INSIGHTS

Cyber made simple.

one brightly cyber

CYBER SECURITY MUST CHANGE WITH THE TIMES

BY JAY BORDEN

Despite cybersecurity tools having grown in number and sophistication, breaches still occur with increasing frequency.

Why? People are the cause of over 90% of the breaches according to CISA, the Federal Government's Cybersecurity and Infrastructure Security Agency. Some research puts that figure as high as 95%.

The exact percentage isn't important. What is important is that people continue to be the cause of a high percentage of the breaches.

We admit the scams continue to grow in believability and AI will make them even harder to detect. But people willingly click a link and enter information.

Why? A number of reasons.

People are under a great deal of pressure to get their work done. When people feel pressured they will not always take the time needed to check if emails, texts or phone messages are real. They will click the link. Once they do that, malware downloads to their device. Once a device is compromised that malware will spread to as many devices as it can to steal credentials and information that can be exploited or sold on the Dark Web.

Cloud based systems have grown significantly in popularity over the past few years. The intricate setup options make them ripe for misconfigurations leaving security holes.

While we're looking at cloud based systems another vulnerability is who is responsible for security in a cloud based system? When systems ran on company computers, the company IT group or cybersecurity group had the final responsibility.

onebrightlycyber.com
(888) 773-1920

INSIGHTS

Cyber made simple.

CYBER SECURITY MUST CHANGE WITH THE TIMES

Continued

Cloud based systems move the processing and data off company computers and networks. Now who is responsible for cybersecurity? The cloud vendor owns some of it and the client company owns some of it. Where the dividing line is can get blurred leaving security gaps. Security gaps get exposed and exploited rather quickly.

Third-parties are another avenue for penetration. It is doubtful if any company today does not use a number of third-parties. Many companies, especially smaller ones rely on third parties but do not have the knowledge or resources to perform due diligence on the cyber precautions taken by the third-parties. The 3rd parties may have login credentials or may have direct access to computer systems and data through APIs, Application Programming Interfaces. If the 3rd party gets compromised it allows the cybercriminals to exploit any company they are connected to.

What to do? As we said at the top of this Insight, people are the cause of most of the breaches. Educate and train your people. Part of the training needs to be to convince them of the seriousness of a breach and that they are a key line of defense. Show them the statistics on the number of breaches and the cost.

Remind them that 60% of small-medium sized companies go out of business within 6 months of a breach. Protecting the company is protecting their job. Remember to do surprise tests to see who takes the bait.

Do not forget the executives and the Board of Directors in the education process. They must understand the seriousness of cybersecurity and the real costs of a breach in dollars and reputational damage. They have access to the most sensitive information and are the most desired targets of cybercriminals.

Security needs be prioritized at the highest levels for it to receive the necessary time and budget.

To help convince them, consider that SolarWinds and the Chief Information Security Officer have been charged with fraud by the Securities and Exchange Commission for the situation leading to their being breached.

If you are ready to see how easy we make cybersecure, contact us and learn what we can do to help you.

Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.