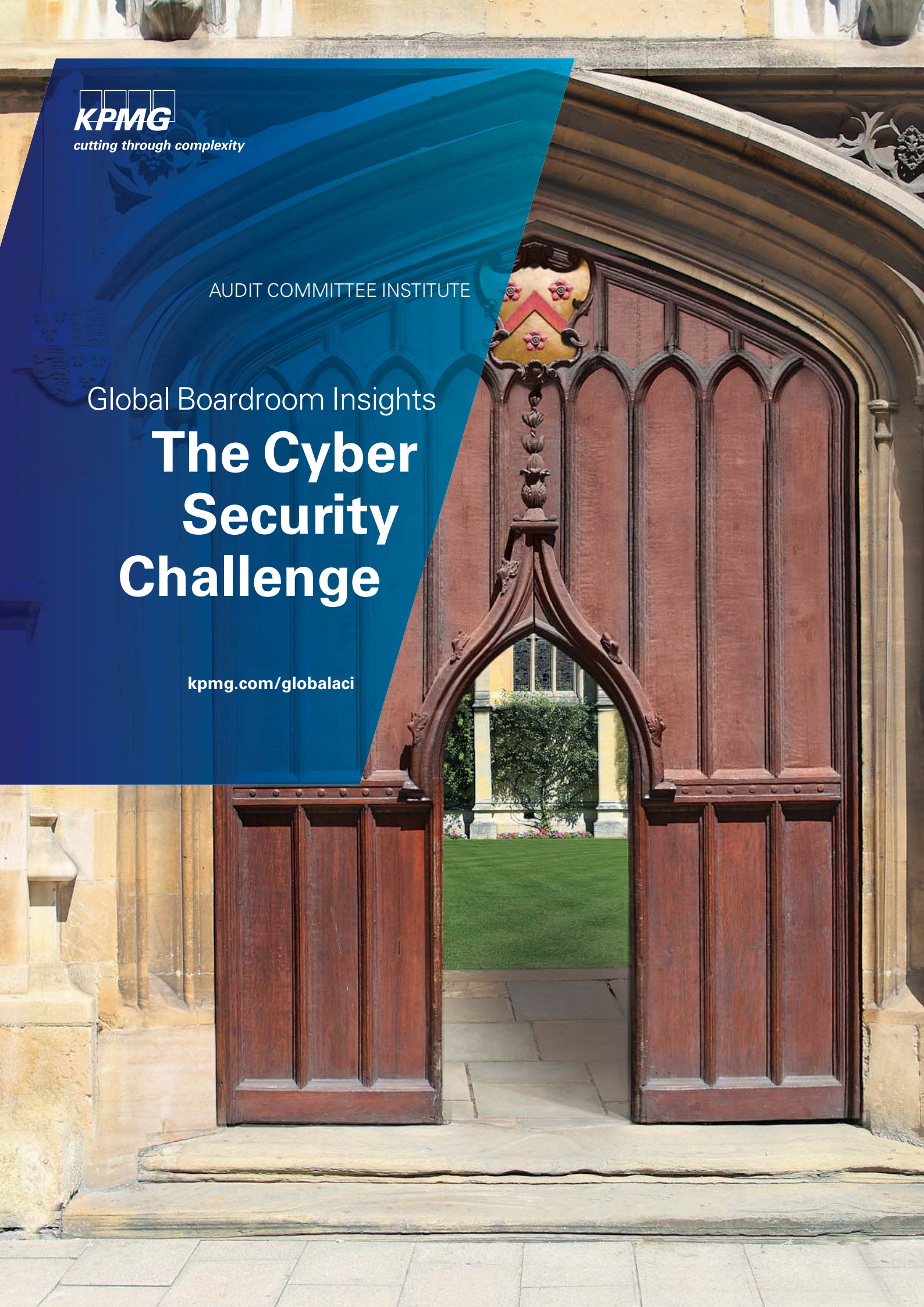


KPMG
cutting through complexity

AUDIT COMMITTEE INSTITUTE

Global Boardroom Insights

The Cyber Security Challenge

kpmg.com/globalaci

About
KPMG's Audit Committee Institutes

Sponsored by more than 30 member firms around the world, KPMG's Audit Committee Institutes (ACIs) provide audit committee and board members with practical insights, resources, and peer exchange opportunities focused on strengthening oversight of financial reporting and audit quality, and the array of challenges facing boards and businesses today – from risk management and emerging technologies to strategy and global compliance.

To learn more about ACI programs at resources, contact us at:

auditcommittee@kpmg.com

Contents

Foreword

As many companies and organizations are recognizing – and experiencing first-hand – cyber attacks are no longer a matter of *if*, but *when*.

Recent cyber breaches at major corporations highlight the increasing sophistication, stealth, and persistence of cyber attacks that organizations are facing today – from nation-states, organized crime, and hacktivists, as well as threats from *within* the organization (which often pose the greatest risk).

The critical challenge of protecting information systems and assets – financial information, customer data, intellectual property – and the reputational and regulatory implications of failing to do so continue to raise the stakes on cyber security and governance. Investors and regulators are increasingly challenging boards to step up their oversight of cyber security and calling for greater transparency around major breaches and their impact on the business.

Not surprisingly, cyber risk is rapidly climbing up on the audit committee's agenda. According to KPMG's *2014 Global Audit Committee Survey* nearly 40 percent of audit committees have primary oversight responsibility for cyber security risks, and 45 percent believe the audit committee (or board) doesn't devote sufficient time to cyber security.

In this edition of KPMG's *Global Boardroom Insights*, we take a deep dive into this issue, exploring key elements of effective cyber risk oversight and governance – from understanding key vulnerabilities and integrating cyber security into the overall risk management program, to ensuring effective communication and reporting from the CIO (or equivalent role) and having a robust cyber-incident response plan in place.

Our sincere thanks to those who shared their time and insights with us – Sir Jonathan Evans, Jeffrey Keisling, Brian Stevenson, Richard Doern, Sridar Iyengar and Jan Zegering Hadders.

Timothy Copnell
Audit Committee Institute
KPMG in the U.K.

Dennis T. Whalen
Audit Committee Institute
KPMG in the U.S.

Wim Vandecruys
Audit Committee Institute
KPMG in Belgium

Sidney Ito
Audit Committee Institute
KPMG in Brazil

Mritunjay Kapur
Audit Committee Institute
KPMG in India

Sir Jonathan Evans HSBC and National Crime Agency (U.K.)

Sir Jonathan Evans is an independent non-executive director of HSBC Holdings Plc where he is a member of the Financial System Vulnerabilities Committee. He is also a non-executive director of the National Crime Agency. Sir Jonathan spent 33 years in the U.K. Security Service, six as Director General. His experience includes counter-espionage, protection of classified information and the security of critical national infrastructure. His main focus was counter-terrorism, both international and domestic, including initiatives against cyber threats. As Director General he was a senior advisor to the U.K. government on national security policy and he attended the National Security Council.

"Good cyber security is not just about a really strong wall on the outside, but also about some kind of immune system within."

ACI: *How important is cyber security for business today?*

Sir Jonathan Evans: I think it's a very important issue not least because it covers a whole range of different risks – risks to businesses and risks to government – and there's a broad range of threats in play. These range from low level/high volume crime, through to more sophisticated crime, through to state 'actors', some of whom are attacking commercial enterprises as well as governments. And then there are those who don't want to steal information at all, but to potentially disable the capabilities of companies or governments. Almost all business's today rely critically on their IT capabilities and those are potentially vulnerable to attack either because people want to get hold of the information or because they want to corrupt the information or because they want to destroy the ability of the company to access the information.

ACI: *How high do you think this whole issue is on the business agenda?*

Sir Jonathan Evans: I think there has been a significant change over the last three or four years. This was once seen as an issue for the CIO or the IT guys, but there is now an increasing recognition that this is something which has implications right across a company.

The current government has prioritised cyber security issues and it was something which in my previous job I was involved with helping to implement. I think the high profile cases which have affected some companies – linked with the increasing government focus – have significantly increased the awareness of many companies, but it's still patchy. Talking to colleagues and people in the industry, there is still a feeling that it is higher on the agenda in the United States than it is in the U.K.; but equally it is probably higher on the agenda in the U.K. than it is in some other parts of Europe or other parts of the world. So I think there is a spread but the overall levels of concern are rising.

ACI: Where does the responsibility for cyber security sit within an organisation?

Sir Jonathan Evans: I think you need to consider this as a risk to your business and from that point of view it needs to be a board issue. That doesn't mean that the board are in a position to make technical decisions on how to protect the business but that board should be confident that they know what their critical information assets are and that they understand the risks to those assets and the potential impact on the business. They then need to think through their

risk appetite – that is very much a board issue – and make sure that at the executive level there are risk management plans in place and that those plans are being properly operationalised. Understanding the risk to the business is critically important and should not be simply delegated to the CIO or the tech guys – or for that matter, the audit committee.

ACI: *Notwithstanding the technical knowhow within (say) the IT function, do you think boards have enough knowledge in this area?*

Sir Jonathan Evans: I think that would depend on the company. There will be companies where cyber security is such a central issue that it is prudent to have somebody with real expertise on the board, in other companies the board might be satisfied with knowing that the 'right' expertise is available to the company. It doesn't necessarily have to be a member of the board in all cases, but the board do have a duty to ensure that the risk is properly identified and that they have access to the people who can ensure the level of protection is right. Some of that might be in-house, some of that might be brought in, but again I think that depends on the scale and the nature of the company. There will be small companies where you couldn't reasonably have a full time person focussed on cyber security, but in companies where it's a major risk there might be a significant number of staff involved. The board's responsibility is to make sure that the risk has been properly assessed and that it is being managed appropriately.

ACI: Do you think there are any specific challenges for boards and audit committees in doing that?

Sir Jonathan Evans: There are a number of challenges in this area. The first is that the 'actors' who are posing the risk are obviously covert and they try to cover their tracks. That means that understanding the exact nature of the risks can be complex and reliable intelligence can be difficult to identify. The second is that the technical aspects of it can be very complex and the bigger and more interconnected your IT system is, the more vulnerabilities there are likely to be in it. Understanding those vulnerabilities can be quite challenging.

Also, it is clear that the market for cyber security expertise is quite tight at the moment. There is more demand than there are people who really know what they are doing and therefore making sure that you have the right quality of staff and the right number of staff can be difficult. There are a number of initiatives underway

to try to increase the supply but nevertheless at the moment the demand is outstripping the supply.

Another issue is that this is not just something which can be tackled on the technical front. It has implications for the behaviour of staff right across the organisation because it is still the case that many successful cyber attacks on businesses, as with government, are as a result of spear fishing – specifically tailored attacks against individuals which are socially engineered to appeal to the victim. All staff need some degree of training and understanding about how they combat such risks. This is difficult and the bigger the organisation the more difficult it becomes.

ACI: *Attackers presumably focus on the weakest link – that must be a big problem for large multinational organisations?*

Sir Jonathan Evans: There are two things to consider. The first is that even companies that feel that their own systems are well protected are exposed when they link their systems to another company – maybe as a result of an acquisition or merger. A lot of thought needs to go into how the desired level of security can be maintained. Furthermore, cyber attackers are always looking for vulnerability. As cyber awareness and defences improve, so too does the sophistication of the attacks. That needs to be thought about – the risk never stands still.

I think there is a wider question here around the protection philosophy within an organisation. The traditional model of cyber security has been a bit like a castle – if you have a big enough set of walls and moats around it you can stop the bad guys getting in. But, I think you have to assume that at some point the bad guys will get in and therefore you need to think about two things – how do you identify activity within your networks and how will you respond. In the event that you are a victim of these sorts of attacks then you need contingency plans in place. Just as with other areas of security you have a variety of elements to consider. You have the protection element; you have to have intelligence of what the other people are trying to do to you; and you need to be able to manage the response when you become a victim. If all these elements are working together then you should have much more confidence of being able to withstand an attack. So, good cyber security is not just about a really strong wall on the outside, but some kind of immune system within and also the ability to recover quickly.

ACI: *That leads to the real cost to business of cyber crime. Not just the money stolen, but reputational damage and regulatory intervention?*

Sir Jonathan Evans: There are rafts of cyber attacks that are there for straight forward acquisitive reasons and I think people are reasonably familiar with those. The amount lost in online banking, for example, is significant but it's sustainable – and there is a continual process of escalation on the part of the criminals and on the part of those who are protecting against the criminality. The difficulty is the reputational damage associated with losing customer data in an attack – that can be just as significant as financial loss and undermining of confidence. People understandably expect that major companies will be able to meet their requirements 24/7 and if your systems are taken down because of an attack then that can affect the creditability you have with customers. It can also affect your share

price and the value of the company so it is a major issue beyond the straight forward financial losses from the criminal fraud aspect.

ACI: *Banks often recompense customers for cyber crime losses – does this mean that cyber crime is not perceived as a big issue by customers and the general public?*

Sir Jonathan Evans: Well, I think people are aware of it and you do meet people who say they won't do online banking. On the other hand, the general approach taken by the U.K. retail banking sector is that losses don't fall on the customer. Interestingly that is not the case in all jurisdictions. There are places where such loses are more likely to fall on the customer and that may have an impact on customer behaviour. Nevertheless, in the U.K., they don't fall on individuals and therefore they can be reasonably confident in using the systems and that is where a lot of the cyber security protection is focused. I think the big reputational issues are probably in major data losses and potentially in the sabotage of systems at a more major scale. These are much less frequent but potentially more catastrophic if they do occur and that, of course, is not something which is in any sense restricted to the financial services industry.

ACI: *To what extent is technology an issue? In a world where cyber criminals have all the latest equipment and sometimes more computing power than the organisations they are attacking, does new technology create a commercial advantage?*

Sir Jonathan Evans: Well clearly there are advantages in building your systems with current cyber security in mind. Retro fitting security is more of a challenge but I don't think it's an issue specific to banking. It's inevitably the case that if you have a series of legacy systems they will not have been built with security in the front of people's minds. But, it also depends on the attackers. There is an impression that cyber criminals are highly sophisticated with large amounts of resources available to them and that is true for some of them but for many of them it's not. There are certain websites out there which provide you with cyber capability for a one-off attack or for a longer period – it's quite a sophisticated market and not all the people who are behind the attacks are necessarily highly technical themselves. It's an unusual model so it's important to have, as far as you can, an understanding of what the nature of the threat is. If you are worried about a major state attack on your infrastructure then obviously that is one level of concern, but if you are concerned about small scale but high volume fraud then that's different. Most small companies are unlikely to be victims of a state attack, but there will be companies that are; that's why getting your risk assessment right is so important. You need to put the resources you have available in the right places for the particular circumstances – and making that happen is part of the board's responsibility.

ACI: *And these days you've also got so-called disruptors who aren't stealing information or anything else but, for whatever personal passions they have, want to bring an organisation down. That must be a difficult risk to get hold of?*

Sir Jonathan Evans: The hactivist threat needs to be considered. It may be purely a publicity thing if they can hack your public website and put their slogans across it – that's quite a good way of drawing attention to their particular issues. Or it may be that they have more malign actors who want to mount a denial of service attack in order to make their point, again this will depend on the industry you're in but it's certainly one of those various aspects of cyber security that need to be considered.

ACI: *To what extent do commercial organisations share information about where attacks are coming from? Do governments share this sort of information with the corporate world?*

Sir Jonathan Evans: Well that was definitely one of the key aims of the government cyber security strategy which was outlined two or three years ago. In my view cyber security should not be a competitive issue between companies and there are well established mechanisms for sharing information on a variety of security issues, particularly for those companies that are part of critical national infrastructure.

The other aspect is the extent of which government is able to share. There are a number of models being developed on this which I think are moving in the right direction. It's not straight forward because some of the information the government holds is highly sensitive and can't be widely shared without losing its value. I think there will be a period of the experimentation to find the best way of doing this and then of course confidence building measures become important; but I think there is a clear determination on the part of government to share as much as they can because national security does not stop with government.

By that I mean that the security of a country depends not just on its government being secure but also public services, financial services and other things, many of which are delivered through the private sector. So there is a national security interest on the government for sharing and therefore balancing those ideals of protection versus sharing is something the government is very much focused on.

ACI: *Do you have any hints or tips for audit committees or boards – what are the top two things to think about?*

Sir Jonathan Evans: I think the first thing, and in some ways the most difficult thing, is to identify your critical information assets. Companies aren't always good at thinking about their information as an asset and therefore recognising what its value is. Everybody understands where their money is and they care about that, but information needs to be thought about in a similar way.

The second is that for most companies cyber security will come down to defence in depth and a variety of different approaches. There are no silver bullets. ❖

Jeffrey E. Keisling Pfizer (U.S.)

Jeff Keisling is Senior Vice President and Chief Information Officer at Pfizer, with responsibility for the company's information technology strategy, including enterprise business systems and global IT shared services. Prior to joining Pfizer in 2009, he was Vice President, Corporate Information Services and Chief Information Officer for Wyeth Pharmaceuticals (which was acquired by Pfizer). Mr. Keisling has also served as the CIO at Advanta Financial Services and Rhone-Poulenc Rorer Pharmaceuticals, and directed the business systems development teams at Knoll International. He serves on the board of the Pharmaceutical Information Services Association, the Research Board, IBM Advisory Board, CIO Strategy Exchange, and Microsoft Advisory Council.

"The audit committee wants us to demonstrate that we're skating to where the puck is going, rather than where it is now."

ACI: *How do you think about the cyber security challenge at Pfizer, and has the recent raft of cyber breaches in the headlines elevated the issue for the company and the board?*

Jeff Keisling: Cyber security has been in the DNA of our enterprise risk management (ERM) program for some time. It's not viewed as a unique program or process, but as an ongoing risk that's integrated with our ERM program. As incidents and attacks have become more sophisticated, cyber threats have certainly moved up in our stratification of enterprise risks.

I think where we've been particularly effective is including cyber security in our mainstream corporate governance activities – in the C-suite and the boardroom – and plugged into the ERM framework in a multi-disciplinary way.

ACI: *Can you elaborate on the multi-disciplinary aspect? Who tends to be at the table with you on cyber security issues?*

Jeff Keisling: It is a business driven process. We receive input from our Commercial, R&D, Supply Chain, Medical, and Finance partners in the business, who define and stratify the risk. Years ago we formed an information security council to help address these defined risks, by bringing together different perspectives on global security, including representatives from our legal and compliance teams, HR, Internal Audit, Communications, and Business Technology. The council is where the governance cycle around cyber security begins – policies, educational programs, awareness, the constant vigilance and reminders. From there, it rolls up into the company's broader governance framework.

ACI: *What role does internal audit play?*

Jeff Keisling: Internal audit is our partner. We work in close collaboration with the audit team on all facets of IT, whether it's cyber security or how we govern IT programs in general.

The audit team provides expertise on policy. For example, when we do a refresh of our cyber incident response policy, internal audit is at the table as we refine the strategy and the policy, and weave it into the ERM program.

Audit has also sharpened its focus on cyber risk as it moves higher on the risk scale, and helps us develop the agenda on IT governance throughout the enterprise and with our audit committee. They also work with us in a very direct and collaborative way when we're investigating specific cyber incidents or issues. Audit is a highly valued partner as they bring an independent and balanced perspective to the table.

ACI: *How do you help the board get comfortable that the company has its arms around cyber risk? When you're communicating with directors about cyber risk and security, what information do they find most helpful?*

Jeff Keisling: The board wants to understand the structure of and governance around our cyber security risk management, and how it fits into the company's overall ERM program. An understanding of the cyber risk strategy is key.

The board also wants to understand where the greatest threats and risks to the company's highest value assets are coming from. They want to see how human capital and financial capital are aligned to manage the greatest threats we face.

Our audit committee is particularly engaged in reviewing the performance of our processes and protections. A cyber security scorecard is routinely reviewed during our sessions which address our principle risk areas, incidents, trending, and a view of what's happening in the external environment.

Finally, they want us to demonstrate that we're skating to where the puck is going, rather than where it is now. It is well understood that our cyber security efforts will

be continuously improving to add capabilities that protect our company as threats and risks change.

We've found that those elements – discussed in an open and frank way – help create a high level of transparency and trust, and the dialogue that we get in return is extremely valuable.

ACI: *Can you talk a little more about the scorecard you use?*
Jeff Keisling: We review with the audit committee and board a scorecard that tracks four broad areas of key risks and trends. This includes the volume of incidents and materiality of any events during the most recent period and how we're managing those events. We also provide information and updates on what's happening outside of the company, in the private and public sector, as well as what is happening on the legislative front.

In general, I think the maturity of cyber risk information and the quality of our dialogue in the boardroom improves with every conversation. Directors bring their own insights from other companies – including those that carry some of the highest risk profiles, such as the financial services sector. It's been a collective learning process with the board, and together we've gotten the language, tools and information tuned-up to a level that supports a really good dialogue.

ACI: *How do mobile technologies and social media factor into your cyber security approach – internally and externally?*
Jeff Keisling: With approximately six billion devices in the world today, mobile technologies and social media create new risk channels and higher volumes of attacks. In many cases, we're seeing the same types of threats that we've seen before, just replayed and retried at a higher volume. To give you an order of magnitude, we've seen a 400 percent increase in about a year's time.

While we still see classic phishing and spamming techniques, the bar is clearly being raised in terms of higher-end sophistication and potential fraud. But we have to keep our eye on the ball whether it's low end or more sophisticated, state-sponsored activities. Social media and mobile technologies unfortunately mean more shots on goal for the opposing team – and that's a big part of our conversation when we talk about how we're using these capabilities to advance our business and science.

Mobile and social media also raise the stakes on reputational risk. One of our four top strategic imperatives is to "earn greater respect from society." As a company in the life sciences space, focusing on therapeutic innovation, nothing is more important to us than our customers and patients. So our reputation and respect from society are top priorities. We have a very active social interactive monitoring program to understand what's happening in the marketplace relative to our patients and our customers. It adds to the volume of work and the challenge of keeping an eye on social media and the marketplace broadly, but it's an imperative for us.

ACI: *We're seeing more companies and boards adopting a mindset of "not if, but when" a cyber breach occurs. What do you see as being the critical elements of a good cyber-incident response plan?*
Jeff Keisling: It's challenging to define a precise process or a set of concrete steps for managing a cyber incident because they don't all have the same attributes and implications for the company or our customers. That said, incident management is a critical component of an overall cyber risk program – and I think a couple of things determine how effective your response will be.

First, early engagement, especially during the planning process, and involving the key players, using a multi-disciplinary approach, is critical. We include our communications and policy teams who are actively involved with scenario planning. Second, it's important to establish clear accountability – if we have a breach, who is responsible for doing what? Even though we don't know exactly what play is going to be called, depending on the incident, we know who's going to be in the game and they know what their role will be.

The third critical piece involves decision making, particularly if an incident has external implications. Internally, it's about and educating our colleagues and that process doesn't change much. But in cases where third parties or customers might need to be notified, it's important to have a framework for making those decisions – sometimes very quickly.

ACI: *A large percentage of cyber breaches are attributed to internal "people risk" – employees not following procedures or internal controls – versus external attacks by hackers. How should companies and boards be thinking about internal risk?*
Jeff Keisling: Media reports tend to focus on the more sensational attacks from external sources. But we continue to advise management and our directors that internal risks and external risks are equally important.

Internal risk comes in different forms. One of the things we're seeing is more social engineering attempts, which are fairly low-sophistication attacks, but present a risk nonetheless. In these instances, a colleague is targeted by using their personal public "digital footprint." The attacker uses this information to create a level of confidence with

that person, with the goal of socially engineering a way into the company's systems or processes.

In addition, when you consider that most large enterprises have many third parties performing high volume or highly controlled transaction services – contractors, vendors, partners – the slope of the complexity curve increases. Whether it involves financial transactions or the exchange of sensitive information or intellectual property, it's a good idea to double-down on the resources devoted to protecting those assets from third-party risks.

ACI: *Does being global pose different types or higher levels of cyber risk?*

Jeff Keisling: I would say that's a deafening yes. We have a physical presence in approximately 175 markets around the world, from manufacturing and R&D sites to a broad range of commercial capabilities. When you combine our physical presence with the amount we spend to fund R&D every year, collaborations with academic institutions and health system payers and others, and our global visibility, you can imagine we get a lot of attention from people looking to penetrate our systems. It comes with the territory, and it goes back to my earlier point about skating toward where the puck is going to be attempting to always stay a step ahead.

A big part of that is communicating and continually reinforcing the company's cyber security policies, protocols and expectations to our people around the world. It's training tools and reminders; it's compliance and governance tools. Every employee goes through training, is tested and periodically retested on compliance, and a 100 percent score is required.

Our colleagues are well aware of our standards and expectations for cyber security; it's burned into the culture of the company. It's a big task, and it's never really finished. Everything we do embeds cyber security more deeply into the company's DNA and our risk management efforts across the enterprise. ❖

Brian Stevenson Agricultural Bank of China (U.K.)

After a long career in banking with Barclays Plc, Deutsche Bank AG and the Royal Bank of Scotland Group Plc, Brian Stevenson is now a non-executive director of the Agricultural Bank of China (U.K.) Ltd where he chairs the risk committee and is a member of the audit committee; and an advisor to Worldpay (U.K.) Ltd where he is a member of the risk committee. He is also a board member of New Model Identity Ltd and an advisory board member at Lysis Financial Ltd.

"Making sure that cyber defences are as up to date as the attackers forms a big challenge."

ACI: *Do you have any experience of cyber-attacks?*
Brian Stevenson: I have a very specific experience of a cyber attack – an organised crime attack where the organisation doing the attacking had more computing power at their disposal than the company being attacked. One of the reasons I have taken an interest in online security is because when I looked around the company to find other people with experience of such a thing there were very few. That led to me becoming the chair of the internal audit committee of a division of that company – I had experience of both running a payments organization (which in some ways are the most vulnerable to organized crime attack because that is where the most money flows), but also because I went through the experience of having to deal with the regulators, pay fines and all those hidden costs of cyber crime. The fact that money was stolen was almost incidental, because the cost of remediation was almost eight times the amount stolen. Reputational damage and loss of money is one thing, but in a regulated industry the fines payable for not protecting your clients' data can cost a lot of money.

ACI: *How high is cyber risk on your board/audit committee agenda and how high should it be?*
Brian Stevenson: How high it should be depends upon the business you are in and the perceived vulnerability of your organisation to a cyber attack. An immune business model is difficult to imagine because most organisations are dependent upon some form of web communications and as soon as your internal computer system is attached to an external computer system you are vulnerable to attack. You have to take a risk-based approach. If you have lots of money to be stolen or know-how or important customer data then the risk will always be higher. If you have a business where you have low levels of client data, low levels of payment flows, no trade secrets and those sorts of things, then the risk might be relatively low.

There are five different types of attackers from the analysis that I have been involved in: governments, competitors (industrial espionage), organised criminals, petty criminals and disruptors or 'hactivists'. A good audit committee will go through these five categories and assess the risk in each case. If you think you are vulnerable to all five forms of attack then it will be high on your agenda. It requires rigorous analysis within the business and enough knowledge and education sitting around the audit committee and boardroom table to understand what the nature of the risks are.

ACI: *Do you think that there is enough knowledge around boardroom tables?*
Brian Stevenson: I would go back a step and ask who's responsible for cyber security in the organisation. Which board member has a daily worry about cyber security on their plate? Very few organisations have an IT director sitting on a main board even though most organisations are critically dependant on their IT infrastructure. Quite often it's the finance director, but finance directors have lots of other things to worry about. It may be delegated by the finance director to somebody who doesn't sit on the main board – but does that person have the right support and the right representation within the governance structure? This is sort of the rigour I think organisations have to go through.

ACI: *Should the oversight of the cyber security risks be allocated to the audit committee or the risk committee?*
Brian Stevenson: The preferred approach within banking is to monitor it through the risk committee but not to ignore it at audit committee level. So, the detailed monitoring takes place at the risk committee including discussions with the IT people. The risk committee has to be satisfied that we are up to speed, we have policies in place, we have appropriate defences, the defences are up to date, that known attacks are reported and how we defended them – including whether new technologies have attacked us.

Risk committees are relatively rare outside the financial sector, so these things would often fall to the audit committee.

ACI: *So what are the other challenges beyond establishing the right roles and responsibilities within the organisation?*
Brian Stevenson: There is an educational piece which is about making sure that frontline businesses understand

the consequences of their actions for cyber threats. For example, is there a standardised approach to the development of websites? In a complex business you don't want a free for all where anyone can go and develop a public website with no recourse to compliance with central governance arrangements because a web page is the front door for a criminal to get into your organization – particularly if the webpage takes you into a payment processing engine as that is exactly what they are looking for. Unfortunately, there should be no freedom anywhere in an organization for anybody to develop a webpage with an internal access route without complying with all the highest possible standards of web security. Today, how many organizations report statistics on this sort of thing to the audit or risk committee and how many establish the vulnerabilities they have in their web infrastructure? This is the sort of rigour that is needed.

In the old world, you wouldn't expect a high street bank to leave the door to the safe wide open, but essentially that's what having ineffective web security means – but people don't think about it like that.

Internal audit should be looking at the website development policy – making sure that not only is there a policy in place but that the policy is actually working. For a bank, which is where most of my experience is, as soon as you allow your customers to go online to make a payment that allows a potential attacker through the first line of defence into the processing engineering of your organisation and that's what they like.

ACI: *Do internal audit teams have the skills to do this?*
Brian Stevenson: Generally no, but this is where outsource arrangements come in. Most of the big accounting firms now have a considerable body of expertise in cyber issues, including in some cases, ex-criminals turned straight that sit there trying to break into systems on behalf of clients to see how vulnerable they are.

ACI: *Which is a neat segue to the technology challenges*
Brian Stevenson: There are certainly technical challenges – not least because cyber attackers can be ahead of the curve in terms of technical knowhow and computing power. Once inside the system they look around for the most vulnerable point to attack – and that can be a subsidiary that isn't up to the same global standards as the rest of the group. So, making sure that your internal IT department and your cyber defences are as up to date as the attackers form a big challenge.

I think one of the areas that could be improved is cross-industry cooperation. For example, do companies share information about where attacks have come from and the technology used with others who might be vulnerable? Would they share it with their competitors or the banks? Then there is the bigger and more vexing question of government to government sharing – but we can save that for another day.

ACI: *Do you feel that audit committees currently have the necessary skills and knowledge required in order to provide effective oversight? Or risk committees for that matter?*
Brian Stevenson: It is very difficult to generalise but from the time I was living and breathing a major breach, I got a clear impression that law enforcement agencies and regulators didn't feel that the banking industry as a whole was on top of this issue. Cybercrime is a relatively new phenomenon and most people sitting on audit committees or indeed boards haven't grown up with it. They have grown up with accounting standards and they have grown up with regulatory concerns and all those sorts of things, but they haven't grown up with the precise knowledge of how cyber criminals could attack and do attack their organisation. So their knowledge is not something that is in their soul, it's something they have had to acquire. By contrast, cyber criminals have often grown up from a young age with the intent to make money by, or disrupt something or make a political point by way of attacking technologies. The intuitive feel for the subject is just not there in boards and audit committees. Of course, the people who sit on boards and audit committees are perfectly capable of learning it – though given their busy jobs it is unlikely that they can stay on the edge of the curve.

ACI: *This is interesting because one of the great advantages of non-executive directors is that they bring additional wisdom and experience to the board – but perhaps not in this case?*
Brian Stevenson: Unless you have a grey haired person like me who's been through a cyber attack, you need much younger people who've probably grown up in the IT industry. They may have little knowledge of banking for example but would have great questions to ask as an audit committee member about the level of cyber awareness within the business and cyber security and cyber defences and all those things. For companies where cyber is very high on the risk register, traditional board members might be supported by new appointees with specialist skills. There are some very good examples of this in banking.

ACI: *So is cyber as high on the agenda as it should be?*
Brian Stevenson: I think it's not as high on people's agenda as it might be because consumers don't worry too much about it. There are various surveys done that show that, even on things like identity theft, most people don't worry about it as much as they should. I think part of the problem is that if you suffer some sort of data loss or identify theft, the organisation that has been vulnerable to that attack (i.e., where your information has been stolen from) puts it right for you. As an individual, you very rarely suffer a financial loss and therefore the attitude of the general public seems to be one of "it's not my problem". It might cause a bit of disruption to my life but it's not going to cost me any money.

Another contributing factor is around transparency. There isn't an easy way of understanding just how much cyber crime costs business. The government have come up with a figure of, I think, 27 billion – but I've no idea

how they arrived at that number. Cyber losses are not just the actual loss of money, but the cost of lost data, fines and reputation which impact future opportunities. And it isn't always clear whether an organisation has suffered a loss – at least not immediately clear. For example, intellectual property might be stolen and the first thing the company knows about it is when a rival product suddenly appears on the market.

This comes back to design of IT systems. So, with old systems, criminals can get into the system, steal information and leave again, and there is no way of working out that they have been there and gone. On newer technologies there is – so as part of your cyber defence it is critical to keep your technology up to date and capable of tracking attacks. If the risks are to be properly assessed, then you need to have the right information and that means you need IT systems that are fit for purpose.

In the cyber attack I lived through, they went into systems and left again and we didn't know they had been and gone. It was only found out when traditional accounting showed a mismatch between the money that clients were actually drawing out and the money that was being drawn out. It was well organised – they were taking money out of cash machines in many countries around the world simultaneously.

ACI: *Presumably the design of IT systems is, to a large extent, reactive. How easy is it to keep on top of the emerging risk?*
Brian Stevenson: The only way you can really keep on top of the emerging risk is to be monitoring what criminals are writing about. There are a lot of black areas within the internet where criminals exchange information. You need to know what's going on and to some extent you are reliant on the law enforcement organisations sharing information about emerging threats with the business community. Some of this may not get discussed at an audit or risk committee, you may have a sub-committee where only key individuals share information that's been given to them by the police or governments and so on.

ACI: *So the information flows from the law enforcement agencies to companies is important; but what about companies disclosing information about cyber crime with investors?*
Brian Stevenson: It's about balance. As a bank you have to tell the regulator immediately that you have discovered something. There is always a flow of information to the regulator and then you go into a period of cooperation with the regulator to help solve the problem. Hopefully the regulator doesn't then fine you for it – but often they do.

The fines are normally at their worst when customer data has been disclosed to third parties and is circulating on the web. The remediation costs can often far way outweigh the fines, because you have to remediate every single customer. This is not just a banking issue. You are still vulnerable if you are (say) a utility company and have the credit card details of bill payers.

The current pattern appears to be that you disclose that you have been attacked but you wait three to six months until you do it. This is not unreasonable because it takes you quite a lot of time to work out the severity of the attack and the magnitude of the losses and the contingent losses related to it.

If you declare it too early, investors will be asking you lots of questions you won't be able to answer and then they will conclude that you don't know what you are doing. There has to be a period of time to collect all the information, to understand your vulnerabilities and crucially to rectify your weaknesses. If you disclose before you've fixed your vulnerabilities you are in effect opening the door to the whole criminal world. It's a delicate balance but I think one of the ways of dealing with it is by time deferral.

ACI: *Any other thoughts for audit committees?*
Brian Stevenson: I think there has been some progress in recent years and the risks associated with technology are creeping up the agenda. However, there is a long way to go. The benefit of having a web enabled organisation was sold to boards a long time ago; but arguably the downside risk was unknown at the time. It wasn't until attackers got better organised and started exploiting the fact that you now have an electronic window into your back office did boards wake up and see the risk. And I still don't think they see it clearly enough. In a competitive world there is a huge temptation to pursue the opportunities presented by web based technologies without paying due regard to the threats. The threat has to be managed; it has to be managed through your infrastructure.

ACI: *So, again it boils down to understanding the risks involved and whether the systems for managing those risks are fit for purpose and working as intended.*
Brian Stevenson: In the past I have spent a week sitting on the desks in the cyber crime unit of the IT function to see what they were doing. If you are my age you can have no idea about the activity that is going on in the black web, and you have no idea what the capability of the technology is and you have no idea about how people can exploit gaps and loopholes in technology. It's just not a world I have grown up in. So, it's like learning another language, you have to immerse yourself in it to get good at it. And even then you still need assistance from the specialists.

ACI: *That's a very good point. We often talk about audit committees kicking the tyres of the business, but I think few of us have really thought about that in a technology context.*
Brian Stevenson: It comes back full circle to where we started. Technology is such a huge part of the modern business world. Whether you are a bank, a retail business or running a power station, the business will be at risk from the five different types of cyber attacker. For some the risk profile will be higher than for others; but it is hard to think of any organisation that wouldn't be vulnerable to at least some form of attack. ❖

Richard Doern Grupo Stefani (Brazil)

Richard Doern has over 25 years of experience leading organizational transformation processes for over 75 companies, of all sizes and market segments, both in Brazil and abroad. As a Director certified by IBGC, Mr. Doern has served as Chairman and coordinator of audit, strategy and governance committees. Currently, he is a Board member and Audit Committee coordinator at Grupo Stefani (transport and logistics), Board member and Strategy Committee coordinator at Grupo Tiradentes (group of for profit universities) and Board member at Kinoplex (movie theaters chain). He specializes in corporate recovery (turnaround management), having been one of the precursors in the country to act as interim CEO during critical phases of restructuring.

"Continued education for all board members is essential to stay up to date on cyber security."

ACI: *What is the mindset that boards need to have today about the cyber risk environment?*

Richard Doern: The increasing access to technology by employees results in greater vulnerability for companies and the inappropriate use of applications, platforms and mobile devices can put classified and important information at risk. I believe that directors must be more aware of the importance of including this topic on the boards` agenda. This subject is still not considered as strategic or relevant by most directors. The overwhelming number of topics to be covered, the scarce amount of time for meetings and, specially, the lack of deep knowledge about this subject by directors result in cyber issues remaining more restricted to the IT area and its professionals.

Another important issue that directors must ponder is high employee turnover. Besides the difficulty of maintaining operational procedures, this factor increases the risks because classified information can be taken from one company to another.

ACI: *What are the 3 or 4 key messages that CIOs should be communicating regularly to the board?*

Richard Doern: One very important consideration is that the desired profile of CIOs is changing. Years ago, the role of the IT department was more restricted to back-office, infrastructure and support, but due to the current stage of extensive access to technology and the relevance of this topic to business, IT needs to play a more strategic and risk management role. Today's IT professionals need to build knowledge on business processes and innovation to be able to anticipate scenarios and propose advanced solutions, rather than acting only reactively.

In this sense, the main messaged that CIOs should communicate must be related to innovation, new applications and technologies that provide productivity, having already evaluated and mitigated the respective risks. Considering that members of the board and the audit committee often do not have deep knowledge in this area, the involvement of IT professionals in mapping the risks and in defining mitigation measures becomes essential.

ACI: *How should CIOs be communicating with the audit committee/board about cyber security?*
Richard Doern: Besides simple and brief periodic reports – that could be monthly or bimonthly – informing about the status of monitoring and mitigation of the identified risks, the CIO should be present in at least one board meeting every year, also to help engage this topic in the strategic agenda and show its relevance. It is also important that directors know the professional that occupies the position of head of IT and have access to him/her when necessary.

ACI: *How are "mobile and social" technologies impacting the way you look at/manage cyber risk?*
Richard Doern: Previously, IT was more centralized and standardized, and had less flexibility. Hence, its supervision and control were much simpler. Today it is more and more decentralized. Each area of a company, aiming at increasing its processes efficiency, needs devices and software tailored to their needs. This situation results in a huge amount of applications, platforms and devices contracted by a company, making it more difficult to monitor and control the related processes.

Another important point is the wide dissemination of cloud computing. Companies file more and more important documents in clouds and many employees have access to this information with a simple password. This is followed by – and is also a result of – the increasing remote work and, as a consequence, the need for remote access by users and the increasing use of mobile devices. This set of new technologies, on the one hand, promotes greater work productivity, but it also increases companies' vulnerability regarding information security.

On the boards I serve, we are always attentive to the implementation of policies and procedures for the use of mobile technologies and social media to minimize risks. The board's role is essential in monitoring the effectiveness of policies and procedures implemented.

ACI: *Statistics indicate that "people risk" is a huge cyber security factor. Are there tone and culture issues that companies should be communicating and boards monitoring?*
Richard Doern: Yes, I believe that measures in this sense indeed help. It is very important to make people feel part of the company, especially nowadays, when the commitment to the company that existed in the past is almost nonexistent. Turnover, particularly in the middle-management level, brings considerable vulnerability to the security of information that is increasingly socialized. Besides, high turnover results in difficulty to maintain continuity of processes and technologies used by the company. In many cases, a new professional will try to adapt the processes to their own habits from previous jobs or will try to implement new technologies, different from those used by the company, with which they are more familiar.

Frequently, it results in lack of continuity of processes and lack of company historical information. One example would be a new business intelligence professional who, used to work with a certain software from a previous job, suggests to switch the currently used software. A change like this seems simple at first, but requires great efforts to adapt to the company`s network, security standards, a new policy for users, etc. Multiplying this by all possible technology changes, it can result in endless work and investment, besides compromising security and information reliability.

ACI: *How concerned should boards be about cyber risks posed by the company's business partners/ vendors along the extended supply chain?*
Richard Doern: This must be a point of concern, especially for companies whose policy is to outsource all activities that

are not core. Once again, policies, processes and procedures must be comprehensively implemented and monitored. This is where internal controls can contribute considerably.

ACI: *Do you see a role for Internal Audit in helping to identify cyber security vulnerabilities and improvements?*
Richard Doern: Absolutely. Internal audit must be the structure responsible for monitoring the compliance with all the company`s processes and policies, including those related to the use of technology and information security. In addition, I recommend that internal audit be subordinated directly to the audit committee and have the adequate authority to report possible changes in identified risks.

ACI: *What are the critical elements of a good contingency plan in the event of a major cyber breach?*
Richard Doern: In the first place, I believe that a contingency plan must be defined during the risk management process. Having a good understanding of the business, the industry and critical risks, the board should define a contingency plan that meets the market needs. The plan should be maintained by top management and put in practice in case of extreme situations, and not depend on board meetings to resolve last minute urgent issues. I believe that the most important element in extreme situations is to act fast. It is not possible to call a board meeting to decide what should be done in these situations. The CEO has to have autonomy enough and previous authorization to act in these cases – of course following the existing approved plan.

ACI: *Do you see audit committees having a particular role to play (versus the full board) in overseeing the company's cyber security efforts?*
Richard Doern: Yes. I believe the audit committee should include this topic in its regular risk management process, together with the management of other risks.
It is important to highlight that audit committee members do not usually have enough knowledge in information technology and security to dig deep in this specific subject and I recommend the work of external consultants to help.

ACI: *Expertise and IT risk awareness on the audit committee/board seem to be an ongoing challenge. What are your thoughts on having IT expertise on the audit committee/board, and providing ongoing education to directors?*
Richard Doern: In my opinion, the presence of an IT expert in the board or audit committee can be very helpful. However, I have some doubts about the general contribution of this professional to the many other strategic topics covered by the board/committee. An IT expert hardly has knowledge enough in other areas to contribute in a relevant way to the various decisions made by boards.

As an example, a member of the audit committee who is an accounting expert can extraordinarily contribute to this subject and to the audit committee in general. However, in a board meeting, this subject represents about 25 percent of the covered topics. The contribution of an accounting expert to the other 75 percent is usually limited, since he does not have enough knowledge in extremely important themes as strategy, human resources, etc.
In most boards, IT related subjects still represent a small part (even smaller than accounting) of the board and the audit committee`s agenda – and I believe there will be no relevant change in the near future.

Certainly, IT is core to some industries and they will have a greater need for an expert in this area, but I believe that for the others, bringing in external professional or consultancy to help seems like the most appropriate measure. Besides, it is certainly necessary to have a program for constant update of the directors. As most of them are not familiar with IT, it is essential that they be updated about new technologies and in this sense CIOs can help by making presentations and providing materials to the board.

ACI: *Other thoughts for audit committee members/ directors to help them get their arms around cyber risk?*
Richard Doern: A couple of thoughts, which go back to some points that I've touched on. It's clear that cyber security needs to receive more attention and time on the board`s agenda – and it should not be completely delegated to the audit committee. It is important to bring it to the board periodically, stressing its importance to the organization.

Be attentive to the change in the CIO profile, which should be more strategic, and invite the CIO to participate in at least one board meeting a year. It is important that directors know the CIO and have easy access to him, and also that the CIO feels comfortable to contact board members to inform about new technologies and risks involved, when necessary.

Continued education for all board members is essential to stay up to date on this subject. One helpful measure is to create a glossary with technical terms and expressions, and to make available simple literature for board members.

Make sure the company is monitoring social media; it helps to have a professionals focused on this work.

Be clear about the roles of the board, the committees, and the CEO, CFO, and CIO in responding to an eventual crisis related to cyber security.

Finally, the investments to mitigate IT risks are huge. These investments do not generate any revenue and consist of technologies that will be obsolete in no time. Thus, great efforts are required to convince board and executive directors who have less knowledge in the subject to approve these kinds of expenses. ❖

Sridar Iyengar Dr. Reddy Laboratories and Infosys (India)

Sridar Iyengar is Chairman of the audit committee of Dr.Reddy Laboratories. He also serves on the board of ICICI Ventures, Rediff.com, Murugappa Group, Mahindra Holidays, Cleartrip, iYogi and other companies in the U.S. and India. He has previously served on the boards of Infosys and ICICI Bank where he was chairman of the audit committee. He is also co-Founder of The Sounding Board, a network of business leaders and entrepreneurs who advise growth-ready companies in India.

"Cyber risk needs to be tackled on the highest strategic level because of its potential impact."

ACI: *Is there one particular instance/example of a cyber security breach that was a real "eye opener" for you in terms of its potential impact?*
Sridar Iyengar: I am aware of a number of high profile incidents in the headlines, but I faced a personal incident as well that brought cyber-attacks starkly home to me.

The attack was simple and at the same time sophisticated. It was a planned and targeted attack. Someone had deliberately hacked my email account and studied my email contacts and – to cut a long story short – persuaded my bank to transfer money to a bogus corporate account from which it was withdrawn immediately in cash. It all happened over a 24/36 hour period. The hacker found out from my emails that I was in a different time zone, knew who my contacts were at the bank, the location of corporates I could logically be dealing with on a personal transaction, etc. Using that information and by simply intercepting, diverting and responding to emails from bank personnel seeking to contact me, the hacker was successful in extracting money from my bank account. Only coincidence alerted me to the hacking while it happened. Too late to stop the transaction but in time to stop the cover-up which would have removed all traces.

This personal incident has some similarities with some of the high profile incidents recently in the headlines. The malware was similarly able to infect user interfaces (my email account) and extract credit card information (my contacts, bank details). Also, the attack came to light only after fraudulent transactions were made using the information that was extracted. But not all attacks originated from online transactions, or something on the internet. This shows that the virtual world and the real world blend and the risks are crossing over. How and when do we know that we have been compromised is therefore a key question one needs to ask. As more personal information and financial transactions go online we will see more and more attacks in the future.

ACI: *How high is cyber risk on your company's risk map and board/audit committee agenda?*
Sridar Iyengar: Information security is extremely high on our agenda. Cyber risk needs to be tackled on the highest strategic level because of the potential impact to reputation, stock prices, etc.

We focus on the education and awareness levels of employees, their culture of compliance to policies and procedures and adherence to both the values and hygiene of good cyber practice. On all the boards I reside, we require recurring information updates on our defences, preparedness, response times and ability to counter and stop attacks. We also encourage the use of ethical hackers to do penetration testing on a regular basis.

ACI: *What are the top three challenges you face when dealing with cyber security risks?*
Sridar Iyengar: My top three would be as follows: being able to stay ahead of the increasing sophistication of cyber-attacks; the pace at which new risks appear and our ability to deal with such risks; and overall general awareness among employees, customers and general citizens of the threats.

ACI: *How should oversight responsibilities for cyber security risk be allocated – i.e. to the audit committee, board, or other committees of the board?*
Sridar Iyengar: Cyber security risk oversight should not just be an audit or a risk committee responsibility. It's a business issue and the entire board should spend dedicated time to become aware of the risk perception, threats and the company's preparedness to deal with them. The audit committee, unless there is a specific information security committee, could however be delegated the responsibility to ensure that the right programs, internal processes, education, testing and reporting are in place.

ACI: *What are the critical success factors in cyber risk governance in your view?*
Sridar Iyengar: Success in this area cannot be defined as the absence of attacks or the successful defence against one. It is a dynamic evolving area. Cyber security should therefore be managed at all levels to have effective governance. As mentioned earlier, the board and the audit committee should proactively engage in cyber security risk oversight. Business leaders should be responsible for cyber security issues. Governance should focus on ensuring that both the people and the systems supporting them are ready at all times to face threats. Therefore, regular reinforcement of the corporate values, education and upgrading of skills, awareness building, upgrading of systems, testing and retesting of defences are the critical factors. The board should ensure that programs and processes are in place for each of these areas and are operational at all times.

ACI: *What do you expect to see from management in terms of policies and procedures and, more specifically, in terms of information provided?*
Sridar Iyengar: Management has the responsibility to protect information belonging to the company. So they need to articulate the risks, how they are educating employees about them and what provisions they have made for a comprehensive framework for cyber security to prevent, detect and remediate any incidence of breach.

In the event of an actual breach, management must not only report the incidence and its disposition but show that they have done a root cause analysis and modified policies or practices necessary to prevent new occurrences, not only in the area of the incidence but everywhere in the corporate network. It is management's responsibility to give the board and/or the audit committee the necessary assurance that information security is a company-wide priority at all times.

ACI: *Do you see the interaction of the audit committee/board and engagement with the CIO changing/evolving – and if so, in what way?*
Sridar Iyengar: Cyber security is a business issue and business leaders must own it. The CIO's function is to support the business leaders by provisioning the most appropriate hardware, software and people necessary to achieve protection consistent with having the least friction to business needs. The role of the audit committee is to understand the risks involved, balance the business needs with the cyber security imperatives and support the CIO and his team in operating an optimal cyber security framework. Therefore, it is imperative that the CIO and the audit committee collaborate and communicate proactively and frequently.

ACI: *How would you expect internal and external audit to cover cyber security risks?*
Sridar Iyengar: Part of internal audit's function is to ascertain whether all policies and procedures of the organization are followed in practice. The cyber security framework of the organization will have its own policies and procedures. Under its audit plan as approved by the audit committee, internal audit should regularly test that these policies and procedures and the necessary controls they entail are operating as designed and should report any significant findings to the audit committee. Audit committees should ensure that internal audit has the requisite skills to do this work itself or through other qualified external experts.

External experts/auditors can provide the board and audit committee with information and recommendations that reflect leading industry standards and also share experiences gained though their interaction with companies.

ACI: *Do you feel audit committees currently have the necessary cyber security skills and knowledge required to assess audit plans and reports on this matter?*
Sridar Iyengar: In my experience, audit committees are aware of both the general need for a robust cyber security framework and the specific areas of information whose leakage could cause the most harm to the organization. But they are unlikely to know or grasp the details of the information interdependencies, the robustness of the technology infrastructure or the required competency of the people involved in providing the protection layer against any breach. Having people on the committee who are knowledgeable in this area clearly helps. This is one reason audit committees are increasingly requiring specialists to staff up in this area.

ACI: *Some larger organizations, primarily financial institutions, are increasingly disclosing cyber-attacks in their regulatory filings. How do you feel about such disclosures?*
Sridar Iyengar: Yes, many banks disclosed such attacks in their annual reports, even in cases where the attacks did not result in any material harm to the institution. As someone who believes more disclosure is always better, it's a step in the right direction. As these incidents become increasingly important from a business risks standpoint, it's good that they are being disclosed. ❖

Jan Zegering Hadders Ageas (Belgium)

Jan Zegering Hadders is chairman of the audit committee of Ageas and also serves as member of the corporate governance committee. He is also member of the supervisory board of GE Artesia Bank and chairman of the audit committee of GE Artesia Bank, amongst others. He also served as chairman of the supervisory board of Grontmij N.V. and as chairman of the board of directors of ING Netherlands.

"People will always keep stealing money, only the techniques change based on the systems we use."

ACI: *Do you have any experiences with cyber attacks?*
Jan Zegering Hadders: Being active in the financial sector, of course I have come across both organized and petty criminals out there trying to steal money from the system.

Stealing money from banks or systems is not new. It happened 600 years ago. All kinds of movies show how it was done, from robbing a post train to blowing up a vault to hacking into the financial system. People have always stolen money and will always keep stealing money, only the techniques change based on the kind of systems we use to store and transfer money.

ACI: *What are the main challenges audit committees face when dealing with cyber security risks?*
Jan Zegering Hadders: Companies, certainly in the financial sector, should take cyber security very seriously and defend their systems in the most modern way or they will find themselves outsmarted by cyber criminals.

IT systems and cyber attack defence systems of financial institutions are usually very sophisticated already but criminals prove to be very intelligent in finding new and more innovative ways to attack. If your defence systems do not factor in the latest cyber attack innovations, you are vulnerable to attacks. As such, an important challenge for audit committees is seeking to ensure that management has its systems and controls up to date and equipped to be one step ahead of the cyber criminals.

ACI: *Is having the right expertise on board a significant challenge?*
Jan Zegering Hadders: By now, virtually every bank and insurance company have built up specific knowledge on preventing cyber-attacks and to minimize the amount of money being stolen from their systems. That knowledge has been mainly acquired from attacks in the past – from lessons learned.

The audit committee is of course not involved in day-to-day management of the company and therefore cannot have detailed knowledge about the specifics of IT and cyber security systems. But in general, I personally do not see many people with specific detailed expertise in cybercrime on the audit committee or board. I do see audit committees getting more and more knowledgeable about the basics of cyber risk. Also, audit committees more proactively request information from management

about the risks and the maturity level of the defence systems to be able to properly assess whether the company is up to speed in preventing at least the most significant cyber attacks.

With audit committee members having a good basic notion of how cyber attacks work and together with specific expertise and focused information from management and external experts, the audit committee should be able to ask the right questions to management, focused on the key risks.

Of course, one could say that specific expertise is still missing in the audit committee, depending on the company, but it is the role of the audit committee to request help in getting that extra expertise, from the CIO or CRO, or external experts.

ACI: *Where to draw the line in defending against cyber criminals might be a challenge on its own…*
Jan Zegering Hadders: Companies have to consider whether the cost of defence is still in balance with risk exposure as a whole. Finding the right balance is indeed an important and difficult challenge the board and/or audit committee needs to consider. Credit card systems for example: Credit cards defence systems do not aim to be equipped to prevent any money being stolen. From an overall risk management perspective the risk of having to reimburse customers for amounts stolen is reflected in the price of the credit card.

ACI: *How high should cyber risk be on the risk map and the board and/or audit committee agenda?*
Jan Zegering Hadders: Usually cyber risk is high on the agenda of the audit committee and/or the board when their company has been attacked or when internal auditors or others have reported major vulnerabilities based on their test work.

I am highly in favour of a more proactive approach also being aware of emerging risks, asking the right question well in time so you also get the information upfront to put pressure on management.

On the other hand, many wonder why cyber risk it is not higher on the risk agenda than it is today. There is logical reason for that in my view. Customers are aware that crime is there every day, every hour, every second and they have accepted it in a way. And of course every financial institution is sensitive to negative publicity and reputational damage, but as long as individuals are not harmed because any damage is reimbursed, the reputational risk related to cyber might be considered fairly low. Because of the relaxed attitude of customers towards cyber attacks, the risk a company is willing to accept might be higher that one would initially expect.

ACI: *What specifically do you expect from management related to cyber security?*
Jan Zegering Hadders: Of course it is nice to hear the people in IT dealing with cyber security in the audit committee and of course cyber should have a place on the risk map and receive the dedication it needs from management based on its relative risk grade. The most important is that management and the company have the right level of expertise to effectively deal with cyber risk.

If cyber has to find its way higher up to the audit and/or risk committee agenda, it should definitely also be higher on the radar screen of C-levels. One of my expectations is to see cyber security being reflected in a formal KPI for chief executives and not only for middle management working on it on a day-to-day basis. Making C-levels formally responsible to ensure cyber security for customers and the company is an important aspect from a broader governance perspective. ❖

KPMG's Audit Committee Institutes around the world


Argentina


Chile


Israel


Nigeria


Singapore


Australia


China


Luxemburg


Northern Ireland


South Africa


Austria


Denmark


Malaysia

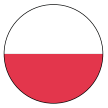

Norway


Spain


Bahrain


France


Malta


Poland


Switzerland


Belgium


Germany


Mexico


Portugal


Thailand


Brazil


India


Netherlands


Qatar


United Kingdom


Canada


Ireland


New Zealand


Russia


United States of America

Contact the ACI

Timothy Copnell

Tel: +44 (0)207 694 8082
e-Mail: tim.copnell@kpmg.co.uk

Wim Vandecruys

Tel: +32 (0)11 28 66 31
e-Mail: wvandecruys@kpmg.com

Oliver Marketing for KPMG I OM013875A I March 2014

www.kpmg.com/globalaci