Cyber security: a failure of imagination by CEOs

KPMG International

kpmg.ca/cyber

Global CEOs walk a fine line between risk and reward

A senior executive at an oil and gas company clicks on an email with a picture of his daughter scoring a goal in last week's soccer game. Two years later, the executive learns that photo was embedded with malware that allowed an attacker to log every keystroke on his desktop, including every email he sent. The cyberspies took screen shots periodically and they turned on his video camera and microphone, giving them eyes and ears to what was happening in the C-suite. The company had bid in a number of closed auctions for oil rights but always seemed to come in just under the winning bid.

A maker of home monitors advertises a brilliant new feature for customers: control your thermostat, your lights and your security system with your smartphone! However, the technology is so easy to use that a group of local thieves hacks the system to engineer a series of break-ins. A simple change to the system's security and log-in procedures could have prevented the hack.

A retailer learns the hard way that an international hacking network has been quietly siphoning every credit and debit card sale processed at its stores for months. The C-suite and board learn about the breach from government investigators, and the news is publicized before they have a chance to contain the breach or deal with the aftermath. Sales plummet, class-action suits follow and the CEO resigns.

Better prevention might have helped in all these cases, but it would not have been enough. While it's important to build better security into the products and the processes, gaining more visibility into who is attacking and having a plan for mitigating threats when they are detected are just as important.

Technology is enabling companies to connect with their customers in ways no one could have imagined a decade ago through: smart devices, the customized marketing and products and automated services that have streamlined back offices as well as offered more immediate and personalized services to customers. We can now do most of our banking transactions through a computer that we carry in our back pocket.

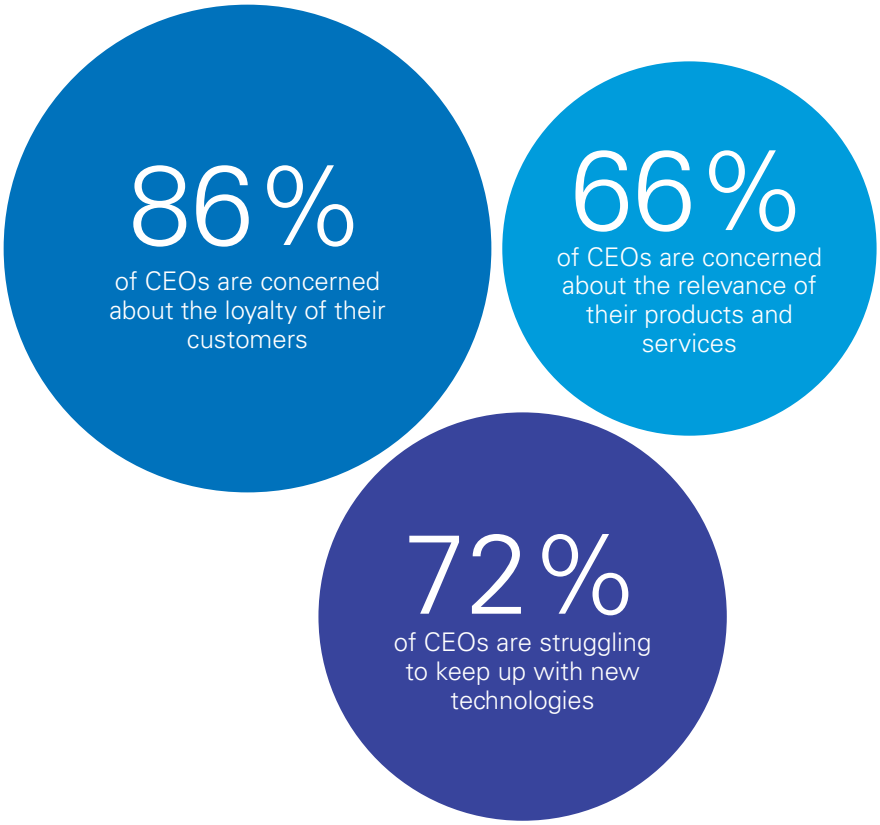
But innovation almost always runs ahead of security. And the bad actors are innovating as well. One of the most innovative marketplaces in the world is the dark net, which supports organized crime as well as basement hackers. Every day there are new tools, new attack services and new cash-out strategies being developed and shared. Everything is changing: the compromise points, the risks and the consequences.

What keeps CEOs awake at night

Keeping data safe is no longer an afterthought at most organizations — whether it's customer data, IP or the more mundane data necessary to run the company. KPMG International recently surveyed over 1,200 chief executives from many of the world's largest and most complex companies and discovered what keeps them awake at night: Two-thirds are concerned about the relevance of their products and services, three-quarters are struggling to keep up with new technologies and nearly all are worried about the loyalty of their customers.[1] Cyber security is closely tied to customer loyalty and trust as well as innovation. A breach can seriously undermine consumer confidence and damage brand reputation.

"In fact, building cyber security into products and processes can be a competitive advantage," says Malcolm Marshall, Global Head of Cyber Security at KPMG. "Some organizations are turning security into a selling point with touch identification," he explains. Banks, for example, are starting to replace clunky security processes with touch ID. "If you are able to authenticate your staff and your customers to very high levels of certainty, it means you're able to provide much more tailored levels of service," he explains.

[1] See survey methodology at the end of this report.



Source: 2015 KPMG CEO Outlook, May 2015.

Every company is a cyber company

One of the biggest mistakes an organization can make is regarding cyber security as something that is purely the domain of the CIO. "The CIO has a very important role, but as more businesses use digital as their route to the customer, they are not always engaging with cyber security experts," says Marshall. "Many senior executives don't appreciate the level of technology that is embedded in their products," he says. "Nor have many C-suite executives thought through the creatively devious ways that cyber criminals might exploit their products or services." Cyber crime is not as well understood as conventional crime.

Ultimately, it's a question of product integrity and reputation and that is a board-level concern. Institutional investors, for example, are less likely to invest in a company that has had a major public cyber breach. That can impact share price as well as the ability to raise capital.

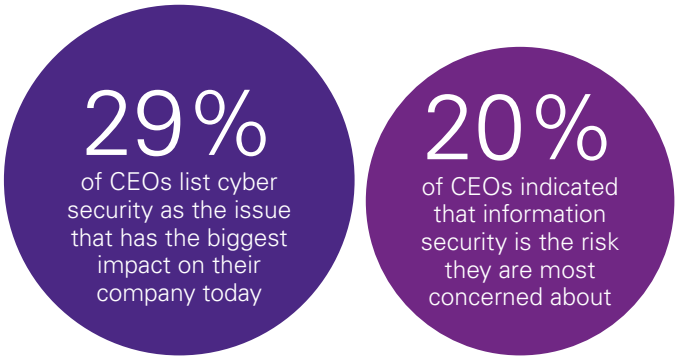
> "Collectively, we sleepwalked into a position of vulnerability and failed to learn lessons of embedding security into products right out of the gate."
>
> — Malcolm Marshall
> Global Head of Cyber Security at KPMG

The bottom line: Every company is now a cyber security company and every company needs to keep an eye on security.

Cyber security: a strategic risk

C-suite and board members traditionally have viewed cyber security as a tactical problem, not a strategic issue. But over the past decade, there is a realization that cyber security can pose an enterprise-wide risk.

In the survey, nearly a third of CEOs list cyber security as the issue that has *the* biggest impact on their company today. One out of five indicated that information security is the risk they are most concerned about. Operational and compliance risk were listed as the top risks. But cyber risk, if uncontrolled, becomes an operational issue and a regulatory issue very fast.



Source: 2015 KPMG CEO Outlook, May 2015.

"Amongst public breaches the issue then becomes: I can't focus on my operations because I'm distracted by a cyber event," says Greg Bell, Cyber Security Leader for KPMG in the US. "Or, I have to stop part of my operations while I try to redress or remediate the cyber issue, and then I'm dealt with a number of complicated regulatory impacts and lawsuits," he adds.

Developing a framework for cyber risk

Reputational, regulatory and legal risks are a concern for all firms. For organizations with a physical infrastructure, the risks multiply. An attack can tamper with controls, destroy an organization's equipment, cripple operations and create liquidity risk. The attacks on state-run oil and gas companies in recent years have been a wake-up call to every organization in the energy and industrial sectors. Without the lines of credit and government guarantees of a state behind them, many would face liquidity problems within days if they were under similar attacks.

"Many organizations already have a framework for assessing enterprise risk, yet cyber risk is still treated differently than other risks," explains Marshall." That is a mistake," he says.

Take third-party risk, for example. Many organizations — particularly banks — have long thought about third-party risk. Some of them have now gone to multiple suppliers, so if one of their suppliers fails, they have resilience. But a deeper look might reveal that the risk gets reconsolidated at the next layer because all of their diversified suppliers are reliant on a single supplier — a phenomenon known as fourth-party risk. This discovery is common in assessing liquidity risk, but the process can be equally revealing for cyber resiliency. For instance, what if all of your suppliers rely on the same cloud provider?

"Every organization should have a framework for analyzing cyber security and that framework should ideally be integrated into an organization's existing enterprise risk framework" says Marshall. There are several frameworks organizations can use: *The Framework for Improving Critical Infrastructure Cybersecurity* published by NIST in the US, *Cyber Essentials* in the UK or the international standard ISO27001, which is the most common framework adopted globally. "The choice of framework matters far less than how it's integrated and implemented," says Marshall. "The key is that it becomes part of the mainstream of risk management within the organization."

Understand your enemy

A first step in this direction is understanding who might attack a particular enterprise, what they would attack and why they would attack. In short, understand your enemy (see sidebar on security intelligence). A framework can also help organizations understand which assets are most in need of protection and which could cause the most damage if they were compromised. "This helps focus investment and protection on the areas that would have the greatest impact on an organization," says Marshall.

Intellectual property is a crown jewel for most tech companies, for example. But what happens when a global business handles product design in one country, software development in another country and parts of hardware design in a third with suppliers located all over the world? The board at one such company identified IP as a going-concern risk. They determined that if somebody gained access to their IP, learned their plans for new product release or was

able to copy their IP it could threaten the existence of the firm.

The firm's weak point proved to be a facility that manufactured the most profitable product at the highest volume. A white-hat hacker hired by a consultant of the firm was able to gain access — in about 30 seconds — to all of the systems on the shop floor. The hacker had full control from a cyber security standpoint to everything, including the IP. Moreover, a moderately talented hacker could control every server, from the quality assurance programs to the manufacturing process. The CIO was not surprised by this discovery. He had tried to work with the manufacturing teams previously, but they were concerned that security controls would impede operations.

Aside from the potential for IP theft, the vulnerabilities meant that there was no integrity in the quality assurance program for the firm's most profitable product. In a class-action suit, a firm that has lost control of its quality assurance would have a hard time mounting a defense.

Another risk that is often overlooked comes in the form of mergers and acquisitions (M&A). Some organizations are learning the hard way that buying a company that has not built security into its products can be costly. In one recent case, the cost of remediating cyber security weaknesses was equivalent to 25 percent of the acquisition price. Due diligence by the acquiring firm did not uncover the weakness because there was no understanding of how critical cyber security was for a product meant to be used in vehicles.

Are you ready?

Half of CEOs surveyed say they are fully prepared for a future cyber event. Yet the survey revealed that only half of CEOs had appointed a cyber security executive or team and less than half had changed internal processes, such as data sharing.

More surprising was that only a third of organizations reported changes to external processes such as data sharing or transaction processing. Cyber criminals are circumventing the more robust security at large organizations by infiltrating their smaller suppliers and service providers with malware. The malware can then ride in on an invoice or sensor monitor.

Some of the most spectacular and well-publicized breaches in recent years were introduced by third-party vendors. Given the growing complexity of supply-chain management and the trend to having more connected equipment and processes, cyber security is something that extends across the entire supply chain — and your vendors' and sellers' supply chains as well. It is also an opportunity to turn cyber security into a competitive advantage. A robust and demonstrable security protocol can be a selling point for any company that connects to its clients on an open network, as the example in the last section demonstrates.

Yet the survey revealed that respondents in several scenarios are either not planning or have delayed planning of important security measures.

Plans to appoint a cyber security executive/team

Have taken preemptive steps	50%
Planning to take steps in the next 3 years	29%
Not planning to do so	21%

Plans to change internal processes (data sharing, device use)

Have taken preemptive steps	45%
Planning to do so in the next 3 years	44%
Not planning to do so	11%

Plans to upgrade current technology

Have upgraded current tech only/ have taken preemptive steps	37%
Planning to do so in the next 3 years	49%
Not planning to do so	14%

Plans to change external processes (data gathering, transaction processing, data sharing)

Have taken preemptive steps	34%
Planning to do so in the next 3 years	53%
Not planning to do so	13%

Source: 2015 KPMG CEO Outlook, May 2015.

Significant investment made in the US

There was a wide geographic disparity in the data for preparedness. How prepared you feel depends on where you are based. In the US, 87 percent of CEOs say their companies are fully prepared. Mandatory disclosure rules for compromised consumer data, a number of widely publicized breaches and an active government cyber agenda have raised awareness beyond what is seen in other regions. The US is a favorite target for cyber criminals and the attacks tend to make bigger headlines in North America.

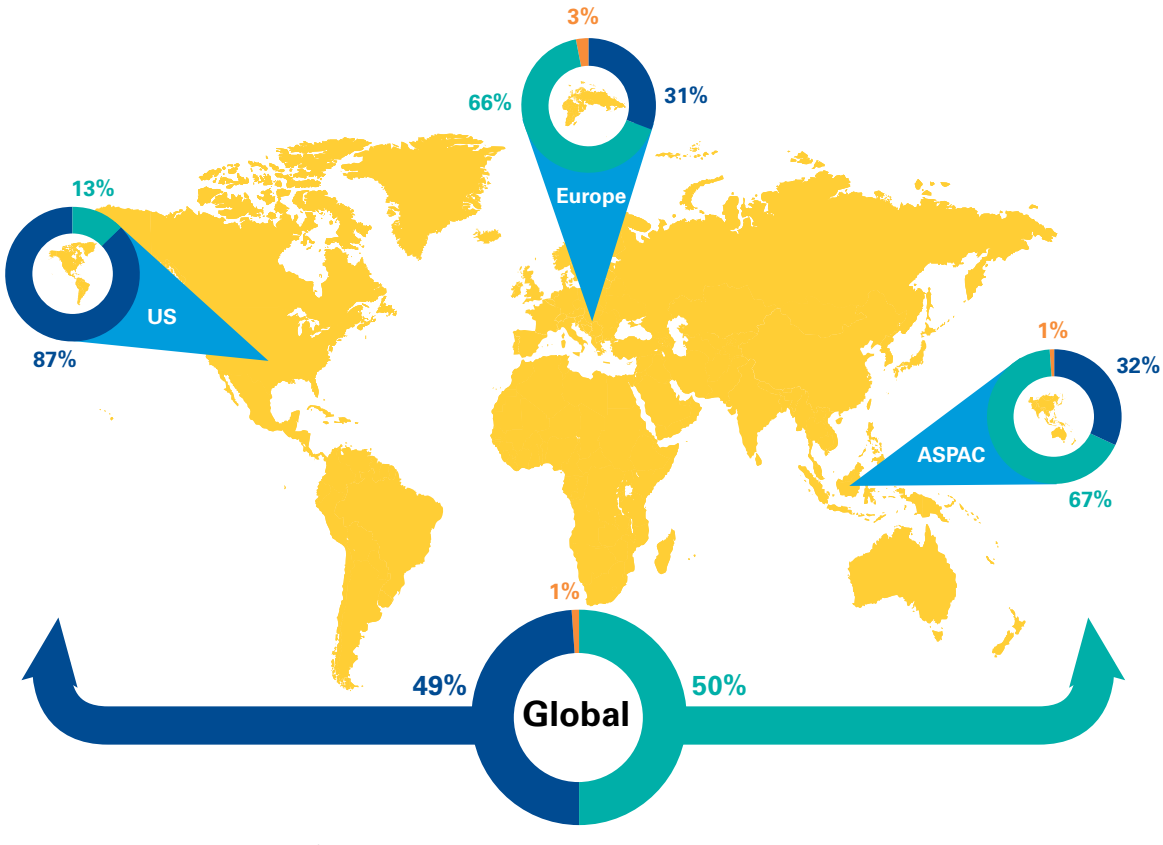
"Consequently, many organizations have indeed invested heavily in preventing an attack," says Bell. "But until recently, there has been too much attention focused on prevention and not enough on protection and response." CEOs are starting to ask: "How do we detect more quickly if we have a cyber incident, and how do we respond effectively?" says Bell. That preparedness makes the difference between those organizations that recover quickly from an incident and those that suffer a lingering impact.

> "The root cause is often a failure of imagination. A failure to imagine the sophistication and persistence of their attackers."
>
> — Malcolm Marshall Global Head of Cyber Security at KPMG

Caution in Europe

In Europe, less than a third say they are prepared for a cyber event. Many European organizations are in a state of flux. "The Snowden revelation gave many European CEOs reason to rethink and realign their cyber strategy and security measures," says Uwe Bernd-Striebeck, Cyber Security Leader for KPMG in Germany. "We see quite a number of European companies moving to domestic security providers and replacing US security tools and applications by European ones, or planning to do so in the near future."

"Many firms in the region are still at the beginning or middle of their cyber security journey," says Bernd-Striebeck. "They are looking for effective and cost-efficient security solutions that provide the best protection and put them into a position to handle cyber incidents adequately. Even if they have invested in security, European CEOs are less likely to declare themselves fully prepared on cyber security because they tend to be more cautious than CEOs in the US," he says.



Source: 2015 KPMG CEO Outlook, May 2015.

Asia: responding to the threat landscape

"In the Asia-Pacific region, the attributes that have accelerated preparedness in the United States are not as visible or progressed," says Dani Michaux, Cyber Security Leader for KPMG in Asia. Only 32 percent of CEOs reported their organizations are fully prepared on the cyber front. Governments are starting to review and provide more active leadership at an individual country level, privacy laws are being reviewed and businesses are now responding to the increasing threat landscape.

For organizations based in the Asia-Pacific region, there is a wide range of maturity levels and appreciations of cyber risk, from those just beginning to acknowledge and understand cyber risk, to those who are fully engaged with high awareness amongst the board and CEO about the importance of cyber security to protect and grow their business.

Beijing's goal of replacing US technology along with strict regulations around security products and services in China has had a huge sway on Asia's largest cyber security market.

"Many Australian CEOs and boards understand the importance of cyber security, however, often their understanding is not yet at a level that can drive action," explains Gordon Archibald, Cyber Security Leader for KPMG in Australia. Part of this is due to the lack of visibility and clarity of what needs to be done. "This falls with management who may sometimes struggle with building impetus to clearly define the problem — what am I trying to protect, what are my risks and how well protected are those assets?" he explains. They are aware of the threat but they don't always see the potential impact to the business and emerging technology.

Who you have is as important as what you know

Together these issues are creating a perfect storm on the talent side and a mounting skills gap is likely to worsen in the coming years. In the survey, CEOs who said they were not prepared for a future cyber event are more likely to be increasing their headcount over the next 3 years, and half of them expect a skills gap to emerge over the same period.

One of the biggest challenges is the sheer scale of the skills shortage. Global estimates suggest that over 23 percent of cyber security posts take more than 6 months to fill, with a further 10 percent remaining unfilled. The US Bureau of Labor Statistics estimates there are almost 300,000 unfilled jobs in cyber security in the country as of August 2015. This skills shortage is most acute for cyber security professionals who blend broader business, management, risk or social sciences skills along with technical savvy.

Finding good IT talent is a challenge for most organizations," says Marshall, and it's a particular challenge for any project that involves embedding technology into the customer experience. "Everyone understands that you need good security people at the back end," he says. "But to design new products, embed new technologies and launch into new markets with a high level of confidence, you need good security people at the vanguard, working with designers and marketers. You need talented people who can make sure the customer experience is enjoyable rather than a security nightmare," he says.

The business-savvy cyber executive

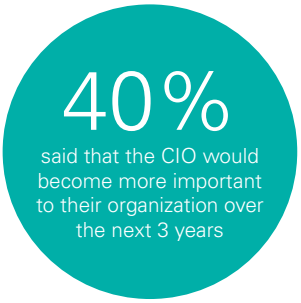
There is also a question of who is ultimately responsible for cyber security within the organization. In the survey, four out of ten CEOs say they expect the role of the CIO will become more important in the years ahead, but many CIOs are neither part of the C-suite inner circle nor are they respected as business partners. There is also an inherent danger that if a CIO is the only senior executive with responsibility for security, the rest of the organization surrenders responsibility to the IT function rather than making sure security is built into behavior and processes.

"Security needs a broader remit," says Marshall. "We would recommend that someone at the board level and a C-level executive, who is not the CIO, be given a wide responsibility to look at how cyber is integrated in the business from a risk point-of-view and also from an opportunity perspective," he says.

This will also send a message to everyone: security is not just an IT issue.

In many well-run companies there is a Chief Information Security Officer (CISO). Today that role typically reports to the CIO. But as companies recognize that cyber security is a business risk that impacts the whole enterprise, this is starting to change. A few CISOs now report to other C-level officers, such as the COO, the CFO, the general counsel or even the CEO in a few cases. Any company that recognizes the cyber risks in M&A and product design will also recognize that the responsibility should go all the way to the C-suite.

Of course, the reporting structure is only one part of a robust security profile. So much depends on the individuals who fill those roles. "It's almost too important to leave under a subject-matter expert," says Marshall. "If you have a strong leader — somebody who can inspire and lead talented subject matter experts — you don't need to have a security expert as your CISO."



Source: 2015 KPMG CEO Outlook, May 2015.

"The CISO should be able to have a meaningful conversation with the C-suite and the board," says Bell. Too many CISOs end up trying to explain these nuanced tech risks and it sounds like so much technobabble to a business audience. "If you have a cyber leader in your organization that can talk to you about business risk as an implication of a cyber issue, that's a much more effective conversation," says Bell.

The right tools

Organizations need to invest in the right tools, as well as the right people. They need visibility first and foremost, to know if they are being attacked. Without visibility it's impossible to identify holes in the security arsenal and weaknesses in infrastructure. There are organizations that have been compromised for years before they discover the damage.

One way companies can expand their expertise is by bringing in security intelligence to pinpoint problems, identify anomalies and highlight unusual or suspicious activity. Intelligence can help in two ways. First, an 'early-warning-as-a-service' can reduce the vulnerability threat window: the time between the detection and the remediation of an attack. Intelligence can also provide a broader picture of global threats than any one organization could gather on its own. Security is an ecosystem; organizations need to know what is going on externally, as well as internally.

Sharing threat intelligence

Organizations can expand their own intelligence by sharing information about their own security threats with peers and competitors. While this is a sound idea in theory, sharing information with competitors is not something many organizations are willing to do — yet. Most organizations are reluctant to share their weaknesses publicly and many never divulge their breaches, unless forced to do so by law. Financial institutions are an exception: the financial infrastructure is so interconnected that institutions are more likely to act on the idea that they will all sink or swim if there is an attack. But many other industries don't yet have a culture of sharing.

Another way companies are dealing with this is to create collaborative networks — offering rewards to white-hat hackers, for example. White-hats are computer hackers who use their powers for good, not evil, by helping organizations find weaknesses in their architecture. Executives who employ them are often surprised at how quickly an accomplished hacker can infiltrate their systems, often within a matter of minutes.

There is no such thing as complete security coverage. Organizations need to develop a proactive and predictive approach to cyber security, instead of relying too heavily on reactive technologies such as firewalls or intrusion prevention. Constantly testing for weak spots is one way to stay ahead of bad actors. Understanding the threat landscape and knowing your enemy with security intelligence is another. What you can't prevent, you should try to detect. And what you can't detect, you should be prepared to respond to quickly.

The four golden rules of cyber security

Get the basics right.

Over 75 percent of attacks exploit failures to put in place basic controls.

Look after your crown jewels.

You have to prioritize where you spend your money to defend yourself, so build a fortress around your most critical assets.

Do your homework on your enemies.

Invest in understanding who might attack you, why and how, so that you can anticipate the most likely scenarios and defend those assets that are most likely to get attacked.

Treat cyber risk as an opportunity to look closely at your business.

Security and resilience can affect nearly every part of an organization. Strategies to protect IT security and business resiliency should align with an organization's broader goals — from protecting intellectual property to maximizing productivity to finding new ways to delight customers.

The most innovative companies have recognized that cyber security is a customer experience and revenue opportunity, not just a risk that needs to be managed. They are finding ways to turn cyber preparedness into a competitive advantage rather than a cost, building security into new products and services at the design stage and realizing that cyber security is not an IT issue: it must work across the entire organization and the ecosystem.

Methodology

The survey data published in this report are based on a survey of 1,276 chief executives from Australia, China, France, Germany, India, Italy, Japan, Spain, UK and the US. Nine key industries are represented, including automotive, banking, insurance, investment management, healthcare, technology, retail/consumer markets and energy/utilities. Three hundred forty-seven CEOs came from companies with revenues between US$500 million and US$999 million, 626 from companies with revenues from US$1 billion to US$ 9.9 billion, and 303 from companies with revenues of US$10 billion or more. The survey was conducted between 22 April and 26 May 2015.

Contributors

Malcolm Marshall
Global Head of Cyber Security

Greg Bell
Cyber Security Leader in the US

Dani Michaux
Cyber Security Leader in the ASPAC region

Uwe Bernd-Striebeck
Cyber Security Leader in Germany

Gordon Archibald
Cyber Security Leader in Australia

Contact us

Global

Malcolm Marshall
Partner and Global Cyber Security Leader
E: malcolm.marshall@kpmg.co.uk

Americas

Canada

Francis Beaudoin
Partner and Cyber Security Leader
E: FBeaudoin@kpmg.ca

Latin America

Frank Meylan
Partner and Regional Cyber Security Leader
E: fmeylan@kpmg.com.br

United States

Greg Bell
Principal and Cyber Security Leader
E: rgregbell@kpmg.com

Asia Pacific

ASEAN (Indonesia, Malaysia, Philippines, Singapore and Brunei, Vietnam and Cambodia

Dani Michaux
Partner and Regional Cyber Security Leader
E: danimichaux@kpmg.com.my

Australia

Gordon Archibald
Partner and Cyber Security Leader
E: garchibald@kpmg.com.au

China and Hong Kong

Henry Shek
Partner and Cyber Security Leader
E: henry.shek@kpmg.com

Japan

Atsushi Taguchi
Partner and Cyber Security Leader
E: atsushi.taguchi@jp.kpmg.com

Europe, Middle East and Africa

France

Laurent Gobbi
Partner and Cyber Security Leader
E: lgobbi@kpmg.fr

Germany

Uwe Bernd-Striebeck
Partner and Cyber Security Leader
E: uberndstriebeck@kpmg.com

India

Atul Gupta
Partner and Cyber Security Leader
E: atulgupta@kpmg.com

Italy

Davide Grassano
Partner and Cyber Security Leader
E: dgrassano@kpmg.it

Netherlands

John Hermans
Partner and EMA Regional Cyber Security Leader
E: hermans.john@kpmg.nl

Nordics

Mika Laaksonen
Partner and Cyber Security Leader
E: mika.laaksonen@kpmg.fi

Switzerland

Matthias Bossardt
Partner and Cyber Security Leader
E: mbossardt@kpmg.com

United Kingdom

Paul Taylor
Partner and Cyber Security Leader
E: paul.taylor@kpmg.co.uk

kpmg.ca/cyber

kpmg.com/app

Download on the App Store