THE TEAM WITH THE BEST PLAYERS WINS..... Jack Welch

Newsletter October 1st, 2020
Volume 8, Issue 10

Independent Captive Associates, LLC, 6900 Jericho Turnpike, Syosset, NY 11791
www.independentcaptiveassociates E-mail address promano@independentcaptiveassociates.com
Offices located in Florida; North Carolina; Connecticut; Long Island & New York

A NEW APPROACH – WORKING FROM HOME

By William York, VP of Marketing

Working from Home requires vigilance and a new approach.

The number of Americans working from home continues to rise. 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.

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 also can 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 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** and multi-factor authentication may not be in place. Both can lead to passwords being cracked with 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 target remote workers with fake Zoom downloaders.

A cybersecurity breach, such as the above examples, can decimate a business and be very costly. Data breaches cost British Airways and Marriott over $100 million each. While these examples are 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 business with a cost of $200,000 on average as well as a significant loss of time.

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 business. 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, what is a business to do in order to protect company profitability? 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 don't 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 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.

Call Independent Captive Associates, LLC sponsored by the National Network of Accountants, to learn how to get started.

Pamela Romano
Ph: 516-629-9045
Email:
promano@independentcaptiveassociates.com

Independent Captive Associates, LLC
6900 Jericho Turnpike, Suite 300
Syosset, NY 11791
www.independentcaptiveassociates.com