panaseer

2022 Cyber Insurance Market Trends Report

ABOUT THE EXPERTS

David Fairman

CSO and CIO at Netskope

David Fairman is an experienced CSO/CISO, board member, investor and coach. He's worked and consulted for large financial institutions and Fortune 500 companies. David has been actively involved in founding several industry alliances and expert groups across multiple regions.

Andreas Wuchner

Security and risk expert

Andreas is a recognised cybersecurity and risk expert, with more than 25 years' experience as a business owner, board advisor and investor in complex global business environments. He advises cybersecurity startups in the US and Europe.

Nik Whitfield

Founder of Panaseer

Nik founded Panaseer in 2014. Previously he built automated trading systems and advanced cybersecurity detection systems for global financial institutions at BAE Systems Detica.

Contents

SECTION 1:

Introduction

Cyber insurance is facing a tipping point. The industry isn't working for insurers, brokers or their customers. Premiums are increasing, policy coverage is being limited, and many insurers are struggling to make money due to the rising number and cost of claims.

This predicament is a result of several factors. Cyber-attacks are increasing, driven by the rise of ransomware. Some estimates suggest ransomware attacks were up by nearly **93% year-on-year in 2021**[1].

Insurers also struggle to accurately assess an organisation's security posture and the risks involved. Whereas risk models for some lines of insurance have been fine-tuned over centuries, cyber insurers only have a few years of data to look back on. Worse still, in cybersecurity the past is not a good predictor of the future, as adversaries are innovating to find new and improved returns on their investment.

What makes this especially challenging is that insurers don't have access to accurate data regarding customers' assets or security controls. Not only is this critical information not currently collected, it changes daily.

A healthy cyber insurance market is one where all parties benefit. Change is needed so the insured can buy the coverage they need at a cost-effective premium, while insurers can accurately understand their portfolio risk exposure, and turn a profit over time. Even better if the process of insuring leads to understanding and change which reduces cyber risk.

To understand where the industry goes from here, we surveyed 400 global insurers to get their view on the trends impacting cyber insurance. We also spoke to CISOs and risk experts, who offered insights on what the survey data means for insurers and the insured.

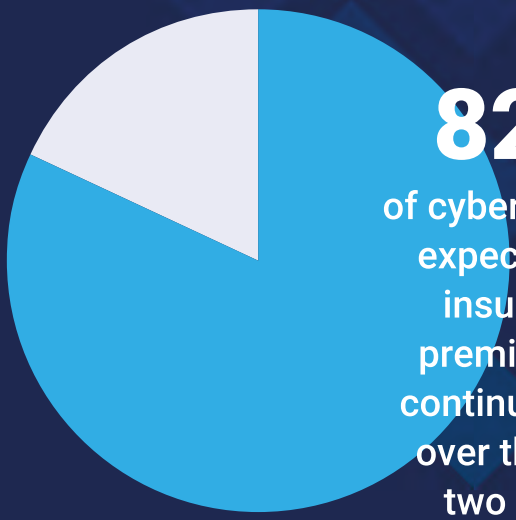
The results show there's an appetite for creating a new approach to cyber insurance that works for both sides.

1 Security Magazine (2022), *Ransomware attacks nearly doubled in 2021*

SECTION 2:

State of the industry

The price of cyber insurance cover grew by **130% in Q4 2021 alone**[2], but any organisations expecting respite will be disappointed. The majority of insurers in our survey (82%) expect cyber insurance premiums to continue rising over the next two years. This is to be expected given the current loss ratio on cyber insurance policies.



82%

of cyber insurers expect cyber insurance premiums to continue rising over the next two years

According to data published by the National Association of Insurance Commissioners (NAIC), the top 20 cyber insurers in the US saw loss ratios averaging **66.9% in 2020**[3] (the most recent year for which data is available). However, three of the insurers in the group saw losses exceed **100%** of their total premiums. In comparison, none of the top 10 car insurers in the US saw loss ratios above **75% in 2021**[4].

> **Rising premiums are causing organisations to question the value of cyber insurance. It's just becoming too expensive.**
>
> David Fairman, CIO and CSO at Netskope

While increasing costs are inevitable, it will likely mean some organisations look for alternative options. "Rising premiums are causing organisations to question the value of cyber insurance," says David Fairman, CIO and CSO at Netskope. "It's just becoming too expensive."

He believes organisations need to make a decision based on their own operational resiliency. "If you've built a very resilient organisation, and you're confident it could absorb an impact and recover, do you really need insurance at that point?" says David.

This is leading to a growing trend for self-insuring, where organisations set money aside to cover themselves should they suffer a breach.

"This is happening more and more because premiums are ridiculously expensive," says Andreas Wuchner, a cybersecurity and risk expert. "Organisations are instead investing in improving their own security rather than making the insurance companies rich."

2 Marsh (2022), *Global Insurance Market Index Report*
3 Insurance Journal (2021), *Top 20 Cyber Insurers in U.S. Including Loss Ratios: NAIC*
4 S&P Global (2022), *US private auto insurers' loss ratios shoot higher in 2021*

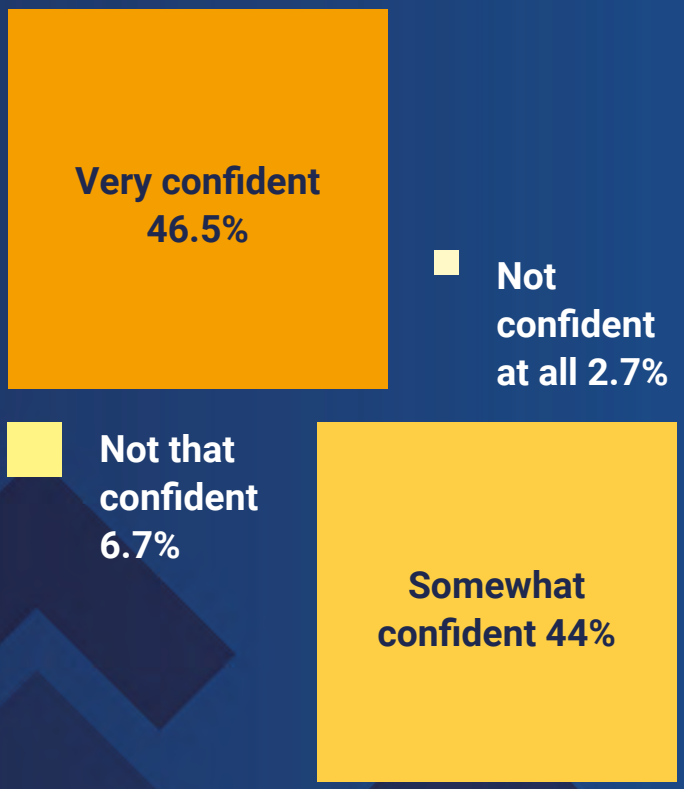
Looking for a new risk model?

Despite the losses made by several of the top US cyber insurers, confidence appears to be high that existing risk models give an accurate picture of a customer's security posture. In our survey, **91%** of total respondents said they have faith in their underwriting process.

But there are indications that many in the industry know a different approach is needed. While **46.5%** said they are 'very confident' in their underwriting process, **44%** are only 'somewhat confident'. Furthermore, **9.5%** said they were 'not that confident' or 'not at all confident', rising to **15%** among UK respondents.

This lack of confidence in risk modelling among a minority of insurers could cause some to exit the market altogether. Around one in 10 UK respondents (**11%**) said they wouldn't continue to offer cyber insurance in three years if their method of assessing risk stayed the same.

Confidence in cyber insurance underwriting process



"Existing methods of measuring cyber risk aren't sufficiently evidenced or dynamic," explains Nik Whitfield, founder of Panaseer. "IT environments and threats are constantly changing. Organisations currently only provide questionnaire-based opinion on security posture, normally once per year, rather than evidenced facts as their risk profile changes."

In response, insurers have begun asking for more information on an applicant's security posture, while also reducing the amount they'll pay out or refusing to cover claims for specific known vulnerabilities. According to one report, insurers that had issued cyber liabilities policies worth $5 million in 2020 were **scaling back to limits of $1 million to $3 million in 2021, even on renewals**[5].

"Insurers are asking more and more questions, and that's putting strain on the organisations trying to get insurance due to the time and resource it takes to collect the information," explains David Fairman. "It's almost like being scrutinised by a regulator, if not worse."

> **"Existing methods of measuring cyber risk aren't sufficiently evidenced or dynamic."**
>
> Nik Whitfield, founder of Panaseer

As applications become more complicated, there's a greater risk that organisations either can't answer the questions or provide incorrect data. Indeed, the data will inevitably become inaccurate the day after the policy is signed, as IT environments, business activities and the threat environment all change. Insurers might then refuse to pay out in the event of a claim, as the policy terms were based on inaccurate information.

Unless something changes, it's likely these pressures will cause more organisations to look at alternative options.

5 Insurance Business Magazine (2021), *Cyber insurers raising premiums, reducing coverage limits – report*

SECTION 3:

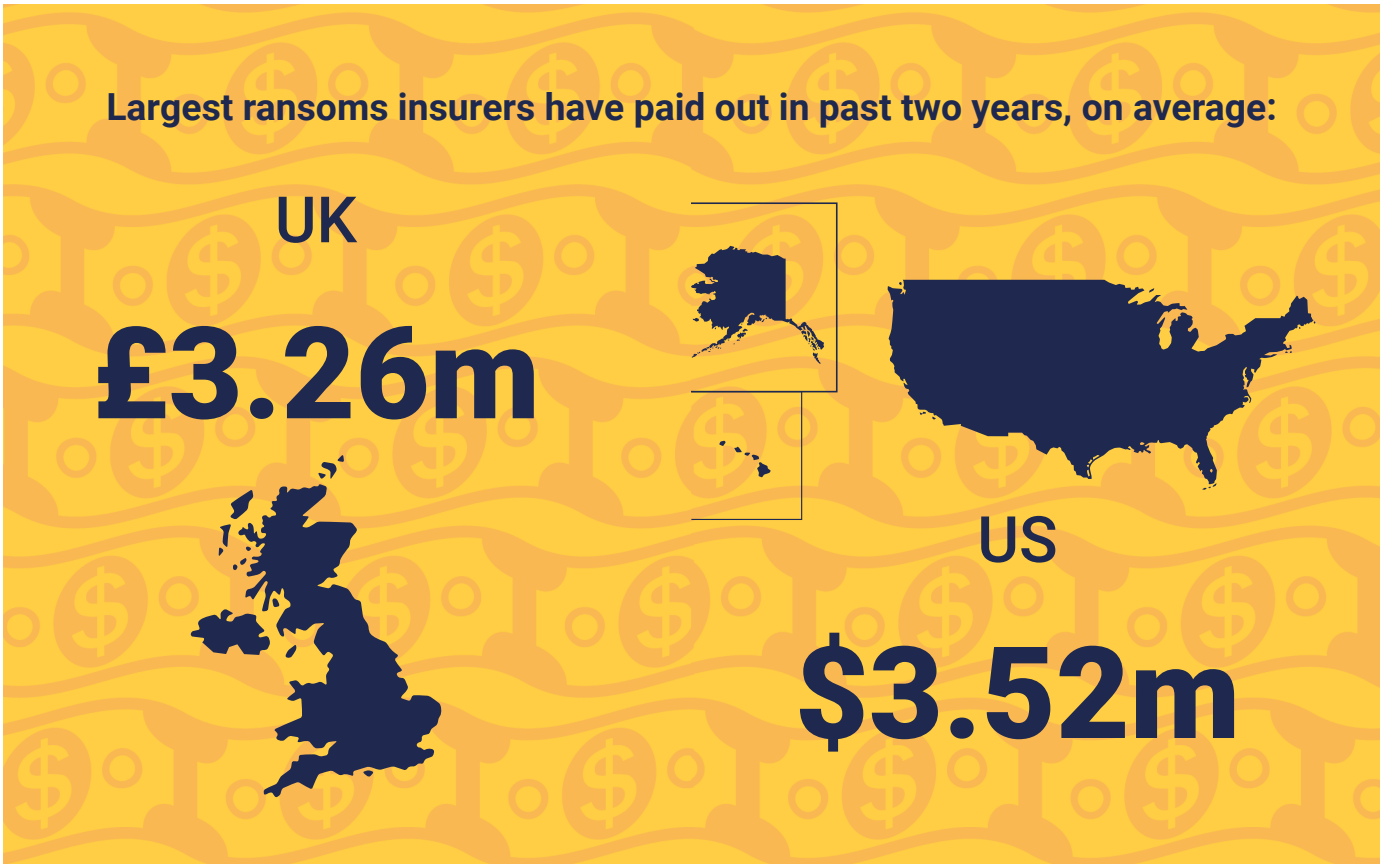
Rising premiums

Ransomware looms large over the cyber insurance industry. Attacks increased by **93%** in 2021, and already this year we've seen ransomware incidents impact Toyota and Puma, while the Costa Rican government was forced to **declare a state of emergency after its ministry of finance and healthcare system were targeted**[6].

In many instances, insurers are required to foot the bill. We asked what the largest ransom is they've had to pay out on in the past two years — the average was £3.26m in the UK compared to $3.52m in the US.

This has contributed to a **27%** increase in the cost of ransomware claims in the same time period.

As a result, insurers are declining to offer cover for ransomware attacks. Andreas Wuchner says this is especially common where brand reputation is a factor. "Brand value is often the trigger point for insurers to walk away," he explains. "Regardless of the maturity of an organisation and its security controls, the potential brand damage is simply too big and insurers refuse to cover it."



6 CM Alliance (2022), *5 Major Ransomware Attacks of 2022*

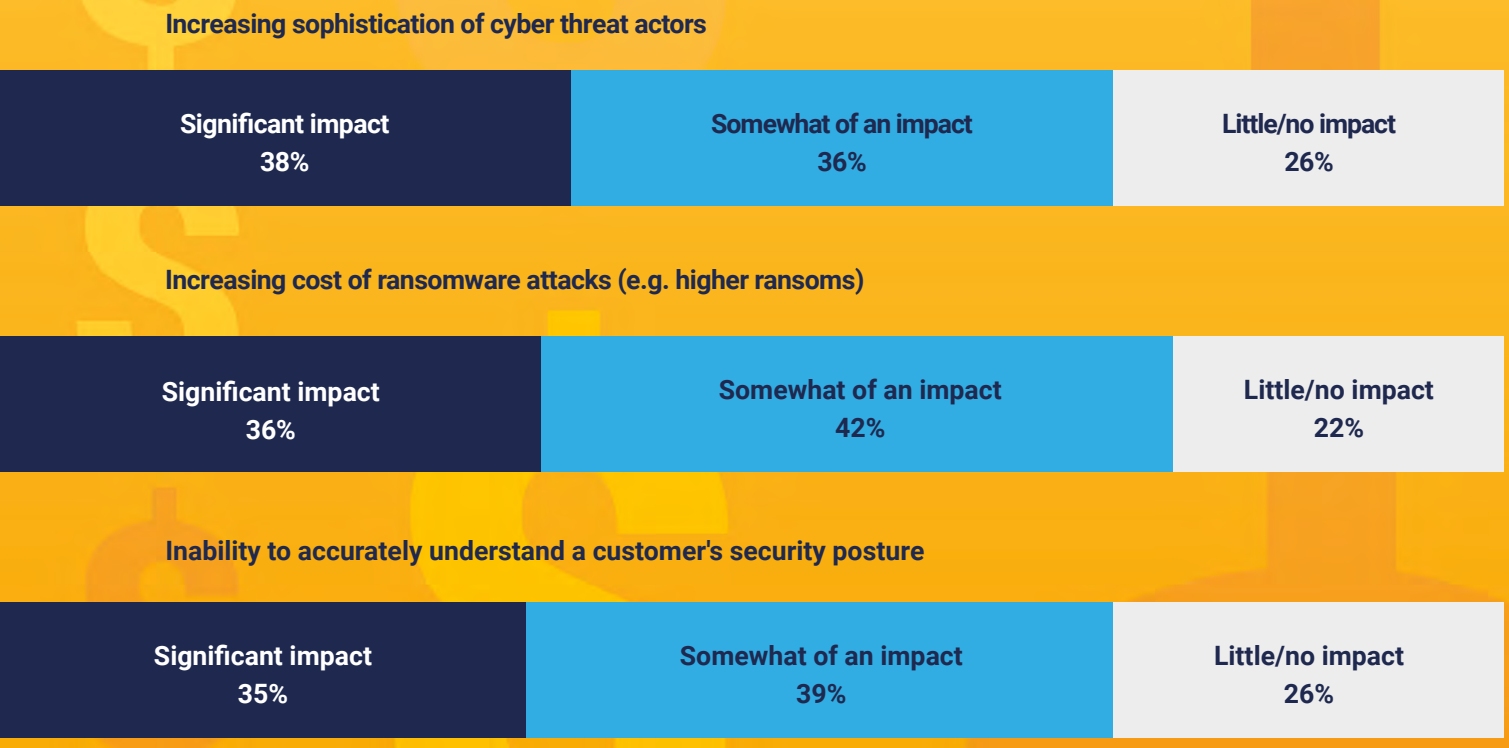
What's having the biggest impact?

The increasing cost of ransomware attacks is driven by the advanced tactics being deployed by criminal gangs. A report published by the Cybersecurity and Infrastructure Security Agency (CISA) noted an "increase in sophisticated, high-impact ransomware incidents **against critical infrastructure organizations globally**[7]."

Unsurprisingly, the increasing sophistication of threat actors and the rising cost of ransomware attacks are the factors identified as having the most significant impact on insurance premiums.

Revealingly, **35%** of respondents rated their inability to accurately understand a customer's security posture as having a big impact on rising premiums. This again highlights the challenges facing the industry in assessing cyber risk and the efficacy of security controls, and indicates that insurers aren't totally confident in their existing underwriting processes.

Which factors are having an impact on rising premiums?



7 Cybersecuirty & Infrastructure Security Agency (2022), *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*

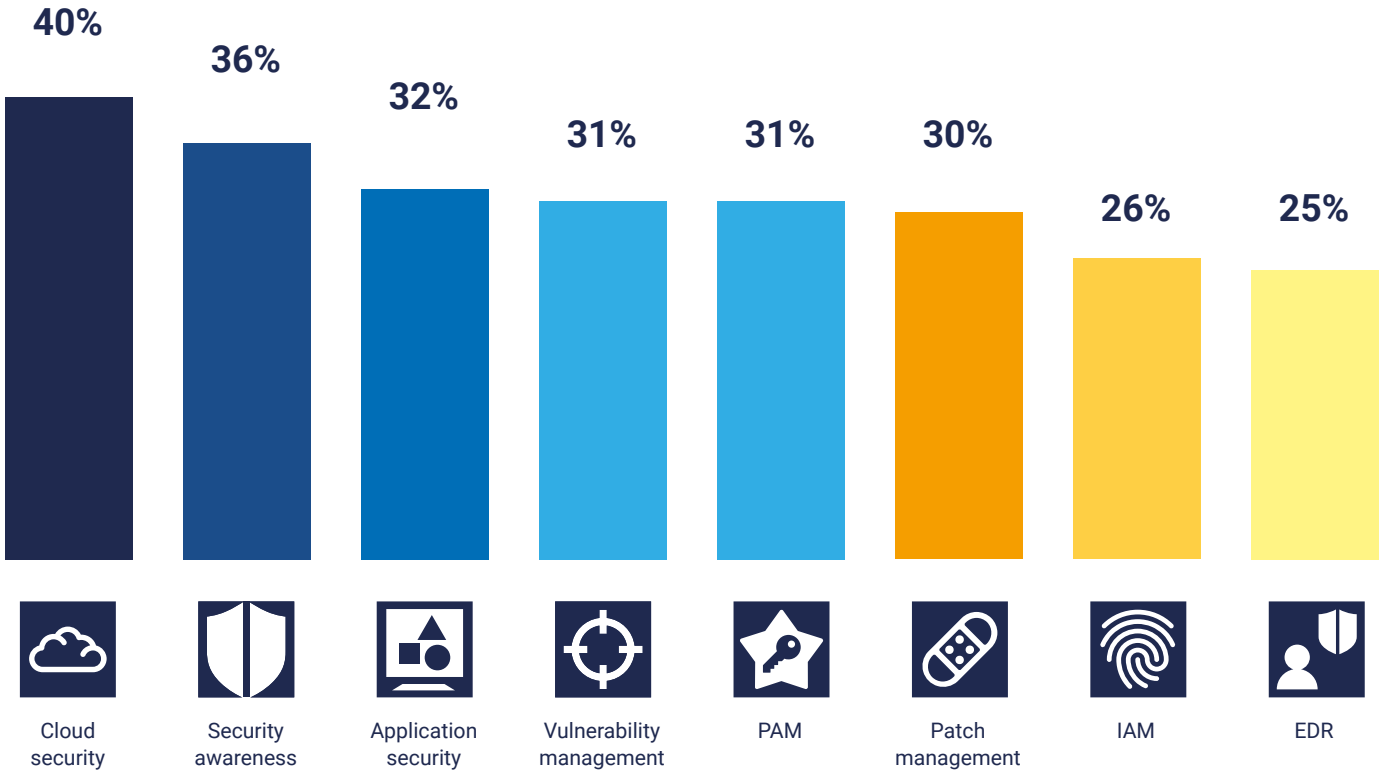
How do insurers assess cyber risk?

To get a better understanding of how insurers measure cyber risk, we asked respondents which security domains were most important when assessing security posture. The results reveal there is no standout priority area for insurers, with only **15%** separating all eight security domains included in the research.

"This shows there are no optional security measures," says Nik Whitfield. "Insurers expect organisations to have good cyber hygiene across a broad spectrum of security areas, both on-premise and cloud environments, with the evidence to prove it. That's why evidenced data and measurement automation is so important."

> **"There are no optional security measures. Insurers expect organisations to have good cyber hygiene across a broad spectrum of security areas, both on-premise and cloud environments, and with the evidence to prove it."**
>
> Nik Whitfield, founder of Panaseer

What are the most important factors when assessing security posture?



Cloud security's position at the top of the list, if only by a few percentage points, is likely a result of the continued move to hybrid environments. Separate research by Foundry shows that the proportion of companies with most or all of their IT infrastructure in the cloud is expected to increase from **41% to 63% in the next 18 months**[8].

According to Andreas Wuchner, this rapid shift is creating security problems through user error. "The security offerings at big cloud providers, like AWS and Azure, are very effective, but most organisations are not capable of using them or don't want to use them," he explains.

"You see people blindly thinking security is great and missing out on these things as they don't have the maturity to use these functions."

Security awareness was rated as the second most important factor when assessing security posture, which reflects the fact that **82% of breaches involve a human element**[9]. Nik Whitfield says this is an area of security that's particularly hard to measure and improve.

> **"Organisations often talk about embedding a security culture, but influencing a group of people to behave differently takes time."**
>
> Nik Whitfield, founder of Panaseer

"Organisations often talk about embedding a security culture, but influencing a group of people to behave differently takes time and an understanding of human behaviour. People will always want to click on things, so it's about making sure you have the right controls in place for when they do."

Ultimately, organisations need to demonstrate good security behaviours across their entire environment. Insurers have told us that they put almost equal weighting on all security domains, whether it's employee security awareness or patch management, so the pressure is on organisations to ensure they have accurate data that proves they're a low risk.

8 Foundry (2022), *Cloud Computing Study 2022*
9 Verzion (2022), *2022 Data Breach Investigations Report*

SECTION 4:

Where next for cyber insurance?

Despite the considerable pressures, our research shows it's not enough to make insurers exit the market. Even if the current rate of cyber-attacks remains the same, a vast majority (**84%**) of respondents said they'd continue to offer cyber insurance over the next three years. A separate report predicts that the global cyber insurance market will **grow from $11.9 billion in 2022 to $29.2 billion by 2027**[10].

87% of insurers believe it's important for the industry to develop a consistent approach to analysing a customer's cyber risk using accurate security metrics and measures.

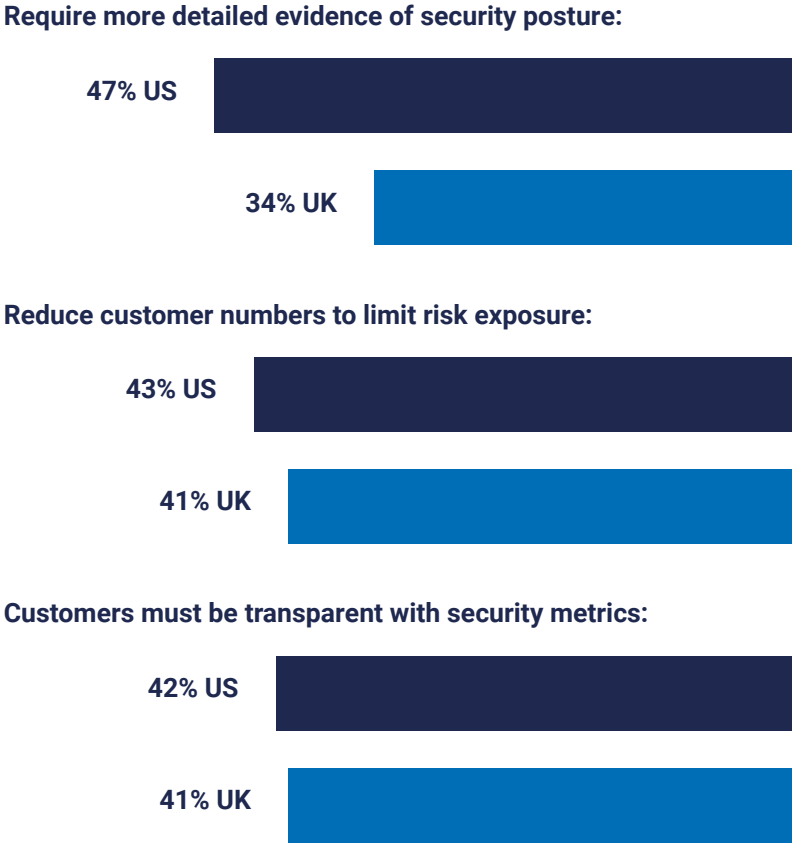
However, there's a clear appetite for transforming the way security posture is measured during the underwriting process. Nine out of 10 respondents (**87%**) believe it's important for the industry to develop a consistent approach to analysing a customer's cyber risk using accurate security metrics and measures. This rises to **95%** among US respondents.

Similarly, **89%** of insurers believe it would be valuable to have direct access to customer metrics and measures proving the status of their security controls.

David Fairman believes a move to greater transparency with security data is inevitable. "Market forces will make it happen," he explains. "You will see some insurers start to mandate a level of expectation about how much data is going to be shared with them, and how that's going to be continuously reviewed. They'll start to drive different standards and more consistency in measurement."

However, he also strikes a note of caution. "There'll be increased friction there, because most organisations don't want to share sensitive internal data with anyone, even third parties that have a right to audit."

How will your method of assessing risk change over the next two years?



10 Markets and Markets (2022), *Cybersecurity Insurance Market*

To encourage greater transparency, insurers will need to prove there is a clear value exchange. In a previous survey of 1,200 security leaders, we found that all respondents would be willing to demonstrate the strength of their cyber programme to cyber insurers, with data-driven metrics, if it meant they could **reduce their cyber insurance premium**[11].

"If the incentive is high enough and we can anonymise data enough, absolutely they will share," says Andreas Wuchner. "Everyone is under cost pressure, and the one who does it first and gets **15%-20%** cost reduction on their premium will be the trigger for everyone else to follow."

> **"The old way of doing cyber insurance is coming under pressure. The industry needs a more mature approach to oversight, otherwise premiums will just continue to increase."**
>
> Andreas Wuchner, security and risk expert

Ultimately, the cyber insurance market needs to develop a solution that works for both sides. Andreas believes this shift will be driven by new market players who use different methods of risk assessment, with less reliance on resource-intensive questionnaires. There is also a trend towards offering customers help with improving their security posture by giving them access to a marketplace of security tools and assessments.

This enables insurers to get a more accurate understanding of security posture and offer lower premiums.

"The old way of doing cyber insurance is coming under pressure," he explains. "The industry needs a more mature approach to oversight, otherwise premiums will just continue to increase. We need to shift towards decisions made on data and information rather than hopes and feelings."

If the industry can seize this opportunity for a data-driven approach to security and risk assessment, it can overcome many of the challenges it faces today and enable organisations to get the cover they need.

11 Panaseer (2022), *Cyber insurance crisis to fuel enterprise shift in cyber protection*

SECTION 5:

Prove you're a safe bet for cyber insurers

Many of the problems facing the cyber insurance industry come down to a fundamental problem with security data. Insurers are asking for more information to prove the status and efficacy of security controls, but organisations don't have an easy way to access it.

Where organisations can provide controls data, there are questions over whether it's accurate and up-to-date.

The answer lies in security automation using **Continuous Controls Monitoring**. It simplifies the application process, giving immediate access to accurate data on the metrics and measures required by cyber insurers, so you get the best possible cyber insurance pricing and coverage.

Our cyber insurance dashboard provides up-to-date evidence on key questions, such as:

- How many employees do you store or maintain data about?
- Are EDR solutions utilised across the organisation on all endpoint devices?
- Do you vulnerability scan, update and patch infrastructure systems on a regular basis?
- Do you provide regular employee awareness training on phishing and social engineering?

Simplify your insurance applications with Continuous Controls Monitoring

Panaseer's CCM platform combines all your security data, giving an independent, evidenced view of enterprise cybersecurity tools, controls, and personnel.

This improves visibility, measurement, and remediation, while enabling you to give insurers an accurate view of the efficacy of your security controls. It means all stakeholders can have more confidence in the information provided during the underwriting process and reduces the likelihood that you'll be refused a claim on the basis that you provided inaccurate data.

Panaseer's Cyber Insurance Dashboard

Connect with our team at **success@panaseer.com** to find out how we can help get cyber insurance coverage that's right for you.

Methodology

We surveyed 400 decision makers working in cyber insurance, with respondents split evenly between the US and UK. It was an online survey conducted by Censuswide between 25th May 2022 to 1st June 2022.

About Panaseer

Panaseer is the first Continuous Controls Monitoring (CCM) platform for enterprise security. The platform uniquely correlates data from all security tools to identify and measure missing assets and control gaps so that organisations can optimise security controls, tools, processes, and personnel.

CCM has become a required capability for regulated organisations as it solves one of the biggest challenges in cybersecurity today – control failure. This emerging technology has been recognised in Gartner's Hype Cycle for Risk Management in 2020, and featured in Momentum Cyber's Cybersecurity Almanac in 2021 as a next generation technology that will shape the future of cybersecurity. Panaseer has been included as an inaugural vendor in both. Panaseer customers include the world's largest institutions and enterprises.

We've got you covered

Continuous Controls Monitoring for enterprise security