DEFINITI

INSIGHTS: CYBERSECURITY

Understand the Cybersecurity Risk and Take Action

October is Cybersecurity Awareness Month — a time that reminds us of the importance of protecting ourselves against cyber threats and how we share private and confidential information via email and online.

The retirement plan world is awash in data of all types, much of it confidential. Safeguarding and securing this information, whether it's employee compensation, Social Security numbers or plan balances, is an ongoing responsibility for retirement plan sponsors.

We spoke with Kurt Simione, Definiti's new Chief Information Officer, about what our clients and their employees can do to safeguard plan-related information and the essential roles automated tools and processes and participant education play.

New Threats Require More Sophisticated Technologies

In today's data-centric world, some of the sage advice about protecting information, such as encrypting emails and creating smart passwords, has been eclipsed by more advanced and automated practices. For example, remembering to encrypt emails requires an active choice by the information-sender. What's needed now is something that protects information exchange 24/7 in the background and doesn't rely on someone remembering a best practice or slowing down to add one more step to a process. ("Being busy makes you less perceptive to security threats," Kurt says.)

This is where technologies like data loss prevention (DLP) and other system-wide solutions come in. "DLP looks for patterns, such as Social Security numbers that have a set number of digits," Kurt says. "This technology automatically checks for these types of patterns in emails and displays a warning, alerting the sender to sensitive information that needs protection — and it can take the next step and encrypt the data for you."

Advanced Threat Protection and Activity Alerting

Kurt's advice about what retirement plan sponsors should know about cybersecurity technologies extends far beyond DLP and includes advanced threat protection (ATP). He explains ATP this way: "Modern email platforms already have junk-mail filters in place. ATP goes a step beyond

that filter, where it analyzes emails for threats and viruses and any links they contain. ATP software can detect links from bad actors and disable them."

Activity alerting — a low- or no-cost technology — is also essential. It can be set up to alert a business owner when, for example, a forwarding rule is added to a person's email box. While email forwarding may be a legitimate business need, the results can be damaging when a hacker does it. In this scenario, a hacker gains access to a person's email account and password and sets up a forwarding rule that allows them to read every email coming into the account. The security breach could be significant if personally identifiable information (PII) is in an email, as it would be with many retirement plan sponsors' accounts.

Critical Role of Participant Education

Having the right data-security technologies in place is essential in managing retirement plan-related security risks. Employee education can also play a role.

Kurt recommends every business conduct security awareness training, using online learning and in-person meetings, when possible, and making participation required for new hires and quarterly for everyone else.

Regular employee education helps employees stay current on advanced tactics like phishing emails and spoofing. "If employees receive an email that looks like it's from HR, asking for their Social Security number, they need to be instinctively suspicious and know how to report the phishing attempt," Kurt says. "Question everything."

Spoofing is another hacker tactic that can harm your business. In this instance, an employee receives an email message that looks legitimate but comes from a forged sender address. An ATP tool can be set up to look for emails like this, but employees should still be aware of sophisticated tactics hackers use and shown examples of phishing and spoofing emails.

Kurt Simione
Chief Information Officer

As Definiti's CIO, Kurt Simione is focused on creating and maintaining a secure, modern IT infrastructure that scales with our rapidly growing company in a fast-paced industry. In the last 20 years, Kurt has managed technology infrastructures for companies ranging from startups to more than 1,000 employees. His expertise covers all issues Definiti's clients face, including cybersecurity, network infrastructure and acquisition integration.

Cybersecurity Risk and Your Role as a Fiduciary

Other cybersecurity technologies and practices go beyond what we highlighted in this article. Understanding contemporary, system-wide solutions and how they help a business is something Kurt strongly encourages retirement plan sponsors to research, saying:

> *Even for a small business, these technologies are no longer optional in our world and when dealing with PII. A smart first step is to audit your current practices and processes and possibly work with a security consultant to conduct the analysis.*
>
> *The retirement industry must recognize hacking is a business, and we are its customers. We need to embrace our corporate responsibility for securing sensitive data and understand that it requires money, training and an ongoing focus to do so.*

As fiduciaries, retirement plan sponsors are bound by the Department of Labor (DOL) and Employee Retirement Income Security Act (ERISA) to properly reduce cybersecurity risks to the plan, and partner with service providers who share that commitment to safeguard plan data.

The DOL provides three easy-to-read resources worth downloading and sharing with your benefits team:

- Tips for Hiring a Service Provider With Strong Cybersecurity Practices (PDF)
- Cybersecurity Program Best Practices (PDF)
- Online Security Tips, a more plan participant-focused resource (PDF)

We're Here to Help

As a trusted partner to the retirement plan industry, Definiti takes its cybersecurity obligations seriously and invests heavily to keep retirement plan sponsor and participant data secure. (Read our commitment to cybersecurity best practices.) We rely on advanced encryption, automated technologies and security best practices, coupled with educating our employees, to help safeguard retirement plan information.

If you already partner with Definiti, you know our cybersecurity commitment and focus on remaining a trusted provider for the clients we serve. If you're a financial advisor or retirement plan sponsor searching for an experienced, data security-conscious third-party administrator, let's start the conversation. Call Definiti at 1-888-912-3653 or email sales@definiti-llc.com.