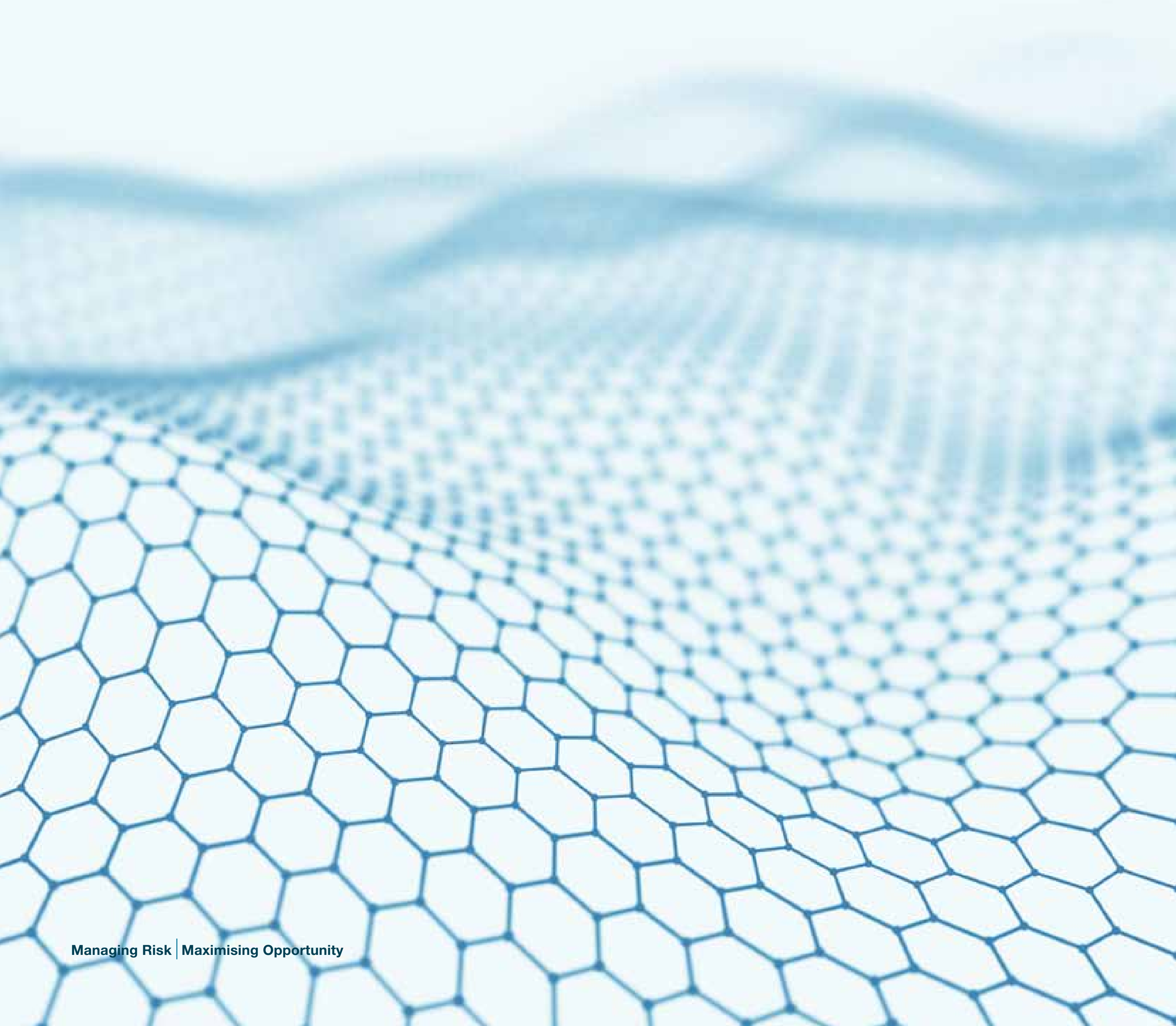
Control Risks

# Cyber Security Landscape

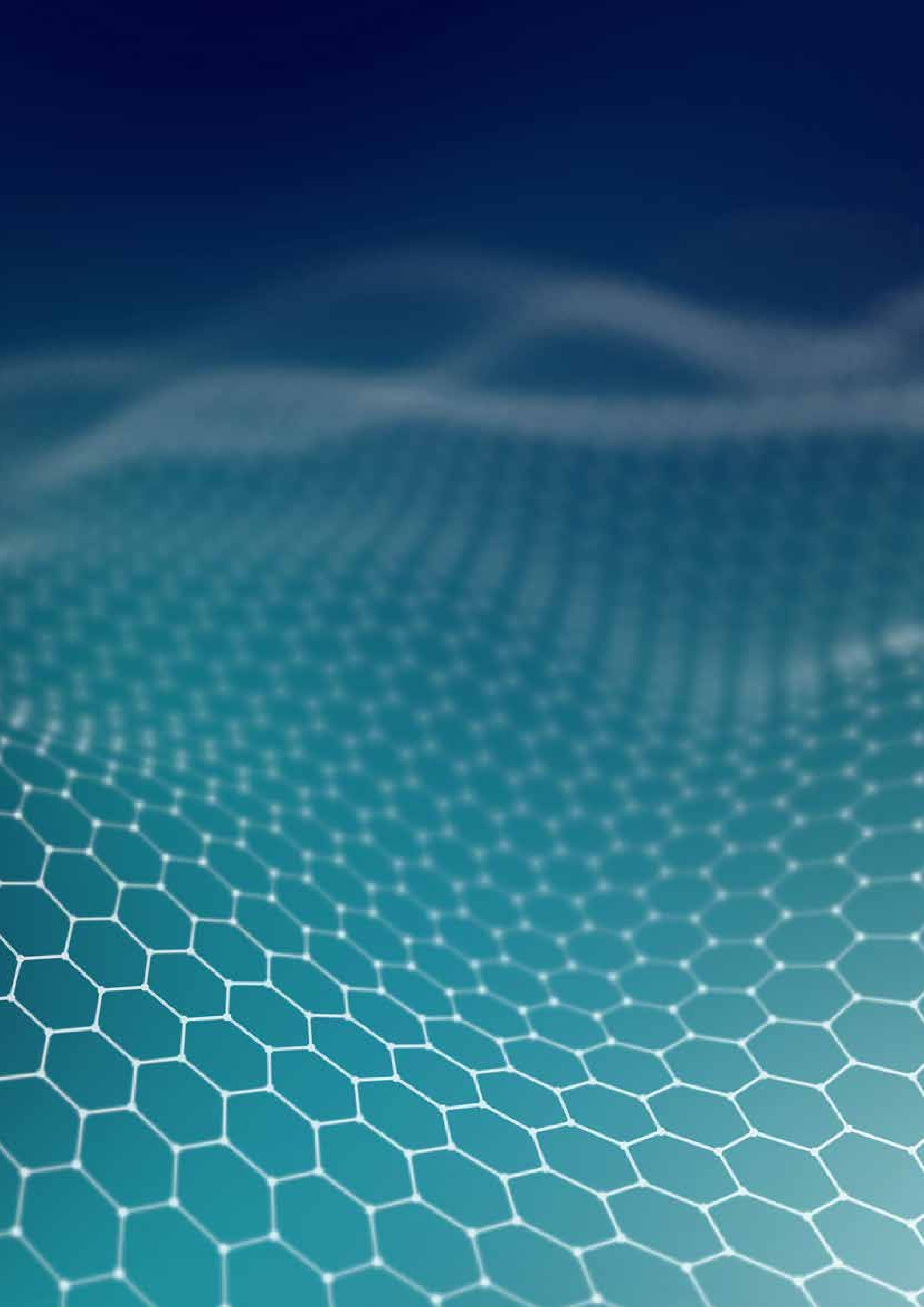
REPORT 2017



Managing Risk | Maximising Opportunity

Control Risks is a global risk consultancy. We help some of the most influential organisations in the world to understand and manage the risks and opportunities of operating around the world, particularly in complex and hostile markets. Our unique combination of services, our geographical reach and the trust our clients place in us ensure we can help them to effectively solve their problems and realise new opportunities in a dynamic and volatile world. Working across five continents and with 36 offices worldwide, we provide a broad range of services to help our clients to be successful.

# TABLE OF CONTENTS



# FOREWORD

**Toby Chinn**
**Partner and head of cyber security,**
**Control Risks**

Welcome to Control Risks' State of the Cyber Security Landscape Report 2017. We are pleased to present an in-depth analysis of the responses of IT and business decision makers from large organisations across 20 countries, each of which has more than 2,000 employees. Conducted in January and February 2017, this report is set against a backdrop of a continued growth in major cyber breaches including one of the largest ever ransomware attacks on 12th May which spread to over 150 countries within 12 hours, the WannaCry Ransom attack. Our analysis of the responses looks at what organisations across the globe are doing to defend against cyber threats, and to determine challenges and best practices to mitigate cyber security risks (the likelihood of those threats affecting a particular organisation).

We have discovered some fascinating insights on the way cyber risk is being managed, and the way in which organisations perceive it is managed. A standout finding is that a third of respondents' companies had not conducted a cyber risk assessment in the past year. Cyber risk changes faster than any other form of risk, so this is worrying.

One of Control Risks' consistent messages has been the need for board-level engagement in cyber security. Encouragingly, this picture is improving: most companies now have notional board oversight in matters of cyber security, but almost half of these companies' key IT and business decision makers think their boards have no proper grasp of the issues.

Control Risks' cyber security practice sits in a company with four decades of global business risk heritage. Our advocacy of board-level engagement in cyber security draws on our firm belief that all business risks have to be assessed in the round, not in silos.

The analysis in this report aims to help business leaders and key stakeholders who own cyber security to understand how other companies perceive their cyber security risk, who owns it and the challenges they experience in the face of a rapidly changing threat landscape.

I hope you find it an enlightening and informative read.

To speak to the cyber team please contact cybersecurity@controlrisks.com

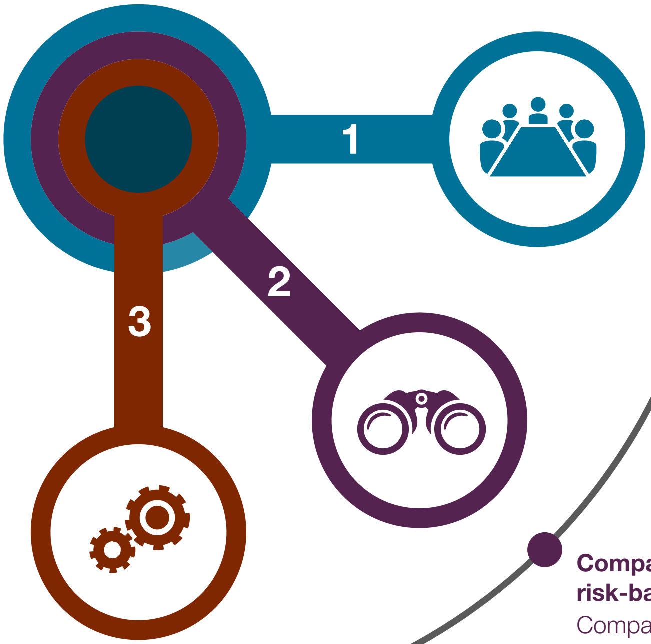
# INTRODUCTION

Cyber risk is frequently cited as one of the top priorities on a board's checklist. Yet all too often in practice it is still treated as 'an IT problem' instead of a major strategic corporate risk. Without full board-level support, the IT department often finds itself under-resourced, isolated from the rest of the business and without sufficient budget to manage cyber risks effectively.

Cyber tools and techniques used to attack organisations are often technically complex compared with other corporate threats organisations may face. Nonetheless, it is important that business leaders do not become overwhelmed by this technical complexity and maintain the same strategic approach as with any other corporate risk, starting by understanding the threat landscape.

This report looks at how global organisations are approaching cyber security in 2017. We asked respondents about their internal structures and accountabilities to manage these threats, cyber security and crisis management plans, as well as how their organisations are approaching the complex landscape of cyber threats. The results shed light on some interesting findings, three of the most significant of which are elaborated below.

## KEY FINDINGS



**Respondents lack confidence in their board's ability to manage cyber security threats:**

Although the assertion that cyber security is a "board-level issue" has been widely accepted, almost half (46%) of respondents reported that they believe their organisation's board-level executives do not take cyber security as seriously as they should.

**Companies struggle to adopt a risk-based approach**

Companies are less concerned with complying with auditable standards than with actually reducing the risk of a cyber attack, but almost half (45%) agree that assessing and managing these risks is their biggest challenge.

**Third-party breaches are a growing concern:**

A surprisingly high proportion (93%) of respondents stated that their organisation has sought to evaluate their third parties' cyber security measures. Against this, almost half (48%) agree that their organisation does not consider the impact of partners' or vendors' cyber security as much as they should.

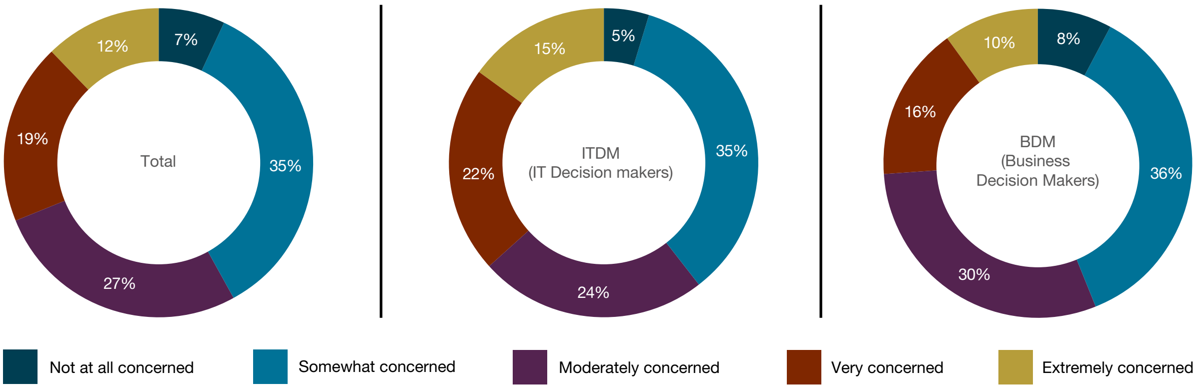
# RESPONDENTS LACK CONFIDENCE IN THEIR BOARD'S ABILITY TO MANAGE CYBER SECURITY THREATS

The threats posed by malicious cyber actors are now clear to businesses and to boards. Our reporting shows that cybercriminals are developing increasingly specialised tools with which to target specific organisations, and that the growing spread of such tools allows a wider range of criminals to attack higher-value targets in SMEs and big businesses. Spending to mitigate this has risen accordingly, and a study released in October 2016 by market intelligence firm IDC forecasted that "world-wide revenues for security-related hardware, software, and services will grow from $73.7 billion in 2016 to $101.6 billion in 2020".[1]

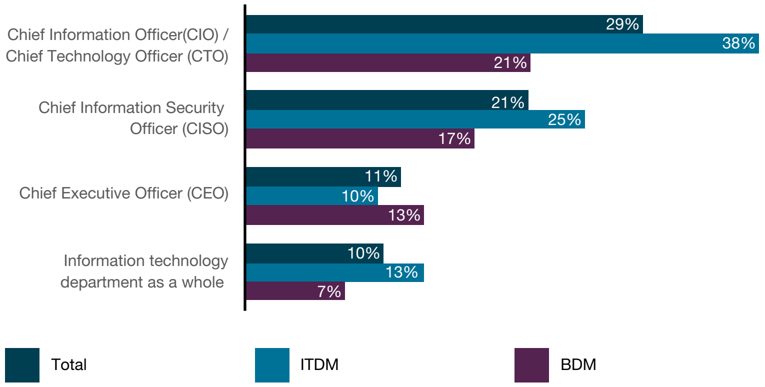
Ownership of cyber risk has also reached senior executive level. When asked about who is most accountable for cyber security management and decision making in their organisation, 77% of respondents cited the C-suite rather than the historic owner, the IT department.

Yet, despite seemingly clear ownership and investment at a senior level, the survey results indicate a lack of confidence in senior management or the board to successfully manage cyber risks. Almost half (46%) of respondents said they do not believe their organisation's board-level executives take cyber security as seriously as they should. Similarly, almost a third of respondents (31%) reported that they are very or extremely concerned that their organisation will suffer a cyber attack in the next year.

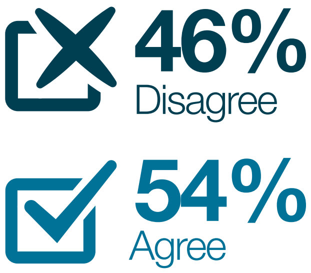
"How concerned are you that your organisation will suffer a cyber-attack in the next year?", asked of all respondents, split by respondent type



Analysis showing the four most likely accountable parties for cyber security management and decision-making within respondents' organisations, asked of all respondents, split by respondent type



Analysis showing whether respondents agree or disagree that their organisation's board level executives do not take cyber security as seriously as they should, asked of all respondents



[1] http://www.idc.com/getdoc.jsp?containerId=prUS41851116

## OUR RECOMMENDATIONS

So what should organisations do to instil greater confidence in the C-suite's ability to manage cyber security?

Organisations should treat cyber security as an enterprise risk and develop a mitigation strategy that not only protects the company, its assets and its operations, but also enables business. Actionable recommendations include:

1. Ensure cyber security becomes a regular board agenda that includes reviewing your external cyber threat landscape, and include an IT expert or create a committee to address the issue as a wider business threat. This also enables you to ensure that the cyber security budget is being spent in the most effective way
2. Conduct regular cyber crisis management exercises that involve all relevant parties – including the C-suite, IT, legal, communications and any other members of your crisis management team – so that all parties understand their roles and responsibilities and the potential implications of a cyber attack
3. Ensure all employees, including the board, are educated to understand their potential cyber exposure and how a breach might occur in any part of the business

### Control Risks in action

Control Risks is supporting one of the world's largest insurance companies to develop and deliver cyber crisis management training at the most senior level of its regional subsidiaries.

Our consultants developed specific crisis plans for the senior management teams of these subsidiaries, as well as an interactive training seminar and practical crisis simulation to be run in each location over the next three years.

The training content is designed to raise awareness and understanding at C-suite level of how cyber threats can impact operations and the issues they raise for the wider business. This is significantly helping to bridge the gap between the technical and the mainstream business functions.

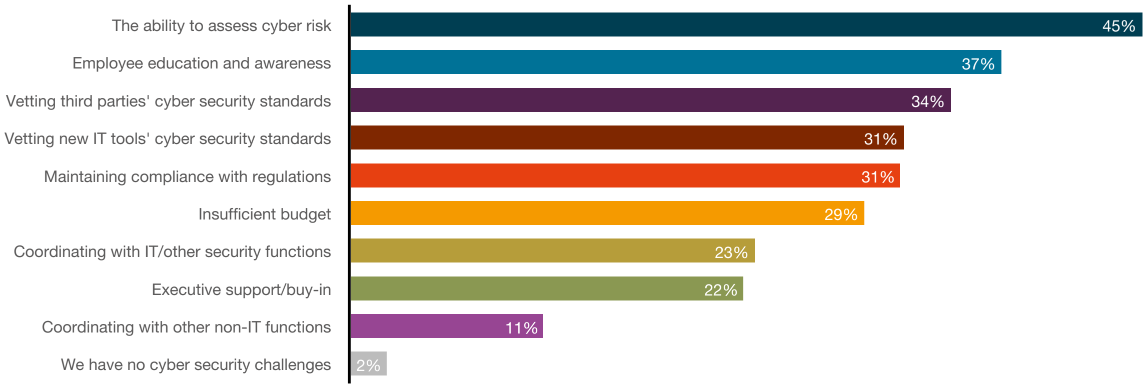
# COMPANIES STRUGGLE TO ADOPT A RISK-BASED APPROACH

Encouragingly, companies acknowledge the limitations of taking a compliance-driven approach to cyber security. Only 9% of respondents said that meeting the latest standards was their top priority. While there can be benefits to standard frameworks (such as ISO 27001) in facilitating a systematic and structured approach to cyber security, they also often fail to communicate with clarity where an individual organisation should focus its efforts.

It seems that companies recognise the importance of using an adaptive framework to assess and monitor cyber risks on a continual basis. However, organisations are struggling with this; even though 68% of respondents had performed a risk assessment in the past year, 45% of respondents cited risk assessment as their primary challenge.

On the one hand, these responses show the importance companies place on assessing cyber risk. On the other hand, the answers could indicate that these risk assessments are not sufficiently meaningful to shape an effective strategy and drive change across the company.

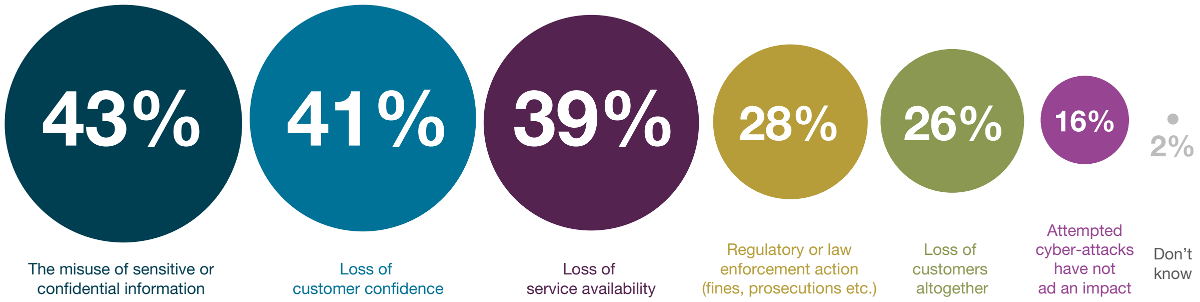
Analysis showing the top-three ranked challenges that respondents' organisations face regarding cyber security, asked of all respondents (482 respondents)



Arguably more concerning are the other 32% of respondents who said they had not conducted a risk assessment at all within the past year. In view of such an evolving threat landscape, these businesses are clearly leaving themselves even more vulnerable by not assessing their cyber risks more frequently, or at all, compared with those that have done so at least once in the past year.

With 43% of all respondents reporting a compromise or data breach, the need for effective risk management is clear. For companies that have not implemented proactive security measures and have fallen victim to a cyber attack, 28% have faced regulatory or law enforcement action while 26% have lost customers.

"Has a cyber-attack on your organisation resulted in any of the following?", asked of respondents who say that a malicious activity has been attempted on their organisation (444 respondents)



## OUR RECOMMENDATIONS

Developing an effective security posture requires a comprehensive cyber risk assessment to identify gaps in cyber security across the wider organisation and potential legal, reputational and financial implications of a breach.

Such risk assessments will start by taking the wider business through the process of how an external threat actor (e.g. a cybercriminal) may utilise a specific attack method to gain access to data and systems and exploit them. Assessing risks on this basis will help to explain exactly why other departments and senior leaders need to take action and champion relevant parts of any cyber security strategy. Such an approach also ensures that the variables that indicate how a risk may evolve over time (threat, likelihood, impact) are fully understood, leading to clearer discussions on prioritising spending and focusing effort on the areas that matter most.

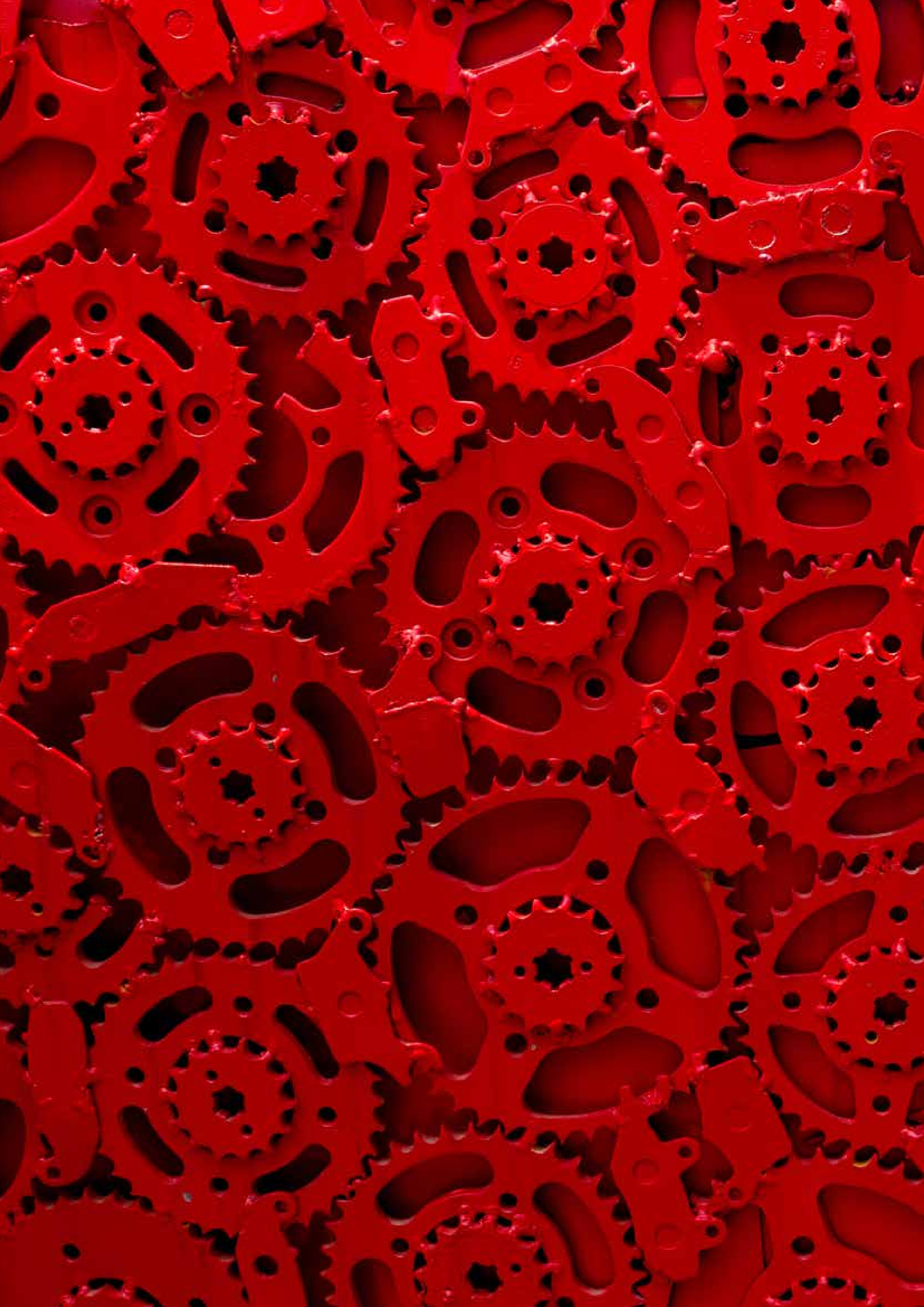
### Control Risks in action

Control Risks worked with one of the world's largest sustainable investment management companies to understand the nature of the cyber security threat it faced, and how attractive it might be as a target.

Our consultants carried out this work in two key parts: firstly by identifying the client's most critical assets (by considering impact and threat) and hence those most attractive to cyber threat actors; secondly through an in-depth cyber threat assessment to determine both the capability and intent of cyber threat actors to target these assets.

Building on this work, we developed a set of scenarios that described plausible methods by which the most likely threat actors might try to access the client's critical assets.

These scenarios were presented to the company's executive committee and used to inform key decisions in cyber security strategy over the following year.



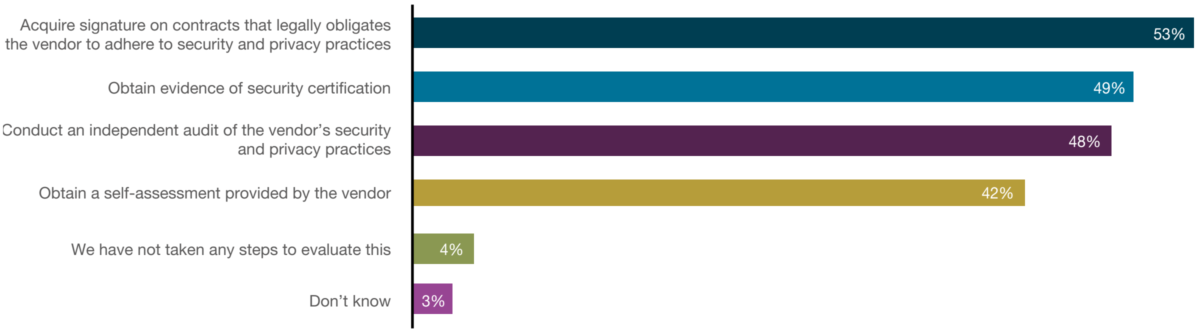
# THIRD-PARTY BREACHES ARE A GROWING CONCERN

In today's business environment, almost all companies rely on third parties in their supply chains. This creates a potential extension of their cyber risk. This is especially the case as organisations increasingly outsource sensitive aspects of their business such as payroll and other finance functions, technology service providers, legal functions and even research and development. A cyber breach on one third party's systems can have significant consequences for the wider network. As Ben Lawsky, New York State's top financial regulator, said in a letter to dozens of US banks: "It is abundantly clear that, in many respects, a firm's level of cyber security is only as good as the security of its vendors."

Just over a third (35%) of respondents said a third-party cyber breach has affected their organisation. This was higher for respondents in Asia (39%) and the Americas (38%), which may reflect regional differences in organisations' willingness to disclose cyber breaches to their customers.

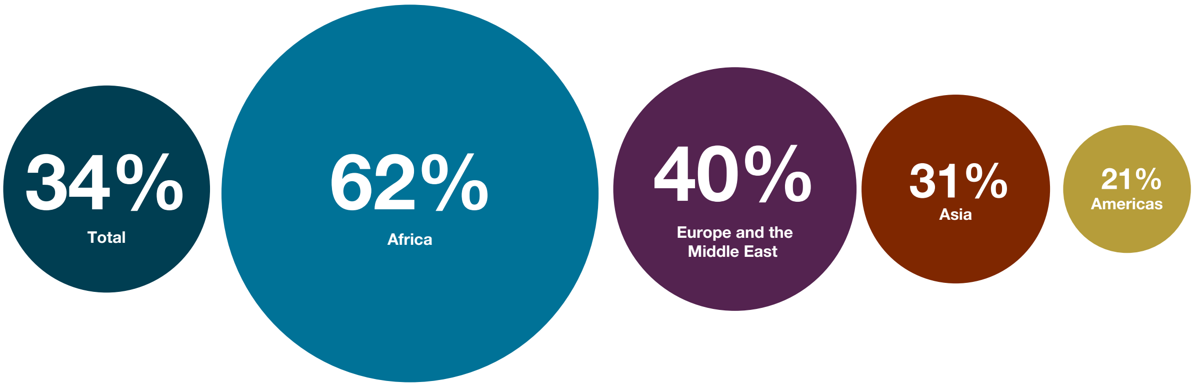
Despite the importance of planning for the breaches of third parties' systems, the measures companies currently take to manage cyber security risk beyond their own IT ecosystems appear insufficient. While more than nine in ten respondents (93%) stated that their organisations have taken steps to evaluate their third parties' cyber security measures, 53% said this just consisted of inserting a clause in contracts to impart obligations on the other party.

"What steps has your organisation taken to evaluate your third parties' cyber security measures?", asked of all respondents (482 respondents)



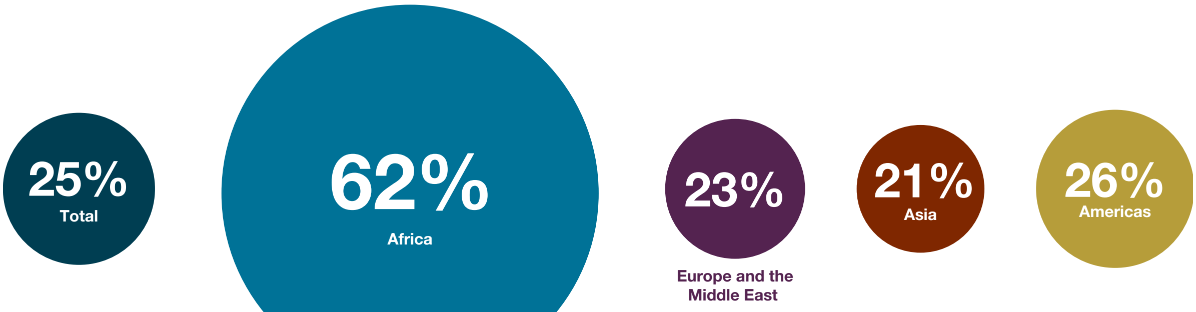
Almost half (48%) agree that their organisations do not consider the impact of partners' or vendors' cyber security as much as they should. Over a third of respondents (34%) said that vetting third parties' cyber security standards is a challenge, and fewer than one in four (23%) respondents described their organisation's approach to cyber risks resulting from the use or acquisition of third parties as excellent.

Analysis showing respondents whose organisations do not have a cyber-crisis management plan for the event of a breach, asked of all respondents (482 respondents), split by respondent region

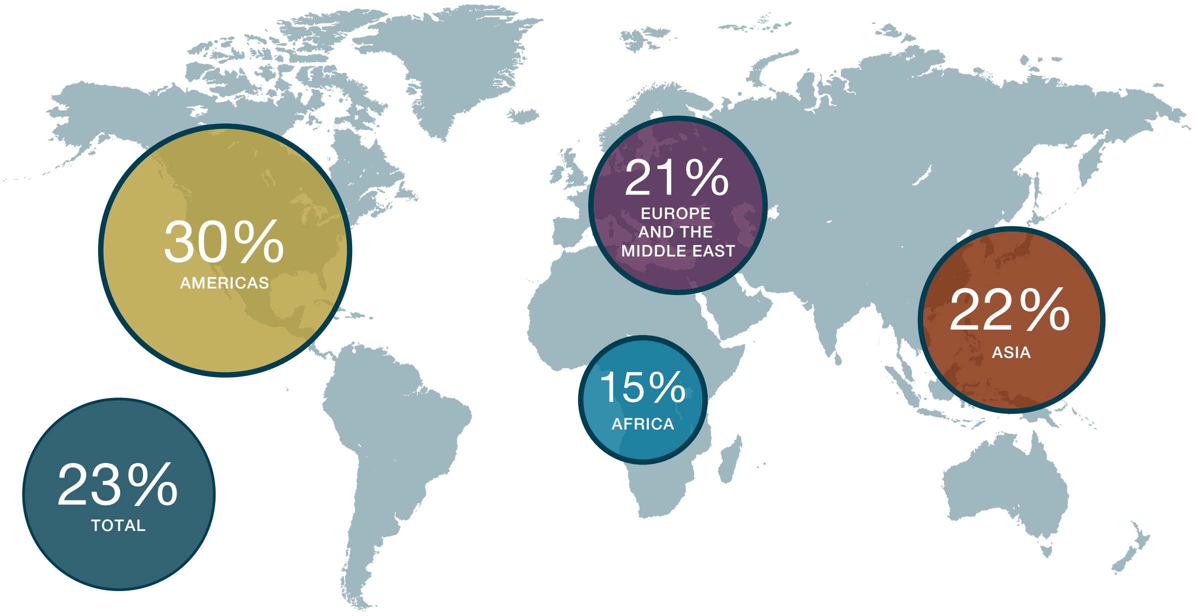


Of respondents whose organisations have cyber crisis management plans, a quarter (25%) say they do not address what third parties should do if they suffer a cyber breach that may impact the respondent's organisation. This was highest (62%) for respondents in Africa and lowest (21%) for those in Asia.

Analysis showing respondents whose organisation's cyber-crisis management plan does not cover what third parties need to do if they suffer a cyber-breach that may impact on them, asked of respondents whose organisation has a cyber-crisis management plan (315 respondents), split by respondent region



Analysis showing respondents who rate their organisation's approach to cyber risk that has been created as a result of the use of, or acquisition of third parties as excellent, asked of all respondents (482 respondents), split by respondent region



## OUR RECOMMENDATIONS

It is clear that organisations recognise the threat that a breach of a third party can pose, with many attempting to take steps to understand the impact on their business. Yet, there is still much that can be improved, including adopting a risk-based approach to vetting third parties. This should go beyond simply acquiring a signature on contracts to legally oblige the vendor to adhere to security and privacy practices, as 53% stated. Therefore, cyber security should be included in a company's broader vendor vetting process, which should consider the company's broader risk strategy and account for accepted risks as well as proactive mitigations.

Beyond this, companies should ensure that their crisis management plan accounts for circumstances that may lead to a loss of customer data, or fines as a result of a third-party breach. Having a comprehensive cyber crisis management plan in place is a prerequisite to real preparation. Crisis management is a discipline that requires practice: communication, proactive response and co-ordination are easier to achieve when scenarios have been rehearsed and managers are familiar with the issues and how to respond. By exercising crisis management plans in a simulated environment, participants can begin to understand the scope of the demands that will be placed on them in the event of a cyber attack.

### Control Risks in action

In 2017, Control Risks supported a client that had received credible reports that it had lost sensitive client data including personally identifiable information. The breach had occurred as a result of a vulnerability in a third party's systems.

Faced with the dilemma of how to respond to the purported hacker and what to report to the regulator and to its own clients, we helped the client to:

- Map out the possible extent of the compromise; this informed the communication with regulators and clients
- Form a profile of the purported hacker, to advise the client on how to react to any demands or further contact from the perpetrator
- Advise the client on what assurance about cyber security it could reasonably expect from its third-party suppliers
- Conduct cyber due diligence on a newly appointed third-party supplier

The effect was to help the client regain control of the situation and communicate effectively and credibly with stakeholders.

# THE VIEW FROM AFRICA

Half a billion US dollars – that's how much cyber-related incidents now cost organisations in Nigeria each year. The figures for many other African countries are similarly high, estimated at USD 50m for Uganda and USD 250m in Kenya. But even these figures are likely to understate the problem; most African countries don't record such losses in a formalised, mandatory manner and most organisations don't report any potential or actual losses to authorities.

Regulation and legislation related to information security and data protection also continue to lag behind other parts of the world. As such, while cyber security is considered an emerging threat in Africa, a lot more work is required in understanding the threat to organisations in specific countries and sectors.

In our conversations with clients, senior executives acknowledge that cyber risk is at the top of their agenda. However, according to African respondents in Control Risks' latest 'Cyber Security Landscape' report, 62% do not have any cyber crisis management plan in place to help them respond to a breach (compared with 40% in Europe & Middle East and 31% in Asia).

This suggests that the threat of a breach remains abstract for many senior executives who have not yet worked out in detail how their organisation would deal with one. Additionally, for most organisations in Africa, cyber risk is still primarily the responsibility of IT staff, who struggle to get buy-in from senior management for investment in cyber crisis planning.

Our survey also found that 62% of African respondents say their plans do not cover what their third parties need to do if they suffer a cyber breach. This is despite the fact that most organisations depend on third parties (such as web hosting and IT service providers, as well as clients) to operate their businesses and are connected to them in many ways – offering cyber threat actors potential points of entry to their own systems.

We spoke to a number of organisations in Africa who indicated that the third party risk is largely covered by their contracts with those third parties. A few organisations indicated that they also carry out independent reviews of third parties, which we encourage all organisations to do on a regular basis. One organisation also indicated that they require their third party partners to obtain cyber insurance before they allow them to access the organisation's network.

As the recent WannaCry ransomware attacks proved, cyber breaches are global in nature; Africa isn't immune, with reports of attempted and successful attacks in more than 10 African countries. These types of attacks should also lead organisations to treat cyber threats as a matter for the whole business, rather than just the IT department. This means the board should set the right information security culture and risk appetite for the organisation, which should then translate into actionable plans for senior management, led by the CEO.

Planning for a cyber crisis should also be the responsibility of senior management rather than just IT. Such planning should involve the whole organisation and start with understanding the key threats an organisation faces, and the key assets needed to continue operations in the event of a breach.

**Patrick Matu**
Associate Director

# VIEW FROM THE AMERICAS

Cyber security risk is a constantly evolving and rapidly growing problem that organisations worldwide must address. Based on reported analysis of cyber threat intelligence by Control Risks, there has been an approximate 11% increase in threats related to cybercrime across the region in the past year, and as high as a 30% increase in Mexico. Fortunately, a number of organisations across Northern, Central and South America are allotting the time and effort necessary to identify timely and cost-effective solutions that can be implemented to reduce the impact of a cyber-enabled breach. As many as 17 national Cyber Security Incident Response Teams (CSIRTs) have been formed in countries all over the region, including in Bolivia, Costa Rica and Paraguay[1].

In spite of investment at the company and national levels, incidents of ransomware in Latin America continue to increase and watering hole attacks are becoming more common. Overall, Latin America remains a target-rich environment where even unsophisticated cybercriminals are often successful, suggesting that current trends will persist.

## CLOSING THE GAP IN CYBER SECURITY RISK MANAGEMENT

While some markets across Northern America are considered more mature in their approach to cyber security risk management, other markets across Latin America are working to close the gaps. This shift in awareness in Latin America is the combination of two factors:

- Rapid market maturity towards digitization creating increased exposure, such as the financial industry in Argentina, Brazil and Mexico pushing towards online and mobile banking
- Significant increases in cybercriminal activities and high-profile breaches, such as the Panama Papers leaks and a data breach at Chile's Ministry of Social Development

Due to the rapid evolution of tactics, techniques and procedures used by threat actors, a compliance-driven approach to cyber security is no longer effective. Companies are actively shifting their cyber security focus by incorporating routine risk assessments, but still require assistance in truly identifying their risks overall.

While 58% of respondents in the American market cited risk assessments as their primary challenge, 78% of respondents had performed at least one risk assessment in the past year. These trends in the Latin America market show a step in the right direction, though there are still improvements to be made.

## MITIGATING THE BUTTERFLY EFFECT

Many companies rely on third party vendors for products and services that are essential to operational success, but third party access can often give cyber threat actors a point of entry from which to breach their main target. Based on our survey, at least 38% of respondents in the Americas reported that a third party cyber breach has impacted their organisation. The true figure may be higher, due to the relaxed requirements for reporting successful cyber breaches in parts of the Americas region.

To combat third party breaches, 96% of respondents in the Americas market said they have taken steps to levy stricter requirements for third party cyber security measures. However, 63% of these steps only consist of inserting a clause in contracts to impart obligations on the third party.

These findings highlight the difficulties of assessing cyber risk, messaging to senior management, and managing third party risks. Each organisation shares similar interests in cyber security risk, and market maturity is in no way a barometer of how well a company will be protected in the event of a breach.

It will take a collective effort – not just among private businesses, but also among public and government institutions – to create and sustain a secure and resilient computing environment. Understanding the threats your company faces is the first step in maintaining and protecting your people, processes and technology.

**Kate Yamashita**
Principal

[1] Ciberseguridad, Estamos preparados en America Latina y el Caribe? Organizacion de los Estabdos Americanos y BID. 2016 (Cybersecurity. Are we prepared in Latin America and the Caribbean? Organization of American States and IDB. 2016)

# THE VIEW FROM ASIA

Asia leads the world in internet usage, but it falls behind other regions in its approach to cyber security. The Cyber Security Landscape report identifies two policy issues that are holding the region back:

## COMPANIES IN ASIA PACIFIC CONTINUE TO VIEW CYBER SECURITY AS A COMPLIANCE ISSUE RATHER THAN A BUSINESS RISK

When it comes to measuring success of their cyber programme, 42% of respondents in Asia Pacific (excluding Australia) benchmark against whether it meets the latest regulatory requirements (versus a quarter in Australia). With cyber policy and regulatory landscape in Asia Pacific (excluding Australia) still largely underdeveloped and unevenly implemented, the struggle to maintain compliance is somewhat unsurprising. In short, the regulations are not strong enough to really enable companies to effectively manage the risk. Solely following the local regulatory standards instead of adopting a more holistic risk- based approach could leave many companies open to a costly and reputation-damaging breach.

Unfortunately, the situation is exacerbated by the fact that cyber security is still not on the board agenda of enough companies in Asia. Half of the survey's respondents in Asia say that their organisation's board does not take cyber security as seriously as it should. One of the main reasons for this is simply a lack of awareness. In many markets in Asia, companies are not required to publicly disclose a cyber-breach, and a cultural tendency to deal with issues privately results in lost opportunities to learn from peers and implement industry best practice defences.

Australia conversely, is a regional and global leader in terms of cyber regulatory developments, implementation and enforcement. Interestingly though, survey respondents are far more focused on adopting this more holistic approach, treating cyber as a 'risk issue' instead of a 'compliance issue'. This is facilitated by two things in particular: an evolving corporate governance landscape which works to support and improve company performance and a commitment by business and government to work together to tackle cyber issues.

## COMPANIES ARE INCREASINGLY CONCERNED THAT THEY WILL SUFFER A CYBER-ATTACK, BUT THEIR ABILITY TO IDENTIFY WHERE THOSE ATTACKS ARE COMING FROM IS LOW

More than 9 out of 10 organisations in Asia Pacific have suffered an attempted attack, and a similar number are concerned that their organisation will suffer a cyber-attack in the next year. However, almost two-thirds of organisations in the region are unable to identify where all attempted cyber-attacks come from. When the threat of an attack is so prevalent, why are organisations so ill equipped to identify, and therefore accurately and economically mitigate against any potential sources of attack? The lack of insight among business leaders tasked with their organisations' cyber security is again a factor, but in many cases (particularly in South East Asian countries such as Indonesia, Vietnam and Thailand), it is also a result of rapid digitisation, combined with a lack of technically skilled and experienced professionals to implement and maintain an appropriate level of cyber hygiene.

In more developed countries in Asia Pacific, such as Singapore, sophisticated companies are now leading a shift towards a more strategic focus on threat actors and their capabilities. A number of organisations in the critical infrastructure industries now have in-house threat intelligence teams focussing on the technical, operational and strategic aspects of threat intelligence, enabling them to meet the challenge effectively.

It is only by adopting this threat-led approach to cyber security that an organisation, wherever they might be operating in the world can really understand the potential impact on the business and adopt the necessary measures to be able to protect it from any potential cyber threats.

**Ben Wootliff**
Partner

# THE VIEW FROM EUROPE

Due to the recent WannaCry attack, cyber security has had a high profile in the press lately. A summary by the BBC points out that, in the first few hours of the attack, 61 National Health Service organisations in the UK were affected. In France, some Renault factories even had to stop production.[2] This poses the question: how do businesses in Europe compare against their peers worldwide when faced with cyber security challenges such as these?

### COMPANIES IN THE UK ARE MORE CONCERNED THAT THEIR ORGANISATION WILL SUFFER A CYBER ATTACK IN THE NEXT YEAR THAN BUSINESSES IN FRANCE AND GERMANY

Only a small minority (3% in the UK and 7% in Sweden) of respondents in Europe are not at all concerned that their organisation will suffer a cyber attack in the coming year. In contrast, 10% in the UK are extremely concerned – twice as many as in Germany and France. Comparing these results with those from the US and Brazil, however, numbers in European countries remain relatively low: 19% of respondents in the US and 45% in Brazil said they were extremely concerned about an attack in the near future.

### CYBER CRISIS MANAGEMENT PLANS CAN PROTECT BUSINESSES, BUT MANY COMPANIES HAVE NO PLAN FOR THEIR ORGANISATION IN THE EVENT OF A BREACH

Responses in countries across Europe differ distinctly. While cyber crisis management plans have become established in German companies in recent years (81% of German organisations that participated in this survey have a clear roadmap in case a breach happens), this is only the case for 36% of respondents in France.

Results for the Netherlands (67%) and the UK (63%) rank in the mid-range whereas 90% of respondents in the US say they would know how to react in the event of a breach. Surprisingly, some of the companies that do not have a cyber crisis management plan are not planning to develop a strategy: 5% in the UK, 6% in France and 7% in Sweden.

### THE MOST SIGNIFICANT CHALLENGES TO AN ORGANISATION'S CYBER SECURITY VARY FROM COUNTRY TO COUNTRY

Employee education and awareness pose the biggest challenge for European organisations dealing with cyber security. Other challenges include their ability to assess cyber risks within the current IT network, though this seems to be a concern for UK businesses (40%) far more than organisations in Germany (27%) or in France (only 8%).

However, French companies struggle with maintaining compliance with current regulations and suffer from insufficient budgets. More than one third of the German companies interviewed face the challenge of vetting cyber security standards in new IT tools and among third parties such as clients and contractors.

As the regional results indicate, cyber security preparedness can vary immensely from country to country, organisation to organisation based on the perceived challenges faced. And yet as major attacks such as WannaCry illustrate, often businesses won't really know how ready they are for a major attack until it hits. With such a fast evolving cyber threat landscape and continual growth of new tools and tactics, it is essential that potential cyber risks to the business are assessed in a holistic manner on a regular basis and that cyber security is not just perceived as something that needs to be handled by the IT team, but is a problem for the entire business.

**Jayan Perera**
Associate Director

[2] http://www.bbc.com/news/technology-39920141

# VIEW FROM THE MIDDLE EAST

Cyber has been in the press extensively in the Middle East with Gulf News running headlines such as: "*The country is now the second most targeted country after the US, according to statistics shown at the UAE's new Cyber Security Centre*[3]."

Yet media headlines such as this apparently have yet to translate into local business fears: None of the of the GCC respondents said that they were "extremely concerned" they would be hit by a cyber-attack this year, compared to 31% of respondents globally. While risk awareness of the cyber threat is rising globally, there appears to be a regional complacency in the Middle East of safety from pervading attacks. However, this is not the case and the number of organisations suffering damaging and often embarrassing attacks is growing daily.

## ACKNOWLEDGING CYBER SECURITY AS A BUSINESS RISK

Part of the issue is the lack of senior management buy-in to the cyber security challenge. With the increasing reliance on, and inter-dependencies between, business processes and IT, cyber and digital security is now widely recognised as a business issue rather than something which rests in the domain of traditional IT function.

Yet despite this, 87% of GCC respondents identified cyber security as an issue still entirely under the ownership of the IT function. Meanwhile mature cyber security markets (Americas, Western Europe and parts of Asia Pacific) have a much wider buy in with only 53% of respondents seeing cyber security purely as an IT issue.

The cyber threat is fundamentally a business risk. It cannot remain solely in the domain of IT. Any high profile cyber event causes global headlines (the recent breach of a regional bank and the Shamoon 1 and 2 attacks being cases in point). These types of attack severely impact the reputation of an organisation as well as its financial performance, with lost revenue (customers not using them for fear that the data is not safe), and a subsequent potential fall in share price.

So why do 87% of GCC respondents believe it's an "IT only" issue? Not having a joined-up, business-led response to this in place is the equivalent to regarding a fire in your headquarters just being a "facilities issue" or regarding having 50% of your staff unavailable through illness as solely being a problem for your human resources function. All of these potential crisis require a business led response.

## CYBER ATTACKS ARE BECOMING ALMOST ROUTINE

Costly attacks are now almost routine: 92% of respondents globally said they have had malicious activity attempted on their organisation, and of those who have 43% said it resulted in the misuse of sensitive or confidential information and 26% said it resulted in the loss of customers. Companies in the region are primarily making new investments in technological solutions to attempt to remediate the growing cyber threat, with organisations investing firewalls and intrusion detection solutions. But too often this is not implemented in conjunction with effective training and awareness for staff. The strongest (and most cost effective) defence an organisation can have to the cyber threat is an informed and vigilant workforce. Ensuring your staff are effectively trained creates a "human firewall". This, in conjunction with technical solutions and a joined up business led response capability, provides the best protection for your organisation.

**William Brown**
Director

[3] http://gulfnews.com/business/sectors/technology/uae-second-most-targeted-country-by-hackers-after-the-us-1.1883164

# CONCLUSION

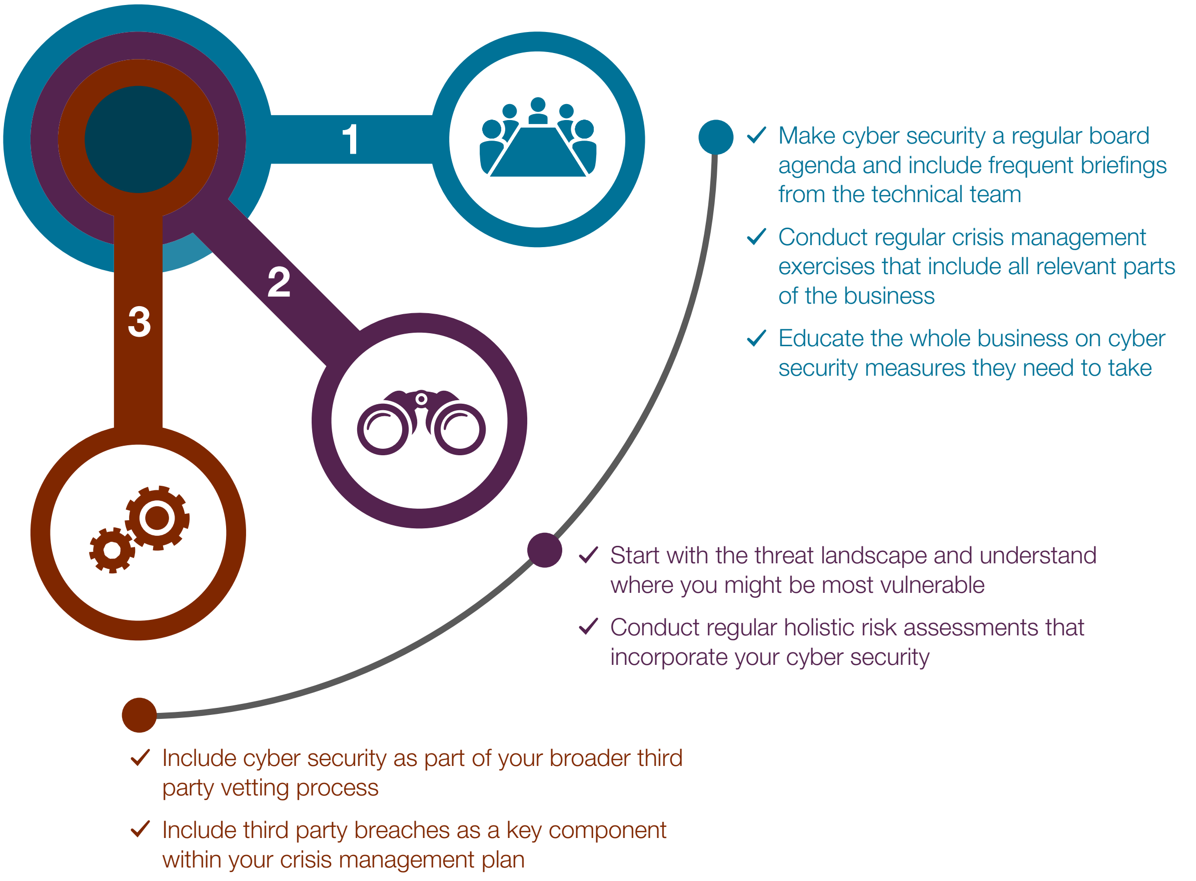
The major challenges for businesses managing cyber security are found in the baseline activity of assessing cyber threats and risks and in communicating these to senior management. Cyber risk among third parties is a growing part of managing the suite of risks presented by complex supply chains, and our report shows that many companies feel they have not got to grips with this.

Another common theme is that perceptions of cyber risk are misaligned within respondent organisations. For example, when evaluating risks, individuals who have focused on addressing IT controls and processes may feel that their defences have improved but that vulnerabilities in other business departments and external parties remain an issue because they are beyond the scope of their influence. A recent example of this could be illustrated with the WannaCry ransom attack, which keenly showed how vulnerable an organisation can become if gaps occur across a business in cyber security measures. Moving toward a common perception of cyber security as a holistic business risk must be the next step in tackling today’s challenges.

Our advice is always to start with the threat; how cyber threats are assessed and communicated throughout the business is key. This should involve considering the specific cyber security threats to the organisation, what impact these threats might have and how current controls mitigate them. Having assessed these risks, the organisation can then integrate them into the organisation’s overall risk management strategy.

Taking the wider business through the process of how an external threat actor (e.g. a cybercriminal) may utilise a specific attack to gain access to data and systems and exploit them will help to explain exactly why other departments and senior leaders need to take action and champion relevant parts of any cyber security strategy. Such an approach also ensures that the variables that indicate how a risk may evolve over time (threat, likelihood, impact) are clearly understood, leading to clearer discussions on prioritising spending and focusing effort on the areas that matter most.

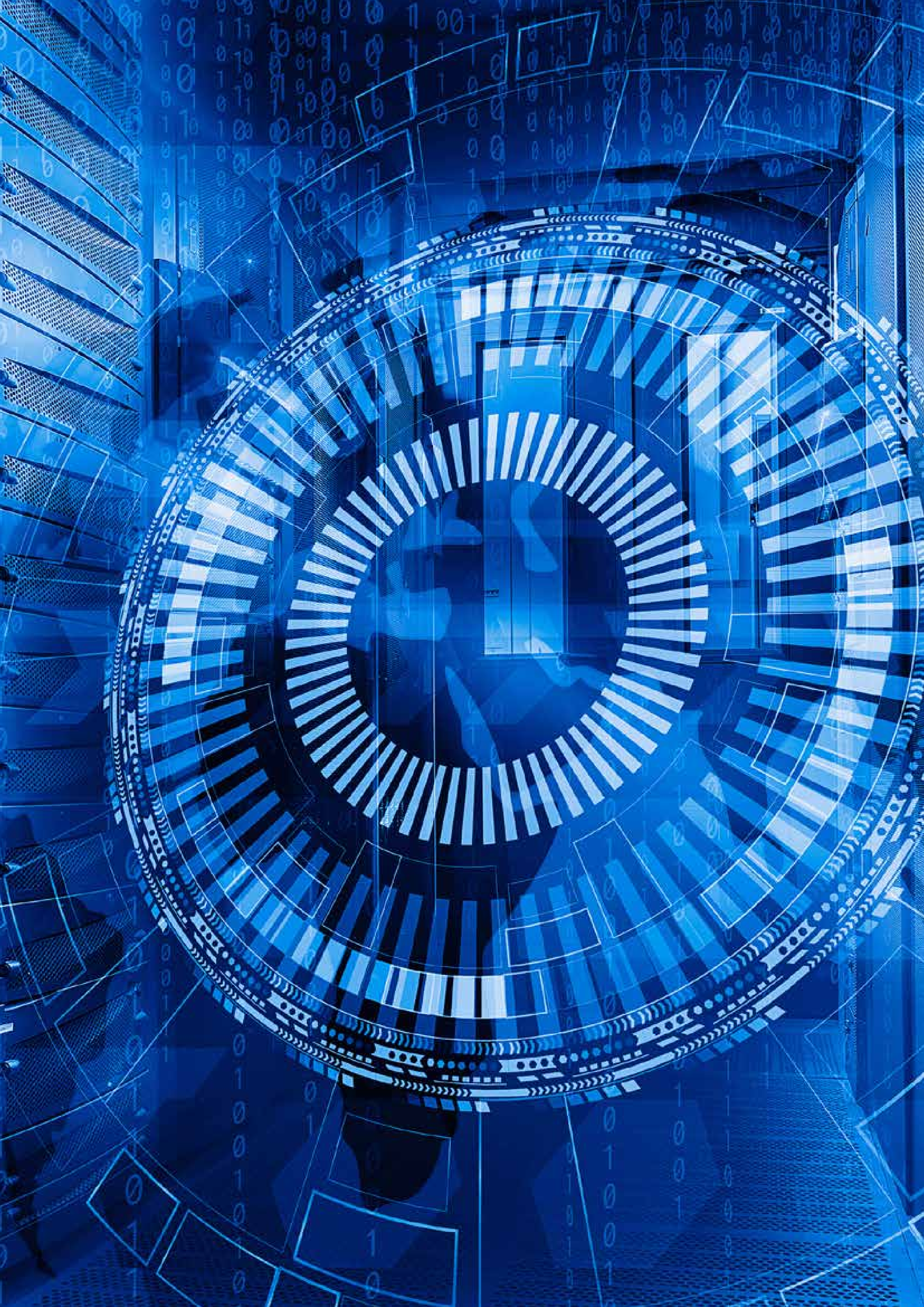
Finally, no defensive line is impenetrable. This particularly applies when new threats are emerging the whole time, as is the case with cyber security. Flexibility and the ability to manage a crisis are key components of any business’s cyber security strategy.



- ✓ Make cyber security a regular board agenda and include frequent briefings from the technical team
- ✓ Conduct regular crisis management exercises that include all relevant parts of the business
- ✓ Educate the whole business on cyber security measures they need to take

- ✓ Start with the threat landscape and understand where you might be most vulnerable
- ✓ Conduct regular holistic risk assessments that incorporate your cyber security

- ✓ Include cyber security as part of your broader third party vetting process
- ✓ Include third party breaches as a key component within your crisis management plan

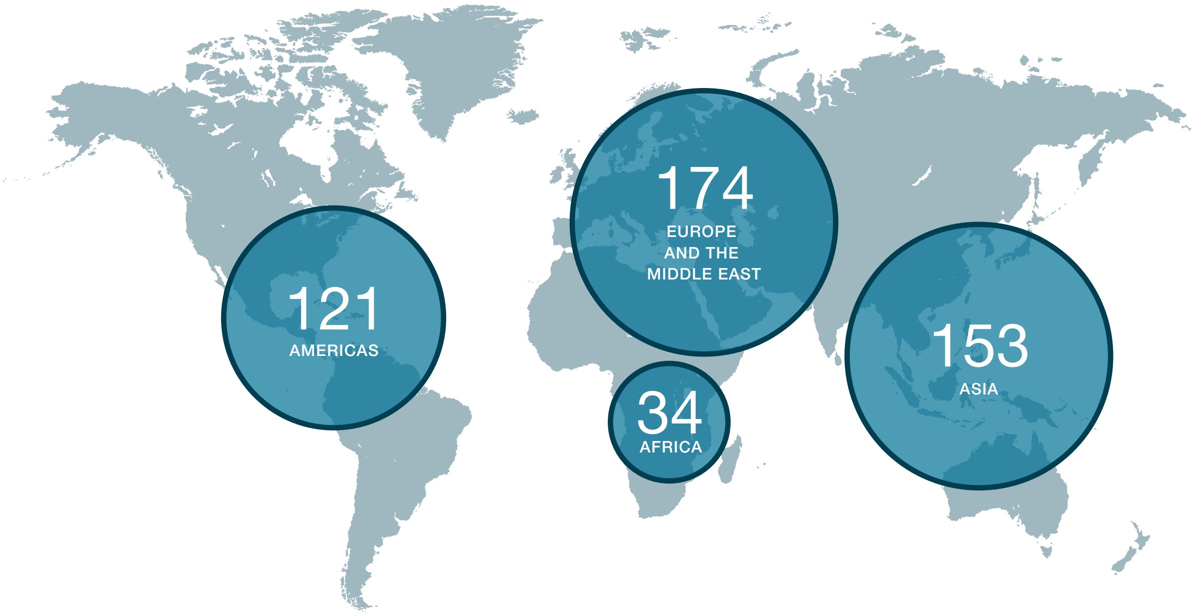


# ABOUT THE REPORT

482

IT DECISION MAKERS AND BUSINESS DECISION MAKERS WERE INTERVIEWED IN JANUARY AND FEBRUARY 2017

RESPONDENTS SPLIT ACROSS 4 REGIONS AND 20 COUNTRIES



RESPONDENTS' ORGANISATIONS HAD TO HAVE AT LEAST

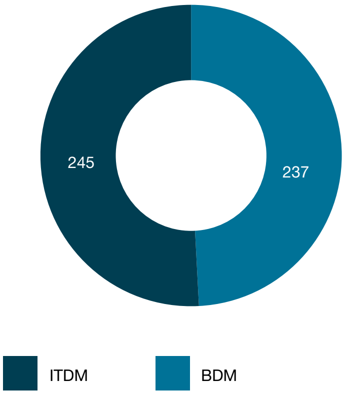
2,000 employees

RESPONDENTS WERE INTERVIEWED ACROSS ALL PRIVATE AND PUBLIC SECTORS

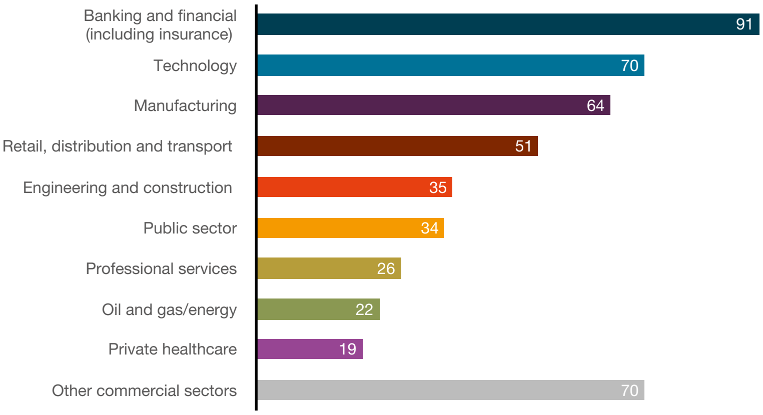
## THE RESEARCH WAS CONDUCTED BY VANSON BOURNE:

Vanson Bourne is an independent specialist in market research for the technology sector. Its reputation for robust and credible research-based analysis is founded upon rigorous research principles and its ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com

Analysis of respondent function (482 respondents)



Which of the following best describes the industry of your organisation?", asked of all respondents (482 respondents)



Control Risks

# CYBER SECURITY LANDSCAPE REPORT 2017

## RESPONDENTS LACK CONFIDENCE IN THEIR BOARD'S ABILITY TO MANAGE CYBER SECURITY THREATS

Analysis showing whether respondents agree or disagree that their organisation's board level executives do not take cyber security as seriously as they should, asked of all respondents

☒ **46%** Disagree

☑ **54%** Agree

**31%**

of organisations are very or extremely concerned that they will suffer a cyber attack in the next year

## COMPANIES ARE STRUGGLING TO ADOPT A RISK-BASED APPROACH TO CYBER SECURITY

**45%**

of respondents cited risk assessment as their primary challenge in monitoring cyber risks

**32%**

of organisations had not conducted a risk assessment at all within the past year

**28%**

of companies that have suffered a cyber attack faced regulatory or law enforcement action and 26% lost customers

## THIRD-PARTY BREACHES ARE A GROWING CONCERN

**35%**

of respondents said a third party cyber breach had affected their organisation

**53%**

of organisations evaluate their third parties' cyber security measures just by inserting a clause into their contracts to oblige them to adhere to security and privacy practices

www.controlrisks.com

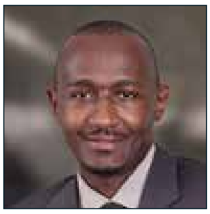
# OUR CYBER EXPERTS

## GLOBAL

**Toby Chinn**
Partner and head of cyber security

**Nicolas Reys**
Associate Director

## AFRICA

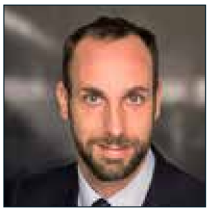


**Patrick Matu**
Associate Director

## AMERICAS

**Kate Yamashita**
Principal

## ASIA PACIFIC

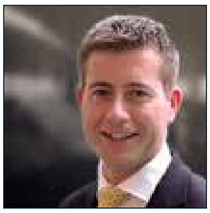


**Ben Wootliff**
Partner

## EUROPE

**Jayan Perera**
Associate Director

## MIDDLE EAST



**William Brown**
Director

To speak to the cyber team please contact

cybersecurity@controlrisks.com

## Control Risks' offices

abudhabi@controlrisks.com
alkhobar@controlrisks.com
amsterdam@controlrisks.com
baghdad@controlrisks.com
basra@controlrisks.com
beijing@controlrisks.com
berlin@controlrisks.com
bogota@controlrisks.com
chicago@controlrisks.com
copenhagen@controlrisks.com
delhi@controlrisks.com
dubai@controlrisks.com
erbil@controlrisks.com
frankfurt@controlrisks.com
hongkong@controlrisks.com
houston@controlrisks.com
jakarta@controlrisks.com
johannesburg@controlrisks.com
lagos@controlrisks.com
london@controlrisks.com
losangeles@controlrisks.com
mexicocity@controlrisks.com
moscow@controlrisks.com
mumbai@controlrisks.com
nairobi@controlrisks.com
newyork@controlrisks.com
panamacity@controlrisks.com
paris@controlrisks.com
portharcourt@controlrisks.com
saopaulo@controlrisks.com
seoul@controlrisks.com
shanghai@controlrisks.com
singapore@controlrisks.com
sydney@controlrisks.com
tokyo@controlrisks.com
washington@controlrisks.com

www.controlrisks.com