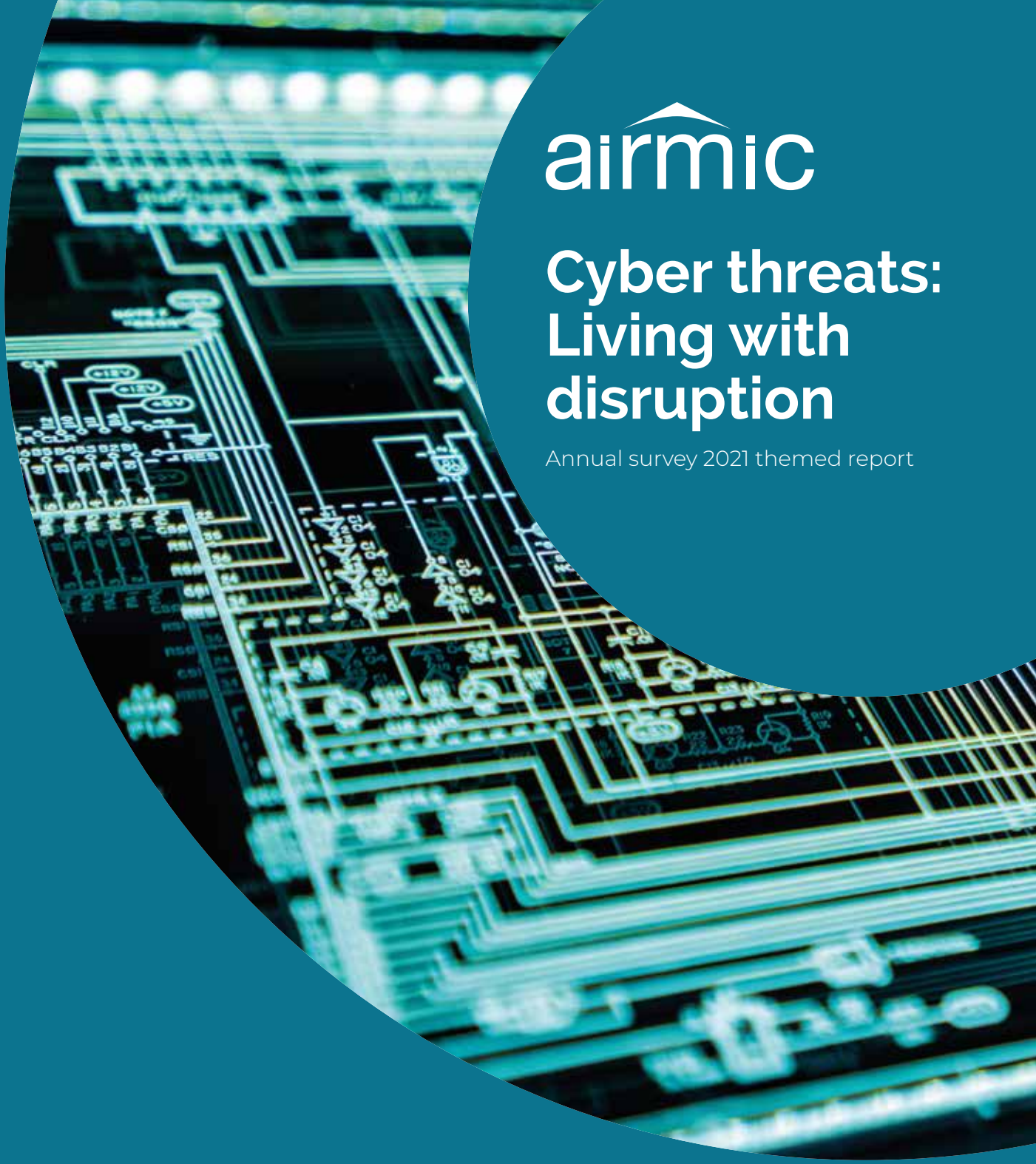


airmic

Cyber threats: Living with disruption

Annual survey 2021 themed report

qrco.de/2021cyber

Control Risks

Contents

> Cyber threats are becoming a form of disruption that organisations must learn to live with. There are steps and new ways of working that they must take as part of a new normal.

Foreword

In a consistently more disruptive and volatile cyber threat landscape, ransomware attacks have continued hitting the headlines, keeping risk professionals across the profession up at night. Ransomware has rapidly become the key cyber threat to organisations globally. This despite an increasingly active and disruptive geopolitical threat picture with individual organisations, global supply chains and critical infrastructure also increasingly targeted by state-linked actors.

As such, the growing and evolving digital ecosystem is both an existential risk and invaluable opportunity for all. Companies that treat it as such and understand the overarching drivers of risk to the digital ecosystem will be better equipped to successfully navigate the complexities of the evolving threat landscape. This approach will prove the most effective and sustainable in building secure, compliant and resilient businesses in the information age.

For organisations, mitigation measures – built on proactive, threat-led cyber security solutions and well-rehearsed and realistic cyber crisis scenarios, including ransomware – can prevent increasingly capable criminal, state and non-state threat actors from forcing your business into unnavigable situations.

In the almost 50 years that Control Risks has supported clients across the globe, the political, technological, environmental and societal landscape has changed beyond all recognition. This has created wealth and opportunities, but also conflict and uncertainty.

Against this backdrop, Control Risks embarked on this study with our partners at Airmic to understand how risk professionals and their organisations are tackling cyber threats today. We hope in turn that this report will be of value to all those seeking to enhance their understanding of the cyber threat landscape, to fine tune risk management strategies to navigate the shifting tides in the global digital threat landscape.

Joseph Buckley,
Associate Director,
Control Risks

Stina Connor,
Senior Analyst,
Control Risks

Executive summary

Cyber threats are becoming a form of disruption that organisations must learn to live with:

- **Ransomware extortion** has rapidly become the key cyber threat to organisations globally.

- A major uptick in **business interruption following a cyber event** is driving changes in the insurance landscape as businesses turn increasingly to insurers for additional protection. Yet, organisations are facing difficulties getting cover for cyber threats from their insurers.

- Disruptive cyber attacks are increasingly becoming normalised as part of **regional rivalries in geopolitical hotspots**. State-sponsored groups have probed the critical national infrastructure of rival states. Disruptive cyber attacks against critical systems in a country's infrastructure increases the likelihood of systemic impacts beyond the intended target, and organisations will need to consider their exposures when operating in geopolitical hotspots.

- **Disinformation campaigns** are likely to become a growing concern over time. The booming 'disinformation-for-hire' market is likely to increase the direct threat of disinformation to private entities.

More than three-quarters of risk professionals have spent more or somewhat more on their cyber budget since the pandemic struck, and they intend to spend even more.

While the pandemic continues to fuel scams, the immediate surge in cyber threats have subsided in 2021, as organisations have got to grips with the threats of operating virtually and populations have become more accustomed to living with the pandemic.

However, the long-term impacts of Covid, most notably through the expanded attack surface, will remain a key challenge for risk professionals.

As organisations increasingly adopt new technologies and solutions, threat actors are likely to follow. For instance, cyber threat actors can leverage AI-powered tools to automate malware or use deepfake technology to improve their social engineering lures. The good news is that many of these technologies also offer real opportunities for defenders to enhance the speed, precision and impact of operational defence, and support organisational resilience.

To manage emerging cyber threats, risk professionals and business leaders should:

- Fine-tune their risk management strategies to navigate these trends in the global cyber threat landscape. They need to adopt a holistic view of how the interconnected global digital ecosystem can impact their organisation and its security.

- Manage IT and suppliers through governance and control, and invest in skills and the broader organisational security culture.

About this research

This study is part of a wider research around the 2021 Airmic annual survey. This is one of five thematic subreports, while the main survey report summarises the full findings of the survey.

Survey & research methodology

The report, produced by Airmic in collaboration with Control Risks, is based on 226 responses gathered in a survey from 21 July to 2 September 2021. Subsequently, roundtables with Airmic members were held to gather qualitative responses. Full details on the survey and research methodology can be found in the main report of the 2021 Airmic annual survey.

Introduction

Just a few years ago, cyber attacks used to be ground-breaking events for companies and organisations. As the scale and frequency of cyber attacks continue to intensify, cyber attacks are now very much an everyday occurrence for organisations across sectors and industries – from disruptive ransomware attacks to large-scale supply chain compromise, companies are increasingly in the targeting focus of cyber threat actors.

It doesn't mean that organisations are just brushing aside cyber threats – far from it. The results of the 2021 Airmic survey show that risk professionals are giving cyber threats the highest priority as a concern. Organisations can now expect to face disruption direct to their IT networks, to their client-facing systems, to operational technologies, to their third-party suppliers, to their IT providers and to the infrastructure they use to power their business, move goods and people around, and communicate through.

For the second year running, business disruption from a cyber event continues to be a front-of-mind risk for risk professionals, according to the Airmic annual survey. There are different developments that lie behind this. Ransomware attacks have been increasingly disruptive, as have been the supply chain disruptions they cause. Cybercriminals in May disrupted the fuel supply to the US East Coast as a result of the ransomware attack on Colonial Pipeline, while hundreds of companies globally were impacted from the attack on software company Kaseya in July.

Cyber threats are becoming a form of disruption that organisations must learn to live with. There are steps and new ways of working that they must take as part of a new normal. What have risk professionals been doing to deal with these growing cyber threats? And what can they do moving forward?

The Covid-19 pandemic triggered a surge in cyber attacks, as threat actors took advantage of the increased reliance on digital services and technological solutions. The pandemic continues to be a key driver of many of these trends. But there are signs that Covid-related cyber threats have been stabilising for much of 2021, as organisations have learnt to operate in the new normal. A critical challenge for risk professionals going forward will be to manage the long-term impacts of the pandemic, as attackers continue to leverage the expanded attack surface – that is, the sum of the different points of access for an unauthorised user to infiltrate to extract data.

One key impediment for organisations in dealing with cyber threats today is having sufficient budgets to deal with these cyber threats within such a narrow time frame. Nevertheless, there are also other steps that organisations can take in the interim to bolster cyber security, most notably in stepping up employees' training and education.

1

Cyber threats

What risk professionals are concerned about

Ranking	Topic	Sub-area	Average score (out of 5)
2	Cyber	Ransomware	**3.89**
7	Cyber	Digital disruption to businesses	**3.66**
10	Cyber	Supply chain threats/third party threats	**3.63**
11	Cyber	State-sponsored disruptive cyber attacks	**3.51**
16	Cyber	Digital transformation of businesses	**3.42**
18	Cyber	Information theft (commercial or competitor espionage)	**3.39**
25	Cyber	Geopolitical technological rivalry	**2.88**
26	Cyber	Disinformation campaigns	**2.76**

1a Ransomware – the no. 2 concern of 2021

"Ransomware extortion has rapidly become the key cyber threat to organisations globally," said Joseph Buckley, Associate Director at specialist global risk consultancy Control Risks. "Organisations' increasing reliance on digital services and interconnected business, IT and operational systems has led to the rising profitability of cybercrime and ever more advanced cybercriminal tactics."

Ransomware was judged the second greatest overall risk in the Airmic survey this year. Almost 70% of respondents see ransomware as a high or very high concern. Operational downtime, out-of-hours and stretched resources, ransom payments, data loss, third-party support and system rebuilds all combine to cripple businesses financially.

To increase the likelihood of organisations paying ransoms, these cyber criminal groups increasingly seek to inflict maximum disruption to their victims and their clients, focusing their attacks on operationally critical and client-facing systems. Groups such as BlackMatter and Conti are increasingly targeting IT, communications and digital service providers to pivot themselves into their targets' client networks, to steal and threaten to leak the clients' sensitive data, and to otherwise disrupt the IT provider and their clients, unless a large ransom is paid.

These often advanced and professional criminal organisations are increasingly taking a leaf from the legitimate business world – they commoditise their ransomware tools and services, create franchises for other skilled cyber criminals to pay a fee to join and then take commission from their franchisees for each successful attack. These groups strategise effectively, focusing on the sectors that are most vulnerable to disruption, such as the manufacturing, pharmaceutical and public sectors, and those companies deemed to hold large volumes of sensitive data, such as digital service providers, law firms and professional services providers.

While these cyber criminals have typically encrypted, stolen and threatened to leak data to extort money, they continue to evolve their extortion tactics to increase pressure on victims through:

- Distributed denial of service (DDoS) attacks
- Data-wiping attacks
- Claiming to have planted backdoors in software products
- Auctioning or selling stolen data to the highest bidder.

Ransoms – to pay or not to pay?

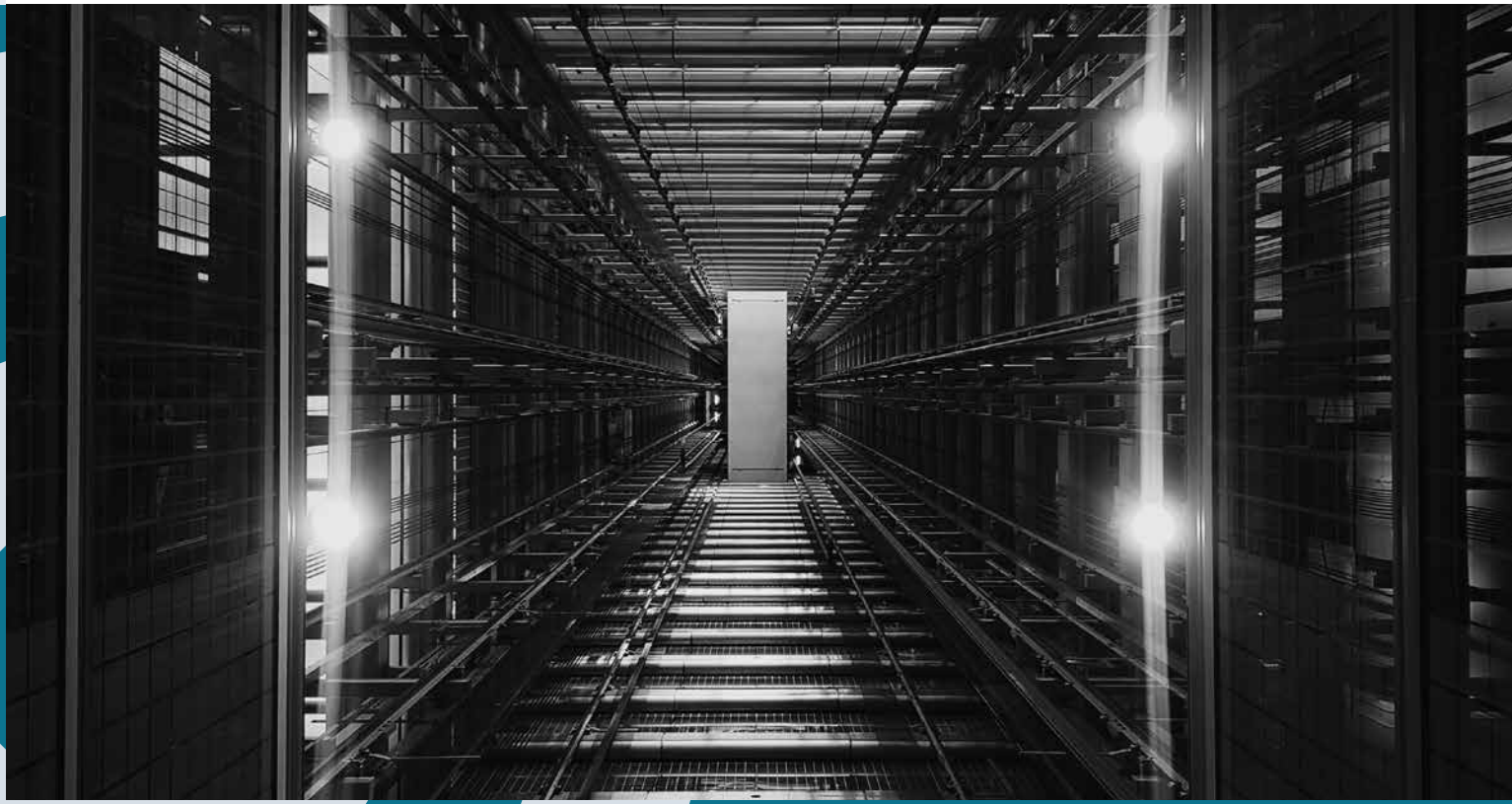
Most authorities and governments strongly advise against making a ransomware payment. This encourages new cyber criminal groups to undertake such attacks and encourages successful groups to do this more often. It also helps these actors learn how best to ensure success for their next cyber attack. Neither is there any guarantee that they will uphold their end of the bargain once a ransom is paid.

When making the difficult decision of whether or not to pay the ransom demanded by cyber criminals in order to minimise further disruption, as did the chief executive of Colonial Pipeline, organisations are advised to inform the authorities, and their own insurers, of the attack. Nearly all insurers would at least require policyholders to show that a ransom payment would not violate financial sanctions imposed on foreign governments, foreign governments, groups and individuals.

Control Risks does not recommend that victims should pay ransom demands. Nevertheless, according to the assessment by Control Risks of most major jurisdictions until mid-2022, the paying of ransoms by organisations will likely be tolerated, so as to mitigate the recovery costs that victim organisations need to shoulder. This may have the effect of emboldening cyber criminals. As such, the severity of ransomware threats will remain high for at least another year.

At the same time, however, authorities will increase pressure on victim organisations to report any ransom payments they make and to share information related to the attacks they face.

The recent recovery by US law enforcement agencies of most of the $4.4 million (£3.1 million) ransom from ransomware actors responsible for the Colonial Pipeline attack demonstrates that law enforcement does maintain the capabilities to respond to ransomware incidents, but this is likely to be reserved for the most impactful incidents and the most threatening and advanced groups. However, ransomware is rising in importance and significance as a challenge to national security, as demonstrated by ransomware now being deemed as big a threat as terrorism by the US Department of Justice. This in turn likely means that more resources will be deployed by state organisations globally to counter this threat. Until then, private companies will be left very much to fend for themselves.



1b Cyber threats and business interruption

Business interruption following a cyber event' emerged as the number one front-of-mind risk for risk professionals in the Airmic survey this year, and 'cyber threats' featured among the top five emerging risks their organisations are facing. Respondents cited major hacks such as the SolarWinds cyber attack, since they have incomplete information about those risks and have limited control over them. In turn, the major upticks in disruption are driving changes in the insurance landscape as businesses turn increasingly to insurers for additional protection against the increasingly financially and operationally crippling cyber threat landscape. Yet, organisations are facing major difficulties getting cover for cyber threats from their insurers, even as systemic threats such as ransomware attacks grow.

There has been a dramatic acceleration in rate increases in cyber insurance this year. In the Airmic insurance market conditions pulse survey of September 2021, 25% of respondents said they are facing rate increases of more than 100% on their cyber lines, with 6.3% of this group of respondents facing rate increases of more than 400%. In the preceding pulse survey of January 2021, no respondents had faced rate increases of more than 100%.

In the roundtables conducted with Airmic members for this report, stories of last-minute rate increases, the reduction of the scope of their policies' coverage or the withdrawal of cover altogether, were the norm this year.

Insurers have also been asking many more questions of their clients, often with little lead time before the expiry of their existing policies. There has also not been a standardised list of cyber-related questions from insurers, which means it makes it prohibitive for insurance buyers to compare quotes from the market.

Insurers have also been removing silent cyber cover – this is where cyber risk is neither explicitly covered nor excluded in insurance policies. This has come in the form of more explicit cyber exclusions in these policies. Organisations have at times relied on silent cyber cover in their property and casualty policies, because a cyber attack could be interpreted as causing 'damage to property' – in this case, to the organisation's data.

The unavailability of cyber insurance has therefore emerged as a major risk in itself for organisations.

Top five front-of-mind risks for risk professionals and their organisations, 2021

	Rank	Rank Distribution
Business interruption following a cyber event	1	
Loss of reputation and/or brand value	2	
Failure of operational resilience	3	
Supply chain failure	4	
Employee health and wellbeing	5	

Source: Airmic survey 2021

Lowest Rank Highest Rank

1c Geopolitical competition puts companies in the crossfire

Geopolitical relations and developments continue to weigh heavily on the cyber risk landscape. 'State-sponsored disruptive attacks' is the fourth most concerning cyber issue highlighted by Airmic members.

Disruptive cyber attacks are increasingly becoming normalised as part of regional rivalries in geopolitical hotspots, such as in the Middle East, where tit-for-tat attacks between Israel and Iran have impacted logistics and transport, port infrastructure, financial, IT and telecommunications, and retail organisations in the past year. Elsewhere, including in Europe and the US, state-sponsored groups have probed the critical national infrastructure of rival states. Disruptive cyber attacks against critical systems in a country's infrastructure increases the likelihood of systemic impacts beyond the intended target, and organisations will need to consider their exposures when operating in geopolitical hotspots.

Cyber activity sponsored by nation states also impacts several other key concerns for Airmic members, including supply chain and third-party compromise. In the past 12 months, large-scale state-sponsored attacks, such as the compromise of IT suppliers SolarWinds and Microsoft Exchange, have impacted organisations globally. Rapid technology adoption and increasing reliance on digital services during Covid-19 have increased organisations' exposure to attacks on IT suppliers and other third parties, while states have intensified their targeting of supply chains as part of global espionage campaigns.

Geopolitical rivalry over technology, most notably the competition between the US and China, is of concern to organisations, especially when they lead to supply chain disruption in high-tech industries. Over 20% of Airmic members consider 'tech wars' to be a high or very high concern, according to the survey, signaling the impacts on the private sector from geopolitical rivalries largely beyond their control.

"Competition among states for technological supremacy and the global rise of digital nationalism is putting global companies in the crossfire," said Stina Connor, Senior Cyber Threat Intelligence Analyst at Control Risks. Kaspersky, Huawei, TikTok, WeChat, Facebook and Google are just the most prominent examples of how the global technological ecosystem is fragmenting, but this technological decoupling will affect a growing number of organisations across sectors.

As Airmic members are expanding their technology investments – in particular in cloud infrastructure, artificial intelligence and smart technologies – they are likely to find themselves increasingly impacted by competing regulation and considerations across the different jurisdictions in which they operate. "Businesses will have to increasingly weigh macro-level political and national security considerations when engaging in a jurisdiction or with a specific supply chain partner about which their host government has a negative view," said Stina Connor.

Competition among states for technological supremacy and the global rise of digital nationalism is putting global companies in the crossfire.

1d Disinformation – an emerging threat

Despite being a lower concern in this year's survey compared to other cyber-related risks, 'disinformation campaigns' is an area likely to become a growing concern over time.

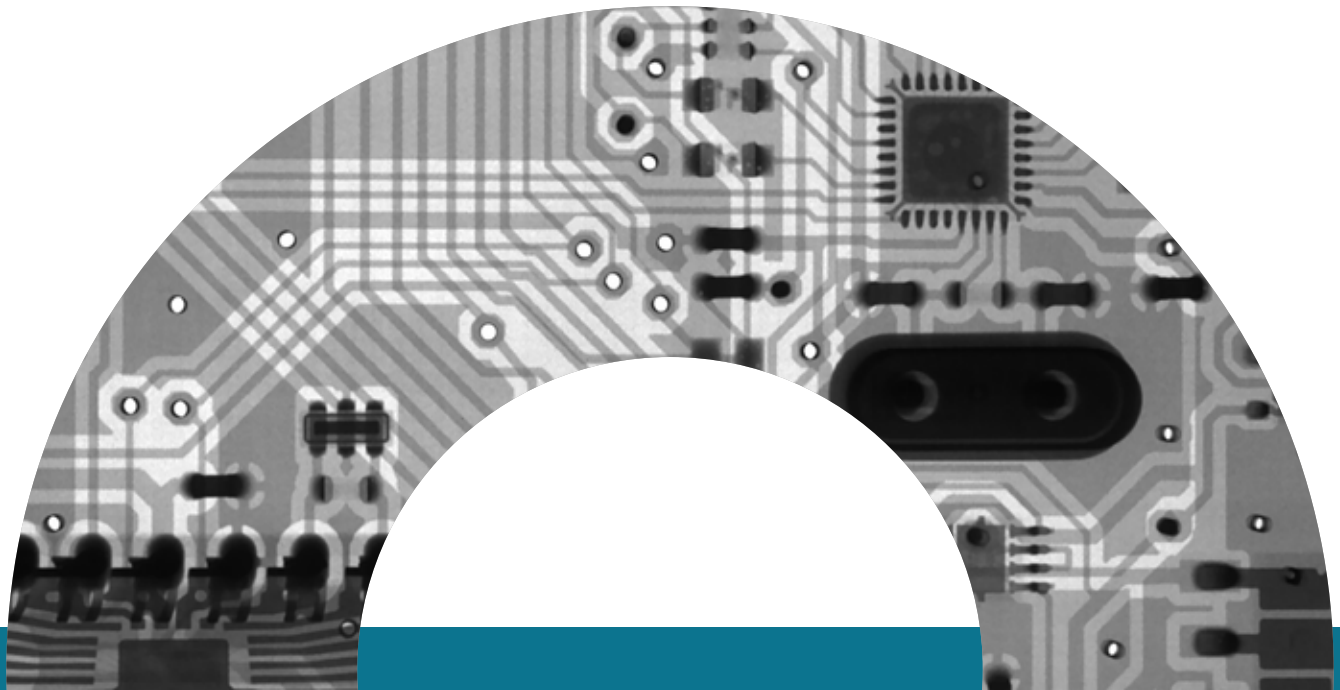
Disinformation operations are often considered as limited to politically driven campaigns, with limited direct impacts on businesses. However, when systemic threats of disinformation emerge, governments and states are not the only targets, as companies associated with them become collateral damage. For example, in 2017, fake memes were circulated stating that Starbucks would give out free frappuccinos to undocumented migrants in the US, at a time when the political debate over undocumented migrants was especially heated. A user on 4chan, a right-wing imageboard, said that the Starbucks hoax "could cripple their business a bit".

The growing scale of disinformation campaigns can pose an indirect threat to companies. Disinformation campaigns – such as those that seek to damage public trust in Covid-19 vaccinations and counter-measures – could hamper efforts behind the post-pandemic economic recovery and therefore impact businesses. Disinformation campaigns also increasingly have a tangible impact on the physical world, not in the least demonstrated in the storming of the US Capitol on 6 January 2021 by supporters of the QAnon online conspiracy, as well as other groups. As such, disinformation campaigns seeking to fuel discord and polarisation in societies can impact organisations operating in targeted geographies.

Looking ahead, the booming 'disinformation-for-hire' market is likely to increase the direct threat of disinformation to private entities. Private disinformation actors include advertising, marketing and public relations companies that offer services designed to manipulate online opinion and sentiments in favour of their clients, whether politicians and governments or commercial actors.

For private sector organisations, such operations will likely manifest as efforts to damage reputations, business operations or the revenue of competitors. One tactic likely to see increased use is the abuse of adverts on social media to target the customers of commercial products and services. For example, in 2020, Facebook removed a network of accounts pretending to be dissatisfied consumers of three telecommunications providers in Myanmar. The campaign was traced to a competing telecommunication operator and was assisted by a PR company in Vietnam.

Organisations likely to be targeted by disinformation campaigns should communicate to stakeholders and educate employees on how to quickly and effectively counter disinformation, and also develop an incident response plan to counter such threats. Those in the public and media sectors should regularly consult on the key trends and threats associated with disinformation in the jurisdictions in which they operate.



2

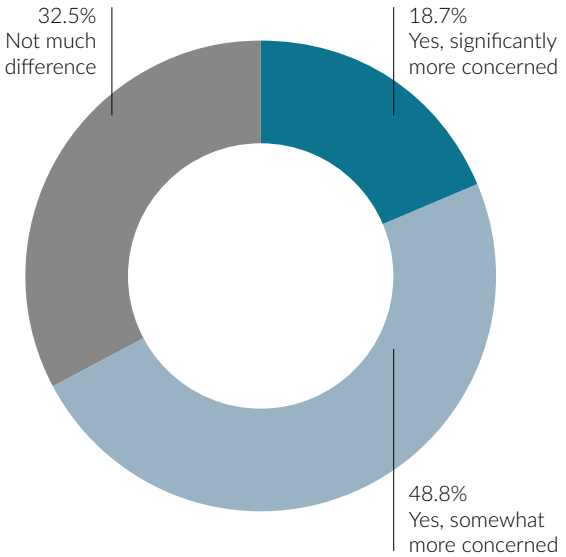
What is the fallout from cyber incidents for organisations?

The speeding up of digital transformation programmes caused by the Covid-19 pandemic has accelerated many of the trends associated with these cyber risks. For many organisations, the switch to remote working needed to be made almost overnight and, with that, the related cyber risks of having employees accessing company data from home increased significantly. Of our respondents, 67.5% have become more concerned about cyber security since the Covid-19 pandemic hit the UK around March 2020.

While the pandemic continues to fuel scams, the immediate surge in cyber threats have subsided in 2021, as organisations have got to grips with the threats of operating virtually and populations have become more accustomed to living with the pandemic.

However, the long-term impacts of Covid, most notably through the expanded attack surface, will remain a key challenge for risk professionals. This has fuelled a significant increase in cyber threats globally, not least in the targeting of IT supply chains and service providers. New malware samples have nearly doubled over the past year, while vulnerabilities have hit a new high, including vulnerabilities to critical infrastructure.

Has your organisation become more concerned about cyber security since the Covid-19 pandemic hit?



To meet the threats related to the expanded attack surface, organisations have:

Strengthened controls and changed technological protection

Undertaken a strategic global review of hardware and software processes

Purchased Cyber Liability insurance for the first time

Implemented additional monitoring and controls

Appointed a Head of Data and Technology

Increased their focus on training and awareness.

More than three-quarters of risk professionals have spent more or somewhat more on their cyber budget since the pandemic struck, and they intend to spend even more.

Since the pandemic struck, how has your organisations cyber budget been impacted? (In terms of cyber controls and cyber insurance)

	Percent
We have spent more, and intend to continue doing so.	49.2
We have spent somewhat more, but intend to spend much more.	27.1
There has been no change, and there is unlikely to be further changes.	22.1
We have spent less, but will now spend more.	1.6

Even in the face of budgetary pressure in tackling cyber threats and risks, organisations need to take a highly prioritised approach to reducing the level of risk they face in the cyber domain. This includes understanding that phishing email campaigns could be part of a mass campaign, where the attacker is just looking to collect some new passwords or make some easy money, or it could be the first step in a targeted attack against an organisation, where the aim could be something more specific such as the theft of sensitive data.[1]

At the Airmic roundtables, one risk professional shared about their organisation's programme on digital safety, which monitors the changing threat and reacts quickly to any new or heightened threats, including having the right to block access or terminate systems links where necessary. Their organisation has also reinforced mandatory training on digital safety.

New malware samples have nearly doubled over the past year, while vulnerabilities have hit a new high, including vulnerabilities to critical infrastructure.

1 https://www.ncsc.gov.uk/guidance/phishing

3

Emerging technologies, digital transformation

Besides cyber threats, the survey results also show that organisations and businesses face challenges from digital transformation. The findings demonstrate that there is an imperative for organisations to transform digitally by investing in new technologies and solutions – and, indeed, the pandemic lockdowns forced many organisations to transform overnight. This technological charge will continue to increase connectivity across all industries and, with it, the exposure to digital threats.

Cloud solutions and artificial intelligence (AI) have emerged as the technologies that most organisations are looking to invest in next. Nevertheless, the investment needed remains the most common obstacle to the adoption of new processes and technologies in their work

What technologies are you looking next to invest more in to adopt? (select all options that apply)

	Percent
Cloud solutions	51.3
Artificial intelligence (AI), machine learning (ML) and other automation tools	36.5
Internet of Things (IoT)	14.8
We have spent less, but will now spend more.	1.6
Smart technologies (e.g. smart factories, vehicles or other smart devices)	20.9
Blockchain	9.6
None of the above	10.4
Others	3.5

What are the obstacles to the adoption of new processes and technologies in your work?

Obstacles	Percentage of respondents who said so
The investment needed. 50.9	**50.9**
The level of skills within your department to use them.	**22.3**
The level of digital maturity in your organisation.	**20.5**
The perceived lack of added value from using them.	**15.2**
Resistance to change internally by your organisation.	**14.3**
Regulatory and legal uncertainty.	**13.4**
Control over tech investment.	**9.8**
Resistance to change internally by your department.	**3.6**
Consumer sentiment.	**2.7**

As organisations increasingly adopt new technologies and solutions, threat actors are likely to follow. Cloud solutions are already facing intense targeting by both state-linked and criminal cyber threat actors. The increasing automation of business and industry is also likely to drive increased targeting of cyber and physical systems by cyber threat actors seeking to cause disruption, whether for geopolitical or financial gain.

Emerging technologies also present an opportunity for cyber attackers to up their game. For instance, cyber threat actors can leverage AI-powered tools to automate malware or use deepfake technology to improve their social engineering lures.

“The good news is that many of these technologies also offer real opportunities for defenders to enhance the speed, precision and impact of operational defence, and support organisational resilience,” said Stina Connor, Senior Cyber Threat Intelligence Analyst at Control Risks. “Security professionals will need to enhance their situational awareness today, boost their understanding of technologies and work closely with business leaders to carefully consider how to mitigate these emerging threats in the face of increasingly complex technology environments.”

Conclusion

What do organisations need to do now to be prepared and stay resilient?

It is no longer a matter of 'if' but 'when' an organisation will suffer a cyber attack. Joseph Buckley, Associate Director at Control Risks, advises: "For organisations, mitigation measures – built on proactive, threat-led cyber security solutions and well-rehearsed and realistic ransomware crisis scenarios – can prevent increasingly capable ransomware groups from forcing your business into a situation where a ransom payment is an enticing option."

The digital technologies and systems used today have brought opportunities and challenges alike for business leaders and risk professionals. The overnight switch to remote working due to the pandemic has provided the context of new ways of working. Digital transformation, in which organisations tap on emerging technologies, is unavoidable if business models are to be kept resilient. Yet, the increased use of emerging technology also brings with it new opportunities for cyber attackers.

To manage these emerging threats, risk professionals and business leaders should:

- Fine-tune their risk management strategies to navigate these trends in the global cyber threat landscape. They need to adopt a holistic view of how the interconnected global digital ecosystem can impact their organisation and its security.

- Manage IT and suppliers through governance and control, and invest in skills and the broader organisational security culture.

Meanwhile, business leaders have strategic decisions to make when developing transformation roadmaps, managing IT and suppliers through governance and controls, and investing in skills and the broader organisational security culture.

Organisations have always had to live with disruption even as they seek to thrive. Cyber threats are the disruption they now have to face, as the digital transformation of business and everyday life takes place.

About Control Risks

Control Risks is a specialist global risk consultancy that helps to create secure, compliant and resilient organisations in an age of ever-changing risk. Working across disciplines, technologies and geographies, everything we do is based on our belief that taking risks is essential to our clients' success. We provide our clients with the insight to focus resources and ensure they are prepared to resolve the issues and crises that occur in any ambitious global organisation. We go beyond problem-solving and provide the insight and intelligence needed to realise opportunities and grow.

www.controlrisks.com

About Airmic

The leading UK association for everyone who has a responsibility for risk management and insurance in their organisation, Airmic has over 450 corporate members and more than 1,500 individual members. Individual members are from all sectors and include company secretaries, finance directors, and internal auditors, as well as risk and insurance professionals.

Airmic supports members through learning and research; a diverse programme of events; developing and encouraging good practice; and lobbying on subjects that directly affect our members and their professions. Above all, we provide a platform for professionals to stay in touch, to communicate with each other, and to share ideas and information.

www.airmic.com

airmic

Marlow House
1a Lloyd's Avenue
London
EC3N 3AA

Tel: +44 207 680 3088
Fax: +44 207 702 3752
Email: enquiries@airmic.com
Web: www.airmic.com