



REINSURANCE

THE ART AND SCIENCE OF CYBER RISK SCORING TECHNOLOGIES

LOCKTON RE EVALUATES EMERGING CYBER RISK SCORING TECHNOLOGIES AND THEIR (RE)INSURANCE USE CASES IN OUR LATEST REPORT.

Lockton Re's reports, market commentary and insights focus on key topics, occurrences or changes in the (re)insurance and broking market place which impact our clients and partners. In order to help guide relevance for the reader we categorise this content in four areas – Exposures, Perils, Risk Transfer and Placement. Lockton Re looks forward to working on behalf of our clients to deliver new insights and innovative products designed to address the multifaceted cyber risk environment.

About Lockton Re (locktonre.com)

Lockton Re, the global reinsurance business of Lockton Companies, helps businesses understand, mitigate, and capitalise on risk. With over 400 colleagues in 19 locations globally, the business is continuing to grow, pushing the reinsurance industry forward with smarter solutions that leverage new technologies—delivered by people empowered to do what's right for clients.

Executive Summary

This paper provides an overview of a selection of external vulnerability scanning technologies used by cyber risk (re)insurers. In our report, we examine key features of their insurance use cases and implications.

For (re)insurers, cyber risk data from third parties is a useful addition to the toolset. In order to study some of the tools available, we obtained risk data from four scanning companies. Using a standardised data set we then conducted an assessment of their different approaches and outputs, to understand the variations in this technology. For the purposes of this paper, we have anonymised the scanning vendors in the results.

Providers offer a mixture of firmographic data, technographic data, as well as risk metrics. Firmographic data provided by the vendors can be used to enhance exposure data, and to aid in sensitivity testing cyber catastrophe modelling outputs.

Technographic data can be utilised to help understand exposures to potential accumulations, and to assist in deriving custom scenarios for portfolio modelling. Best practices in exposure management encourage the consideration of more than one view of risk. Furthermore, in a fast-changing technological landscape with shifting accumulations, an annual snapshot of risk may no longer be considered sufficient to monitor risk.

Most (re)insurers are looking to optimise diversification in their portfolio as they grow. It's clear that limiting potential systemic aggregations in a portfolio is one way to promote diversification.

The development of this specialist technology illustrates the pace of innovation taking place in the cyber insurance industry. There is still a wide range of techniques deployed, as well as outcomes delivered, and users should be aware of the limitations of these tools. When used in conjunction with other underwriting and aggregation methodologies, scanning solutions can provide valuable additional insights.



Introduction

The increased complexity of digital networks simultaneously raises both the potential for growth and exposure to risk for companies. By 2025, it is estimated that 50% of the world's data will be stored in the cloud¹. The potential attack surface increases each year for companies both internally and through their downstream suppliers, including indirect reliance on services or technologies used by third parties.

Cybersecurity Ventures have predicted that the annual cost of cybercrime will hit \$10.5 trillion annually by 2025, up from \$3 trillion in 2015². Supply chain risks are increasing, and their consequences are still not well understood or modelled. A 2024 UK

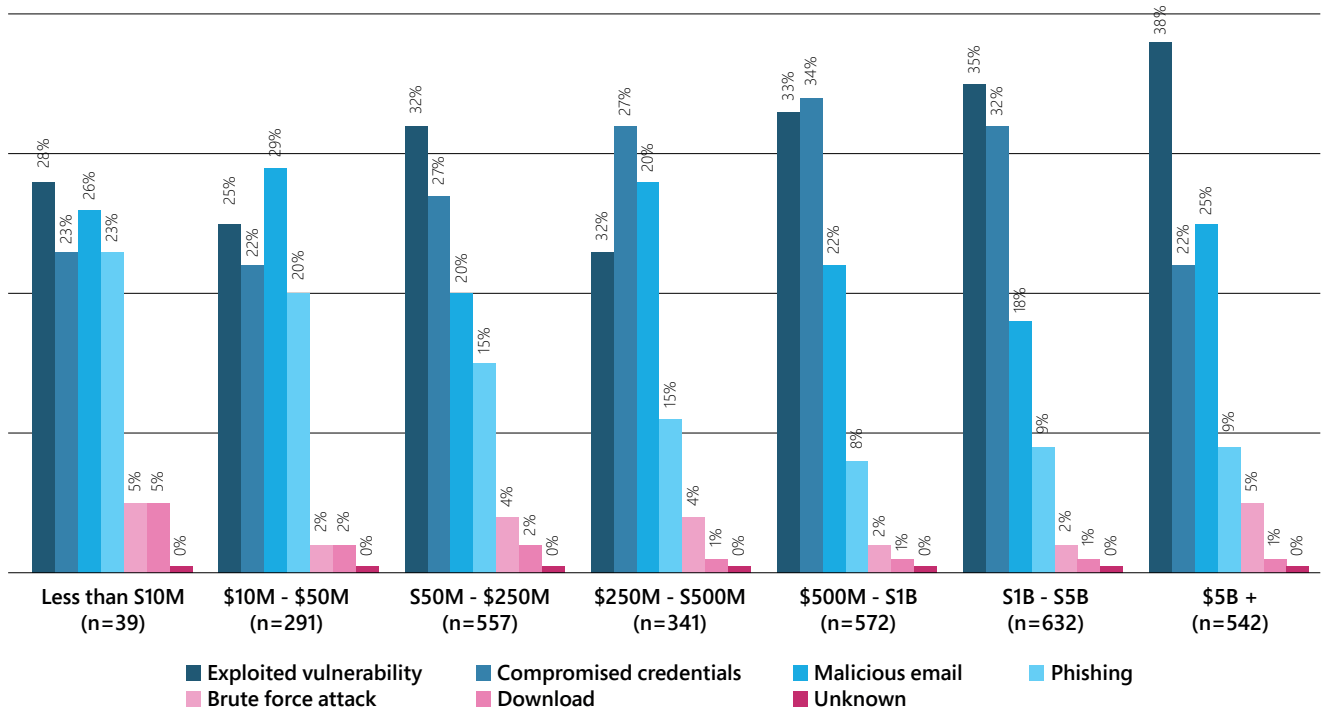
government survey found that only around one in ten businesses say that they review the risks posed by their immediate suppliers (11%), and that close to one in twenty are looking at their wider supply chain (6%)³.

There are numerous and varied economic and business consequences from cyber incidents including the impact on resources, reputation, and from regulators. There can also be knock-on effects due to the interruption and distraction of dealing with a cyber incident. As the cyber insurance industry has grown, it has borne an increasing burden of insured losses.

Data breaches and ransomware have been a driver of insured losses. The average cost of a breach to a US business is nearly \$10m, and the largest publicly known ransomware payout made to date (\$75 million) was made to the ransomware gang Dark Angels.⁴

The Sophos paper "The State of Ransomware 2024"⁵ illustrates the root cause of ransomware attacks by company size (see figure 1). It shows that exploited vulnerabilities are the leading cause of attacks across companies of almost every size.

Figure 1: State of Ransomware Report 2024, Sophos



^{1&2} Steve Morgan 2023. "Boardroom Cybersecurity Report 2023" Secureworks blog December 13, 2023. <https://www.secureworks.com/centers/boardroom-cybersecurity-report-2023>

³ Cyber security breaches survey 2024. (2024b, April 8). GOV.UK. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024>

⁴ ThreatLabz. (2024). ThreatLabz 2024 ransomware Report [Report]. Zscaler, Inc. <https://www.zscaler.com/resources/industry-reports/threatlabz-ransomware-report.pdf>

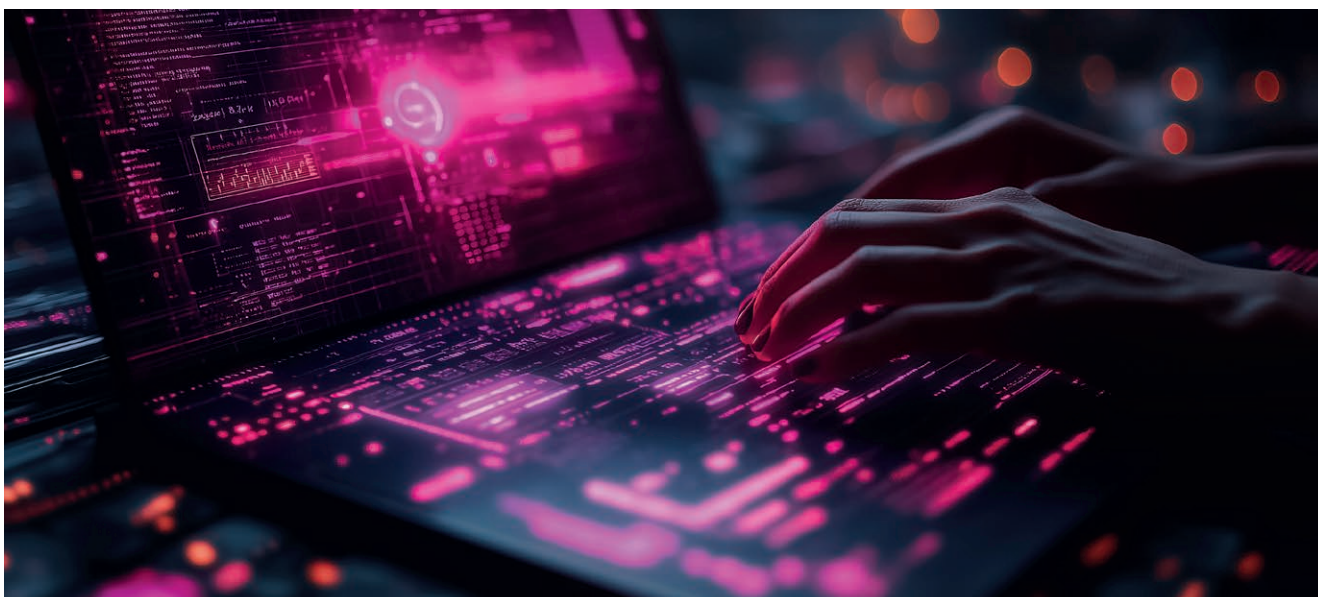
⁵ Sophos (2024). The State of Ransomware 2024 <https://www.sophos.com/en-us/content/state-of-ransomware>

According to the Sophos Report,⁶ organisations with an exploited unpatched vulnerability as the root cause of an attack report considerably more severe outcomes than those where the attack started with compromised credentials, including a higher propensity to:

- have backups compromised (75% success rate vs. 54% for compromised credentials)
- have data encrypted (67% encryption rate vs. 43% for compromised credentials)
- pay the ransom (71% payment rate vs. 45% for compromised credentials)
- cover the full cost of the ransom in-house (31% funded the full ransom in-house vs. 2% for compromised credentials)

Companies with unpatched vulnerabilities also reported four times higher overall attack recovery costs (\$3M vs. \$750K for compromised credentials), and slower recovery times (45% took more than a month vs. 37% for compromised credentials).

The CVE list⁷ is a list of publicly known vulnerabilities maintained by the MITRE Corporation and supported by US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Coalition's Cyber Threat Index 2024⁸ predicts a 25% increase in the rate of discovery of CVEs, compared to the first 10 months of 2023. The report discovered that scans looking for exploitable technologies, like Remote Desktop protocol, increased by 59%.



⁶ Sophos (2024). The State of Ransomware 2024 <https://www.sophos.com/en-us/content/state-of-ransomware>

⁷ CVE – Search CVE list. (n.d.). https://cve.mitre.org/cve/search_cve_list.html

⁸ Coalition Security Labs. (2024). Cyber Threat Index 2024. In Coalition Security Labs. https://info.coalitioninc.com/rs/566-KWJ-784/images/Coalition_Cber-Threat-Index_2024.pdf?version=0

Vulnerability Scanners

One solution in an underwriter's toolkit to mitigate some of the exposure to incident root causes is a vulnerability scanner. Risk Optics defines a vulnerability scanner as "an automated vulnerability assessment tool that searches for, discovers, and reports on potential vulnerabilities in your organisation's IT infrastructure. You can then address these weaknesses before they lead to operational disruptions, downtime, security breaches, ransomware attacks, zero-day exploits, and other cyber events".⁹

Broadly speaking, there are two main types of vulnerability scanning tools available: external (also known as outside-in) and internal (also known as inside-out). Risk Optics defines these as follows:

"An internal vulnerability scan operates within internal network firewalls to identify at-risk systems and potential vulnerabilities inside the network.

In contrast, an external scan is performed outside your network. Like external penetration testing, external scanning can detect open ports and protocols. An external scan also looks at specific IP addresses to identify open, exploitable vulnerabilities that jeopardize network security."

External vulnerability scanners can highlight potential concerns such as open ports, out of date Secure Socket Layer (SSL) certificates, remote desktop protocol (RDP) access, unpatched versions of software, patching cadence, exposure to CVEs, etc. When software is misconfigured or exposed to the public internet, it can signal insufficient security controls or unprotected infrastructure.

External scanning can also be used to help assess the hygiene of a company's third-party and extended indirect technology providers. Supply chain attacks have been a key source of cyber incidents over the past few years, including notable attacks against Kaseya¹⁰ and SolarWinds.¹¹

A recent report found that 97% of the top 100 companies in the UK had suffered a breach in their third-party or fourth party eco-system.¹²

Scanning tools use a combination of cyber risk and contextual factors. For example, they may combine technological data derived from scans with threat intelligence data on attacks in a particular region or industry.

⁹ Risk Optics November 17, 2021. Blog. Internal vs. External Vulnerability Scan: What Are the Differences? — ZenGRC (reciprocity.com)

¹⁰ Paganini, Pierluigi. 2023. "Kaseya Ransomware Attack Here's What you need to Know" Cyber News. December 07, 2023. <https://cybernews.com/security/kaseya-ransomware-attack-heres-what-you-need-to-know/>

¹¹ Kerner, S. O. S. M. (2023, November 3). SolarWinds hack explained: Everything you need to know. WhatIs. <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>

¹² The United Kingdom Top 100 companies: Cybersecurity threat report – SecurityScoreCard. (2024, June 28). SecurityScorecard. <https://securityscorecard.com/research/the-united-kingdom-top-100-companies-cybersecurity-threat-report/>



External vulnerability scanners typically have at least two of the following steps:

1. **Collate assets – IP addresses, domains, etc**
2. **Collate signals / data findings**
3. **Calculate a risk score based on findings**

The minimum requirement to run a scan is typically a web address / URL (or DUNS number). However, some scans may also require additional data such as revenue, if they are also modelling insured losses. Most scans require some additional curation to ensure the correct data is being looked at. Indeed, only one of our sample scanning companies stated that they automatically verify all data without any manual intervention.

External scans will not provide a complete picture of risk. For example, a multi-factor authentication policy may reduce the risk from exposed credentials on the dark web – but would not appear in scanned results. Some scanning companies provide questionnaires to capture this additional information, adjusting scores to account for it. It may be possible to see scores pre-and post-questionnaire, to determine the impact of these factors on the score.

Scans return multiple items to be addressed. These should be considered in conjunction with internal company knowledge, to ensure that resources for addressing these issues are prioritised correctly. External vulnerability scans may pick up old IP addresses or assess machines that are segregated from the network, and additional context may be needed to filter false positives out.

Vulnerabilities need to be interpreted with care. Not all vulnerabilities are equal, and only some have exploits in the wild. News headlines may overstate the potential impact of a vulnerability, which will often require other factors to occur simultaneously for a company to be vulnerable.

No Silver Bullet

Scans are not a silver bullet for the cyber security question, but rather part of a larger set of measures that can be combined to show the overall security posture of a company. They can be very useful to identify immediate areas that need to be examined further, and for measuring trends in security over time, e.g. to show an improvement in security due to security spend.


From an insurance point of view, the use of vulnerability scans to address cyber security issues can be viewed at both the micro individual company level, and the macro portfolio level. At the micro level, vulnerability scanners can identify potential issues at individual insureds, highlighting concerns to help strengthen their security posture, such as open ports known to be exploited by threat actors.

The availability of this data allows companies to chart their progress over time, and to address the relevant issues in order to improve their cyber hygiene and reduce risk. Companies can increase their resilience and mitigate threats by using scans, increasing their attractiveness to insurers. The utilisation of scanners has positive implications for the cyber insurance industry when the results are actioned to improve security posture.

At the macro level, these technologies allow (re)insurers to identify potential widespread vulnerabilities across many risks, and to use this to optimise their portfolio. Rapid 7 defines a widespread threat as “when a vulnerability is exploited to compromise many organizations across many verticals and geolocations”.¹³

The data captured by external scanners can be used to identify common operating systems, technologies and dependencies which could lead to risk accumulations within a portfolio. Identifying vulnerabilities across a portfolio aids diversification strategies, enabling risks to be written more knowledgeably, and (re)insurers to grow their book more confidently.

As the cyber (re)insurance market continues to develop, portfolio optimisation and utilising more than one view of potential systemic risk become increasingly important.



The data captured by external scanners can be used to identify common operating systems, technologies and dependencies which could lead to risk accumulations within a portfolio.

¹³ 2024 Attack Intelligence Report – Toolkit | Rapid7. (n.d.). Rapid7. <https://www.rapid7.com/research/reports/2024-attack-intelligence-report-toolkit/>

Study Methodology

A diversified data set of 221 companies who purchase cyber insurance was compiled from cleaned data provided by Lockton Re. The companies were domiciled in the US and the UK, and split between six industries: Education, Financial, Retail, Healthcare, Manufacturing, and Professional Services. The companies varied in size between micro (smaller than \$10Mn in revenue) and very large (over \$2Bn in revenue).

Four cyber risk data providers processed the companies and provided results. The four companies who took part in our study, in alphabetical order, were: Cyberwrite, ISS-Corporate, KYND, Orpheus. For the purposes of this report, we have anonymised the outputs.

Some of the vendors focus on technology exposure, while others provide modelled insurance losses to complement technology risks.

All four companies provide outside-in scanning, which may also be combined with other data such as threat intelligence, dark web data, and third-party data such as endpoint compromise detection data. All four of the vendors bring different strengths and capabilities in their software, and figure 2 below shows a high-level overview of some of the main features available.

Figure 2: Vendor capabilities comparison

	Vendor A	Vendor B	Vendor C	Vendor D
Technographic data	✓	✓	✓	✓
Risk score	✓		✓	✓
Portfolio metrics	✓	✓	✓	✓
Track CVEs	✓	✓		✓
Loss Estimates	✓	✓ Scenarios	✓	

The data has also been modelled in established third party cyber catastrophe models, to measure the impact on losses due to changes in the underlying data.

The results provided are anonymised with the scanning companies referred to as Vendors A to D, and cyber catastrophe modellers referred to as Models A and B.

Company Matching

Vulnerability scanners have varying methods of matching company data. Some companies scan all traffic on the web and then attempt to match the company name with the company names assigned in their existing data. Other companies may add companies to the data they scan as required.

Some scanners may be better matching larger companies than micro companies, and some scanners may be better matching companies in the US than elsewhere. Our sample provided no distinction between vendors in this regard.



Scores

The signals captured by vulnerability scanners can be weighted and combined to provide a relative, normalised score. The score may be related to the probability of a breach at a company or may reflect the risk assigned to the findings. One company does not provide a numeric score, but the individual signals are instead rated red, amber, or green to aid prioritisation by the underwriter.

Scores are generated from data findings collected from digital assets identified as being either owned or operated by the company, or by the company's subsidiaries.

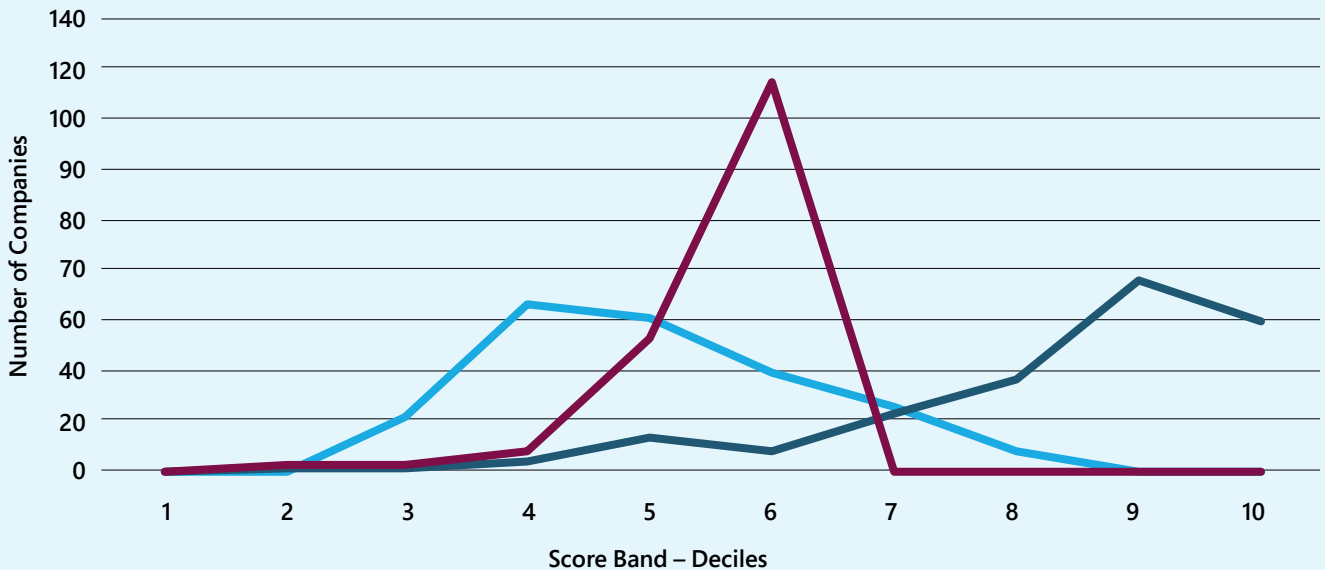
Every scanning vendor has their own scoring methodology, range of scores, and interpretation of what the scores mean (see figure 3). For example, some companies link their scores to breach probabilities. That means a company with a score of 200 might be half as likely to have a breach as a company with a score of 100. For some companies, a high score correlates to high risk, and for others a high score correlates to lower risk.

Figure 3: Scoring methodology

	Vendor A	Vendor B	Vendor C	Vendor D
Score represents	Probability of an incident for the next 12 months.	Risk rating for company.	Probability of an incident for the next 12 months.	Cyber Risk Rating.
Ratio to odds	A score of 34 means 66% of companies are better off from a cyber risk perspective, and 34% of companies are worse off.	Severe vulnerabilities discovered are 3x more likely to lead to a loss.	The score doubles, or halves, every 100 points, so 700 is twice the risk of 800.	Very High-Risk companies 4x more likely to claim on cyber insurance policy than Low Risk companies.
Adjustments	Adjusted for exposure, e.g. normalised by number of employees.		Adjusted by sector and employee count.	Adjusted for sector, countries, size.
Industry benchmarking	✓	✓	✓	✓
Scores updated	On Demand	Continuously	Weekly	Weekly / On-demand

The scoring methodology also impacts the distribution of scores – some vendors returned a large range of scores for the sample set, and others returned scores that are more clustered. Figure 4 below shows the score distributions for our test data; the methodology of the scoring system may explain some of the shapes below.

Figure 4: Score Distribution



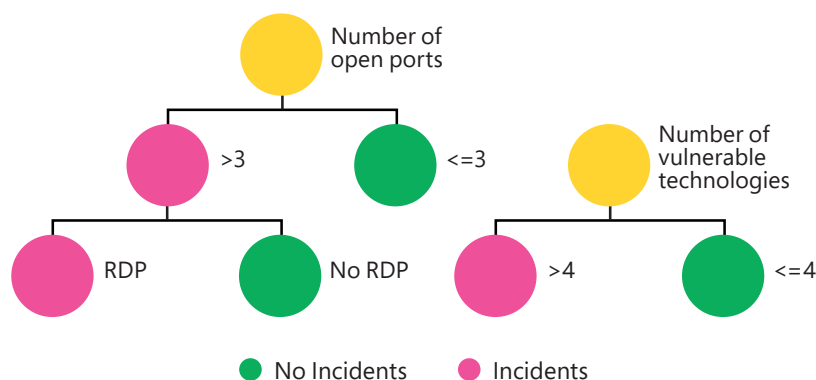
Most companies use machine learning to generate scores. The most typical machine learning application for scoring identifies the data points that are most important, and then weighs the data points to calculate the score.

A training set of data is compiled containing (signal) data for companies along with their (public) breach history. The machine learning models iterate over the training data to compare differing combinations of data points, to see which are predictive of an incident.

The data points that are identified as predictive of cyber incidents become the “classifiers” in the model and are weighted by importance. A hypothetical example of classifications derived from training data is shown in figure 5. In this example, the number of open ports, RDP presence and the number of vulnerable technologies, are all potential classifiers in the model.

For example, in the fictitious example, companies with more than three open ports and using RDP saw incidents, whereas companies with fewer than three open ports had not seen incidents. Companies with four or more vulnerable technologies saw incidents, whereas companies with fewer incidents did not. In this example number of ports, RDP use and number of vulnerable technologies would apply as classifiers in the model.

Figure 5: Classifier example of RDP presence



Care needs to be taken to ensure that classifiers are only included if they are the cause of loss and not merely correlated with the cause.

The greater the number of times a classifier appears in a group of predictive classifications, the greater its weight. Classifiers and their weights may be assessed separately for each cyber insurance coverage, e.g. data loss or ransomware payment.

Care needs to be taken to ensure that classifiers are only included if they are the cause of loss and not merely correlated with the cause. For example, newer companies may have fewer legacy systems, newer and more secure technologies and their lower profile can make them less of a target. So, date of incorporation for the company may be correlated with loss but wouldn't be the cause of loss.

Scores may also incorporate the CVSS (Common Vulnerability Scoring System) score, or other measures of severity or exploitability, to ensure the most potentially dangerous vulnerabilities have the highest weight.

One vendor has their own proprietary scoring system. This builds in not only the score, but also whether exploitation of the CVE is likely to be widespread or limited, as well as the dynamic likelihood of future exploitation.

Scores may also incorporate other factors, such as exposure weighting or threat intelligence. For example, some vendors may adjust a score based on industry, or based on the ratio of leaked employee credentials to total staff headcount.

The scores have been validated by the vendors against a combination of publicly available information and claims data. Figure 6 below highlights some of the differences in the methodologies behind the scores. The detail behind some of the nuances in these decisions is beyond the scope of this paper.

Figure 6: Variation in scoring methodologies

	Vendor A	Vendor B	Vendor C	Vendor D
Rating Mechanism	Score	Insurer-customisable criteria	Score	Score
CVE / CVSS Impact	✓	✓		✓
Dark web exposed credentials	✓			✓
Threat intel	✓			✓
Machine Learning	✓		✓	✓
Number of ML classifiers in score	Hundreds	N/A	25	22
Score varies by industry?	✓	Depends on UW rules	✓	✓

Score Weighting

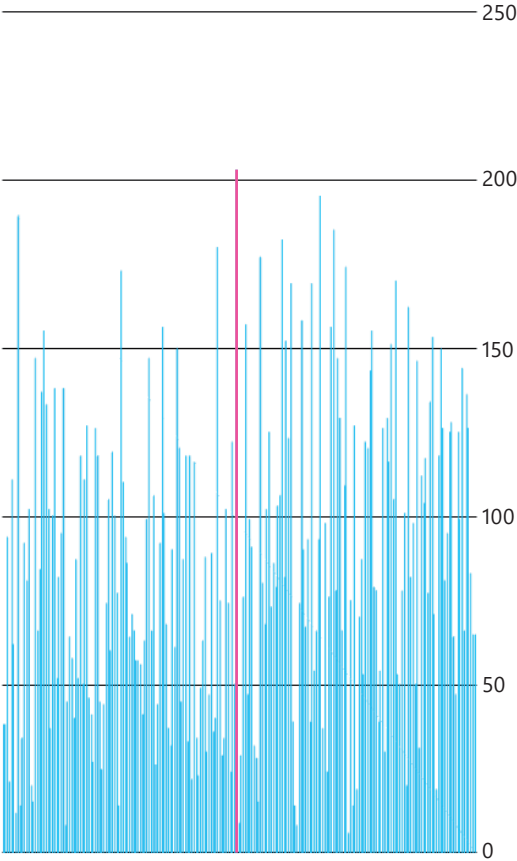
The correlation between cyber signals and cyber incidents / insurance claims is the holy grail of the cyber insurance analytics industry. There is no definitive work yet to determine the importance of signals for determining loss. That is, it is not currently possible to show for each Control X, a definite change in loss of Y.

Since signals may be correlated among themselves, there may be some double counting within them. For example, multiple open ports and unpatched versions of software, are likely to be correlated with the cyber security hygiene practices within an insured. This double counting is typically accounted for within the machine learning methodologies.

The difference in scoring methodologies, and signal data collected, leads to differences in how vendors score the same companies. There is a wide variation between vendors on their view of the scores for different companies. Figure 7 shows the difference between the minimum and maximum relative rank of the scores for each vendor in the sample portfolio of 221 companies.

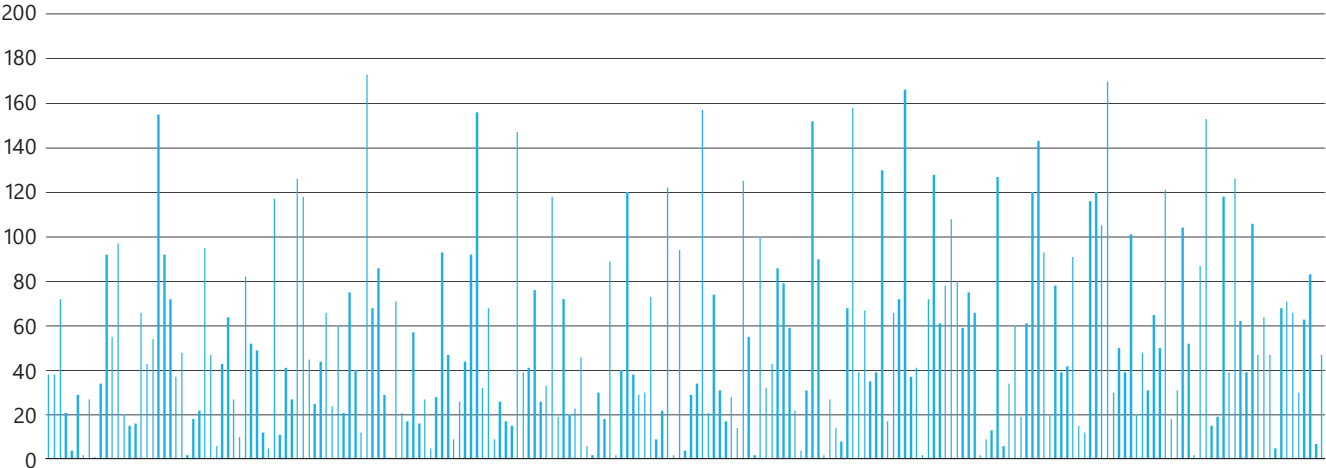
The line in pink represents the most extreme difference in ranking between vendors. The measured company was ranked 2nd, 96th and 205th out of 221 companies by the three companies providing scores, leading to a difference in rank of 203. The company is in retail and suffered two different ransomware attacks in 2023, and multiple credential breaches in 2022 and prior. These may impact on how the company is treated by some scoring methodologies.

Figure 7: Difference in Ranks by Company



To test whether or not there was a specific vendor driving this variation, the ranks were also compared solely between the two vendors with the closest technographic matches (see figure 8). There is still variation between scores assigned, due to the interpretation of threat intelligence and other factors beyond just the technographic signal.

Figure 8: Difference in Rank between Two Closest Vendors

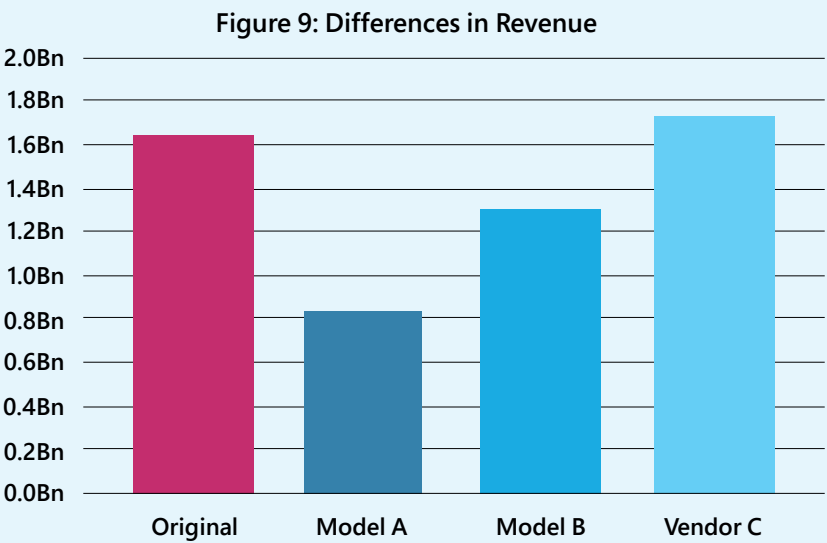


Firmographic Data

Firmographic data refers to demographic information about a company or organisation. It includes characteristics such as industry, company size, location, revenue, and number of employees.¹⁴ This information is a key driver of loss in catastrophe models and some scanners can provide an alternative source of this data. Two vendors provided industry data and one provided revenue data.

Updating the original data with additional firmographic data provided by vendors, where it exists, can provide an interesting stress test on modelled results. Two cyber catastrophe models were also used to match the companies against their proprietary industry exposure databases to return another view of revenue and industry.

Two cyber catastrophe models and one scanning vendor were utilised to return the total revenue of all 221 companies within the set. Figure 9 below shows the variation in total revenue of the sample data set by source. As illustrated below, there were significant differences in the total revenue data, dependent on source.



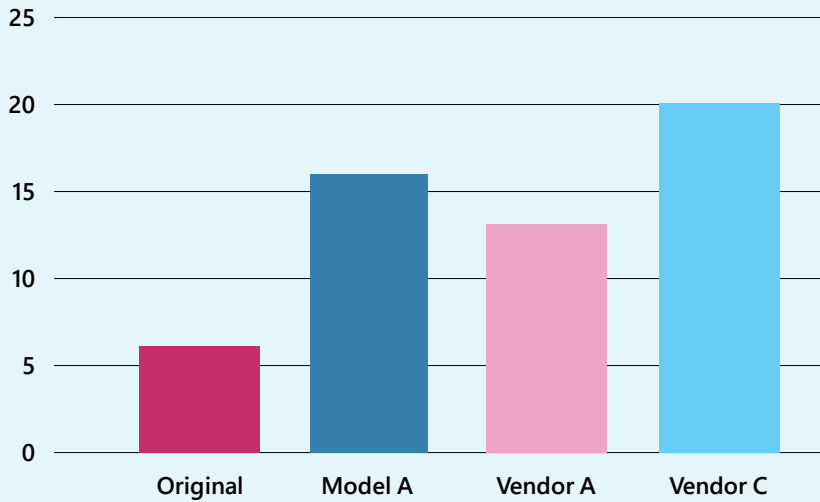
Industries may also be mapped differently using data provided by the scanners, in part because some companies operate across multiple sectors. One of the limitations of catastrophe models today, is that they typically only allow a company to be assigned to one industry (see figure 10). For some (especially larger) companies, there may be several industries to which they could be categorised, and this is relevant to the threat assessment.

While the original data was condensed into a few industries, both the cat models and the scanning tools attributed a larger number of industries to the data.



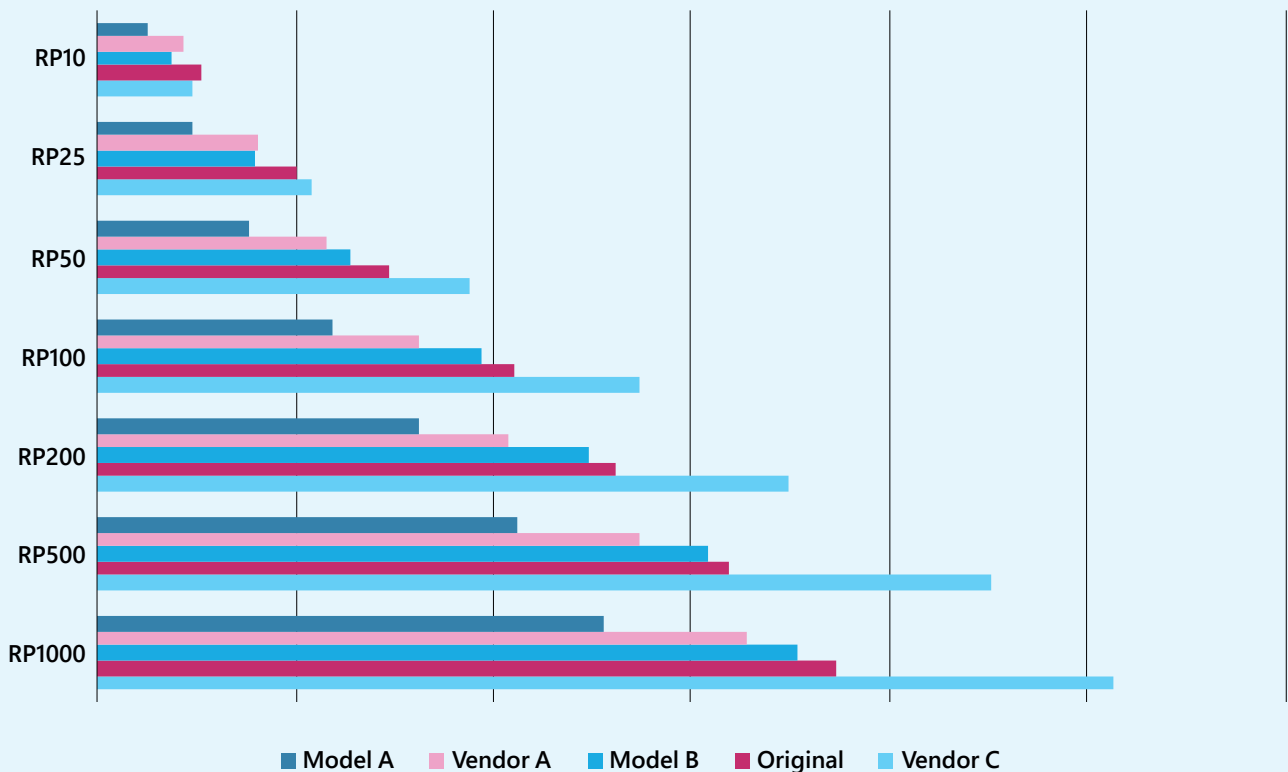
¹⁴ Specialist, D. (n.d.). What is firmographic data? Uses, Types & Dataset Examples | Datarade. <https://datarade.ai/data-categories/firmographic-data>

Figure 10: Number of Industries



Modelling the portfolio with new augmented data for both revenue and industry highlights the potential impact on losses of using an alternate data source, and the sensitivity of the losses to these key fields, as shown in figure 11 below.

Figure 11: Ground Up EP Impact



Technological Aggregations

Catastrophe models provide a representation of cyber loss outcomes – but should not be used in isolation. Given that a major cyber catastrophe has not yet occurred, the models are still untested and do not address the complete universe of cyber risk. As has been illustrated above, even if the models were comprehensive, changes in data can dramatically alter losses, which can further impact on required capital.

A complimentary methodology for managing cyber aggregations is to limit the amount of risk that can be seen to be exposed to any one technology. While some cat models have their own capabilities for these estimates, scanning tools can provide an additional view of risk on accumulations.

Technology aggregation monitoring is a useful tool in assessing the diversification of portfolios, helping to ensure that the risk is split evenly between technologies. Improved diversification supports increased confidence to write more cyber business.

Technological aggregations also provide insurers with a means of generating their own internal disaster scenarios, as a stress test on their portfolios. These scenarios should represent a worst case for directly



Improved diversification supports increased confidence to write more cyber business.

impacted companies, since it is unlikely that a single technology could be impacted everywhere it is observed. This is because of the different ways in which technologies can be implemented in the technology stack.

A Lloyd's study¹⁵ on best practices described Active Portfolio Management as the ability to “identify a dynamic / fluid grouping of risks that can be analysed to a suitable detailed level of granularity, to drive specific actions that will improve the performance of one or more portfolios across a book of business, on both the top and bottom line”.

This is very apt in cyber portfolio management, where the risk groupings can be captured dynamically and can change over time. Risk aggregations are also useful for monitoring the overall health of a portfolio.

An industry report found that policyholders with one unresolved critical vulnerability of any kind were 33% more likely to experience a claim than those who resolved the vulnerability.¹⁶ A recent study involving a meta review of security control effectiveness¹⁷ found that attack surface management and patch cadence were consistently the first and second most effective interventions.

The study also found that specific VPN providers were associated with much higher rates of incidents, showing the value of being able to aggregate a portfolio by technology provider or product.

The table shown in figure 12 highlights some of the features that can be used to derive technology aggregations, as provided by the different vendors.

¹⁵ Portfolio management in the London market What separates the best from the rest – Lloyd's. (n.d.). <https://www.lloyds.com/news-and-insights/risk-reports/library/portfolio-management-in-the-london-market-what-separates-the-best-from-the-rest/>

¹⁶ Coalition, Inc. (n.d.). Download here: Coalition's 2023 Cyber Claims report. <https://info.coalitioninc.com/%20download-2023-cyber-claims-report.html>

¹⁷ Woods, D. W., & Seymour, S. (2024). Evidence-based cybersecurity policy? A meta-review of security control effectiveness. *Journal of Cyber Policy*, 1–19. <https://doi.org/10.1080/23738871.2024.2335461>

Figure 12: Technologies used to inform aggregation potential

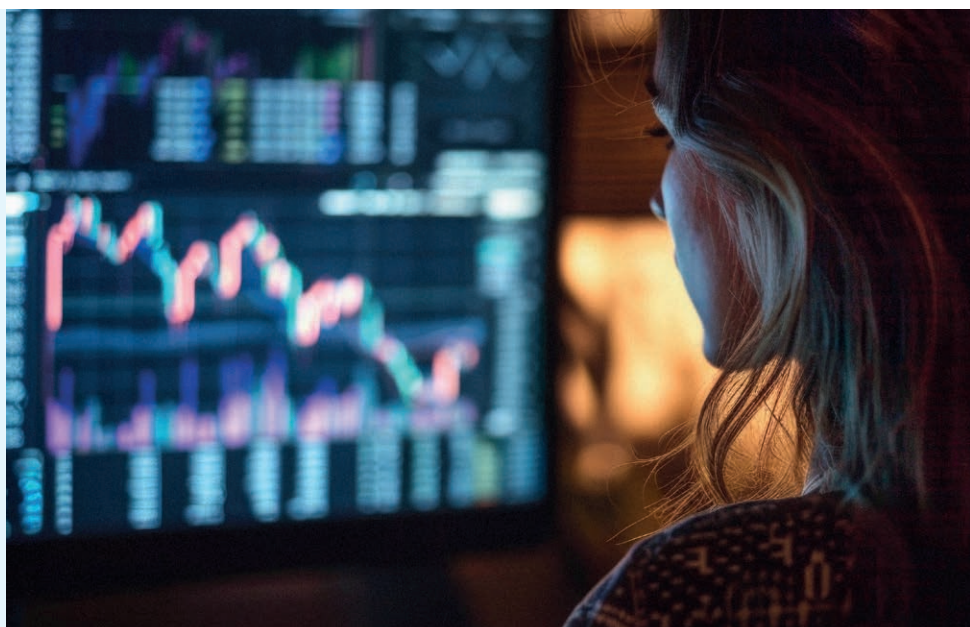
	Example	Vendor A	Vendor B	Vendor C	Vendor D
Technology Used	jQuery	✓	✓	✓	✓
CVE Technology	jquery/3_3_1	✓	✓		✓
DNS Provider	Amazon Route 53	✓	✓		
ISP Provider	AT&T, MS Azure	✓	✓		✓
Hosting Provider	Amazon.com MS Azure	✓	✓		✓
Payment Provider	Visa	✓	✓		
Cloud Provider	AWS	✓	✓	✓	✓
Cloud Service	EC2	✓	✓	✓	✓
Cloud Data Centre	us-east-1	✓	✓	✓	✓
Email Services	SPF, DMARC	✓	✓		✓
Domain Checks	PhishTank, Registrars	✓	✓	✓	
Open Ports		✓	✓	✓	✓
SSL Certificates	Checks or providers	✓	✓	✓	✓

As well as technological data, some vendors may also provide additional data about the scores. For example, one vendor provides the type of incident most likely to impact the insured in addition to the scores, e.g. Ransomware or Third Party.

Modelled Losses

Some of the scanning tools also have the capability to provide modelled losses, either in the form of Probably Maximum Losses (PML), or scenarios. One of the companies modelled 17 different scenarios, and their impact on insurance policies.

Over time, these loss estimates can provide useful sensitivity tests against the primary cyber loss quantification methodology.




Conclusion

Cyber risk data providers can play a valuable part in assessing cyber security risk. They can provide sensitivity tests for the exposure data used in the catastrophe models, and also provide a key second view of risk.

Best practices in portfolio management, like those promoted by regulatory bodies and Lloyd's of London in their regulatory capability matrix, promote using more than one view of risk.

In the uncertain world of cyber modelling, combining tools for a more comprehensive view of risk is an important way to benefit from the technological developments in vulnerability scanning, whilst avoiding some of the pitfalls of over-reliance on one model. Historically, the natural catastrophe world has seen several examples where outsized losses have occurred where models were found to be missing potential exposure. Scanning tools can be a useful addition to the modelled view of risk, to help mitigate this pitfall.

Cyber risk data providers can play a valuable part in assessing cyber security risk.



In the uncertain world of cyber modelling, combining tools for a more comprehensive view of risk is an important way to benefit from the technological developments in vulnerability scanning, whilst avoiding some of the pitfalls of over-reliance on one model.

Acknowledgements

Lockton Re are most grateful to Cyberwrite, ISS-Corporate, KYND and Orpheus for their help and participation in this study. Features mentioned are correct at the time of writing, but these companies regularly release updates to their software.

Cyberwrite

About Cyberwrite: Founded in 2017 Cyberwrite is a leading cyber insurance technology company that empowers brokers and carriers worldwide to assess, and mitigate cyber insurance risks. Through advanced analytics, AI, and cyber intelligence technology, Cyberwrite provides actionable insights into cyber threats, enabling brokers to offer tailored risk management solutions to their clients and underwriters to make data-driven decisions in seven languages worldwide. For more information, visit www.cyberwrite.com



About ISS: ISS Corporate Solutions, Inc. ("ISS-Corporate"), a part of the ISS-STOXX group of companies, is a leading provider of cutting-edge SaaS and high-touch advisory services to companies, globally. Companies turn to ISS-Corporate for expertise in designing and managing governance,

compensation, sustainability, and cyber risk programs that align with company goals, reduce risk, and manage the needs of a diverse shareholder base by delivering data, tools, and advisory services. ISS-Corporate's global client base extends across North America, Europe, and Asia, as well as other established and emerging markets worldwide. For more information, go to <https://www.iss-corporate.com/>

KYND

About Kynd: KYND is a cyber risk solutions provider dedicated to demystifying complex cyber risks, making them more manageable for insurers and their clients. Our next-generation solutions empower partners to comprehensively assess, understand, and enhance their risk resilience with unprecedented ease. Through innovative approaches, KYND transforms the way cyber risks are handled, fostering a safer and more secure digital landscape for all stakeholders. For more information, visit: <https://www.kynd.io/>

ORPHEUS

About Orpheus: Orpheus provides cyber risk rating for the insurance sector through our data, ground breaking platform, and managed services.

We are a highly accredited cyber threat intelligence company (CREST, Bank of England and FCA) and combine our unique understanding of the threat to any company with detailed insight into the current vulnerabilities of that entity. We use advanced technologies, including AI, to prioritise findings and we accurately calculate the likelihood of a company becoming a victim of a cyber attack – automatically giving any company a dynamic cyber risk score, supported by detailed reporting. For example, data science tests with global cyber insurance firms have shown that when Orpheus scores a company as high risk, that company is significantly more likely to suffer a cyber breach in the future, and to claim on their insurance policy. For more information, visit: <https://www.orpheus-cyber.com/>

About Lockton Re (locktonre.com)

Lockton Re, the reinsurance business of Lockton, helps businesses to understand, mitigate, and capitalize on risk. With over 400 colleagues in 19 locations globally, the business is continuing to grow, pushing the reinsurance industry forward with smarter solutions that leverage new technologies – delivered by people empowered to do what's right for clients.

Lockton Re Insights

Lockton Re's reports, market commentary and insights focus on key topics, occurrences or changes in the (re)insurance and broking market place which impact our clients and partners. In order to help guide relevance for the reader, we categorize this content in four areas – Perils, Exposures, Risk Transfer and Placement.

Lead author: Jacqueline Yeo,
Cyber Analytics Lead, Lockton Re
Jacqueline.Yeo@lockton.com

Co-author: Oliver Brew,
Cyber Practice Leader, Lockton Re, London
Oliver.Brew@lockton.com

Enquiries:

Isabella Gaster
Lockton Re Global Head of Marketing
isabella.gaster@lockton.com

Elizabeth Miller Kroh
Lockton Re Head of Marketing, North America
elizabeth.kroh@lockton.com

Addresses:

United Kingdom

The St Botolph Building
138 Houndsditch
London EC3A 7AG
United Kingdom
Office phone number +44 020 7933 0000

New York

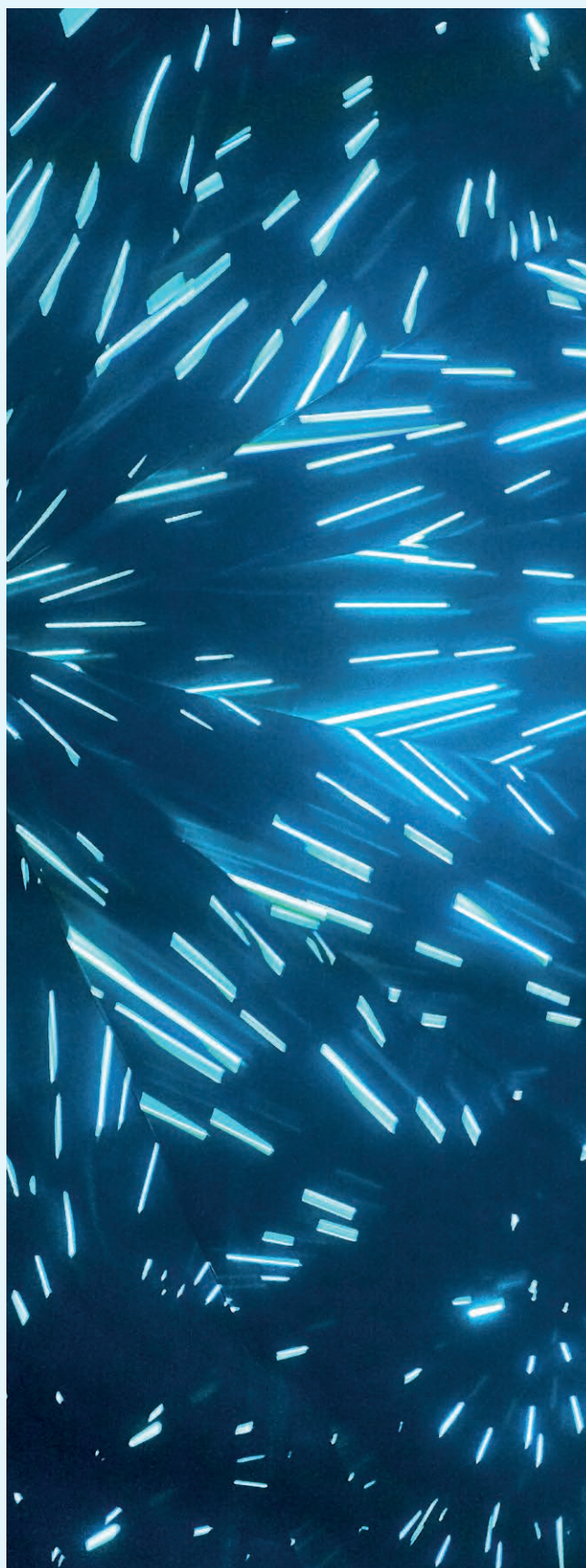
261 Fifth Avenue, 10th floor,
New York, NY 10016
United States
Office phone number +1 646 572 7300

Bermuda

Seon Place, 141 Front Street, 3rd Floor
Hamilton HM19
Bermuda
Office phone number +1 441 294 4864

Zurich

Freigutstrasse 26
8002 Zurich
Switzerland
Office phone number +41 (0) 79 944 84 74



Sources

Steve Morgan 2023. "Boardroom Cybersecurity Report 2023" Secureworks blog December 13, 2023. <https://www.secureworks.com/centers/boardroom-cybersecurity-report-2023>

ThreatLabz. (2024). ThreatLabz 2024 ransomware Report [Report]. Zscaler, Inc. <https://www.zscaler.com/resources/industry-reports/threatlabz-ransomware-report.pdf>

Cyber security breaches survey 2024. (2024b, April 8). GOV. UK. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024>

Sophos (2024). The State of Ransomware 2024 <https://www.sophos.com/en-us/content/state-of-ransomware>

CVE – Search CVE list. (n.d.). https://cve.mitre.org/cve/search_cve_list.html

Coalition Security Labs. (2024). Cyber Threat Index 2024. In Coalition Security Labs. https://info.coalitioninc.com/rs/566-KWJ-784/images/Coalition_Cyber-Threat-Index_2024.pdf?version=0

Risk Optics November 17, 2021. Blog.

Internal vs. External Vulnerability Scan: What Are the Differences? — ZenGRC (reciprocity.com)

Paganini, Pierluigi. 2023. "Kaseya Ransomware Attack Here's What you need to Know" Cyber News. December 07, 2023. <https://cybernews.com/security/kaseya-ransomware-attack-heres-what-you-need-to-know/>

Kerner, S. O. S. M. (2023, November 3). SolarWinds hack explained: Everything you need to know. WhatIs.

<https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>

The United Kingdom Top 100 companies: Cybersecurity threat report – SecurityScoreCard (2024, June 28). SecurityScorecard. <https://securityscorecard.com/research/the-united-kingdom-top-100-companies-cybersecurity-threat-report/>

2024 Attack Intelligence Report – Toolkit | Rapid7. (n.d.). Rapid7. <https://www.rapid7.com/research/reports/2024-attack-intelligence-report-toolkit/>

Specialist, D. (n.d.). What is firmographic data? Uses, Types & Dataset Examples | Datarade. <https://datarade.ai/data-categories/firmographic-data>

Portfolio management in the London market: What separates the best from the rest? Lloyd's. (n.d.). <https://www.lloyds.com/news-and-insights/risk-reports/library/portfolio-management-in-the-london-market-what-separates-the-best-from-the-rest/>

Coalition, Inc. (n.d.). Download here: Coalition's 2023 Cyber Claims report. <https://info.coalitioninc.com/%20download-2023-cyber-claims-report.html>

Woods, D. W., & Seymour, S. (2024). Evidence-based cybersecurity policy? A meta-review of security control effectiveness. *Journal of Cyber Policy*, 1–19. <https://doi.org/10.1080/23738871.2024.2335461>

Legalities:

Please note that our logo is Lockton Re; our regulated entities are Lockton Re, LLC in the USA Lockton Re, LLC, 261 Fifth Avenue, NY, NY 10016 and Lockton Re LLP in the UK Registered in England & Wales at The St. Botolph Building, 138 Houndsditch, London, EC3A 7AG. Company number OC428915.

Lockton Re provides this publication for general informational purposes only. This publication and any recommendations, analysis, or advice provided by Lockton Re are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. It is intended only to highlight general issues that may be of interest in relation to the subject matter and does not necessarily deal with every important topic nor cover every aspect of the topics with which it deals. The information and opinions contained in this publication may change without notice at any time. The information contained herein is based on sources

we believe reliable, but we make no representation or warranty as to its accuracy. Lockton Re shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as reinsurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your applicable professional advisors. Any modelling, analytics, or projections are subject to inherent uncertainty, and the information contained herein could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. This publication is not an offer to sell, or a solicitation of any offer to buy any financial instrument or reinsurance product. Nothing herein shall be construed or interpreted as

a solicitation of any transaction in a security or commodity interest as defined under applicable law. If you intend to take any action or make any decision on the basis of the content of this publication, you should seek specific professional advice and verify its content.

Lockton Re specifically disclaims any express or implied warranty, including but not limited to implied warranties of satisfactory quality or fitness for a particular purpose, with regard to the content of this publication. Lockton Re shall not be liable for any loss or damage (whether direct, indirect, special, incidental, consequential or otherwise) arising from or related to any use of the contents of this publication.

Lockton Re is a trading name and logo of various Lockton reinsurance broking entities and divisions globally and any services provided to clients by Lockton Re may be through one or more of Lockton's regulated businesses.



REINSURANCE