STERLING NATIONAL BANK

Cybersecurity: Finding Your Weak Links

MEET OUR EXPERTS
LYNN BAGLIEBTER, Executive Vice President, Westchester Market President and **JASON VAZQUEZ**, Deputy Chief Risk Officer weigh in on cybersecurity.

Whether simple check fraud or sophisticated cyberattack, financial crimes continue to plague businesses, causing financial losses, disrupted services, and headaches. Identifying your company's areas of vulnerability can help mitigate cyber risk and keep your assets secure.

Despite trillions of dollars spent in cybersecurity over the years, companies are still exposed to financial cyberattacks. As banks and large corporations become more sophisticated in their security efforts, fraudsters are taking advantage of smaller companies with fewer resources.

While the Internet of Things (IoT) allows criminals more access points to your financial information, your weakest link is most likely a human. Exploiting human nature to manipulate fraudulent transactions—also known as social engineering—is a tactic commonly used by criminals. Some thieves can hack into email accounts and impersonate a legitimate person to initiate transactions. In some cases, the fraudster will include bits of company news gathered from press releases to lend credibility and gain trust. The criminal can then impersonate you to appeal directly to your banker for a wire transfer. In another scenario, the email may appear to come from you to your bookkeeper ordering an urgent transaction, or it might look like it's from your supplier to your accounts payable clerk with a change of address for payment.

As criminals become craftier at finding your weakest links, you can mitigate the risks by following our tips.

THE TRUTH About Cyber Safety

Think your cyber risk is too high and you should avoid electronic transactions altogether? Think again. Whether someone steals a blank check or duplicates one using design software, check fraud still reigns as the most prevalent form of financial crime.

Practice sound bookkeeping.

Reconcile bank statements monthly and review your online activity several times a week. The sooner you alert your banker to a problem, the more time there is to remedy it satisfactorily.

Protect yourself.

Consider offsetting costs related to cyber-related breaches with Cyber Risk Insurance, a relatively inexpensive policy to protect your assets and data. Also, take advantage of any bank services available to you, such as online banking or transaction verification systems.

Prepare your team.

Layer authority so that every transaction requires dual controls to complete. Train your staff to scrutinize all emails and be wary of ones that have a tone of urgency or use language out of the ordinary for the sender.

Contact your relationship manager today at 855.274.2800 to discuss ways of reducing financial threats, including Sterling National Bank's own transaction verification service Positive Pay.