Driving Fast and Forward: Managing Information Security for Strategic Advantage in a Tough Economy

Recommendations from Global 1000 Executives

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

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

An industry initiative sponsored by RSA, the Security Division of EMC

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.

The Security for Business Innovation Initiative

Business innovation has reached the top of the agenda at most enterprises, as the C-suite strives to harness the power of globalization and technology to create new value and efficiencies. Yet there is still a missing link. Business innovation is powered by information; yet protecting information is typically not considered strategic; even while enterprises face mounting regulation and escalating threats. In fact, information security is often an afterthought, tacked on at the end of a project or worse, not addressed at all. But without the right security strategy, business innovation could easily be stifled or put the organization at great risk.

At RSA, we believe that if security teams are true partners in the business innovation process, they can help their organizations achieve unprecedented results. The time is ripe for a new approach; security must graduate from a technical speciality to a business strategy. While most security teams have recognized the need to better align security with business, many still struggle 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.

RSA has convened a group of highly successful security executives from Global 1000 enterprises in a variety of industries which we call the "Security for Business Innovation Council." We are conducting a series of in-depth interviews with the Council, publishing their ideas in a series of reports and sponsoring independent research that explores this topic. RSA invites you to join the conversation. Come to www.rsa.com/securityforinnovation/ to view the reports or access the research. Provide comments on these and contribute your own ideas. Together we can accelerate this critical industry transformation.

Table of Contents

I. Executive Summary

Enterprises worldwide face escalating economic uncertainty; yet at the same time, the forces of globalization and technology continue to offer tremendous opportunities. Navigating the road ahead will be challenging. It will require that enterprises use not only the power of business innovation but also the ability to manage risk for maximum reward.

In these economic times, it is key that information security teams continue to move ahead with their efforts to achieve business alignment, leveraging the progress they have made over the last few years. In fact, it is now critical that information security teams know how to deliver higher levels of business value.

Based on in-depth conversations with some of the world's top security officers, this report offers an invaluable road map for building a lean yet effective information security program. It provides specific recommendations for driving efficiencies, covering key aspects such as determining priorities, resourcing security, rationalizing processes, sharing costs and automating manual tasks. The recommendations of this report provide a winning formula for continuing to speed ahead and gain competitive advantage through business innovation, while making the most of the time and resources spent on information security.

"To get budget in any organization is always difficult because it needs justification. It needs buy-in. It needs to be balanced against what the company's strategy is for that year. If your priorities are not aligned with the business, security will be seen as an overhead. You won't get funding if you're working from an island and you're not part of the bigger picture. Be part of the bigger picture."

Dr. Claudia Natanson
Chief Information Security Officer
Diageo

"The path to efficiency is, to a large degree, driven by the mechanics of how the organization works and does its job. It's an alignment issue. So you've got to find that optimized collaborative model to use within the context of your own organization."

David Kent
Vice President, Security
Genzyme

II. Introduction to the Third Report

With the world's economic woes taking center stage, business innovation is vital. Even before the financial crisis hit, economists and business leaders identified innovation as the best way to solve today's economic problems*. New ways of doing business, new products and new services enable long-term prosperity. It would be a mistake for organizations to shy away from innovation, either out of the fear of failure, the weight of regulations or the climate of uncertainty. Business leaders should continue to embrace opportunities and, together with their security partners, mitigate the risks and reap the rewards of business innovation.

In the current economic climate, enterprises are taking a hard look at their spending, including investments in information security. As budgets tighten, many security programs could be expected to achieve more with less. This tough economy is unfolding as many security departments are in the midst of making the transformation from being a siloed technical specialty to a strategic business consultancy focused on helping their organizations achieve competitive advantage. Has this become too lofty a goal given the tough economy? Absolutely Not. Now more than ever, information security must be lock-step with the business.

This third report in the "Security for Business Innovation" series builds on the findings of the first two reports and explores how the effective and efficient use of resources can keep an innovation-enabling security program moving fast and forward, particularly in a troubled economy.

The impact of the downturn on security organizations will vary, depending on the industry, as well as the compliance and risk posture, etc. Some could experience massive budget cuts and others only slight decreases. But even in the best of times, every security team should be continuously striving to run a tight ship. Enabling business innovation requires building the business case for security expenditures, using resources wisely and achieving efficiencies so that there is more to invest in strategic endeavors. The following report takes a close look at building and managing an efficient security program based on real-world guidance from the Security for Business Innovation Council.

"The best way to make your process efficient is to automate, embed and right-source (right organization and location)."

Dr. Paul Dorey, former Vice President, Digital Security and Chief Information Security Officer, BP; and Director, CSO Confidential

*Business Week, September 11, 2008

III.. Recommendations for Managing an Efficient Program

1. Prioritize based on risk/reward

In this tough economy, security teams are facing hard decisions about where to invest their time, money and efforts. Even though the economy has taken a downturn, the demands on security programs are not letting up. In fact, budgetary and staffing pressures are coupled with heightened regulatory requirements and threats. Knowing how to prioritize is the key.

Right across the board, Council members recommend that security professionals prioritize based on risk and the impact to the business. Decisions should factor in not only where the greatest risks lie, but also where the greatest opportunities can be found; in other words, the risk/reward equation (see Report 2 of the Security for Business Innovation series, "Mastering the Risk/Reward Equation"). By focusing on both the potential risk and reward, security teams can align resources to business needs. Making good risk/reward decisions takes an understanding of the business objectives and the ability to quantify risks and rewards. Especially in a tough economy, companies cannot afford to waste money on bad decisions.

"A lot of it is risk-based decision making. You need to be able to quantify the risks and say for example, "We've got a $300 million exposure, and we need to spend $30 million this year getting it down to a reasonable level." Beyond that, the fear, uncertainty, and doubt stuff isn't working anymore. People just aren't buying it. Even if it does raise their concern, it doesn't do anything to loosen their wallets. Because most companies are looking at very tight budgets so you're going to have to have a very good business case as to why you should get funding."

Dave Cullinane
Vice President and Chief Information Security Officer
eBay Marketplaces

Tough judgement calls

In a restricted financial environment, one of the biggest challenges is determining how to weigh risks. Tough judgement calls are inevitable as you strive to separate the risks your organization can live with from those that must be immediately addressed.

This difficult process of allocating resources based on risk and the impact to the business is not a one-time deal. Risk is not static and neither is the business environment. You must continually re-assess the risk/reward calculations so that resources are in the right places at all times.

Risk convergence

You'll be much more likely to get funding for your risk management efforts if you can demonstrate that your security controls will address multiple areas of risk at once. For example, knowing who has access to what systems can help prevent fraud. Those case controls can also help ensure compliance, including privacy protections as well as Sarbanes Oxley requirements.

It is imperative to shift focus from the deployment of the latest security technologies and move the focus to where the business is going. Many security practitioners tend to fall back on a technology approach. While there is definitely a role for technology, the focus of your security program should be on enabling business. Go to the different divisions within your company and figure out what innovation means to each one of them, then look for areas where security is not executing against the business objectives effectively or efficiently.

"If you have a good risk overview and know which business processes are critical, which roles, data assets, or systems are important; then you can say for example, "Okay I have my top ten priority business processes, and these are the IT systems supporting them." And if you have this full picture, when you are under budget pressures, you can prioritize the list of projects to reduce the risks to the business."

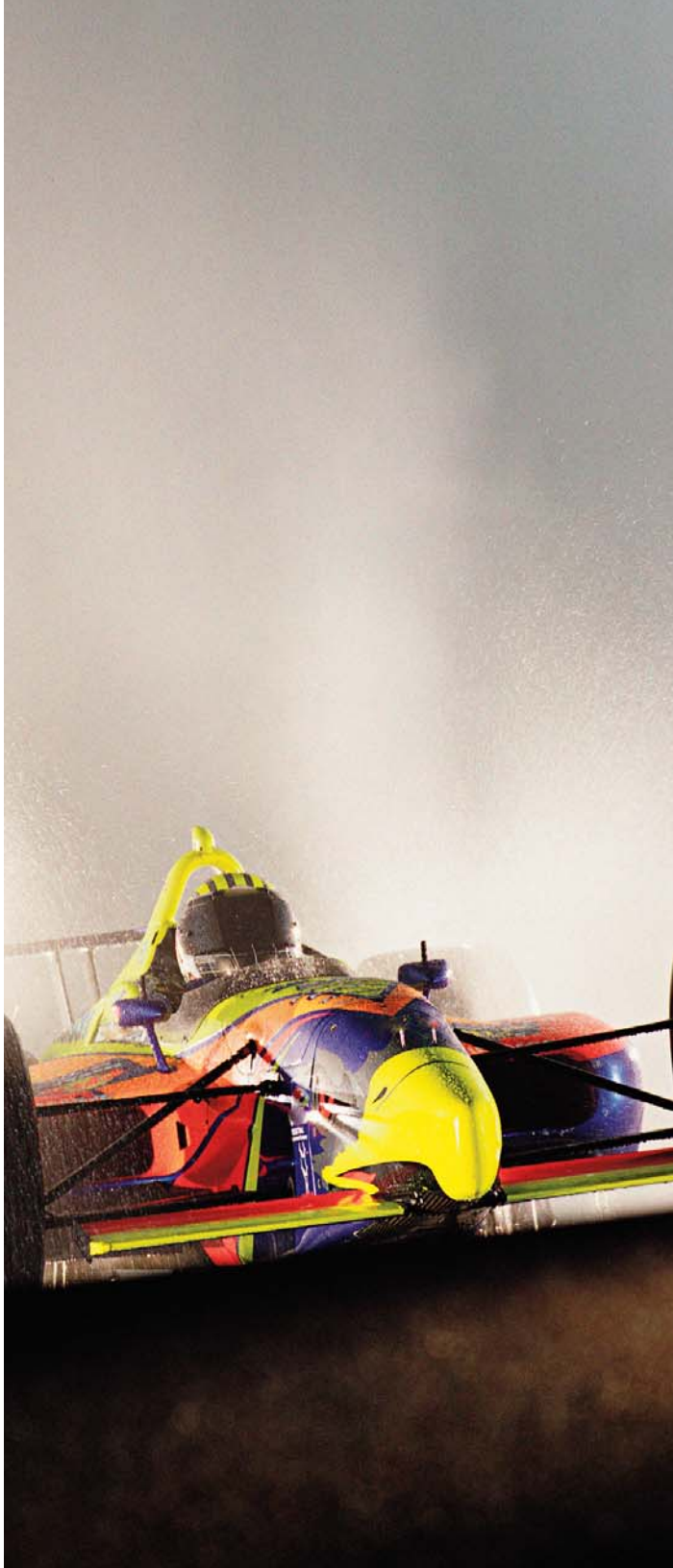
Andreas Wuchner
Head IT Risk Management, Security & Compliance
Novartis

"Resource prioritization should focus on understanding the business. Don't just focus on brick and mortar protection technology if the business needs to go outside the box. The question is, 'How do we adjust our risk management methodology to allow the business to be innovative and yet still reduce risk to the company?' It's not easy and it doesn't always mean money. Sometimes it means a different approach. Step back and say, "The business is changing, so is what I'm protecting even the right thing anymore?" You need to continuously make these assessments."

Roland Cloutier
Vice President, Chief Security Officer
EMC Corporation

"Look at it from a risk standpoint. Where do you see the highest risks in the organization that are going to have the biggest impact to the business? Then you'll need to continually re-focus from a risk standpoint. Part of your struggle will be without having that incremental increase in resources and spend, you'll continually be challenged to make judgments as to how, and where, you can effectively put your resources. And something that may have been a medium or a low or a medium-low, may not make the radar screen this year."

Craig Shumard
Chief Information Security Officer
Cigna Corporation



2. Have the right mix of people on your team

Human resources is often the biggest line item in the security budget. Even in the best of times, many security departments are stretched pretty tight. In tough times, hiring additional full-time security practitioners may be cost-prohibitive. Unfortunately, some security departments may lose people. Therefore, having the right people on the core security team is more important than ever because you'll have to rely on them even more.

Members of the core security team need to have a risk/reward frame of mind and an exceptional set of skills; be good at risk assessments and understand the business and its processes. They should be able to partner with the business, offer alternatives and speak to issues beyond those associated with security. These kinds of people are not easy to find. It's usually a matter of training them, and mentoring is often the best way to go about it. It can be difficult to evaluate security practitioners, either as potential employees or third-party contractors. Choosing the wrong people can cost a lot. They can take an inordinate amount of time to do the work; or at worst, cause you to redo their work.

Security capability management

One way to think about managing resources effectively is security capability management. Some tasks can be managed by the business itself with the deployment of the right tools, training and standards; some will require assistance from the security team; and some will need dedicated security specialists.

Make sure that you select the right person for the right job. For example, if you are augmenting your internal team of security specialists with contractors and/or consultants, don't assign them to major new projects. The inside team is probably a better choice for these. They have enough knowledge about the business to make well-informed decisions and will be less likely to make costly mistakes or slow things down. Also remember that if a consultant works on a new project, they will take all of the knowledge they build about the business and the project with them when they leave, resulting in a costly loss for your team.

If the security team really doesn't have the expertise in-house to tackle a problem, bring in consultants to help, but have your team members closely work with them so that the knowledge transfers. If it's a simple demand problem, hire consultants to help support peaks of work and give them the day-to-day, mid-range activities rather than the innovation projects. Those should be left to the inside team so that you maximize the team's knowledge value.

> "Especially as the economy is turning sour and things are slowing down around the world, it's getting even more important to make sure that you have the expertise on your team to make good risk/reward decisions so your investing in the right things. Get your whole team thinking and speaking in terms of risk. That's how they should be doing calculations and managing processes. And when they're having conversations with others they'll spread the word."
>
> Dave Cullinane
> Vice President and Chief Information Security Officer,
> eBay Marketplaces

Extending your team

To achieve coverage across the enterprise, build an extended team consisting of internal and external resources. Depending on the organization, hiring more security people may not be an option because of costs or business strategy. Even before the economic downturn, some organizations were making conscious decisions to keep their core security teams relatively small and resource security efforts with other internal and external personnel.

A potentially cost-effective way of resourcing security is to distribute and decentralize

security capabilities. Make sure that key personnel (such as network administrators, application developers and system architects) are trained in security. Then find others in the organization who, although not full-time security practitioners, have an aptitude and an interest in security. You may be able to work with HR to provide them with incentives, such as recognition or bonuses.

Security "delegates" or "proxies" can be trained regarding policy, practices and the basics of technology risk controls. Because they are in the local business units and closer to the front lines, they can often be very effective in responding to security problems. They know the geography, business environment, personalities, politics and priorities better than you do. Often they can respond earlier and help to ensure problems don't escalate and become really expensive to solve. Having security "delegates" or "proxies" at a local level also helps put ownership of security on the individual businesses.

"A key job of a CISO is security capability management, i.e., getting the right person in the right job. And so a mature program balances self-assessment and self-help, support from full-time security specialists and contractors and also uses third-party consultants. And a CISO needs to do that in a proportion appropriate to the workload and fixed plus variable cost requirements. The reason that you use the security specialists, in my view, is to focus on those assignments with the greatest risk and also the greatest innovation."

Dr. Paul Dorey
former Vice President, Digital Security
and Chief Information Security Officer, BP;
and Director, CSO Confidential

"I think the days of big budgets, big battalions of security practitioners standing in the overhead cost line are well past. Part of the challenge is that the bigger the team becomes, the more challenging it is for leadership to really align that kind of large cost with large value."

Bill Boni
Corporate Vice President
Information Security and Protection
Motorola

3. Build repeatable processes

Creating standardized ways of doing things can go a long way towards creating efficiencies. In most organizations, there are lots of opportunities for rationalizing processes and achieving economies of scale. Whether an organization has grown organically or through mergers and acquisitions, often different business units or divisions have ended up doing things in different ways. By driving efforts to rationalize processes and tool sets, the security team can help the enterprise become much more productive. There are areas that are considered "low hanging fruit," for easily gaining efficiencies, such as identity and access management. Does every division really need, for example, a different ID Admin Request mechanism or a different Privilege Access Management System?

To become as efficient as possible, think about security operations like a factory and apply the same sort of traditional operational metrics. Develop concrete, consistent definitions for measuring processes. For example, if access controls are measured on a qualitative scale, interpretations can vary widely. Instead define precisely what access controls are. Get granular; every account should have an owner, accounts are periodically re-certified (in a specific time period), things are de-provisioned (by a specific timeframe) when somebody leaves, and every piece of access can be traced back to an access request, etc. You should be able to get to a point where you know that, "It took X minutes to on-board this person," or "This person left and their access was terminated in X minutes." If processes are defined in a granular way, you can measure results, reach milestones and improve operations.

Get security embedded

To achieve efficiency, it is also crucial that security is not managed separately from business processes. Don't talk about managing security processes, but work with your business partners and engage your stakeholders to manage business processes that have embedded security. For example, have information risk assessments be part of project reviews. Get new employee access requests to be part of standard HR processes. Build security into the Product Development Lifecycle (PDLC) process.

If you build security into business processes, it just becomes part of how the enterprise is run. It's ultimately less expensive and faster than having a separate stream for security processes. As well, if security is a separate line item in a project and a project has to cut costs, security will stand-out as an easy area to cut. Instead, embed the costs of security into the costs of business processes and it will be less likely to get cut. Make sure that the security component of business processes is well-understood, socialized and institutionalized across the organization.

Leverage existing resources

Another key strategy is to leverage existing resources that are already available in the enterprise. For example, IT probably already has a change management process in place, so instead of creating a whole new process for security, leverage IT's process. Or rather than doing a separate security assessment of a business unit, leverage internal audit's assessment.

Data collection is one area where there are enormous opportunities for leveraging other departments' efforts. By doing so, you not only save time for the security department, but you also help the enterprise increase productivity. Data is typically being collected for many areas including: business continuity, business intelligence, safety, security, compliance and quality. Continually doing assessments and answering questions can slow business owners down and make them audit-weary. Security should access data that is already being collected by others and leverage it for security purposes.

"You need to take a productivity angle to Information Security, rather than a pure controls angle. Then the trick is to take what you save and throw it into further investments to help you get even more efficient in other places."

For example, if you need to ask the business a compliance or risk question, rather than create an entirely new workflow to get the answer, check if the question has already been answered in pieces within the corporation's mosaic of global information. Just pick those data pieces out of the mosaic to answer your own questions about the compliance or risk posture. Or if the data doesn't already exist, try to "piggy back" on an existing system. Add a few questions to an already existing workflow that can be enhanced to generate the right information for you. Often when you need to collect data, much of the work has already been done by other groups. The information is already there, you just need to augment it a bit or look at it through a different lens.

It is also important to maximize the solutions that the Security department has already purchased, such as security information and event management or change management systems. Often tools like these are acquired as a point solution, but their use can be extended more broadly across an enterprise and provide value much beyond the original purpose.

"A key point is, don't reinvent the wheel. There are incredible opportunities throughout a company to leverage assets from other groups to reduce the cost of ensuring the protection of a company. That may be from IT, Audit, or the Finance group. Spend the time looking at what's already been done rather than just going and doing it again. Then trust and use the information from your internal partners."

Roland Cloutier
Vice President, Chief Security Officer
EMC Corporation

"Fundamentally we don't want to have a huge security team; you know we want to have security built into the knowledge of every person working for the company. For example, if there is an IT Operator on the UNIX side, or the Windows side, he has to have some security knowledge. For us, it wouldn't work to have a huge security work force going out to the organization saying, "That's bad, you're doing this wrong, that won't work." You need to get security built in, into the business processes; into the development of new software...I don't think there is another way to win this race."

Andreas Wuchner
Head IT Risk Management, Security & Compliance
Novartis

4. Create an optimal shared cost strategy

Different enterprises have different budgeting processes, cost structures and ways of determining who pays for what. Costs for security are often shared between the centralized enterprise security organization and the various business units and departments that need to protect their information assets. The formula varies from one enterprise to the next but the goal is to make sure that spending matches objectives and needs, and that there is accountability and transparency.

Generally, there are three categories of security activities, and each is typically paid for differently. First there is security strategy and knowledge management, which involves policy development, threat research, architectural direction and enterprise-level problem solving. The security department usually covers the costs for this level of activity.

Allocating some security costs to the business

The second category involves critical day-to-day operations such as assessing the status of patches, running tools to examine configurations, and watching and responding to intrusion detection alerts. Depending on the organization, operations may be run by Security or IT or a combination. Some are run as central services, whereby Security or IT covers the costs directly and then allocates those costs back to the business based on a flat tax or per usage basis.

Part of the rationale for allocating the costs back to the business is to hold the service provider, be it Security or IT, accountable for their transactional costs. In other words, is the service being provided at a reasonable cost or for what the business (i.e., market) actually values? External benchmarking can help determine whether the services are priced right. The rationale for not allocating costs is that the administration for doing so ends up being too costly. How and if costs are allocated depends not only on the organization but also on the specific activities. Some costs may be allocated and not others.

Paying for project-specific controls

The third category of activity is project engagement, specifically working on a business innovation initiative, such as a new optimized supply chain or a joint venture. Typically the security department will cover the costs of the initial risk assessment and then, once the risks are identified, the project pays for the security controls required to manage those risks. Some of the risks may be handled through existing central services. Above and beyond those risks, there may be others that are unique to the project which require new project-specific security controls. New controls would be funded by the project. For example, if the project is to open up a new location in a riskier geography, the business would pay for any incremental security costs beyond the standard provided in other geographies.

> "There are baseline risks that a corporation faces no matter where they're conducting business. In this case, the corporation ought to absorb the cost to stand up a posture against those risks, and then allocate it out based on a formula that makes sense....To be an effective organization in the face of those risks, they need to have a consistent posture. But over and above that, if there are risks unique to a particular environment, that particular business may have to contribute to standing up a more specific posture."
>
> David Kent
> Vice President, Security
> Genzyme

During any project lifecycle, there will always be some project-specific security costs that will have to be paid for by the business, such as code reviews, penetration testing or third-party audits. It is key that all project-specific security costs are understood early on and included in the project budget up front.

Determining cost sharing can be tricky if a project requires new security controls that will ultimately be re-usable across the enterprise. Some organizations try to ensure that a business innovation project doesn't get penalized for being the first to implement new

security controls. In this case, the security department will fund the initial investment in reusable controls.

Security may have included estimates for potential new projects in their budget. If not planned for, covering these costs may be challenging. One approach is to convince the business partners to at least partially fund the initial investment (since they will be the initial beneficiaries). The approach often depends on the culture. Some enterprises advocate a decentralized model whereby costs for incremental assets are covered by the business units and they own the incremental assets.

One such model could be thought of as a "Center or Excellence" model, whereby the core security team develops policies and guidelines that enable the businesses to carry out security themselves. Centralized security creates standards and has executive oversight, based on measurement and reporting frameworks. Security leads the assessment of the need for new controls – driven by changes in external business conditions, strategies, markets, or technologies. Then they advise the business on their security responsibilities and accountabilities and how the risks need to be managed. There may be two levels of control, basic and enhanced. Some projects may need additional protection resources to meet their requirements for security, privacy, and availability to successfully achieve their business goals.

In general, security innovation projects – such as investments in new tools to automate security processes – are funded by security. In some cases, it's possible to convince business partners of the value and direct cost savings a project will bring, spurring them to fund part of it. For example, say the security department allocates costs back to the business based on usage, such as charging X dollars a month to monitor a server, Y dollars a month for desktop security controls, Z dollars per access request, etc. Once security automation tools are in place and security is able to achieve efficiencies, the costs the business pays for security services will go down. The business partners may see that by working with security to fund a security innovation, they'll be able to reduce their costs.

Ultimately, the best way to share any of the costs for security will be determined by the security team in collaboration with their business partners. The most important goal is to have a standardized method for determining risk and budgeting for the relevant necessary controls that works within your organization's cost accounting structure and collaboration model.

"The groundwork is getting people to come to the table to agree on a common problem and how each area would benefit from a common solution. And that is often very challenging, but it's worth the time up-front. Before you even tackle the problem, have a cross-functional forum where you get together your main stakeholders and get buy-in, so that going forward you have a common understanding and an agreement about how to leverage things like economies of scale, which clearly is going to help you in discussions about pricing and resourcing"

Dr. Claudia Natanson
Chief Information Security Officer
Diageo

In an era when the business environment is very dynamic, how do you distribute the resources where they're needed? How does the security team guess how many resources they're going to need in order to manage all of the requirements across the organization? Instead of building a security empire, have the organizations own the incremental assets. Security provides the standards and has a governance program. This is how one could achieve a responsible degree of information risk management without an exorbitant investment in staff and in budget and capital to do so.

Bill Boni
Corporate Vice President,
Information security and Protection
Motorola

"I want to get to a point where people don't have to go out and do manual risk assessments. I want to get to continuous controls monitoring. We don't need a person to go and check those things. We can get that from the system itself. As much as possible, take the humans out of the data gathering process. And then use the people for the interpretation of that data, or for the governance part. So my point is, the more you automate the easy stuff, the more cycles you free up for people to do the hard stuff."

5. Automate and outsource – but wisely

Using technology to automate manual processes and moving to outsourced services for some security functions can provide significant efficiencies and cost reductions. But it's important to plan and manage these efforts carefully in order to maximize cost benefits.

Risk management is one area that many organizations have identified as critical. Many are working hard to reduce the time and effort it takes to evaluate the risks involved with specific business innovation projects and gauge the enterprise's overall risk and compliance posture on an on-going basis. Risk assessments and evaluating risk/compliance posture are resource-intensive activities that are ripe for automation. If security departments can use technology to reduce the time and effort required, it will really help cut organizational costs.

Both in-house and off-the-shelf tools are being used to help manage risk assessments. These systems enable the business to perform self-assessments and then monitor the workflow and track the follow-up work. Some of the self-assessment tools also provide information on the security solution required. The objective is to automate the process so that the business doesn't always have to meet with the security people, which is expensive and time consuming. Also, increasing the automation and effectiveness of workflow controls helps increase visibility and make the unknowns a little more predictable.

Governance, risk and compliance

Some market analysts have categorized tools for risk monitoring and risk management as "governance, risk and compliance" or GRC tools. Their features and functionality vary, but in general, the promise of GRC tools in general is that they will help do risk assessments; prioritize risks on an ongoing basis; monitor threats and changes in compliance requirements; and allow you to have a more timely understanding of the impact of certain risks to the business.

Some GRC tools take feeds from throughout the environment including from security information and event management (SIEM) or anti-virus (AV) systems. Opinions vary about how well this works. Some believe that although GRC tools can make it easier to do self-assessments, they are not really at a point where data can be automatically populated. Because the current GRC technologies require so much customization, some think it may be more efficient to build a system in-house. Ultimately, a common goal for security departments is to move away from people doing risk assessments and move to what could be called "continuous controls monitoring."

Technology is not a silver bullet

Risk management or GRC tools do offer the potential for increasing efficiencies, but security teams need to do a thorough evaluation of how these tools will fit within their enterprise. Integration can end up being quite difficult and costly, especially considering all of the legacy systems that will need customization. For any kind of automation technology, it is important to recognize that just buying the technology is not going to make the security processes more efficient. Organizations should not rush into buying off-the-shelf tools or developing in-house solutions without first having all their processes, standards and rigors in place. Even if some technologies can increase efficiencies, they may not actually reduce costs because they require so much additional investment to deploy and manage.

Another way to reduce costs and increase efficiencies is to squeeze every last drop of productivity out of your existing tool set. Some Council members commented that security departments are not using the full feature set and functionality of many of the security technologies and automation tools they already have. Figure out how to leverage the tools you've got. Perhaps instead of investing in new technologies, invest in the expertise to learn how to fully exploit existing systems. Often a tool can do a lot, but the security team is stuck on the first level, using only the basic functionality and never fully tapping the true potential of the tool.

Outsourcing requires careful oversight

Some organizations are huge fans of outsourcing and others are not so sure it will save money in the end. Outsourcing can help because it is often much too expensive to retain in-house expertise. It's a good way of accessing talent without having to employ dedicated people. Outsourcing the routine, standard and highly-repeatable security functions can be an excellent road to cost effectiveness.

However, while outsourcing may appear to make security cheaper and more efficient, it may not always be the most secure or cost-effective thing to do. In the end, you have to really trust your outsourcer. If you are spending a lot of money on significant oversight, you won't end up saving costs. And it may be difficult for you to even assess whether or not they're doing the work properly because you don't have the right expertise in-house anymore.

Vendor sourcing also provides huge opportunities for efficiency gains, not just for security vendors but for many areas such as general IT, application development and business process outsourcing. Typically within large enterprises, a single vendor has completely separate business relationships with many different business units. This means, for example that each business unit is doing their own separate security assessments of the same vendor. For maximum efficiency, this siloed situation must be changed to an enterprise-wide approach to vendor relations.

Security organizations also face inefficiencies based on having to manage too many technologies in the "security stack." The reality is that there is much overlap between the tools in the stack creating major inefficiencies. Security tools need to be converged and built as unified devices that combine the functionalities of many different tools into one.

Additionally, with the adoption of virtualization and cloud computing, enterprises will begin to get rid of physical servers. Security should focus their efforts on these new initiatives rather than spending a lot of time and effort securing technology that may soon be gone.

"I would venture to guess a fair amount of folks really only leverage a small part of the functionality of many of the tools that they have in their organization because they don't either have the resource time or knowledge to be able to fully leverage them. And a lot of what the hype is geared on is the newest and greatest tool as opposed to leveraging everything that you possibly can and then see if there's a gap".

Craig Shumard
Chief Information Security Officer
Cigna Corporation

"In terms of looking for efficiencies, I think that there are too many security products now in the environment, and there is tremendous overlap. The security product stack has become unsustainable. I've challenged every vendor that I've met with recently to help me define the seven or eight products that we need to achieve the same level of security that we have today. We can't continue to operate fifteen to twenty--five (or more) security products. I don't believe that we can continue to just add new security products to the environment and expect that we will use them effectively. I keep visualizing the Leaning Tower of Pisa. Maybe the security control tower is standing today. I think that if we keep adding products, the tower will fall over and bury the folks trying to manage it".

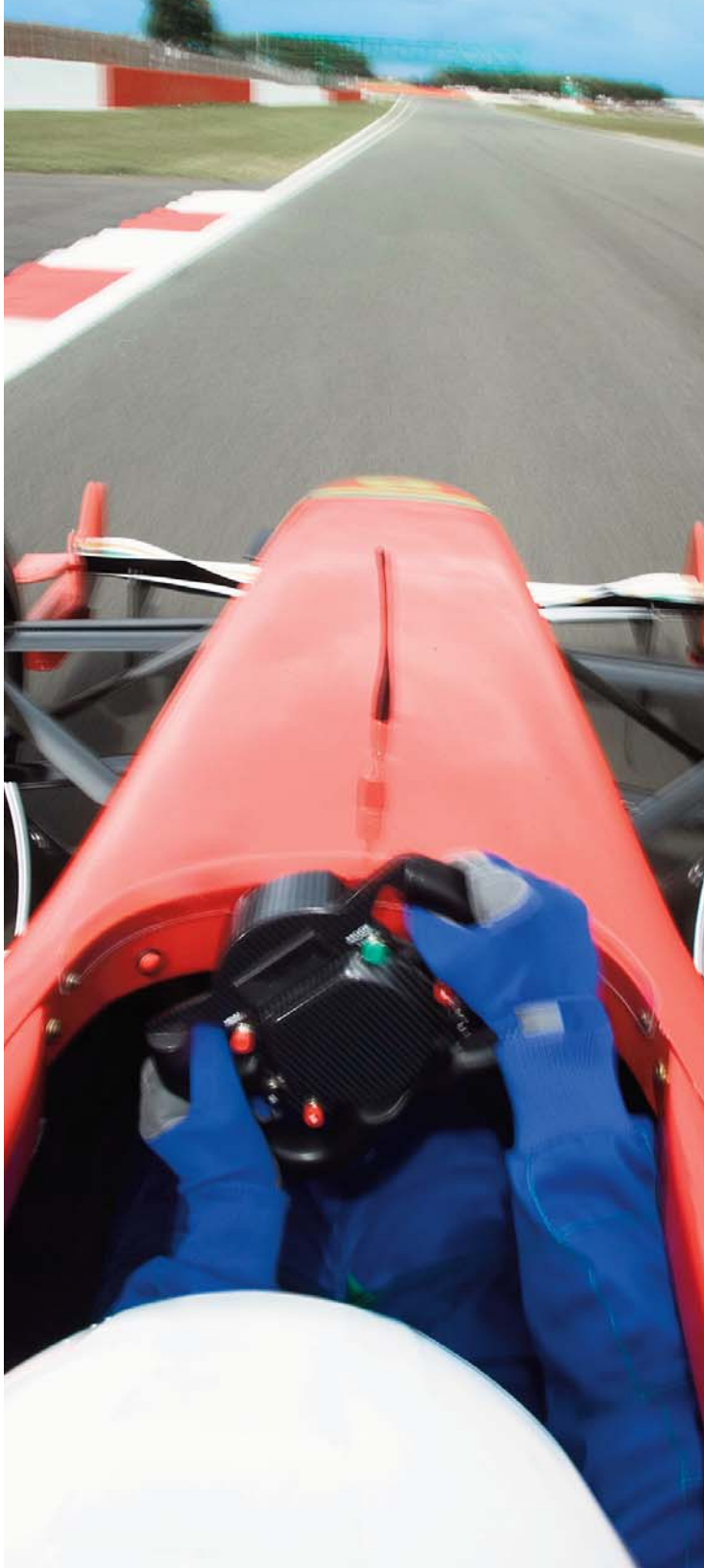
IV. Conclusion

By all accounts, it's going to be a difficult road ahead. The tough economy adds to the many challenges already facing security organizations. But armed with the right knowledge and experience, information security teams can continue to make bold advances.

Over the past few years, security teams have made significant strides in becoming true strategic partners to the business. Now, in the midst of the economic turmoil, it's important not to lose ground. In fact, this is actually the perfect time to leverage the hard-won relationships and lessons learned to achieve increased business value.

A security-enabled enterprise can gain many advantages; security can enable everything from advanced supply chains to collaborative workspaces through expertly managing the risks to information. So, even against the backdrop of an economic downturn, security organizations need to drive fast and forward in making security more strategic to business innovation.

Central to this mission will be the ability to identify the right priorities and make every single investment count – including investments in people, processes and technology. Without this capability, the wrong projects will get funded while business-critical efforts will languish. Based on this understanding, top security professionals recommend a laser-focus on not only the risk picture but also business objectives, while building the most efficient and cost effective security programs possible.



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.

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.

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."

Dr. Paul Dorey
former Vice President Digital Security and Chief Information Security Officer, BP;
and Director, CSO Confidential

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 Committee member of the world Forum of Incident Response and Security Teams and is currently Chair of its Corporate Executive Programme. She is active in a number of European Initiatives involving areas such as 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' 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 Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

CISO RPT 0109