CyberCube | Munich RE

Key insights into systemic cyber risk

Findings from CyberCube and Munich Re's joint expert survey

Authors

Munich RE

Stephan Brunner
Senior Cyber Actuary

Tim Davy
Cyber Innovation Consultant

CyberCube

Jon Laux
Vice President of Analytics

Ethan Spangler
Lead Economist

Editorial Manager:

Yvette Essen
Head of Communications
& Market Engagement
at CyberCube

Editorial Design:

Felix Paula
Growth Marketing Creative
at CyberCube

Executive summary

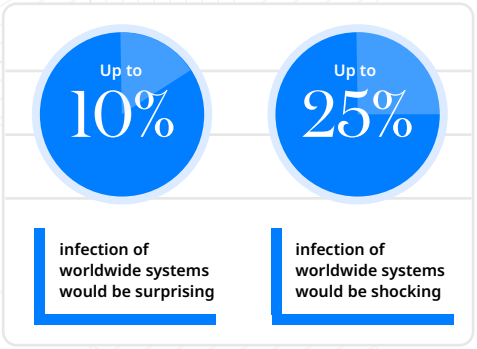
CyberCube and Munich Re have collaborated on a survey of cybersecurity experts to advance the insurance industry's understanding of systemic cyber risks, focusing primarily on widespread malware and cloud outage events. This initiative was designed to gather expert judgment in different areas of accumulation modeling where empirical data is limited or non-existent, to test and refine cyber catastrophe modeling assumptions, and to explore the practical realities of cyber resilience and mitigation.

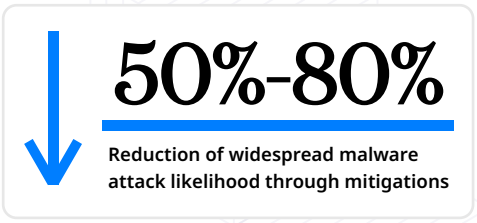
With responses from 93 cybersecurity experts spanning a range of disciplines and industries, the survey provides nuanced insights into potential impacts, attack vectors, and mitigation effectiveness. We are aware that the sample of experts is not representative but rather selective, with a high weight on the US and large corporations. This sample reflects the current cyber insurance market very well, but of course, we would like to learn more about companies from other regions, industries, and sizes.

Key findings:

Widespread malware risk

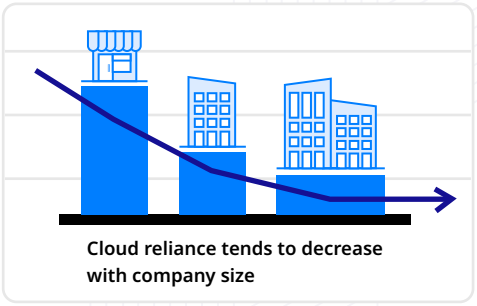
- Extent of Infection: Another event on the scale of WannaCry or NotPetya would not be seen as surprising to most experts. A 10% global infection rate would be surprising, while a 25% rate would be truly shocking.
- Effective Mitigation: Patch management, network segmentation, and data backups are identified as the most effective mitigations that organizations have against widespread malware attacks. When done effectively, such mitigations can reduce the chance of being affected by a widespread malware attack by 50% to 80% and reduce the financial impacts of such an event by a similar amount.

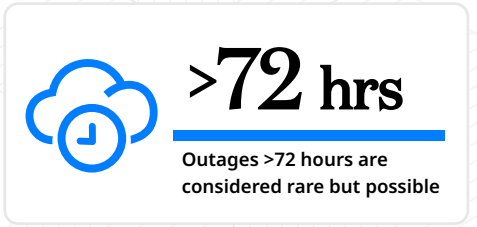




Cloud risk

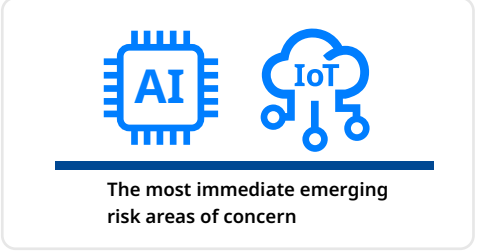
- Growing and Varied Dependency: Most industries now exhibit at least a medium level of dependency on cloud services, with critical business operations increasingly reliant on them. Reliance tends to decrease with company size, although micro firms show more variation.
- Outage Duration and Impact: Cybersecurity experts expect broad cloud outages to last hours to days, with outages beyond 72 hours considered rare but possible.
- Mitigation: The most effective mitigation against cloud outages is to establish a multi-region architecture with the cloud service provider(s) (CSPs) used for critical business applications. Having multiple CSPs was not found to be effective, as organizations commonly use different CSPs for different objectives, and the option to transfer service during an outage of one provider was seen as unfeasible.
- Perceived Resilience: The top 3 global cloud providers are viewed as the best-prepared to mitigate against a major cloud outage and to recover from such an event.





Emerging risks

- Internet of Things (IoT) devices and Large Language Models (LLMs) are seen as the most immediate emerging risk areas of concern.



Survey objectives

Whenever building a model for cyber risk accumulation, there are two major challenges. Firstly, to find out what can happen, and secondly, to parameterize the scenario once the first question is answered. In terms of cyber, the two straightforward ways to answer the above questions are data and expert judgment.

For other perils like earthquake and storm, historical data is available. In cyber, however, this is a bit more challenging as there have not been many events in the past (cyber is still quite 'young') and the underlying risk is constantly changing due to continuous technological development and a dynamic risk landscape.

Therefore, the use of data is limited since it either does not exist or severe events must be extrapolated from data with a high degree of uncertainty (e.g. deriving the impact of a severe long-duration outage from a short-duration outage). Thus, expert judgement on cyber events holds particular value and can help to better parameterize cyber accumulation events.

Currently, the cyber insurance market widely agrees that a widespread malware event and a long and widespread cloud outage are the biggest accumulation scenarios for most portfolios. Therefore, the survey focused on these two scenarios as well as other emerging risks that could have large magnitude losses for the cyber insurance industry.

Consequently, the goals of our survey were threefold:

1. To inform cyber catastrophe modeling by capturing expert perspectives on scenarios where data is sparse, such as the footprint of a large-scale cloud outage or the spread of a major malware event.

2. To test whether model assumptions, particularly with regard to risk mitigation, still hold true in today's cyber landscape.

3. To gather informed and relevant views that could validate or challenge model hypotheses through expert interpretation.

Overview of survey respondents

We conducted the survey from April to September 2024 and reached 93 seasoned professionals. Most respondents have over a decade of cybersecurity experience (see **Exhibit 1**) and include cloud architects, malware specialists, cyber risk managers, and operational security leaders. Each respondent only answered questions relevant to their area of expertise.

Exhibit 1

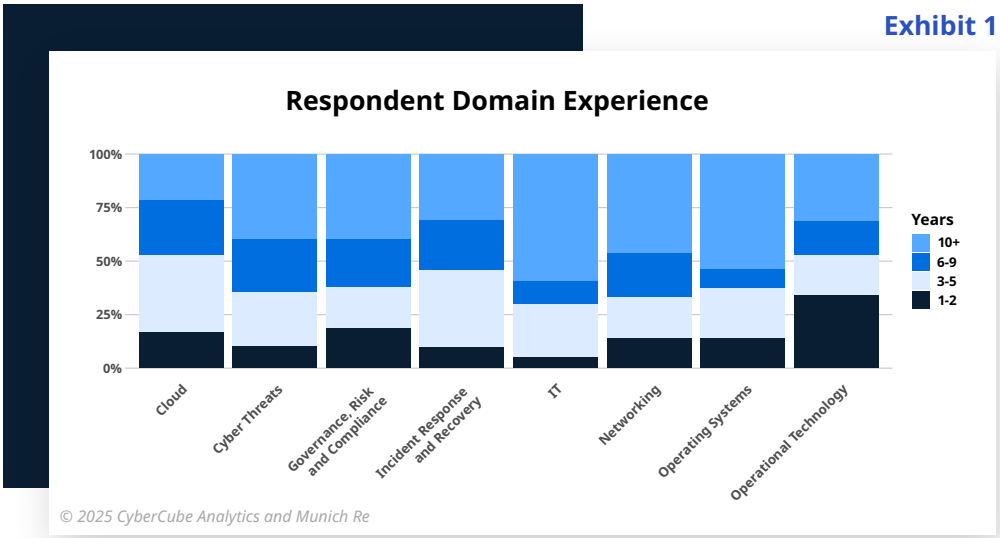
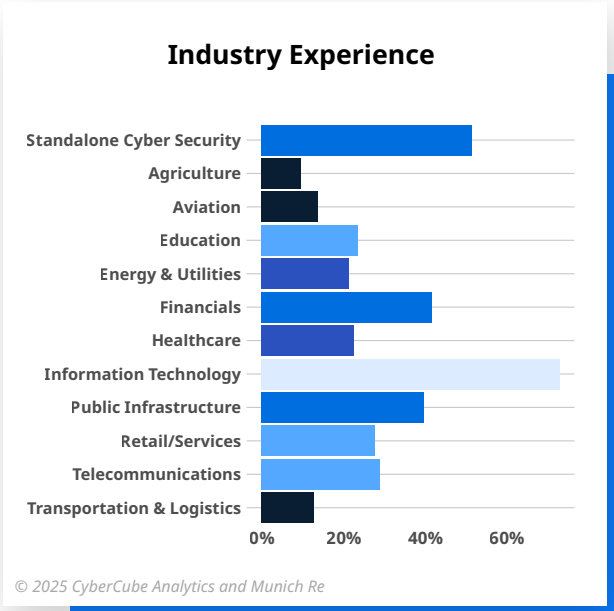


Exhibit 2



As shown in **Exhibit 2**, these experts have applied their cybersecurity experience across various sectors, including IT, finance, public infrastructure, energy, and standalone cybersecurity firms. Notable participants were employed at companies including Google, CrowdStrike, and Deloitte. The breadth and depth of their expertise allowed for a comprehensive view of the systemic cyber threat landscape.

Methodology

While risk quantification is a key objective for us as cyber risk modelers, we recognize that most people, including cybersecurity experts, are not accustomed to thinking quantitatively. As a result, we found it more effective to frame many questions qualitatively that could be grasped intuitively, as well as constrain questions to focus on the near-term technological landscape. Additionally, for further context, some respondents chose to participate in an interview to elaborate on their responses.

We also asked experts to consider extreme outcomes rather than averages. For example, in the case of a global malware event, instead of asking for an "expected" number of affected systems, the survey asked respondents what percentage of global systems infected would surprise, shock, or seem impossible to them. While not immediately translatable to statistical measures such as the 90th percentile, this approach to data collection allowed us to gather perspectives from a wide range of experts. Subsequent analysis of the results reinforces this approach, showing sensible and consistent responses.

We would like to reiterate that the data gathered through this survey reflects the opinions of the participants and does not necessarily reflect reality. We used this data to add another perspective to already existing parameters and maybe amend them. It is essential to note that a different set of participants or a change in question phrasing could lead to slightly different results. The aim of this survey, however, is to obtain a directionally reliable perspective on extreme events that would also be robust with another set of experts.

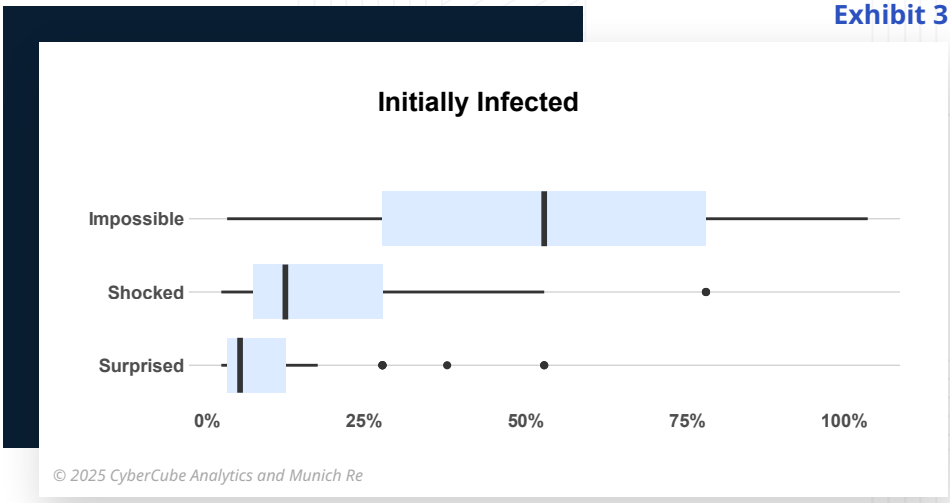
Widespread malware risk

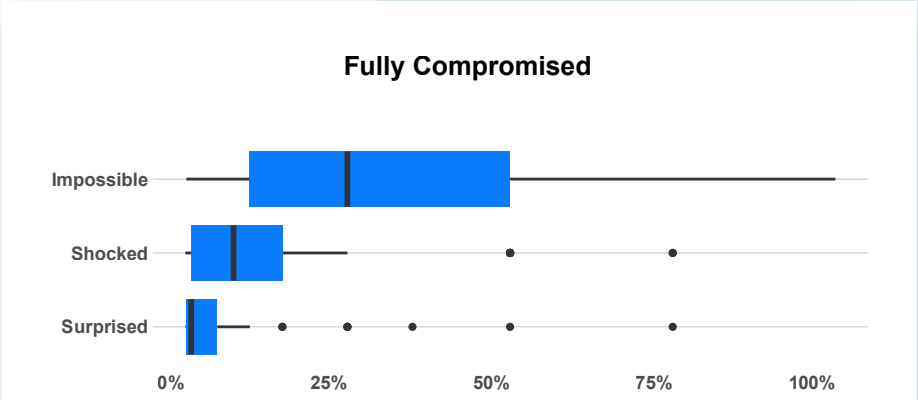
Malware propagation and infection rates

The results indicated that a 10% global infection rate would surprise many experts, while a 25% rate would be shocking (see **Exhibit 3**). A full compromise affecting even 5% of systems was considered a surprising scenario. These insights are particularly valuable for modeling the tail of the risk distribution, where catastrophic insurance losses would occur. They also put events like WannaCry and NotPetya in context, which each affected at most ~0.5% of global machines according to the upper bound of estimates. This means that another event on the scale of WannaCry and NotPetya would not be seen as "surprising" by most experts.

This means that another event on the scale of WannaCry and NotPetya would not be seen as "surprising" by most experts.

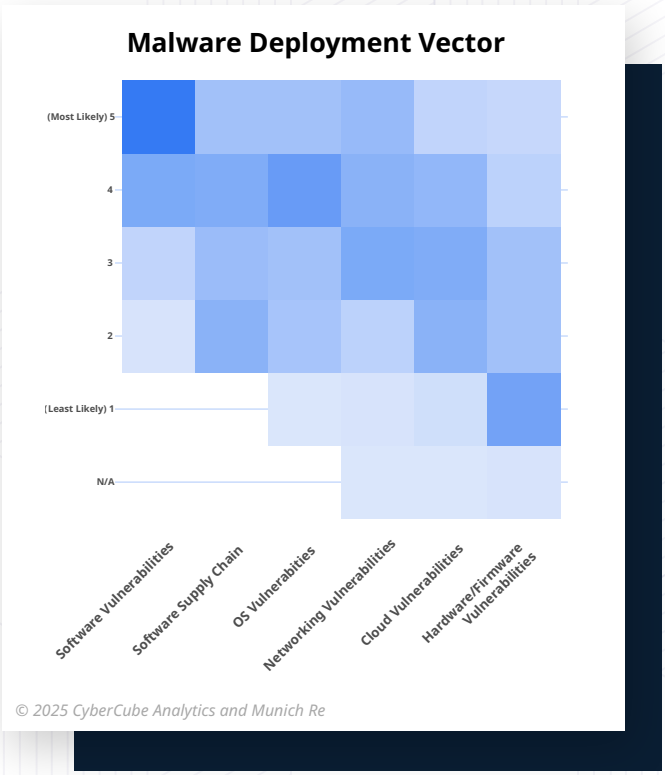
Exhibit 3





The survey also asked for perspectives on the time required to achieve such a level of global infection. Respondents indicated that reaching a 5% global infection rate within **one week** would be expected, while achieving that level in just **three days** would be unexpected but plausible. An infection spreading to that level within **12 hours** was considered extreme; however, it was still within the realm of possibility. These findings highlight the rapid potential escalation of malware and the importance of early detection and containment.

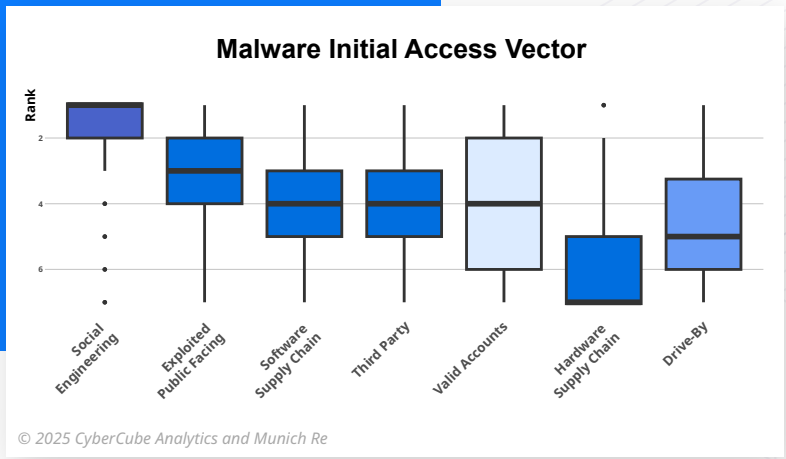
Exhibit 4



Regarding initial access and spread, the most plausible factors contributing to widespread malware events were identified as software vulnerabilities, software supply chain updates, and operating system vulnerabilities (see **Exhibit 4**).

Hardware-based vectors were considered more complex and thus less likely to cause mass-scale outbreaks, while cloud vulnerabilities were ranked moderately. **Exhibit 5** shows, interestingly, social engineering was overwhelmingly seen as the top vector for initial access, but it was not regarded as a major driver of events due to its low scalability. This points to a critical vulnerability-exploitation pathway that is both preventable and persistent.

Exhibit 5



Mitigations for malware risk

Experts were asked which mitigations are deemed to help reduce the likelihood of being affected by a widespread malware event, as well as which would help reduce the financial impact of such an event once infected. Patch management, network segmentation, and maintaining up-to-date backups emerged as the most effective strategies. These three controls significantly reduced both the likelihood and impact of malware events, with the former two reducing likelihood and the latter two reducing impact. Meanwhile, Antivirus and MDR/XDR solutions were seen as moderately effective; the lack of significant distinction between these two mitigations was surprising. Although social engineering was rated a top vector for malware, security awareness training was only rated as "somewhat effective", revealing a misalignment between threat recognition and mitigation confidence.

Experts were asked to translate the effectiveness of these controls into numerical terms. Many experts estimated that organizations with strong cyber hygiene could expect a 50-80% reduced likelihood of being impacted by a widespread malware event, as well as a 50-80% impact reduction if they were in fact compromised (**Exhibit 6**). Interestingly, no expert believed that adopting all of these mitigation methods could completely 100% protect an organization, highlighting that there always remains a perceived degree of risk. These insights are particularly valuable given the shortage of prior catastrophic events available to learn from.

> *Many experts estimated that organizations with strong cyber hygiene could expect a 50-80% reduced likelihood of being impacted by a widespread malware event, as well as a 50-80% impact reduction if they were in fact compromised.*

Exhibit 6

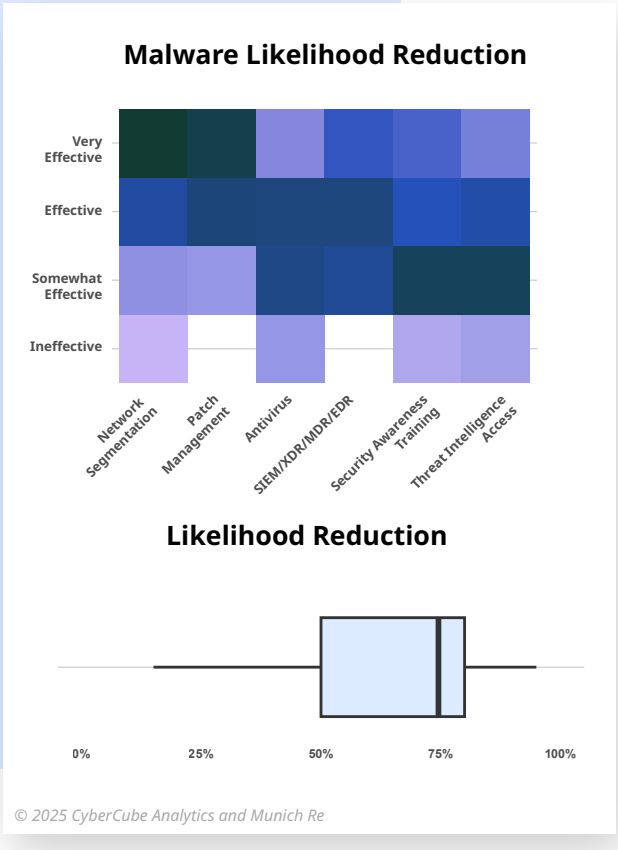
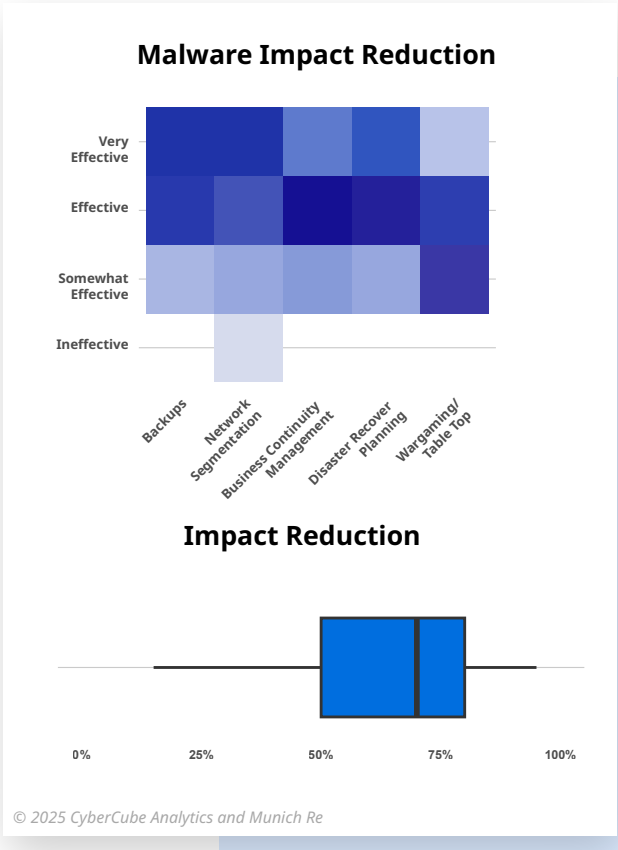


Exhibit 7

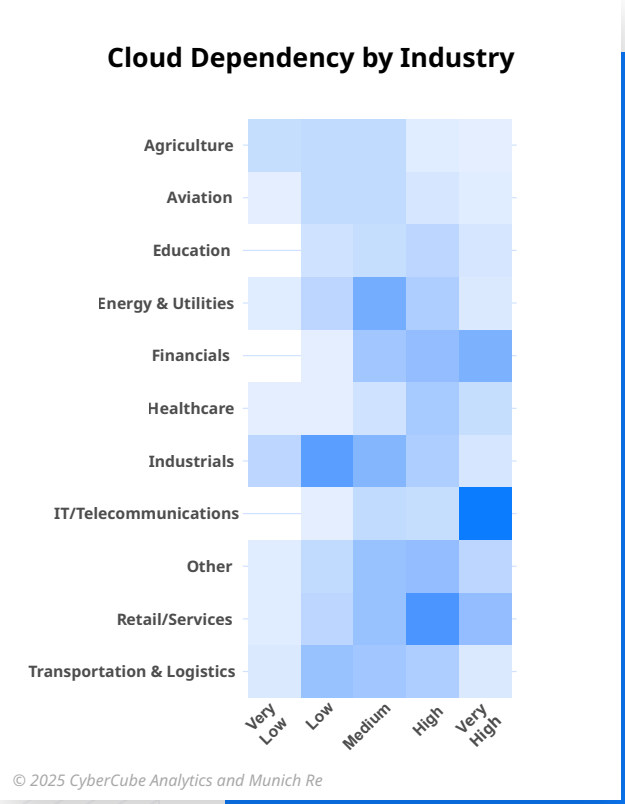


Cloud risk

Cloud reliance

One of the most significant insights regarding Cloud risk was the extent to which today's critical business processes rely on cloud service providers (CSPs). **Exhibit 8** highlights how reliance was commonly estimated at "High" or "Very High" for technology-forward industries such as IT, Telecommunications, Financials, Healthcare and Retail. Moreover, in heavy industries such as Construction, Marine, Mining, and Energy/Utilities, "Low" or "Medium" dependency was seen as the most common. We have witnessed the growth of CSPs' businesses over many years, but this survey result was a tangible reminder that they have indeed gained importance for many businesses around the world.

Exhibit 8



One of the most significant insights regarding Cloud risk was the extent to which today's critical business processes rely on cloud service providers (CSPs).

It was interesting to see that security practitioners who focus on the Cloud consistently rated CSP reliance as higher than corporate risk managers did. Cloud practitioners estimated that between 40% to 90% (the interquartile range) of business-critical functions are cloud-based, while risk managers generally estimated a lower range of 35% to 75%.

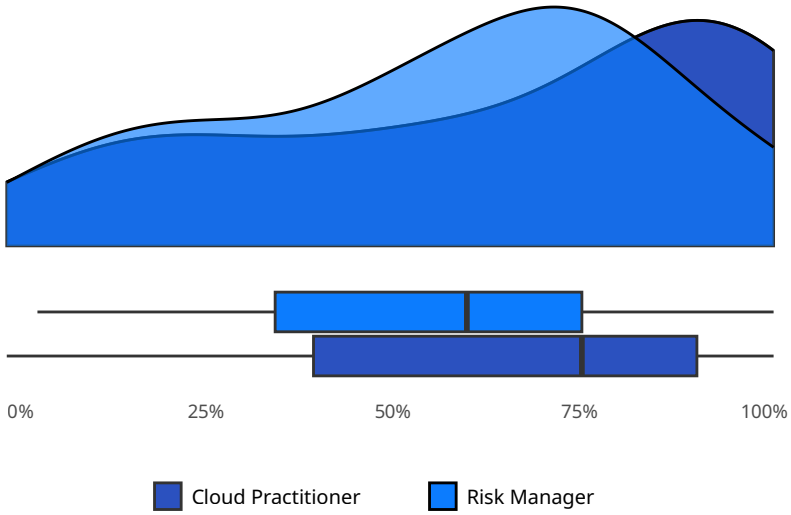
As **Exhibit 9** shows, there is an overlap between these ranges. Nonetheless, it does suggest there are different levels of understanding about the cloud's criticality. The difference in estimation could be due to risk managers having a greater understanding of their own networks.

On the other side, this difference could be from cloud practitioners having a greater understanding of the indirect reliance on the cloud, such as processes that occur off the cloud but are a function of cloud-based processes. This is compounded by the complexities of today's IT infrastructure where on-premises and IT services are closely integrated, making it more difficult to distinguish between them from a risk perspective.

Exhibit 9

Cloud Reliance

What percentage of business-critical processes rely on at least one CSP?



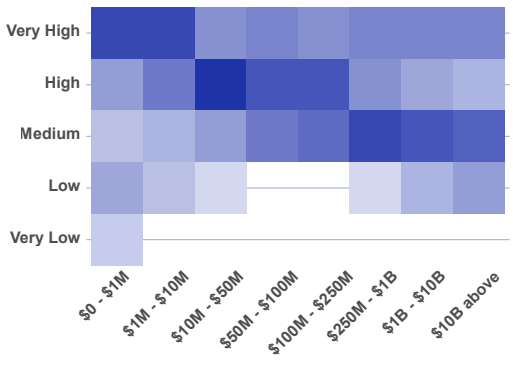
According to respondents, dependency levels on the cloud varied by company size (see **Exhibit 10**). Small and mid-sized firms, particularly those with revenues between $10 million and $100 million, were found to be the most reliant on cloud services. Larger organizations showed declining dependence, likely due to more robust on-premise and hybrid architectures.

Micro firms displayed the widest variability, with some heavily reliant on lean IT structures, and others minimally dependent due to limited digitization.

Exhibit 10

The majority of organizations utilize multiple CSPs, though typically for separate processes. We asked risk managers how complicated it would be to switch over from one CSP to another when their primary CSP was down. Respondents noted that although some services by sophisticated firms can run across multiple CSPs and be dynamic in their deployment, it was perceived as unlikely that an organization could move from one CSP to another during a severe outage.

Cloud Dependency by Revenue

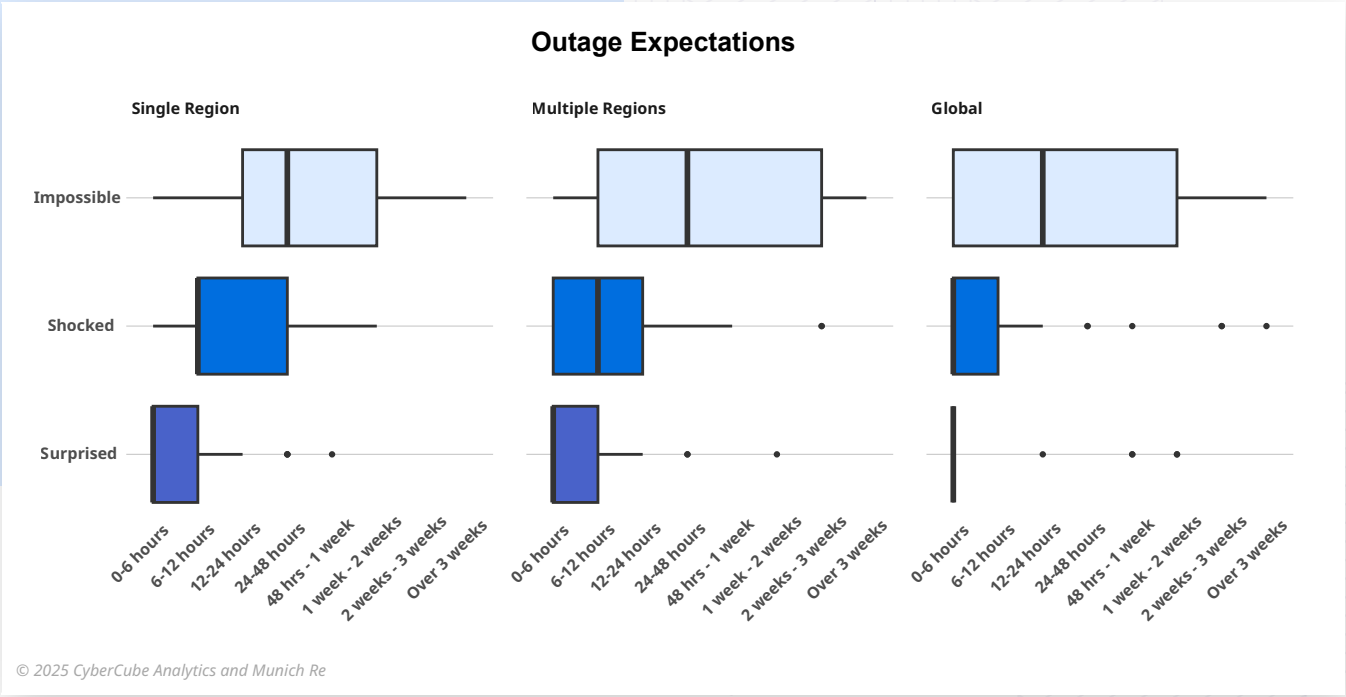


Outage expectations & loss scaling

Experts agreed that cloud outages lasting hours to a few days are plausible (see **Exhibit 11**). Still, a significant minority foresaw the possibility of multi-day or multi-week outages in the long run. While extended outages were not considered likely, they were not dismissed as implausible, especially for multi-region disruptions.

The answers from the experts showed that the larger the extent of an outage (availability zone vs. region vs. global), the shorter the expected duration.

Exhibit 11



We were also interested to understand how financial losses scale with cloud outage duration.

Respondents reported that a single-day outage of their most critical CSP would likely result in a financial loss equal to 1% of their yearly revenue. If the outage were to extend to five days, over half of the respondents stated that losses would increase by at least a factor of 7, whereas others stated that it was less than 5 times their one-day loss.

This variation in losses for some firms reflects differences in dependency on the cloud, based on an organization's size, sector, and contingency planning.

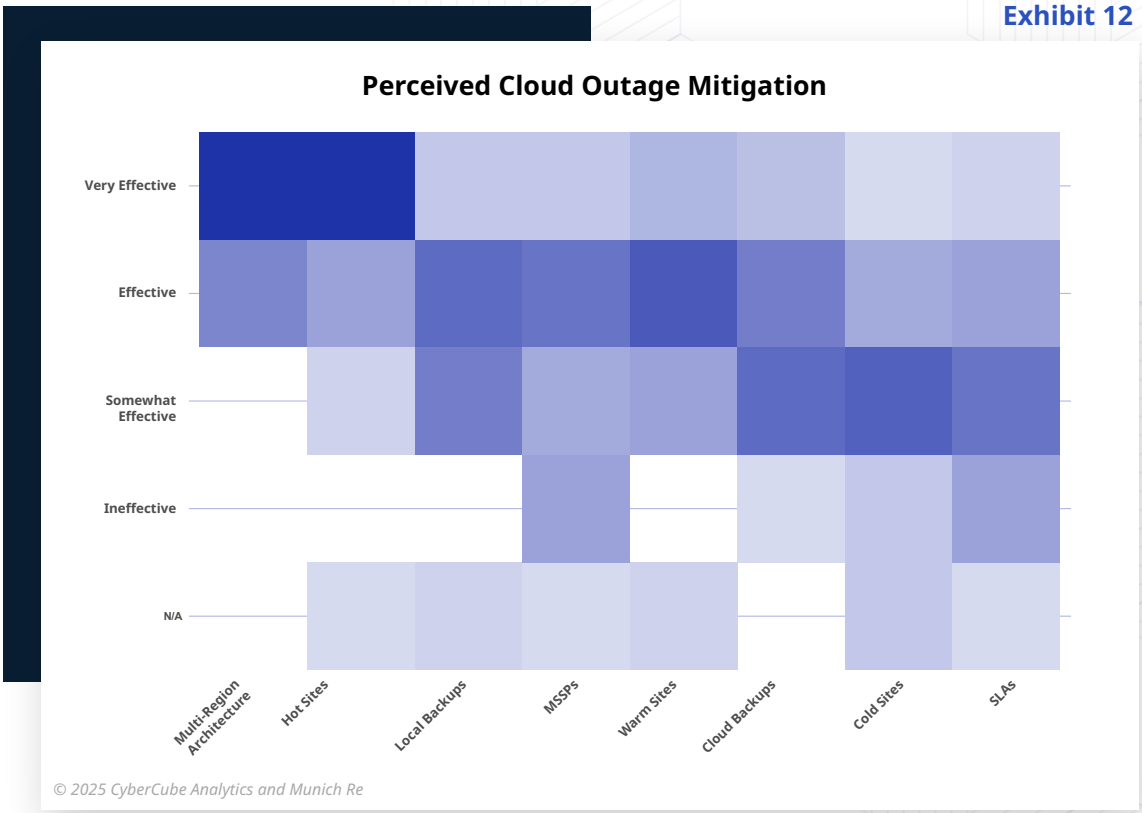
Furthermore, it implies that for certain segments, a cloud outage would become increasingly costly the longer it persists, while other segments may see the opposite.

Cloud risk mitigations

The survey also aimed to gain a better understanding of the best ways organizations can mitigate their exposure to cloud outages. Whereas traditional on-premises architecture would utilize combinations of backups and site replication depending on the business requirements, cloud infrastructure is often seen as offering a key advantage through its underlying architecture of availability zones and regions. These allow production systems to be replicated and transferred in accordance with outages and business needs whilst optimizing costs.

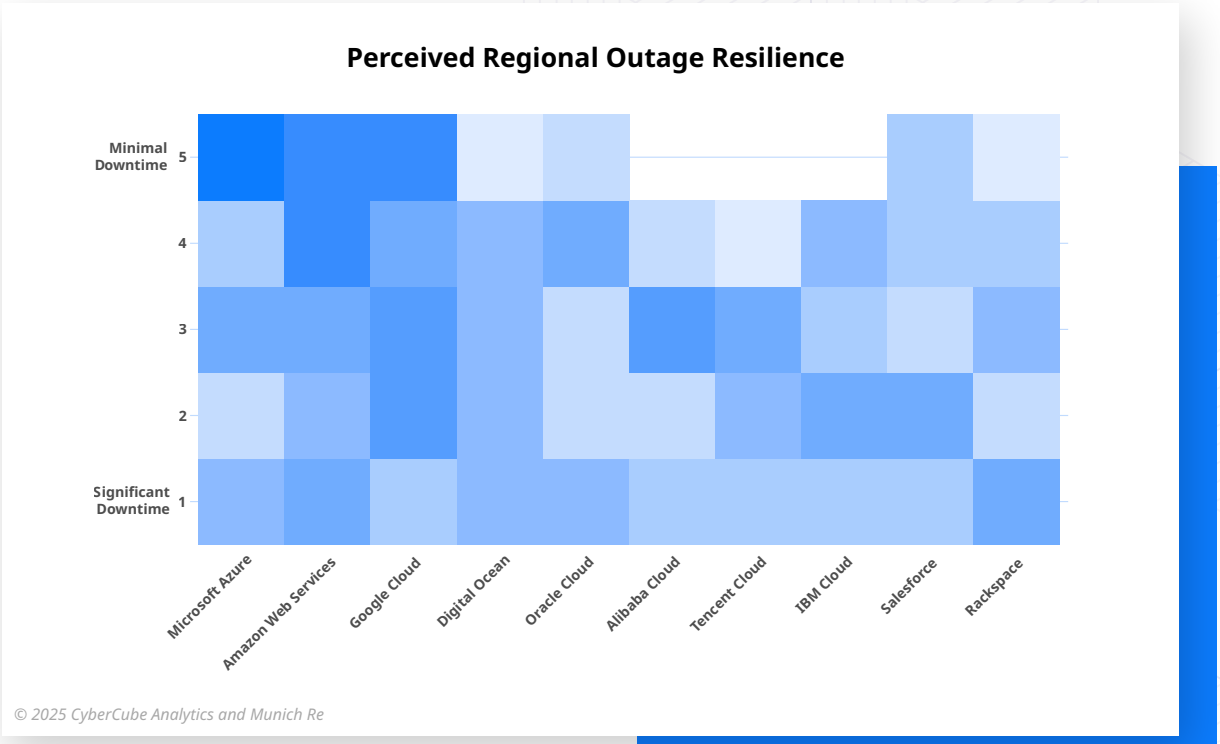
This explains the response in **Exhibit 12**, where survey respondents echoed this hypothesis. In interviews, additional insight highlighted that technical complexities and cost implications were key for organizations when deciding which mitigation strategy to use. Companies generally maintain offline backups for their most critical data, with certain sectors demonstrating particularly high adoption. Banking is the most likely to implement offline backups, followed closely by the Financial, IT, and Telecommunications sectors.

Exhibit 12



As illustrated by **Exhibit 13**, Azure was perceived to be the best-positioned CSP for multi-region resilience, followed closely by AWS and then Google. Most large organizations use multiple CSPs, but typically for separate workloads rather than redundancy. This means the appearance of diversity may not equate to actual resilience in practice. More than half of all firms were found to configure their cloud environments internally. The survey indicated that internal configuration resulted in a nearly 2x greater risk of misconfiguration, compared to setups handled by external experts. This highlights a major operational vulnerability that standard risk assessments may not fully account for.

Exhibit 13



Emerging and systemic risks

The survey also explored perceptions of broader systemic risks and sector-specific threat profiles. Experts were asked to assess the likelihood of various cyber events, including software supply chain compromises, device-level ransomware, and wiperware attacks. The results showed that many of these scenarios, although remote, are still considered plausible and may be interpreted as being underrepresented in current risk models.

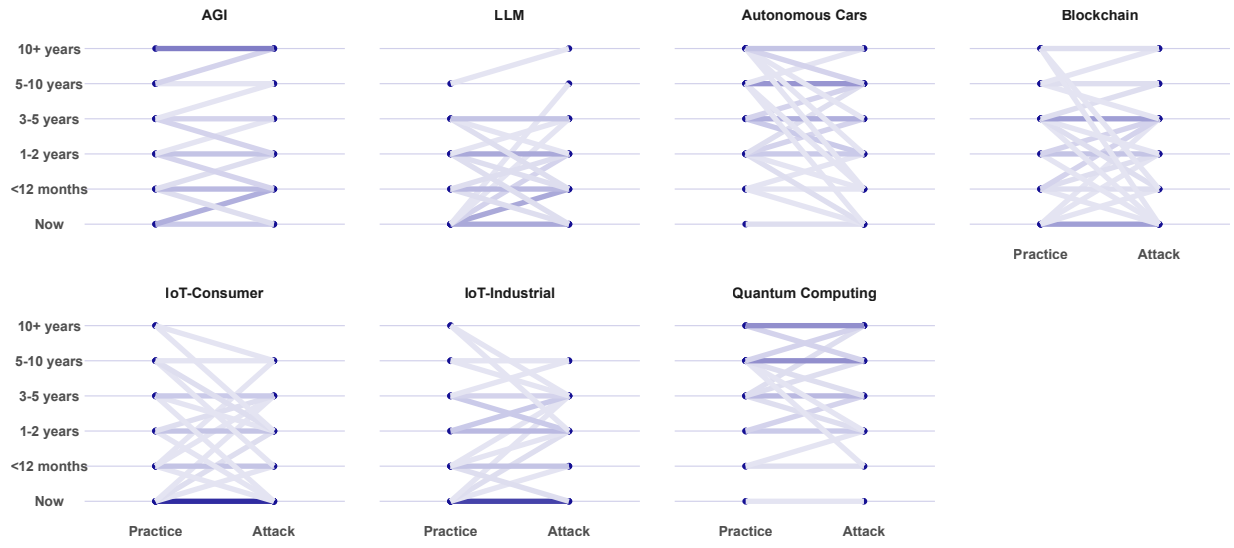
In general, experts believe that a new technology will begin to affect the threat environment ("Attack") at about the same pace that it is being adopted in cybersecurity practices ("Practice" – see **Exhibit 14**). In the near term, Industrial and Consumer Internet of Things (IoT) devices pose the biggest concern. Respondents differentiated their views between Artificial General Intelligence (AGI) and Large Language Models (LLMs), with LLMs being regarded as having an impact now and AGI being a greater concern in five or more years. This difference is due to LLM tools already being widely available to practitioners and attackers, while true AGI does not currently exist.

LLMs have shown to be productivity enhancers across industries, allowing users to quickly learn and implement cybersecurity methodology on both the defense and attack side. For example, LLMs allow for scaling sophisticated spear phishing operations, whereas previously those were laborious exercises. Conversely, LLMs also allow practitioners to analyze the sentiment, origin, and prior communications of messages to better detect phishing attempts.

Exhibit 14

Emerging risks

Applied to current technology, how many years are there until the following technologies have a significant impact to cybersecurity practices? Or until they lead to new areas of large-scale cyber-attacks?



Conclusions

The survey reinforced many existing modeling assumptions while also revealing new dimensions of cyber risk. It did not produce new data in the traditional sense – instead, it validated model hypotheses through qualitative insight that can be quantitatively parameterized. A fundamental challenge in cyber risk modeling is the deficiency of concrete tail-risk events, such as systemic malware or multi-region cloud outages. This survey represents the best attempt to parameterize plausible worst-case scenarios and establish expert consensus, adding credibility to CyberCube's model forecasts and feeding into Munich Re's internal model and accumulation risk understanding.

The findings also highlighted the growing ability to differentiate organizational resiliency using expert-driven variables, such as hygiene maturity, backup practices, and dependency structures. These insights help shape a more nuanced view of how systemic cyber events might unfold and the factors that drive wide variation in risk exposure across firms.

CyberCube and Munich Re collaborated on this research with the aim of gaining external perspectives on key ideas currently under consideration. More importantly, this initiative focused on building out critical data sets in areas where existing information is limited or non-existent. The objective was to advance market understanding, particularly concerning risk mitigation strategies for systemic cyber events. As cyber accumulation modeling is a joint effort of the whole insurance industry, the main survey results are made public to foster dialogue between different market participants. This survey is the third of its kind. CyberCube and Munich Re will conduct another survey in 2026, where all interested experts are invited to participate.

The research has contributed to a more refined understanding of the relative resiliency of organizations to systemic events and the key variables that influence an organization's ability to withstand such incidents. These findings represent an important input into CyberCube's and Munich Re's evolving view of cyber risk and help inform ongoing enhancements to their modeling approach. CyberCube has incorporated these insights into Version 6 of its risk aggregation platform, Portfolio Manager.