

DIGITAL TRANSFORMATION

Keeping pace with the ever-evolving threats
of technological progress in business

DIGITAL



CHUBB®

airmic

Foreword by Airmic

As we all know, the world is set to change at an exponential speed and the risk and insurance profession is part of that change. At Airmic, we want to understand the nature of this transformation, so we can help to shape the future of the risk management profession for the benefit of our members and to inform our future research and knowledge and skills programmes.

We launched our largest ever survey in partnership with Longitude, provider of world-class expertise in thought leadership and research, to understand the nature of this transformation and its impact on businesses, the risk landscape and the roles and responsibilities of those in the risk management profession. The result is a differentiated and valuable insight that will make unique contributions to the 'profession debate'.

The results show risk and insurance managers are embracing change in a transformative business landscape – and that there are opportunities for all. We review a number of these opportunities in detail in three deep-dive mini reports:

- *The value of risk and insurance management* – how to demonstrate the value of insurance management and the strategic contribution members can make in a fast-changing business landscape, supported by JLT
- *Digital transformation* – how digitalisation is

transforming business models while creating strategic opportunities for members, supported by Chubb

- *Is the insurance market fit for the future?* – an exploration of the changing risk and business landscape and the insurer's role in tomorrow's world, supported by Axa Corporate Solutions.

These mini reports are part of the larger survey report, *A profession in transformation*, which provides the bigger picture and further horizon-scanning analysis to inform today's risk and insurance managers as tomorrow's risk professionals.

It is clear from our research that risk and insurance managers are key contributors to the future success of business. Increasingly they should operate at a strategic level to provide perspective and understanding, to help organisations build resilience with sustainability and release opportunities and potential. Based on a foundation of specialised knowledge, skills and experience, the risk management role is about supporting decision-making and creating value.

**Julia Graham, Deputy Chief
Executive and Technical
Director, Airmic**





**Emerging
technologies set to
transform business
are increasingly on
the risk radar of
corporates**

Foreword by Chubb

As an organisation constantly evolving our own understanding of cyber risk, the AIRMIC survey on digital transformation is valuable for us to consider how organisations and those charged with risk management view the risks their organisations face.

The results of the survey reiterate our own views and highlight just how far risk has moved from traditional tangible risk to intangible threats.

The speed of digital advancement, the increasing reliance on emerging technologies and the rapidly changing cyber risk landscape are pivotal areas where insurance and risk management can work together to create real value from protecting a business.

The key to truly managing the risk is to accurately assess it, to engage with the information security and technology experts and other stakeholders in each business, and to understand just where the most relevant stress points are in each organisation.

Without understanding the risk it cannot be managed – threats cannot be mitigated and opportunities cannot be realised.

For us the final stage in the process is being ready and prepared if an incident occurs. The sooner experts are on hand to manage the problem the less damage is done to the business.

Kyle Bryant, regional manager, cyber risks, Europe at Chubb



Inside...



8 EXECUTIVE SUMMARY

Key findings from the Airmic survey

12 HYPERCONNECTED RISKS

The risks associated with a technologically enhanced business world mean insurers must change – and fast

18 KEEPING UP

With cyber crime evolving fast, insurers are under pressure to collaborate more effectively and comply with new regulations

28 CYBER INSURANCE

How are insurance products likely to evolve?





About this research:

This study is part of a wider survey project into the future of the risk management profession, entitled *A profession in transformation*.

While the main report summarises the full findings of the research project, this document is part of a three-part series that delves deeper into the three core themes within *A profession in transformation*.

The three mini-reports include:

The value of risk and insurance management Articulating the value of insurance in the face of an evolving risk landscape

Digital transformation and the risk landscape The risks and opportunities for risk and insurance managers

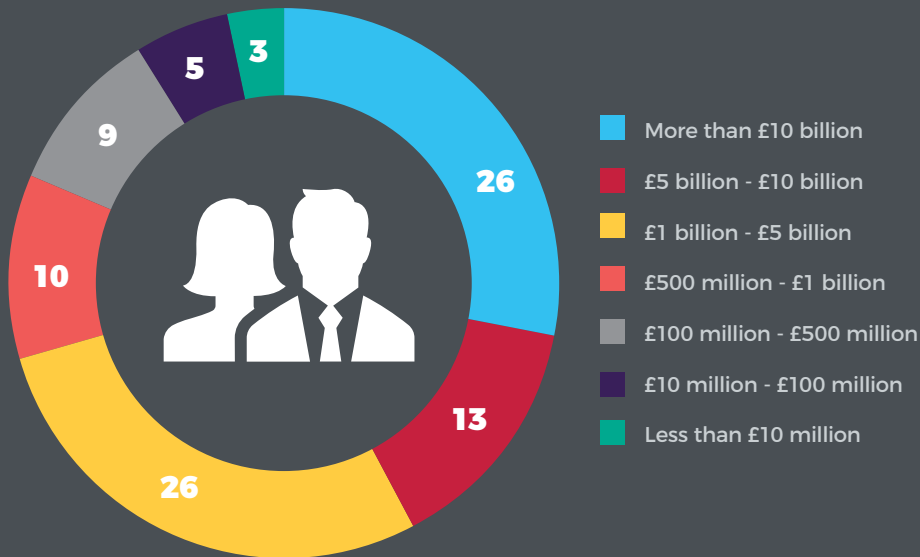
Is the insurance market fit for the future? How this risk landscape is transforming the role of risk managers and the wider insurance market

The survey is based on the responses of 152 risk managers at companies of varying sizes and across a range of business sectors, as well as on a series of qualitative interviews.

Due to rounding, and the use of multiple-choice questions, some figures and charts in this report may not add up to 100%.



Respondents' business size (%)



Split of respondents by company size

About the respondents



Split of respondents by job title

Executive summary





17% of respondents are concerned about the risks of digital transformation - today



22% of respondents see emerging technology as a top three risk - in 3 years' time



Cyber risk is seen as a top five threat but also a key learning area

Risks of a new digital era

Digital advancement is enabling business efficiency like never before, but at the same time it is driving fundamental innovation and disruption and transforming business models along the way. The risks linked to digital transformation are a growing concern for risk and insurance managers. Some 17% of respondents are worried about this, with 23% projecting that the risks will increase in the next three years. Risk and insurance managers also highlight critical learning curves in the risk management of the threats.

Corporate disruption

Emerging technologies that are set to transform business operations – the internet of things and artificial intelligence – are increasingly on the risk radar of corporates. While 13% of risk and insurance managers cite risks related to these technologies as their biggest priority now, 22% project that these will be a top priority in three years' time.

Dangers and opportunities

Cyber-related risks are in the top five threats for risk and insurance managers as businesses become more and more digitally connected. Cyber risk causing business interruption (BI) and data loss and theft are ranked second and fourth, respectively, behind loss of reputation and market developments – and are likely to remain a top risk in the future as digital advancements hasten. However, respondents say that managing BI-related cyber threats and data loss and theft are key learning and development areas for them.

Need for engagement with IT

Cyber risk is still being managed as a technology risk – only 34% of respondents agree strongly that within their organisations cyber is an enterprise risk. This may be down to a disconnect between the risk management department and the technology department. Less than half of respondents (45%) have regular and close collaboration, based on a clear mandate, with their information security functions. This figure falls to only 32% when it comes to collaboration with their technology functions – however respondents say they plan to improve these partnerships in the next three years.

Governance framework gaps

There are gaps to close in cyber governance. Only 31% of respondents strongly agreed there is a clear cyber governance framework that applies across all business units.

Opportunities for innovation

Insurance is recognised as an important tool for the management of cyber risks. Just under half (48%) of risk and insurance managers plan to transfer cyber risks resulting in loss or theft of data, while 52% say the same for cyber-related business interruption. However, respondents also see areas for greater innovation, particularly in data breach recovery services and legal support in an event of data breach or theft of intellectual property.




only 34% of respondents see cyber as an enterprise risk



just 32% of managers have close links with technology departments



52% of managers plan to transfer cyber-related business interruption



**Only 31% of
respondents
strongly agreed
there was a clear
cyber governance
framework across
all business units**

Hyperconnected risk



Digitalisation is leading to unprecedented transformation across multiple lines of business and sectors. Advanced digital technologies, particularly in mobile, social and automation, are converging to create a hyperconnected business world.

While opportunities for growth are plentiful, digital transformation is a major source of risk, disrupting traditional business models, changing consumer demand and competition and challenging the ways in which companies develop and execute strategy – at an accelerated rate.

As business leaders and executive management grapple with the strategic, financial and operational implications of digital transformation, the risks linked to changing business models are a growing concern for

risk and insurance managers across the UK. Some 17% of respondents are worried about this, with 23% projecting that the risks will increase in the next three years.

TECHNOLOGY WARNING

Correspondingly, emerging technologies that claim to revolutionise business operations, such as the internet of things (IoT) and artificial intelligence (AI), are increasingly on the risk radar for corporates. While 13% of risk and insurance managers cite risks related to these technologies as their biggest priority now, 22% project that these will be one of their top risks in three years' time.

The percentages are likely to rise even further in the next decade, as

these technologies advance, says Kyle Bryant, regional manager, cyber risks, Europe at Chubb. "Digital transformation is, and will continue to exacerbate, the interconnected nature of the risk landscape.

"The risks linked to this transformation transcend better known risks such as physical damage, business interruption, loss and theft of intellectual property. This is spreading and driving vendor and third-party exposures, as well as creating strategic challenges for businesses. The risks will be amplified by technologies such as IoT and AI, particularly as providers develop and refine these offerings."

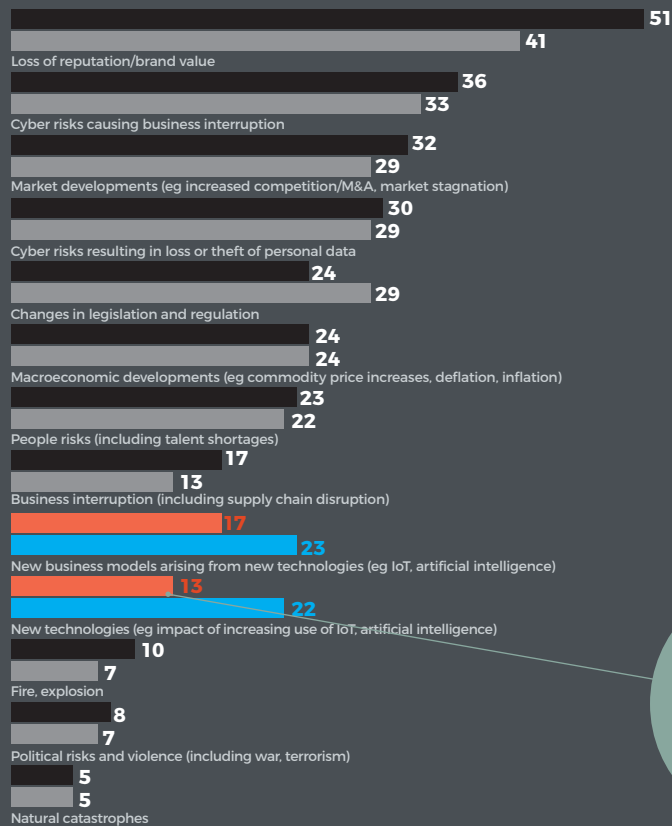
He adds: "Risks triggered by digital transformation are here to stay and will continue to expand."

This creates fresh opportunities

>

Chart 1: New business models arising from emerging technologies are a growing cause for concern

Q Of the following, please pick the top three business risks for your company today, and the top three risks in three years' time



Now (%)
Three years' time (%)



13% of respondents identify increasing use of new technology as a top three risk

for risk and insurance managers to get involved at a strategic level and demonstrate the added value of their role.

There are barriers to overcome, however, with few risk and insurance managers involved in strategic conversations about digital transformation. So says the head of

risk and compliance at a global retail company that has transformed its business model, integrating digital technologies with its core operations to better compete with 'on-demand' mobile and online fashion retailers.

He says: "I ensure that I am involved in these strategic discussions, but it takes a lot of hard work. Executive

managers do not always come to me; I have to go to them.

"The barrier may be a consequence of where risk and insurance managers are generally positioned within the governance structure of an organisation.

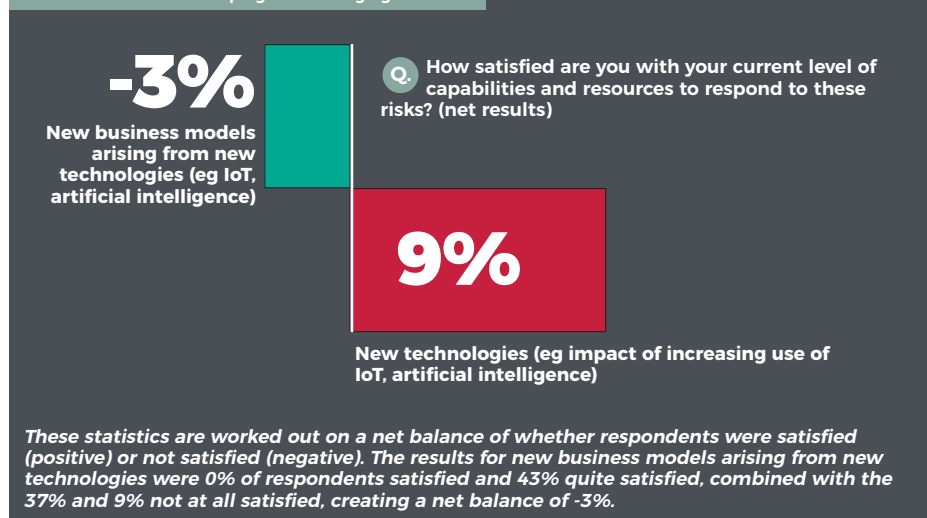
"But we most certainly have a part to play when it comes to digital transformation and should be advising and influencing strategic decisions to help avert any potential risk that may get in the way of these opportunities.

"To do this effectively, we must as a profession be fleet of foot, nimble and quick to change direction, because new risks, trends and capabilities – particularly relating to digital transformation – are introduced very quickly."

NEED FOR CHANGE

This sentiment is echoed by the majority of survey respondents (74%), who recognise that to be at the forefront of the evolving risk landscape the profession must undergo significant change.

Chart 2: Confidence in coping with emerging risks





**We must as a
profession be
fleet of foot,
nimble and
quick to change
direction**

A BUSINESS IN TRANSFORMATION: A RISK MANAGER'S VIEW

Emerging technologies such as the internet of things (IoT) and artificial intelligence (AI) are affecting my business. I am a risk manager for a multinational retail company and the supply chain is a core area of our operations that is, and will continue to be, digitally transformed. We are beginning to digitalise and automate our supply chains and this will only advance in the future.

Our products are designed and sourced by international suppliers. We then need to transport the products from A to B and then from B to C. Frankly, 95% of that is done through the technologies we currently use – and with little human intervention.

We have systems that are looking at the most efficient routes to market, making recommendations about where, along the supply chain, items should be placed – as opposed to a human being manually inputting this information.

In addition, our systems are all interconnected. Orders are placed over the internet, then terms and conditions are communicated through the web; invoicing is done and completed through internet routes and we pay via BACS.

Will AI and IoT be involved in the efficiency of our supply chains? I would say it already is.

This may particularly relate to developing knowledge about the risks linked to new business models, as well as threats associated with IoT and AI.

Compared with traditional physical risks such as fire and explosion – which 100% of risk and insurance managers, unsurprisingly, say they are confident about managing – the risks linked to the brave new world of digital transformation have been identified as core learning curves for the profession.

New business models arising from emerging technologies, for example, prompt a negative response (-3%) in terms of how risk and insurance managers perceive their capabilities in responding to the risks. And only 9% say the same for IoT and AI.

MOVE QUICKLY

Risk and insurance managers must get to grips with these risks, says Wouter Wissink, information and communication technology specialist, risk engineering services, at Chubb.

“The risk landscape is like Moore’s Law, where the number of transistors per square inch on integrated circuits has doubled every year since their invention. Similarly, digital threats are growing and evolving very quickly, introducing new and complex risks.

“This is an opportunity for risk and insurance managers to be at the forefront, but the profession must move quickly. The future belongs to the fast.”



KEY TAKEAWAYS

- While there are learning curves in understanding and managing the risks linked to digital transformation, digitalisation also creates fresh opportunities for risk and insurance managers to get involved at a strategic level and demonstrate the added value of their role
- Risk and insurance managers may not be heavily involved in strategic conversations about digital transformation today, but they have an important part to play in advising and influencing decisions to “help avert any potential risks that may get in the way of the opportunities”
- Risks linked to emerging technologies, while recognised by a small proportion of risk and insurance managers (22%), will increase in the near future as these technologies advance and gather pace in the business world

Keeping up

Cyber crime, in its many guises, shows no sign of slowing down

In today's hyperconnected world, cyber crime is a real and present danger that proliferates between economies and industries. Digitalisation is driving greater frequency and severity in cyber crime, creating new paths for malicious attacks, IP loss and theft, business interruption, and first- and third-party exposures, to name but a few. And these risks show no sign of slowing.

Roger Francis, senior strategic consultant at Mandiant, a cybersecurity firm that helps businesses respond to and protect against advanced cyber threats, says: "I don't see a world where cyber

risk will lessen. It will only expand exponentially because the reward gained from committing a malicious attack considerably outweighs the risk of being prosecuted for the crime. The tactics used by criminals are constantly evolving, but the techniques for catching them are ineffective."

It is no surprise then, that cyber-related risks feature among the top five risk priorities for risk and insurance managers today and in the future. Some 36% of respondents singled out a cyber incident causing business interruption (BI) or leading to data loss and theft (30%) as the

biggest threat to their business – second and fourth, respectively, behind loss of reputation and market developments.

BUSINESS INTERRUPTION

As reliance on technology increases, BI will remain a focal point for risk and insurance managers, as will data loss and privacy. The EU's impending General Data Protection Regulation (GDPR) will place regulatory pressure on corporates to safeguard data.

Both BI and data theft and loss remain within the top five risks for risk and insurance managers in the next three years.

>

Chart 3: Cyber-related risks feature among the top five risks today and in the future

Q Of the following, please pick the top three business risks for your company today, and the top three risks in three years' time



30% of managers see cyber risks that result in loss or theft of data as a top three risk

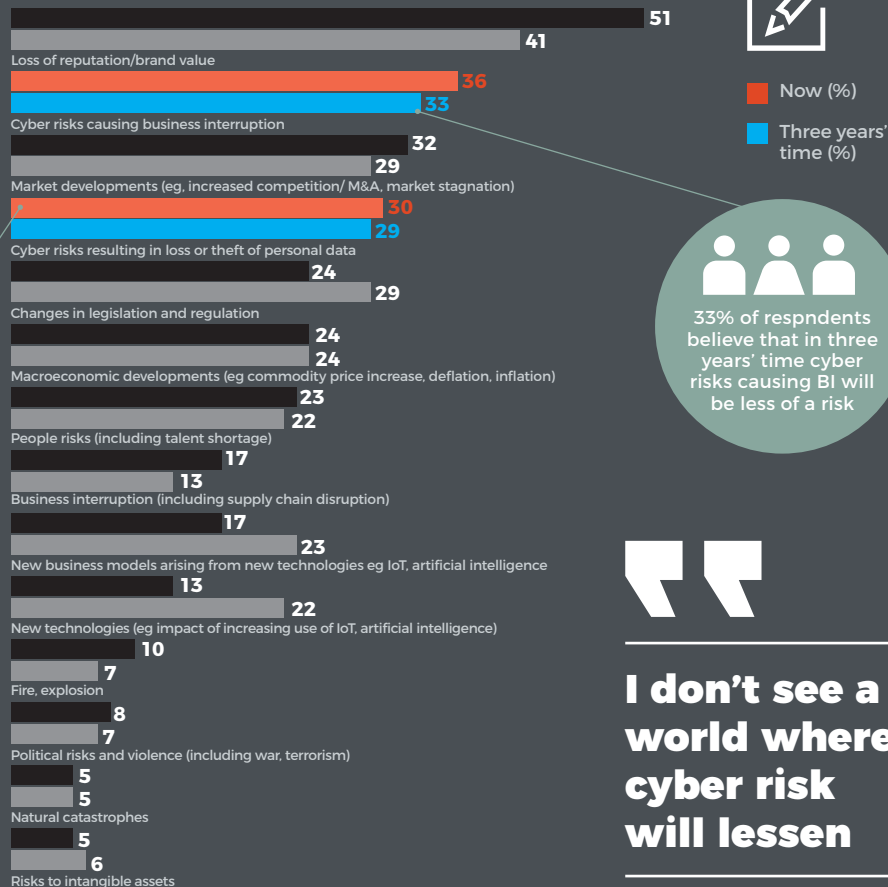
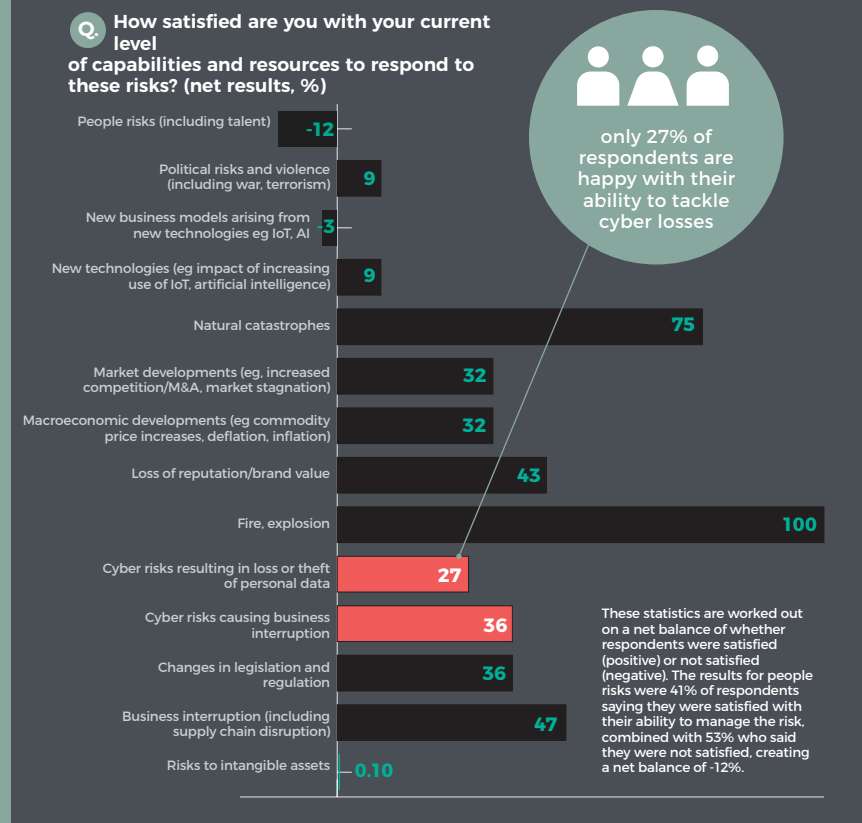


Chart 4: The mixed picture of risk-handling capabilities



- > Yet the prevention of and response to these risks have been identified by risk and insurance managers as areas for further learning and development. Less than half of respondents (36%) are satisfied with their ability to manage cyber-related BI (compared with 47% who are happy with their ability to manage BI resulting from supply chain interruption). Even fewer (27%) said the same for data loss and theft.

GDPR COMPLIANCE

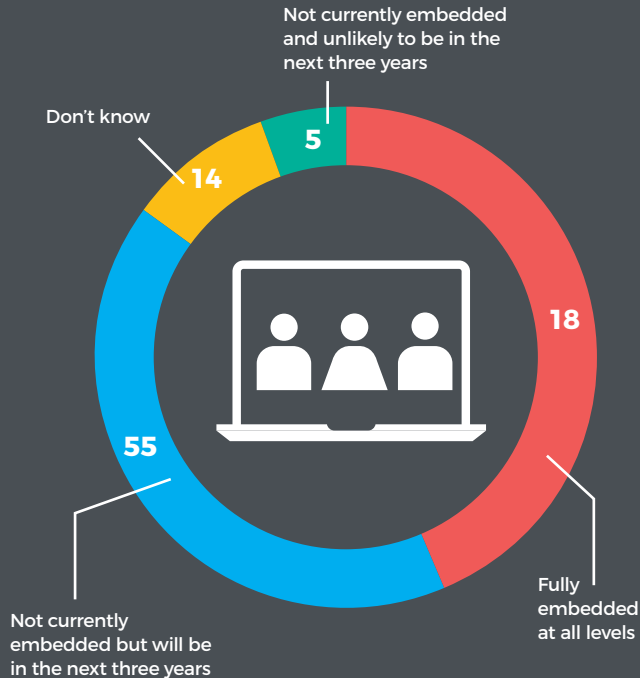
Correspondingly, the minority of respondents (18%) say that GDPR measures are fully embedded across their organisation, although many more (55%) plan to be fully compliant with GDPR in the next three years.

The risk is that many will not meet the May 2018 implementation deadline – an area in which regulators have the power to fine businesses up to 5% of their global annual turnover for serious failures.

There are also development areas in preparing an incident response

Chart 5: A minority of organisations have GDPR procedures fully emdedded

Q. To what extent is advice on issues relating to GDPR embedded at all levels in the organisation?



plan to a general cyber attack and in conducting independent tests of these plans against a recognised framework. Only 39% and 32% of respondents, respectively, agree – strongly – that these protocols are embedded within their organisations.

IMPROVING DEFENCES

Plans to improve defences against a cyber attack perform better, with just under half of respondents (45%) who say they strongly agree with this statement. Corporates tend to rely on prevention rather than planning for a breach, says Mandiant's Francis.

>

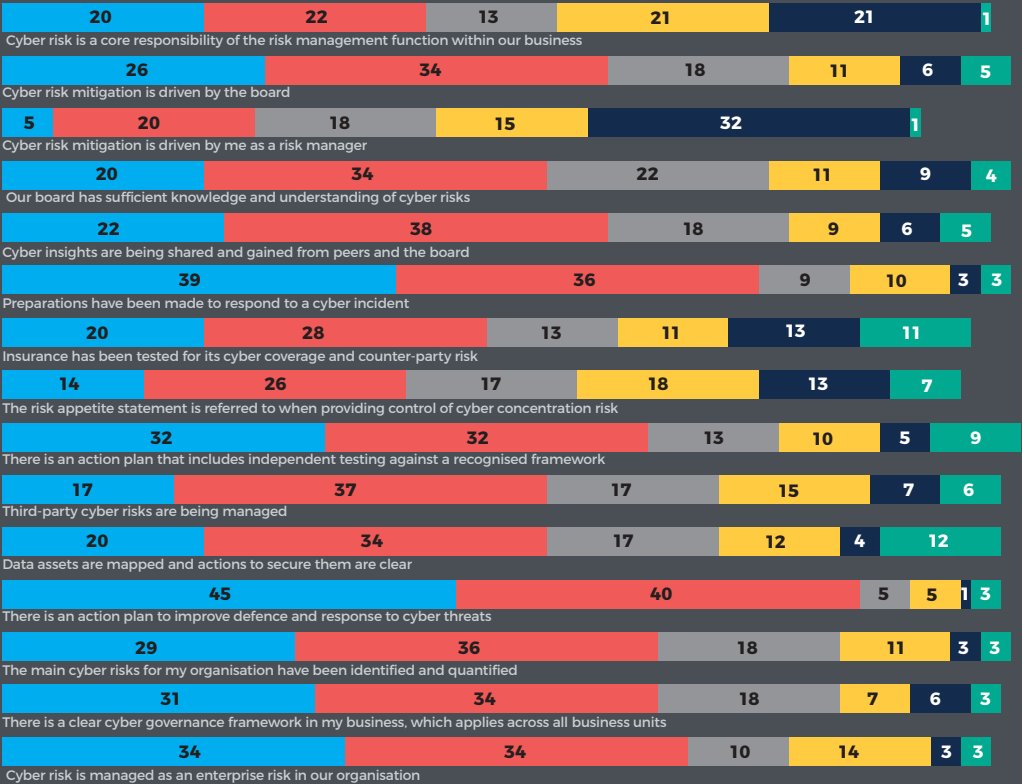


Corporates tend to rely on prevention rather than planning for a breach

Chart 6: Attitudes to cyber risks reflect a disconnect between business units



Thinking specifically about cyber risks, please indicate whether you agree with the following statements



- Agree strongly
- Agree slightly
- Neither agree nor disagree
- Disagree slightly
- Disagree strongly
- Don't know

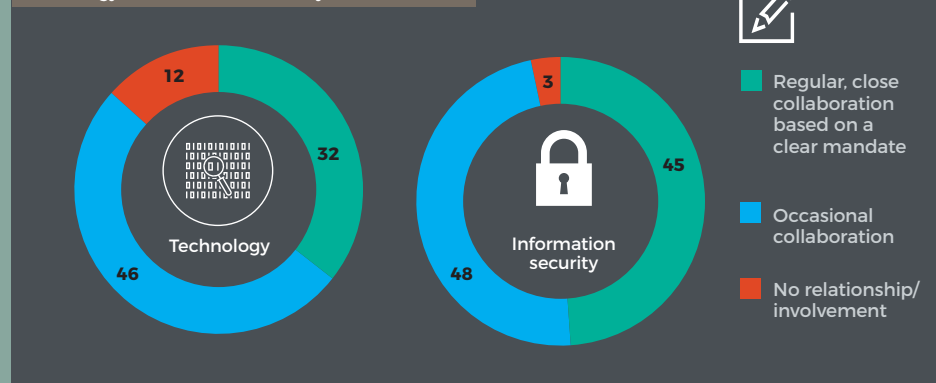
- > “There is a worrying disconnect between risk managers and technology and security personnel, particularly when it comes to detection and response.

And this disconnect is perhaps more defined in detection and response than in prevention, where risk managers may be more involved in auditing and in reviewing preventative and security controls.

“It is during times of crisis – when a cyber attack has taken place – that the risk management, technology and security teams come together for the first time, which isn’t best practice,” says Francis. “We conducted our own research into the cyber risk landscape and found that 47% of businesses are notified of an attack or a breach by an external party and that on average an attacker remains in the system for more than 100 days without being detected. Companies need to be ready for a breach.”

This disconnect may be down to many organisations treating cyber as technology risk and not an enterprise

Chart 7: How often do risk managers collaborate with technology and information security teams?



risk management threat. Only 34% of risk and insurance managers agree strongly that cyber-related threats are being managed as an enterprise risk – with the input of broader business functions, not just the chief information officer and chief information security officer.

LACK OF COLLABORATION

Less than half of respondents (45%) have regular and close collaboration, based on a clear mandate, with their

information security functions. This figure falls to only 32% when it comes to collaboration with their technology functions.

The good news is that risk managers recognise this weakness. Some 46% and 39% of respondents expect to have closer relationships with information security and technology, respectively, over the next three years.

But for cyber to be managed successfully as an enterprise-wide risk



Having risk management embedded in all business functions is the perfect model for preventing and managing technology-related risks

- > and not a technology risk, cyber risk needs to be addressed in the wider business context. Partnerships should extend from information security and technology to business unit leaders in HR, finance, legal and others, says Kyle Bryant, regional manager, cyber risks, Europe at Chubb.

"Risk management needs to be embedded into all areas of the business. Cyber risk and the risk landscape in general are not static, they are constantly evolving at speed. Today's risks have fallen out of reach of traditional methods, so having risk management embedded in all business functions is the perfect model for preventing and managing technology-related and other complex risks."

GOVERNMENT ADVICE

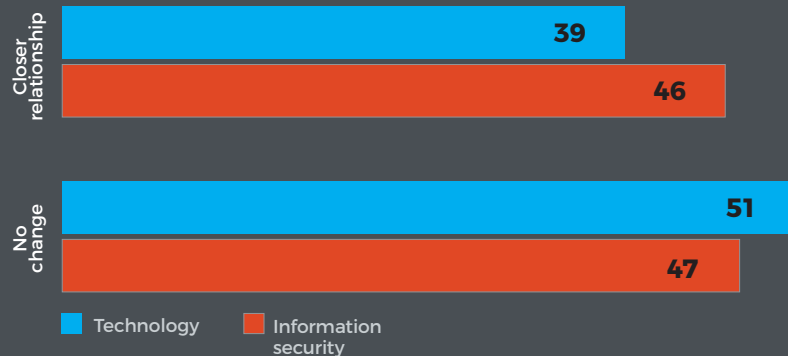
Having clear and robust cyber governance is just as important. This is scrupulously recommended by the UK government's recently formed National Cyber Security Centre (NCSC), as well as the insurance industry.

Adapted from the NCSC's 10 steps to cyber security and Marsh's *Cyber in the city* guidance, Airmic asked respondents to assess their cyber governance against the recommended processes and procedures (see Chart 6, page 22).

The results indicate gaps in cyber

governance (Airmic's newly launched report, *Cyber risk: understanding your risk and purchasing insurance* summaries appropriate structure for effective cyber risk governance). For each recommendation, fewer than a third of respondents strongly agreed that their business had implemented >

Chart 8: In the next three years, what change do you expect to the quality of the relationship that you have with the following functional areas?



the necessary protocols. Only 31% say there is a clear cyber governance framework that applies across all business units; 20% say data assets are mapped and actions to secure them are clear; 17% are fully happy that third-party cyber risks are being managed; 14% say the risk appetite statement is referred to when providing control of cyber concentration risk; 20% say insurance has been tested for its cyber coverage and counter-party risk; and 22% say cyber insights are being shared and gained from peers and the board.

The challenge is to turn these recommendations into action, says Wouter Wissink, information and communication technology specialist, risk engineering services, at Chubb.

ORGANISATION-WIDE THREAT

"Anecdotally and from conversations with clients, some risk and insurance managers tend to treat cyber as one general risk. But it can manifest from anywhere and can be found everywhere. It's not just data theft



Changing the perception of cyber to a risk that will threaten every business unit will create the urgency needed

and vulnerabilities in systems – it's a financial, operational, strategic and reputational risk. So it affects more than just the IT and security department.

"Changing the perception that cyber is one large obstacle that is with the board to viewing it as a risk that will threaten every business unit – and having all department heads as well as risk and insurance managers involved in managing it – will create the urgency needed to improve governance, defence and response."

In other words, people matter as much as the processes.

TOP THREE STEPS FOR INCIDENT RESPONSE

- 1. Define a list of stakeholders**
- 2. Define and categorise the severity of the risks**
- 3. Create a clear escalation matrix and steps for response**



KEY TAKEAWAYS

- **Digitalisation is driving greater frequency and severity in cyber crime, creating new paths for malicious attacks, IP loss and theft, business interruption, and first- and third-party exposures. Cyber-related business interruption and data loss and theft will be significant focal points for risk and insurance managers in the future**
- **For cyber risk to be managed successfully as an enterprise-wide risk (and not a technology risk), the risk needs to be addressed in the wider business context, with partnerships extending from information security and technology managers to business unit leaders in HR, finance, legal and others**
- **Having clear and robust cyber governance is important for the successful management and detection of cyber risk and is scrupulously recommended by the UK as well as the insurance industry**

Cyber insurance

Chart 9: Businesses are increasingly recognising the importance of cyber insurance

Q What approach do you expect to take in future to mitigate the risks that you identified in the previous question?

■ Reduce
 ■ Transfer to the insurance market
 ■ Retain
 ■ Don't know



Cyber crime costs the global economy more than \$400 billion a year and continues to grow, epidemically. With significant sums at risk, businesses are recognising the importance of cyber insurance as part of a wider risk management strategy, as indicated by respondents to Airmic's survey.

Some 48% of risk and insurance

managers, for example, plan to transfer to the insurance market any cyber risks resulting in loss or theft of data, while 52% say the same for cyber-related business interruption.

These figures would have been far lower two or three years ago, said risk and insurance managers interviewed for this report. Many cited a lack of

appropriate and cost-effective risk transfer options as the principal reason for their past dissatisfaction.

EVOLVING PRODUCTS

But cyber insurance is evolving. Products that were limited to property and liability now offer a greater range of cover – for business interruption

as a result of network security failure or attacks, human or programming errors; data loss and restoration; first- and third-party exposures; physical damage and even bodily injury, to name a few. The offerings are a step closer to meeting the complex needs of corporates.

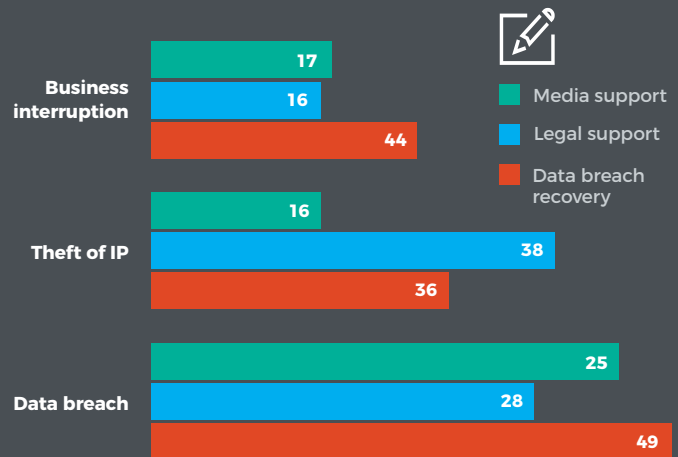
The head of risk and insurance at a UK-based telecoms company says: "There has been a lot of advancement in cyber insurance in the past two years, but prior to that the offerings were very disappointing.

"We now have third-party insurance for our liability; non-physical damage as part of our property damage policy; and business interruption. I'm not dissatisfied but there is still room for improvement and innovation."

>

Chart 10: Managers are calling for greater innovation in key cyber areas

Q. Where should the market focus be on developing services to better support management of the following cyber and digital risks?



That ‘room for innovation’, has been defined by the majority of risk and insurance managers as investing in data breach recovery involving business interruption and data breach risks. Just under half of respondents – 44% and 49% respectively – are calling for more innovation in these areas.

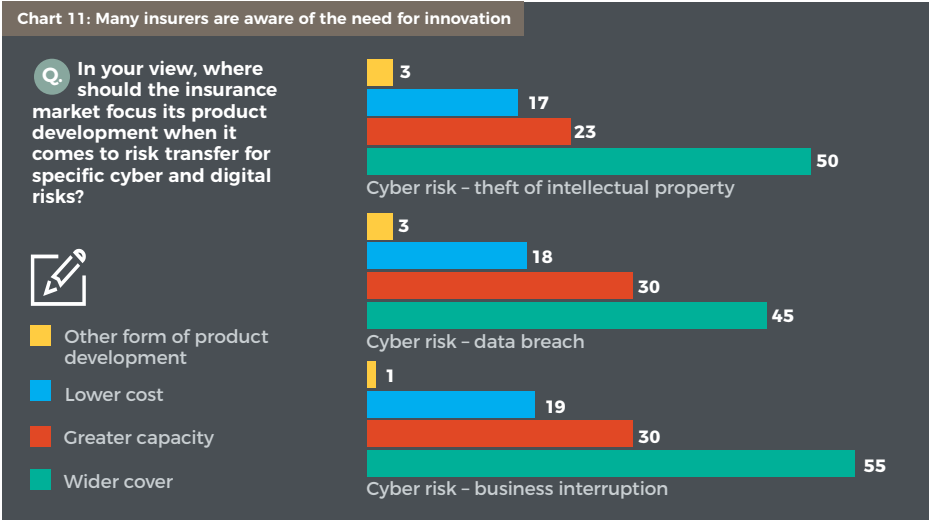
There are also gaps in legal support for theft of intellectual property and data breach, with 38% and 28% respectively wanting to see these areas bolstered with greater investment.

BREADTH OF COVER

Improvements are also needed in the breadth of cover for intellectual property theft, data breach and BI, according to the majority of risk and insurance managers.

The good news is that the cyber insurance market is not at a standstill, with many insurers continuing to invest heavily in the next phase of innovation, says Kyle Bryant, regional cyber risks manager, Europe at Chubb.

“The challenge for insurers, as well as risk and insurance managers, is that



cyber risk is constantly changing and the speed of change outpaces the progress we are making.

“But that hasn’t stifled our efforts to innovate. The insurance industry is making huge strides in innovation to widen and provide clarity in cover. This is evident in the number of products insurers launched recently. The same could be said of the London market, with syndicates offering expanded

cover with increased capacity.”

He adds: “We see the next step for innovation in further developing risk engineering services. To help us do that at Chubb, we are investing in and expanding our in-house risk engineering team, as well as bringing in third-party vendors, to help companies assess and benchmark their exposure and identify key points of weakness.”



KEY TAKEAWAYS

- **Cyber crime costs the global economy more than \$400 billion a year and continues to grow. With large sums at risk, businesses are turning to cyber insurance and integrating it as part of a wider risk management strategy**
- **Just under half of risk and insurance managers (48%) plan to transfer risks related to loss or theft of data, while 52% intend to do the same for cyber-related business interruption**
- **Cyber insurance is evolving and risk and insurance managers are calling for innovation in data recovery and legal support services**





**The speed of
change outpaces
the progress we
are making. But
that hasn't stifled
our efforts to
innovate**

CHUBB®

Chubb is the world's largest publicly traded property and casualty insurance company. With operations in 54 countries, Chubb provides commercial and personal property and casualty insurance, personal accident and supplemental health insurance, reinsurance and life insurance to a diverse group of clients. As an underwriting company, we assess, assume and manage risk with insight and discipline. We service and pay our claims fairly and promptly. The company is also defined by its extensive product and service offerings, broad distribution capabilities, exceptional financial strength and local operations globally. Parent company Chubb Limited is listed on the New York Stock Exchange (NYSE: CB) and is a component of the S&P 500 index. Chubb maintains executive offices in Zurich, New York, London and other locations, and employs approximately 31,000 people worldwide. Additional information can be found at: chubb.com/uk



Airmic
6 Lloyd's Avenue
London EC3N 3AX
Phone: 020 7680 3088
Web: www.airmic.com



The Chubb Building
100 Leadenhall Street
EC3A 3BP
www.chubb.com

