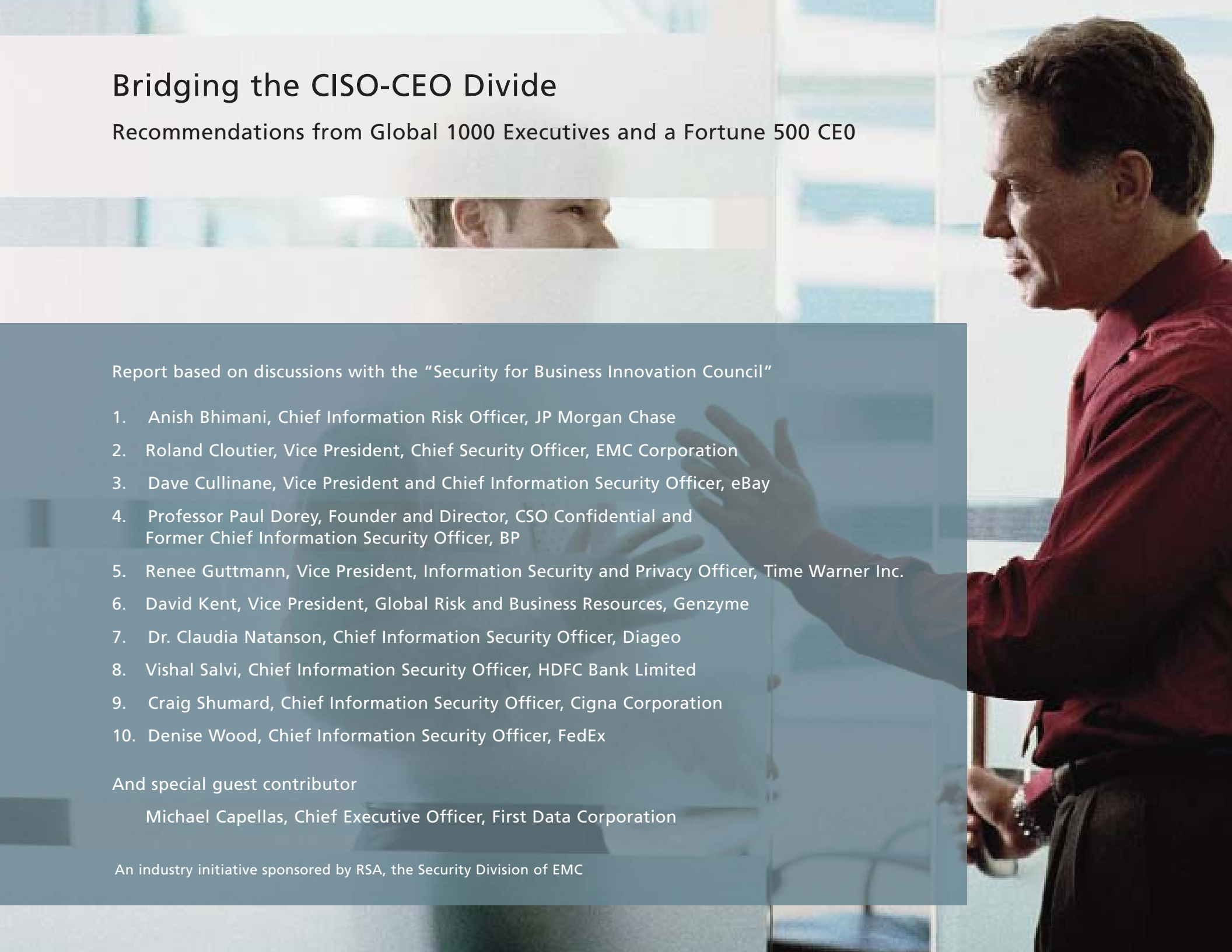
Bridging the CISO-CEO Divide

Recommendations from Global 1000 Executives and a Fortune 500 CE0



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

1. Anish Bhimani, Chief Information Risk Officer, JP Morgan Chase
2. Roland Cloutier, Vice President, Chief Security Officer, EMC Corporation
3. Dave Cullinane, Vice President and Chief Information Security Officer, eBay
4. Professor Paul Dorey, Founder and Director, CSO Confidential and Former Chief Information Security Officer, BP
5. Renee Guttmann, Vice President, Information Security and Privacy Officer, Time Warner Inc.
6. David Kent, Vice President, Global Risk and Business Resources, Genzyme
7. Dr. Claudia Natanson, Chief Information Security Officer, Diageo
8. Vishal Salvi, Chief Information Security Officer, HDFC Bank Limited
9. Craig Shumard, Chief Information Security Officer, Cigna Corporation
10. Denise Wood, Chief Information Security Officer, FedEx

And special guest contributor

Michael Capellas, Chief Executive Officer, First Data Corporation

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 the organization could be put 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

Introduction

Will 2010 be the year that information security comes of age? There are signs that information security, previously viewed as a necessary evil or inconvenient afterthought of corporate strategy, is becoming core to organizational success. And this central role is recognized not only within the ranks of information security but also by senior executives across global organizations. In the recent "Global State of Information Security 2010" study, 52 percent of C-levels reported that the increased risk environment created by the economic downturn has elevated the role and importance of the security function.[1]

The elevation of information security represents a critical opportunity and responsibility for information security leadership. Now more than ever, security professionals must demonstrate expertise in aligning with the highest priorities of their organizations. To do that they must effectively convince the Chief Executive Officer (CEO) that security must be a core component of business strategy. After all, it's the CEO who owns the business strategy; he/she sets the agenda and establishes the objectives for the entire corporation. Therefore for information security to be strategic, the CEO must see the link between his/her objectives and the protection of information assets.

Given current economic conditions, a key focus of most CEO agendas is the drive towards cost reductions and operational efficiencies to strengthen the overall balance sheet and profitability. Corporate leaders today are beginning to see encouraging trends toward recovery though. The NYSE Euronext 2010 CEO Report indicates that nearly half of CEOs think

Security for Business Innovation Report Series

The Time is Now: Making Information Security Strategic to Business Innovation
Recommendations from Global 1000 Executives

Mastering the Risk/Reward Equation: Optimizing Information Risks While Maximiz ing Business Innovation Rewards
Recommendations from Global 1000 Executives

Driving Fast and Forward: Managing Information Security for Strategic Advantage in a Tough Economy
Recommendations from Global 1000 Executives

Charting the Path: Enabling the "Hyper-Extended" Enterprise in the Face of Unprecedented Risk
Recommendations from Global 1000 Executives

www.rsa.com/securityforinnovation

the U.S. economy will have fully recovered by the end of 2010, with the global economy recovering by the end of 2011. However, the vast majority of CEOs believe it will be a weak and patchy recovery, and their intention is to continue to run tight ships even as the economy improves.[2]

The reality is that there is a strong link between current CEO priorities and information security strategy. Many of the measures organizations are adopting to manage cost and efficiency are both innovative and risky. Chief among them is accelerated adoption of new technologies and global business models. Putting customer data, intellectual property, or proprietary corporate information into new IT environments; and sharing information with more and more third-parties spread out across the globe creates risks. Organizations also face an increasingly risky socio-economic environment, as insider threats and external attackers are more motivated and capable of targeting enterprise information assets.

The aggressive business goals and heightened risk environment facing the enterprise today puts the information security officer in a crucial postion: making sure the company takes the right risks in the right ways. The right information security strategy can not only help meet cost-savings and efficiency goals in the near-term, but it can also help position the company for recovery and strong business performance in the long term. The prerequisite for taking on this crucial role is that the security leader must have the confidence of the CEO.

This fifth report in the "Security for Business Innovation" series explores the link between CEO priorities and information security strategy, examining how a divide between an organization's CEO and its security officer can detrimentally impact its risk profile and ultimate business success.

This report takes a very practical approach. It provides ten important techniques for gaining and maintaining the support of the CEO (and other C-suite executives and the Board) for a strategic information security effort. It then analyzes the flip-side; taking a candid look at potential missteps and mistakes, and offers ten tips for what not to do when dealing with your CEO. The last section is intended as food for thought for the CEOs themselves; showing how their lack of support for strategic information security could put their companies at risk.

The guidance in this report was derived from conversations with a group of top security leaders from the Global 1000. As a special feature, the report includes contributions from a Fortune 500 CEO, who as the leader of the largest payment card processing company in the world, is no stranger to risk. The stakes are high, information security is taking center stage and your performance could mean the difference between a future where information security takes a leading role or is relegated to a bit part within the organization.

"Understand that for the CEO, everything is about balance. A CISO has to demonstrate a sense of balance; the ability to weigh risk and return. Then the company will be putting the appropriate resources towards security. It's a trade-off between risk and return."

Michael D. Capellas
Chairman & Chief Executive Officer
First Data

"Every day CEOs must assume the role of risk-takers. This is one component that defines a good CEO. What risks should he take on behalf of the company in order to grow it? The CISO must be able to contribute to the wider risk discussion and help the company take the right risks."

Claudia Natanson
Chief Information Security Officer
Diageo

"One of the main things in maintaining credibility with your CEO is you have to be heavily steeped in reality."

Denise Wood
Chief Information Security Officer
FedEx

The Perspective of a CEO who "Gets It"

Michael Capellas is a Chief Executive Officer who "gets it." A 30-year veteran of the IT industry, Michael is a recognized global thought leader in the technology space, with significant expertise in information security. He has long understood the value of protecting information, not only as a strategic imperative in corporate environments, but also for the United States as a nation. Michael has served on two separate Presidential Advisory Councils on National Security.

As CEO of First Data, Michael currently leads a company where information security is central to the business. As the global technology leader in information commerce, First Data helps businesses, such as merchants and financial institutions, safely and efficiently process customer transactions and understand the information related to those transactions. The company securely processes transactions for millions of merchant locations and thousands of card issuers in 36 countries.

Michael has also had the experience of leading companies where information security was not a core competency, yet he made it a key aspect of the organizational strategy. For example, as the CEO of Compaq, Michael worked to develop a secure technological infrastructure for numerous governmental agencies as well as the New York Stock Exchange. As CEO of MCI, Michael worked to develop resilient telecommunications infrastructures that supported the federal government, the automobile industry and financial services. He also established a focused security practice within MCI to serve the enterprise market.

Earlier this year, Michael addressed over 100 security and privacy executives at the RSA Conference Executive Security Action Forum (ESAF), a gathering that hosts the largest global enterprises and government agencies in the world. Michael's talk at the event was the single most highly rated session ever at an ESAF event. His unique perspective as a CEO with a deep understanding and commitment to information security provided invaluable insight for the group on how to focus the C-suite on the value of information security.

This report brings his unique perspective together with the views of some of the most successful security executives in the world; and offers tangible recommendations for security professionals at this time of unprecedented opportunity and challenge.

> "You have to be able to understand risk analysis as the premise. That's where you start. This is about risk. The language of business is about risk. And if you sit in a CISO position and you can't meaningfully talk about measures of risk and layers of risk, you're probably not going to be successful. You can spend all your money having the latest virus protection put on your PCs and miss the fact that you've got massive enterprise risk because of vulnerabilities to the power infrastructure or legal liabilities of doing business in certain countries."
>
> Michael D. Capellas
> Chairman & Chief Executive Officer
> First Data

State of Affairs: How CEOs View Information Security

Convincing a CEO that information security should be strategic starts by knowing where he/she currently stands. The CEO's view will depend on the vertical industry, regulatory regime and intellectual property – does the company have market, legal or competitive reasons to protect information? It will also depend on third-party relationships and global reach – how much and with whom does the company exchange information?

Overall, CEOs tend to think more about information security issues today than they did in the past simply because most enterprises today rely heavily on IT to support business operations. And most CEOs use the web and mobile communications themselves in the course of their daily work and lives. By now, many have also had direct or indirect experience with a security incident or identity theft. The awareness level of CEOs has also risen because of increased regulation – government and industry mandates for data protection and the high-profile media coverage of massive data breaches, especially in the business press. Information security is now squarely on the CEO's radar screen.

Most CEOs today will acknowledge how important it is to have an information security strategy. In a recent survey of CEOs, 87 percent rated "developing a data protection strategy for the organization" as important or very important.[3] However the same survey shows that although they see it as important, CEOs may not have a realistic picture of information security yet. 77 percent of CEOs surveyed view the greatest risk to data as lost/stolen laptops or incorrect disposal of storage media.[4] This is in contrast to a recent SANS Institute report on the top cyber security risks. The study found that attacks on Web applications and targeted phishing attacks currently carry the greatest potential for damage.[5]

Not only do CEOs seem to misunderstand the risks, they tend to underestimate them compared to other executives. For instance, the majority of CEOs surveyed (68 percent) believe hackers try to access corporate data rarely, or at most once a week. While those in other executive positions believe that their company's data is under attack on a daily or even hourly basis (53 percent).[6]

Of course CEOs cannot be expected to be information security experts; that's why they have security officers. It is up to the information security officer to help the CEO build a realistic understanding of the risks. But the CEO can and should be expected to provide authoritative support for information security.

So how supportive are CEOs today? There are encouraging signs. One sign is that more companies are beginning to address information security governance by putting in place more formalized enterprise risk programs which include information risk management. Recent research indicates that 35 percent of companies surveyed conduct enterprise risk assessments twice per year; and 33 percent continuously prioritize information assets according to their risk level.[7] In addition, Board-level and company-wide enterprise risk councils that incorporate information risks in the overall risk management effort are emerging in many industries.

Another positive sign is the increase in the frequency of reporting to the CEO, other C-level executives and the Board on information security. When information security feeds into ongoing business reporting, it is more integrated with the business strategy and more likely to get the right level of funding. In the financial sector, which tends to be on the leading edge, nearly half of companies now have regular reporting to the CEO on information security on a monthly or quarterly basis (39 percent); or once or twice per year (10 percent).[8]

So it is clear that CEOs are increasingly aware of information security issues; and they have started to establish formalized support structures. At this point it's up to information security officers to better educate CEOs about the real risk picture and build on the momentum to position information security as a strategic business endeavor.

"There is no question that the issue of cyber security has become highly escalated in the last two years. The awareness is coming from several places. It's being driven by the head of audit departments of large public firms. It's being played out at the Board level. It's risen with the extent of globalization and the rapid adoption of the internet and technology. And there have been some pretty well known cases which have hit the press. So there are lots of reasons that it is top-of-mind now with virtually every CEO."

Michael D. Capellas
Chairman & Chief Executive Officer
First Data

Top Ten Ways to Make the Case to Your CEO

Here are ten key techniques to keep in mind as you strive to convince your CEO and other executive leaders that information security has an important role to play in the business strategy. It's not a comprehensive plan; but a list of some of the most important things to consider.

1. Earn a strategic position

Don't expect the CEO to just hand you a strategic position, you have to earn it. Demonstrate that you have an understanding of the business and you'll build credibility. Organizational management skills are also essential. Information security is never going to be completely centralized because it sits across the organization; CISOs need to be able to work in a matrix environment and across organizational lines. Also, recognize that formality matters in this job. If you're reporting to the C-levels or the Board – don't just give verbal updates – make presentations in a formalized, standardized and consistent way.

2. Establish security champions within the CEO's circle of trust

To engage the CEO, you'll need to win over those who influence and interact with him/her on a regular basis – the Board and C-level direct reports. In some organizations, the Board may be savvier regarding information security than the CEO. Board members tend to focus on big picture risk concerns and fiduciary responsibilities, and they bring perspectives from their broader experience in other companies. Impress them with your strategic vision for managing information risks and they will influence the CEO. Typically it will be the C-levels and/or business unit executives who will need to be convinced to fund information security initiatives. Be cognizant that they have to reconcile their responsibility to protect information with their goals of managing budgets and reducing costs. Securing funding at the operational level requires proving that your program makes the best possible tradeoffs between security and cost. If you build strong allies with the C-levels, they will represent you at the CEO's table.

"Being a great Chief Information Security Officer requires interpersonal skills. The CISO cannot just be a technical person. You have to have the skills to be able to relate to people right across the organization and have enough business savvy to communicate to senior people in a way they'll understand."

Michael D. Capellas
Chairman & Chief Executive Officer
First Data

"Data drives the quantification of risk and there is analysis and logic to be applied. Ideally you should be able to say, "Here's what could happen – a security lapse – here is the cause, here are the operational effects, here's a quantification of what it would cost us, and here's some alternatives that we have for preventing it."

Michael D. Capellas
Chairman & Chief Executive Officer
First Data

3. Make security relevant

Know the CEO's strategic agenda and how that maps to specific business goals – then contribute to realizing them. For example, if a CEO is focused on costs, each business area will have cost-reducing goals. In marketing, they could be aiming to reach new markets more cost-effectively by partnering with social networking sites; security could help protect the customer data collected so that the investment is not jeopardized and customer trust is maintained. HR might be looking to decrease the costs of on-boarding and off-boarding contract workers; with optimized identity management, security could help achieve this. In accounting, they may be working on reducing compliance costs; security could help drive down the hours spent on managing access to data and on conducting audits. Part of the customer strategy may be to make service more efficient; security could help reduce phone service by enabling more data to be safely accessible on-line. It will be an education process to help the CEO and other executives understand how security is relevant to their specific objectives.

4. Show him (her) the money

The business exists to generate a profit and ultimately, this is what the CEO wants to see. To gain support for your information security program, be able to calculate how it improves the bottom line – by enabling the company to make or save money.

For example, a recent study by the Aberdeen Group revealed top performing companies that have adopted cloud computing have reduced IT costs 18 percent and data center power consumption by 16 percent. The study also showed that in order to get the benefits of cloud computing, top companies realized they had to establish a governance model around Services Oriented Architectures and cloud-based service delivery. Best practices included a formal cloud evaluation process for monitoring cloud applications as well as formal training for the cloud team.[9]

In other words, the report showed that cloud computing enabled by an information risk management program can achieve measurable and meaningful cost-savings for the company.

Another way information risk management can enable cost savings is through better vendor management. Companies are engaging in global sourcing, business partnerships and strategic vendor relationships to bring down costs. In forming these relationships, companies must assess and mitigate the risk posed by third parties having access to their data or network. Due diligence efforts can be challenging and costly. A study by the Information Risk Executive Council (IREC) found that companies with leading information risk programs can reduce their third-party risk management budget by up to 64 percent.[10]

5. Dispel media hype

The CEO, other C-level executives and the Board get much of their information about security risks through the media. Although media coverage helps raise awareness of information security, it is often a distorted picture. Leadership can end up focusing on the wrong things, such as cyber terrorism or laptop theft – which may not represent the highest priority risks. The CISO's role is to break any misconceptions, actively educate the CEO, C-levels and the Board and help them make more informed risk decisions.

For example, every time there is a major news story on information security, one that you know will get their wheels turning and asking, "What ifs?", provide an email before they even start asking you these questions. Give a brief analysis and relate it to your own company's

"Whether it's to a C-level or a Board member, talk about alignment to the strategies of the company – global expansion and global collaboration – and how you enable that to happen; how protecting resources and trade secrets is a competitive advantage. Talk about being a trusted partner to your customers and how your security program becomes a reason for people to do business with you."

Roland Cloutier
Vice President, Chief Security Officer
EMC Corporation

situation. If information security is represented on an Enterprise Risk Management Committee, this is also a good vehicle for effectively disseminating more accurate information about your company's risk profile to executive leaders.

6. Make it real

To help the CEO and executive leaders understand the risk, make it real. As much as possible, quantify the risks. Don't just give vague explanations of high, medium or low risk events. Instead describe detailed and realistic scenarios for your company, with actual numbers for probabilities, impact and financial losses – in the context of your organization's market position, vertical industry and regulatory regime. Admittedly, since information security is still in its early days, coming up with numbers is not easy, there's no handy "actuarial table." But numbers are what will make it real for business leaders.

Research incidents that have occurred at other organizations but make sure to present that data in the context of your company. For example, estimate how much it could cost your company if you had a data breach exposing card holder data protected under PCI. Or explain what a Denial-of-Service attack could mean, and how much money your company could lose if your e-commerce site were down for a day. Work in partnership with others such as the VP Marketing and General Counsel to derive these numbers and when you present them, have the partners there backing you up.

Also, detail a framework for evaluating risk and making risk decisions. Conversations about risk invariably come down to who has the authority to make what level of risk decision. Having a formalized risk assumption model for information risks brings clarity and transparency to the process and delineates where and with whom risk decision responsibilities lie.

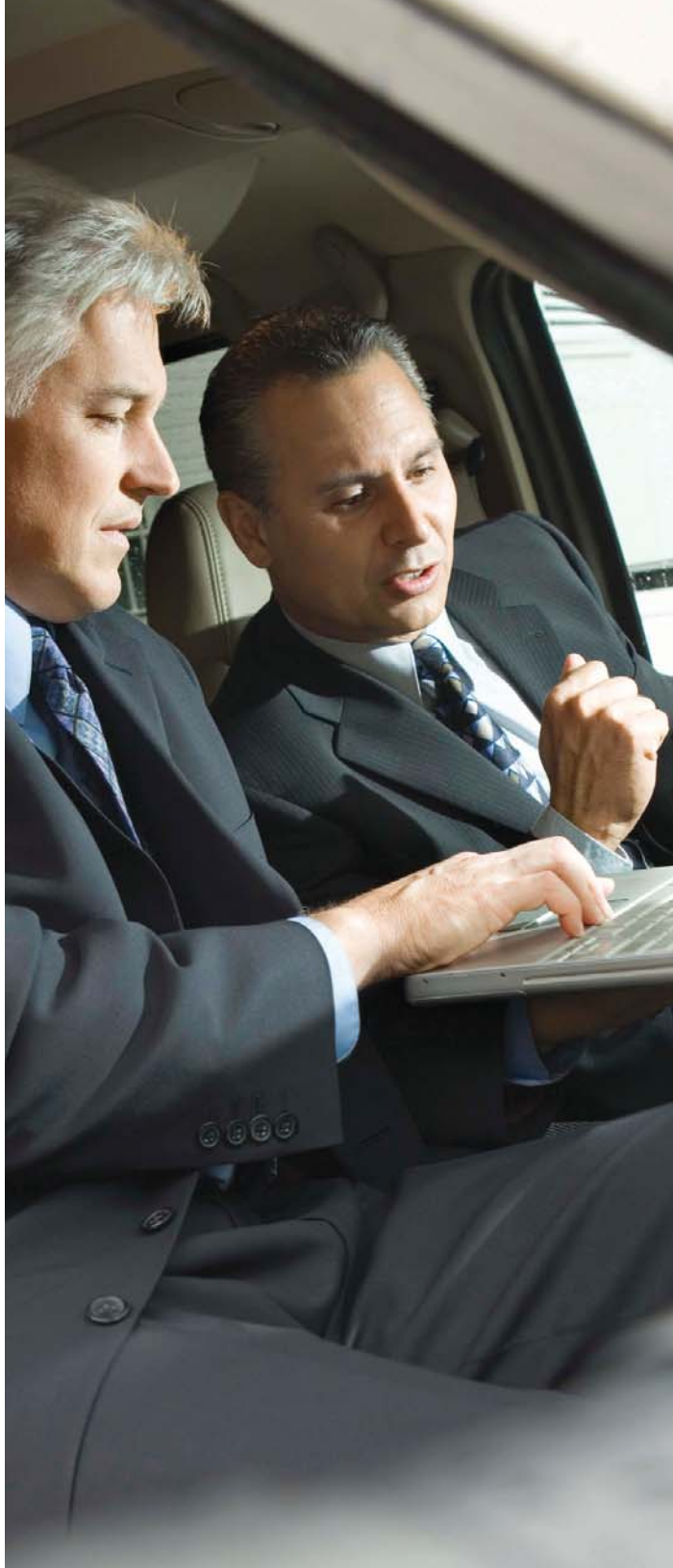
7. Develop good metrics

Good metrics accurately measure the value of information security investments; and they show how the security program manages risks to acceptable levels to meet business goals. Communicate the trade-offs between investment and risk by using visual diagrams that clearly depict the effects (benefits vs. costs) of various investment scenarios. For example, show how risk decreases if the information security program contains certain elements and how it increases if the company forgoes those elements for now.

Get data about how your program compares to other similar organizations. External comparisons and benchmarking establish credibility for the security program and provide evidence of "commercially reasonable" practices. To get this data, security officers need to actively participate in peer groups and forums for information sharing.

8. Set up a clear organizational structure

The security organization should have an absolutely crystal clear organizational



structure. Whether it's centralized, de-centralized, based on lines of business, or functional, etc., it must be clearly articulated, socialized and institutionalized across the whole enterprise. The biggest weakness for security practitioners is organizational management. In other functional areas, the policies, hierarchies and roles are well-defined and well-understood by those outside the functional areas. For example, people "get" what departments like accounting and finance do because their function has been institutionalized. This is how it should be for security as well. This will help security develop better working relationships throughout the organization.

"It's an amazing process. Once you establish your value with a business unit, they'll tell others that, 'Security did this really cool thing, they came up with a strategy which took the money I was already spending and got me twice as much for it. You should have a conversation with them.' And then others will come knocking on your door. This is the kind of thing that comes up in the CEO's staff meeting."

Dave Cullinane
Chief Information Security Officer
and Vice President,eBay

9. Have a plan

Build and document the information security strategy including a detailed road map, clearly defined goals and manageable milestones. Measure and evaluate your progress and communicate this to the CEO and other executive leaders. Divide the strategy into the technical and business strategies; these may be inextricably linked, but have two very distinct audiences. Line managers are not going to be interested in the technical aspects of the strategy, but they will be interested in the business aspects.

"The CISO's job is about managing risk and coming up with the best possible way of doing it given a particular business context. In the current climate, the context is cost minimization. In another business climate, the context might be long-term business flexibility."

Professor Paul Dorey
Founder and Director, CSO Confidential; and
Former Chief Information Security Officer, BP

10. Know the person and speak to the person

For dealing with the CEO and other C-levels, it's important to get to know as much as you can about the individual. Learn their personal styles and preferences and tailor your communication method accordingly. Know what level of detail they expect. Know how they make decisions and what they pay attention to. Find someone you trust who has regular interactions with the CEO (or other leaders) and ask for advice about the best approach. Do a mini tabletop exercise: "Would this work? If I presented this to the CEO in this way, how would he react?"

"Understand the rhythm of the way your CEO is communicated to by other C-level officers. Get familiar with how your CEO is briefed. There is a tone, a rhythm, a format expectation."

Denise Wood
Chief Information Security Officer
FedEx

How Does the "New Economy" Change Making the Case?

Some may balk at the idea of trying to convince the CEO that security should be more strategic in the middle of the worst economic conditions in decades. How can you have a strategic security effort if you can't even get funding? But it turns out that most information security programs are still getting funded. In a recent global security survey, 63 percent of respondents say spending on security function will increase or stay the same in the next 12 months in spite of the economic downturn. Of those facing budget cuts, most will be reducing spending by less than ten percent or deferring initiatives by less than six months.[11]

But that doesn't mean the going is easy. In fact, security programs are under intense pressure to "perform." Although most organizations are not cutting too deeply into the security budget, at the same time, risks are increasing rapidly – potentially outpacing security's ability to keep up. The security team is also expected to take on more and more responsibilities as the funding remains basically the same.

Ultimately the approach to making the case for strategic information security doesn't change in the current economic conditions. It is still risk-based and business-driven. What changes is the focus on costs. This means looking at what must be done rather than what should be done and prioritizing based on the risks that are most relevant to the organization's strategic imperatives. The security officer needs to proactively determine what pieces of the information security program could be deferred, making it completely clear how deferrals change the risk picture.

"Get the data. There is an enormous amount of relevant data on broad macro trends and the internal company. Get the data to be able to say, 'Here are the three or four things we must do because of enterprise risk; here are the three or four things that are on the edge that we will want to implement over time; and here are three or four things that we can have compensating controls for and handle with a little more training.'"

Michael D. Capellas
Chairman & Chief Executive Officer
First Data

As economic conditions change, the CEO and other leaders may change their appetite for risk. If they decide cost savings trump risk reduction, it's the CISO's job to make sure that they understand exactly what level of risk they will be accepting as a trade-off, and get them to agree to accept that increase. Ultimately, security will always be adequately funded because "adequate" means it matches the level of risk that the business deems acceptable.

Even if the security department is not directly facing budget cuts, many security teams recognize that they need to share in the burden of curtailment. They are scrutinizing their operations and looking for ways to achieve efficiencies. For example, going through the entire program item by item and asking hard questions like, "Are we doing this just because it's been past practice or is it really adding value at this point?" This demonstrates an alignment with the CEO's efficiency goals.

Self-funding projects out of productivity gains is another way to build credibility with the CEO and C-suite. If information security can get as efficient as possible at basic operations, it frees up monies for new investments for meeting increased threat levels. The current downturn may present an excellent opportunity for cleaning up security operations to make them more efficient and scaled for future growth.

"You know you're doing a good job as a CISO when you can raise your hand and say to your colleagues, 'I have some budget that I should surrender because you need it more, I think I can keep the risk to an acceptable level.' It may mean you just gave yourself a harder job, but seeing the needs of the business as a whole is expected of an executive leader."

Professor Paul Dorey
Founder and Director, CSO Confidential; and
Former Chief Information Security Officer, BP

"Having less funding is not necessarily a bad thing because it forces us to get smarter about how we use that money. The most important thing is to have as much impact on the organization as we can with the resources that we have. It challenges us to bring more quality to our operation."

Claudia Natanson
Chief Information Security Officer
Diageo

"Understand the reality, understand the business dynamics and adapt your strategy. For example, even if you have approval for hiring people, you might choose not to because the rest of the organization is being cautious. This will demonstrate that you are trying to be agile. When things get better, you can start hiring again."

Vishal Salvi
Chief Information Security Officer and
Senior Vice President, HDFC Bank

Top Ten Ways to Alienate Your CEO

Information security is a relatively new function in organizations; for example, the role of "Chief Information Security Officer (CISO)" has only emerged in the last few years. Research indicates that only 44 percent of companies have established the role of CISO; and that's after a significant jump from last year when only 29 percent of companies had a CISO.[12]

Given the relative newness of the role, it can be expected that as some information security professionals try to establish themselves as strategic players, they are going to make mistakes. Along the way, there may not be many opportunities to make a good impression on the CEO – so it's important to know what not to do.

The following list provides ten surefire ways to alienate your CEO or other leaders. If you do these things, not only will you potentially blow your chance to assume the role of strategic advisor to the organization, you might even find yourself looking for a new job. This list was compiled from Council member observations over the years and from our guest CEO who has had experience with green CISOs who stumble along the way to figuring it out.

1. Waste their time

When you are reporting to the CEO (and possibly other C-level executives or the Board), don't waste their time by talking about details that don't matter to them, for example the number of viruses detected or the number of firewall hits. This is your 15 minutes of fame – don't spend it on minutiae. If you've gained access to the CEO, choose the issues you put in front of him/her and carefully prioritize around situations when there is a high impact risk and you need the CEO to make a decision. Show up too often with minor problems and you'll just be noise.

2. Waste money

Making unnecessary investments is a good way to rile your CEO. Some CISOs have a "gotta have it" approach to technology and simply go down a list, buying everything every security department should have rather than ensuring that every investment ties back to business risk. If this is your approach, the CEO won't consider you a good steward of the company's money. Other ways to waste money include running an inefficient operation rife with redundancies or implementing excessive security procedures that slow everyone down and reduce productivity.

3. Use FUD

Frequently resorting to messages of fear, uncertainty and doubt (FUD) is another good way to annoy the CEO and other C-levels. Yes, it's important for them to be educated about threat levels, data breaches and regulations, but if your objective is to scare them into spending on security, you're not going to get very far. Don't overuse headlines of cyber threats and data breaches in your presentations to the CEO, especially if you can't back it up with real data on how these media reports specifically relate to your company's situation. And don't show slides with photos of prisoners in orange jump suits entitled, "Could this be you?"

"I think the biggest alienation comes from scare tactics. From the perspective that security is the single and sole item that I should worry about. Yes, it's important, it needs to have its place high in the organization, it needs to have more awareness, but at the end of the day scare tactics never win. Data and logic are always the more powerful tools."

Michael D. Capellas
Chairman & Chief Executive Officer
First Data

4. Talk technical

If you want to make your CEO's eyes glaze over, talk about how the security team isolated malware samples or selected an encryption algorithm and key size. Many CISOs have technical backgrounds and specialized expertise, which can be a double-edged sword. You might know the intricacies of cyber attacks and defensive technologies, but fall down when it comes to communicating risks in a way the business understands. Some CISOs have a tendency to speak only in technical terms that are inappropriate for business audiences. Security is a business issue, discuss it as one.

5. Say "I told you so"

Want a fast track to the exit? When an incident occurs, go to the CEO's office screaming, "I told you this would happen!" It may be true that you tried and failed to convince the CEO and/or others about a potential risk. But if an incident does occur, you have to accept some responsibility for the security failure. A better attitude is, "There was a decision to accept the risk, unfortunately an incident occurred, let's solve the problem."

6. Bring up a problem but have no solution (or the wrong solution)

Don't raise a problem with the CEO if you don't have some possible ideas for solving it. Come to the table with alternatives and solutions – not problems. When you do propose a solution, make sure it's the right one. Don't suggest something that doesn't match the organizational culture, current business objectives, or economic climate, or is the wrong scaled approach – like recommending a massive application re-write just when the company is laying off developers. It has to be reasonable and actionable.

7. Expect special treatment

Want to get on your CEO's nerves? Portray security as more important than other functions and therefore deserving of extra attention. Or think that security should automatically be exempt when budget cuts are being implemented across the whole company. Some information security professionals believe if risks are increasing, so should their budget. But it's not necessarily a direct line from more risk to more spending. Consider the fact that the business units may face increasing competitive threats, but that doesn't mean their budgets automatically increase in order to fend off competitors.

8. Operate in a vacuum

A good way to become completely irrelevant is to have goals that are not aligned with those of leadership and the rest of the organization. For example, continuing to focus on fortifying network perimeter protection while all the business units are busy trying to save costs by moving data processing to service providers.

"Your mitigation strategies, your approaches and the way you bring your ideas to the CEO, the way you communicate, have to reflect the CEO's vision for the company. It has to be in that context. Otherwise you're going to be out of bounds with your solution."

David Kent
Vice President, Global Risk and Business Resources, Genzyme

"Don't discuss things in the old FUD manner – fear, uncertainty and doubt. If you walk into a meeting waving the latest article of some huge breach saying, 'Look, this is going to happen to us!' their response will be, 'Yeah, give me a break, we see that every day! And aren't you supposed to be doing something to make sure that doesn't happen to us?'"

Craig Shumard
Chief Information Security Officer
Cigna Corporation

9. Create frustrating policies

A really easy way to annoy the CEO and everyone else is to issue frustrating policies. Like decree that no one can have access to the enterprise network except employees; meanwhile the business depends on partner access to be competitive. Or have a blanket policy that no one is allowed network access from home; yet employees need flexible work hours. Or declare that no one can have a cell phone with a camera in it, when it is nearly impossible to buy a cell phone without a camera and everybody will have to check their cell phones at the security desk. Policies that are well-intended can sometimes be completely impractical. You have to be realistic.

10. Say no

This has been a strong, recurring theme in the Security for Business Innovation report series. Previously, information security officers have often been seen as the ones who say, "No, you can't do that." But if you want to be a strategic player, you can't say no. Instead consider how you can help the business reach their objectives safely.

One of the previous reports in the series entitled, "The Time is Now: Making Information Security Strategic to Business Innovation" builds on this premise and offers a complete set of recommendations for how to move from being the naysayer to saying, "Okay, this is how security can help make this happen." Another report in the series, "Mastering the Risk/Reward Equation: Optimizing Information Risks to Maximize Business" provides practical advice on how to find the right balance between risk and reward.

"If an incident happens, don't take the position of, 'I told you and you didn't listen to me.' It just means you were not able to sell the solution and hence you allowed that risk to be accepted. You need to be more accountable for that, because it's your job to make sure people listen to you."

Vishal Salvi
Chief Information Security Officer
and Senior Vice President, HDFC Bank

"CEOs don't want to hear about projects. They want to hear about transformational programs – how are you going to get the organization to where it needs to be? And what are the metrics you'll use so you know you're making improvements? That's what they care about."

Denise Wood
Chief Information Security Officer
FedEx

Ten Ways CEOs Can Put their Organizations at Risk

The previous sections covered what the CISO should and shouldn't do in order to convince the CEO that security must be more strategic for the benefit of the organization. But the CEO also has some skin in this game. The CEO needs to understand how his/her actions and attitudes will impact the effort to protect information at the company. To that end, this list looks at some of the top ways that the CEO, other C-levels and the Board can put the company at risk when it comes to information security.

1. Ignore risks to information

For whatever reason, the CEO and other leaders may not consider risks to information all that relevant and may not spend much time thinking about them. After all, there are plenty of other risks to worry about; such as competitive threats and financial risks. But given the current socio-economic conditions and the business climate, protecting information has become a strategic imperative that warrants executive attention.

An information breach could cause loss of intellectual property, a major hit to the company's brand, lawsuits and regulatory issues. But the stakes are getting even higher. Companies are increasingly suffering direct financial losses as targeted attacks and tailored malware now orchestrate illicit transactions (e.g. fraudulent ACH transfers), transferring money right out the door. CEOs and other leaders ignore risks to information at their company's peril.

2. Set the wrong tone at the top

The CEO can put the organization at risk by creating a culture of apathy when it comes to protecting information. If the leaders don't consider it important, the rest of the organization won't either. Leadership needs to set the right tone at the top. This means actively communicating the importance of information security, being visibly supportive of the security mission, and establishing it as a responsibility of everyone in the organization.

3. Get swept up in the media hype

As previously mentioned in this report, media hype about cyber threats can steer the CEO and other executives in the wrong direction. If they get caught up in all of the hype, they will not be focused on the risks that are most relevant to their organization, but rather on the risks that make the best headlines.

4. Think of it as just a technology problem

Since information security often sits within the information technology department, it continues to be seen by many as a technical specialty. But it's not just a technology problem; it's a risk management problem. For example, the CEO may believe the information security problem is solved because the CISO encrypted all of the laptops. Not seeing the bigger picture leaves the company exposed to all kinds of other risks.

5. Think of it as just a compliance issue

Regulations that call for data protection – from Sarbanes Oxley to the many state, national and international privacy laws – have certainly helped CEOs and other leaders become aware of information security. However if the C-level approaches it as just a compliance issue, they will not be addressing the most pressing risks. Often a compliance focus causes a "check list" mentality, whereby it's all about minimally meeting requirements rather than examining risks. Compliance is definitely an important driver for information risk management, but it is not the end goal.

"An important part of the CEO's role is to ensure there is a sustainable baseline with on-going objectives. This cannot be a one-time, one-shot deal. It needs to be a sustainable, continual evaluation and assessment."

Michael D. Capellas
Chairman & Chief Executive Officer
First Data

6. Don't set up a governance structure

With no governance structure, the security program will not have the power or the means to adequately manage the risks across the organization; nor will the effort be sustainable. Ideally information risk management should be built into an overall enterprise risk program and an Enterprise Risk Committee – a cross-organizational and cross-functional team consisting of the most senior executives – should be set up. A governance structure should ensure risk decisions are based on a well-understood and defined methodology, which is well-communicated throughout the organization.

7. Assign information security too low in the organization

If information security does not have the right level of authority, it will not be taken seriously. This role cannot be relegated to a database administrator who does security part-time. An actual security leader needs to be appointed such as a CISO or equivalent. Something as crucial to the business as protecting its brand, reputation and information assets should not be low on the totem pole. The CISO should report at least to the C-level and be on the Enterprise Risk Committee or well-represented on that committee.

8. Don't recognize you own the risk

It's the CEO, C-levels and the Board who ultimately own the risk, not the information security officer. The CISO's job is to help the risk owners make the best risk decisions. If the business leaders don't recognize they own the risk, they won't adequately consider the risks nor consciously determine the company's risk appetite.

9. Don't enforce the security policy

The CEO, C-levels and the Board not only own the risk; ultimately they own the information security policy. They should know, approve and ensure enforcement of the policy. One way that CEOs undermine security policy is by flaunting it themselves; such as getting the security controls taken off their computer because they are too much of an inconvenience. The CEO needs to lead by example. Lack of leadership support for the security policy means the information security program cannot be effective and puts the organization at risk.

"It's prioritization and tone-setting. If it's important to the CEO, it's important to the company. If he or she makes it a priority, then it becomes part of the DNA of the organization."

Roland Cloutier
Vice President, Chief Security Officer
EMC Corporation

10. Live in a bubble

The nature of our Western, post-industrial society is to put the "princes of commerce" into a different level of interaction in many organizations. If the CEO and other leaders are insulated from the grim realities at the front lines of the organization, they may put the organization at risk. Senior executives need to be prepared to know the true risk picture and the actual capabilities of their company's safeguards and protections.

"If the right governance structure is in place, the CEO and Board don't have to pay undue attention to security, as long as the committees responsible – the Board committee and/or executive committee – and the CISO are doing their jobs."

Vishal Salvi
Chief Information Security Officer and
Senior Vice President, HDFC Bank

Conclusion

In the past it may have seemed like an uphill climb just to get the executive leadership and business teams to recognize the importance of information security, but increasingly this is a given. This is a testament to the hard work that information security leaders have been doing. Now the campaign must shift from creating awareness of the need to actually implementing a strategic approach to information security.

The CEO is your most important ally in this endeavor. He/she needs to lay the foundation on which you will build across the entire organization. It is absolutely key that you earn the confidence of the CEO; he/she must trust that you know what you're doing and have the company's best interests in mind.

The benefits are clear. As enterprises navigate through a long and spotty economic recovery, a strategic, risk-based approach to information security will optimize risk-taking and maximize the rewards of business innovation.

Appendix: Biographies

Guest Contributor

Michael Capellas
Chairman & Chief Executive Officer
First Data Corporation

A 30-year veteran of the IT industry, Michael became First Data's Chairman and CEO in 2007. Previously, Michael was CEO of Compaq Computer Corporation and President of HP; and President and CEO of MCI, where he oversaw the successful rebuilding of the company. Michael began his career with Schlumberger Limited and has also held senior management positions at Oracle and SAP Americas. Michael serves on the board of directors of Cisco Systems and holds a bachelor's degree from Kent State University.

Security for Business Innovation Council Members

Anish Bhimani, CISSP,
Chief Information Risk Officer
JPMorgan Chase

Anish has global responsibility for ensuring the security and resiliency of JPMorgan Chase's IT infrastructure and supports the firm's Corporate Risk Management program. Previously, he held senior roles at Booz Allen Hamilton and Global Integrity Corporation and Predictive Systems. 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. He authored "Internet Security for Business" and is a graduate of Brown and Carnegie-Mellon Universities.

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 30 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."

Security for Business Innovation Council Members

Professor Paul Dorey
Founder and Director, CSO Confidential
and Former Chief Information Security Officer,
BP

Paul is engaged in consultancy, training and research to help vendors, end-user companies and governments in developing their security strategies. Before founding CSO Confidential, Paul was responsible for IT Security and Information and Records Management at BP. Previously, he ran security and risk management at Morgan Grenfell and Barclays Bank. Paul was a founder of the Jericho Forum, is Chairman of the Institute of Information Security Professionals and a Visiting Professor at Royal Holloway College, University of London.

Renee Guttmann
Vice President, Information Security
& 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, Global Risk
and Business Resources,
Genzyme

David is responsible for the design and management of Genzyme's business-aligned global security program, which provides Physical, Information, IT and Product Security along with Business Continuity and Crisis Management. Previously, he was with Bolt Beranek and Newman Inc. David has 25 years of experience aligning security with business goals. He received CSO Magazine's 2006 "Compass Award" for visionary leadership in the Security Field. David 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. Claudia is Chair of the Corporate Executive Programme of the World Forum of Incident Response and Security Teams. She holds an MSc. in Computer Science and a Ph.D. in Computers and Education.

Security for Business Innovation Council Members

Vishal Salvi, CISM
Chief Information Security Officer
and Senior Vice President,
HDFC Bank

Vishal is responsible for driving the Information Security strategy and its implementation across HDFC Bank and its subsidiaries. Prior to HDFC he headed Global Operational Information Security for Standard Chartered Bank (SCB) where he also worked in IT Service Delivery, Governance & Risk Management. Previously, Vishal worked at Crompton Greaves, Development Credit Bank and Global Trust Bank. He holds a Bachelors of Engineering degree in Computers and a Masters in Business Administration in Finance from NMIMS University.

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.

Denise Wood
Chief Information Security Officer
and Corporate Vice President,
FedEx Corporation

Denise is responsible for security and business continuity strategies, processes and technologies that secure FedEx as a trusted business partner. Since joining in 1984 she has held several Information Technology officer positions supporting key corporate initiatives, including development of fedex.com; and was the first Chief Information Officer for FedEx Asia Pacific in 1995. Prior to FedEx, Denise worked for Bell South, AT&T and U.S. West. Denise was a recipient of Computerworld's "Premier 100 IT Leaders for 2007" award.

References

1. *Global State of Information Security 2010*, Price Waterhouse Coopers
2. *NYSE Euronext 2010 CEO Report*
3. *Business Case for Data Protection*, Study of CEOs and other C-levels, Ponemon Institute
4. *Business Case for Data Protection*, Study of CEOs and other C-levels, Ponemon Institute
5. *Top Cyber Security Risks September 2009*, SANS Institute
6. *Business Case for Data Protection*, Study of CEOs and other C-levels, Ponemon Institute
7. *Global State of Information Security 2010*, Price Waterhouse Coopers
8. *Global Security Survey 2009*, Deloitte Touche Tomatsu
9. *Business Adoption of Cloud Computing*, Aberdeen Group
10. *Manage the Costs and Risks of Third-Party Assessments*, Information Risk Executive Council
11. *Global State of Information Security Survey 2010*, Price Waterhouse Coopers
12. *Global State of Information Security 2010*, Price Waterhouse Coopers

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

The Security Division of EMC

CISO RPT 1209