FIRM MANAGEMENT

Remote Work and Cybersecurity Risk – Protect Clients Through Captive Insurance

The COVID-19 pandemic has drastically altered the workforce with companies across the country suddenly moving to a remote or semi-remote structure to protect their employees. The numbers of Americans working from home continues to rise, and ...

Jul. 27, 2020

The COVID-19 pandemic has drastically altered the workforce with companies across the country suddenly moving to a remote or semi-remote structure to protect their

employees. The numbers of Americans working from home continues to rise, and according to the latest Gallup Panel data, the percentage of workers who say their employer is offering them flex time or remote work options has grown from 39 percent to 57 percent since mid-March. Also, 62 percent of employed Americans currently say they have worked from home at some point during the crisis, a number that has doubled over the same time period.

Overall, studies find workers tend to prefer working from home. One of the biggest reasons cited is saving on commute time. A study by getAbstract found that on average, Americans spend roughly 27 minutes on their way commute into work equating to over 200 hours per year. And a joint CNBC/Change Research survey found employees have been spending the time they save commuting on valuable activities such as more time with family, more sleep, various hobbies and even getting more work done.

While a remote workforce has benefited employees and saves employers upwards of $11,000 per year per employee in reduced overhead, it does create vulnerability—companies are more susceptible to cybercrime.

The current pandemic climate provides a perfect storm for cybercrime to happen. A crisis like the coronavirus creates a sense of uncertainty, and combined with the use of new remote workforce technology, a business's systems are weakened. Also, even the most well-meaning employees can make mistakes leading to data breaches.

Employees working remote tend to pose risks in these five ways:

1. Scams in the form of phishing attacks are a leading cause of data breaches. Employees may unknowingly click on an email that seems legitimate but is really a hacker's email link or attachment, enabling the hacker to access important data.

2. An employee's remote access in a public setting can expose sensitive information. While teleworking, employees may be handling, accessing, discussing or transmitting sensitive data, including trade secrets, and confidential financial data.

3. Employees may transfer files between work and personal computers or devices. This could leave to sensitive information being stored on a device that the company doesn't have access to. In addition, failing to keep software up-to-date creates security issues.

4. **Employees may use passwords that aren't strong enough** or multi-factor authentication may not be in place which both can lead to passwords being cracked and sensitive information and data accessed.

5. **Remote-collaboration tools like Zoom and Google Hangouts** have experienced privacy issues and a problem known as Zoom bombing—where an outsider can join a virtual meeting. In some cases it allows the rogue person to access sensitive information. In other cases hackers target remote workers with fake Zoom downloaders.

A cybersecurity breach, such as the above examples, can decimate a business and be costly. Data breaches cost British Airways and Marriott each over $100 million. While these were high-profile and severe, a report from IBM and the Ponemon Institute found the average cost of a data breach has risen to $3.92 million. Small businesses are not immune to cybercrime. According to data from Accenture, 43 percent of cyberattacks are aimed at small businesses and cost $200,000 on average.

As trusted financial advisors, it's important for CPAs to help protect company revenue and health by advising clients on how to mitigate the risk of a cybersecurity breach—especially as more and more workers are working remote from home.

Businesses can prevent cyberattacks these ways:

- Educating employees
- Protecting passwords and utilizing multi-factor authentication
- Keeping systems updated
- Backing-up and configure all data and utilize data encryption
- Conducting regular risk assessments

These best practices are not bullet proof. Cyberattacks can still happen with these measures in place – employees are always a difficult variable and cyberattacks are ever-evolving. Criminals can harm even the most security-conscious businesses though. Another alternative is that a business can insure against this threat with cybersecurity insurance through a third-party commercial insurance company. However, commercial cyber policies often contain exclusions that limit their effectiveness. For example, many policies exclude cyber breaches due to employee error, which is the most common cause of a breach. So what is a business to do to protect company profitability? A business can supplement that insurance with a captive insurance company.

Captive Insurance: A Financial Strategy to Address Cybersecurity Risk

Captives can write broad coverage for data losses and insure gaps. And, if cyber-related losses don't occur, the company or business owner keeps the profits accrued in the captive insurance company.

A captive can also accumulate loss reserves and grow into another profit center for the business. This aspect of a captive insurance company is helpful in the event of a cyberattack since the loss reserves can be used to cover revenue loss. A company's leadership also has the option to liquidate the captive to fund the company through the fallout of the loss which can shield a company from potential bankruptcy.

Captive insurance companies also receive beneficial tax treatment. Taxes deferred on loss reserves enable the company to invest and grow a large pool of funds.

Lastly, as a licensed insurance company, a captive allows a business to gain access to reinsurance and excess insurance markets.

Captive Insurance is Vital to Financial Strength

The primary reason for a captive is risk management, but all risk management is financial. A financially strong captive insurance company is a powerful tool and it is why 90 percent of Fortune 1000 companies utilize captive insurance.

When it comes to crafting a risk management strategy for cybersecurity, it is critical for companies to recognize that the stakes are high and would-be data thieves are tireless and their craft is ever-evolving. This is not a place to cut corners. Businesses need robust strategies that combine active and passive safety measures with employee training and comprehensive insurance coverage that addresses all facets of cybersecurity risk.

==========

Randy Sadler started his career in risk management as an officer in the U.S. Army, where he was responsible for the training and safety of hundreds of soldiers and over 150 wheeled and tracked vehicles. He graduated from the U.S. Military Academy at West Point with a Bachelor of Science degree in International and Strategic History with a focus on U.S. – Chinese Relations in the 20th century. He has been a Principal with CIC Services, LLC for 7 years and consults directly with business owners, CEOs and CFOs in the formation of captive insurance programs for their respective businesses. CIC Services, LLC manages over 100 captives.

Firm Management • Technology • News

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.