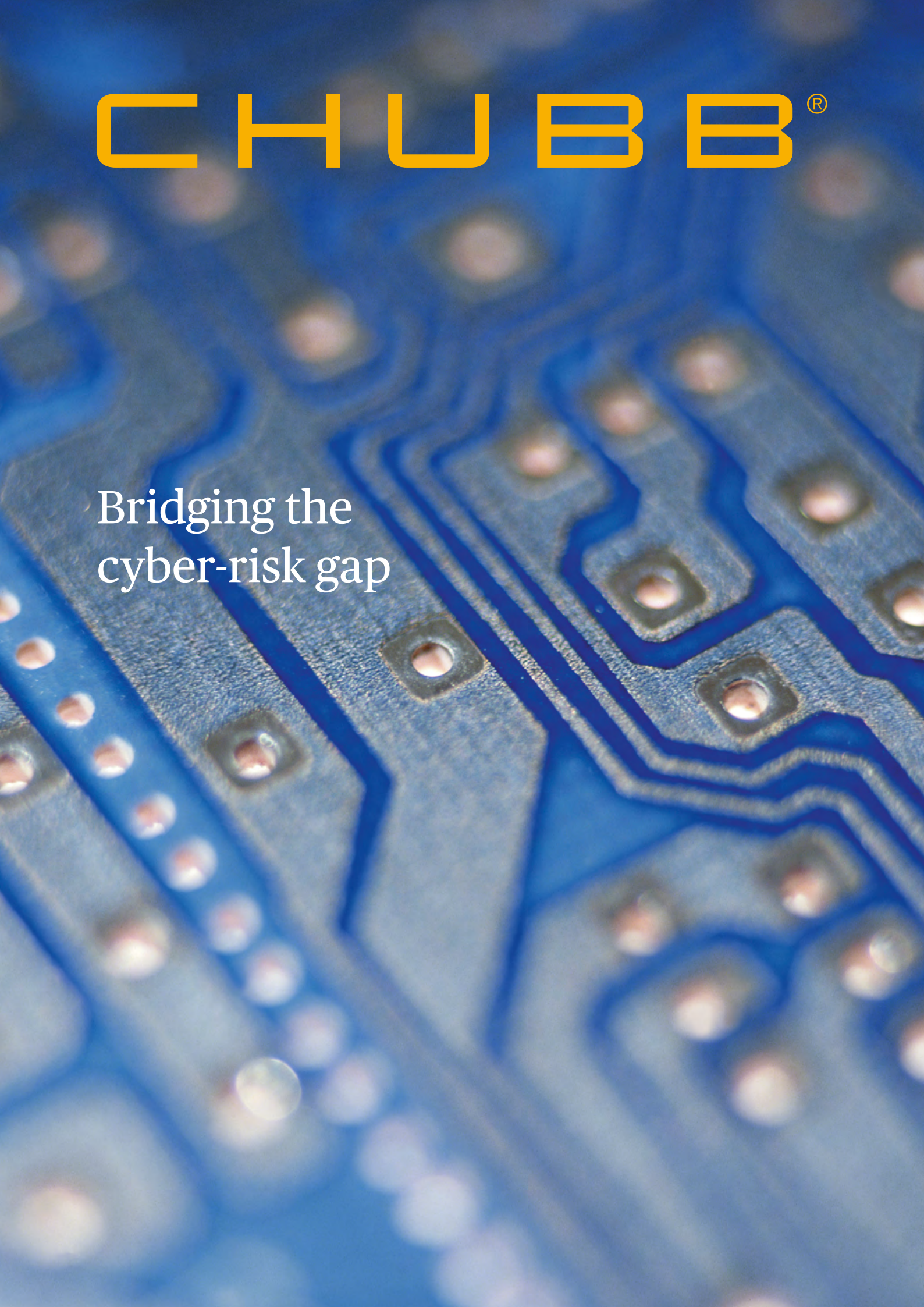
CHUBB®

Bridging the cyber-risk gap



Contents

Introduction

The call for a united front

No organisation can afford to be complacent about cyber risk. The scale of the threat is sobering, and attacks are becoming more common and more sophisticated. The latest cyber-risk research from the European Union Agency for Network and Information Security (ENISA) identifies no fewer than 15 categories of threat [1], and warns that "cyber-threat agents are always a step ahead of the defenders" [2].
Our study is based on a survey of the views of senior managers in both IT and risk from more than 250 businesses across Europe, with annual revenues exceeding $500m. In this report, we identify the fundamental differences of opinion that departments within an organisation can have on cyber risk - and explore ways to resolve them.

A muddled response

Our findings vindicate the ENISA warnings. More than a quarter of our respondents have suffered a notable cyber incident or breach of information systems in the past 12 months alone.

Cyber risk has moved rapidly up the boardroom agenda, but there is little consensus on how to mitigate the threat. For many, the response is led by the IT function. For others, the risk function is expected to play the most prominent role.

Unanswered questions abound. Why? Often, it's because IT professionals and their counterparts in risk have conflicting views about how to proceed. Is it better to assume that a breach is inevitable and to prioritise rapid response, or should the organisation focus on building 'impregnable' defences? Do defences in one area of the business need greater support than elsewhere? And what is the role of third parties such as insurers?

Collaboration is key

Resolving these questions calls for greater collaboration between IT, risk, the rest of the organisation and insurers. Firms that fail to reach consensus will create gaps in key areas of their cyber-risk management - and leave vulnerabilities that can be exploited.

In the battle against cyber criminals, a united front is crucial.

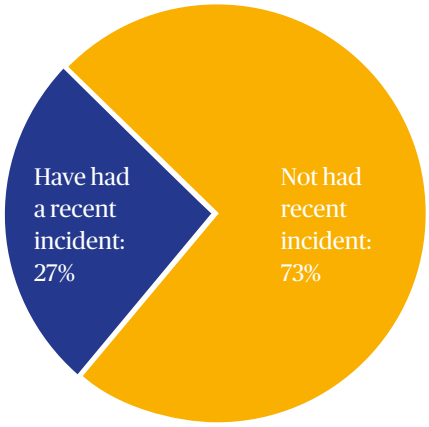
[1] Malware, web-based attacks, web application attacks, denial of service, botnets, phishing, spam, ransomware, insider threats, physical manipulation/damage/theft/loss, exploit kits, data breaches, identity theft, information leakage and cyber espionage.

[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

The nature of the threat

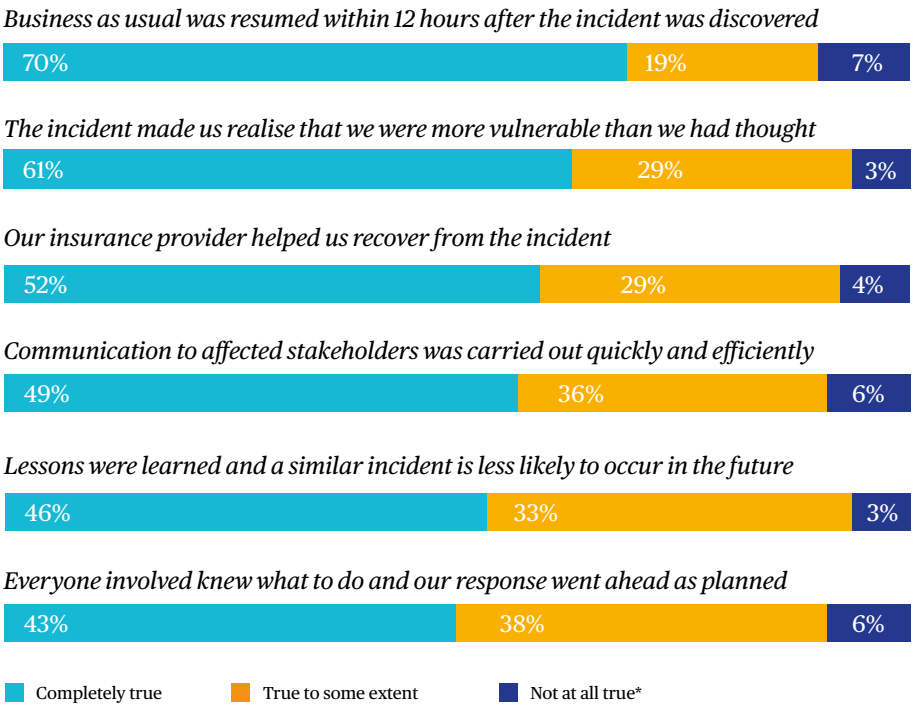
The number of firms that have suffered a notable cyber incident or a breach of information systems in the past year shows that cyber risk is a real and present danger.

Chart 1: Respondents who have been hacked or suffered a notable incident in the past 12 months



Most say they coped well and returned to business as usual within 12 hours - but there are clear fault lines. For many, the incident exposed unforeseen vulnerabilities, and only a minority say that a similar incident is less likely in the future (see Chart 2).

Chart 2: The extent to which respondents agree with these statements about their hack



* Remaining % responses were 'not applicable'

> “IT professionals are more worried about the preparedness of their colleagues”

Organisations are disjointed

Businesses may well have response plans and policies that kick in when an incident occurs but not everyone is fully aware of their responsibilities.

Fewer than half of those who suffered a hack or notable cyber incident completely agree that everyone involved in the response knew what to do and that it went ahead as planned. This is worrying. To contain an incident effectively, it is crucial that everyone involved acts quickly and is part of a strategic response.

“It’s not good enough to assume you can defend against all events,” explains Lauren Webb, Chubb’s London Cyber Underwriting Manager. “A plan has to be in place to deal with the consequences, so that you make the incident as small as possible once it does take place, rather than the problem spreading because no one is dealing with it - and that plan must be shared widely .”

Such concerns are particularly acute in IT, where just 29% of respondents say they are completely confident that everyone who was affected by the breach knew how to respond. This contrasts sharply with respondents in risk, where the figure is 54%, and suggests that IT professionals are more worried about the preparedness of their colleagues.

What can companies do about this? “To create consistency across the organisation, you have to start in the C-suite,” believes Kyle Bryant, Chubb’s Cyber Risk Manager for Europe. “You need a person of influence across the organisation who can break down the silos and ensure that cyber is treated as an enterprise risk.”

Awareness is increasing, differences persist

Cyber risk is moving up the agenda but businesses have more to do to raise its profile at every level of the organisation. Most executives say they have spent more time on the issue over the past two years and more than two-thirds of IT professionals (69%) say that cyber risk is now a board-level issue at their organisation. However, this falls to 57% for risk professionals, and a majority worry that cyber risk is still largely seen as an IT concern (see below).

Respondents who agree with these statements

65%

Our company has spent more time considering and improving cyber risk in the last two years

62%

Cyber risk is a board-level issue in my organisation

60%

Cyber risk is still largely seen as an IT concern in my business

54%

I don't think we are aware of all the cyber threats we are facing

50%

Our employees generally don't recognise how severe the threat of cyber risk is for our business

40%

There isn't a consistent understanding in my organisation of what cyber risk means

There is also disagreement between the IT and risk functions about their organisation's readiness for a hack. Some 75% of IT professionals say their organisation has spent time improving cyber risk, only 58% in the risk function share this view.

Daniel Jacobs, Cyber Insurance Manager for Benelux at Chubb, warns that organisations must resolve disconnects like these if they are to protect themselves coherently and comprehensively. "IT people understand that it is not possible to protect everything but risk managers are not yet so certain about that," he says.

More than two-thirds of IT professionals (69%) say that cyber risk is now a board-level issue at their organisation but this falls to 57% for risk professionals.

Danger from many directions

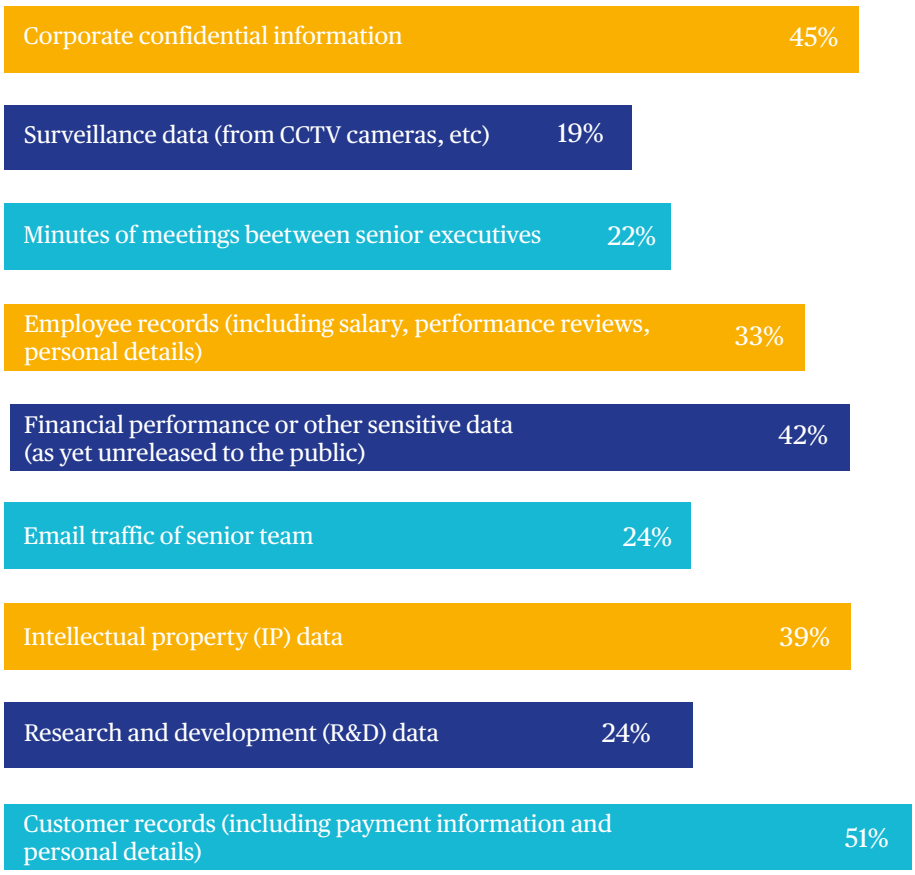
The potency and diversity of the cyber threat makes any vulnerability an urgent priority. Organisations may otherwise struggle to mitigate the risk effectively.

Respondents say the biggest threat to their organisation would be posed by a hacker compromising customer records but data loss, malicious parties disrupting operations, cyber criminals holding data to ransom and business interruption are also seen as serious cyber-risk threats (see Chart 3).

Chart 3: Respondents who believe these factors pose the greatest threat to their business

In many cases, the threat is multi-faceted. Data loss is a good example. More than half of respondents (see Chart 4) say their customer records, out of all the data they hold, pose a significant risk in the event of a data loss. This could be because this data is a particular focus of the EU's General Data Protection Regulation (GDPR), which comes into force in 2018 along with tough new penalties for organisations that fall foul of the rules. But the data threatened by breaches also covers confidential corporate data, intellectual property and R&D data. To mitigate the risk of the cyber threat, organisations will have to protect data on each of these fronts – simultaneously.

Chart 4: Proportion of respondents who say the following types of data represent the greatest threat to their business if breached



> “The reality is that many organisations find it extremely difficult to quantify the potential consequences of a cyber incident or attack”
>
> - Lauren Webb
> London Cyber Underwriter
> at Chubb

Differences of opinion

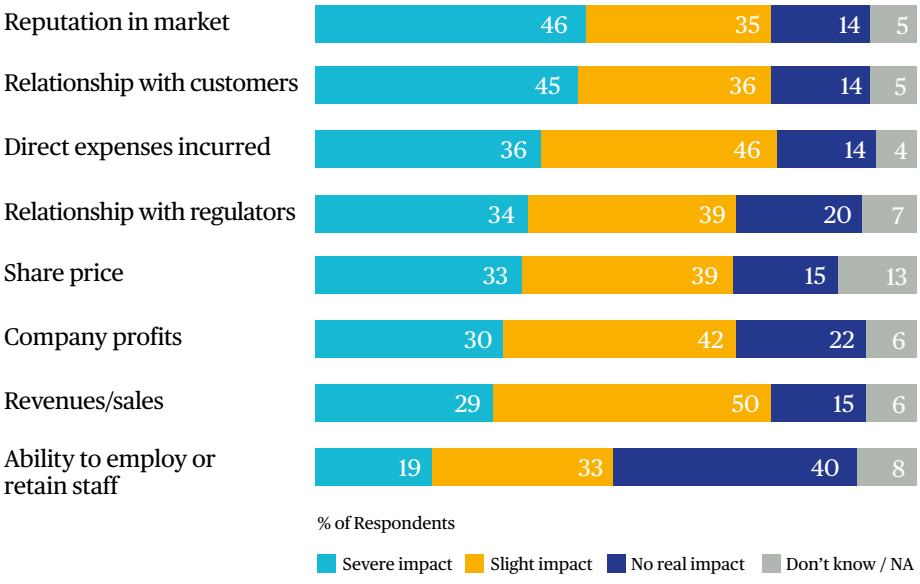
IT professionals are more likely than their counterparts in the risk function to expect the impact of a cyber event to be severe (see Chart 5). This is further evidence that not all organisations have reached a single view of the scope of the threat or how to tackle it, which can leave them vulnerable.

“The reality is that many organisations find it extremely difficult to quantify the potential consequences of a cyber incident or attack,” explains Chubb’s Lauren Webb. “IT and risk are going to have to work together holistically to look at the various threats their organisations face and to assess the financial implications of such exposures.”

Chart 5: The areas where IT and risk teams would expect a cyber event to have a severe impact

	Risk team	IT team
Direct expenses incurred	32%	41%
Share price	27%	41%
Ability to employ or retain staff	17%	22%
Relationship with regulators	35%	33%
Company profits	23%	42%
Revenues/sales	26%	34%
Relationship with customers	42%	50%
Reputation in the market	42%	53%

Chart 6: Respondents’ expectations of the impact of a worst-case-scenario cyber incident



States of readiness

In our view, the most significant factor in a business's ability to limit the damage of a cyber event is its ability to respond quickly. And while our respondents are generally positive about their preparedness to respond, they are conscious of their potential shortcomings – and IT's confidence is not necessarily shared by colleagues in risk.

Respondents say that their overall cyber defence capabilities are in good shape: 72% score themselves at 4 or 5 on a scale of 1 to 5, where 5 is excellent and 1 is poor. They are, however, more confident in some areas than in others. Four-fifths (81%) are confident that their organisations could safeguard their IT networks and systems in the event of a cyber attack, and 74% say the same about their sensitive information. They are also confident about their abilities in data back-up, antivirus and firewall software and incident response plans – at least 68% rate themselves 4 or 5 in each. **They are much less confident about calculating the cost of an incident (58%).**

Response planning

Many respondents are not sure that their incident response plans are up to scratch. Fewer than half of those who say they have never been hacked completely agree that they have a clear plan in place for a cyber incident and that they test and update that plan regularly.

Worryingly, 55% of this group say their organisation assumes – to some extent – that it won't ever suffer a serious cyber incident.

At worst our findings suggest that cyber defence is a fractured picture, exacerbated by disjointed processes.

"It's the detection and response element where there is often a lack of clarity and coordination," says Roger Francis, Senior Strategic Consultant and Cyber Insurance Lead, Mandiant. In order to effectively respond to an incident, it is key that some pre-planning has occurred and that the associated processes and escalation matrices are in place to govern the various response activities. Furthermore, whereas the incident responders are good at piecing together the 'what' and the 'how' of a particular breach, they likely need support from the wider organisation to contain and recover.

Self-assessment

For almost all areas of cyber risk, IT respondents think more highly of their capabilities than their peers in the risk function. Chart 7 shows the differences across several key areas of cyber defence.

Xavier Leproux, Chubb's Underwriter Senior Technical Lines, suggests that IT may need to work harder to explain its cyber-risk mitigation work to the rest of the organisation. "Risk managers know there is a risk but it's hard for them to evaluate it themselves," he says. "But when they talk to IT, they don't necessarily get the simple explanations they need to form a considered judgment."

Chart 7: Where IT and risk executives rate their organisations as excellent or very good

	Risk team	IT team
Establishing and testing an incident response plan	64%	74%
Developing a robust cyber security policy	63%	75%
Putting a number on the total cost of a cyber incident	53%	65%
Training staff on best practice around cyber risk mitigation	58%	76%
Assigning risk profiles to specific data sets and information systems	64%	70%
Implementing antivirus, firewall and patching procedures across the business	68%	82%
Finding and buying the most suitable antivirus, firewall and patching procedures for our business	63%	75%

So the onus is on IT professionals - those at the sharp end of protecting the business against hackers - to build better communication channels with colleagues. Closer collaboration will reduce the understanding gap and create a seamless approach to cyber risk.

Governance and responsibility

Successful cyber-risk mitigation depends not only on technical ability but also on governance and whether functions work together to manage the threat along clear lines of responsibility.

An enterprise risk

"Cyber risk is ultimately an enterprise risk, with the potential to directly impact the business and even the organisation's very existence," asserts Saïd Dami, Chubb's Cyber Risk Engineer for Europe. "It has to be the responsibility of the executive risk management, with a framework that is then implemented throughout the organisation."

For many, there is work to do to achieve such a framework. They have little confidence in their governance structures and the perceptions of their IT and risk professionals diverge significantly.

Who owns the risk?

Only 37% of respondents strongly agree that there is clear ownership of cyber risk in their organisations, and even fewer - just 35% - strongly agree that there is good crossdepartment collaboration.

Across the board, IT professionals are more optimistic about organisational readiness than risk professionals (see Chart 9).

The risk function is likely to take responsibility for driving enterprise-wide collaboration and governance on cyber risk, so its relative pessimism must lead to some tough conversations with its more optimistic colleagues in IT.

37%

Only 37% of respondents strongly agree that there is clear ownership of cyber risk in their organisations

35%

Just 35% - strongly agree that there is good crossdepartment collaboration

Chart 8: The extent to which respondents 'strongly' or 'slightly' agree with these statements about governance

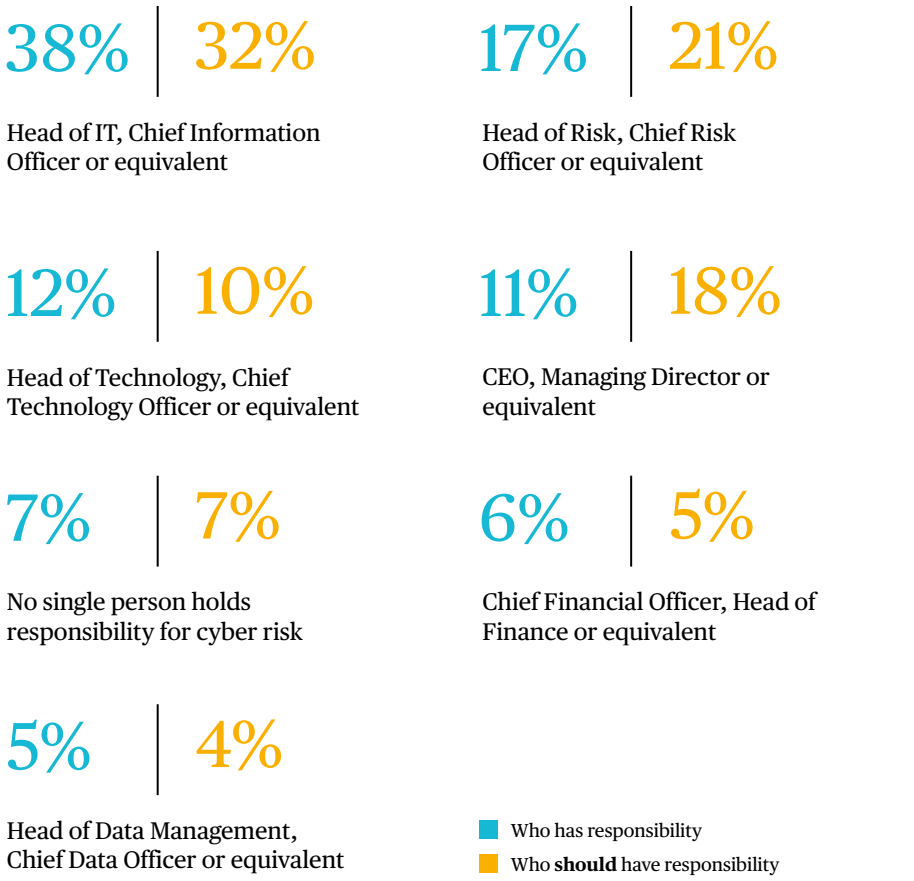
Chart 9: Different views between IT and risk team, showing those who 'strongly' or 'slightly' agree

	Risk team	IT team
There is good cross-department collaboration in my organisation	63%	84%
There is clear ownership of cyber risk in my organisation	64%	80%
When it comes to cyber security, a quick response is better than extensive levels of protection	53%	63%
It is better to build defences around the most critical data rather than trying to protect everything equally	60%	75%

This tension is all the more likely because there is a clear division when it comes to rightful responsibility for cyber risk: 38% of respondents say their head of IT or CIO is responsible; 12% cite their head of technology or CTO; and 17% say the head of risk, or equivalent, is in charge. This is broadly in line with who respondents think should be responsible (see bellow).

Once again, views differ markedly from function to function. Close to half (43%) of IT respondents say cyber risk should be the responsibility of the head of IT but only a quarter (25%) of risk professionals agree. However, IT respondents are also more likely to think the head of risk should take responsibility: 23% of IT executives take this view, compared with 19% of respondents from risk itself.

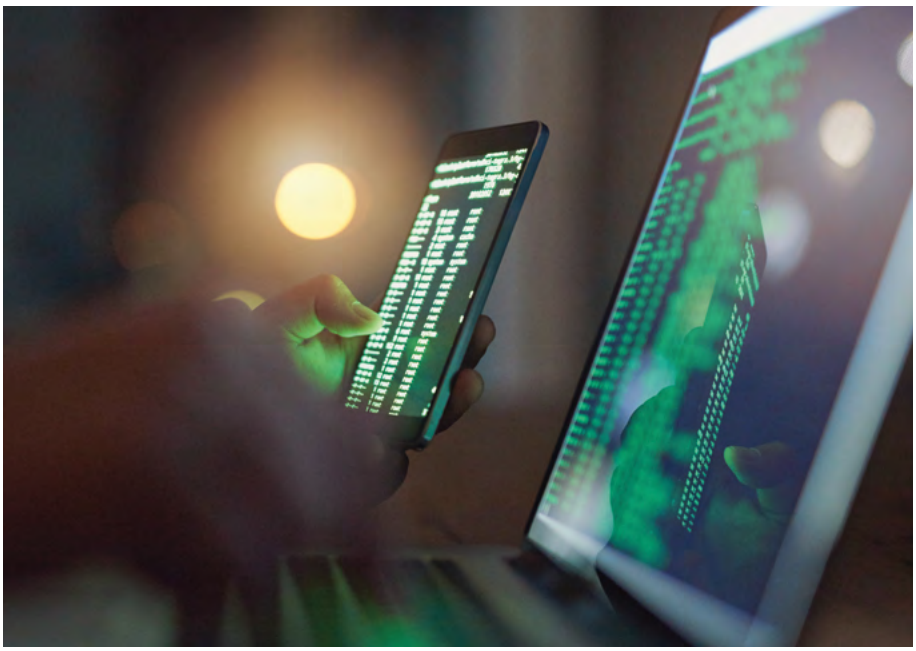
Who has responsibility for cyber - and who should be responsible?



It seems that while some in IT are keen to retain their historic responsibility for cyber security, many professionals in that function now see the issue in broader terms - and so do their colleagues elsewhere.

"There was a time when cyber risk was a question only for IT," says Chubb's Saïd Dami. "But as technology and digital systems have become ever more important to the enterprise as a whole, the recognition that cyber risk is ultimately a business risk has increased."

> “Fundamentally, security should be a separate entity that advises everyone else. If security is run out of IT, it tends to be technology focused. If it’s run out of legal, the focus is on compliance. If risk takes the lead, the risk calculations are to the fore”
>
> - Roger Francis
> Senior Strategic Consultant and
> Cyber Insurance Lead at Mandiant



Approaches differ

Strikingly, risk managers are much more likely than IT teams to think an organisation can go without a single individual who is ultimately responsible for cyber: 11% say no one person should hold responsibility for the risk, compared with just 1% of IT professionals.

This difference of opinion is widened further by the assumptions that each department makes about the other. Two-thirds of IT respondents say that risk managers leave their comfort zones to deal with cyber risk, for example, and 56% of risk respondents think their IT colleagues overlook the ‘human’ side of risk.

Resolving these differences will take time – particularly as these functions also hold conflicting views on what is practical. For example, IT respondents are more likely to complain that management expects invulnerability (66% IT vs 56% risk) and are more likely to think a quick response is better than extensive protection (63% IT vs 53% risk).

The key may come down to **better communication**, says Chubb’s Xavier Leproux. “The rest of the business needs to be able to feel greater confidence in the message coming from IT,” he says. “That will only happen when internal communication is simple and accessible to a wider range of people who are speaking the same language.”

Ultimately, of course, there will be no one-size-fits-all approach but Mandiant’s Roger Francis does urge organisations to think about lifting cyber out of any one function and establishing a collaborative approach.

“Fundamentally, security should be a separate entity that advises everyone else,” he says. “If security is run out of IT, it tends to be technology focused. If it’s run out of legal, the focus is on compliance. If risk takes the lead, the risk calculations are to the fore.”

Obstacles and shortcomings

Whether they are from IT or risk, those who manage cyber know that success means confronting several challenges.

Respondents to the survey point to a number of hurdles. They cite employees neglecting their data protection responsibilities. They worry about the constantly changing nature of the threat. And they warn of the growing sophistication of attackers.

"Nothing is fool proof," cautions Chubb's Kyle Bryant. "There is no silver bullet because the human element is always there behind the computer."

Threats from inside the organisation, and threats from outside

Compared with their colleagues in risk, IT professionals tend to be more worried about 'the bad guys': **42% cite the sophistication of bad actors**, compared with only 27% of their counterparts in the risk function. This is unsurprising: IT professionals are likely to be most aware of the evolving sophistication of hackers and the technologies they use to breach security. This knowledge appears to be increasing their wariness.

The picture is reversed when it comes to concerns about fellow employees: only 30% of IT respondents cite fears of employees neglecting their data protection responsibilities, compared with **45%** of risk respondents. As IT professionals are more immersed in technology, these respondents are perhaps less likely than those in risk to identify this as a cause for concern.

Yet the workforce must be a clear priority for many organisations. Just over a third **(34%)** of all respondents cite employee behaviour overall as the weakest link in their cyber defences (see Chart 10), a view that is largely consistent between IT and risk.

Chart 10: What is the weakest link in your cyber defences?

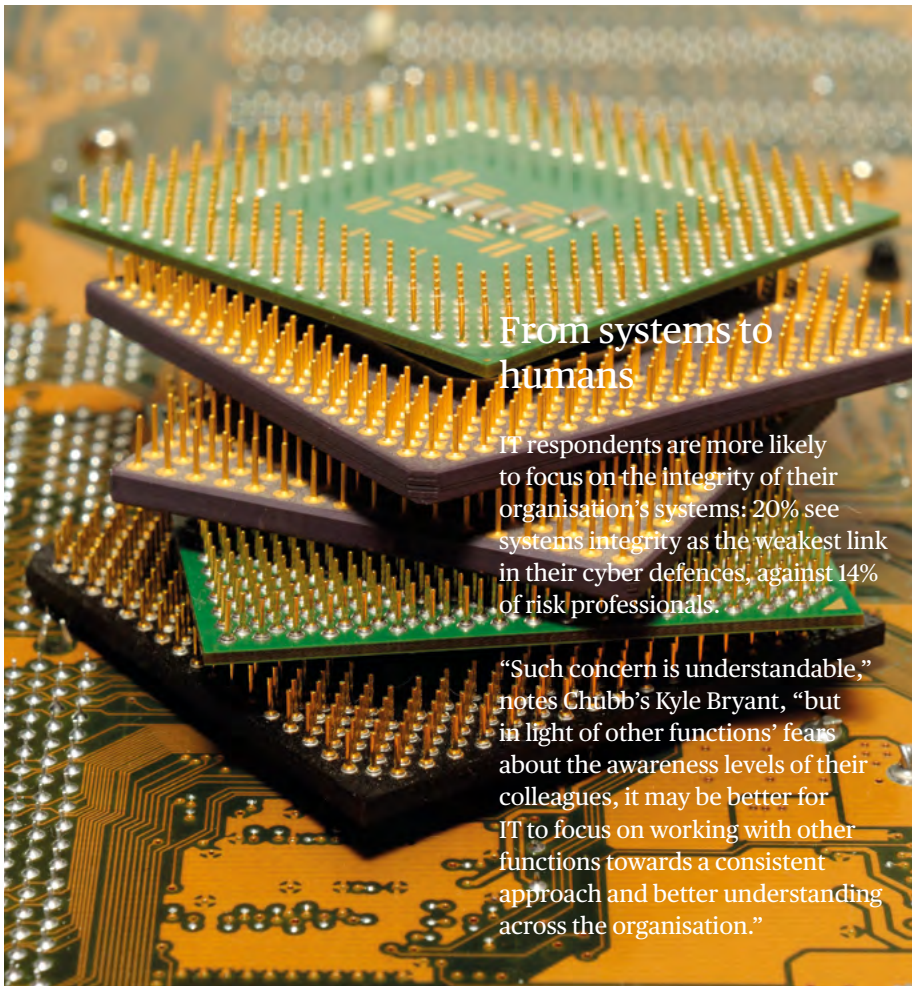
	Risk team	IT team
Our employees	34%	35%
The defences of our suppliers and partners	11%	12%
The integrity of our systems	14%	20%
Our security software	16%	7%
Our monitoring of our security software	10%	4%
Our insurance solution	3%	3%
Our senior leadership	3%	0%
Our IT function	3%	7%
Our risk function	1%	2%

The understanding gap

The view of the workforce as a potential weak link reflects concern about employees' lack of knowledge and understanding of cyber-risk issues. It is surprising that only 41% of respondents describe IT employees' cyber-risk understanding as excellent; and only 32% say the same for risk management. Even more concerning perhaps, are the limitations of those who should be most knowledgeable - the executive team: only 31% of respondents describe the senior leadership's cyber-risk understanding as excellent.

Reflecting the focus on – and fears about – employees, more than a third of respondents say that better training for all employees is a key priority in the move to improve cyber-risk management across the organisation, along with regular monitoring of staff behaviour and clearer communication with employees.

Once again, better links between IT and the rest of the organisation will be a huge step forward. "The minimum we need from organisations is better awareness – just having a widespread awareness that your firm holds private data, say, or that it could be attacked," says Chubb's Daniel Jacobs. "If there's no awareness, any sophisticated defence you install or process you put in place will not protect you."



From systems to humans

IT respondents are more likely to focus on the integrity of their organisation's systems: 20% see systems integrity as the weakest link in their cyber defences, against 14% of risk professionals.

"Such concern is understandable," notes Chubb's Kyle Bryant, "but in light of other functions' fears about the awareness levels of their colleagues, it may be better for IT to focus on working with other functions towards a consistent approach and better understanding across the organisation."

Collaboration between IT and risk

Our research points to a gulf between IT and risk when it comes to mitigating cyber risk. This must be bridged: a collaborative approach to cyber offers organisations the best possible chance to increase their cyber resilience and manage the threat effectively.

"The collaborative approach demands a concerted and enduring effort but the functions are starting from a poor position," warns Xavier Leproux.

Indeed, fewer than half of our respondents say that IT and risk work together as part of a formal structured programme to address cyber risk, 27% describe their collaboration as regular but more ad hoc, and a disconcerting 18% concede that collaboration only happens in response to an imminent threat or following an attack.

43%

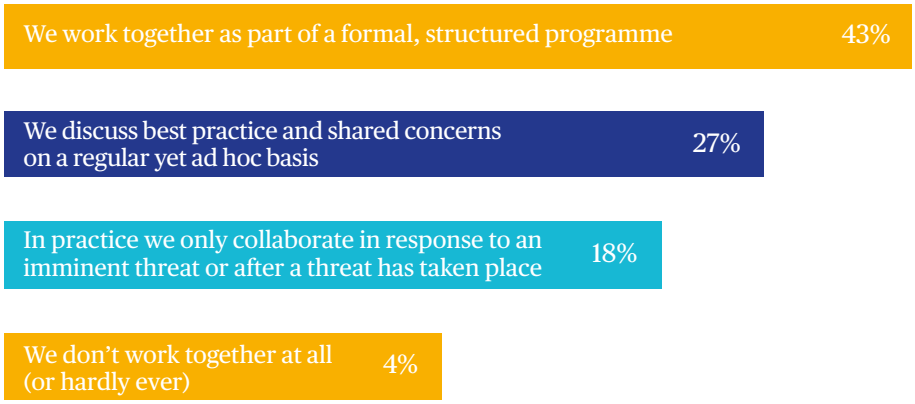
Fewer than half of our respondents say that IT and risk work together as part of a formal structured programme to address cyber risk

18%

Concede that collaboration only happens in response to an imminent threat or following an attack

> “Starting with a more joined-up approach to risk management represents an organisation’s best chance to mitigate the danger effectively”
>
> - Lauren Webb
> London Cyber Underwriter
> at Chubb

Chart 11: How risk and IT teams work together in practice



As in their responses in other parts of this research, IT professionals are more positive than their colleagues in risk: they consistently report better levels of collaboration, and are more likely to say that progress is being made towards improved cooperation.

Perhaps IT professionals need to consider whether there is scope for them to work more closely with the rest of the organisation – and with the risk function in particular.

The prize on offer for those organisations that can bring their functions together is a valuable one, according to Chubb’s Lauren Webb. “The implications of a cyber incident are wide-ranging and dealing with them will not be the responsibility of IT alone,” she says. Starting with a more joined-up approach to risk management represents an organisation’s best chance to mitigate the danger effectively.

The role of insurance

Overall, almost two-thirds of respondents see a role for insurers in helping organisations to protect themselves from cyber risk, and among the organisations in this research that say they suffered a cyber incident over the past 12 months, more than half (52%) sought help from their insurer.

IT recognises the insurance need

IT professionals are pushing the case for such cover particularly hard: 67% advocate insurance as valuable protection, against 60% of risk professionals.

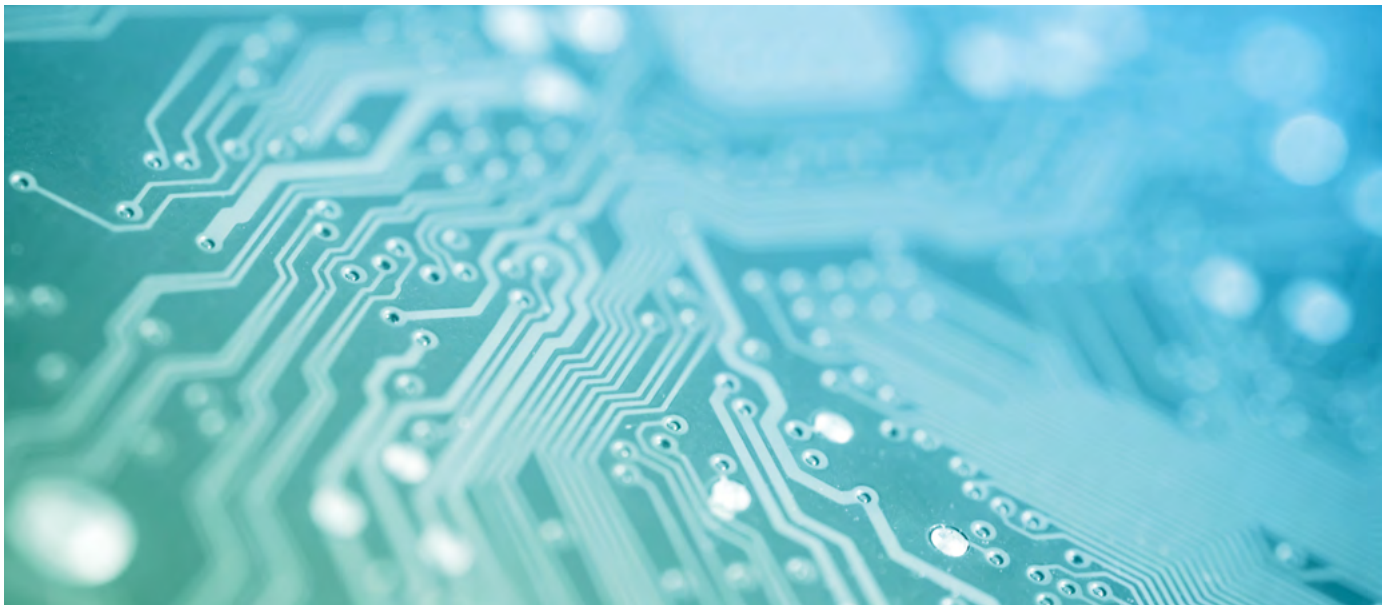
This could reflect a tacit acceptance in the IT function that protecting the organisation in all circumstances is almost impossible. Breaches will occur, and this is where insurance comes in.

But fewer than half of our respondents say their organisations have taken out insurance cover for cyber risk, and there is frustration about what is available.

Chart 12: The extent to which respondents agree with these statements

Two-thirds (66%) agree that insurers need to do more to meet their needs, and 61% say insurers are not moving quickly enough to keep up with the evolving nature of cyber risk. These figures are lower for risk than for IT professionals, which likely reflects the risk function's closer engagement with insurers and its knowledge of industry innovation and advances in this area.

The insurance market is evolving quickly, according to Chubb's Kyle Bryant. "This is a relatively young market, but in the past 10 years we've seen simple data breach policies expand into cover for business interruption, data asset loss and data reconstruction, and to responding to ransomware events," he says. "It's been very agile."



> “As an insurer, we try to help you understand and evaluate risk and improve security – as well as responding as effectively as possible when an incident happens”
>
> - Saïd Dami
> Technical Lines Risk Engineer
> for Continental Europe at Chubb

A range of support

In practice, support from insurers comes in different guises. Six in ten respondents praise the way insurers provide advice and expertise in the aftermath of an incident and advise on best practice to prevent incidents from happening.

Insurers are also doing a good job of putting a price on cyber events – a notoriously thorny subject for all industries: 56% say insurers are good at helping them to price the impact of a breach. Meanwhile, the same proportion say that claims are handled fairly.

Respondents are looking for insurers to provide good service in a number of areas. Speed, easily accessible incident response services, regulatory advice, impact minimisation and legal advice are all considered to be important by clear majorities of respondents.

“As an insurer, we try not only to provide a policy that protects you from cyber risk,” says Chubb’s Saïd Dami, “but also to help you understand and evaluate risk and improve security – as well as responding as effectively as possible when an incident happens.”

In conclusion

There is widespread concern among risk and IT professionals about the scale and diversity of cyber risk but there is little agreement about how organisations should assess, manage and mitigate the threat.

What was once an issue managed by organisations' IT functions is increasingly viewed as a crucial C-suite priority, and functions as diverse as risk, legal and HR are all expected to play a part in responding. Despite this broad response, many organisations are struggling to build governance models that allow for a consistent approach.

Resist pressure from above

Six in ten respondents say that their senior leaders expect the business to be invulnerable to cyber attack. This is worrying in an era of constant, evolving threats, and places intense pressure on their risk and IT teams to mitigate these threats with a 100% success rate. Yet respondents concede that they are unable to deliver on this expectation: 66% admit that it makes sense to build defences around the organisation's most critical data rather than trying to protect everything equally.

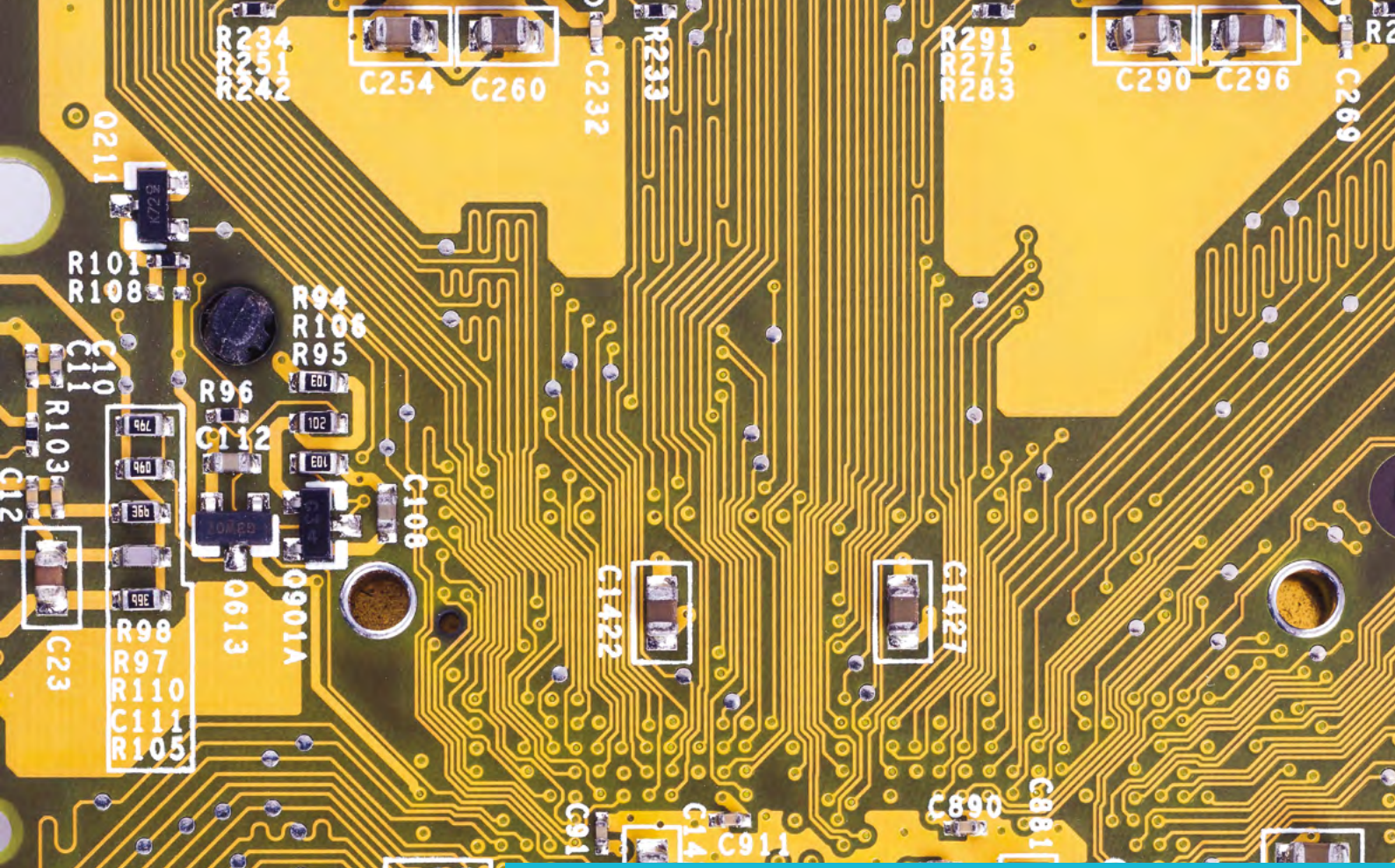
This is a realistic approach but cyber professionals must do a better job of informing their colleagues – and their leaders – about the rapidly evolving nature of the threat. Otherwise, they will be blamed for breaches when they occur. This education demands far greater cooperation between IT, risk and the rest of the organisation.

More than four in ten respondents believe that ultimate responsibility for cyber risk should lie with the technology function. But, again, collaboration remains essential: even if IT takes ownership of developing and maintaining a framework for cyber risk management across the enterprise, it will have to work much more closely with every function of the organisation to implement such policies.

Get third parties involved

The insurance industry has recognised that it needs to offer much greater support to organisations grappling with cyber risk – support that includes cover on which organisations can rely in the event of an incident but which also comprises a much wider range of services. Ultimately, insurers may hold the key to bringing functions together to assess, quantify and prioritise different cyber risks, and build stronger defences and protections.

"Nothing will provide you with total assurance that an incident won't happen," concludes Kyle Bryant. "But insurance now provides a practical solution to help you identify, mitigate and protect your organisation's vulnerabilities."



About this research

This report has been produced by Chubb in collaboration with Longitude Research. It is based on a survey of 257 respondents, comprising 103 from IT roles and 154 from risk and insurance positions.

Respondents were based in Belgium, Denmark, France, Germany, Italy, the Netherlands, Norway, Spain, Sweden and the UK. The research was carried out online and respondents were not compensated for their participation. All respondents were from businesses exceeding $500m in annual revenues; 24% were from businesses with revenues exceeding $5bn.

We also carried out qualitative interviews with a range of senior Chubb experts on cyber. As well as these individuals, we would like to thank Roger Francis, Senior Strategic Consultant and Cyber Insurance Lead, Mandiant, for providing his time and insight.

Chubb

The Chubb Building
100 Leadenhall Street
London EC3A 3BP
United Kingdom

T +44 (0)20 7173 7000
chubb.com

Chubb. Insured.℠

UK7279-JD 01/19