RISK MANAGEMENT CORNER

Cybersecurity and Small Business

It's nearly impossible these days for businesses to operate without the help of Internet-connected devices, which exposes them to cybercrime. It's the small- to medium-sized businesses that are especially vulnerable: half are victims of cybercrime and nearly two-thirds of those victims go out of business.[1] Hackers increasingly target small businesses because there is a low risk they will be caught and a high probability they will be successful.

Maintaining personally identifiable information (PII) on a computer connected to the Internet creates a nearly unavoidable risk. More than likely, names, addresses, and employment information are stored. If PII is acquired by someone without the authority to do so, that may result in a data breach.

Banking, credit, and vendor account information is also vulnerable. Even if that valuable information is not stored on an Internet-connected computer, employees who have access to it can be duped into handing it over to criminals.

Best Practices and Security Tips

Tip 1: Train Employees in Information Technology Security. Training should be offered, especially to those who are responsible for accounts payable, human resources records, and wire transfers. Training for all employees should be reinforced periodically.

Employees should be instructed to refrain from clicking links or attachments in e-mails, and not to pay an invoice until it's confirmed that the sender actually sent it. Even if the e-mail appears to be from a trusted source, employees should learn to always copy and paste links or type URLs into a browser to see if the address is valid.

Tip 2: Funds Transfers. Put a policy in place to have an in-person or telephone conversation to confirm e-mail requests for funds or personal information. It can greatly reduce the likelihood of fraudulent transfers or information sharing.

Tip 3: E-mail Authentication. Phishing can be substantially reduced by verifying that the e-mail originated from the domain it is associated with. If your domain is hosted, it's worth taking some time to look at how your e-mail is set up to ensure proper authentication schemes are used.[2]

Tip 4: Change default passwords on your router and other Internet-connected devices.

Tip 5: Use a trusted VPN service when using Wi-Fi.

Tip 6: Back up your data regularly both to the cloud and to a removable device.

Tip 7: Update firmware and software regularly.

Tip 8: Provide firewall security for your Internet connection. Ensure your operating system's firewall is enabled, especially if have employees working from home.[3]

Tip 9: Limit employees' authority to install software and their access to only necessary information and data.[3]

Tip 10: Require employees to update unique passwords every three months.[3]

Security professionals used to strive for perfect security, but today they accept that goal as unachievable. Instead, they strive for optimal security by combining best practices with a risk management program that considers purchasing data compromise and cyber coverage through a knowledgeable insurance provider.

Cyber Shield® from Federated Insurance is a two-part coverage program designed to help provide essential protection against many of the critical cyber and privacy exposures businesses face. Data Compromise Coverage and Cyber Coverage can help your company recover from intentional or accidental breaches.* Visit federatedinsurance.com for more information or to find your local Federated representative.

[1]"Small Business, Big threat: Protecting Small Businesses from Cyber Attacks," Statement for the Record: Dr. Jane LeClair, Chief Operating Officer, National Cybersecurity Institute at Excelsior College Before the United States House of Representatives Committee on Small Business, 4/22/15. https://smallbusiness.house.gov/uploadedfiles/4-22-2015__dr.__leclair__testimony.pdf

[2] The leading e-mail authentication protocols are SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting & Conformance); best practice is to utilize the three protocols together. https://dmarc.org/2016/03/best-practices-for-email-senders/

[3]"Cybersecurity for Small Business." Online at https://www.fcc.gov/general/cybersecurity-small-business

* Coverage will be determined solely by the circumstances of the event and the terms of your policy, if approved for issue. This article is not an offer of insurance.