As secure as you can be

Understand your cyber vulnerabilities, and what you can do about them

INTERVIEWED BY JAYNE GEST

PAUL SEMS
General manager
Blue Technologies Smart Solutions

(216) 271-4800
psems@btohio.com

FOLLOW UP: To request a free business assessment, contact a Blue Technologies expert today at www.btohio.com/contact-us.

Whether you run a roofing business or a business services company, technology has become more sophisticated and important to day-to-day operations. But with greater reliance comes concerns about security and hacking — especially for those that can't monitor their systems to know if they're being attacked.

Paul Sems, general manager at Blue Technologies Smart Solutions, says Verizon's 2016 Data Breach Investigations Report highlights persistent issues, such as:

- 75 percent of breaches have financial motives.
- Ransomware — malicious software that limits users from accessing their system until a ransom is paid — is a pervasive threat costing organizations an average of $156,900 per incident.
- Despite filtering and education, phishing emails were opened 30 percent more often than the previous year — and of those opened, 91 percent of the time people shared information or credentials.

"Every organization needs a security program to protect its systems and assets, whether that's company files, the financial system, personal and/or health information, or its reputation," Sems says.

Even companies that do not process credit cards in volume still have cybersecurity risk. For example, a country club's list of members could be targeted for robbery during an event. Or, a ransomware attack could shut down your business, forcing you to pay money to access to your own data.

Smart Business spoke with Sems about cyber vulnerabilities in today's businesses.

How are the cyber vulnerabilities you described complicated further?

Threats are on the rise. Verizon's report found that 91 percent of companies surveyed had at least one IT security incident in 2016. That's why at many companies, senior management wants a plan in place to do something about these risks that keeps the organization secure today and tomorrow.

But it's difficult to have the time and resources to run an assessment of your technology risks. It takes more than installing a firewall and antivirus software, particularly as companies are challenged to secure many types of operating systems with more personal device use at work. That's why organizations may need a third party specialist to gather the right data, and then turn that knowledge into actionable items to ensure they're as secure as possible.

What can employers do to mitigate these security concerns?

The first step is to define the ideal security posture that the company needs to take. What is it trying to protect against? What are its goals? A company that holds health care information, for example, might consider protecting that its No. 1 priority.

Then, it needs to understand where it is today. The company should do an assessment of what its infrastructure currently looks like, while also bringing in a third party for further analysis.

Next, once an employer understands where it is currently and where it wants to go, the third party can help it build a road map to bridge the gap between the two. What is the company going to do to start solving these problems, and how should that plan be rationalized and ranked in order to maximize the benefits?

The final step is to execute the changes, while adding governance and monitoring so the company moves closer to its goals.

Why is a third party critical to the process?

Many organizations don't have a chief security officer and/or expert support staff, but security shouldn't be taken lightly. You wouldn't show up in court without a lawyer, and you shouldn't assess, monitor and mitigate your security without the right advisers at your side.

The expertise to purchase and run the right software tools require skill, and one piece of software or a better firewall won't end the risk. It also takes education and processes to continually monitor and adjust your security policies. How do the people, processes and technology work together to limit your cyber vulnerabilities?

It sounds silly to say, 'I won't hire a contractor to build my house. I can go to Home Depot and get what I need,' but that's what people say about their security: 'I don't need an expert to secure our information. I can go to Amazon and buy a firewall.' It may be true, but it's not the best way. It's not as efficient and effective. ●