aunalytics

Cyber Insurance Continues to Skyrocket—Do You Have a Documentable Security Strategy in Place to Show You're Prepared?

By: Katie Horvath, CMO, Aunalytics, Inc.

> Cyber risk is a growing critical concern for organizations of all sizes and public entities globally, as we continue to rely on information technology and digital devices.

Ransomware, malware, phishing activity, and network intrusions pose unabated threats that increase the need for more protection and defensive tactics. In addition to taking security measures, businesses are purchasing cybersecurity liability insurance to help counter any potential losses from cyberattacks. But in the wake of steadily rising digital threats, cyber insurance is getting increasingly expensive—and difficult—for companies to procure.

In addition to businesses, local governments and states are finding that cyber insurance premiums are skyrocketing and that they must meet stricter guidelines if they want to get coverage or renew their policies. One county in South Carolina was shocked earlier this year when it discovered its cyber insurance premium would be spiking from $70,000 last year to about $210,000. And if it couldn't satisfy the insurance company's requirements and prove the county had the robust controls needed to protect and defend itself against cyberattacks, it wouldn't be able to secure its $5 million policy renewal at all.

Cyber Insurance Rates Are Increasing

Cyber insurance used to be relatively inexpensive, but that is changing. Insurance companies are increasing their rates dramatically, raising the bar and making it harder to obtain—if not impossible. Higher premiums for both public and private organizations are a result of rising demand for coverage in light of frequent and costly cybercrime incidents. The FBI reported in May that more than US $43 billion has been lost through business email compromise attacks since 2016.

> Higher premiums for both public and private organizations are a result of rising demand for coverage in light of frequent and costly cybercrime incidents.

Insurers have had to pay out more, resulting in more expensive premiums and tighter standards for getting a policy. Some companies have also lowered caps on coverage or limited how many policies they write.

An IDC Survey identifies the following emerging trends:

- Cyber insurance is being utilized by a slight majority of organizations worldwide with **70% required to have a separate policy for ransomware**.
- Cyber insurance **premiums are expected to increase in 2023,** and cyberinsurers continue to use self-assessment forms for 44% of organizations.
- The majority, **91%, of organizations need an assessment before buying cyber insurance**, and a number of cyber insurers are leveraging cybersecurity service providers.

Many cyber policies include exclusionary language related to certain types of software and email platforms with known vulnerabilities. If an organization has not invested in remediating these weaknesses or has experienced a recent network intrusion, it portrays substandard cybersecurity and related controls. In that case, insurance may not be available at all without investments to buttress vulnerable IT systems against attacks.

Security Strategy Checklist

It is not surprising then, that organizations with a demonstrable and documented strategy for protecting their data against cyber threats are in a better position to ensure the insurance renewals they've come to expect, albeit, at a higher cost. Here is what your security strategy should include:

- □ Employ 24/7/365 monitoring with remote remediation to quickly stop attacks in their tracks.
- □ Push patches frequently so that user devices are equipped with the latest security protections.
- □ Monitor cloud security including application use across the organization to be on the lookout for atypical user behavior signaling an attack.
- □ Continuously update security technology and protocols as threats evolve and adapt. This means you need a dedicated full-time security team—not an overworked IT department handling system stability and help desk, while also trying to keep abreast of the latest security threats and technologies, piecing together security tools as a solution. This is not a solution.
- □ Train employees on cybersecurity threats quarterly.
- □ Monitor endpoint devices to stop attacks before they hit networks. User devices are the most likely entry point for attackers to compromise an enterprise due to the high propensity for innocent user error opening doors.
- □ Monitor email and Office 365 using tools specially designed to thwart attacks on these platforms, such as expertly recognizing and removing phishing scams before employees have an opportunity to unleash horrible consequences with a rogue mistaken click.
- □ Have a dedicated security team and SOC, or hire an expert outside managed security services firm that embeds tools, technology, and 24/7/365 monitoring to serve as your SOC. This has been a must for highly regulated industries, and now applies to everyone.
- □ Develop a solid business recovery plan for when an attack occurs.
- □ Adopt deep learning or AI monitoring, mitigation and context investigation that can more quickly identify threats.
- □ Encrypt data so that it is not compromised even if a breach occurs.
- □ Use multi-factor authentication to protect against unauthorized access.
- □ Instruct employees and customers to only access data in a secure location over a non-public Internet connection.

Conclusion

Many companies and public entities may find such a checklist to be daunting, particularly midmarket businesses. Having a dedicated security team in place, for example, can by itself be a large and expensive undertaking. Rather than hiring and trying to retain these highly skilled and scarce engineers, partnering with a security services provider transfers the high cost of maintaining this talent to the services partner. This is one way to check off the list of requirements associated with implementing a strong security posture that you can document—one that not only facilitates insurance renewals, but keeps your business running smoothly with minimum downtime due to cyber threats.

About Aunalytics

Aunalytics is a leading data management and analytics company delivering Insights-as-a-Service for mid-sized businesses and enterprises. Selected for the prestigious Inc. 5000 list for two consecutive years as one of the nation’s fastest growing companies, Aunalytics offers managed IT services and managed analytics services, private cloud services, and a private cloud-native data platform for data management and analytics. The platform is built for universal data access, advanced analytics and AI—unifying distributed data silos into a single source of truth for highly accurate, actionable business information. Its Daybreak™ industry intelligent data mart combined with the power of the Aunalytics data platform provides industry-specific data models with built-in queries and AI for accurate mission-critical insights. To solve the talent gap that so many mid-sized businesses and enterprises located in secondary markets face, Aunalytics’ side-by-side digital transformation model provides the technical talent needed for data management and analytics success in addition to its innovative technologies and tools. To learn more contact us at +1 855-799-DATA or visit Aunalytics at https://www.aunalytics.com or on Twitter and LinkedIn.