INSUREtrust

Employees and Cybersecurity Risks—Why Negligence Is the Biggest Threat

So much effort has been put into educating people about hackers, viruses, ransomware and other cybersecurity threats and a key component of the problem has been largely overlooked—employee negligence. In fact, a recent report from IT security firm Shred-it has revealed the number one cause of data breaches is human error. Usually, these data breaches are accidental and are the result of an employee losing a mobile device or document containing passwords or sensitive information. In fact, the study revealed that 47% of surveyed businesses, including more than 1,000 U.S. small businesses and executives, had suffered a breach in this fashion.

The Cost of Data Breaches to Business

A 2018 report revealed that such data breaches cost companies an average of $3.9 million. This could be cataclysmic for a small business. Besides the potential for lost revenues from the breach or from potential exposure to ransomware, the hack could also damage a business' credibility with consumers. The latter could actually hurt a business more in the long-term.

Employees Cyber Bad Habits

The study goes on to point out there are several bad habits employees perform that can lead to these data breaches. These include:

- Computers left unlocked and/or unattended;
- Taking down notes on paper and then leaving those papers out on your desk; and
- Working from home or in public on an unsecured Wi-Fi connection.

This last habit is especially troubling since many experts agree that remote work is such a growing trend that it is probably the future of the business world. Unfortunately, many companies do not have a policy in place for remote access. (If you would like to review our IT Security Policy Guide, which covers a variety of security best practices, please contact us.)

External Vendors Are a Significant Factor in Data Breaches

The report also shows that 25% of executives and 20% of small business owners pointed to external vendors as being the cause of data breaches. This is largely due to the victimized company failing to adequately manage access given to vendors.

There are several takeaways and suggestions stemming from this report. These include:

- Create a comprehensive policy to cover everything from cybersecurity to physical security;
- Conduct multiple training sessions as it is impossible to assume that a one time (or annual) training session will solve all data breach problems;
- Institute a clean desk policy so that all documents are secured, and old documents are properly shredded when no longer needed;
- Properly dispose of old hard-drives and flash drives;
- Create a remote access policy to extend cybersecurity outside the workplace;
- Designate a chain of command for who an employee should call in the event they misplace a document or device.

Because employee training is key to reducing cyber threats, we've partnered with a top-notch content provider. Contact us for information on how to affordably train your employees.

The report points out that most of these examples aren't meant to be malicious, but instead are accidental in nature. It is important to create a policy to prevent these types of accidental breaches from occurring.

Newsletter Signup

Name:

Email:

REGISTER

Contact Us

Please fill out the form below to receive a quote from one of our specialists. If you need immediate assistance, please call us at 1-888-932-7475.

Your Name

Your Email

Phone

Organization

What information are you interested in?

□ Cyber Risk Insurance Application □ Cyber Risk Insurance FAQ □ Recent Article on Cyber Risk

□ Contract for Independent Agents

I am a/an

Estimated Annual Revenue (if insurance buyer)

Comments

Please type the following word: Cyber

SEND