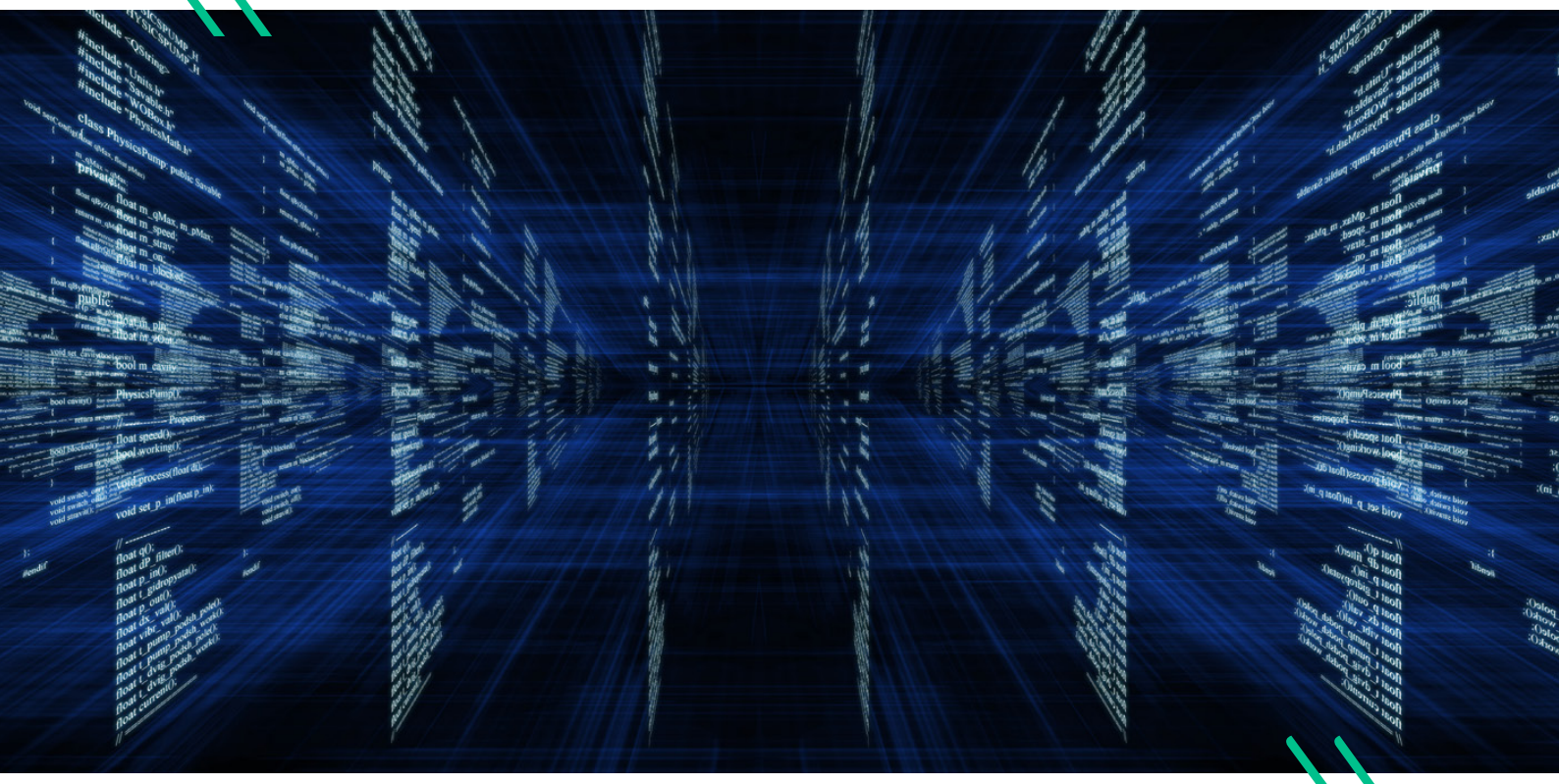
WHITEPAPER

# The future of cyber insurance: navigating risk with real-time data

## How to drive better underwriting, and reverse rising loss ratios

By Malcolm Wheatley, IT journalist and editor, and Matthew Hogg, Strategic Head of Cyber Underwriting at Liberty Specialty Markets



QUOD ORBIS

Liberty Specialty Markets

Cyber risk is growing, according to the world's largest cybersecurity benchmarking study, 2022. Material breaches rose 20.5% from 2020 to 2021— and over the next two years, security executives expect further increases in attacks as nation-states and cybercriminals become more prolific.†

Insurance premiums and business costs are rising too.

So,is there an answer?

†Source: ThoughtLab 2022 cybersecurity benchmarking study, 'Cybersecurity Solutions for a Riskier World'

# Cyber insurance: the state of the market

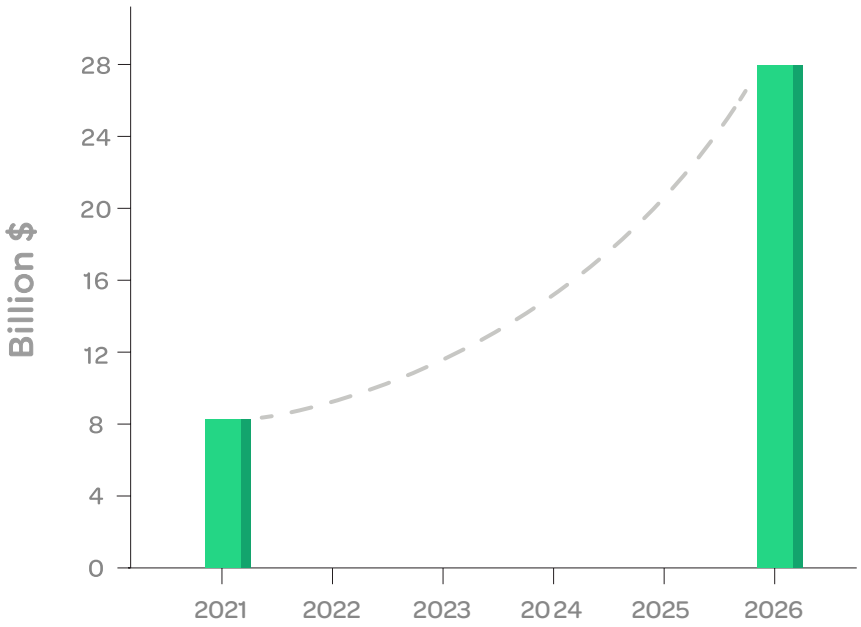
Cyber insurance is big business. Global cyber insurance premiums totalled $8bn US dollars (£6.07bn) in 2021*, and are growing rapidly: one estimate envisages a market size of $28bn US dollars (£21.27bn) by 2026.**

It's not difficult to see why. Businesses are hugely dependent on IT systems, and even small-scale interruptions can have significant costs in terms of recovery, lost revenues, customer service, and reputational damage. Cyber insurance offers financial protection, should IT systems be disrupted by events such as malicious attacks, accidental damage and administrative errors and mistakes.

Increasingly, security breaches are a source of loss and disruption. In particular, it's the threat of ransomware (see page 3) that is propelling cyber insurance sales and driving up insurance costs.

*Source: The Insurer. **Source: Statista.

## Forecast growth of global cyber insurance market




It is estimated that the global cyber insurance market will grow at a compound average of almost 25 percent per year from 2021 to 2026, to reach a total market size of almost 28 billion US dollars in 2026.

Source: Statista.

"Training employees how to recognise and defend against cyber-attacks (including phishing simulation programs to maximise the effectiveness of training) is the most under spent sector of the cybersecurity industry—and yet it holds out the greatest hope for combating ransomware attacks."

Source: Cybersecurity Ventures.

# The rise of ransomware

Ransomware attacks—in which malicious actors encrypt companies' data, providing the encryption key only when hacked companies have paid a ransom—are growing rapidly.

The average ransom paid following a ransomware attack is estimated to be around $1.9m US dollars (£1.44m)*, with ransoms rising year-on-year.

Ransomware cost the world around $20bn US dollars (£15.2bn)** in 2021—a figure that could well rise to around $265bn US dollars (£201bn) in 2031.**

*Source: Elliptic. **Source: Cybersecurity Ventures.

## Mounting costs

It's not just the price of the ransoms that contribute to that cost. A ransomware attack locks companies out of their IT systems, and prevents them from accessing their data. The impact on revenues and profitability is obvious, and so too is the expense associated with dealing with the aftermath of a ransomware attack. Again, the attraction of defraying these costs through cyber insurance is clear.

And let's not forget that cyber-criminals are becoming ever more sophisticated. Take the rise of 'double extortion ransomware', for example. Not content with just encrypting data, double extortion ransomware surreptitiously extracts the data first. Then, if the targeted company refuses to pay up they are hit with the threat of confidential and commercially sensitive data being leaked online or sold to the highest bidder. In such a scenario, backups and data recovery plans—and a ramping up of security after the event—are not enough.

A ransomware attack locks companies out of their IT systems, and prevents them from accessing their data

Insurers are insisting on ever-tighter standards and frameworks: NIST, PCI, ISO 27001, and the mandatory use of technologies

# Towards more sophisticated risk assessment

Undoubtedly for cyber insurance providers, this burgeoning demand poses a problem, as well as offering an opportunity.

For insurance companies, it's a relatively new class of business. Although a great deal of effort often goes into technical underwriting and R&D for this type of risk assessment, risk modelling in any real-time, dynamic sense is very much in its infancy. Data on which to inform decisions on coverage and premiums is therefore generally not as detailed and as current as it could be.

Generally, loss ratios have been rising with increasing premium rates and coverage restrictions contributing to this. Nevertheless, there seems to be an industry-wide acceptance that a better view and understanding of controls and processes related to cyber cover should be a focus for constant improvement. One particular focus area in the cyber insurance market in the past year has been the driving of multi-factor authentication adoption amongst clients, but more advances are needed.

## Higher premiums, tighter standards

Premiums are rising. Insurers are insisting on ever-tighter standards and frameworks: NIST, PCI, ISO 27001, and the mandatory use of technologies such as end-point detection and two-factor/multi-factor authentication. And insurers are also decreasing cover, including multiple policy exclusions and clauses—or simply refusing to offer cover at all for certain sectors and industries that are seen as particularly high risk.

It's clear to most cyber insurers that technology and real-time data will have a key role to play in driving better underwriting, reversing loss ratios and delivering an improved service to their insured customers. But how, and when?

### Problems for the cyber insurance industry, but also opportunity

# The risk of throttled demand

Higher premiums and tighter standards are understandable. Few underwriters and brokers have technical backgrounds: in the face of steeply rising claims and sharply increasing attacks, minimising risk as much as possible is deemed sensible, and rising premiums unavoidable.

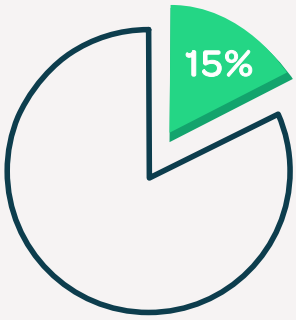
The problem for the cyber insurance industry is that such tactics serve to throttle demand or—at the very least—make customers unhappy, worried and, often, unsure of where they stand in respect to negligence or ignorance preventing a payout in the event of a claim.

## Is cyber insurance worth the cost?

Without doubt, say industry insiders, some organisations are asking themselves if cyber insurance is worth the cost, and worth the internal administration overhead in terms of hoops through which they must jump, and standards and frameworks to which they must adhere.

What's needed, in short, is a more sophisticated and visible approach to assessing risk, and a smarter—and less invasive—means of monitoring and assuring cyber security compliance.

> What's needed is a more sophisticated and visible approach to assessing risk and assuring cyber security compliance




Percentage of organisations with cyber insurance in the US, the world's most developed market for cyber insurance

# Market opportunity

For the cyber insurance industry, what's the prize if this more sophisticated approach to assessing risk, and smarter means of monitoring could be achieved?

More business, in short. More *profitable* business. And happier customers—happier to see more affordably-priced premiums, and happier to benefit from risk-mitigation approaches that genuinely link effort to reward, helping to reduce risk vulnerability.

## The prize for the cyber insurance industry


### Massive potential

The statistics speak for themselves. A single country—the United States—makes up three-quarters of the global cyber insurance market. And even in this most developed of marketplaces for cyber insurance products, only 15%* of organisations have cyber insurance coverage at all. And many of those organisations possessing cyber insurance cover do so because they have already experienced a disruptive breach of security.

The potential is evident. A recent survey of risk and audit executives by analyst firm Gartner Group, for instance, found cyber security control failures to be the number one top emerging risk.

*Source: The Value of Cyber Insurance to the UK Economy. Report prepared for the ABI, the Association of British Insurers.

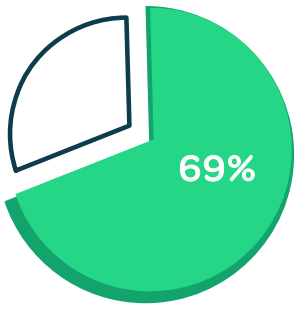
> Cyber security control failures are seen to be the number one emerging risk for businesses

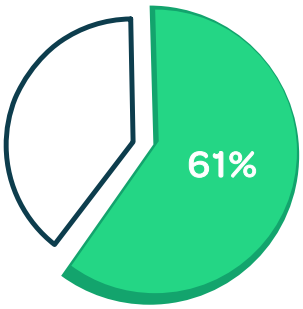
The corporate world needs better cyber security, and affordably-priced cyber insurance should find a ready market

# A market ready to invest

Financial services firms are particularly worried by the risk posed by malicious actors, especially those deploying ransomware. In PwC's 19th Annual Global CEO Survey, 69% of financial services' CEOs reported that they were either somewhat or extremely concerned about cyber threats. This compares with 61% of CEOs across all sectors.

**Percentage of financial services' CEOs somewhat or extremely concerned about cyber threats**




**Percentage of CEOs across all sectors somewhat or extremely concerned about cyber threats**

Source: PwC 19th Annual Global CEO Survey.

## Investment intentions are high

Moreover, the financial services industry has deep pockets, and—according to the PwC-CBI Financial Services Survey of December 2021—investment intentions in the area of information technology are high.

The message seems clear. The corporate world needs better cyber security, and—all things being equal—affordably-priced cyber insurance should find a ready market. Especially within industries and sectors where many cyber insurance providers presently decline coverage.

Once again, the finger points to the need for a more sophisticated approach to assessing risk, and a smarter—and less invasive—means of monitoring and assuring cyber security compliance.

> A rear-view mirror on risk, or a snapshot-in-time view—once a quarter, say—is pointless. Breaches and disruption can happen any time

# Real-time risk assessment and mitigation

What might that more sophisticated approach to assessing risk look like? And what might that smarter—and less invasive—means of monitoring and assuring cyber security compliance look like?

As a thought experiment, consider the requirements that such an approach should meet.

### ALL-EMBRACING

It should be extensive, for a start, covering all of an organisation's security controls—potentially hundreds of them—and every device, system, individual piece of network infrastructure, and server.

### CERTAIN

Is an end-point ransomware detection and response installed on absolutely 100% of assets? Answering such a question with 100% certainty can be problematic—but for both businesses and insurers, such certainty is important.

### AUTOMATIC

It should be automatic, rather than manual. People make mistakes, and are costly. Automatic systems are obviously to be preferred.

### OBJECTIVE

It should deliver hard, concrete, quantified data on cyber security—not subjective judgements or opinions.

### GANULAR

It should offer a more granular assessment than a simple 'yes or no, go or no-go' approach, and also be capable of prioritisation, and focus. Not all security controls are equal, and many are best interpreted with the aid of tolerance bands.

### CONTINUOUS

And it should be real-time, and continuous. A rear-view mirror, or a snapshot in time—once a quarter, say—is pointless. Breaches and disruption can happen any time.

> What if an insurer knew that they could see key evidence-based output from a client's Continuous Controls Monitoring system whenever they needed to?

# Introducing Continuous Controls Monitoring

The list of requirements for a more sophisticated approach to assessing risk, as presented on the previous page, is demanding for sure. But too demanding? No.

Insurance professionals have been doing something similar to assess risk for many years, albeit on a much smaller scale: the 'black box' telematics fitted to the vehicles of younger and riskier drivers, which provide continuous real-time monitoring of drivers' habits and driving styles. The benefits of 'black box insurance' are, of course, a two-way street: these riskier drivers pay lower premiums for driving safely and according to certain parameters, while insurers have a view of a set of controls on the car that provide vital data and reassurance.

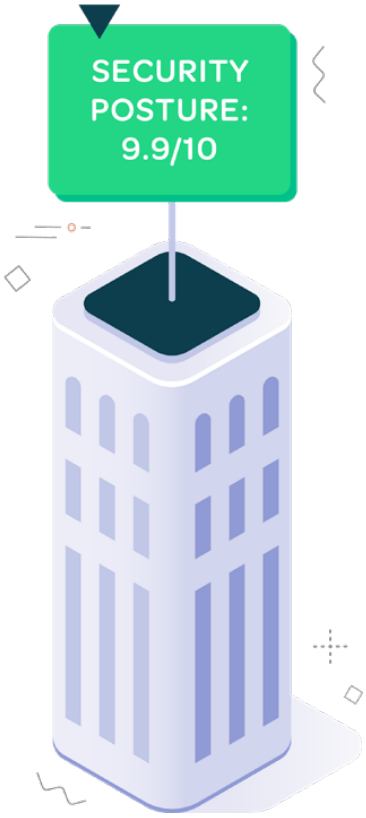
## Could the corporate world learn from 'black box insurance'?

Could something similar to young driver 'black box insurance' be developed for the world of cyber insurance? In some respects it already has, and it's called Continuous Controls Monitoring.

Continuous Controls Monitoring has been described as a paradigm shift in how IT security audits are carried out. Already in use within many larger organisations with cutting-edge IT departments, Continuous Controls Monitoring technology gathers—continuously, and in real-time—all the data and evidence required for an organisation to see and understand the state of its IT security, by continually monitoring all of the business's risk management systems and internal controls, via telemetry.

Of course, the direct connection of an insurer's systems to a client's corporate network and its Continuous Controls Monitoring system is unlikely to be feasible. After all, these client networks are much larger and more complex than the relatively simple black box in a young driver's car. And what is being monitored is considerably more complex than the times and style of driving.

But what if an insurer knew that they could see key evidence-based output from a client's Continuous Controls Monitoring system whenever they needed to? At the time of the client's initial insurance application, for example. At policy renewal time. At regular pre-agreed intervals, maybe? And what if the insurer had the opportunity to rewind and examine any of the historical output related to any claim event? Just think how that could improve the current situation in the cyber insurance sector for both the insurer and the insured.




# IT security data delivered automatically

Continuous Controls Monitoring is:

- IT security data that is factual and objective
- IT security data that is immediate
- IT security data that is drawn from right across the organisation's risk and vulnerability landscape
- IT security data that's delivered automatically.

If a part of the IT security apparatus isn't activated, or isn't operating within specified parameters, then Continuous Controls Monitoring finds it and reports it. In real-time. And the importance of this latter point can't be stressed enough: again and again, when data breaches occur, and hackers succeed, the root cause is often that controls have been de-activated, or warning signals ignored.

## A more robust and cost-effective approach

Continuous Controls Monitoring is also fast and efficient, and it's a far more robust approach to IT security than—say—costly and people-intensive questionnaire-based approaches, frameworks, or periodic audits. It can also deliver rapid ROI, so for the client organisation the system can pay for itself very quickly.

For cyber insurance providers, the appeal of a client with Continuous Controls Monitoring is obvious: here is a way to objectively—and accurately—assess cyber risk.

If the insured organisation has Continuous Controls Monitoring deployed, their security posture is a known quantity, updated in real time, and covering every asset, and every designated control. They feel the benefits—and so could their insurers, who should see risks reduced, and risk assessment become far more scientific.

Continuous Controls Monitoring could well be the missing link in the cyber insurance world. For organisations, and their insurers.

> The insured organisation feels the benefits—and so could their insurers, who should see risks reduced, and risk assessment become far more scientific

An insurer could have sight of specific output from its client's Continuous Controls Monitoring system at the time of the client's initial insurance application, at policy renewal time, and perhaps at pre-agreed intervals, to accurately determine and monitor the risk profile

# A Gartner-recognised security technology

Continuous Controls Monitoring is an advanced, Gartner recognised, security technology solution that delivers real time visibility into the status of security controls—organisation-wide, across every asset and designated control, and every system and item of network infrastructure.

## Huge benefits for insured organisations

Cyber risk, and digital risk in general, will not go away. On the contrary, the risks are likely to increase. Any organisation currently covered by, or considering, cyber insurance, would be well advised to assess Continuous Controls Monitoring as a matter of urgency.

The organisation should look carefully at their existing or proposed cyber insurance policy and clauses and the expectations of the insurer. Then they should consider the benefits that would flow—and not just in terms of insurance cover—from having an automatic, evidence-based way to continuously monitor their digital processes, platforms, tools and products and to ensure the necessary compliance.

## Increased insurer confidence

Consider also the confidence level that Continuous Controls Monitoring will give the insurer and, with that, the likelihood of lower premiums and enhanced cover for its clients.

As stated earlier, the insurer could have sight of specific output from its client's Continuous Controls Monitoring system at the time of the client's initial insurance application, at policy renewal time, and perhaps at pre-agreed intervals, to accurately determine and monitor the risk profile. Should a claim need to be made, the insurer could also be able to examine month on month snapshots of technology and controls performance within the client organisation, or even precise moments in time prior to any breach.

The insurer could also get a detailed picture of coverage—exactly where the client has EDR (Endpoint Detection and Response) installed, for example, and what assets from across the organisation are included. Also, where antivirus, encryption, mobile device management and protection, patches et al are installed.

## Visible, evidence-based proof

Continuous Controls Monitoring can provide all of this. And under agreed, mutually beneficial policy terms, the insurer could be allowed approved access to what is necessary to provide enhanced and more cost-effective cyber insurance cover.

Finally, consider the fact that Continuous Controls Monitoring is an evidence-based system that provides visible proof of the safeguards an organisation has in place to protect its assets and alignment to applicable risk and security frameworks. For the insured organisation, this should ensure that any claims do not become unnecessarily complex and protracted.

## Want to find out more about Continuous Controls Monitoring?

Visit www.quodorbis.com, call Quod Orbis on 020 3962 2206 or email contact@quodorbis.com

## Get insights direct to your inbox

Register for updates at www.quodorbis.com/news-blog

## About Quod Orbis

Quod Orbis is at the forefront of delivering cyber security and Continuous Controls Monitoring-based solutions that demonstrably help to reduce business risk. Quod Orbis clients include large corporations, government, household name brands, as well as many medium size organisations, and operate across sectors such as financial services, banking, aerospace, retail and health.

## About Liberty Specialty Markets cyber insurance

Liberty Specialty Markets' cyber insurance product 'Cyber Suite' provides coverage tailored to the challenges a business may face due its dependence on IT networks, third party IT and business processing providers, as well as the digital assets and data they keep. LSM's experienced underwriters can provide your business with the protection it needs against a range of losses, including losses arising from cyber extortion, reputational harm and property damage.

---

Quod Orbis Limited
2nd & 3rd Floor
2 Burgon Street
City Of London
London
EC4V 5DR
United Kingdom

T +44 (0)20 3962 2206
www.quodorbis.com

Liberty Specialty Markets
20 Fenchurch Street
London
EC3M 3AW
United Kingdom

T +44 (0)20 3758 0000
www.libertyspecialtymarkets.com