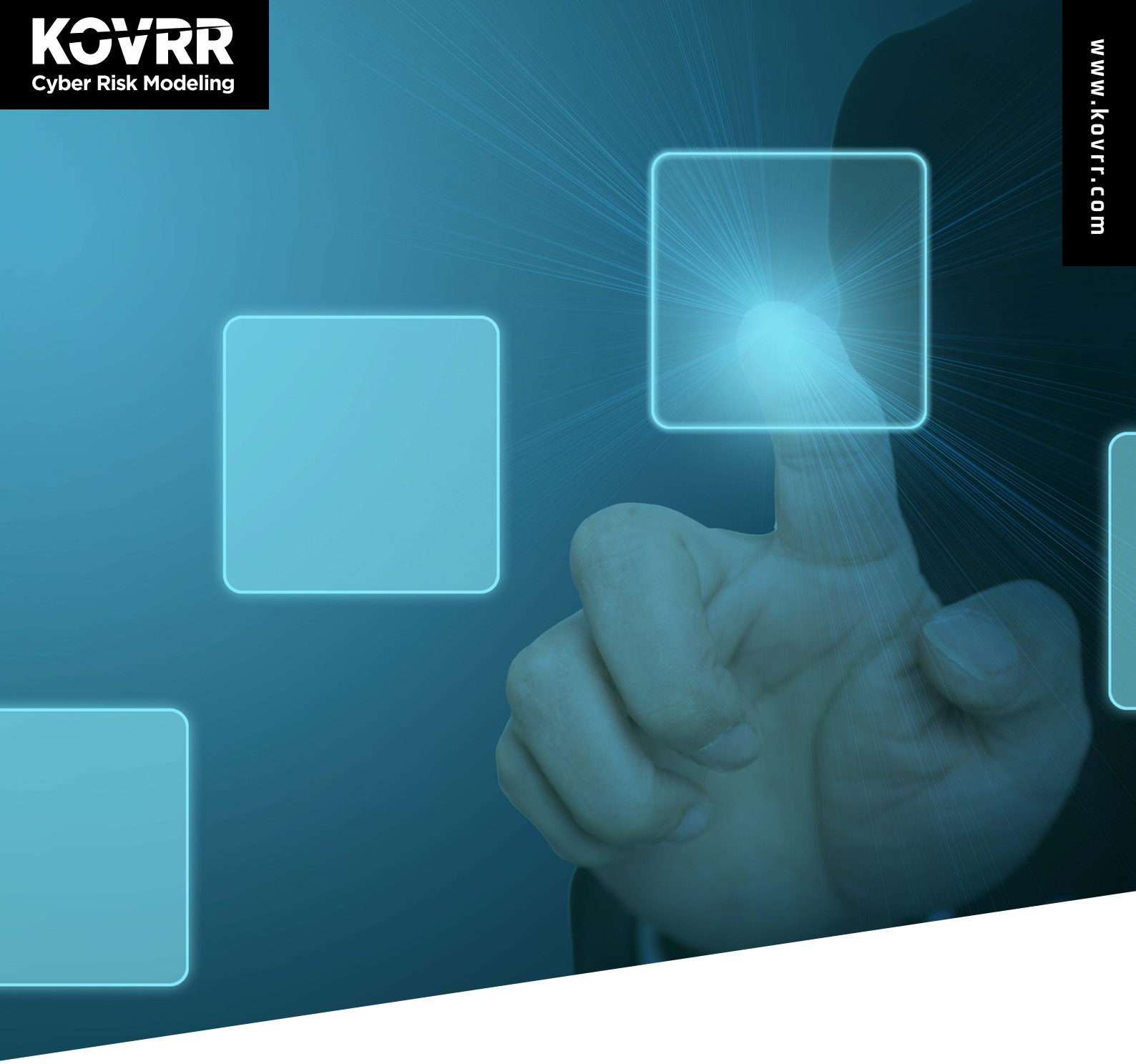
KOVRR
Cyber Risk Modeling

www.kovrr.com



7 Reports That Can Help You Understand the Cyber Insurance Landscape

DECEMBER 2021

The explosion of ransomware attacks and cybersecurity risk as a whole have made life tough for so many organizations across industries globally. Enterprises need to face these risks in what's often a challenging business market anyway, and turning to potential solutions like cyber insurance comes with its own difficulties. The cyber insurance market continues to harden, with insurers facing eroding margins and often struggling to quantify the risk enterprises face.

But it's not all bad news. Cyber insurance companies and other enterprises who want to know the cyber landscape better have a wide range of resources to turn to. As the market matures, many quality research reports have emerged, including several that provide overviews and predictions for what will happen within cyber insurance and cybersecurity as a whole for 2021 and beyond.

But which of these research reports should you read to strengthen your cyber knowledge and feel more prepared for what may come? In this article, we'll provide a brief overview of seven of the top cyber insurance research reports for you to consider diving into more.

1 Munich Re
Cyber insurance: Risks and trends 2021

In the report "Cyber insurance: Risks and trends 2021," the reinsurer Munich Re shares the results of the company's first "Global Cyber Risk and Insurance Survey."

Some of the key findings include that amidst rapid digitization within companies, approximately four out of five C-suite executives do not think their company has adequate cyber threat protection. The top cyber threats feared by this group include fraud, data breaches and ransomware.

The survey also finds gaps in cyber insurance knowledge, but the market could soon grow, with 35% of C-level respondents likely to soon take out a policy.

Munich Re also notes the importance of cyber risk accumulation. While the company mentions its own accumulation models, "it is important to monitor the market and seek external expertise from different vendors in order to assure state of the art accumulation management," the company says.

2 AON
Cyber insurance Market Insights Q1 2021

In one report from Aon, "Cyber Insurance Market Insights Q1 2021," the firm highlights how the cyber insurance industry is changing amidst evolving cyber risks. In particular, the company highlights how issues such as ransomware, silent cyber exposure and the SolarWinds event have affected the cyber insurance market.

With SolarWinds, for example, the "theft of investigative tools from a globally recognised cyber security and forensics firm is likely to lead to improved hacking tools in the hands of cyber criminals," notes Aon.

Amidst this backdrop, Aon sees more hardening within the market through 2021 and 2022. Insurers are looking closely at their underwriting practices while also assessing retention, limits and premiums to figure out the right mix to make cyber insurance viable.

3 AON
2021 Cyber Security Risk Report

Another report by Aon, the "2021 Cyber Security Risk Report," focuses more on the overall risk landscape from an enterprise perspective. In particular, Aon highlights four main cyber-related risks facing organizations today:

- **Digitization:** As companies rapidly digitize, particularly with Covid-19 changing the way many companies work, only 40% say they have "adequate remote work strategies to manage this risk."
- **Third-Party Risk:** Organizations need to be aware of risks in their supply chains and among the various vendors they work with, yet only 21% have implemented "baseline measures" to oversee third-party risk.
- **Ransomware:** Ransomware attacks have been prevalent and damaging recently, and many are unprepared. Less than one-third of organizations say they've implemented "adequate business resilience measures" to handle this risk.
- **Regulation:** As stronger data security laws come into place, organizations need to be mindful of how they manage data and comply with relevant laws. The Aon survey finds 36% have adequate data security preparedness.

4 Marsh
Cyber trends and predictions in 2021

A report from insurance and risk management firm Marsh, "Cyber trends and predictions in 2021," highlights some of the top cyber issues that organizations may need to pay more attention to.

For example, many companies use managed service providers (MSPs) to handle their IT needs, yet an increase in cyber attacks on MSPs means many organizations could be at risk. Other issues include changing cybersecurity regulation, such as with Australia's Security Legislation Amendment (Critical Infrastructure) Bill 2020. The bill expands what's considered to be critical infrastructure, which would then mean facing stronger cybersecurity measures.

Moreover, in addition to looking at issues that seem to be common across many reports, like the growth of remote working and ransomware, this report also examines some issues that don't necessarily get as much attention, such as hyper automation.

5 AdvisorSmith
Cyber Insurance Market Update

This mid-2021 review, "Cyber Insurance Market Update," looks at some of the top trends related to cyber insurance.

In addition to noting the rise of cyberattacks, including major ransomware incidents, AdvisorSmith points to a growing demand for cyber insurance, both in terms of the number of policies written and the total amount in premiums. The company notes that mid-size and large businesses have faced the highest premium increases.

At the same time, insurers are also scrutinizing cyber policies more, such as with some putting in more stringent limits and/or putting in more "restrictive policy terms and including additional exclusions to their cyber and non-cyber policies," notes AdvisorSmith.

6 U.S. GAO
Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market

A report from the U.S. Government Accountability Office (GAO), "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market," examines some of the key trends in the cyber insurance space.

For example, some insurance companies are seeing higher take-up rates for cyber policies, which coincides with a trend for insurers to offer cyber-specific policies, instead of putting this coverage into another type of policy.

At the same time, however, the cyber insurance industry has trended toward higher prices, due in part to more demand and more cyberattacks. In many cases insurers are also reducing coverage limits to account for the increase in cyberattacks.

7 Gallagher
2021 Cyber Insurance Market Conditions Report

Another piece of research, the "2021 Cyber Insurance Market Conditions Report" from insurance, risk management and consulting company Gallagher, examines what's happening in cyber insurance.

In particular, Gallagher notes that the cyber insurance market started to significantly harden in 2020 and that could continue even more in 2021. With more attacks, including on companies such as managed security service providers, which handle security for multiple organizations, cyber insurers have had to adapt.

For one, Gallagher projects 15-50% higher cyber insurance prices. The company also foresees more underwriting scrutiny. "We will see a wider underwriting lens that will expand to an increasing use of loss modeling tools and continual system scanning, utilizing both in-house and outsourced IT security resources as they evaluate prospective insureds," says Gallagher.

Some companies also may take on more retentions and might take advantage of pre-breach services from insurers to reduce their risk.

What's Next for Cyber?

As these reports show, the cyber insurance and broader cybersecurity landscape are changing rapidly. Insurers and enterprises need to keep an eye out on what's to come so they can reduce the risk of unexpected events derailing their businesses.

In addition to learning more about what's happening in the broader market, insurers and enterprises also increasingly need to quantify their own cyber risk so they know what they're up against. Insurance-validated models like Kovrr's include data from both insurers and enterprises to continually assess cyber events and predict what the financial impact of cyber events could be and how they may financially impact your business.

> Want to learn more about how to prepare for cyber events? Kovrr's cyber risk modeling capabilities can help. Get in touch today to quantify your cyber risk.

KOVRR
Cyber Risk Modeling

The Author

Yakir Golan

CEO

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.

To learn more please contact the Kovrr team: contact@kovrr.com