Henderson Brothers, Inc. White Paper

Cyber Liability & Multi-Factor Authentication

In a post-SolarWinds world, what do you need to know now about your application for cyber liability insurance?

Throughout December 2020, the cyberattack of the major tech firm, SolarWinds, came to light. As the situation unfolded, we learned more about the extent of that attack and the other organizations potentially affected—FireEye, Microsoft, the Department of Homeland Security, and the U.S. Treasury. The significance and breadth of this event, at least from the perspective of the cyber liability insurance market, could not be understated. Many large 1-1-2021 renewals were impacted, and many more questions began to be asked by insurers relative to internal controls and protocol.

HENDERSON BROTHERS®

Since the calendar flipped to 2021, not much has changed in that buying process. The applications are more comprehensive, coverage forms are adjusting, and the availability of limits for single insured are somewhat scaled back. Considering this, you may ask what do I need to know now for my organization's own cyber liability application/policy? To answer this, we first start with the basics of the cyber liability application. A typical, pre-SolarWinds, application included a few questions aimed at whether basic security tenants existed. The carriers would ask regarding the existence of firewalls, the types and amount of data records the organization stores, and the organization's practices for back-ups and log monitoring. These questions were very much binary. Does the organization do these things or not? Now, post-SolarWinds, these legacy questions remain, but the underwriters are digging much deeper for new categories of questions and qualitative responses—not a binary yes/no. Some of these post-SolarWinds application questions were are observing now are for the organization to:

- Identify specific encryption software(s) used and the bit level,
- Describe whether you do and how you do asset tracking for laptops, mobile devices, and virtual machines,
- Explain how the organization handles its wireless networks (internal and external) (new and more questions than in the past),
- Specific to the issues resulting from SolarWinds, describe in detail the organizations' patch management procedures,
- Identify its social engineering testing and training program(s),
- Explain how the organization handles vendor and other third-party network access (new and more questions than in the past), and
- Confirm whether the organization has implemented Multi-Factor Authentication (MFA)
- Has the organization implemented a formal Incident Response Plan and has the plan been tested?
- What type of Business Continuity Planning is in place?

These items are not only illuminating for the underwriters, but they are also helpful guideposts for the organization to assess its security posture. Conceptually, this is what the underwriters are now driving toward more than ever—that the insured at least has the architecture and systems in place to defend against the most modern malware and cyberattack methods. As a result, even

though carriers are keeping applications somewhat abbreviated, the questions and responses are much more technical in nature. This means your tech staff, risk management staff, finance team, and your insurance partners all need to be able to understand the organization's security posture and articulate that out to the now more dynamic markets.

In our most recent observations, patch management and MFA seem to be the most critical. In relation to MFA, we know that it may be difficult to install, configure and deploy to all employees. To that end, and to help organizations achieve MFA more efficiently, we suggest considering some outside resources. For instance, it is possible to purchase software licensing and internally implement MFA, but it is recommended to use a local information technology partner to assist with deploying,

testing and training the new MFA solution. MFA integrates with a company's directory service (Microsoft Active Directory as an example) and this integration could have negative implications if improperly deployed. Using a local IT partner that has experience working with many organizations in multiple business verticals is very important to ensure compliance requirements are understood and met with any MFA implementation. There are many MFA solutions on the market today, but some suggested options are:

1. DUO: (Multi-Factor Authentication (MFA) | Duo Security)
2. Ping ID: (PingID MFA (pingidentity.com))
3. OKTA: (Multi-factor Authentication (MFA) Solution | Okta)

IT partners in Pittsburgh, PA with MFA implementation services are plentiful, but Ideal Integrations (Managed IT Services Company in Pittsburgh, PA | Ideal Integrations®) is a full-service solutions provider that has dedicated infrastructure and security practices that is very capable of deploying MFA solutions for any size company (local, national or global). If a large, national reseller is preferred for identifying and deploying a new MFA solution, companies can use partners such as Insight (Computer Hardware, Software, Technology Solutions | Insight) or CDW (CDW - Business Resources, Products and Solutions).

When evaluating a corporate MFA solution, it is also important to consider the implementation of a comprehensive Identity and Access Management (IAM) system. An IAM solution can deliver Multi Factor Authentication, but it will also provide a single location to manage enhanced security options such as:

1. Single Sign On
2. Password Management
3. Integration with cloud-based/Software as a Service applications

Recommended IAM solutions:

1. DUO
2. PingID
3. OKTA
4. OneLogin

Your organization may see non-renewals from current carriers and many declinations from new carriers if these security items are not implemented. Executing on these security protocols and initiatives, including training your staff, will not only help keep your cyber liability cost down but also make you insurable to more carriers. When cyber liability was a new insurance product, it was priced without much data to support the rates being charged to policy holders. Now that there is claims experience, the carriers are using the claims and cyber operations/security information to underwrite accurately with the possibility that premiums will increase or decrease as a reflection of the organization's risk. Thus, we would like to stress the importance of a robust cyber security posture. Cyber threats are ever evolving, and your cyber security controls and procedures need to keep pace with this changing landscape.

Contact a Henderson Brothers' Cyber Expert Today:

Jared Sadowski
Email: jjsadowski@hb1893.com
Phone: 412-754-3148

Dan Coast
Email: dmcoast@hb1893.com
Phone: 412-754-3279