LegalWeek Intelligence

Cyber risk:

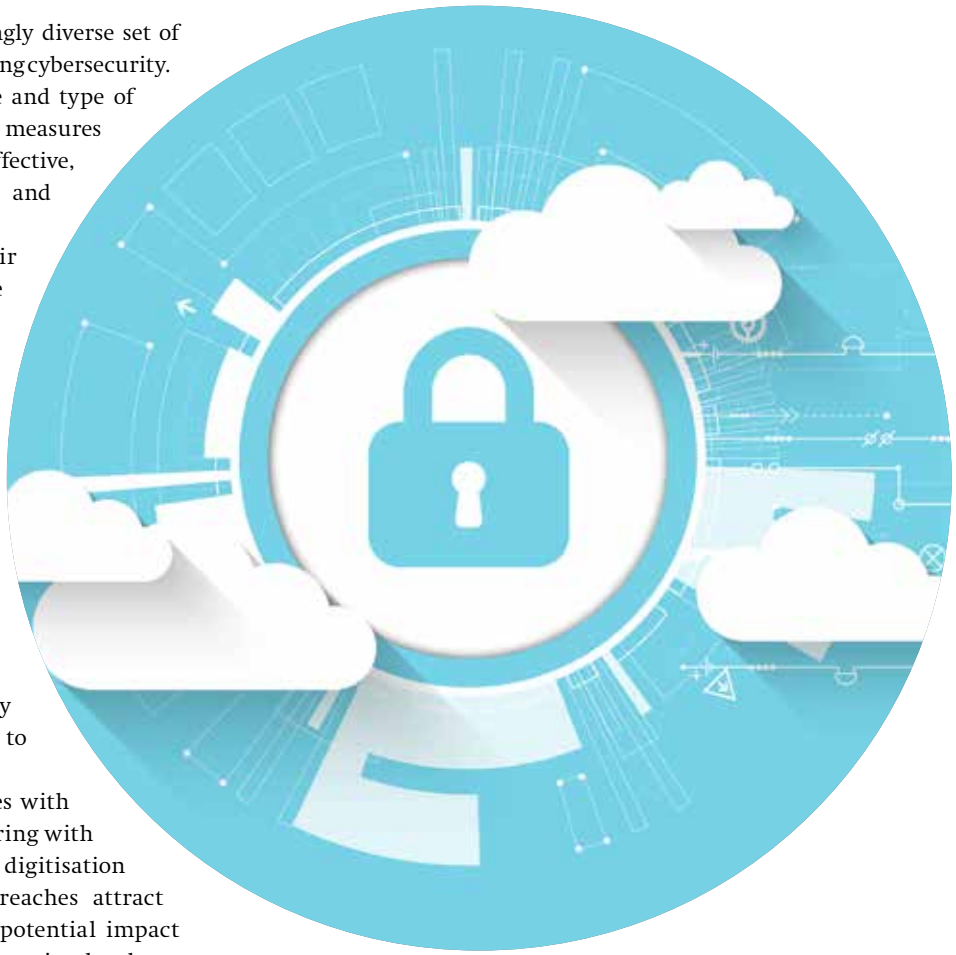
GCs take responsibility

Kroll®


PHP
JAVA
C#

A global report on the cyber-related challenges facing in-house teams

By Dominic Carman

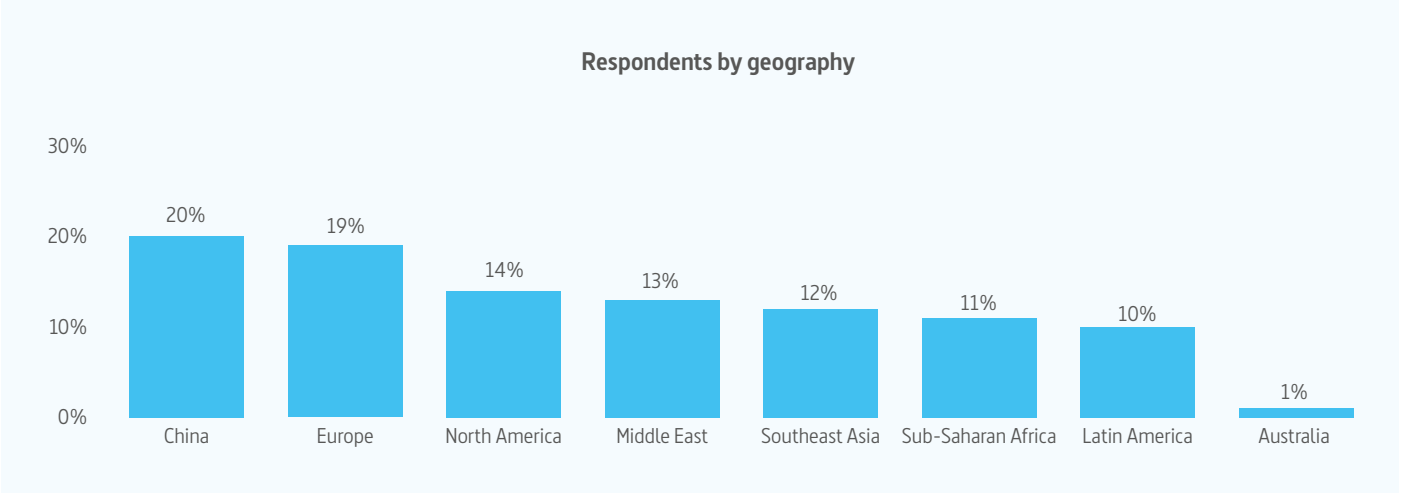


Confronting constant threats from an increasingly diverse set of cyber risks, no business can doubt the need for strong cybersecurity. Or at least none of them should. As the nature and type of threat continuously evolves, existing security measures can suddenly be rendered inadequate or ineffective, exposing sensitive company or customer data and making that data vulnerable to compromise.

Cyber risks are not only increasing, but their nature and scope have evolved to include financial, legal, regulatory, and reputational risks. As a result, the responsibility of the general counsel is expanding to address these additional areas of risk. Some GCs have fully embraced their widening mandate, particularly driven by the global expansion of data protection and privacy regulations. Others may not yet realise the full breadth of their increased responsibility, perhaps where the lack of a mature regulatory framework in their region has kept organisational cyber risk lower on their priority list. Further, some may even be avoiding the increased responsibility because they consider themselves unprepared to understand or manage cyber risks.

The public manifestation of cyber risk comes with the disclosure of data breaches, which is occurring with increasing frequency due to the ubiquitous digitisation of valuable information. Inevitably, these breaches attract considerable media attention focused on the potential impact of the breach on those individuals whose information has been lost. Last year, Yahoo revealed two separate data breaches — the largest in U.S. history — with hackers stealing information relating to 1 billion user records. The company did not disclose the 2014 data breach to the public until September 2016.

Yahoo general counsel Ron Bell had to resign after an investigation initiated by a Special Board Committee concluded that the company's legal team failed to inquire sufficiently into the circumstances surrounding the cybersecurity breach. Yahoo explained in a March 2017 filing with the US Securities and Exchange Commission that certain senior executives at Yahoo as well as members of its legal team "had sufficient information to warrant substantial further inquiry in 2014" about a hack into

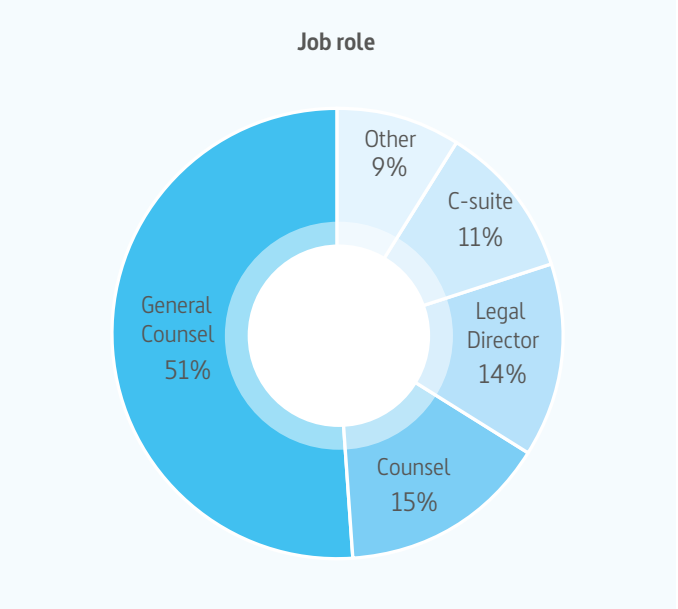


the company's networks, but "they did not sufficiently pursue it". For many GCs, this very public assignment of blame was a wake-up call.

More recently, the enormous data breach suffered by Equifax serves to accentuate the critical need to commit time, energy, and resources to cybersecurity. In September 2017, Equifax announced that it had suffered a cyber-attack which resulted in the loss of the personal information of more than 145 million consumers, both in the US and globally. The fall-out was immediate and dramatic — demonstrating in real terms the devastating impacts that a data breach can have on a company's value, reputation, and management. In a matter of days Equifax's stock value had plummeted by more than 40%, and in a matter of weeks, the company's CEO and other senior officials were either forced to resign or otherwise exit the business.

Surpassing oil, data has suddenly become the world's most valuable commodity. Alphabet (Google's parent company), Amazon, Apple, Facebook and Microsoft are now the five most valuable listed companies in the world. Predictions for future levels of cybercrime are remarkable with the annual cost of data breaches forecast to exceed $2tn globally by 2020, nearly four times the 2015 level. To combat its effects, annual spending on IT security is also predicted to exceed $170bn by 2020, more than double the 2017 figure.

This report addresses the themes of cyber resilience and responsibility, in particular what general counsel are doing, and should be doing, to adjust to the changes in this dangerous new world. Invariably, the result is an ever growing level of responsibility for protecting, planning, monitoring, reporting, training, and responding to the myriad elements of cybersecurity



that now fall within their domain. Critically, GCs also have to take ownership of the company's cyber incident response plan, and ensure that it is tested, up to date and ready to implement in the event of an incident.

In partnership with Kroll, Legal Week surveyed 138 respondents: general counsel (51%) counsel (15%) legal director (14%) C-suite (11%) and other (9%). Research was undertaken globally in July and August 2017 across the following regions: Europe, Latin America, Middle East, North America, Southeast Asia, Sub-Saharan Africa, and China. Further in-depth interviews

The expanding role of the GC before and after a cyber incident (% saying role has expanded)

	Global	China	Europe	Lat Am	Middle East	N America	SE Asia	SS Africa
Planning	45%	30%	50%	64%	50%	63%	31%	33%
Responding	43%	48%	30%	57%	35%	63%	44%	27%
Monitoring	40%	44%	26%	57%	41%	47%	38%	33%
Reporting	37%	30%	35%	50%	41%	47%	31%	33%

were conducted with general counsel in North America, Europe, Asia, and the Middle East.

Interviews with general counsel drawn from different organisations in disparate locations reveal many of their concerns to be similar, even if their levels of concern, awareness of risk and proportionate responses are often very different. How each general counsel responds also differs because the structure and operation of each organisation is unique. Accordingly, the majority of the report focusses on universal themes before examining specific regional issues and stages of development in corporate response to the cybersecurity challenge.

The expanding role of the GC

According to Philip Bramwell, GC at BAE Systems, "general counsel have become the Ministry of Thorny Issues in many large enterprises." There is substance in his humour. The survey data shows that the role of the GC has grown in relation to cyber risk: 45% say their role has expanded in the area of planning, 40% monitoring, 37% reporting, and 43% responding to a cyber incident. The detail behind the headline global response figures show wide variations, both between regions and across different areas of responsibility within regions.

45%
of GCs say their role has expanded in the area of planning for a cyber incident

These increases stretch well beyond compliance and keeping up with, and staying within, the law. It is also driven by practical concerns from C-suite executives about what is being done to mitigate possible threats and ensuring that best practice is implemented and the highest standards applied uniformly throughout the organisation. Increasingly, the buck stops with the GC.

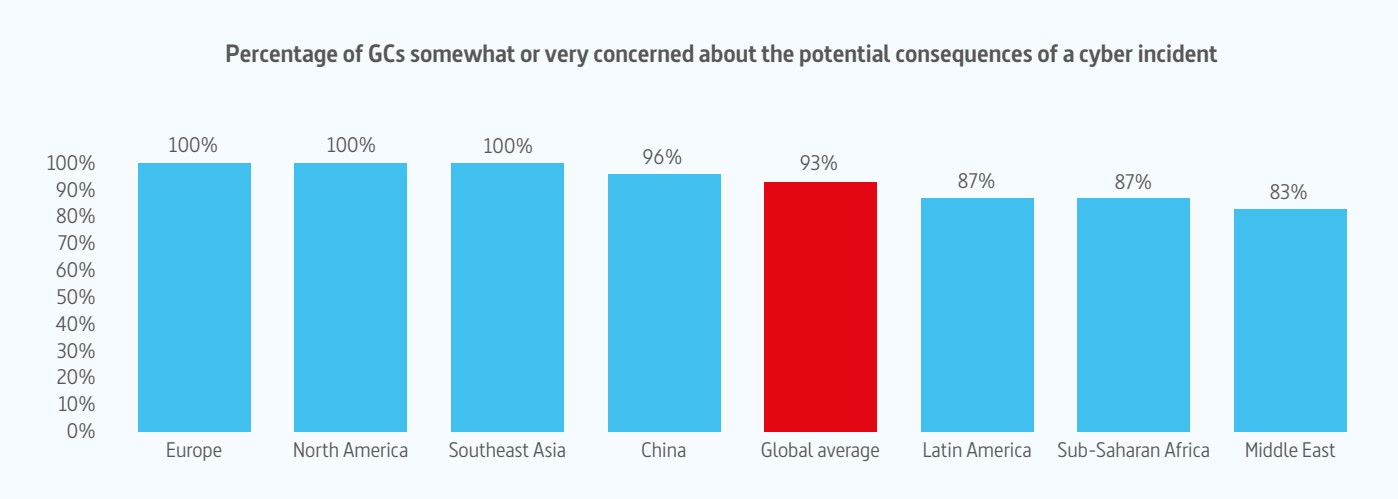
"If you take a pie-chart of my time, a significant part of it is going towards thinking about, talking to and working with others to make sure that our cyber-posture is strong and robust," says Martin Felli, CLO at Arizona-headquartered JDA. "You need to have a voracious appetite and prioritise this issue," adds Alexander Niejelow, Senior Vice President and Group Head of Global Public Policy at MasterCard and a former Director of Cybersecurity Policy at the White House from 2013-15. "And that frankly, is going to be a fundamental advantage for you as an individual in your role as a general counsel, and more specifically with the business and shareholders, if there are shareholders that you represent."

A global issue

Of course, businesses are no more uniform than the customers that they serve. Distinct regional variations emerge from the survey between different parts of the world, dependent upon the prevailing legislation, regulation, culture, education, and business norms.

Yet cyber threats have no borders. With global data communications, every hacker, regardless of their physical location, is the virtual neighbour of every one of their potential targets.

A common international standard for cybersecurity legislation and regulation remains a distant prospect. Although U.S. cybersecurity legislation has been in force for many years, other jurisdictions have only more recently started to play catch up. Additionally, the SEC, FCC, FTC and other U.S. federal agencies have released several iterations of regulations that, though not being codified, have the effect of being laws for organisations subject to those regulatory bodies. Regardless, there has been a protracted political impasse in updating outdated parts of existing U.S. legislation — most of it enacted between 1996 and 2002 — to reflect significant changes in technology and the multiple attendant risks which it creates. Despite the recent data breaches that have befallen U.S. companies, new legislation and regulation to enforce stronger cybersecurity requirements more widely still has some way to go.



In 2015, two major new pieces of EU legislation were agreed: the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS). GDPR was adopted in April 2016 and becomes enforceable from May 2018. Any firm that handles personal data of EU residents will be affected. Non-compliance could lead to substantial penalties, with fines of up to €20m or 4% of global turnover — whichever is the greater. As the first piece of EU-wide legislation on cybersecurity, the NIS Directive (with the goal of setting high common standards for network and information security across the EU for essential service providers) came into effect in August 2016 with each EU member state also having until May 2018 to incorporate the Directive's requirements into their national laws, and six months to identify companies subject to those requirements.

"We are collectively better off, from a safety and security, innovation, and trade standpoint – by working towards a common set of strong baseline cybersecurity standards"

Alexander Niejelow, SVP, MasterCard

Regulation changes behaviour, especially corporate behaviour: every general counsel wants their company to comply with the law. "GDPR is very much a top three item on most general counsel's list," says Bramwell. "It is a big opportunity for data security providers," suggests Robert Blok, Group Legal Director at Virgin Management, "for the way that the Virgin businesses work — being able to manage customer data well, as well as being a very responsible holder and user of that data."

One Middle East-based GC says: "The EU approach to data protection is a tide that raises all boats. If you're going to handle the data for customers in the EU, and pretty soon if you're going to be marketing to people in the EU, you've got to meet a certain standard which is set by the EU. And once legal obligations are there, then a sensible business puts in place a process to ensure that those obligations are met."

Compliance matters elsewhere, too. Stephen Hibbert, GC at Qatar Rail, has seen his authority and time spent both increase in response to cyber prevention over the last year. "It comes off the back of laws being enacted in Qatar that are specifically addressed to cybersecurity, as well as the high media profile of stories relating to cyber activities by adverse parties," he says.

Working closely with regulatory authorities can also pay dividends. In Singapore, RedMart (owned by Lazada Group (Alibaba)) has been recognised by the Personal Data Protection Commission (PDPC) as a model e-commerce company, explains general counsel Chris Chan. As the country highlights the importance of cybersecurity and data protection, this also gives RedMart a platform to share its best practices. The PDPC even filmed Chan for a prime time TV show as a new way of engaging Singaporeans about the digital economy.

"I spend approximately 30% of my time on government affairs and meeting the various agencies to discuss e-commerce," says Chan. "The Ministry of Manpower, the Competition Commission, the Economic Development Board, the Agri-Food and Veterinary Authority, the Academy of Law, and the PDPC are just a few that are learning more about e-commerce." Singapore is considering amending the Personal Data Protection Act (PDPA) of 2012 and recently released a new Cybersecurity Bill for public consultation.

"In most African jurisdictions, cybersecurity and data privacy laws really are at the very early stages," says Bertandt Delport, Head of Legal Africa at British Telecom. "There are a lot of conferences starting to look at that and a huge contingent looking at the European standards. But most of it is in the early development phase now, even in South Africa."

Multinational companies have to consider a range of jurisdictional issues where laws vary widely, or are in different stages of development. "We have a presence in a lot of geographic locations," says Felli. "Some regions are more problematic. There are some countries in particular where there is a heightened circumspection in the way we look at them. Do we want to have data centres in that country? It becomes a potential concern when there are local regulatory regimes that could impact on the business."

"With the EU and GDPR, we need to be focused on how we design our cybersecurity. From a security perspective, we want to be best in class, or attempt to be best in class. So that the bottom, the lowest common denominator would at least address across the globe, whatever regulatory regime is brought up."

At Kroll, Senior Managing Director, Global Cyber Security and Investigations Practice Leader Jason Smolanoff concludes: "Everyone's waiting for GDPR to be enforced. Is GDPR much different from the Privacy Shield program from a roll out perspective? Not really, with the exception of enforcement. Fines can be significantly higher and more importantly, many are waiting to determine if the courts will uphold the penalties. That obviously hasn't been tested yet."

Understanding the specific risks to your business

Reggie Davis, GC at DocuSign, demonstrates his appetite. "Cybersecurity can be quite technical and complicated," he says. "But if you're going to be effective in terms of understanding and communicating the risk and explaining it, both to your board of directors, your executives and to a judge if you find yourself involved in litigation, you really have to reduce it down to more simple, human terms.

"This means having the support of very good technical people and developing a good relationship with them, and then basically sitting them down and having them walk you through, in excruciating detail, and explaining to the point that you

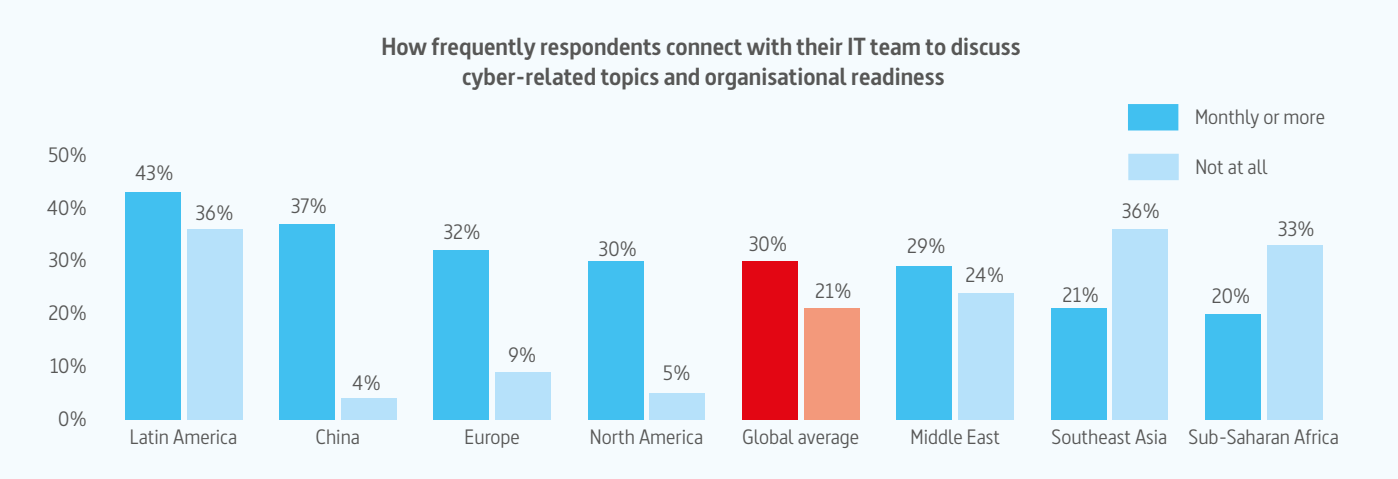
actually understand it. What is the technology involved? How is it working? Is it working well? What is the potential gap analysis that we need to do and where are we at in terms of augmenting any gaps? That's quite interesting and fun, and I've got a captive audience from people at the board meeting."

Andrew Beckett, Managing Director, EMEA Cyber Security and Investigations Practice Leader, Kroll, adds: "Lawyers are highly intelligent. It helps if they're IT literate, but they don't have to be an expert. Spending time with your IT security team in advance of a breach and rehearsing those scenarios will give you sufficient exposure to the language and the technicalities that you can do the job effectively. Barristers in court, if they're prosecuting a surgeon for malpractice, they don't need to understand brain surgery; they need to understand the process that the surgeon is supposed to be following and how you make risk decisions about what they're doing next."

30%
of GCs discuss cyber-related topics and organisational readiness every month with their IT team

Survey data shows that 30% of GCs at US companies discuss cyber-related topics and organisational readiness every month with their IT team. Comparable figures for China (37%) and Europe (32%) are slightly higher. Figures for those who never discuss these matters at all are more revealing: South East Asia (36%) and Latin America (36%); Sub-Saharan Africa (33%); Middle East (24%); Europe (9%); North America (5%) and China (4%).

Davis adds that "We're seeing more movement towards GCs having a broader management role around security issues: driving security committees and security councils. It is one of the largest risk factors out there. Anyone in a general counsel function would do well in terms of understanding the technical issues and then being able to translate that in a way that makes sense to the board of directors around how are we assessing and understanding what



our true risk and potential exposure is, and what are the steps we're taking to mitigate that risk and exposure."

The Middle East-based GC further develops the point. "Within my peer group I'm increasingly seeing general counsel here in the Middle East become COOs," he says. "I've had the conversations with people in the last month who that's either happened to here, or they've indicated that's going to happen. This change is indicative of the extent to which the GC role is really broadening into a back office process management and risk management role."

He offers a strategic risk management approach. "Is data security or a data security breach a massive iceberg on the horizon for a business like ours, or indeed any other business? Absolutely yes. If you contextualise it in that way, then this is something general counsel should be doing. They should be looking for these kinds of risks. They should be steering the company away from them. They should be preparing to handle this kind of stuff. That is completely in line with what they are really there to do."

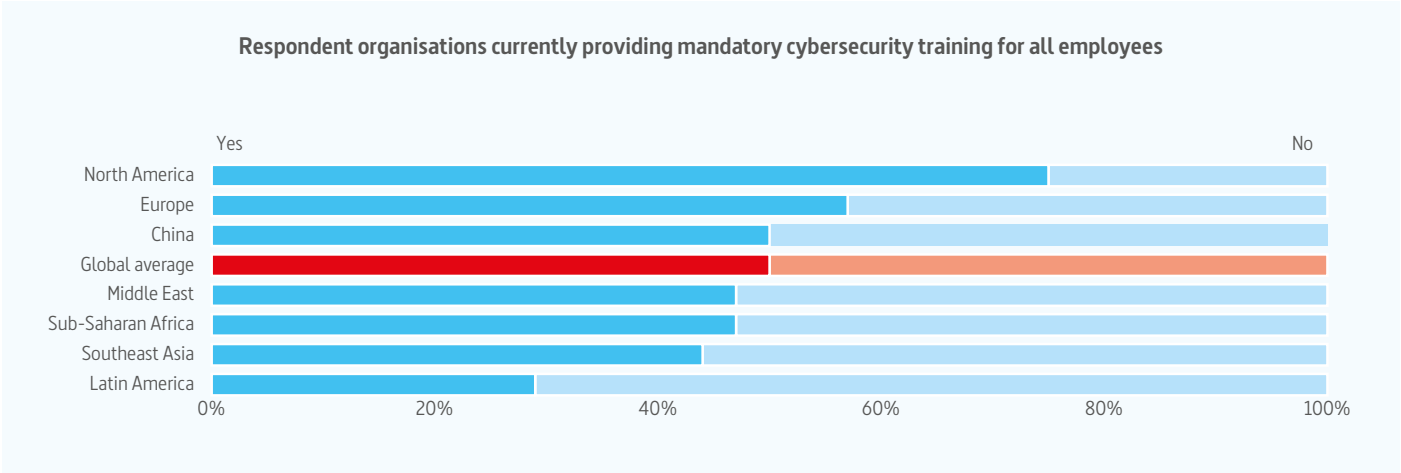
Although general counsel are increasingly tasked with monitoring, preventing and reporting various facets of cybersecurity because of compliance, a practical problem frequently arises: how much they really understand the technology. "If you drew a Venn diagram of lawyers and those with a profound understanding of information technology and communication networks, there's probably a pretty thin overlap," says Bramwell. He offers a different take from Davis: "I don't think we should expect to be gifted naturals in this area. We can apply the general principles, but specialist expertise is critical. Some of the law firms do an outstanding job of building cybersecurity expertise themselves and are able to advise general counsel."

Alan Konevsky, Group Head, Strategic Initiatives Counsel at MasterCard, explains the internal challenge: "The core thing that's evolved — quite clearly — is that it used to be that anyone could be in the frame or frame of mind of being a cybersecurity expert — you were an IT person, a data privacy person, a technology person. You're the 'computer guy', you deal with it. That simply doesn't work anymore. You need people who understand this evolving landscape and crucially, the technology, in a holistic, prophylactic way that captures the significant opportunities to innovate and differentiate, as well as the existential risks. You're looking for a skill set that is not a unicorn, but it's scarce."

"If you drew a Venn diagram of lawyers and those with a profound understanding of IT and communication networks, there's probably a pretty thin overlap"

Philip Bramwell, GC at BAE Systems

Beckett adds: "One of the best things that a general counsel can do is understand the limitations of some of their internal team, and surround themselves with trained experts who are skilled



in managing complex data breach and computer intrusion investigations — to help them properly manage very complex regulatory, reputational, legal and other financial matters that could arise as a result of those incidents."

Mandatory training for all employees delivers one of the sharpest regional divides in the data. While 75% of all North American respondents have it, only 29% of those from Latin America do with most other regions falling somewhere in between. "More attention is being paid to the on boarding process of new employees, in the continuous education of employees on an ongoing basis through online training," says Bertrandt.

Beyond formal training at the outset, effective continuous training is multidimensional. The Middle East-based GC adds: "It's a cliché, but information security is a team effort. Given the likeliest sources of a data compromise, it's critical to the effectiveness of cyber risk mitigation strategies that awareness of cybersecurity risks is raised among all staff members. In most companies this necessitates the involvement of senior personnel (up to and including the CEO) to highlight the threat and the actions which staff are expected to take in response."

Felli speaks to the international training challenge. "We have robust training that our employees need to take across the globe," he says. "Where we've found specific issues that have impacted or affected us, we have put in place targeted specialised training, either to the group, the individuals, or the region so that there's a heightened awareness that a particular issue pertains to them. We don't necessarily take a peanut butter approach, which is where you spread the same training around the whole world, although there is an element of that. There's also an element of targeted tailored training to very sensitive groups: finance, legal, HR, internal audit, and some other groups."

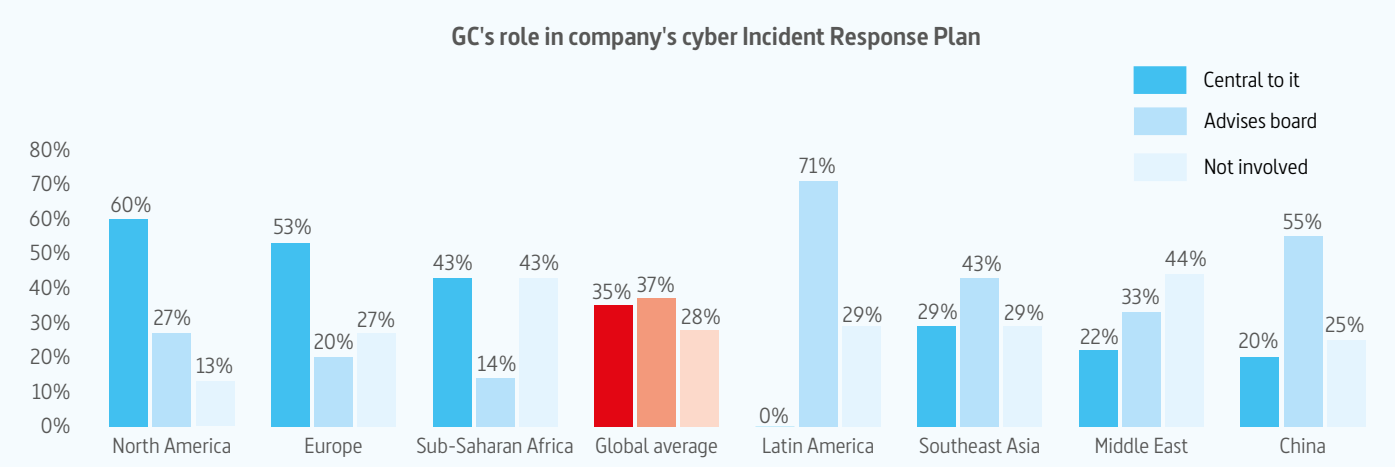
Incident response planning

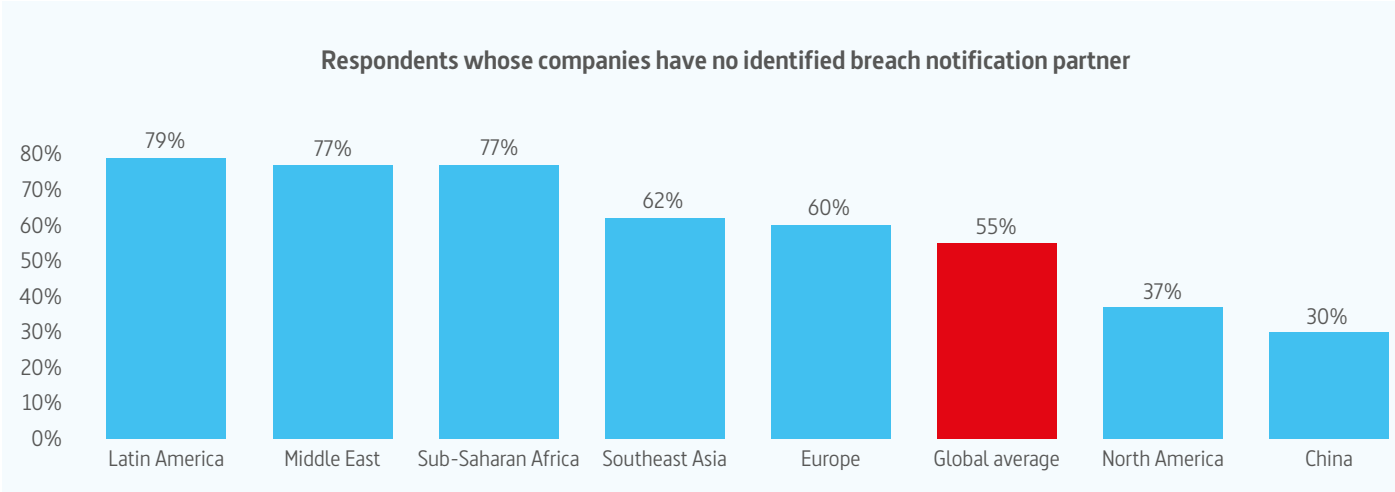
Should the worst happen, general counsel need to have a plan of what to do in the event of a cyber incident. That means having an Incident Response Plan (IRP) which determines the critical stakeholders within a company and their respective roles and responsibilities when responding to an incident. However, the level of direct central responsibility that GCs have for IRPs varies enormously: Latin America (0%); China (20%); Middle East (22%); Southeast Asia (29%); Sub-Saharan Africa (43%); Europe (53%); North America (60%).

"Where we've found specific issues that have impacted or affected us, we have put in place targeted specialised training, either to the group, the individuals, or the region"

Martin Felli, CLO, JDA

Planning for breach notification is perhaps a key litmus test of how well-conceived an IRP may be. When asked whether





they had identified a breach notification partner, the level of negative response — no identified need for a breach notification partner — was as follows: Latin America 79%, Sub-Saharan Africa 77%, Middle East 77%, Southeast Asia 62%, Europe 60%, North America 37% and China 30%.

Much of the difference in breach notification may be driven by different levels of compliance regulation across jurisdictions, ranging from non-existent to significant. Looking at the wider picture of communication, further divergence appears, both between regions and with whom communication is planned.

Cybersecurity is "not a risk that should stay within the expert IT community within an enterprise because it will tend not to get allocated sufficient resource and attention," says Bramwell. "There will not be appropriate response plans if the risk should impact you. Pretty much all large enterprises will be subject to routine attacks and one will get through sooner or later. General Counsel had better have a plan in place for an incident response. They've got to practise it. Then they'll get the appreciation, get the resources, and get the understanding."

Beckett adds: "General counsel need to have an inquiring mind, an intelligence that they bring to the table which is essential in running the Incident Response Plan, but they do not need to have an absolutely detailed knowledge of cyber forensics. Surrounding yourself with experts, skilled in Incident Response preparation and execution is critical to augmenting the general counsel's team."

Konevsky explains how this has developed: "You need people who understand how these things flow into your industry, to your business model, and to your organisation. Then you engineer a response plan. From a corporate readiness perspective, you

Percentage of respondents whose cyber IRP includes communications with external stakeholders

	Global	China	Europe	Lat Am	Middle East	N America	SE Asia	SS Africa
Law enforcement	74%	85%	86%	100%	33%	67%	80%	20%
Regulators	68%	68%	79%	71%	17%	60%	100%	83%
Partners	64%	63%	82%	83%	33%	60%	60%	60%
Investors	54%	40%	73%	57%	29%	73%	40%	60%
Insurers	54%	40%	50%	57%	43%	67%	60%	80%
Vendors	53%	63%	73%	57%	0%	53%	40%	40%
Customers	50%	47%	54%	57%	33%	53%	40%	60%

can't lurch from crisis to crisis and believe this is kind of an emergency response plan that you put in place and that's great. It's a fundamental part of your business DNA."

Insurance

Insurance is another aspect of cyber risk for which increasing numbers of general counsel have either a supervisory or direct role. The cyber insurance market is growing fast. A recent Financial Times report said that global written premiums for cyber insurance at Lloyd's estimated the 2016 figure at $2.5 billion — up 50% on the year. Citing Allianz estimates, the FT said the figure may grow to $20 billion by 2025. But there are regional variations. While 53% of Middle Eastern and 45% of US respondents have it, surprisingly, only 27% of those in Europe do. Less surprising is that only 21% of those in Latin America and 20% of those in Africa have cyber coverage.

However, when asked about the coverage and exclusions which apply to their cyber insurance, how much GCs know about the detail of what is covered varies widely. For example, 33% of GCs in the Middle East, 67% of GCs in Latin America and 75% of GCs in Southeast Asia do not know if employee mistakes are covered. For coverage of third party providers/vendors and Hacking/Phishing/Malware/Ransomware, 100% of GCs in Southeast Asia do not know if their organisations are covered.

"You used to have an absolutely huge document full of things that you had to do and things that would invalidate your policy," says Blok. "Now it seems there really is a broad spectrum of policy covers that you can opt for. The balance is also crucial between considering insurance, and whether that's appropriate, but also considering whether whatever money you're paying on a premium might be better spent on your security measures: to make sure it dœsn't happen at all, rather than you've got compensation in the event it dœs. The PR side, for example, is something you can't really insure for, in practice." In talking about the Virgin Group, which is so intertwined with its founder Sir Richard Branson, Blok's point is very specific.

In a wider context, Beckett says: "Effectively, for any risk, an enterprise has three choices. They can accept the risk; they can mitigate the risk; they can transfer the risk. Whether it be the risk of fire or the risk of a cyber breach, insurance has a role to play. The issue that GCs face on behalf of their companies is making sure that the insurance they buy is relevant and covers the aspect of risk that needs to be transferred. Too often, we see inappropriate broad scope cyber insurance with relatively high premiums being looked at or taken by our clients. When in fact what they actually need is something far more specific for specific risk."

Bramwell adds: "Being based in London, we're fortunate that we've got the world's most sophisticated insurance market: we're able to get coverage. Business interruption insurance is held by most companies. Whilst you're unlikely to be able to insure against consequential losses or sometimes for reputational damage, to the extent that your physical infrastructure is denied to you for a period of time and your business suffers as a result, then you're likely to be able to get cover, albeit it may always not be huge."

Felli adds: "Many people in the cybersecurity world would tell you it's not a matter of if, but when you get hit in one form or

Percentage of respondents whose cyber insurance policy covers/excludes the following risks

	Covered	Excluded	Don't know
Hacking/phishing/ malware/ransomware	75%	0%	25%
System glitch/error	74%	5%	21%
Employee mistakes	72%	5%	23%
Lost/stolen items with sensitive data	71%	24%	5%
Malicious insider	69%	5%	26%
Mistakes by third-party providers/vendors	55%	24%	21%

other. Either you have been attacked and you don't know about it, you've been attacked and you know about it, or you will be attacked at some point.

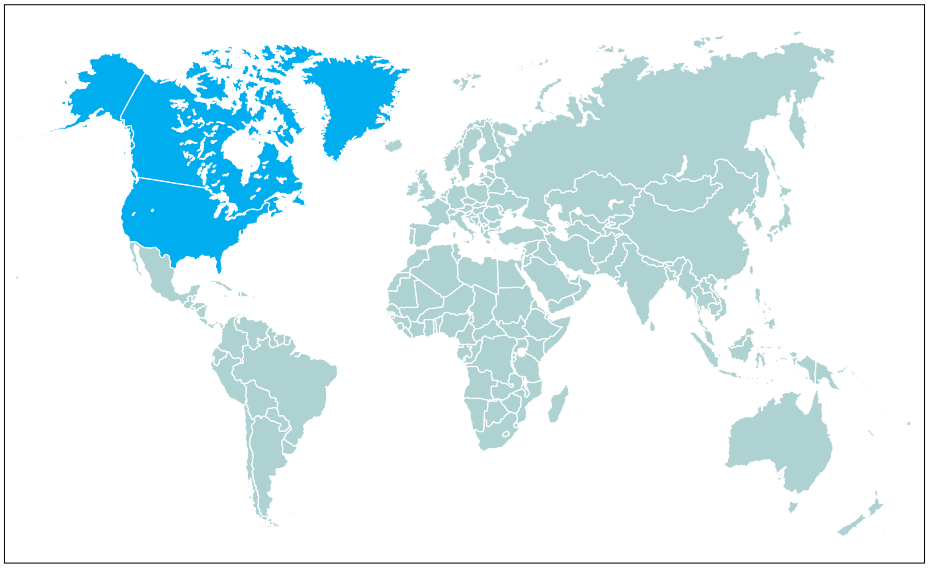
Insurance has to be a component in your arsenal in trying to fight this menace. Protecting against it is an important investment. Having insurance definitely does make a lot of sense, even if it's only for the purpose of your customers or vendors being comfortable that you're a responsible business partner."

At Qatar Rail, Hibbert has been looking at an insurance programme for the railway project. "It appears that it's being readily offered these days by most major insurance providers, a hot topic in the insurance market. But it's a different question as to what is the thing that's being insured. You can take security from insurance if you've got a huge consumer base like a bank and you get claims for a cyber-attack causing data loss. It's not irrelevant for us, it certainly is relevant, but it's probably a far more second-order issue than the primary protection."

Likewise, Madeleine Truter, GC of Setso, comments: "In South Africa, we are ranked number three in 2017 for cyber attacks. Insurance is very difficult for us because it's hard to quantify. There's no financial metrics that you can use to quantify. You only really know what the damage is after the fact. That's not even really for reputational damage. The actual cost of having to appoint experts to remedy and put in fixes for business interruption factors. We're not really sure that the quantum that we've insured for would be adequate. I think that is the case with most companies."

Smolanoff develops the point: 'reading the policy carefully and understanding what you need is really quite important. That goes to the bigger picture of risk management. A GC overseeing information security should really take a step back and ask themselves a big question: "Why do I need an information security program?" Many times when I ask that question, you'll hear crickets in the room afterwards because people naturally think, "Well, we must have one". The question is: why do you have one? Because if you don't understand why you need it, you can't appropriately manage the risks that the company is facing."

Region focus: North America



Although other regions are catching up fast, a uniform consensus exists that North America is currently the most advanced in cyber resilience. This is reinforced by domestic laws together with moves towards updating a raft of aging legislation being repeatedly frustrated. Yet on virtually every metric determined by the survey — from training and monitoring to insurance and planning — North America is ahead at least by a nose, sometimes by a distance.

Perhaps in recognition of the dangers, GCs in North America have a lower level of confidence about their organisation's ability to detect a cyber incident: only 15% are very confident compared to 26% in Europe, 40% in Sub-Saharan Africa, 43% in Latin America, and 44% in both the Middle East and China.

15%
of GCs in North America are very confident about their organisation's ability to detect a cyber incident – compared to 44% in China

The commentary provided by survey respondents offers some valuable insight into GCs' thoughts about cyber risk and its potential impact. Their concerns are palpable. "We hired a department to monitor cybersecurity and protect data," says a GC respondent." Another offers a frank insight: "Financial, reputational and operational risk (especially for those engaged with protected health information) pose a significant concern at the executive level of our organisation."

Neither complacency nor hubris are evident. This is perhaps a key benchmark of how seriously general counsel perceive the potential threat. "The sophistication of hackers probably exceeds our capability to detect all intrusions but I think we can detect almost all of them," suggests one GC.

"We have procedures and programs in place to

detect cyber incidents but you can never be TOO confident," says another. "Computer hackers always seem to be one step ahead," volunteers a third. A final comment shows how concerned one GC is: "Our inability to properly adapt leads to an ever emerging threat ratio.

Underpinning these comments is an acute awareness by general counsel of data breaches and cyber risks, what those risks mean for their company and their responsibility for managing them. "The largest risk that a company faces, comes not from the investigation or remediation, but from the disclosure of the incident itself," says Smolanoff. "That carries with it reputational risk, legal risk, regulatory risk, and financial risk. That's where the rubber meets the road. The GC is going to be the person who owns all of that risk."

CASE STUDY: NORTH AMERICA

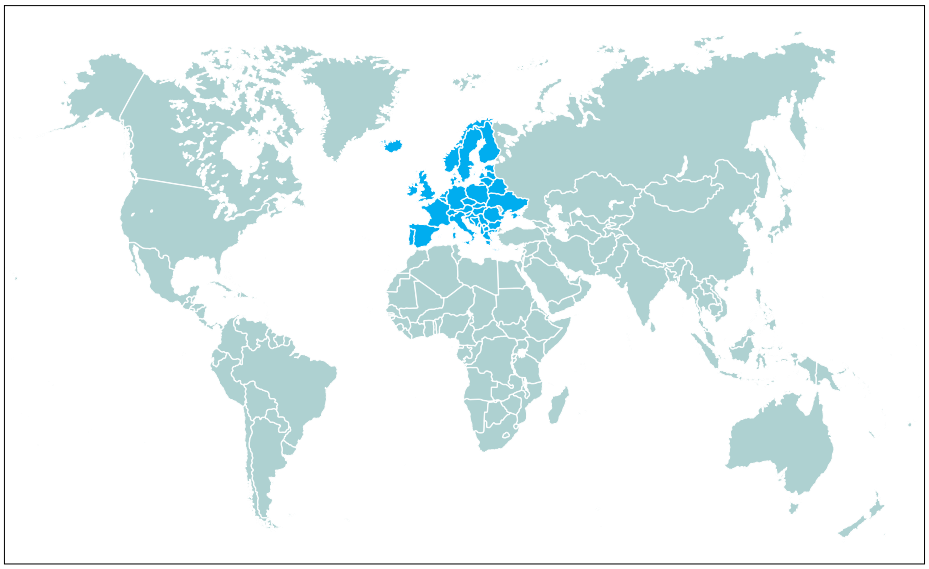
Supporting client with managing an advanced persistent threat

Kroll responded and provided incident response services to an airline company after it identified a significant computer security incident. Over the course of six weeks, Kroll characterised the incident as an advanced persistent threat attack, worked with the company to deny the attacker further access, and remediated the affected systems. Kroll also assisted the company and outside counsel with the identification and documentation of all sensitive and regulated data which may have been exposed and provided comprehensive breach notification and credit monitoring services to assist the client in satisfying its disclosure obligations.

"General counsel are becoming the quarterbacks. They're increasingly owning the risk that's associated with a breach and as a result, are taking on more and more cybersecurity responsibilities"

Jason Smolanoff, Senior Managing Director, Global Cyber Security and Investigations Practice Leader, Kroll

Region focus: Europe



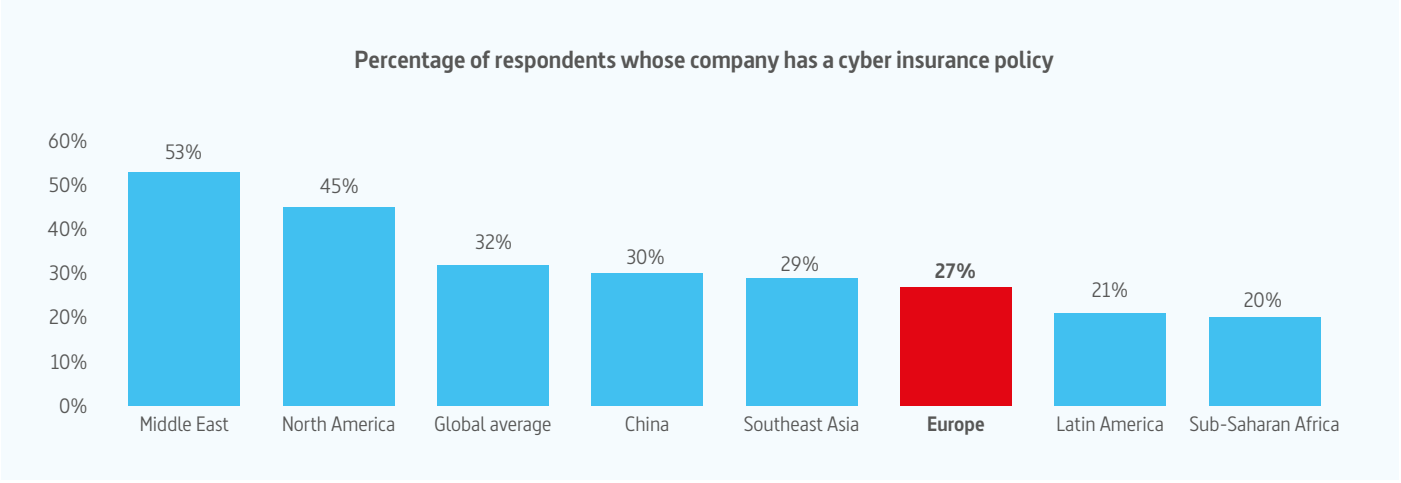
The introduction of two EU Directives, GDPR and NIS, is a game changer for Europe and for the businesses which will operate there in the future. They put data privacy and cybersecurity centre stage. This is reflected in the high percentages of European respondents who often rank just behind North America in their collective survey responses. However, in some areas, for example cyber insurance coverage (North America — 45% purchase coverage; Europe — 27% purchase coverage) and cyber training (North America — 75%, Europe — 57%), the gap is more notable.

European general counsel interviewed for this report express their own views on the issue, sometimes with alarming candour:

- "No one really understands the concept of cyber risk, or its likelihood"
- "Cyber risk is getting more attention recently because losses to companies are very large and many people are not aware of the risks"
- "Whilst the main risk functions recognise the issues, investment is not currently matching those concerns"
- "Cyber attacks can be very elaborate and may not be easy to detect regardless of how competent staff are and how good internal systems and controls are"

One GC, who is certainly alert to the danger, adds: "It requires continuous attention; the nature of threats keeps changing; the effects of a successful attack will probably be enormous." There are others who express more confidence in their company's response:

- "We have considered this important for a long time; the relevant monitoring and personnel have been in place for a long time"



57%
of respondents in Europe have mandatory staff cyber training, compared to 75% in North America

- "Our CSO has made it a priority to create awareness, to monitor continuously and to have external parties flag threads and incidents"
- "Cyber risk is high on our list of priorities and we follow up on making sure that we are as prepared as we can be"

"If there are GCs in companies who have decided not to address the new directives, their lives could get very interesting over the next two to three years, as regulation around data protection increases," says Beckett.

"Roughly 75% of boards in Europe don't have anybody, either executive or non-executive, who understands cyber and the cyber threat, who could provide top level leadership — unlike North America where GCs are taking a huge role in terms of the lead," he adds.

CASE STUDY: EMEA

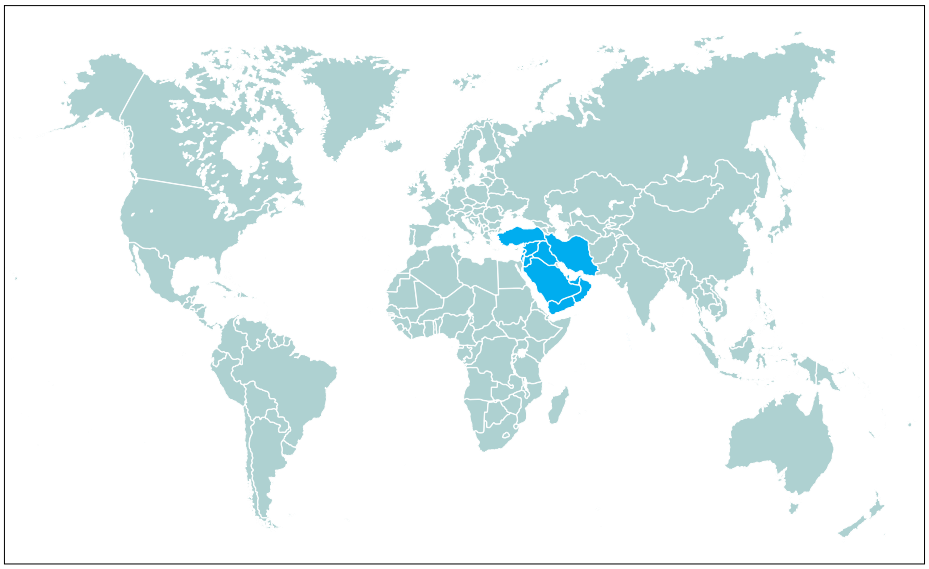
Whistleblower Investigation of Insider Data Theft

Kroll was contacted by the general counsel of a private equity house whose investee company had received a whistleblower letter. The letter suggested that various senior employees were preparing to leave the investee company and were actively downloading client data ahead of their departure. Kroll engaged directly with the investee company and, having taken specialist legal advice concerning data privacy issues, undertook a forensic electronic retrieval of information at the investee company's premises. This forensic review, together with a series of onsite interviews, validated the whistleblower's claims. The investee company commenced legal proceedings against the departing staff.

"Roughly 75% of boards in Europe don't have anybody, either executive or non-executive, who understands cyber and the cyber threat, who could provide top level leadership – unlike North America"

Andrew Beckett, Managing Director, EMEA Cyber Security and Investigations Practice Leader, Kroll

Region focus: Middle East



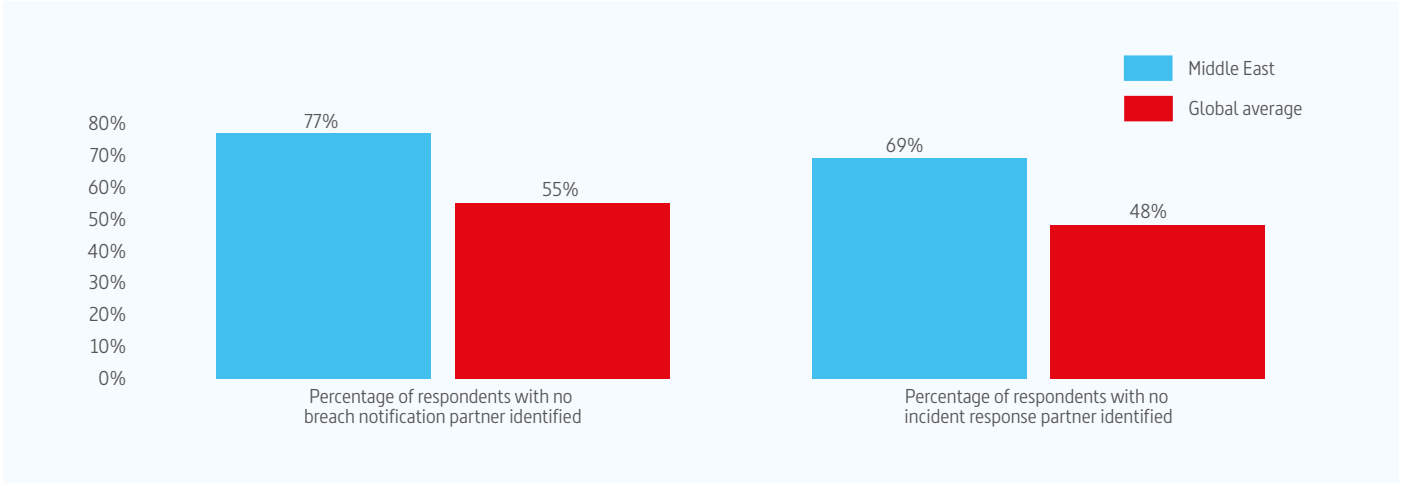
Although some Middle East countries have data protection or cybersecurity laws in place, the development of both, where applicable, is in its infancy. Last November, Qatar was one of the first GCC member states to issue a data protection law comparable to those applicable in the EU, though the UAE has also had a data protection law since 2007. With differing levels of regulatory maturity across the region, it is perhaps no surprise therefore that 69% of respondent GCs in the region have no technical incident response partner identified while 77% of them have no identified need for a breach notification partner.

Commentary from survey respondents is much thinner on the ground. "Risk management focuses a lot on cyber risks attacks and latest developments," says one. "A very efficient department handles cyber attacks," suggests another.

Stephen Hibbert, GC of Qatar Rail, says that his role for monitoring and implementing cybersecurity has increased notably. "Qatar Rail was established in 2011," he says, "and is considered a new industry in Qatar and the surrounding area. Nevertheless, there is a potential risk for every business. Our technology record would show that in the last 18 months we've gone up another level of cyber protection. There has been a heightened awareness in our organisation and across government in Qatar."

77%
of respondents in the Middle East have no identified need for a breach notification partner

In the UAE, the Middle East-based GC adds: "General counsel here are seeing trends in how data subjects expect their data to be handled, and the direction of governance trends in their home countries — particularly if they are from the EU or



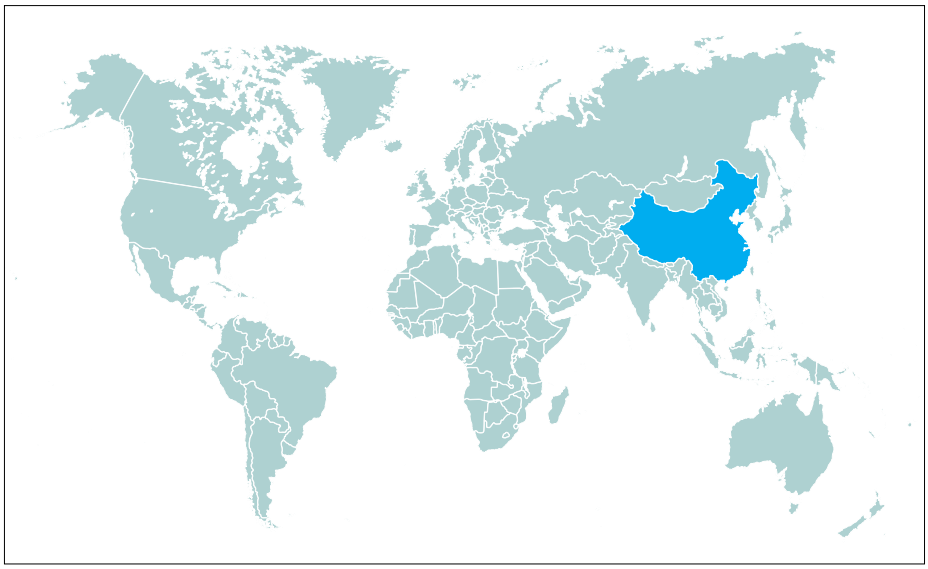
North America. They're trying to bring those strategic themes into the day to day operations of the businesses that they advise."

Beckett agrees: "Our clients have traditionally contacted us to help them address cyber crime, cyber enabled crime or leaks of information across the region. These days they are increasingly asking about cyber defence and for advice on preparing for GDPR compliance in relation to the data they hold on European operations or relating to European citizens."

"Our technology record would show that in the last 18 months we've gone up another level of cyber protection. There has been a heightened awareness in our organisation and across government in Qatar"

Stephen Hibbert, GC, Qatar Rail

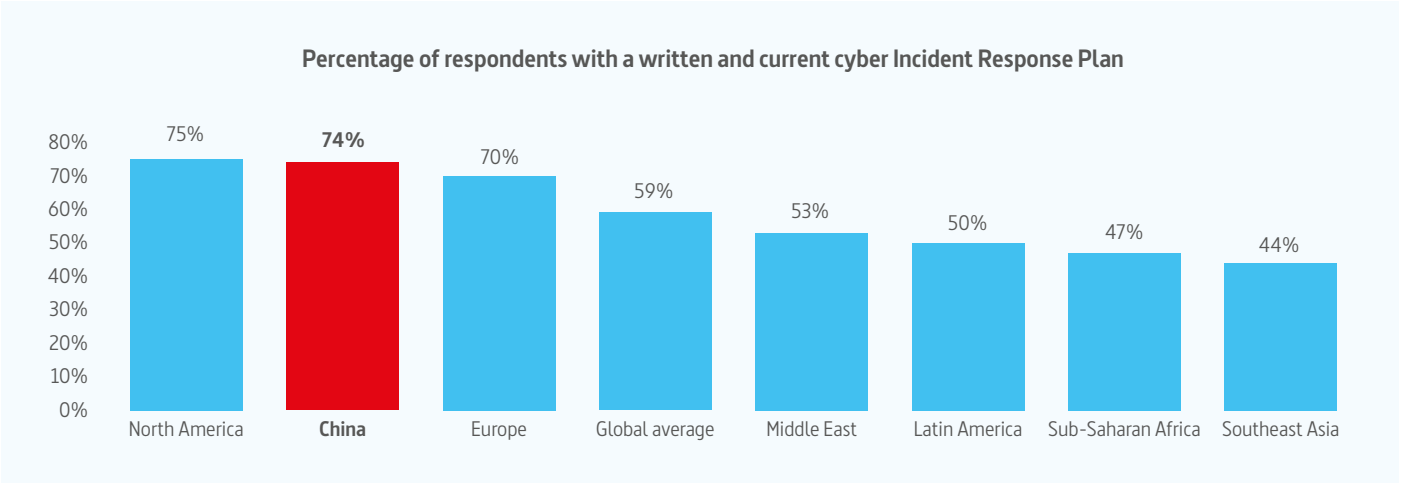
Region focus: China



China's first cybersecurity law became effective in June 2017. The introduction of a much needed data protection law was a milestone. But there are concerns about cost and other factors in relation to data localisation requirements, especially regarding trade secrets and intellectual property. Some aspects of the law are wide-ranging and vague because interpretation of them is as yet untested, which creates significant uncertainty.

Notwithstanding the legal changes, China ranks near the global average in areas such as insurance, training, monitoring and responsibility, although respondents (74%) almost match North America (75%) in having a written and current cyber IRP. Overall, they speak to a clear perception of risk, as well as some alarm:

- "We can obviously see that the amount of cyber risks are much higher than before, more and more companies are losing because of network leaks"
- "The network risk is serious, but as long as we have prevention, it can be controlled"
- "We're in a really bad cyber environment, but other senior executives of our company have not yet attached importance to this work"
- "Cyber-hacking is terrible for corporate secrets, and if this happens, we will suffer huge economic losses"
- "Because the network risk factor is very high now. Once it happens, the loss can be very serious"
- "We still have a lot of work to do, and the company's defence level is not up to par"
- "There are too few employees on this and hardware firewall is not good enough"
- "Risks here are unique, and we worry about things that don't take into account, unexpected risks are not controllable"



74%
of respondents in China have a written and current cyber Incident Response Plan

- "The organisation has a very rich experience of resisting cyber events and has not made any mistakes over the years"
- "Our team is experienced and can control the risks"

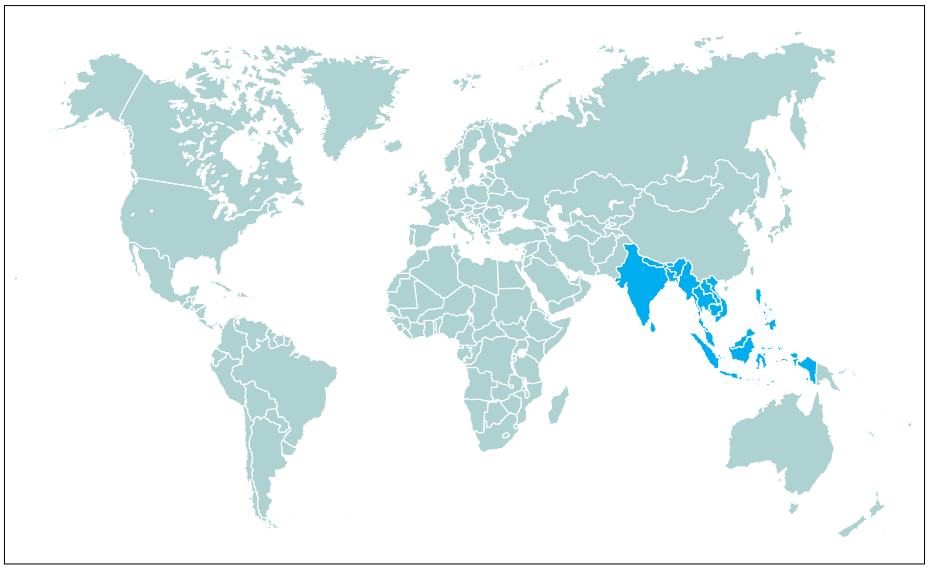
Many businesses in China are investing heavily in cybersecurity with 63% of GCs there very concerned and 33% somewhat concerned about the potential consequences of a cyber incident.

Paul Jackson, Managing Director, Asia-Pacific Cyber Security and Investigations Practice Leader, Kroll, says: "The message I try and get across is: Your organisation is spending huge amounts of money on cybersecurity, in terms of people, process, and technology. The real questions you should be asking are: Is it being spent in the right places? Has it been correctly spent? Are you getting value for your money, and is it really protecting you?"

"Your organisation is spending huge amounts of money on cybersecurity, in terms of people, process, and technology. Is it being spent in the right places? Are you getting value for your money, and is it really protecting you?"

Paul Jackson, Managing Director, Asia-Pacific Cyber Security and Investigations Practice Leader, Kroll

Region focus: Southeast Asia



Southeast Asia traditionally has a diverse set of laws. The response to cybersecurity legislation in the region is no different. The hardest part for general counsel, many of whom operate across multiple jurisdictions in the region, is the struggle to maintain an up-to-date knowledge and understanding of the different cybersecurity and privacy laws and their implications for multinational businesses.

The survey revealed that general counsel in the region have seen their remit expand to encompass responsibility for cyber planning (31%); monitoring (38%); reporting (31%) and responding (44%) — one of the lowest regions overall.

Apart from one respondent who admits "We prioritise cyber risk to a lesser level than other risks," responses from other general counsel sometimes indicate that cybersecurity decisions are made elsewhere in the business: "Our network department has a very strong ability to deal with such events with specialised mechanisms'; "The company has also invested a lot of money in this'; "The company's supervision department is very strict and it is very good for our network environment".

Elsewhere, there may be some problems, as suggested by the following:

- "We are still in the process of building out a standard process for responding to cyber threats in our organisation"

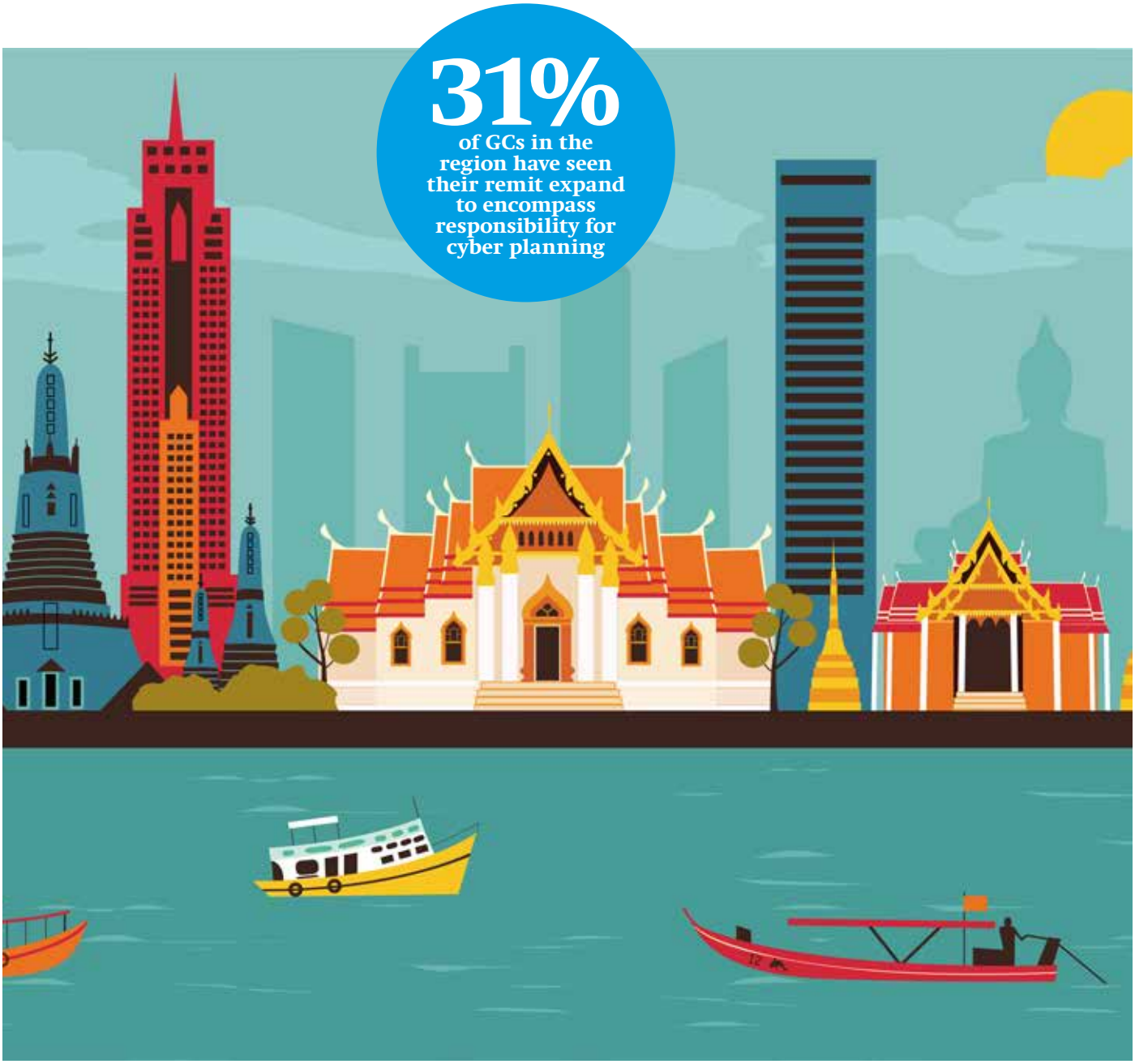
CASE STUDY: APAC

Security review of websites hosted in five countries

An Asia-headquartered global logistics company engaged Kroll to review the security posture of its primary and subsidiaries' websites hosted in five countries. In addition to penetration testing, Kroll's team scrutinised the security controls of the websites' supporting processes operated by third party vendors. Kroll identified critical security issues on multiple websites, attributable to lapses in the vendors' security patch management process and an ineffective secure software development lifecycle. Kroll advised the client to improve its vendor oversight and to resolve the technical vulnerabilities, which could permit unauthorised access to the websites as well as to the underlying IT infrastructure and stored customer data.

Percentage of respondents whose remit has expanded over the past 12 months to include:

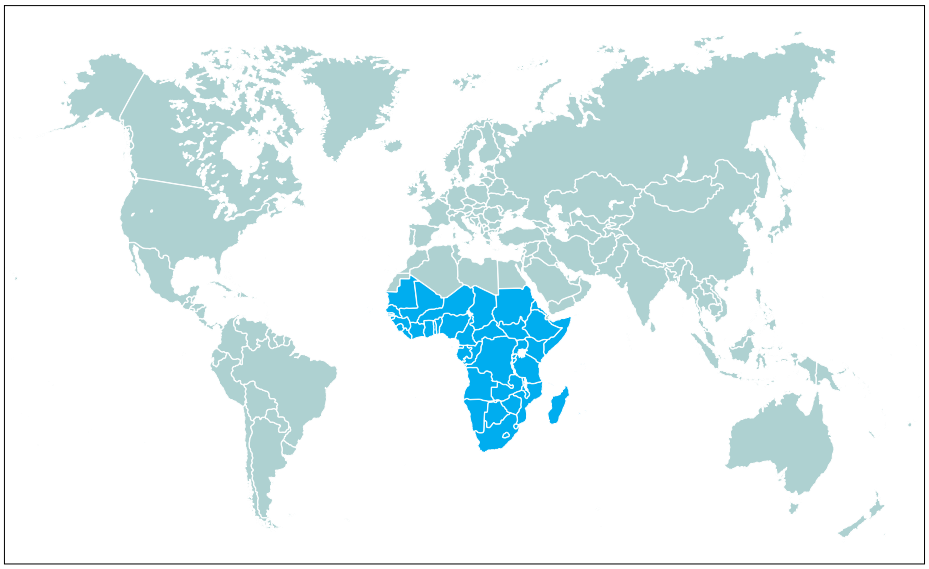
	Global	China	Europe	Lat Am	Middle East	N America	SE Asia	SS Africa
Planning for a cyber incident	45%	30%	50%	64%	50%	63%	31%	33%
Responding to a cyber incident	43%	48%	30%	57%	35%	63%	44%	27%
Monitoring a cyber incident	40%	44%	26%	57%	41%	47%	38%	33%
Reporting on a cyber incident	37%	30%	35%	50%	41%	47%	31%	33%



- "We now have more and more Internet applications, but the risk is harder to control"
- "While there are steps put in place, these may not be adequate in the long run"
- "Unfortunately, the IT security measures we have in place have not been tested. It is therefore difficult to say if it is in fact adequate to withstand a cyber incident"

Jackson says: "In the region, there needs to be more reliance on independent third parties to verify. Given the changing legal and regulatory landscape, general counsel probably need to take more seriously their current cybersecurity posture and look to independent verification that the measures they've taken are effective. Otherwise, they run the risk of transgressing the governments' frameworks that are in place."

Region focus: Sub-Saharan Africa

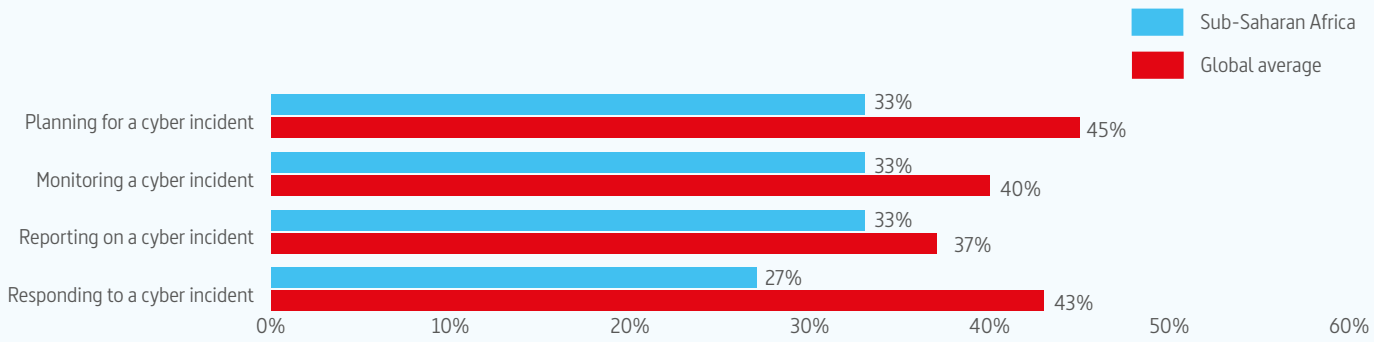


"I was certainly out of my depth," says Madeleine Truter. As GC of Setso Property Fund in Johannesburg, she recently dealt with the consequences of a cyber attack. "It was a very steep learning curve. I had to upskill myself on cybersecurity." Enhanced training and an upgraded response plan have been put in place. "In South Africa, there is an awareness of the risk of cyber attack, but most companies hope that it's not going to happen to them," she says.

That sentiment is echoed by the survey findings. Awareness, education, protection and acceptance of responsibility in Sub-Saharan Africa are generally among the lowest of any region. Only 27% of general counsel have seen an expansion of their responsibilities for responding to a cyber incident in the last year, compared to the global average of 43%, with 7% experiencing a decline. Responses cover the spectrum:

- "With the recent cyber attacks worldwide, we have become more concerned and have consulted with experts in the field of cybersecurity for additional interventions to those already in place"
- "Cyber and data security is a top risk for our firm"
- "We have spent a considerable amount of time over the past year improving our processes, infrastructure and training"
- "Since we have not yet had to deal with a cyber incident, I do not know whether our systems are robust enough to withstand such an incident"
- "Although we have taken steps to address a cyber incident when it occurs, there is still some work to be done to improve this"

Percentage of respondents whose remit has expanded over the past 12 months to include:



27%
of GCs in SSA have seen an expansion of their responsibilities for responding to a cyber incident in the last year, compared to 43% globally

As GC of BT Africa, which operates in 34 Sub-Saharan countries, Bertrandt explains the problem which his company has across the region: "There's a huge tension that we've been experiencing between what the business customer wants, and what they are willing to pay for. Very often, the requirements at the contracting stage will be: we like all the bells and whistles as far as cyber protection and information protection is concerned. However, we are only willing to pay for a small portion of that."

Beckett adds: "Most of the large reported breaches have happened in traditional western markets. That's where the examples are of brand damage, share price damage that GCs and boards worry about so much.

"In Sub-Saharan Africa they've not had those examples: the cases, the press coverage of such incidents are far fewer and therefore the GCs don't appear to have that on their radar to the same extent."

"In South Africa, there is an awareness of the risk of cyber attack, but most companies hope that it's not going to happen to them"

Madeleine Truter, General Counsel, Setso Property Fund

Region focus: Latin America

Although a good number of general counsel were interviewed for the survey, none of those in Latin America agreed to a more in-depth interview on the detail of their approach to cybersecurity. In their narrative, many respondents in Latin America commented that they were "very confident" in their organisation's ability to detect a cyber incident. Only 47% of survey respondents in the region said they were very concerned about a cyber attack, the joint lowest of any region, alongside Africa, while 57% said they were very confident of withstanding one, by far the highest, compared to 20% for North America and only 7% for Southeast Asia.

Of those who provided a written comment at the end of the survey, not one expressed any anxiety or concern about the risks that they might face. Quite the contrary. Their comments included the following:

- "There are a lot of dedicated departments to this with a lot of capable people"
- "I have knowledge of all the policies we apply"
- "I believe we have the right infrastructure for a crisis event"
- "I am very confident because of the people who work on this and the use of state-of-the-art technology"
- "We have a robust contingency plan scheme to address business continuity"
- "The IT department is prepared for these types of risks"
- "We have the technical knowledge"

Such confidence may often be well-founded and entirely justified. Sometimes, it may not. Fernando Carbone, Senior Director, Cyber Security and Investigations at Kroll in Brazil, notes that "in talking to local companies, larger businesses are

much more concerned with the protection of client and other sensitive data". He adds: "They have developed more mature planning for cybersecurity and incident response, but detection is still a major concern. However, many smaller companies are still deficient in their cybersecurity posture."

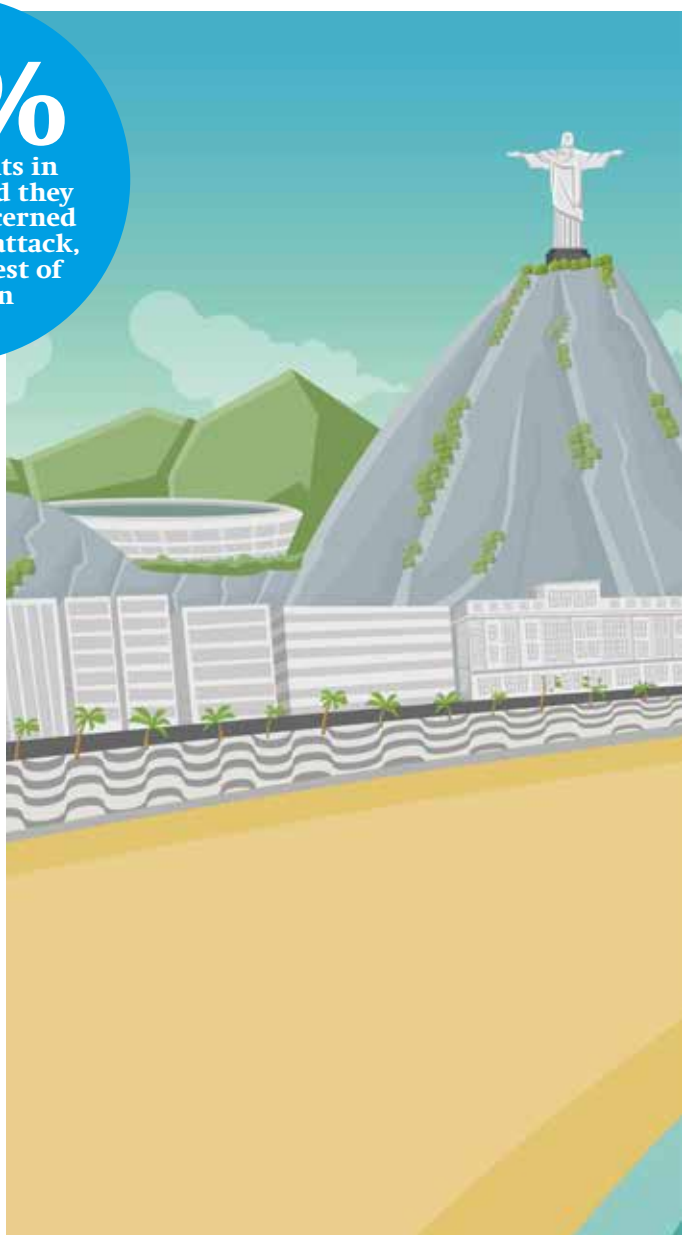
Carbone continues: "In Brazil, cybersecurity has not yet become a priority for most executives. In many companies, the responsibility for information security continues to remain with the IT team. Often there is a lack of understanding of the specific risks to the business, and how they should be addressed from a variety of perspectives, not just an IT viewpoint.

"By integrating cybersecurity into the corporate risk management program, companies can widen their scope to address additional areas including human, regulatory and reputational risks, as well as IT related issues."

He concludes that the market is less mature with less data protection regulation in place, often making cybersecurity a lower priority for GCs than in some other regions.

47%

of respondents in the region said they were very concerned about a cyber attack, the joint lowest of any region



CASE STUDY: LATIN AMERICA

Investigation and remediation of three-year network compromise

Kroll was engaged to provide incident response services for a large services and facilities management company in Brazil. An internal audit had alerted the client to a potential incident in its network. After completing an extensive computer forensic analysis, Kroll's experts determined that the company's internal systems had indeed been compromised – in fact, it was found that the network had been under attack for more than three years and the client's sensitive data had been exposed on the internet. Through advanced techniques, Kroll determined the root cause of the attack and assisted the client in the remediation process, which included the implementation of new security controls.

"Larger businesses in the region have developed more mature planning for cybersecurity and incident response. However, many smaller companies are still deficient in their cybersecurity posture"

Fernando Carbone, Senior Director, Cyber Security and Investigations, Kroll

Conclusion

However important cybersecurity may be, there will never be an unlimited supply of resources to throw at the problem. Money, people and time are always limited. What is important is to understand that unless the risks are fully understood and put into context, the resources that are available are unlikely to be used in an optimal fashion.

Ignoring cybersecurity problems does not immunise an organisation against an incident. No security regime is perfect, but those that spend time understanding the risks and making the best use of available resources are more likely to succeed in protecting the organisation, and being prepared to act swiftly and effectively when incidents occur.

What is clear from many survey respondents is yet another facet of human instinct: the desire not to admit something. To do so can be embarrassing. Very few of us readily want to admit to others: our mistakes, our weaknesses, our vulnerabilities, our lack of ability, our lack of understanding, or our lack of confidence. Professionally, lawyers sometimes have to, for the greater good of the organisation.

All of those admissions routinely apply to cyber risk and cyber protection. Mistakes are made. Systems are

vulnerable. People often do not, or cannot, understand the extent of cyber threats or the true capacity of technology to resist them. They do not fully understand the role that risk transfer through insurance products can play in their overall strategy.

But denial and complacency are not the answer. They ignore existing risk and create further potential risk. Resilience and responsibility — the themes of this report — depend upon recognising and making those admissions continuously. Those who are less prepared often have more pressing regulatory priorities, dependent upon the regions they cover. To help drive the necessary changes, local regulation has a way to go.

The true quality of an effective general counsel therefore comes with the wisdom to recognise and admit their own areas of weakness, and more importantly, those of their business and the environment in which they operate. Then they do something about managing the risks facing them. In a word: responsibility. Taking responsibility for the cyber risks in their business is a hallmark not of weakness, but of real strength.

And increasingly, GCs are taking responsibility. "General counsel are becoming the quarterbacks," says Smolanoff. "They're increasingly owning the risk that's associated with a breach and as a result, are taking on more and more cybersecurity responsibilities."

ABOUT KROLL

Kroll is the leading global provider of risk solutions. For more than 40 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security and data and information management services.

Headquartered in New York with more than 35 offices in 20 countries, Kroll has a multidisciplinary team of nearly 1,000 employees and serves a global clientele of law firms, financial institutions, corporations, non-profit institutions, government agencies and individuals.

ABOUT LEGAL WEEK INTELLIGENCE

Legal Week Intelligence is the independent research division of Legal Week, part of the ALM Media group of leading business publications.

For more than 12 years, Legal Week Intelligence has conducted research for global and national law firms, companies and vendors as a group or individually, under strict Market Research Society guidelines, on generic and industry-specific topics. Research can be in the public domain or form part of a confidential project for individual clients on a bespoke basis.

Over the years, we have reached out to thousands of associates, partners and general counsel.

We advise business leaders on their critical issues and opportunities including strategy, marketing, operations and technology. We work with leading organisations across the private, public and social sectors. We have deep functional and industry expertise, as well as breadth of geographical reach.

In all cases, Legal Week Intelligence benefits from access to the industry expertise of Legal Week editors and journalists, a dedicated research and analysis team, and the global reach of ALM Media and its affiliates.

This enables our clients to improve the quality of their decision making by providing them with reliable data, robust analysis and actionable advice.

We focus debate on the most important and pressing issues using scalable research products and a flexible multimedia output. Furthermore, we emphasise the conversion of our information into actionable advice and we strive to leave businesses stronger after every engagement.


HTML

Kroll®

Kroll's experienced leaders help clients make confident decisions about people, assets, and operations across the globe.

INVESTIGATIONS AND RISK MANAGEMENT SOLUTIONS

- Cyber Security & Incident Response
- Fraud & Corruption Investigations
- Asset Search & Recovery
- Dispute Advisory & Litigation Support
- Business Intelligence & Due Diligence
- AML & ABC Compliance
- Third-Party Screening
- Security Risk Management

kroll.com