BLACK KITE

A FIGHT FOR COVERAGE

CYBER INSURANCE RISK IN 2022

TABLE OF CONTENTS

INTRODUCTION

Volatility and complexity have toppled the cyber insurance landscape, forcing the industry to reassess cyber risk overall. By 2026, the global cyber insurance market is forecasted to grow at a compounded average of 25% yearly[1], while simultaneously pricing out insureds and establishing an extremely stringent criteria for coverage.

Underwriters are working expeditiously to accurately assess the cyber health of each insured. As a result, more extensive applications and increased due diligence are bogging down carriers worldwide, causing frustration and burnout at an exorbitant rate. To top it all off, the supply chain of cyber insurance companies has subsequently compounded, making their ecosystems as susceptible, if not more susceptible, to a data breach or ransomware attack.

In addition to performing research on the emerging threats for underwriters and the cyber insurance market as a whole, Black Kite Research analyzed the top 99 insurance companies[2] by net premiums in 2019 to better understand their cyber posture and the impact of increasing risk levels.

The goal of this research is to provide insight for both CISOs and underwriters in the insurance sector around emerging cyber threats. Whether you are responsible for preventing risk to your own organization and vendors, or writing cyber insurance policies for other companies, this report is for you.

KEY FINDINGS

- More than half of the largest insurance carriers are 3x more likely to experience a cyber breach than those with top ratings
- 18% of the insurance companies analyzed are above the critical ransomware threshold of a 0.6 rating, indicating a high level of ransomware susceptibility
- 82% of the largest insurance carriers are susceptible to a phishing attack
- Software vendors are the most common source of supply chain attacks, accounting for 25% of all third-party incidents in 2021

CYBER TRENDS & EMERGING THREATS

The rise of the virtual office means more networks, more devices, and exceedingly more interconnected growth for companies across the board. The most impactful result of this growth for cyber insurance carriers is an ever-increasing level of risk to cover. As a result, these carriers implement higher premiums, which mirror the increasing risk.

In fact, according to a survey by Woodruff-Sawyer Co[3], 62% of underwriters expect cyber insurance premiums to increase greatly over the next 12 months. This increase is a direct result of the rapid upswing of ransomware and supply chain attacks. It also stems from an overall market correction, as pricing has risen to properly reflect the level of risk covered previously.

RANSOMWARE

Today, a ransomware attack occurs every 11 seconds[4], and in 2021, six ransomware attacks occurred every minute. In fact, the largest ransom paid to date[5] was by an insurance company in 2021, totaling just under $40 million. The average payment in 2021 sat at around $130,000[6].

A ransomware incident's impact goes far beyond the ransom itself, often exceeding the amount initially demanded, creating a substantial remediation cost.

This ripple effect cost includes **higher insurance premiums,** reputational damage, and interruptions to the overall business.

Consider the unplanned downtime. How much money and progress is lost if essential systems are down for even a day, or perhaps a week? According to Coveware[7], the average time lost thus far this year due to ransomware attacks is three weeks. The average full remediation cost is nearly $2 million, doubling from 2021's financial impact average of $1 million[8].

100% of underwriters ranked ransomware and supply chain attacks among their top 3 threats.

HOW DOES CYBER INSURANCE HELP?

Cyber insurance can cover lost profits and fixed expenses expelled during unplanned downtime, but as risks rise and more claims are filed, premiums become extremely high.

Damages are beginning to exceed estimates, which puts insurance companies in a tough position, intensifying the need for automated, continuous risk assessments that policyholders can use to evaluate their portfolios.

$2 MILLION
AVERAGE REMEDIATION COST FOR RANSOMWARE IN 2021

DIGITAL SUPPLY CHAIN

Companies worldwide have seen an increase in cyber attacks, specifically targeting their digital supply chain as a method of access. Software and tech companies with consumers across multiple industries have especially experienced the 'shock waves' of third party incidents.

In fact, according to the Black Kite Research team in our latest annual Third-Party Breach report[9], software vendors were the most common source of supply chain attacks, accounting for 25% of all incidents in 2021. Additionally, 1.5 billion user's PII were leaked as a result of a third-party breach. Recovery after exposing sensitive data is expensive and time-consuming, and plays into the aggregation risk of a situation.

What is aggregation risk?

Aggregation risk takes into account the risk associated with the scale and scope of a cyber incident. Essentially, one larger incident could cause a ripple effect that creates smaller incidents across several critical industries, triggering the collapse of systems if impactful enough. Within insurance specifically, an incident causing business interruption or leaked credentials across numerous insureds in a cyber insurer's portfolio could trigger losses across a group of policyholders from said single event.

Throughout the most impactful 2021 incidents, attackers were particularly strategic - they targeted products and companies that provided a solution or service to thousands, if not millions, of people across the globe. In turn, these targeted attacks raised a red flag for insurance carriers covering risk: *what if the full customer base of a single compromised company experiences the cyber attack effects simultaneously?*

Software supply chain attacks increased by 300% in 2021.

As software supply chain attacks have sharply increased - up 300% in 2021[10] - predictions for 2022 and beyond continue on the same trajectory. Forrester[11] predicts 60% of security incidents in 2022 will result from third-party incidents. Even if a company considers itself to have a robust security protocol, it only takes one vulnerable vendor to be susceptible to an attack.

For insurance providers, this spike means stricter protocol for companies obtaining coverage in the first place, particularly if their risk level is already high. According to Evident's latest report [12], 75% of third-party vendors do not meet the insurance requirements established by the companies that hire them, often due to unattainable requirements and high premiums. Furthermore, the average compliance rate for third parties across all requirements is **merely 25%.**

PUBLIC SECTOR

As ransomware attacks on public and private sector organizations increase, insurance adjusters have been forced to increase premiums and prerequisites for cyber policies. Among U.S. public finance (PF) entities, cyber insurers paid out 73% of premiums in 2020 compared to 34% in 2018 [13].

The term '**Left of Bang'** was popularized in 2006 in the U.S. Marines' Combat Hunter doctrine. In the context of cybersecurity, it urges proactivity and using threat intelligence to make informed decisions before an incident occurs. 16 years later, staying 'Left of Bang' requires an ongoing effort that uses automation and continuous risk monitoring, leaving no room for assumption.

In 2021, President Biden identified cybersecurity and supply chain risk management as top priorities across all levels of government. Although government systems are more likely to report cyber attacks due to transparency mandates, the issue of consistent, reliable attack data globally makes it difficult to assess risk. Furthermore, underwriters are more carefully scrutinizing risk posed by not only the insured, but by the third-parties the insured works or contracts with.

Today, states regulate the insurance market, but do not generally establish minimum standards. More often they focus on the solvency of cyber insurers and ensure policy terms are fair, affordable, and comply with state laws. As more regulations are put in place to report attacks, public and private collaboration at the national, state, and local level will be paramount to help protect U.S. critical infrastructure.

Currently, there are no specific regulations requiring cyber insurance. However, having insurance is part of an assumed standard, or second order of expectation. A company that knowingly entertains unprotected risk and endures a breach is going to have significant financial and legal ramifications. If a company doesn't have cyber insurance, they will be in a much less defendable position from a legal perspective in the case of an incident.

PREDICTABILITY

Predictability is a key part of maintaining a 'Left of Bang' approach within cyber insurance. For underwriters, upfront intelligence is extremely important as they vet and determine which applications are worth granting risk coverage - and how much to cover. Necessary intelligence includes the state of health for each policyholder (or potential policyholder), how that policyholder approaches digital supply chain security, and how they are managing their data. With a constant rise in payouts for attacks, such as ransomware, underwriters have to be picky as they determine what companies are healthy enough to warrant coverage.

By quantifying risk, and translating risk levels to a dollar amount, underwriters can better define risk thresholds with each policyholder. By using an international standard, such as Open FAIR™, trustworthy calculations of probable impact, if a breach were to occur, are possible. This intelligence provides unmatched insight into potential payouts in the future, reducing loss ratios over time.

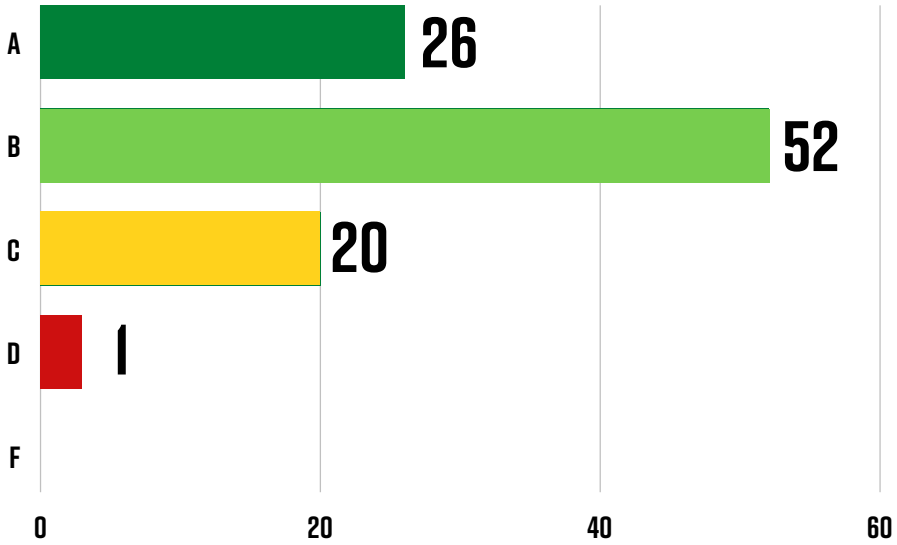
THIRD PARTY RISK MANAGEMENT POSTURE
CYBER INSURANCE COMPANIES

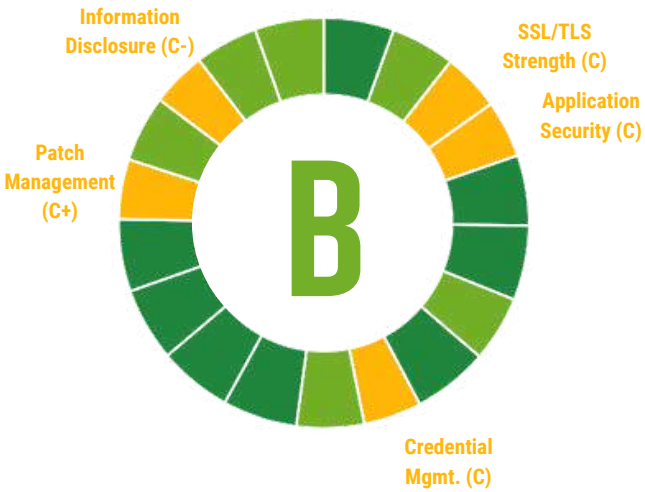
Black Kite Research took a deeper look into the cyber posture of insurance carriers from a third-party risk lens. For this study, our team analyzed the largest 99 insurance companies by net premiums in 2019 to uncover the industry's cyber risk and potential areas of concern.

Overall, insurance carriers have an average, or "Good", grade of B, and technical rating of 84.6.

Black Kite follows and applies commonly-used frameworks developed by MITRE to determine the overall company rating, converting highly technical terms into simple letter grades. The cyber rating, an aggregation of open-source intelligence, gives a look into the overall health of a company.

INSURANCE COMPANIES' GRADE DISTRIBUTION



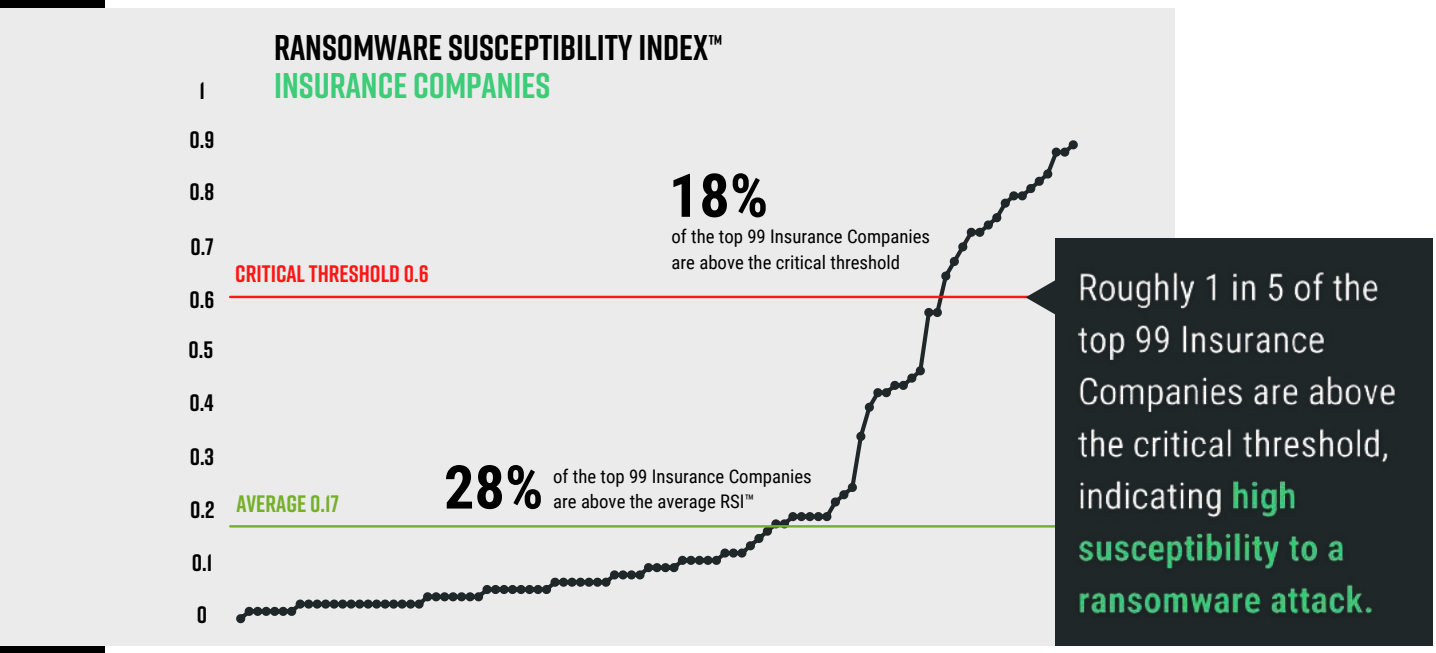


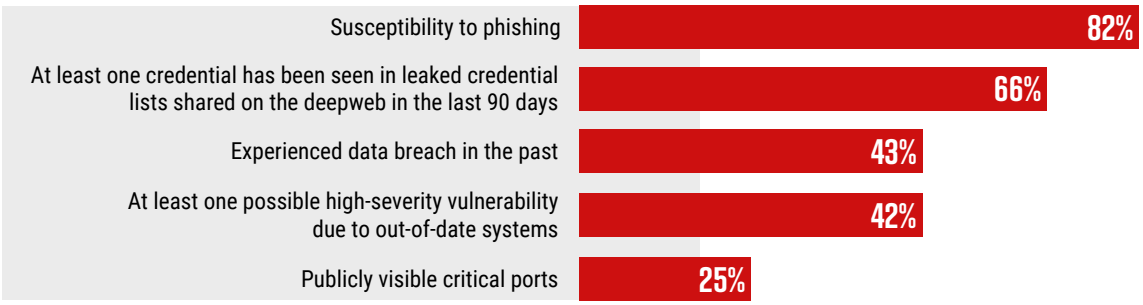
The total rating is a weighted average of 20 defined categories, providing unmatched breadth and insight into detected vulnerabilities. Each category, as well as each control point, has a different weight in the overall grade.

Black Kite has 290 control points with various weights corresponding to MITRE's TTPs, eliminating false positives. In this case, with a "B" rating, a company is 3x as likely to experience a data breach than a company that achieves an "A" rating.

RANSOMWARE POSTURE

Black Kite is the only cyber ratings platform that can identify ransomware susceptibility for a company in advance of an attack. The average Ransomware Susceptibility Index™ rating for insurance companies reflects a **0.17** - an extremely positive score on a 0.0 to 1.0 scale of susceptibility. However, **18% of the insurance companies analyzed received an RSI™ above the critical threshold of 0.6,** indicating a high level of ransomware susceptibility. It's important to note *low susceptibility does not mean no susceptibility.* Threats and vulnerabilities emerge every second, making a continuous and proactive response a prerequisite.





Of the top ransomware-related security issues for the insurance companies studied, susceptibility to phishing tops the list. With 82% of the companies emerging vulnerable, it is important to discuss why phishing still creates results for threat actors. Phishing is known to be extremely low risk for threat actors, but if successful, can create high gains.

Often, a lack of training or education in the company is the cause of a successful phishing attack, and it only takes one employee not paying attention or staying vigilant. In fact, CISCO's 2021 Cybersecurity Report[14] suggests that 86% of organizations had at least one person click a phishing link last year. Furthermore, the data suggests that phishing accounts for around 90% of data breaches.

The most common requests include revealing a credential, sharing personal information, or giving access to a platform. Even something as simple as a credential can be all a bad actor needs to gain access to a company's entire database.

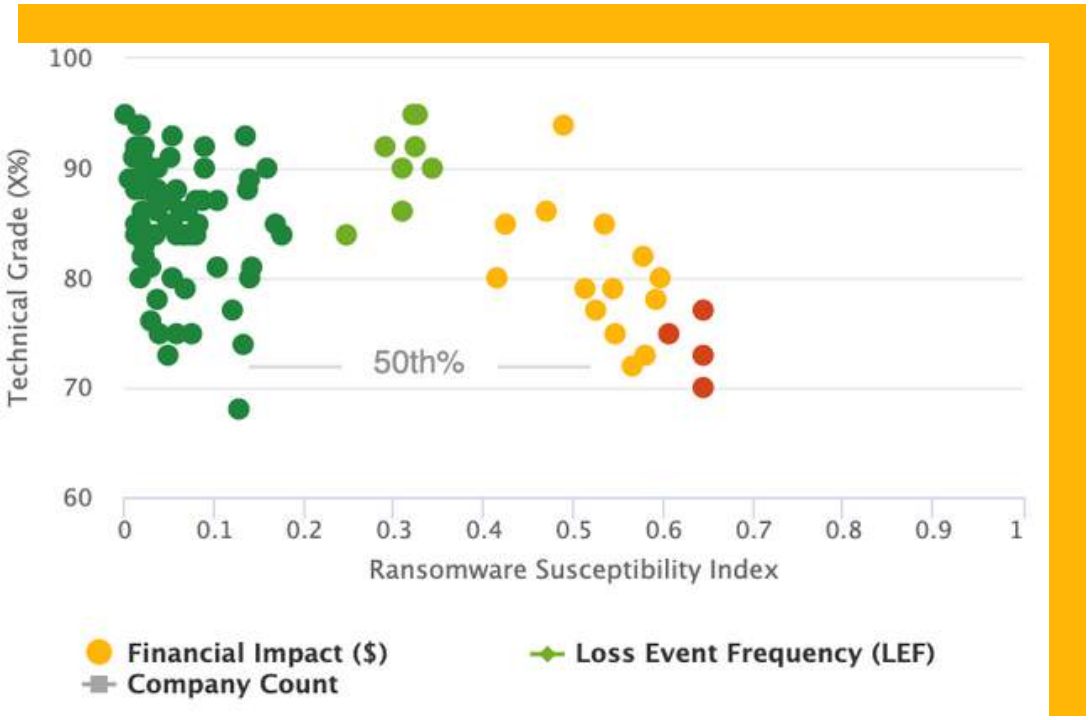
This leads to the second pressing issue: leaked credentials. Once a credential is secured, leaking it on the deep web is a second step that can lead to a domino effect of risk, giving access to not only the original cyber criminal, but anyone who can find the credential.

42% of insurance companies have at least one possible critical vulnerability due to out-of-date systems. Out-of-date systems are an obvious, but often overlooked issue, that facilitate access points for hackers to exploit, such as the beginning of the far-reaching Log4j incident.

46% of underwriters believe cyber risk will increase greatly in 2022.

As Black Kite Research further examined the RSI™ vs. Technical cyber rating, high susceptibility to ransomware directly correlated to a low rating and overall poor cyber health.

According to Woodruff-Sawyer, **85% of underwriters believe companies should focus on strengthening their cyber security.** None of the underwriters surveyed thought that companies should be purchasing higher limits as a means to mitigate risk.



MARKEL CORPORATION GAINS VISIBILITY INTO POLICYHOLDER RISK WITHIN MINUTES

Markel Corporation, (NYSE – MKL), a holding company for insurance, reinsurance, and investment operations around the world, uses the Black Kite platform to create the strict protocol for analyzing risk, streamlining the underwriting process. Headquartered in Richmond, Virginia and founded in 1930, Markel reports its ongoing underwriting operations in three segments, and products originate from four insurance divisions and one reinsurance division.

Before Black Kite, Markel was in need of an automated platform that could continuously assess their cyber insurance portfolio, and reduce the time it took to analyze their portfolio from days to hours. By analyzing each applicant quickly through the platform, Markel is now able to identify accounts with elevated risk metrics sooner in the process.

Ransomware is currently one of the most immediate concerns in the cyber insurance space, and Black Kite's Ransomware Susceptibility Index™ has been an extremely important component of monitoring for high ransomware risk levels. Using the RSI™, Markel was able to build Black Kite findings into their guidelines when assessing individual risks: any rating over a particular RSI threshold or below a particular cyber rating requires additional analysis to be deemed appropriate for the portfolio. Underwriters are now more informed when deciding which risks to pursue.

IT ALL BEGINS WITH THE INITIAL SCAN,

where underwriters:

1. Identify their prospective policyholder
2. Scan for susceptibilities and vulnerabilities

The data then impacts the underwriting analysis.

"The Black Kite platform makes unknowns known, and educates our team internally around those findings. This assists in underwriting, portfolio management, and advocacy, to work with management in a crisis situation." *Lou Botticelli, Senior Director of US Cyber Product at Markel*

According to Markel, underwriters are seeing 100%-500% more submissions.

By providing visibility into each policyholder's risk in as little as several minutes, as well as insight into ransomware risk levels, the window of time spent negotiating terms and conditions has been significantly reduced. This allows for a nimble and responsive working process, and has proven to be a driver of efficiency at Markel to identify where best to deploy their capital.

EXPERT INSIGHTS

BOB MALEY

Chief Security Officer, Black Kite

A Look Into Today: *What do underwriters need to understand about the current risk landscape?*

One of the challenges for cyber insurance underwriters is the lack of contextual, historical data. In traditional insurance markets, strong trend data is available to help make informed decisions. For instance, driver data signals that younger drivers are typically more accident-prone. This concept goes back to insurers requiring the ability to predict the level of loss in order to charge enough to cover those potential losses.

In the realm of cyber insurance, there are three glaring issues:

1. The actual amount of data for the type of perils that underwriters are looking at is lacking, preventing a strong prediction of loss.
2. In the world of cyber, things change far too rapidly to base decision-making on historical data.
3. Cyber insurance has no standard policy form, preventing data comparison and consistency between policies and coverages.

If we think back to automobiles, the perspective around safety and risk changed very slowly, an example being seatbelts and airbags. However, cyber is changing nearly every month. New controls may be added for a particular threat, but the bad actors are so agile that they just change their tactics and procedures.

Suddenly, new cyber incidents negate the old work done for the previous policies, and uncertainty rises, raising premiums. In my observation, CISOs across the nation are struggling with how quickly insurance is changing, and the high price alongside decreased coverage.

EXPERT INSIGHTS

CHUCK SCHAUBER

VP of Product & Strategy, Black Kite

A Look Inside: *Was the insurance landscape in 2021 an aberration, or is it the new normal?*

Cyber insurance carriers are facing increased difficulty in choosing which policies to underwrite and what premiums to offer. It used to be sufficient to know what policies, procedures, and protections were in place to determine if an organization could be underwritten. An even better methodology was to benchmark organizations against their peers and choose to underwrite "best-of-breed" organizations. But, in today's landscape, is it enough to continue using these snapshot techniques?

Insurance companies have faced these types of challenges before. The traditional tenets to managing any insurance business are deductibles, premiums, and underwriting selection, which remains the case today. Carriers can certainly weather this storm by ensuring better outcomes for themselves by raising deductibles, lowering limits, and utilizing sub-limits on specific coverages.

However, cybersecurity risks follow rules more akin to a supply-and-demand market rather than something that occurs randomly. These attacks are not random acts, but rather acts of opportunity. So how can a carrier ensure the best possible outcome for their insureds? Insureds don't want to be hacked either. So what role does education and monitoring play in cyber?

In the same way that driver education and monitoring lowers auto insurance claims, can cyber education and continuous monitoring have the same effect? The carriers and brokers who will come up on top in the end will likely find mutually beneficial ways to work with their insureds.

One mutually beneficial approach would assume shared responsibility between the carrier and the insured. Cybersecurity tools exist that can continuously track the external attack surface of an organization and rate its effectiveness. If carriers were to mandate a level of continuous compliance, they could continuously manage their risk.

This is achieved by using a standard way of communicating risks and vulnerabilities, like the MITRE and NIST frameworks. Setting baseline expectations between the carrier and the insured is the cornerstone of stabilizing outcomes.

EXPERT INSIGHTS

JEFFREY WHEATMAN

Senior VP, Cyber Risk Evangelist, Black Kite

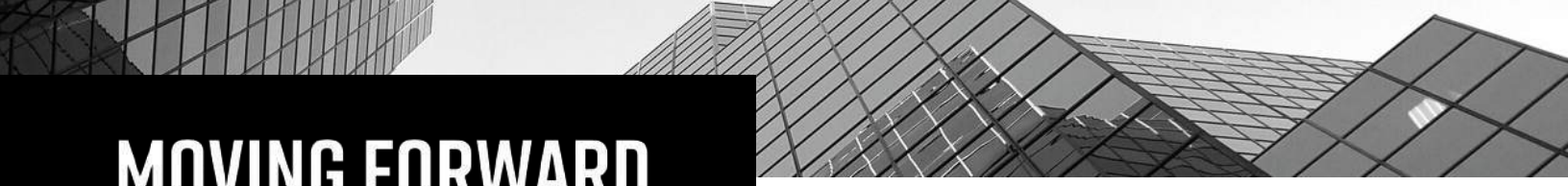
A Look Ahead: *Where is the cyber insurance market going in the next 5-10 years?*

Cyber insurance continues to evolve and is quickly becoming a must-have for most organizations. In some cases this is due to legal and regulatory expectations, and for others due to partner requirements as part of due diligence for vendor risk management. We expect there to be significant adjustments regarding expectations for what cyber insurance provides.

I believe it's fairly unlikely that cyber insurance will continue to pay off significant damages as a result of cyber claims and, for the most part, is going to be primarily used for simple things such as paying postage for breach notification mailings, paying for incident response and postmortem investigations. Situations involving larger attacks within the third-party ecosystem may lead to larger liabilities for the insured that cyber insurance won't cover.

One of the biggest challenges that we've heard is insurance companies are not cybersecurity experts and they continue to struggle or be challenged by an inability to fully understand the cyber security posture of their customers and prospective customers. The market seems to be fractured with regard to how these postures are assessed, with some insurance companies trying to roll their own, others using questionnaire-based approaches with dubious and limited benefits, and others or partnering with consultants, GRC vendors, and of course rating service vendors. The lack of standards about what constitutes 'good' or 'reasonable' makes things worse – and it is likely to get worse before it gets better.

I think at the end of the day, procurers of cyber insurance must have reasonable expectations of the value expected from the engagements. Organizations that expect cyber insurance to address all of their concerns and can be used as a "get out of jail free card" will be disappointed, frustrated, and potentially held liable in the court of law and the court of public opinion. Cyber insurance should absolutely be part of a risk management portfolio but should not be viewed as a panacea.



MOVING FORWARD

In a time where cyber attack damages often exceed expectations, it is crucial to have insight into an organization's risk profile to prepare for what you can't see coming. There are several challenges when it comes to writing cyber insurance policies, but possibly the most notable is the issue of external risk. Policies written for one organization may not take into consideration vendor, partner or supplier relationships that can cause catastrophic cyber incidents from simple activities like sharing vulnerable data or providing access to internal systems.

REVIEW YOUR RISK PORTFOLIO ON A CONTINUOUS BASIS

A comprehensive risk assessment looks at both internal and external threats, seeking to understand where vulnerabilities exist leaving an organization open to an attack. A point-in-time analysis does not provide an accurate picture of cyber risk, nor take into account how quickly the threat landscape can change.

Black Kite's continuous cyber risk assessments support the needs of insurance underwriters by offering near real-time attack surface monitoring. Whether you need critical vulnerability highlights or a deep dive into an organization's full risk profile, you only need one top-level URL to get started.

SEE THE PLATFORM

BRING AUTOMATION INTO YOUR UNDERWRITING PROCESS

Before automated cyber risk ratings platforms became available, cyber insurers used mathematical equations and relative (high, medium, low) or ordinal (1-10) grading methods to determine an organization's cyber risk. Using a standards-based rating tool like Black Kite takes the manual burden away by analyzing externally-facing data from over 400 open-source intelligence resources. The results are distilled down to simple dashboards and reports that can be used to quickly and accurately make cyber policy decisions.

REFERENCES

1. https://www.statista.com/statistics/1190800/forecast-cyber-insurance-market-size/
2. https://www.reinsurancene.ws/top-100-u-s-property-casualty-insurance-companies/
3. Woodruff Sawyer: Looking Ahead to 2022
4. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021
5. https://securityintelligence.com/news/ransomware-costs-expected-265-billion-2031/
6. https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority
7. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
8. Sophos State of Ransomware 2021 Report
9. Black Kite Third Party Breach Report
10. Argon Supply Chain Attacks Study
11. https://www.forrester.com/blogs/predictions-2022-continued-uncertainty-forces-attention-on-securing-relationships/
12. Evident State of Third-Party Insurance Verification Report
13. https://www.fitchratings.com/research/us-public-finance/rising-insurance-costs-add-to-us-public-finance-cyber-pressures-18-11-2021
14. Cisco Cybersecurity Threat Trends Report 2021
15. Gartner: An Executive Leader's Guide to Cybersecurity Insurance
16. https://www.backblaze.com/blog/the-true-cost-of-ransomware/
17. https://www.gao.gov/assets/gao-21-477.pdf
18. https://processbolt.com/cybersecurity-predictions-2022

ABOUT BLACK KITE

One in four organizations suffered from a cyber attack in the last year, resulting in production, reputation and financial losses. The real problem is adversaries attack companies via third parties, island-hopping their way into target organizations. At Black Kite, we're redefining vendor risk management with the world's first global third-party cyber risk monitoring platform, built from a hacker's perspective.

With 350+ customers across the globe and counting, we're committed to improving the health and safety of the entire planet's cyber ecosystem with the industry's most accurate and comprehensive cyber intelligence. While other security ratings service (SRS) providers try to narrow the scope, Black Kite provides the only standards-based cyber risk assessments that analyze your supply chain's cybersecurity posture from three critical dimensions: technical, financial and compliance.

CONTACT US

info@blackkite.com

+1 (571) 335-0222

800 Boylston Street, Suite 2905
Boston, MA 02199