MANDIANT
NOW PART OF Google Cloud

THREAT INTELLIGENCE
WHITE PAPER

Minimizing Risk to Obtain Cyber Insurance

The content in this document was originally published in The Defender's Advantage Cyber Snapshot Issue 3.

U.S. banks identified $1.2 billion in ransomware transactions across 1,489 reports to regulators in 2021– a steep increase from $416 million across 487 reports the previous year.[4]

Ransomware payments more than doubled between 2020-2021[1] forcing insurers to take bigger losses and sending the cybersecurity insurance market on a volatile path that has only recently begun to stabilize. And while the end of 2022 saw an 80% deceleration in cyber insurance rate increases, improving market outlook for 2023[2], most carriers believe cyber risk will continue to rise as ransomware remains a top threat[3]. As a result, organizations can expect increased scrutiny during the underwriting process on their security controls and internal processes and procedures concerning cyber risk. Additionally, there remain troubling exclusions for widespread events (i.e., Log4j) and incidents that can be tracked to the war in Ukraine or nation-state sponsored attack groups. In fact, carriers continue to reduce or even exclude ransomware-related coverages if the organization fails to demonstrate adequate controls in managing this risk.

Over the last 12 months, Mandiant has seen an increase in cyber insurer involvement during incident response engagements. While CISOs are not consistently consulted in policy coverage decisions, we recommend CISOs work hand-in-hand with an organization's risk manager and legal counsel to ensure accuracy in the application process and review policies so they are not caught off-guard during a breach.

Cyber Insurance 101

In the mid-2000s, insurers expanded coverage to reimburse companies for the costs of cyber attacks that directly affected their business[5]. Since then, expanded coverage has become a useful tool for financial risk managers and cybersecurity leaders to mitigate risk and offset costs from data breaches or other security incidents. Policies generally cover cyber risk to the company (first-party risk) and liability from consumers or businesses (third-party liability). Initially, underwriting for cyber insurance focused on the costs associated with data breaches and as such, organizations were required to provide information about the types of records, client data, and regulated data they processed to the underwriters and certifying compliance to regulatory standards like HIPAA and PCI DSS. Ransomware and multifaceted extortion pose an additional risk of business interruption that can cripple a business and generate substantial costs.

1. Wall Street Journal, Reported Ransomware Incidents, Cost Soard in 2021, Treasury Says, November 4, 2022
2. Marsh, US Cyber Insurance Market Update Signs of improvement in third quarter of 2022, October 7, 2022
3. Woodruf Sawyer, 2023 Property & Casualty Looking Ahead Guide, January 10, 2023
4. Wall Street Journal, Reported Ransomware Incidents, Cost Soard in 2021, Treasury Says, November 4, 2022
5. The Federal Reserve Bank of Chicago, Chicago Fed Letter, No. 426, 2019 The Growth and Challenges of Cyber Insurance, 2019

TABLE 1: Common Cybersecurity Risk Coverages.

First-Party Coverage	Third-Party Liability
Incident Response and Forensic Fees	Security and Privacy Liability
Notification, Credit and Identity Monitoring	Multimedia/Media Communications Liability
Data Recovery	Regulatory Defense and Penalties
Business Interruption	PCI DSS Liability
Cyber Extortion and Cyber Crime	Telephone Consumer Protection act Defense
Reputational Damage	

*Source: Honigman LLP Attorneys and Counselors, Cyber Insurance 101, May 19, 2021

As a result, insurers have sharpened their pencils to take a deeper look at an organization's technical controls and mitigation activities against interruption and other associated business loss. This translates to a rigorous underwriting process to determine risk and policy pricing. Today, underwriting involves additional questions, interviews, and submitting to external scanning of your environment.

Beth Burgin Waller, Chair of the Cybersecurity and Data Privacy Practice at Woods Rogers, who spends significant time reviewing and negotiating cyber insurance for clients in addition to being incident response counsel, recommends working with your risk management team and legal to prepare for the underwriting process.

Underwriting questionnaires often include black and white questions that don't apply to today's complex multi-cloud, multi-network corporate infrastructures. For example, when answering a question about whether you have multi-factor authentication (MFA) across the enterprise, your underwriters may ask for proof that MFA is present in every part of the enterprise from back-ups, to cloud business applications and the VPN. Your counsel and risk management team can help flag sweeping statements made in the application and assist with supplemental responses that clarify current production controls and any plans for improvement.

Understanding nuance of IR coverage

Burgin Waller highly recommends reviewing the specimen (sample) policy. "As the market stabilizes, cyber policy language is standardizing similar to other insurance policy products," says Burgin Waller. The sample policy may indicate you have business interruption coverage to a certain limit, but without careful examination of the specimen policy, you may have exclusions built into the policy for legacy software, widespread events such as Log4j, or the latest exclusion–acts of war, covering incidents attributed to nation-state threat actors. Burgin Waller suggests paying particular attention to policy sub-limits. In one example, a base-level cyber policy included a sub-limit for incidents initiated via phishing and expected the organization to have supplemental coverage for ransomware. "A careful read of your specimen policy on the front end," says Burgin Waller, "can save you significant headaches during an incident by clarifying what may or may not be covered for your organization in advance of an incident."

Can you expect the incident response provider and associated costs to be covered? Mandiant incident responders encounter three common scenarios:

1. The IR provider is an approved vendor with pre-negotiated rates. This streamlines kicking off the engagements and can make it easier for clients to submit claims.
2. The IR provider is not pre-approved and the insurer will cover $x/hour. The client will have to make up the difference if the IR rate is higher than the covered amount.
3. The IR provider is not pre-approved and the insurer won't provide any coverage if that IR provider is used. This scenario can create the most disruption during a breach event.

It is important to review the specimen policies for coverage of the entire incident response process. Some policies only cover the investigation, and exclude ransomware payouts, general counsel costs, or costs associated with recovery and long-term remediation efforts. Additionally, insurance carriers may not cover a full investigation to determine exactly how an attacker got in and to verify that they didn't leave any backdoors that would make the client vulnerable to reinfection. At that point, it becomes a business decision on whether to move forward with a deep investigation aimed at reducing future risk.

A new approach

Overall the cyber insurance market is maturing such that providers are partnering with their customers to enhance overall cyber resilience. The insurance industry has very advanced risk modeling programs that are being applied to help make organizations safer.

Many insurance partners offer a set of vendors and solutions they have vetted to help their customers navigate the cybersecurity marketplace and reduce risk by employing technologies that have demonstrated effectiveness.

Insurance partners have even identified security controls that can make a positive impact on an organization's cyber risk and related policy costs[6]. Mandiant embraces recommendations from the insurance industry and highlights the following five practices that, properly implemented, can mitigate the impact of or prevent typical attacks:

1. **Multi-factor authentication:** MFA, or two-factor authentication, is a technology that combines two or more independent credentials (e.g., passwords, security tokens, and face or fingerprints) to provide user access. Throughout numerous incident response investigations, Mandiant has observed that while organizations have increased their adoption of traditional MFA methods, attackers continue to advance threat tactics to compromise identities. Implementing strong MFA tools and methods – such as number matching, contextual telemetry notifications, and inputting time-based one-time passwords (TOTPs) – across all externally accessible login portals and for any sensitive internal applications can reduce risks of common adversarial initial access techniques.
2. **Identity and privileged access management:** Identity is the new security boundary in today's hybrid operational model. Mandiant sees the compromise of directory and access management systems in many incident response engagements. These systems are often used by threat actors to escalate privileges. Organizations should ensure users and systems have proper access and that directory and access management systems are properly configured to prevent unauthorized privileged access escalation.
3. **Secured, encrypted, and tested backups:** Mandiant recommends organizations have a tested plan for securing and encrypting backups to facilitate restoration of systems and data in the event of a cyber attack. Backup and external storage solutions can help decrease the likelihood of IP loss and ensure valuable records are protected from loss. Companies are increasingly using cloud service solutions as a way to maintain a copy of their cloud or hybrid networks in case of a cyber attack that would otherwise stall operations.

4. **Cyber incident response planning and testing:** Mandiant views cyber incident response planning and testing as a critical activity involving the review of existing technical controls, network architectures, and first response capabilities. Mandiant suggests developing plans for typical response scenarios and continuously validating cyber defense capabilities to enable rapid containment in the event of an incident.
5. **Retain legal and incident response partners:** An important part of cyber incident response planning is being prepared to engage outside support to protect the company from legal risks and obtain expertise in incident response. Legal counsel–especially those focused on cyber issues–should be able to work seamlessly with forensic responders in the event of an attack to assess legal liability and risks that may arise from the event. External incident response support can significantly reduce the response time, thereby reducing the impact of a breach. An Incident Response Retainer (IRR) allows companies to agree upon terms and conditions for incident response services before a cyber security incident is suspected.

Insurance partners also offer security consulting and services to help navigate the application process. Many brokers and carriers are differentiating their services by extending their consultancy with assessments, cyber hygiene, and processes needed to develop effective defensive capabilities.

Get more help navigating cyber insurance from Mandiant partners, podcasts, webinars and Google Cyber Risk offers.

Read more articles from **The Defender's Advantage Cyber Snapshot**.

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud