Managing Cybersecurity Risks
What to Do Now to Protect Your Plan

It seems that barely a week goes by without news of another major cyberattack at a large corporation. Employee benefit plans aren’t immune from the risk of a cyberattack, either.

This makes it critical to devise a strategy that minimizes your plan’s exposure to cyberattacks and other cybersecurity risks.

Specific ERISA Duties
As a plan sponsor, you have certain duties under ERISA related to the impact that a cyberattack or data breach could have on plan participants and beneficiaries. Specifically, you should be prepared to respond to and recover from an attack. This involves anticipating critical actions and decisions before an attack occurs, not during or after the attack.

Cybersecurity issues are different for ERISA employee benefit plans than they are for other areas of your business. Therefore, your cybersecurity risk mitigation plan should be separate and distinct from your enterprise-wide cybersecurity plan, although it may align and integrate with other existing plans.

The first step in formulating your employee benefit plan cybersecurity strategy is to identify what data is the most critical to protect and what the greatest threats to this data are. Then you can devise the best strategy for minimizing these threats and responding to cyberattacks or data breaches that may occur.

Start by asking these five questions:

1. What participant data needs to be protected, and how is it classified? Participant data files contain sensitive personally identifiable information (PII) such as participants’ names, Social Security numbers, birthdates, bank account information, and account balances. They also contain protected health information (PHI) such as medical claims data.

2. Where is this data stored, and who has access to it? Participant data may be retained by many different parties, including third-party administrators, custodians, actuaries, auditors, and trustees. You should determine every location where data could be held and the retention periods and make sure all parties storing data meet strict security requirements.

3. What are the greatest threats to this data? For example, data could be stolen and sold to the highest bidder, or cybercriminals could freeze your computer systems until you pay a ransom (this is known as ransomware). The source of threats is dynamic, coming from email, the

Continued on page 3
Many plan sponsors today have added an auto-enrollment feature to their employee retirement plans. With this feature, new employees are automatically enrolled in the plan and given the option to opt out if they’d rather not participate.

Some sponsors are taking auto-enrollment a step further by also adding auto-escalation to their plans. This feature automatically increases the percentage of pay that’s contributed to participants’ accounts on an annual basis—usually by one percentage point up to a set deferral rate, such as 10 percent.

Employee Savings Coming Up Short
A common rule of thumb for retirement saving is that individuals should save at least 10 percent of their pretax earnings to increase their chances of having a financially comfortable retirement. But many employees only save enough to receive the maximum employer match, which is typically around six percent of pretax earnings.

In testimony before the U.S. Senate Finance Committee, retirement experts have recommended that plan sponsors automatically enroll all employees in the plan and automatically increase contribution levels. They suggest that a model 401(k) plan template include the following:

- Auto-enrollment at a rate of six percent of employees’ pretax earnings, with an employee option to contribute less if they want.
- Auto-escalation of contributions in annual increments of one percent until a total contribution rate of 10 percent is reached, with an employee option to escalate less if they want.

According to a research report prepared by J.P. Morgan Asset Management, employees are less likely to increase their contributions if they are automatically enrolled in a plan at a set deferral rate. While auto-enrollment increases the percentage of employees who participate in a plan, it results in a lower overall savings rate among all participants when not paired with auto-escalation, the report concluded.

Meanwhile, a report prepared by the Defined Contribution Institutional Investment Association (DCIIA) found that in plans with auto-escalation, nearly one-third of employees were actually contributing more than 10 percent of pay to their plan. In plans without auto-escalation, just one-fifth of employees were contributing more than 10 percent of their pay.

Why Aren’t More Sponsors on Board?
The DCIIA found that 62 percent of large plan sponsors automatically enroll all new employees in the plan, but only 48 percent also use auto-escalation. So why aren’t more plan sponsors combining auto-escalation with auto-enrollment?

The DCIIA report identified three main reasons:
1. 21 percent of sponsors said they are too paternalistic toward employees.
2. 13 percent of sponsors said it would be too costly from an employer-match standpoint.
3. You can ward off employee complaints by improving communication, especially when it comes to stressing that employees can opt out of auto-enrollment and auto-escalation. You should also stress to employees how the power of compounding interest can boost their savings over long periods of time.

According to a research report prepared by J.P. Morgan Asset Management, employees are less likely to increase their contributions if they are automatically enrolled in a plan at a set deferral rate. While auto-enrollment increases the percentage of employees who participate in a plan, it results in a lower overall savings rate among all participants when not paired with auto-escalation, the report concluded.

Meanwhile, a report prepared by the Defined Contribution Institutional Investment Association (DCIIA) found that in plans with auto-escalation, nearly one-third of employees were actually contributing more than 10 percent of pay to their plan. In plans without auto-escalation, just one-fifth of employees were contributing more than 10 percent of their pay.

**Stretch Your Employer Match**
A simple shift to your 401(k) matching formula could help encourage participants to boost their deferral rates.

For example, suppose you’re matching 100 percent of employee contributions up to five percent of their salary. Many employees will contribute up to five percent of their pay in order to get the full employer match.

But if you change the formula to match 50 percent of employee contributions up to 10 percent of their salary, many employees will increase their contribution to 10 percent to get the full match. The cost to your business remains the same.
Internet, social media, and even unrelated applications.

4. How is the data accessed, and is access being properly controlled?
Plan administration systems are sometimes linked to unrelated systems that can open the door to hackers while data is being transmitted. Encryption is a critical step in securing data—not just during transmission, but also at the points where it resides.

5. What data needs to be retained?
Not all the data being stored is necessarily needed to support your plan or execute tasks. Determine what data is unnecessary and then remove it from your system to reduce the risk of it being unnecessarily compromised.

Find the Right Balance
As the plan fiduciary, you must determine the appropriate level of cybersecurity prevention given the scope of the threat, potential loss exposure, and cost of taking preventive action. Here are a few things to consider in devising an appropriate cybersecurity risk management strategy for your plan:

- **Available resources:** Are cybersecurity prevention resources available internally, or do you need to invest in external resources and tools?
- **Strategy integration:** Can your strategy be integrated with the rest of your organization and, if so, what are the cost-sharing protocols?
- **Implementation costs:** Of course, cost will be a major factor in your strategy, but you should also factor in the potential cost of a major cyberattack and data security breach.
- **The feasibility of purchasing cyber insurance:** This type of insurance typically covers third-party damage and defense costs as well as first-party coverage. Here, you wouldn’t have to wait for a third party to sue the plan; instead, coverage is triggered as soon as a data breach occurs.

Reducing Cybersecurity Risks
The National Institute of Standards and Technology (NIST) has developed a standard framework designed to reduce cybersecurity risks to critical infrastructure, including ERISA employee benefit plans. The NIST cybersecurity framework includes the following five components:

1. **Identify cybersecurity risks.** The weakest cybersecurity links can present the greatest risks. Often the weakest link is employees who haven’t been properly trained in how to handle sensitive data or who are careless in handling this data.

2. **Protect sensitive data.** This starts with creating a culture of awareness within your organization about the importance of data security. Ideally, data protection will incorporate both technology solutions such as encryption and human solutions such as ongoing training in how to handle sensitive data.

3. **Detect data breaches.** This is critical given the fact that experts say cyberattacks aren’t a matter of if, but when. Perform penetration testing before an attack happens so you’ll be able to detect one when it occurs.

4. **Respond to cyberattacks.** Your framework should detail specifically what your organization’s response to a cyberattack will be in order to minimize any damage from the attack.

5. **Recover from cyberattacks.** The framework should also detail how your organization will recover from any damage that does occur from a cyberattack.

- **Contracts with service providers:** Third-party administrators and other service providers with access to participant data are a possible source of data breaches. So you need to ask them detailed questions about their own cybersecurity risk management strategy.

In particular, you should ask plan record keepers and custodians for a SOC for Cybersecurity Report. This new report will contain detailed information and assurances about controls affecting the security and integrity of the systems used to process data, as well as the privacy of the data processed by these systems.

Not If, But When
Many cybersecurity experts say it’s not a matter of if, but when a cyberattack will occur. Therefore, you should be proactive when it comes to managing plan data to minimize exposure to cybersecurity threats—both now and in the future.
Are Your Plan Investment Options Appropriate?

This is a question all plan sponsors should ask from time to time. Offering an inappropriate or inadequate menu of plan investment options could lead to lawsuits from participants who believe their retirement accounts have underperformed.

Applying the “prudent man” standard can help you answer the question. This standard requires plan fiduciaries to behave as they would if they were protecting their own money. For example:

- Are investments diversified among different asset classes to reduce correlated risks?
- Do the investment options allow participants to maintain sufficient liquidity so they don’t have to sell assets at an inopportune time?
- Is each investment position judged on its own merits, and are any deemed speculative rejected?
- Is the underlying investment performance being regularly monitored for fundamental changes in its nature or risk?

Here are a few more questions to ask as you evaluate the appropriateness of your plan investment options:

- Is the investment lineup easy for participants to understand?
- Are there enough funds to build a globally diversified allocation?
- Is there a suite of asset allocation funds (e.g., target-date or risk-based) to simplify the investment process for participants?
- Is the investment information clear and concise enough to help participants make good decisions?
- Are the investment fees reasonable, and are low-cost investment options available?

It’s a good idea to perform an annual review of your plan investment options to gauge how appropriate they are. This review will help you determine whether:

- Investment options are well-diversified and meet the fund’s objectives.
- Costs are appropriate based on the fund’s performance.
- The plan offers a good mix of different types of investments (e.g., small-cap and large-cap stocks, bonds, index, and target-date funds).
- Participants have access to investment advice.

Please contact us if you would like help determining the appropriateness of your plan investment options.