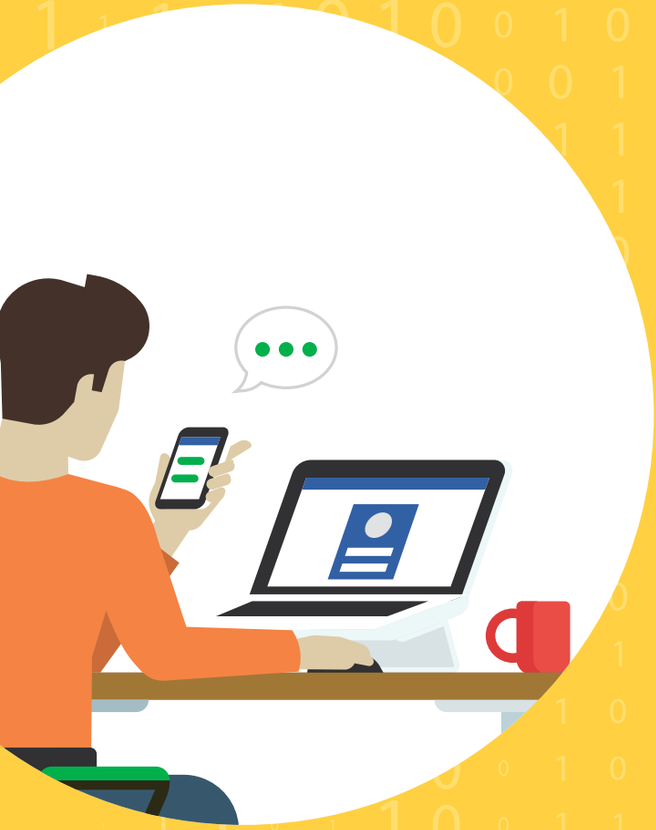
FEATURE

Cyber (In)Security

{ What you need to know — and do — about cybersecurity threats }

BY JUDY WARD



For cyber-criminals, retirement plans make appealing targets. What makes retirement and other employee benefit plans particularly susceptible to cyberattacks?

"Number one, benefit plans are an information-rich source of data," says Neal Schelberg, New York-based partner at law firm Proskauer Rose LLP. "They're holding personally identifiable information on lots of people: It is 'gateway' data that, once hackers have it, they're off to the races" with identity theft and other crimes, he says.

"Benefit plans also often transmit information electronically to third parties: recordkeepers, TPAs, actuaries and other providers," Schelberg continues, noting that the ongoing flow of data offers numerous hacking opportunities. And one side of the data transmission (the plan sponsor) generally has weaker cybersecurity protections than the other side (the provider). "The level of cybersecurity sophistication that a plan sponsor has, as compared to a Fidelity, is probably far less," he says. "Many plan sponsors are in the process of converting from paper to digital data, so it is not like they have a long history of protecting digital data. They are kind of feeling their way, so they're somewhat beginners."

Those factors could put retirement plans at real peril, if employers don't take the right precautions. "There's too much exposure, when it comes to cybersecurity risks, to not pay attention to it," says Trey Maust, chief executive officer of "Sheltered Harbor," a Reston, Virginia-based financial services industry initiative to ensure consumers have access to critical account assets if a major incident happens. "As a sponsor, it is important to allocate some time to this, to ensure the protection of your participants' accounts and your company's reputation."

Advisors should make this a priority in working with sponsors, recommends attorney Michelle Capezza, a New York-based member of the firm at Epstein Becker & Green, P.C. "From a plan advisor perspective, whatever your touchpoints are with the plan sponsor, I think this should be item number one on the agenda, until you are satisfied there are adequate data privacy and security protections in place for the plan and participants," she says.

> "Data is an asset of the plan, just like any other asset of the plan, and sponsors have a fiduciary duty to protect their plan's assets."
>
> *— Neal Schelberg, Proskauer Rose LLP*

The Risks for Sponsors and Advisors

What could happen in a retirement plan cyber-crime? Think about how many plans now handle loan and distribution processing electronically, says advisor David Hilton, principal at El Segundo, California-based Kaye Capital Management. Picture hackers gaining access to a participant's account, changing the participant's mailing address to their own, and then posing as that person to request a loan or distribution. "The check will go to the 'new address' within days," he says. "But it usually takes 15 to 30 days, from a payroll perspective, for a participant to find out that it has happened." By the time the participant learns of the request, the check likely has been cashed. Hilton says he has been told confidentially by recordkeepers that this type of scam already has been executed successfully.

And cyber-criminals have become a lot more sophisticated in their "phishing" attacks on recordkeepers. "Now, they're less likely to send an email to every employee at a recordkeeper saying, 'Hey, there's this Nigerian prince who needs your help,'" says Ben Taylor, San Francisco-based senior VP and DC consultant at Callan LLC. "They are more likely to go on LinkedIn, and other social media sites, to try to learn which individuals at the provider are likely to have access to 'crown jewel' (participant) information. Then they create similar email accounts to those employees, contact other employees at the provider pretending to be those people, and try to get access to that data." If they get the data, they can use it for a crime like identity theft.

The U.S. Department of Labor has not yet taken a stance that sponsors have an affirmative fiduciary responsibility on cybersecurity, Taylor says. "Reading the tea leaves," he adds, "it is not a question of *if* that is going to happen, but *when*."

Likewise, while retirement plan participant lawsuits over cybersecurity aren't prevalent yet, it seems possible that they could occur, Capezza says.

"A lawsuit like that could be very costly for a sponsor," she says. "Think about participants' account balances: What if all of those got wiped out by a hacker?"

Whether cybersecurity falls under an ERISA fiduciary duty remains a legal question, Schelberg says. "Some say that it's a settlor function," he says. "I would argue that there is a fiduciary duty. Data is an asset of the plan, just like any other asset of the plan, and sponsors have a fiduciary duty to protect their plan's assets. Because of that, the 'prudent man' standard would hold that plan sponsors need to take steps to make sure that the data is protected. Particularly because of the financial repercussions of a breach, the failure to take preventative measures raises fiduciary concerns."

Beyond the ERISA issues, Schelberg says, participants also might bring lawsuits under state privacy laws that could apply to data in retirement plans. "Every state has some level of data-privacy requirements," he explains. "Some are more stringent than others, but they exist."

And plan advisors also could be vulnerable in participants' cybersecurity lawsuits, Schelberg says. "Whether a case is brought under ERISA or under state privacy laws, there could be some significant risks out there, and some significant potential liabilities," he says. "Keep in mind that typically when these things happen, it's not one or two people who are impacted; it could be hundreds, thousands, or more. So when you start calculating the total of the potential damages awarded, you may be talking about significant sums of money."

Looking Inward

Sponsors and their advisors can help protect a plan and its participants by looking at these issues within the employer's organization:

Loan, Hardship Withdrawal and Distribution Requests

Sponsors should review all the processes and procedures they have for these requests, Hilton recommends. What stopgaps does the employer have to ensure participants' protection, and does it need more? "For anything involving a distribution request, you should make sure there are security protocols in place," he says.

> "There's too much exposure, when it comes to cybersecurity risks, to not pay attention to it."
>
> *— Rrey Maust, Sheltered Harbor*

For example, Hilton says providers can implement a simple solution to the address-change scam. "If a mailing address is changed on an account, you can add a 30-day-lock window to your system. During that time, no loan or distribution can be made without a written consent that is signed on paper by the employee and hand-delivered to his or her HR manager, requesting the loan or distribution," he says. "Thirty days provides enough time for HR to verify the request with the participant. Something has to happen: There has to be a 'red flag' that takes it out of the purely electronic realm, if address changes are made."

And plans shouldn't allow any ACH (electronic) transfers from a participant's account, Hilton recommends. A policy that requires distributions to be paid by check only provides more protection by preventing an overly quick electronic process, he says.

Participant Data Protections

Plan sponsors need education about how their plan data gets stored, accessed and transmitted, Schelberg says. "For example, how does the sponsor maintain participant data? Does the sponsor keep it in-house, or store it with a third party?" he asks.

Employers should get a clear understanding of who within their organization has access to participants' personally identifiable information, and restrict it further if that makes sense, Taylor says. "Almost any recordkeeper or TPA can create on its system various 'tiers' of access to personally identifiable information of a plan's participants," he says. "It's important for employers to know not just who has access to the information for their plan, but who has the access to change it or alter it, and who has the access giving them the ability to move assets around."

And employers should train their HR staff members who have access to participant data on how to handle it, and how not to handle it, says Wendy Carter, Washington, D.C.-based vice president and DC practice director at The Segal Group. "There is the potential for major things coming from small human errors," she says. An HR staffer who momentarily walks away from his or her desk with a computer screen full of participant data may unintentionally open the door to cyber-crime by someone else who walks by and sees it.

Self-protection Education

It helps to provide participant education such as how to identify phishing emails, Carter says. "Your employees are, to some degree, your weakest cybersecurity link," she says. "Unfortunately, humans are always going to be human."

Participants need to know what they should and shouldn't do to safeguard their account, such as not using a public computer to access their account data, Capezza says. "People will actually go to a public library and use the computers there to pull up their 401(k) account information," she says. "Participants need to understand how important it is for them to protect their own information."

And every three to six months, participants should change their 401(k) account password, making sure not to use the same password they utilize elsewhere online, Hilton says. "It's not rocket science," he says. "There are easy steps people can take to make it more difficult for their account to be hacked."

There's an element of "social engineering" to heading off cyber crimes, Maust agrees. "Participants need to understand things like they shouldn't click on links in emails from unknown sources or suspicious sources," he says. "There are very basic practices like that, which are — surprisingly — the most common ways for criminals to gain access to the system, and gain access to sensitive data."

Cybersecurity Insurance

Schelberg recommends that all plan sponsors consider this insurance, and learn how coverage differs among policies. For example, some policies provide only

GAUGING RECORDKEEPER CONTROLS

How can advisors break down the complexity of evaluating a recordkeeper's cybersecurity into a manageable process? "I'd suggest that advisors start with these categories, because it takes cybersecurity and organizes it into the main things that everybody looks at," The SPARK Institute's Timothy Rouse says. "Then use these categories to say to a recordkeeper, 'What are you doing in each of those areas?'"

SPARK has identified these 16 key areas for cybersecurity controls:

1. **Risk Assessment:** The provider understands (such as by completing technology risk assessments) the cybersecurity risk to its organizational operations, organizational assets and individuals.
2. **Security Policy:** The provider has an information security policy.
3. **Organizational Security:** The provider has defined information-security roles and responsibilities and aligned them with both internal staff and external partners.
4. **Asset Management:** The data, personnel, devices, systems and facilities used in running the provider's business are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
5. **HR Security:** The provider has taken steps (such as doing background checks) to ensure that its staff and external partners are suitable for their roles, that they receive cybersecurity awareness education, and they get the necessary training to perform their information security-related duties and responsibilities consistent with related policies, procedures and agreements.
6. **Physical and Environmental Security:** Physical access to assets (like data centers) is managed and protected.
7. **Communications and Operations Management:** A provider's networks and systems utilize appropriate data-security tools (such as firewalls and antivirus software) to ensure the security and resilience of systems and assets.
8. **Access Control:** Access to assets and associated facilities is limited (by a control such as unique, complex passwords for all employees) to authorized users, processes or devices, and to authorized activities and transactions.
9. **Information Systems Acquisition Development:** The provider implements a technology system-development lifecycle, and develops and implements a vulnerability-management plan that includes performing vulnerability scans.
10. **Incident and Event Communications Management:** The provider develops and maintains communication processes and procedures (and regularly tests them) to ensure timely response to detected cybersecurity events.
11. **Business Resiliency:** The provider has incident response plans and recovery plans in place, and manages them.
12. **Compliance:** The provider has policies and procedures to ensure that it follows all cybersecurity legal requirements, including privacy and civil liberties obligations.
13. **Mobile:** The provider has a formal policy and takes appropriate security measures to protect against the risks of using mobile devices (like cell phones).
14. **Encryption:** Data-at-rest and data-in-transit are both protected.
15. **Supplier Risk:** The provider takes steps to ensure the protection of any of its assets that suppliers can access, such as by subjecting suppliers to periodic security reviews.
16. **Cloud Security:** The provider ensures the protection of data it stores or processes in cloud environments, such as by subjecting cloud providers to periodic security reviews.

first-party coverage (if a breach happens at the plan sponsor level), while others also provide third-party coverage (for a breach at a third party like a recordkeeper). "Many policies just cover first-party cyberattacks," he says. "But if you get third-party insurance, if the system of your recordkeeper or TPA gets hacked, the insurer will cover you as a sponsor."

As part of getting coverage, the insurer may come onsite and do a mini-review of the employer's cybersecurity controls to assess the risk, Carter says. So by that point, an employer needs to have already implemented some protections, like training employees who have access to personally identifiable participant data. "To get the policy," she says, "an employer needs to demonstrate that it is taking appropriate precautions."

Ongoing Governance

Putting together a benefit plan cybersecurity policy and procedures takes multiple kinds of expertise: not just benefits, but IT, risk management, and legal, and often from both within and outside an employer. Then cybersecurity requires ongoing monitoring and changes as threats shift. "It is definitely not a 'one and done,'" Capezza says. "It's something you need to monitor and update."

Employers also should go through an internal cybersecurity risk audit at least annually, Carter recommends. "Cybersecurity is a constantly evolving target," she says. "The 'bad actors' are continually looking for ways to impersonate people and get access to their account information and make withdrawals. They are continually trying to penetrate the recordkeeping systems."

Evaluating Recordkeepers

For sponsors, their big question for providers boils down to, "How do I know that once I give the data to you, it's safe?" says Timothy Rouse, executive director of The SPARK Institute, Inc., a Simsbury, Conn.-based trade association for retirement plan providers. "The answer for sponsors is, 'I evaluate you and make sure you're safe.'"

Sponsors can best protect their participants' data by evaluating their providers to ensure they engage in a constant diligence process, says Callan's Ben Taylor, who also serves as vice chair of SPARK's Data Security Oversight Board. "Make sure that cybersecurity protection is a core competency for that provider. That's not driven so much by technology as by governance. To protect participants' data, providers have to take a series of steps all the time."

To evaluate recordkeepers' cybersecurity governance, sponsors and their advisors can get much of the information they need from looking at a third-party audit, says Segal's Wendy Carter, who serves with Taylor as the other vice chair of SPARK's Data Security Oversight Board. "There's no way that all employers can go onsite and do an annual evaluation of their recordkeeper's cybersecurity," she says. "So the next step is a trained professional (retained by the recordkeeper) going onsite and doing the due diligence on their behalf, and sharing it with the plan sponsor."

The Data Security Oversight Board has developed standards to help recordkeepers communicate to sponsors and advisors/consultants about their cybersecurity controls. SPARK identified the 1,500 cybersecurity questions most commonly asked on RFPs and determined that they fall into 16 main categories (see "Gauging Recordkeeper Controls" sidebar). The idea is that sponsors and advisors can look at an annual third-party audit that shows, for each of those 16 areas, whether a recordkeeper's controls for that area passed the auditor's testing.

In addition to evaluating their recordkeeper's controls, plan sponsors need to understand what their service agreement with the recordkeeper stipulates about cybersecurity issues, Capezza says. "They may have been with their service provider for some time, and may not have ever looked at what their service agreement says about cybersecurity," she adds.

Capezza recommends looking at what the service agreement spells out about a recordkeeper's procedures, controls and audits. "For example, what does it say about what happens if there is a breach?" she says. "How will the recordkeeper notify the sponsor? Will the recordkeeper notify participants? Who is responsible for the cost of those participant notifications? And does the service agreement say anything about who is responsible legally for that breach?" The service agreement should clearly state any limitation of liability, indemnification and insurance protections for the sponsor related to a breach, she says.

A plan sponsor's obligation does not end after an initial cybersecurity evaluation of its recordkeeper's controls and the service agreement, Schelberg says. "As a sponsor, you have a continuing obligation to monitor your provider," he says. "As cyber-risks evolve, has the recordkeeper updated its processes and the technology available to improve its data security?"

The financial services industry continues to work on ways to protect Americans' accounts and data. The Sheltered Harbor initiative, for example, aims to give financial providers a way to rapidly recover from a destructive cyberattack and make customers' accounts and data available to them again. Each participating financial institution securely stores critical individual-customer data in an offline data vault, and pairs with another financial institution or third party (a "restoration partner") for restoration capability.

"The idea is that in the event of an attack, this ensures that customers' critical account information is preserved, and that the critical account data cannot be compromised," Maust says. The Sheltered Harbor project currently encompasses U.S. bank deposit accounts and retail brokerage accounts, but doesn't yet include qualified retirement plan accounts. That will happen at some as-yet-undetermined point, he says.

"Then let's say a significant, destructive cyberattack against a financial institution occurs, and the financial institution cannot access the production systems that it utilizes to retrieve and act on sensitive customer data," Maust says. "That critical customer information has been stored at a secure data vault, so the financial institution could then bring that critical data back online through a restoration partner within 24 to 48 hours, and customers could act on it again."

» Judy Ward is a freelance writer who specializes in writing about retirement plans.