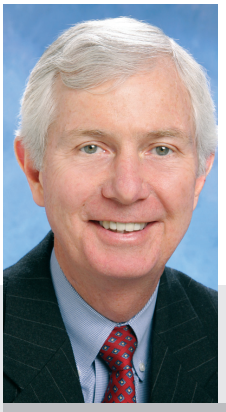
Cybersecurity

How to protect your company from cybercriminals

INTERVIEWED BY ROGER VOZAR



WILLIAM M. GODDARD, CPCU
Principal,
Insurance Advisory Services
Brown Smith Wallace
(314) 983-1253
bgoddard@bswllc.com

TONY MUNNS, FBCS, CITP, CIRM, CISA
Member,
Risk Advisory Services
Brown Smith Wallace
(314) 983-1297
amunns@bswllc.com

WEBSITE: We can help you with cybersecurity. Visit www.bswllc.com/riskinsights to learn more.

Insights Accounting is brought to you by **Brown Smith Wallace**

Data breaches are becoming more commonplace, causing millions of dollars in damages for companies that have personally identifiable information (PII) hacked by cybercriminals.

"Think about all of the losses you can incur. Not only do you have to hire a security expert to find what happened, you may be assessed fines or penalties by the merchant's acquiring bank or payment card brand. In addition, you could be responsible for credit card charges made by the criminals and lose business because no one trusts you anymore," says William M. Goddard, CPCU, Principal, Insurance Advisory Services at Brown Smith Wallace.

Smart Business spoke with Goddard and Tony Munns, FBCS, CITP, CIRM, CISA, Member, Risk Advisory Services, about protecting companies from cybercrime.

How do cybercriminals access networks?

One typical method is spear phishing. Unlike traditional phishing attempts, which are fraudulent emails sent at random claiming to be from a reputable organization like a bank or eBay, spear phishing emails are sent to targeted employees or customers of a company.

The email appears to be coming from the company and requests that the recipient click on a link, which then goes to a fraudulent website. They may ask for personal information or they may launch a virus they'll use to get into your network.

If you click on the link, it launches a program in the background that goes onto your workstation and canvasses the network for other vulnerabilities. The program collects data, whether that's credit card information or other PII, and uploads it to the cybercriminal.

How can you reduce cyberattack risk?

The first thing to do is develop an information security policy, document it and disseminate it throughout the organization.

Other protective measures are:

- Conduct an inventory of authorized devices on your network. Guests can come into your place of business with a laptop and leave a device on your network that goes undetected. That device could have Trojan horses or viruses that, when executed, plant a program on your network.
- List an inventory of software allowed to run on workstations or servers. That helps when looking for rogue programs or software installations.
- Install an anti-virus program to detect malware. Anti-virus protection also needs to be maintained and updated for the latest definitions.
- Run vulnerability and penetration tests on servers and networking equipment to make sure you don't have unnecessary services running that could lead to a vulnerability and potential unauthorized access.
- Prevent data loss by running programs to detect outbound calls or connectivity to remote sites that are not authorized to receive data output.
- Create security awareness within your company to ensure that people who have access to information are not sharing anything that is confidential or private.
- Develop an incident response plan to react to a breach and quarantine activity before it spreads throughout the network.

Companies think they're protected because they are compliant with some standard such as PCI, but that's no guarantee their systems will not be compromised. Your security program needs to go beyond PCI and focus on more than credit card information. Cybercriminals go after the easiest target along with whatever PII is available that has value. For instance, not-for-profit organizations may have names, addresses and checks with banking information; all of that information is valuable to somebody. For similar reasons, credit cards are often targeted because they're so widespread and it's the easiest information to sell.

What can companies do to protect against losses if they are hacked?

A variety of insurance policies cover things like the cost of fines, notification that PII has been compromised, liability and business interruption. All cyber policies are slightly different, and you have to be careful to buy the right coverage.

Businesses are smart enough to buy fire insurance in case a building burns down. Cyberattacks can be just as damaging, depending upon what happens and what information has been compromised. ●