beazley

Article

Cybersecurity steps to help decrease incidents

Craig Linton • August 23, 2023

As we enter the second half of 2023, the cyber claims data in our Cyber Services Snapshot continues to show a steady number of ransomware incidents, with data exfiltration a key component in nearly 90% of claims. While ransomware has been a persistent theme over the past few years, our Claims and Cyber Services professionals are still handling a large number of matters resulting from business email compromise (BEC) and fraudulent payment instructions.

Despite these trends, we have seen a reduction in frequency and severity from the improved cybersecurity controls that our policyholders have undertaken. In 2020, we began to increase the scrutiny of cybersecurity controls on the accounts that we underwrite, asking more detailed questions and requiring a more sophisticated security approach from our policyholders. Just a few years later, we are already seeing that this approach is having a meaningful, positive impact on our policyholders as it has reduced the likelihood of them suffering a cyber incident.

What cybersecurity controls seem to be having the most impact?

There is no silver bullet that will protect our policyholders from all cybersecurity threats, but we've seen a significant impact from focusing on two critical controls: implementation of Multi-Factor Authentication (MFA) and closure of Remote Desktop Protocol (RDP) ports. These two controls can prevent a number of different types of losses – not just ransomware.

While we are pleased to see that MFA is helping to protect our policyholders, it is important not to lose sight of other important cybersecurity controls, including screening emails for malicious attachments/links, providing a quarantine service for suspicious emails, implementing a Sender Policy Framework (SPF) and other email-integrity technologies, and sandboxing suspicious emails. Though the

cyber insurance industry as a whole is still seeing significant incidence of claims, the security steps taken by our policyholders appear to be reducing the frequency of ransomware claims – for the first time since 2021.

In the second quarter of 2021, RDP represented the most frequent threat for ransomware attacks. Just nine months later, the frequency at which RDP is used as an access point for ransomware attacks is the lowest we've seen since the first quarter of 2021, when we began keeping records. We have little doubt that this attack route is still attractive to cybercriminals, but the reduction in RDP-based attacks reflects our insistence that policyholders close RDP ports and thereby remove this attack route. Insistence, however, is not enough; remediating RDP as an attack route has required significant support from our Cyber Services Team, which has helped us to educate and retain policyholders by making us part of the security solution for our clients, beyond simply being their insurance provider.

What should we be protecting against next?

Though some emerging cyber trends are too fresh to be reflected in our claims data just yet, there are three broad trends that we expect to see:

- We anticipate that artificial intelligence (AI) risks, especially those risks associated with the use of generative-AI, and intellectual property theft will be on the rise.
- While phishing has been a long-standing attack method, we may see attackers slowly transition away from this method of "initial access" in favor of other tactics. For example, cyber criminals are purchasing and weaponizing zero-day (previously unknown) exploits that bypass the need for a user to fall victim to a phishing attack.
- Attackers are becoming increasingly specialized, with Initial Access Brokers procuring access to a victim's system and then selling that access to a ransomware gang or other cyber- criminal. It is clear that internet-facing systems (i.e. systems that are accessed via the internet, including web applications, Virtual Private Network (VPN) gateways, cloud services, etc.) will continue to be key targets[1].

In addition to these three broad trends, we expect that third-party risk will be a major trend in the years to come. It is not enough for our policyholders to focus on their own systems; they also need to consider how much they rely on third-party suppliers, and whether their systems are resilient and properly secured. As policyholders increasingly utilize third parties, it is important that they know and understand that they are exchanging some risks for others. While there are many benefits of relying on cloud service providers – increased uptime, automation of patch management, and professional security monitoring – the cloud is not without its pitfalls – misconfigurations, aggregation issues, lack of control over resources – to name a few. Therefore, it is incumbent on policyholders to conduct and frequently refresh their financial evaluation of their electronic threats when applying for and determining the scope of their cyber insurance needs.

How do we help our policyholders?

Our underwriters and our Cyber Services Team are continuously working with our policyholders to help them understand their cybersecurity position and what areas should be prioritized for improvement. For example, when a client applicant answers our application questions, we get a holistic view of their cybersecurity position. Any deficiencies that we discover during the underwriting process can drive a conversation with our Cyber Services Team, who are then able to work with our future policyholders to remediate potential issues before the policy is bound.

The resources that we have invested to identify, track, and remediate cybersecurity vulnerabilities on behalf of our policyholders are paying off. Of course, as the cyber threat landscape continues to evolve, we will likewise need to identify new threats, track their propagation, and develop solutions for our policyholders. So far, it has been good to see our “long game” efforts pay off for our policyholders in the form of reduced claim frequency and severity. We look forward to continuing to forge strong relationships with our policyholders in our continuous drive to help them protect their business against the ever evolving cybersecurity threats that they face.

Craig Linton

Head of US Underwriting Management

[1] The Current Risk Landscape | beazley

1 Back to "Spotlight On Cyber and Technology Risks 2023"

beazley