TEXAS LAWYER

Texas Takeaways: Is Your Business a Good Candidate for Cyber Insurance?

Managers, partners, high ranking executives, owners and other decision-makers have the very important task of evaluating their risk and cybersecurity status and making the decision of whether or not they want to get cyber insurance.

By Kenneth Artz | May 19, 2022

Credit: Illus_man/Shutterstock

---

*I'm Kenneth Artz, and this is **Texas Takeaways**. We're always looking for feedback from our readers. Please send a note to kartz@alm.com with ideas, questions or comments. We look forward to keeping in touch!*

Unfortunately, in the world we live in today, firms that experience a cyberattack will feel an increased pressure to gather all the information, uncover the root of the issue and respond in a meaningful way without elevating the crisis, **Heather J. Oden (https://www.balljanik.com/our-team/heather-j-oden/)**, COO at **Ball Janik (https://www.balljanik.com/our-team/heather-j-oden/)** said in a **recent column (https://www.law.com/newyorklawjournal/2022/04/25/firms-bolstering-investment-in-cyber-insurance-to-transfer-risk/)**.

"We must be proactive as cyberattacks continue to cause widespread disruptions in business," Oden said.

"Cyber breaches continue to happen at an alarming rate, and we must be prepared," says Oden. "While we can't expect cyber insurance to fix all our issues, it does help provide an offset of the costs to respond if you are a victim of an attack; this is another tool to help us protect our firms."

A cyberattack on a law firm presents special concerns that ought to be considered well before the cyberattack hits, **Franklin Zemel (https://www.saul.com/attorneys/franklin-zemel)** and **Erik VanderWeyden (https://www.saul.com/attorneys/erik-vanderweyden)**, attorneys with **Saul Ewing Arnstein & Lehr (https://www.saul.com/attorneys/franklin-zemel)**, said in another **recent story (https://www.law.com/dailybusinessreview/2022/05/19/why-law-firms-should-not-pay-ransomware-demands/)**.

Texas Lawyer spoke recently on these topics with **Chad Hammond**, a security expert at **NordPass (https://nordpass.com/)**, a password manager which allows users to generate strong passwords and keep them in a secure vault.

NordPass helps users to stay one step ahead of a data breach and mitigate other cybersecurity threats with a business password manager, says Hammond. In addition, it also helps to secure credentials and easily apply company-wide settings to enforce a secure perimeter and focus on growing your business rather than worrying about the next potential cyberattack.

Why is cyber insurance important?

Chad Hammond: Cybercriminals are quick to adapt to the new normal: cybercrime is on the rise and the threat landscape grows ever more sophisticated by the day. Data breaches are also incredibly expensive. According to IBM, the average cost of a data breach was $4.24 million (https://www.ibm.com/account/reg/us-en/signup?formid=urx-50915&_ga=2.222449944.2059295313.1627595142-409667326.1627595142) in 2021.

On one hand, a long line of high-profile data breaches have demonstrated that digital security is not a given even among industry titans. On the other, the booming cybercrime industry is benefitting economies of scale, making smaller and smaller businesses more affordable and attractive targets.

Unfortunately that means that, now more than ever, no one is immune from a potential attack. Which is daunting given that the impact of a single cyber event can be devastating, threatening insolvency.

This is the reason why cyber insurance is becoming more important than ever. Companies are looking for a way to protect their businesses from the devastating impact of a possible cyberattack.

What does this mean for managing partners (MPs) and firm managers?

Managers, partners, high ranking executives, owners and other decision-makers have the very important task of evaluating their risk and cybersecurity status and making the decision of whether or not they want to get cyber insurance. This means that MPs have to be fully informed of their cybersecurity status and aware of any risk their business might face and the impact that a potential cyberattack can have.

What should MPs and firm managers be doing to determine if they should get cyber insurance?

MPs and firm managers should be evaluating the risks they might face and, overall, their cyberattack preparedness level.

Starting with risk assessment, first assuming that an attempted breach or attack is highly likely, they should then assess their vulnerabilities and the impact that an attack would have on their business. The higher the vulnerability and higher impact means higher risk — which is when cyber insurance is most needed.

Overall, because of the increase in frequency (likelihood) and cost of ransomware attacks (impact), the experts suggest cyber insurance in all cases.

In the meantime, what can MPs and firm managers do to increase their cyber hygiene?

A few cost-efficient policies can help companies get insured and save themselves from major crackdowns. These include but are not limited to the following:

1. **Adapting perimeter security practices -** A virtual private network (business VPN (https://nordvpn.com/)) service that is widely accessible in the market helps protect a company's privacy online and secure access to internet connection, creating an encrypted tunnel for data. Connecting to a business VPN is possible from anywhere in the world. Thus it addresses the risks insurance companies have concerning remote work options that a vast number of companies offer. Extensively used by both individuals and companies, this solution is often named among the critical go-to tools for cybersecurity.

2. **Setting password management rules -** The latest research (https://nordpass.com/business-executive-passwords/) by NordPass showcases that business executives have similarly poor password habits as regular internet users do. The most common password remains "123456," followed by other easy-to-crack variations of numbers and letters. While these can be guessed in less than a second, passwords, in general terms, are usually considered the most vulnerable place on a company's cybersecurity map. For this reason, insurers are likely to require a company to present proof of using password management (https://nordpass.com/business-password-manager/) software with safety protocols in place. This tool can also be connected to a multi-factor authenticator (MFA) for double security.

3. **Storing data in a secured environment -** Insurance companies are also concerned with data management within the client's organization. Data is an invaluable asset to most companies, and thus any compromise can cause significant losses. A secured cloud service (https://nordlocker.com/) that restricts access of third-party individuals helps ensure only company employees can view and manage documents, spreadsheets, or other stored materials.