

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

Recommendations from Global 1000 Executives

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

- **Anish Bhimani**
Chief Information Risk Officer,
JPMorgan Chase
- **Bill Boni**
Former Corporate Vice President,
Information Security and Protection, Motorola
- **Roland Cloutier**
Vice President, Chief Security Officer,
EMC Corporation
- **Dave Cullinane**
Vice President and Chief Information Security
Officer, eBay Marketplaces
- **Professor Paul Dorey**
Founder and Director, CSO Confidential; and
Former Chief Information Security Officer, BP
- **Renee Guttmann**
Vice President, Information Security and
Privacy Officer, Time Warner
- **David Kent**
Vice President, Global Risk and Business
Resources, Genzyme
- **Dr. Claudia Natanson**
Chief Information Security Officer, Diageo
- **Craig Shumard**
Chief Information Security Officer,
Cigna Corporation
- **Andreas Wuchner**
Director IT Security & Risk, Deutsche Bank

This synopsis is a small teaser of the wealth of information provided by the Council. For a deeper dive, please view the full report at www.rsa.com/securityforinnovation.

Innovation in a Tough Economy

Innovation will be central to surviving today's economic downturn. Enterprises need to find new ways of doing business, and develop new products and services in order to enable their long-term prosperity. Business leaders should embrace opportunities and partner with security to mitigate the risks and reap the rewards of business innovation. However, with budgets tightening, security programs will likely be expected to accomplish more with fewer resources. This will be a difficult task, especially as many security departments are in the midst of making the transformation from being a siloed technical specialty to a strategic business consultancy. In this economic climate, information security must strive to be lock-step with the business. The following recommendations, based on real-world guidance from the Security for Business Innovation Council, are important steps towards building and managing an efficient security program that continues to drive business innovation even in a tough economy.

Recommendations for Managing an Efficient Program

Prioritize based on risk/reward

As security programs face budgetary pressures on top of heightened regulatory requirements and increased threats, knowing how to prioritize is key. Security professionals must prioritize based on risk and the impact to the business. Factor in not only where the greatest risks lie, but also where the

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.

greatest opportunities can be found. Continually re-assess risk so that resources are allocated to the right places at all times.

Think in terms of 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. Certain controls can also help ensure compliance, including privacy protections as well as Sarbanes Oxley requirements. Be careful not 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 and focus on these areas.

Have the right mix of people on your team

Security's human resources budget may be limited so it is imperative to have the right people on your team. Team members need to have a risk/reward frame of mind, be good at risk assessments, understand the business and its processes, and be able to leverage partnerships. Finding employees already armed with these skills is very difficult. It's usually a matter of training them, and mentoring is often the best way to go about it.

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. The trick is selecting the right people for the right jobs. To achieve coverage across the enterprise, build an extended team of internal and external resources. Distribute and decentralize security capabilities by finding security

Recommendations for Managing an Efficient Program

1. Prioritize based on risk/reward
2. Have the right mix of people on your team
3. Build repeatable processes
4. Create an optimal shared cost strategy
5. Automate and outsource – but wisely

“delegates” or “proxies” out in the business lines who, although are not full-time security practitioners, have an aptitude and an interest in security and can be trained in technology risk controls. These delegates will not only increase efficiencies and hasten security responses, but also help to put more ownership of security on the individual businesses.

Build repeatable processes

Having standardized processes can go a long way towards increasing efficiencies. As organizations grow, different business units or divisions often end up doing things in different ways and having their own processes. This is an inefficient way of operating. The security organization can help the enterprise become much more efficient by driving efforts to rationalize processes and tool sets. Think about security operations like a factory and develop concrete, consistent definitions for measuring processes that are very granular so that you can measure results, reach milestones and improve operations. Get security embedded into business processes as this is ultimately cheaper and faster than having a separate stream for security processes.

“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 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 Nathanson
Chief Information Security Officer
Diageo

Another key strategy is to leverage existing resources that are already available in the enterprise. Data collection towards risk assessments or audits is one area where leveraging existing resources can be especially beneficial. Data is typically being collected by others for many areas throughout the organization and security should access that data and leverage it for security purposes. This not only saves time for the security department, but also helps the enterprise increase productivity by not having to continually do assessments. It is also important to maximize the technology solutions that the security organization has already purchased as these tools can be extended more broadly across the enterprise and provide value beyond their original purpose.

Create an optimal shared cost strategy

Different enterprises have different ways of determining who pays for what security controls. Although organization's methods may vary, the goal is to ensure that spending matches objectives and needs, and that there is accountability and transparency in the process.

Generally, there are three categories of security activities, and each is typically paid for differently. First, security strategy and knowledge management is usually paid for by the security department. Second, for critical day-to-day

operations, some of the cost may be allocated to the business unit. How and if costs are allocated will depend on the nature of the organization but also on the specific activities. Third, for project-specific controls, the security department typically covers 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. If new controls are required for a project and they are reusable, then the security department may fund the initial investment.

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. It's important to plan and manage these efforts carefully in order to maximize cost benefits. One area ripe for automation is risk assessments and evaluating risk/compliance posture which are resource-intensive activities. Governance, risk and compliance (GRC) tools offer some promise. Keep in mind that technology is not a silver bullet. Even if some technologies can increase efficiencies, they may not actually reduce costs because they require so much additional investment to deploy and manage. Outsourcing the routine, standard and highly-repeatable security functions is another way to be cost-effective but it requires careful oversight. 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.

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, move from silos to an enterprise-wide approach to vendor relations.



Don't Lose Ground

By all accounts, it's going to be a difficult road ahead. But armed with the right knowledge and experience, information security teams can continue to make bold advances. Over the past few years, security organizations 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. This is the perfect time to leverage the hard-won relationships and lessons learned to achieve increased business value.

“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

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, although business innovation is powered by information, protecting information is typically not considered strategic and information security is often an afterthought. 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. 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 have 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 publishing their ideas in a series of reports and sponsoring independent research that explores this topic. RSA invites you to be part of the conversation. To learn more about the initiative and the Council members, and to read the full reports, please visit www.rsa.com/securityforinnovation.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA and RSA Security are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2008 RSA Security Inc. All rights reserved.