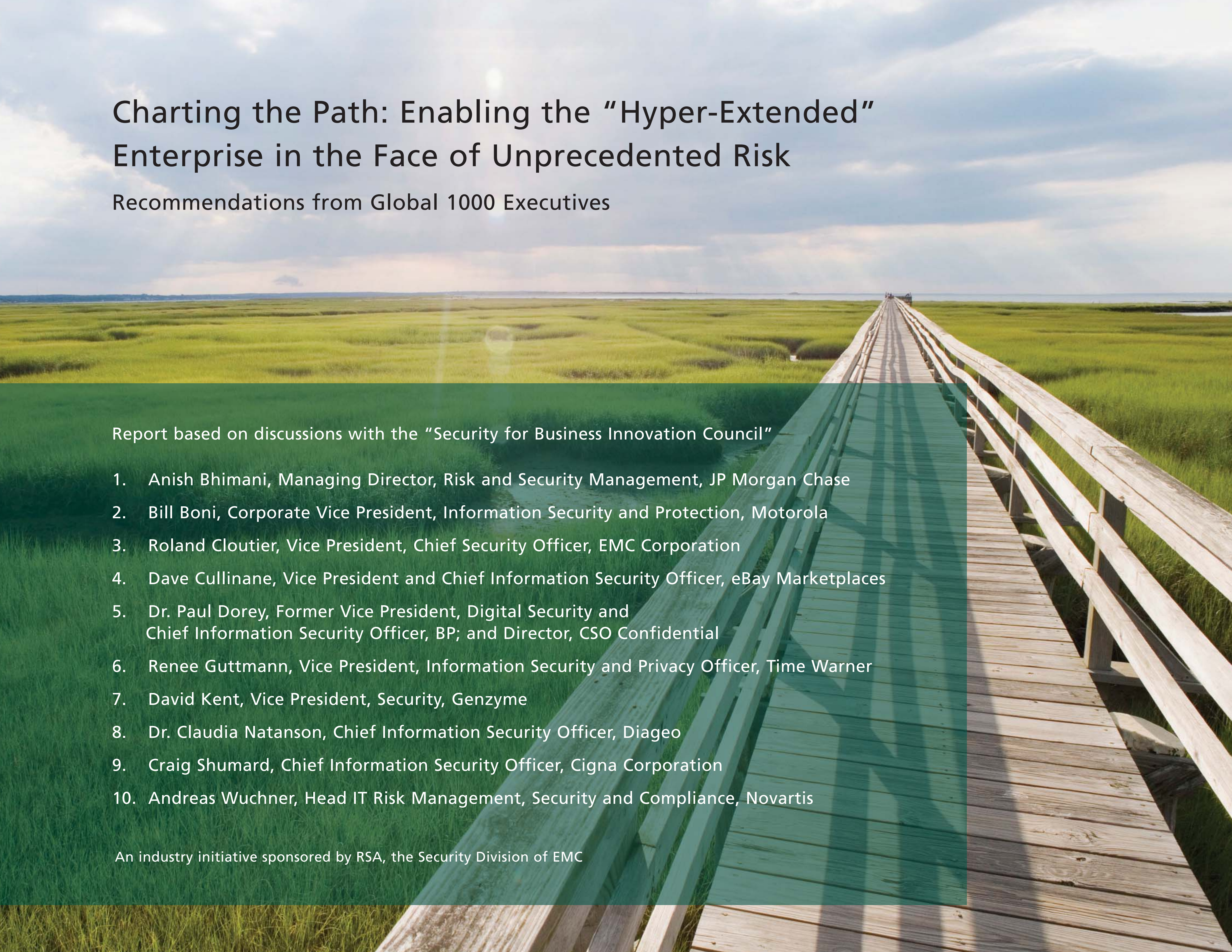

Charting the Path: Enabling the "Hyper-Extended" Enterprise in the Face of Unprecedented Risk

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 and 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 and Compliance, Novartis

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

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. Though business innovation is powered by information; protecting information is typically not considered strategic; even as enterprises face mounting regulatory pressures and escalating threats. In fact, information security is often an afterthought, tacked on at the end of a project or – even 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 specialty 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. Go to www.rsa.com/securityforinnovation/ to view the reports or access the research. Provide comments on the reports and contribute your own ideas. Together we can accelerate this critical industry transformation.

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.

Table of Contents

I. Executive Summary

The traditional boundaries surrounding our organizations, assets and information are rapidly dissolving. At the same time, the difficult economic climate is forcing enterprises to achieve extreme levels of efficiencies and speed of operations. In this environment, business innovation means faster and cheaper ways to reach customers, identify new markets, come up with new products, and collaborate across a vast array of partners.

Promising new technologies such as cloud computing, virtualization, and social networking are being touted for their power to help achieve corporate objectives. And outsourcing continues to gain favor as a strategy to reduce costs and drive organizational focus on core business. But many security leaders are realizing that without a strong vision for the end destination and an acute awareness of the changing threat environment, well-intentioned actions to drive new business value could create dangerous exposure to risk.

This is not a time to sit back and see what happens, or alternately – to rush forward without careful thought in the interest of being opportunistic. Now is the time to chart a strategic path, to capitalize on new possibilities while avoiding the potential pitfalls that could throw your organization off course.

Based on in-depth conversations with some of the world's top security officers, this report looks at where information security is headed and offers specific recommendations for developing an updated information security model that reflects the emerging opportunities and dangers at hand. It provides tangible advice that will help you tap the hyper-extended enterprise for business advantage, even in the face of unprecedented risk.

"Where we are at today in information security makes me think about Andy Grove's concept of a strategic inflection point. When the old strategic picture dissolves, it can mean an opportunity to rise to new heights or it can be deadly. Trying to conduct business as usual isn't going to fly. But the good thing is a strategic inflection point does not always lead to a disaster. It creates opportunities for players who are adept at operating in a new way."

Council Member

"The biggest business driver for security is now innovation – enabling the business to be rapid, flexible and adaptive in this environment. It's sort of the antithesis of what security traditionally has been, but building a new model of security means also being rapid, flexible and adaptive."

Dave Cullinane
Vice President and
Chief Information Security Officer
eBay Marketplaces

II. Introduction to the Fourth Report

Recent events have given rise to what many are calling the "new economy;" one in which enterprises are confronted by immense challenges. This new economy has arrived just as several key transformational technologies are entering the scene and being heralded as highly-charged engines of efficiency and growth. At the same time, outsourcing has come of age. It has gained enormous credibility as a business strategy for reducing costs and sustaining competitive advantage. The stage is now set for enterprises to accelerate the adoption of new web and communications technologies and more deeply integrate a much larger number of third-parties into their operations.

What does all of this mean? The enterprise is extending well beyond the already-expanded frontiers ushered in by the Internet age. Coined several years ago, the term "extended enterprise," acknowledged that organizations are no longer just made up of employees and management, but also encompass partners, suppliers, service providers and customers.

Taken to the next level, the "hyper-extended" enterprise is exchanging information with more constituencies in more ways and more places than ever. And the tools of connectivity, collaboration and communication are enabling operating speeds never thought possible.

This is all becoming a reality faster than anyone imagined. This transformation is accelerating out of necessity, as enterprises do whatever it takes to reduce costs, decrease time-to-market and stay competitive. Understanding these trends is essential to developing a strategy that will protect information while enabling the hyper-extended enterprise to operate successfully.

This fourth report in the "Security for Business Innovation" series looks at how information security programs must respond to these trends, given the dramatically changing risk picture. As the hyper-extended enterprise attains higher levels of openness and reaches new terrain, it has the potential to drive enormous business benefits. Yet at the same time, it exposes organizations to higher levels of risk. Mix in the desperation created by the economic downturn and the growing sophistication of insider threats, fraudsters, and attackers, and you have a complex and treacherous risk environment without precedent. And what makes it all the more perilous is that these risks are increasing exponentially while the resources available to mitigate them are on the decline.

At this juncture, a new paradigm for information security is sorely needed. This report offers an analysis of this emerging terrain and puts forth some recommendations for charting a path forward. The guidelines in this report do not provide the complete answer, but rather suggest concrete steps which can be taken to align information security to intense business innovation, reduced levels of resources, an unprecedented risk environment and the relentless pace of change.

"These are the most urgent and critical issues facing CISOs beyond the active intruders, the botware, the malware, the things that we're already fighting today. This is an area that's going to come up very quickly on people. All of a sudden they're going to realize that their IP is no longer in their data store within their environment, it's in some service provider's. Or their customer data is now in a CRM infrastructure outsourced by another third party. And they don't have any security insight into those resources at all. This is going to happen faster than I think anybody in the industry believes."

Roland Cloutier
Vice President, Chief Security Officer
EMC Corporation

"The ability to define the perimeter of the enterprise has now firmly disappeared. That's both in a technical and business sense, with the level of third-party workers, outsourcing, supply chain, and "in the cloud" services. All of these are making it much harder to define where one enterprise ends and where another begins."

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

III. The Dawn of the Hyper-Extended Enterprise

The hyper-extended enterprise is defined by extreme levels of connectivity and information exchange, as the enterprise assimilates a range of new web and communications technologies and distributes more business processes to even more service providers.

Cloud computing is one of the technologies that is taking the enterprise by storm. IDC predicts that in just three years cloud computing will move from "early adopters" stage to mainstream market adoption.[1] Also according to IDC, spending on IT cloud services will grow almost threefold by 2012, reaching $42 billion and capturing 25% of IT spending growth.[2] Virtualization is another technology on the rise. According to the Goldman Sachs Group, Fortune 1000 companies will have virtualized 34 percent of their servers within a year – double the current level of 15 percent.[3]

Enterprises are also moving quickly to capture the power of social networking. Facebook, with 175 million users, is on track to surpass 300 million by the end of 2009.[4] Globally, social networking has enjoyed a 25 percent growth in unique visitors in the last year, with some sites doubling their user base. And the demographic profile is quickly changing. Social networking is no longer a tool just for high school and college students. On some networks around 40 percent of users are over 35. So it’s no wonder that businesses have taken notice; given shrinking budgets, most are eager to take advantage of that kind of reach. And they will.

> “The enterprise is drastically changing, not just who we connect to or how we connect to them or who has access to what information, but the basic premise that our enterprise or corporate operating environment is now migrating outside of our basic operational control infrastructure.”
>
> Roland Cloutier
> Vice President, Chief Security Officer
> EMC Corporation

According to Deloitte,[5] 2009 will be the breakout year for social networks in the enterprise.

The enterprise is also accelerating the adoption of mobile devices. North American enterprises will be supporting more mobile phones than desktop phones by 2011.[6] By then, close to 75 percent of the U.S. workforce will be mobile, with workers increasingly dependent on devices like the consumer-oriented Apple iPhone or the Palm Pre.[7]

Another way consumer technology is taking hold in the enterprise is the increasing use of consumer VoIP services such as Skype, as businesses seek lower cost communication. With a total head count of 405 million registered members (as of the end of last year), Skype is adding 380,000 members per day. Already 62 percent of business subscribers are using Skype to better communicate with their customers.[8]

While technology is being quickly adopted in the enterprise, outsourcing is also being aggressively pursued. Enterprises are expected to intensify outsourcing in an effort to streamline costs, do more for less with their budgets, and increase competitiveness.[9] The economic downturn is expected to boost demand for business process outsourcing[10] and IT outsourcing.[11]

Although things look gloomy for the larger global economy, outsourcing is a growth market. Service providers globally have reached new levels of process specialization and sophistication. More outsourcing will be adopted by more organizations as they focus on their core businesses, and work through financial and competitive challenges.

Another significant trend in outsourcing is enterprises are seeking partners in new locations. Some enterprises are now reversing their previous offshoring strategies and forging relationships with new partners on-shore. Others are considering service providers outside of traditional offshoring centers such as Bangalore and Chennai and instead turning to new locations such as Belfast, Sofia and Cairo. These destinations are among a group of approximately 30 new “locations to watch,” according to some analysts. And these new locations may take up a larger proportion of the new outsourcing work, as more traditional locations rapidly approach a saturation point.[12]

IV. The Unprecedented Risk Environment

Several factors are coalescing to create an unprecedented risk environment; and it is becoming much more difficult to assess risk.

The threats: faster than ever and more unpredictable

This report does not intend to provide an in-depth analysis of current threats; there are many other sources for that information. Instead, a few striking examples are presented that characterize today's threats and demonstrate how rapidly they are evolving.

The pace of malware has reached staggering levels. Security professionals are actually getting used to numbers such as: a new infected web page is discovered every 4.5 seconds; there are over 20,000 new samples of malware every day[13]; and botnets change their malware signatures every 10 minutes.[14] Malware is infecting not only traditional operating systems, but also mobile devices. Web sites are the new favorite vector and malware is also being spread through social networking. So it's no wonder current defenses against malware are no longer effective. For example, a recent study shows some signature-based anti-virus technology, a major part of security infrastructure, now only detects 30 percent of all malware.[15]

Beyond malware, security professionals also have to deal with an alarming number of data breaches and identity thefts, with incidents affecting organizations of all sizes and types, including governments and companies. These events, in which thousands or even millions of records have been compromised, are regularly featured in the headlines. They are the work of insiders and external hackers, or both working together.

It is now a common mantra in security that the nature of the threats has changed. Gone are the days of script kiddies looking for fame and notoriety; now enterprises face a very sophisticated worldwide fraud machine run by organized crime; with many players, each having their own niche. This system is very adaptable, changing tactics quickly to outwit any attempt to foil their operations.

The end result is that there are more threats coming faster than ever before and they are changing all the time. It is no wonder that some security professionals feel outpaced. What security professionals are expected to absorb on a day-to-day basis has reached near impossible levels. And the evolution of the threats is constant. The threats are more significant today than they were six months ago or last year, and they will be more

significant six months or a year from now. There is also the unpredictability of today's attacks. Zero-day (or zero-hour) attacks and viruses, which work to exploit unknown, undisclosed or patch-free computer application vulnerabilities, are now commonplace.

Vulnerabilities have also increased through the proliferation of information on social networking sites. Although social media is great for collaboration, it's also a great way for the bad guys to learn all about the company and its personnel, including real-time location updates. This potentially paves the way for novel types of social engineering attacks or even blended attacks. These attacks could use data obtained electronically to commit crimes against information assets, physical property or people. It's hard to keep up with the possibilities for new attacks.

When enterprises are operating in geographies and cultures that they have never done business in before, such as new locations for outsourcing or off-shoring, it's a lot harder to predict behaviors or develop possible scenarios. Globalization increases the complexity of risk assessment. It requires factoring in different norms and ethics, which may not be fully understood.

The increasing skill set of the bad guys

It is well-known that countries and corporations use cyberspace to spy on each other for political and commercial gain. Even cyber-warfare has transcended the realm of best-selling novels to become reality. Nation states may believe developing information warfare capabilities is critical, but the downside of this strategy is that not everyone who gains these capabilities stays within the control of the nation state under which they've trained. It's a relatively recent skill set. Over the last 20 years or so, militaries and intelligence agencies all over the world have trained agents in cyber-warfare activities. At some point, some of the people with these skills start leaching out into the criminal economy. This is increasingly putting the global economy at risk.

High levels of risk tolerance

Today's economic conditions are creating an atmosphere in which business people may be much more willing to take on potentially dangerous levels of risk. Many cash-strapped business units are rushing ahead and "leaping before they look," rapidly entering relationships with cloud vendors and/or outsourcers. With the intention of squeezing timelines, decreasing costs, and/or making their quarterly numbers, they may forgo thorough due diligence or comprehensive security reviews. All the while, enterprise data is spinning out of enterprise control.

An added dimension to the problem is that service providers often sub-contract the work or elements of it to other service providers, who then push it off to their own sub-contractors. Ultimately, there can be many layers between the original client and the organization that is actually handling the information.

> "The historic models are insufficient and should not be relied on to predict the future. We are entering unknown information security and risk management territory."
>
> Council Member

Cloud computing is a relatively new concept. According to Forrester Research's glossary, cloud computing is, "a pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption."[16] It creates a new category of service providers and a new set of risks. Because the cost savings are so compelling and it is very easy to start using cloud computing in stealth mode, many businesses may be lured in before all of the security issues have been addressed.

For example, it is now possible for developers to do production scale tests without even having to involve IT. Infrastructure services in the cloud are built on the notion of renting virtualized machines so that infinite capacity is available on very short time scales. The customer can acquire and release resources on demand, and only get charged for what they use. Previously, developers needed to work with IT to configure hundreds of servers for an

architectural experiment which would take several months and a huge capital expenditure to complete. Now developers can use their credit cards to rent cloud services and get the required computing power for $10–$50, and get it all done in one afternoon. Computing power is now very accessible but it is also no longer exclusively under the control of the enterprise.

The newness of cloud services means that enterprise customers have not yet defined all of their security, privacy and compliance requirements and that cloud vendors have not adequately addressed all the related issues; and there are many. Just to name a few: If cloud services are processing data from multiple enterprises, how will the cloud vendors ensure the integrity of co-mingled data? How is it segregated from other customers' data? If a business process moves to the cloud, how does an enterprise meet compliance obligations? How does it meet requirements for detailed security assessments or penetration testing? In addition, cloud vendors are reluctant to reveal the details of their security as they consider it proprietary information. Many of today's privacy regulations mandate where information must be stored or processed. How will customers know the geographic location of their data as it is moves around the globe using available capacity in the cloud? This is all still unclear. But despite this lack of clarity, many enterprises might just decide to take the risk in an effort to tap the enormous cost savings, flexibility and other benefits that cloud computing promises.

Business process outsourcing (BPO) is another area where enterprises might just take the risk. As cost pressures mount, enterprises looking to remain competitive may be forced to follow other enterprises as they move more business processes to service providers and new on-

"Why are the risks increasing? Without a doubt, it is the pace of change in the environment. You can wake up tomorrow and a risk that wasn't there yesterday is there today. There is no period of development; there is nothing necessarily on the horizon that will let you say, "I can see what's coming."

Dr. Claudia Natanson
Chief Information Security Officer
Diageo

"Business is now inherently on a global scale with the complexity of different cultures and normative behaviors, and the breadth of ethics around the world. In this context, it's a tremendous challenge to ascertain, what's the true risk of doing business as a global enterprise?"

David Kent
Vice President, Security
Genzyme

shore and off-shore locations. Service providers may be able to entice a few Global 1000 customers with extremely low-cost contracts. To make their offerings look attractive, some BPO companies try to present an a la carte menu instead of a full meal deal. Beyond their very low-cost core services, they offer a menu of options, including security controls. The problem is that companies often put together their business case based on the initial sticker price. All the rest is additive cost, including security controls. Blinded by the initial promised savings, customers may accept untested security assurances or forgo the more expensive security "options." The service providers may then use these brand names as proof of the level of trust they have earned to entice other Global 1000 customers.

The significant issue of service provider risk has faced large enterprises for years now; it is not a new concern. The sheer volume of service providers and the increasing number of business areas they touch were already making it very difficult to manage the security, privacy and compliance issues. In the new economy, the proliferating number of service providers and their deep reach into enterprise business processes may be kicked into overdrive.

The shifting moral compass

In desperate times, people do desperate things. In a tough economy, disgruntled and laid-off employees and contractors may be much more willing to pursue malicious acts that are outside the realm of their normal behavior. The reality is that desperation can trigger otherwise law-abiding and rule-following people to engage in criminal activities. For example, according to a recent survey 9 out of 10 IT administrators would take company secrets and remote access credentials with them if they were fired.[17]

Adding to the dangers, security departments are becoming resource-constrained. This environment opens up increased opportunities for people to take advantage of gaps in security. By way of analogy, when you can no longer afford to have a security guard at the door 24/7, people will determine when the guard is not around and target that timeframe to gain entry.

Today's enterprises are operating in an environment with unprecedented levels of uncertainty. This kind of setting may make "Black Swan" events more conceivable. Most security professionals are familiar with so-called Black Swan events, which are defined as large-impact, hard-to-predict, and rare events that go beyond the realm of normal expectations. How do you realistically anticipate these types of events in a risk assessment? In a rapidly-changing world, the value of using historical data to predict possible scenarios, impacts and losses is called into question.

"There is a new dimension now that affects the risk picture. I think we'll see a behavior change in how people do business under high economic pressure when every deal, no matter how small, is an important deal. Business people will be more open and willing to take risks because the pressure on them to reach targets is higher given this economic downturn."

Andreas Wuchner
Head IT Risk Management,
Security & Compliance
Novartis

"What will happen is people will talk in terms of risk acceptance. And essentially they'll move the bar to satisfy whatever they want to spend as opposed to necessarily looking at it from a risk standpoint. I think there will be a very high risk tolerance when they don't want to spend the money on security."

Craig Shumard
Chief Information Security Officer
Cigna Corporation

V. The Need for a New Information Security Paradigm

The current security model is ill-equipped for a hyper-extended enterprise operating in an unprecedented risk environment. Security teams are often still fighting yesterday's battles and focused on tactics like securing the perimeter with firewalls, updating anti-virus signatures, pushing out patches, and encrypting laptops. All of these things may still be necessary, but they are not sufficient to match today's world.

If we do not figure out a better information security model and fast, there could be devastating consequences. The possible worse-case scenarios are actually nothing new to security professionals. They have outlined these types of events for ages. What is new is the likelihood of these kinds of incidents occurring and the magnitude of their potential impact.

For example, on a national security scale – terrorists could take a hold of a country's electricity grid. The number of people capable of doing something like this has increased, as has the number of Internet-enabled devices that make these systems more vulnerable to attack.

Another potential scenario is a major attack for economic gain, such as extortionists threatening to take down a company's entire operations or revealing the personal data of millions of customers. Blackmail and extortion have been realities in the online world for years. While the perpetrators used to target fringe industries such as online gambling and pornography sites located in offshore locations, this is quickly changing. Extortionists are now targeting mainstream businesses. Take for example the situation facing a pharmacy benefits management company in November 2008.[18] The company received a letter with the names and vital information of 75 members. The sender of the note threatened to release millions more if they were not given an undisclosed amount of money.

With more and more enterprises relying on cloud vendors and outsourced service providers, a major outsourcer or cloud vendor going down could result in large-scale disruptions to the business operations of huge numbers of companies. We have already witnessed the fall of a major outsourcer in India. Satyam Computer Services, a huge information technology outsourcing firm based in Hyderabad, India, serves many blue-chip clients. Satyam is currently under investigation after the CEO admitted to a decade of ongoing fraud. In cases such as this, what if the local law enforcement decides to seize operations in order to investigate? What happens to all of the customers' business processes? What happens to their data?

The current risk environment also raises the stakes for security breaches. For example, with social networking, the impact goes well beyond the loss of IP because developers collaborate across company lines. Since it is now commonplace to "twitter" about travel itineraries, criminals can use this information to track down the geographic location of company personnel in order to steal laptops or much worse, kidnap executives. And for the companies that do experience a data breach in today's environment, the consequences could be grave. It's one thing for a company to face regulatory fines, law suits, and loss of share price when it is healthy financially; but if it is unstable financially, it could be entirely wiped out.

In aggregate, if competitive pressures force enterprises across the globe to take on higher levels of operational risk, the level of risk within the entire economy could reach unsustainable levels. Unfortunately, this situation has eerie parallels to the banking industry reaching unsustainable levels of financial risk.

"My concern is that security practitioners will fail to appreciate the singularity that we've approached here. If they don't understand their crucial role of being the risk specialist, the advisors to the management, the wheels could come off globalization and the global internet. At this moment in time, security bears a huge responsibility for the benefits that are possible, that are necessary for the survival and success of their enterprises."

Bill Boni
Corporate Vice President
Information Security and Protection
Motorola

VI. Recommendations for Updating the Information Security Model

Updating the approach to information security, including the management of people, process and technology, is essential to successfully protect information. It must be stressed that it's not all doom and gloom. Information security teams are not starting from scratch; they will be building on all the work they have already done to protect against threats and defend the enterprise.

Also, it is important to remember that most systems are assumed to be running securely most of the time. It is easy to subscribe to a pessimistic view, given the daunting risk environment. But security teams do have the advantage of knowing the architecture of their systems better than any potential attackers.

Especially if the security team has been part of the design and operation of a set of systems, they will be in a strong position to overcome any attempts at subversion.

That being said, during a time of upheaval, it is essential to take a step back to consider where information security is headed. As the terrain dramatically shifts, so must information security. Developing an updated information security model that is better-equipped for the times at hand represents an evolution, but in the current climate time is of the essence. This evolution must progress more rapidly than many in IT history. The following section provides some recommended steps to take for moving forward.

"One of the challenges for security professionals is to be able to make informed triage choices that are necessary when you're dealing with such a fast-paced, dynamic, global set of threats, challenges, risks and domains. So you have to develop this ability."

Bill Boni
Corporate Vice President,
Information security and Protection
Motorola

"At this particular point in time, when we have such a rapidly-changing environment, we need to absolutely cry, "Time out!" We need to step away from it, and we need to examine if our program has all the right gears. Does it have the flexibility it needs? Does it have not only the technological capability, but the resources, the staying power? Is your program road-ready for the rough ride that you may be about to embark on? Because only the most agile, only the fittest, only the most flexible will make it to the end."

Dr. Claudia Natanson
Chief Information Security Officer
Diageo

1. Rein in the protection environment

In the current economic climate, information security programs are resource-constrained. Figure out ways to use resources more efficiently. For example, curtail the use of security resources for protecting extraneous information assets, stored data, and devices. If you can reduce your protection environment, you will not only reduce risk but also free up resources that can be reallocated to high priority projects and/or achieve operational cost savings that can be used for strategic investments.

Asset management

Take a complete inventory of the assets protected by the security department; including who has access to them and how often they are actually used. In most enterprises, there are many systems and applications that are rarely used, yet they are not retired "just in case." Now is the time to get rid of them. It simply costs too much to protect them at this point. Work with the IT group to determine which legacy systems should be retired. Asset management is a net gain for security and IT, since it reduces the number of applications and systems that security is protecting and IT is maintaining.

Also take a close look at data retention. Many enterprises continue to retain data for many years beyond its usefulness or required retention. Storing confidential data for inordinate amounts of time is a security and privacy risk. Find the sensitive data that is being stored for unnecessary periods of time and retire this data. This will reduce the amount of data that the information security team must protect.

Another opportunity to achieve efficiencies is to reduce the number of different desktops, devices and servers that security supports. For example, analyze the variety of desktop configurations that your enterprise supports and reduce it down to a manageable number that meets your business needs. If a user needs e-mail, Word, PowerPoint, and Excel for ninety percent of what they do, it is no longer realistic to provide them with that extra special application that is used just once a year. Security departments no longer have the resources to support so many custom desktops. While it may have been difficult to clamp down on customizations in the past when users felt they were entitled to custom desktops or devices, in this economy, it should not be expected given the cost considerations. Cut down the flavors of desktops, devices, and servers that security supports and create a set of solid enterprise standards.

> "Many enterprises don't typically get rid of legacy systems, they hold on to them for no good reason for a hundred years just because somebody might need them. You don't have the luxury anymore of protecting systems that don't get fired up every year. Get rid of them."

Council Member

> "Don't support every server or PDA known to humankind. Cut down the flavors and the colors that you are required to support. You don't have the resources to be able to give everybody their personal customized 'X'."

Council Member

2. Get competitive

For many enterprises, it makes sense to move away from silos of security to centralized shared services which are provided by the information security department to business customers across the enterprise. The degree of centralization and type of services offered by the central department depends on enterprise needs and organizational structure but the idea is that by delivering at least some components of information security as a set of centralized services, it can achieve not only increased efficiencies but also better risk management.

The information security department should strive to offer such competitive services; their customers would not consider looking for other solutions. Being competitive may be a challenge for a lot of core security organizations. Some tend to believe that they are somehow different than other internal services because of their special role in protecting the business. But especially now, security must increase the focus on quality and efficiency of services. As business units examine their costs, they will be expecting the right product at the right price for all internal services. Otherwise, they will seek a better deal by doing it themselves or going directly to an external service provider. It is now a very realistic scenario that a business or division head will be on the plane and read all about some fantastic security service that he can get just by plugging into some cloud. He may come back to the security team and say, "Well, why should I use your centralized security services?" And security has to have a good answer.

Service-oriented program management

Take a service-oriented approach to program management. This forces the information security organization to be much more nimble in responding to the needs of the business. Security must continually "take the pulse" of their market and ensure that their offerings consistently meet the demands of their customers. The portfolio of service offerings might include:

- Risk assessment and compliance management
- Third-party security assessments
- Awareness and training
- Identity and access management (authentication, provisioning, authorization)
- Security hygiene (anti-malware, configuration and patch management)
- Data protection (data loss prevention, encryption, and rights management)
- Network security (perimeter protection, firewall, and IDS)

Looking forward, security services in many enterprises will be delivered by an internal team in conjunction with a tightly-integrated supply chain of vendors and external service providers. This will require the internal team to determine their set of security offerings and then honestly assess their own internal capabilities. They will have to figure out what they as the core security team will do and what will be outsourced to external service providers. Ultimately, it will be a mix of internally and externally-provided services which are provided seamlessly and transparently to customers.

As enterprises use more external service providers for security, the core security team should be involved in carefully managing this growth. Security is in a much better position than any individual business unit to hire external service providers. The security department has the required expertise to assess the service providers' capabilities and performance; and to ensure that all security activities are integrated into the enterprise's overall information risk management program. With a siloed approach to information security, it will be increasingly difficult to assess all of the myriad risks facing enterprises and to manage these risks. In addition, if the core team manages the use of service providers across the enterprise, they can achieve economies of scale and reduce the costs of security to the business units.

Quality service at the right price

Information security must be able to articulate the value of the services they offer to their customers. Help your business customers understand the level of quality you provide for the price. Keep in mind that if the businesses are mandated to use centralized security as their provider, some groups will inevitably find a way to subvert the security program because they think they can do it better. Instead, incentivize the business to use your services by offering quality services for a competitive price.

"Provide centralized shared services that are compelling enough to the business from a cost point of view, from a service levels point of view, from a controls point of view, and everything else, that it would be stupid for the business to do anything else because it's such a compelling case. Not because they have to use it, but because it makes sense for them to use it."

Council Member

"Remember, security is a product. Products today have to be at the right cost to be competitive. So cost is always going to be important, because you're not going to have the comfort of big budgets now. All organizations will be addressing how they can scale down. And the other part is how you deliver that program. So it has to be efficiently and effectively executed."

Dr. Claudia Natanson
Chief Information Security Officer
Diageo

"Just like some of our business partners have really focused on business processing outsourcing to try to reduce their costs and improve the value proposition to their customers, security needs to be able to do the same thing. While there have been some attempts, I don't think that we've even scratched the surface yet as to what we should be looking at potentially. Companies should be able to plug into and leverage repeatable cost effective solutions so that we don't have to continually re-invent things."

Craig Shumard
Chief Information Security Officer
Cigna Corporation

3. Proactively embrace new technology on your terms

Information security departments must accept that it is not feasible to simply say "no" to new and emerging web and communications technologies; rather they have to figure out a way to enable their secure use. Develop a roadmap and set realistic expectations for the business. Understand the risks and devise a plan to mitigate the risks. Also, keep an eye on emerging technologies that are being implemented for other reasons, but may actually help decrease security risks.

Transition plans

Work with the business to create a transition plan for the use of cloud computing. If you haven't already started these plans, get started. It must be emphasized that security professionals need to get involved early and stay involved in the business decision making process. It's too late when you discover your company has already moved into the cloud and then you come along and ask them to put on the brakes. Move from reactive to preventive security.

One possible route is to cherry pick what goes to the external cloud first, i.e., the processing of non-sensitive or non-regulated data. Some companies that are using the external or "public" cloud to manage sensitive data have taken the approach of de-identifying the information first. Once it is "anonymized", then it can be sent for processing in the cloud.

Many enterprises are large enough to develop their own "private cloud," which uses the same technology as public cloud services without sharing computing resources between multiple enterprises. Instead, they are dedicated to one enterprise and managed by that enterprise. This approach provides the benefits of consolidated, scalable and flexible computing power while alleviating many of the security and privacy issues of having a third-party entity process enterprise data. Information security can work with IT and the business to ensure that the enterprise's private cloud is secure.

To support the use of cloud computing, you won't necessarily need an entirely new technology platform; it may be possible to use your existing security infrastructure in new ways. For example, investigate using a Federated Identity Management gateway to authenticate to cloud services. Design it so that the cloud vendor only accepts authenticated traffic from the enterprise. For cloud vendors providing infrastructure services, work with them to determine if it is possible to send audit logs for your applications in the cloud to your enterprise security information and event management (SIEM) infrastructure for analysis, so you control the audit logging for your applications in the cloud.

Another technology that must be planned for is social networking. Security can't just block the use of social networking sites anymore. The benefits, including low-cost ways to recruit employees, distribute marketing materials and enable employee networking, are simply too great. Figure out how to allow the use of social media at least for certain applications without putting the company at risk. You may also want to investigate the use of tools designed specifically to allow enterprises to use consumer sites securely or work with IT and the business to bring in business-specific social software.

First and foremost, you'll have to attempt the development of an Acceptable Use Policy (AUP). Put emphasis on user education and training; this is the key to securing information when it comes to social networking. Help employees understand the risks and the rationale behind the policy; and institute a way to monitor the activity. Not that this is going to be easy. Balancing social networking's benefits with educating participants on what and where they should and should not post and what they can and cannot post is going to be incredibly challenging – particularly as people mix their use of social networking sites for personal and business purposes.

"There's a lot of complacency in large companies. You do it this way because you've always done it this way. Well, how do you sort of obsolete the technology you're using now, before somebody else does?"

Council Member

Security benefits of emerging IT

Security practitioners need to be better versed in general technology issues, in order to understand how developments in IT can deliver significant security benefits. One such area is virtual desktops, which are a growing trend in most enterprises today.

With this technology, fundamentally the desktop is an image of a full desktop that actually sits in a virtual machine in a data center somewhere. The concept is to stream applications to the desktop, rather than have a dedicated copy on it. Therefore, when the user logs in, they're not logging into their own desktop, they're logging into something that is immediately built for them on the fly. The drivers to move to virtual desktops are mostly cost, efficiency, and flexibility, but there are security bonuses as well.

First of all, you will no longer need to manage the "gold build" on everyone's machine. Instead, you will make changes on the back-end. The end result is that you can react a lot more quickly when changes are needed. It is a lot tighter and easier to control because for example, you don't have 200,000 desktops; you have 200,000 instances of one desktop. Instead of pushing patches to 200,000 physical desktops that need to be rebooted, you send it to 200,000 VMs in a bank of servers somewhere. Since data is stored on a file share as opposed to on the desktop or laptop, you need not worry about encrypting data on the machine. If somebody steals it, there's no data on it. From a recovery point of view, if the enterprise needs to evacuate the building (due to a gas leak or other event), users don't need to take their machines with them. If they have access to a PC, they can get to their virtual desktop. When they log in remotely from a non enterprise-owned PC, the remote machine can be checked to make sure it has the right controls on it.

"Security officers have to be out there explaining to other executives and senior people in the company how they're going to approach the move to the cloud, and the risks associated with moving faster than they're able. And if the business wants to move faster, you better have an answer about what resources you'll need to get it done faster, because if the business asks you "Well, how we can get it done faster?" and you say, "I don't know", you're going to be a former CISO."

Roland Cloutier
Vice President, Chief Security Officer
EMC Corporation

4. Shift from protecting the container to protecting the data

More and more, enterprise data is processed and stored in containers not controlled by the enterprise. For instance, the data may be processed by service provider facilities or held in a PDA used by an individual employee or in a laptop used by a contractor with multiple enterprise clients. Therefore, security needs to shift the focus from protecting the container to protecting the data.

For example, in the old model, enterprises would give a contractor a corporate standard laptop in order to do his or her job, something which is both expensive and which leaves the contractor (assuming s/he has multiple relationships) with multiple devices. The new model would let the contractor use their own device and secure the data. This would require finding a way to partition the device and define a trusted component. The simplest approach today is to push out a virtual machine. It's not the most secure and there needs to be advances in technology which provide better methods but it's a good stop-gap for the moment.

Rights management is another example of an up-and-coming technology that focuses on protecting the data versus the container. One such vision is "digital XML paper." The emergent model uses metadata to define the data's origin, attributes, level of trust, ownership, where it resides, where it can go, who can access it, the lifetime and appropriate protections, etc. In other words, the digital xml paper would contain the security requirements and applications would enforce those requirements. To demonstrate using a simplified example, think of a situation where a contractor is working for a company. While he works for this company, he uses their digital xml paper, which is tagged with that company's security requirements. Anything created with this digital xml paper is tagged as the company's and gets protected in accordance with their rules. Once the project is over, all the xml paper gets recalled back to the owner and it expires.

"The security model is moving to protecting the content not the container, because increasingly the container is not owned by the enterprise. The data is being processed by another enterprise or held in a device used by an individual for their own personal use."

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

"Consumerization will force enterprises to allow people to bring in their own devices. From the security point of view, you need to be able to focus completely on the data elements and not care about the kind of device or if it's internal or external or whatever. I'm not saying that all the solutions are here already today and that they're easy to solve, but we have to focus on the data."

Andreas Wuchner
Head IT Risk Management,
Security & Compliance
Novartis

5. Adopt advanced security monitoring techniques

Updated approaches to monitoring for abnormal and malicious events must move away from concepts such as signature-based anti-virus and blacklisting and move towards more accurate techniques such as behavior-based monitoring and whitelisting.

The most common approach to malware detection is signature-based, which has major disadvantages. It identifies malware by detecting malicious byte code patterns – malware signatures. A program is scanned and compared to a database of known malware signatures. If a program contains a pattern that exists within the database, it is deemed malicious. This approach cannot detect unknown malware and is susceptible to evasion. Rather than looking for signatures, behavior-based approaches typically monitor the stream of system calls that the program issues to the operating system. Since behavior-based monitoring looks at what a program does rather than at specific patterns in the code, this approach is not susceptible to the shortcomings of signature-based detection.

Behavior-based monitoring can also be applied to databank monitoring, looking for abnormal patterns of activity. For example, these tools are able to detect when SQL injection attacks are happening or when people are trying to use elevated privileges from unusual locations. The behavior-based monitoring system is put between the application and the database. If the application gets manipulated in an unusual way, the instructions to the database will look abnormal.

While blacklisting blocks access to known malicious sites or software, whitelisting allows access to sites or software considered safe, blocking all others. For examples, whitelisting can be used to manage software installed on a computer. By whitelisting software, the security organization would only permit approved software to install and run. If a software product is not explicitly on the list, it is not allowed. Keep in mind that while whitelisting is a potentially promising way to protect computers, it can create a very rigid environment where rules about what software can be downloaded are too restrictive, creating a frustrating user experience.

6. Collaborate to create industry standards

There have been discussions for years about the need for more standards in information security. However we have reached a critical point where the lack of uniform standards is simply not sustainable. Without standards, enterprises will not be able to truly evaluate security professionals, manage third party risk nor reap the full benefits of new technologies such as cloud computing.

Professional accreditation of security professionals

Many in the information security field think it's time to mature as a profession and begin to accredit security professionals in similar way to the accreditation of engineers. For example, when an engineer provides a piece of steel that they've worked on, the receiving engineer knows that it's come from an individual with a rigorously defined level of capability. A similar approach in the security industry would ensure a more accurate evaluation of skills.

Currently many security professionals acquire the Certified Information Systems Security Professional (CISSP) or other designation. Professional accreditation would take this up a level and involve two-tiers of assessments. First,

> "There is now a recognition that information security has become too important a subject to allow someone to read a book and then carry out the work. This is especially a growing view in the UK and emerging throughout Europe. Professional accreditation would ensure that security knowledge and capability meets an accepted standard and skills can be cross-recognized."
>
> Dr. Paul Dorey, Former Vice President, Digital Security and Chief Information Security Officer, BP; and Director, CSO Confidential

sufficient knowledge would be acquired and examined through for example, the CISSP exam. The second tier would be gained after in-job experience and consist of a competency assessment by peer review, similar to medical or engineering professional qualifications. This actually tests through independent assessment interview that a security professional has the ability to apply theoretical security knowledge in practice. This model is already working in the UK with the Institute of Information Security Professionals (www.instisp.org) accrediting professionals in both the public and private sectors. Stepping up as security leaders also recognizes that the successful professional is expected to perform as a business leader as much as a specialist and much broader skills will be required of the leaders of the future.

Standards for third-party assessments

In an environment where the demand for cloud services and BPO is escalating, the level of effort required to assess service providers is already reaching the breaking point. Adding more budget for additional assessments is simply not going to be sustainable. Ongoing assessments and on-site audits are labor intensive and costly for both enterprise security departments and the service providers.

Information security professionals must work across enterprises to create standards to enable third-parties to conduct assessments. But traditional tools such as the SAS70 audit process do not contain consistent measurement standards that can be widely adopted.

However, this is changing and a variety of potential approaches are promising. For example, the BITS Shared Assessments Program provides third-party assessors with a set of standardized best practices for evaluating service providers. It originated from the financial industry, but could be leveraged by other industries. The BITS program allows a service provider to present the third-party assessment of their systems to their clients in lieu of an on-site audit or more often, it enables a reduction of scope of the on-site audit. ISO 27001:2005 certification may also be part of the answer. It would require enterprise security officers to accept certification to the ISO standard as proof of sound security practices. Whatever method or methods are agreed to, security practitioners need to define a much more standard way of assessing the security of service providers.

> "You have to have a 360 degree view of risk over the extended enterprise and all the elements that are critical to your core business's success. This is where things are headed. As companies start to cooperate on these things, you may even see certification efforts like you're seeing between some governments now, around Customs programs, where if you have a certain certification, you get fast-laned."

David Kent
Vice President, Security
Genzyme

Interoperability standards

Cloud computing creates the need for interoperability standards, since one enterprise will want to be able to interact with many different cloud vendors. As one of many clients, one enterprise won’t be able to insist that the cloud vendor provide customized security controls. Rather, the enterprise will have to ensure that the cloud vendor meets the standard for controls.

Without standards, enterprises are faced with the prospect of having to interact differently with each one of their cloud vendors based on a diverse set of proprietary standards. It creates a possible scenario in which the end-user would need multiple trust-brokering agents on their devices to exchange information with multiple cloud vendors. For example, an enterprise might need to load 100 agents on one machine to talk to 100 relevant service providers in a trusted way. With multiple incompatible models, instead of one open cloud, there will be multiple closed clouds and the industry will have lost the potential benefits offered by the cloud. It is in everyone’s best interest to create these standards and doing so will require the cooperation of the clients as well as all of the cloud vendors. Security practitioners need to actively engage in the creation of these standards now before it is too late.

7. Share risk intelligence

Enterprises will not be able to defend against international attackers and the fraudster ecosystem without cooperating with other enterprises, law enforcement, and government. There is now a premium on the value of threat and risk intelligence. Working together is essential for developing enhanced intelligence capabilities so there is more information about who the fraudsters/attackers are and what they are planning. For example, working with industry experts and government bodies to get operatives to go undercover in fraudster chat rooms has been proven to be valuable in some cases.

In addition, enterprises need more robust systems for sharing information whereby they can periodically review incidents, describe exploited vulnerabilities, or name perpetrators so other enterprises can avoid hiring specific people, protect resources and assets as needed, and plan mitigation while simultaneously learning from one another's experiences. Various governments and industry associations have worked to create and sponsor information exchanges. For example, the Information Sharing and Analysis Centers have been set up to establish and maintain a framework for interaction on cyber and physical security issues between and among private and public sector organizations in North America.

In general though, information sharing is still inhibited by liability issues, privacy concerns, and competitive fears. Security officers are often advised by their general counsels to not share valuable information with other enterprises because doing so might cause their enterprise to be subject to discovery in the case of a lawsuit. Therefore, information sharing vehicles are less effective than they could be. This will need to change.

Finally, organizing an information sharing network requires resources, time, and money, not to mention an ongoing commitment by some or all parties to maintain and update this central hub. In some cases, relying on stable and large third-party vendors for such work enables enterprises to both support and gain from such infrastructure without having to bother with the overhead typically associated with such projects.

"We need to develop an intelligence capability so we know what's coming, and we can prevent things from happening in the first place. We need to be able to figure out what these guys are going to do and then try to stop it. It means moving to a more preventative security model and being able to share information with each other."

Dave Cullinane
Chief Information Security Officer
and Vice President, eBay Marketplaces

VI. Conclusion

Working towards a new information security paradigm will enable the "hyper-extended" enterprise to operate securely and successfully in the current environment. If we achieve this goal, the enterprise will reap the rewards of globalization and technology even in the face of unprecedented risk and severe economic conditions. A strategic approach to information security will better equip organizations to deal with the constant evolution of technology and escalating pace of change. In addition, increased collaboration between enterprises will help build a stronger global business community.

> "Security is no longer optional because the operating models companies are working towards actually need security to sustain them. Whereas in the past, in some cases, there was a level of "optionality". If you're running something in a locked data center that's not got any wires out of it you can arguably say you don't need any IT security and you can do it all with a key. But the more you decentralize and the more you open up into public environments, the more it's the security that gives you the level of certainty and integrity that you need in order to operate."
>
> Dr. Paul Dorey
> Former Vice President, Digital Security and
> Chief Information Security Officer, BP; and
> Director, CSO Confidential

Appendix. Security for Business Innovation Council Members' Biographies

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

Anish has global responsibility for ensuring the security and resiliency of JP Morgan Chase's IT infrastructure. He supports the Corporate Risk Management program and participates in the firm-wide technology governance board. Anish was selected Information Security Executive of the Year for 2008 by the Executive Alliance and named to Bank Technology News' "Top Innovators of 2008" list. Previously, Anish was a senior member of the Enterprise Resilience practice in Booz Allen Hamilton and SVP and CTO of Global Integrity Corporation (an SAIC Company) and Predictive Systems. Anish has written and spoken widely on information security. He is the co-author of Internet Security for Business, is a U.S. patent holder, and 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 Marketplaces

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 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.

References

1 "Clouds and Beyond: Positioning for the Next 20 Years in Enterprise IT", Doc # DR 2009_GS5_FG, IDC, February 2009

2 "Clouds and Beyond: Positioning for the Next 20 Years in Enterprise IT", Doc # DR 2009_GS5_FG, IDC, February 2009

3 "Is virtualization adoption recession proof?" *Network World*, February 5, 2009

4 "Breaking: Facebook Surpassed 175 Million Users, Growing By 480,000 Users a Day," *All Facebook*, February 13th, 2009

5 "Technology Predictions: TMT Trends 2009," Deloitte, January 2009

6 "Gartner Says Enterprise Mobile Phones Will Replace Desktop Phones in North America by 2011", Gartner Press Release, February 4, 2009

7 "Trust Digital Solidifies Position as Enterprise Mobility Management Leader in 2008", *BNET,* February 10, 2009

8 "Skype Growing by 380,000 Users a Day" *PC World*, February 10. 2009

9 "Outsourcing Predictions for 2009", *ZDNet*, December 31, 2008

10 "Recession set to boost outsourcing", *InfoWorld*, October 29, 2008

11 "Down economy fuels IT outsourcing" *Network World*, February 13, 2009

12 "Exploring Global Frontiers: The New Emerging Destinations," KPMG, February 2009

13 Sophos 2009 Threat report

14 Security Now Blog, Blue Ridge Network, August 22, 2008

15 Security Now Blog, Blue Ridge Network, August 22, 2008

16 Forrester Glossary http://www.forrester.com/ER/Glossary

17 "Security Survey Reveals Exiting Employees Have The Power: IT Savvy Employees Likely to Steal Company Data Before They Leave" CyberArk press release, August 2008

18 "Data Breach Used in Attempted Extortion", *IT Business edge*, November 7, 2008

RSA

The Security Division of EMC

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

©2009 RSA Security Inc. All Rights Reserved.
RSA, RSA Security and the RSA logo are either 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 and services mentioned are trademarks of their respective companies.