICER, CIGNA CORPORATION

To really ensure you get in early, the security validation system needs to be built right into company's formalized processes for budget approvals so that information risks have to be reviewed before projects are even funded. As projects progress, you will need to ensure there are checkpoints or gateways along the way at which security provides their "sign-off."

Repeatable processes can really help prove that building security in creates value. Give the business repeatable processes to use for certain types of business innovation initiatives. Align these "templates" or "playbooks" to the types of innovation initiatives in the current strategy, such as acquisitions, outsourcing or new applications and help accelerate the innovation process. For example, create a playbook for doing new acquisitions, providing a standard set of security criteria for reviews. Without standard criteria, it may be unclear how reviews are being done and some divisions will need to redo the review before they trust exchanging information with the new entity. A playbook allows multiple divisions to more easily and quickly leverage those new relationships. Another example is security templates for off-shore call centers. Create a standard set of requirements for security which can be used for any call center regardless of where it may be located. This is significantly more cost-effective than approaching security as a one-off each time the business wants to open a new center.

"The problem is that success breeds more work. So you still have to get resourced, and that's not easy. So, now you've got to build approaches that integrate other people outside the group."

DAVID KENT, VICE PRESIDENT, SECURITY, GENZYME

It is crucial for security to be part of the software development lifecycle (SDLC), whether for product design or web site design. Security should be part of the project methodology from the mandate phase to production, consulting on the proper controls that need to be put in place and testing to ensure certain baselines are met before the software is released or goes live. To "bake security in" also requires training courses for developers so they know how to build secure code. Have the training be ongoing so that as new vulnerabilities are discovered or new threats arise, the developers are aware of them.

To deliver an innovation-enabling program, you will have to be budget-wise and smart about getting resourced. Security teams invariably face budget and resource constraints so you will need to think carefully about how to extend the security program beyond its current activities and priorities. To gain credibility with the other teams, work hard to keep a tight rein on your budget; don't expect to continually get new funding, even try to reduce spending. Focus on ways to continually increase efficiencies. Think of ways to redeploy your existing technologies in new ways.

If you are lock-step with the business strategy and are demonstrating value, your team might get more budget and resources. But it will never be "enough" and you'll still need to find creative ways to get it all done. Form teams by seamlessly combining full-time staff with security champions in the business and/or external resources. Leverage others in the organization. Consider outsourcing and offshoring some security operations. Companies are doing it securely with significant cost savings.

"Use automation and optimization. Get your foundation right – things like access administration and baseline controls should be automated – and then you can spend less time on blocking and tackling and more time on higher-level thinking."

7 Make time to be strategic

"If they've gone to the trouble of creating a CISO position, there is usually a honeymoon period, when he or she's got a chance to build the case for a more strategic approach. Buy yourself enough time to step back and get smart. Use the time to solve problems by thinking about them differently."

PAUL DOREY, VICE PRESIDENT DIGITAL SECURITY AND CHIEF INFORMATION SECURITY OFFICER, BP

Creating new approaches to security that align with business innovation projects takes time. Carving out time for strategic thinking and planning may seem impossible when you are already strapped just handling the basics. However, it will be essential.

You may choose to deliberately decide not to tackle some issues. If there are relatively low-risk problems that have existed for a while, you can probably leave things as they are for now. With some high-level thinking, you'll likely come up with some solutions to bigger-picture issues and get a big win. Keep in mind that even if you are given funding to expand your activities, your biggest challenge will often not be reaching your goals, but organizational capacity for new ways of doing things. There's only so much you can load a company with at once before you eventually get push back.

Strive to make your traditional security operations as efficient as possible so you can make time for high-level thinking and planning. This will also free up budget so that you can invest in more forward-looking pursuits.

Evolution of the Role of the Security Executive

Knowing there is significant change on the horizon for information security, the Council was also asked to look ahead and describe what the security executive role might look like in three years. Today's security professionals need to consider these predictions and the impact on their own careers, whether they are managers, aspire to be managers, or want to continue to grow and be a valued team member.

A common thread in all of the predictions was that there will be more focus on risk. In fact, some Council members believe the concept of traditional information security will go away. They see the current role of a chief information security officer morphing into a chief information risk officer.

> "If you are a CISO who is thinking in the past and not watching, understanding, what is happening, you are going to be securing for the past and impeding the present and the future."
>
> CLAUDIA NATANSON, CHIEF INFORMATION SECURITY OFFICER, DIAGEO

Some see the role moving beyond information risk and evolving into a general "chief risk officer" or "CRO" position, although others thought this would depend on the industry and the company. There are many elements of risk; some members didn't see all of these moving into one CRO, but rather remaining distributed across positions such as the CFO, General Counsel, and/or General Auditor, etc. Perhaps a CRO might have responsibilities for operational risk. Regardless of how risk responsibilities and titles play out and whether it will be an individual or a committee, most Council members believe most enterprises will continue to strive for a more consolidated view of risk and take a more holistic approach using an enterprise risk management (ERM) framework. Many believe that logical and physical security risks will be looked at and managed in a converged environment.

Council members agree that security professionals will need a much more international outlook. The ability to think globally will be key; you will need to have a keen perception of what it means to do business in places like China and India and understand the associated risks and rewards. In the future, security executives will also have to be able to manage more formalized liaisons with other organizations to fight cybercrime. Given that cybercrime is growing so quickly and is driven by well-organized international operations, companies will have to begin to spend more time cooperating with law enforcement, government, and each other. Right now, the liaison is episodic, voluntary and limited. But it will become consistent, broad, wide-ranging and probably at least trans-national if not international and/or global.

Additional responsibilities might include partner management; not just the security around it, but an influential role in how partners are selected and managed. There may also be fewer responsibilities for security operations. As these become more standardized and automated, they may move into areas of IT or out to the lines of business. As well, some security operations will move to managed service providers, external partners and offshore.

What Vendors Can Do

"It's a co-development, co-creation exercise as opposed to – we'll sit here in our labs, and we'll figure out what you need, and then we'll come and sell it to you."

BILL BONI, CORPORATE VICE PRESIDENT, INFORMATION SECURITY AND PROTECTION, MOTOROLA

"If they step back strategically, and try to describe a world of the future, they should then ask themselves, well, what's the sensible approach? It requires some big step outs and collaboration."

PAUL DOREY, VICE PRESIDENT DIGITAL SECURITY AND CHIEF INFORMATION SECURITY OFFICER, BP

The Council also commented on what vendors can do to help security become more strategic to the business innovation process. Vendors need to invest more time developing knowledge of their customers' specific businesses and industries and should be able to relate the value of their security solutions directly to their customers' business goals. Developing a collaborative and partnered relationship with customers is key to making this happen.

Several of the Council members suggested that in today's globalized business world, vendors should put more emphasis on how their technology can be used to enable secure business-to-business integration. Vendors should have use cases, solutions or designs that show organizations specifically how to enable security in a multi-corporate environment.

Consider adopting a service delivery model that is solutions-driven. This means transforming the traditional seller/buyer relationship into a collaborative partnership. Be willing to make technology deployments a co-development, co-creation exercise. Through this type of collaboration, vendors will have a vested interest in driving security's ability to innovate within the business. Vendors also must do a better job of collaborating to come up with better solutions for the sake of security. There have been a lot of really good ideas for standards in the security world, but they do not seem to go as far as they should.

Many Council members commented that organizations would be able to pay more attention to innovation if they were not wasting resources fixing problems introduced by insecure products. A number of Council representatives suggested the formation of a watchdog organization that serves as a third-party certifier of vendors and provides a "Good Housekeeping" seal of approval for example, for secure software or network components. Vendors, therefore, would be more motivated to provide secure programming and products to earn their certification and win contracts. Organizations could spend less time and money assessing products, and feel more confident they were buying quality products that would not generate unforeseen costs down the road.

Conclusion

At most companies, security is not strategic to business innovation because of a combination of factors. If security leaders have been too focused on control standards, they need to change their attitude; this is the first step towards an innovation-enabling security program. If the business lacks understanding but is open to new ideas, there is hope; the Council's recommendations could go a long way for these security teams. But the grim reality is that if the business simply doesn't care and has absolutely "closed the door" on security becoming more strategic, ambitious security practitioners may want to consider moving on. If you are the kind of security professional who wants to drive an innovation-enabling program, you need to find a company willing to benefit from a new approach to security.

Next steps

RSA is honored to be working with the some of the brightest minds in security; we hope you can learn from the Council's experience and apply it to your own programs. Watch for our next reports which will take a deeper dive into specific topics regarding security's role in the business innovation process.

We invite you to be part of this initiative. Go to www.rsa.com/securityforinnovation to access all of the reports as well as other research. Sign up to receive notices when reports are released or research published. Contribute your own ideas. We've built a platform for collecting and promoting the best ideas. Here you'll also find tools to evaluate your own security programs to determine how far you've come and how far you have to go. Join the conversation. Help define a new approach to security that enables business innovation.

Appendix: Security for Business Innovation Council Members' Biographies

Anish Bhimani, CISSP
Managing Director,
Risk and Security Management,
JP Morgan Chase

Anish has global responsibility for ensuring the security and resiliency of JP Morgan Chase's IT infrastructure and supports the firm's Corporate Risk Management program. He oversees security architecture and participates in the firm-wide technology governance board. Previous roles include being a senior member of the Enterprise Resilience practice in Booz Allen Hamilton and Senior VP and CTO of Global Integrity Corporation and Predictive Systems. Anish authored "Internet Security for Business" and is a graduate of Brown and Carnegie-Mellon Universities.

Bill Boni
Corporate Vice President,
Information Security and Protection,
Motorola

Bill has spent his professional career as an information protection specialist and has assisted major organizations in both the public and private sectors. Bill has helped a variety of organizations design and implement cost-effective programs to protect both tangible and intangible assets. He has pioneered the innovative application of emerging technologies including computer forensics and intrusion detection to deal with incidents directed against electronic business systems.

Dave Cullinane, CPP, CISSP
Chief Information Security
Officer and Vice President,
eBay

Dave has more than 20 years of security experience. Prior to joining eBay, Dave was the CISO for Washington Mutual, and held leadership positions in security at nCipher, Sun Life and Digital Equipment Corporation. Dave is involved with many industry associations including as current Past International President of ISSA. He has numerous awards including *SC Magazine*'s Global Award as CSO of the Year for 2005 and CSO Magazine's 2006 Compass Award as a "Visionary Leader of the Security Profession."

Roland Cloutier
Vice President,
Chief Security Officer,
EMC Corporation

Roland has functional and operational responsibility for EMC's information, risk, crisis management, and investigative security operations worldwide. Previously, he held executive positions with several consulting and managed security services firms, specializing in critical infrastructure protection. He is experienced in law enforcement, having served in the Gulf War and working with the DOD. Roland is a member of the High Tech Crime Investigations Association, the State Department Partnership for Critical Infrastructure Security, and the FBI's Infraguard Program.

Dr. Paul Dorey
Vice President Digital Security and
Chief Information Security Officer,
BP

Paul has responsibility for IT Security and Information and Records Management Standards & Services globally across BP, including the digital security of process control systems. He has 20 years management experience in information security and established one of the first dedicated operational risk management functions in Europe. Prior to BP, he set up strategy, security and risk management functions at Morgan Grenfell and Barclays Bank. Paul has consulted to numerous governments, was a founder of the Jericho Forum, is the Chairman of the Institute of Information Security Professionals and currently sits on the Permanent Stakeholders Group of the European Network Information Security Agency.

Renee Guttmann
Vice President, Information
Security and Privacy Officer,
Time Warner Inc.

Renee is responsible for establishing an information risk management program that advances Time Warner's business strategies for data protection. She has been an information security practitioner since 1996. Previously, she led the Information Security Team at Time Inc., was a security analyst for Gartner, and worked in information security at Capital One and Glaxo Wellcome. Renee received the 2008 Compass Award from *CSO Magazine* and in 2007 was named a "Woman of Influence" by the Executive Women's Forum.

David Kent
Vice President, Security,
Genzyme

David is responsible for the design and management of Genzyme's business-aligned global security program. His unified team provides Physical, Information, IT, and Product Security along with Business Continuity and Crisis Management. He specializes in developing and managing security programs for innovative and controversial products, services and businesses. Previously, he was with Bolt Beranek and Newman Inc. David has 25 years of experience aligning security with business goals. He consults, develops and coordinates security plans for international biotechnology trade meetings and serves as a pro-bono security consultant to start-up and small biotech companies. David received *CSO Magazine's* 2006 Compass Award for visionary leadership in the Security Field. He holds a Master's degree in Management and a Bachelor of Science in Criminal Justice.

Dr. Claudia Natanson
Chief Information Security Officer,
Diageo

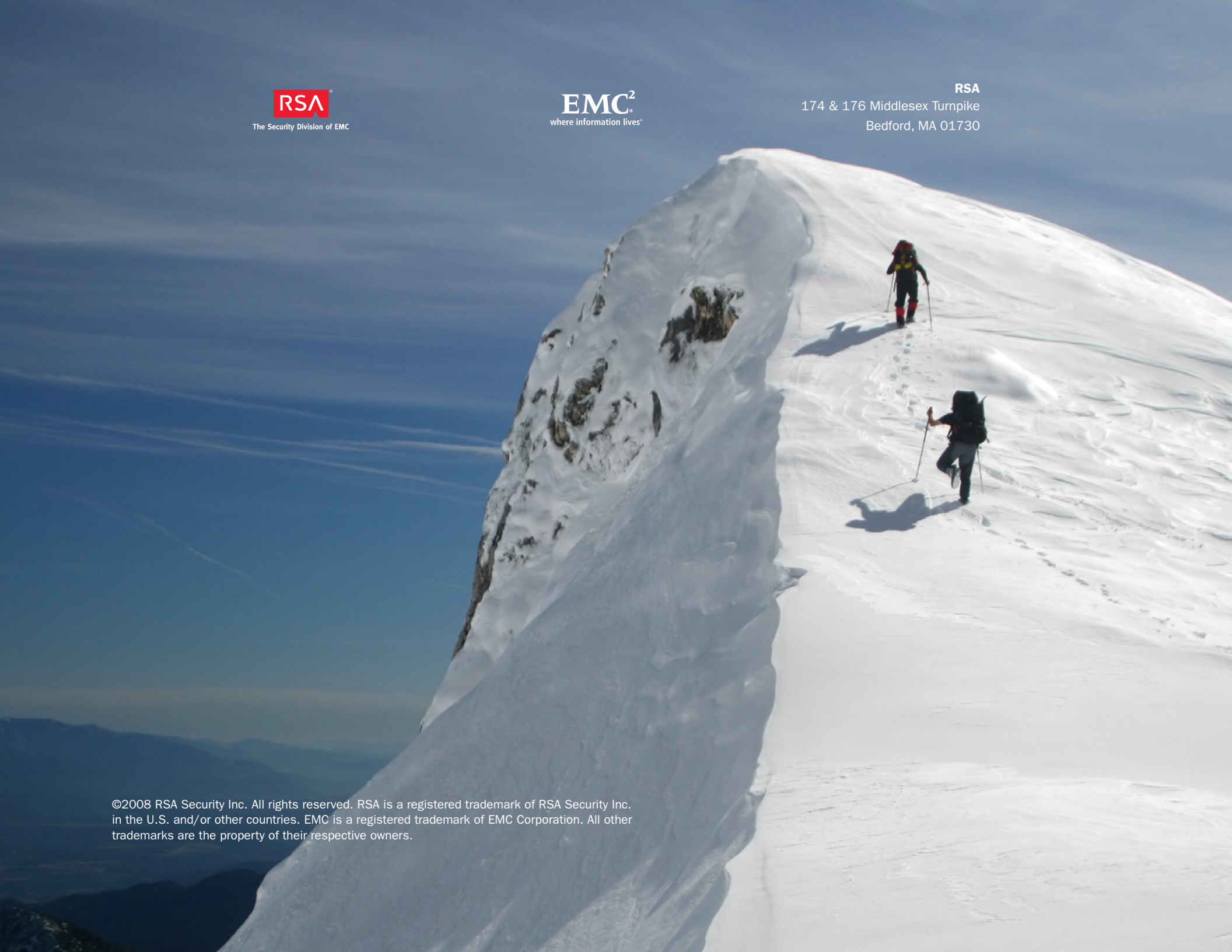
Claudia sets the strategy, policy, and processes for information security across Diageo's global and divergent markets. Previously, she was Head of Secure Business Service at British Telecom, where she founded the UK's first commercial globally accredited Computer Emergency Response Team. She has served as Board and Steering Steering Committee member of the world Forum of Incident Response and Security Teams and is currently Chair of its Corporate Executive Programme. Claudia is active in a number of European Initiatives involving areas such of privacy, e-government and network and system security for the ambient population. Claudia holds an MSc. in Computer Science and a Ph.D. in Computers and Education.

Craig Shumard
Chief Information Security Officer,
Cigna Corporation

Craig is responsible for corporate-wide information protection at CIGNA. He received the 2005 Information Security Executive of the Year Tri-State Award and under his leadership, CIGNA was ranked first in IT Security in the 2006 Information Week 500. A recognized thought leader, he has been featured in the *Wall Street Journal* and *InformationWeek*. Previously, Craig held many positions at CIGNA including Assistant VP of International Systems and Year 2000 Audit Director. He is a graduate of Bethany College.

Andreas Wuchner, CISO, CISA, CISSP
Head IT Risk Management, Security & Compliance,
Novartis

Andreas leads IT Risk Management, Security & Compliance right across this global corporation. He and his team control the strategic planning and effective IT risk management of Novartis' worldwide IT environment. Andreas has more than 13 years of experience managing all aspects of information technology, with extensive expertise in dynamic, demanding, large-scale environments. He participates on Gartner's Best Practice Security Council and represents Novartis on strategic executive advisory boards of numerous security organizations including Cisco and Qualys. Andreas was listed in the Premier 100 IT Leaders 2007 by *ComputerWorld Magazine*.



RSA
174 & 176 Middlesex Turnpike
Bedford, MA 01730

©2008 RSA Security Inc. All rights reserved. RSA is a registered trademark of RSA Security Inc. in the U.S. and/or other countries. EMC is a registered trademark of EMC Corporation. All other trademarks are the property of their respective owners.