APPSIAN SECURITY

EXECUTIVE BRIEF

Understanding Cyber Liability Insurance: Securing System Access to Secure Coverage

Piyush Pandey • CEO at Appsian

Organizations purchase cyber liability insurance as a way to mitigate the impact of data security incidents. However, as with any liability policy, cyber risk insurance incorporates a set of exclusions that allow insurance companies to deny coverage. While most policyholders and insurance professionals assume that external monitoring acts as the only way to ensure coverage and reduce the likelihood of costly coverage litigation, digital transformation has shifted the perimeter away from external controls such as firewalls towards a more focused approach on identity and access.

Understanding Cyber Insurance Exclusions

Everyone reads the Insuring Agreement or the part of an insurance policy that provides coverage. Typically, this section lists out all of the events for which an organization can submit a claim. For example, many cyber insurance policies will cover unauthorized access to systems, networks, and software that leads to a data security event.

However, as in life, all promises come with conditions. In the insurance world, conditions are called the exclusions, or the activities that are reasons allowing an insurance company to deny coverage. Generally located at the end of a policy, these may seem logical. For example, in a cyber-risk policy, an insurer does not need to cover the loss if the policyholder failed to enforce reasonable security practices and systems maintenance procedures.

In other words, if a data security event is the result of failure to enforce best security practices, the insurance company can deny the claim.

Why Identity and Access Matter to Data Security

As evidenced by the recent Twitter breach, cybercriminals increasingly target users as a way to gain unauthorized access to privileged locations in an organization's IT ecosystem. This tactic makes sense in many ways because privileged accounts traditionally have universal access to an organization's most important services and data.

For example, to do their job, IT administrators need nearly unfettered access to an organization's ecosystem. They need to create accounts and grant access to other users. However, that also makes them a high-risk user. They could conceivably create fake accounts and grant themselves privileged access then engage in malicious data theft or credential theft, moving around in the organization's systems and networks without looking suspicious.

Similar to the Twitter breach, this type of activity is hard to recognize unless the organization is actively monitoring who has access, how they use their access, what they access, and why they need it.

Enforcing Identity and Access Controls as Data Security Best Practices

Data security best practices pose problems for organizations as no set definition exists because cybercriminals continue to evolve their methodologies. With most organizations embracing remote workforces for the foreseeable future, on-premises security controls no longer provide the necessary protection. In order to secure data and protect privacy, companies should look to the Identity perimeter to limit access and monitor privileged access within their ecosystems.

Enable Zero Trust

Zero trust, aka “never trust, always verify,” is a cornerstone of enforcing identity. This is widely becoming not just best practice, but a table stakes identity and access management strategy – especially for users with elevated privileges. In a business application landscape overrun by phishing and brute force attacks, there is little confidence in usernames and passwords being the primary driver for identity and access management. That’s not to say that usernames and passwords don’t have their seat at the table, but they can’t be sitting alone. Combining them with dynamic controls that evaluate the context of access to determine risk is critical. Trusting the same access privileges, no matter what the circumstances, will lead to security threats. IT leaders must assume that cybercrime can circumvent their perimeter identity controls and be acting accordingly.

Apply the Principle of Least Privilege (PoLP)

The first step to creating best Identity and Access Management (IAM) practices is to ensure all users have only the access they need to fulfill their job functions and nothing more. For example, someone in human resources (HR) might need access to an employee's address, but that individual may not need all the banking information attached to the record if they are not in the payroll area.

Enabling PoLP Using Attribute-Based Access Controls

For legacy business applications, PoLP is a non-starter because access governance is dictated by static, roles-based access controls (RBAC). For example, an HR manager needs a certain set of rights within the organization's system. However, RBAC only limits access based on what the user does in the company (unless manually changed). With attribute-based access controls (ABAC), organizations can set additional contextual attributes such as geographical location, IP address, or time of day. This additional context allows the organization to limit access to high-risk resources on a more detailed level. With the explosion of remote work, ABAC provides a way to limit users' access when the organization has determined that a location or time of day would be considered riskier. For example, someone using a public WiFi is at a higher risk of a man in the middle attack than someone using their home WiFi. If the organization sets trustworthy IP addresses, users cannot access sensitive information from public WiFis, reducing the attack surface.

Continuously Monitor Access

The same continuous monitoring mantra that exists at the network perimeter also holds true at the Identity perimeter. With user access monitoring, organizations can review the resources accessed to ensure they are appropriate to the users' needs. Organizations need a way to detect suspicious access to sensitive information. For example, if an HR representative is accessing healthcare information at 2:00 AM, the organization needs to know whether that employee typically works late at night or whether this is an outlier signaling a potential data security incident. Without visibility into when and how users interact with data, organizations cannot prove that they enforced their access policies as a best practice.

Digital Transformation, Remote Work, and Securing Coverage

Digital transformation, accelerated by the rapid move to remote workforces, streamlines productivity but also increases risks. With more users connecting more devices from more places at less regular times, identity and access is an integral part of an organization's data security.

Establishing and enforcing strict access policies is now more important than ever before. Malicious actors will continue to look for user accounts that act as back doors to organizations' systems, networks, and software. In order to secure cyber liability coverage, companies need to be more actively engaged in monitoring access and mitigating potential threats arising from compromised accounts.

Piyush Pandey, CEO at Appsian (www.appsian.com) is a technology executive with 19 years of global experience in strategy, sales, mergers & acquisitions, and operations within software companies. Over the last 10 years, he has worked with enterprise software companies including Oracle, Epicor, Concur, Citrix and Microsoft on various transactions. He has held various leadership positions at Procera, Deutsche Bank, Stifel, Wipro Technologies and a wireless startup.

This article was originally published at Global Trade Magazine

APPSIAN SECURITY

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

+1 (469) 906-2100

info@appsian.com

www.appsian.com