THE PREFERRED PROVIDER TO THE MOST TRUSTED ADVISOR

Newsletter November 2022

Volume 3, Issue 11 4

National Network of Accountants, 6900 Jericho Turnpike, Syosset, NY 11791
www.nnaplan.com E-mail address: rroth@nnaplan.com
Offices located in Connecticut, Florida, New York, and Israel

THE REALITIES OF WORKING FROM HOME

By William York, VP of Marketing
National Network of Accountants

It appears that working remotely is a phenomenon that is here to stay. At least for the time being.

Gallop figures show that the September update on employment trends remains unchanged from the July and August period. This would suggest a holding pattern on remote working.

According to Gallop, statistics show that 45% of full-time U.S. employees worked from home either all (25%) or part of the time (20%). Gallop also suggests that these remote workers anticipate keeping their remote hours for the foreseeable future. Nine in ten want to maintain their remote work to some degree.

While a remote workforce has been beneficial to employees and at the same time saves employers upwards of $11,000 per year/per employee in reduced overhead, it can also create severe threats as companies are more susceptible to cybercrime.

The current work from home climate provides a perfect storm for cybercrime.

Employees working remotely tend to pose risks in five ways:

1. Scams in the form of phishing attacks are a leading cause of data breaches.
   Employees may unknowingly open an email that seems legitimate but is in fact 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 lead to sensitive information being stored on a device that the company does not have access to. In addition, failing to keep software up-to-date can also create security issues
4. Employees may use passwords that are not strong enough and multi-factor authentication may not be in place. Both can lead to passwords being decoded and sensitive information and data accessed
5. Remote-collaboration tools like Zoom 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 can target remote workers with **fake Zoom downloaders.**

A cybersecurity breach, such as the above examples, can be extremely costly and even prove to be fatal to a business. In 2022, the average cost of a data breach has reached a record high of US$4.35 million, according to the 2022 cost of a data breach report by IBM and the Ponemon Institute.

Small businesses are not immune to cybercrime. According to data from Accenture, 43 percent of cyberattacks are aimed at small business and 60% of all small business victims of a data breach permanently close their doors within six months of the attack.

Since the shift to remote working, businesses have been exposed to far greater cyber risk and suffer more data breaches as a result. According to a new report from Malwarebytes, a cybersecurity firm, 20 percent of businesses have suffered a breach due to the actions of a remote worker since the lockdown was introduced. As a consequence, these businesses faced higher costs, with almost a quarter (24 percent) having faced unexpected expenses.

Businesses can prevent cyberattacks by implementing certain procedures: • Educating employees • Protecting passwords and utilizing multi-factor authentication • Keeping systems updated • Backing-up and configuring all data and utilizing data encryption • Conducting regular risk assessment.

However, these best practices are not bullet proof.

Cyberattacks can still happen with these measures in place as criminals can harm even the most security conscious company. Many businesses 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, the question becomes, what can a business do in order to protect company profitability? The answer -- a business can supplement that insurance with a private (captive) insurance company.

Private insurance companies can write broad coverage for data losses and insure gaps. And, if cyber-related losses do not occur, the company or business owner keeps the profits that have accrued in the captive insurance company.

A private insurance company can also accumulate loss reserves and grow into another profit center for the business. This aspect of a private 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 has the option to liquidate the captive in order to fund the company through the fallout of the loss which can shield a company from potential bankruptcy.

Private 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 private insurance company allows a business to gain access to reinsurance and excess insurance markets. A private insurance company is vital to the financial strength of a business!

The primary reason for a private insurance company 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 a company to recognize that the stakes are high and that 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.

Ron Roth
Phone: 516-629-9063
E-mail: rroth@nnaplan.com
National Network of Accountants
6900 Jericho Turnpike, STE. 300
Syosset, NY 11791
www.nnaplan.com