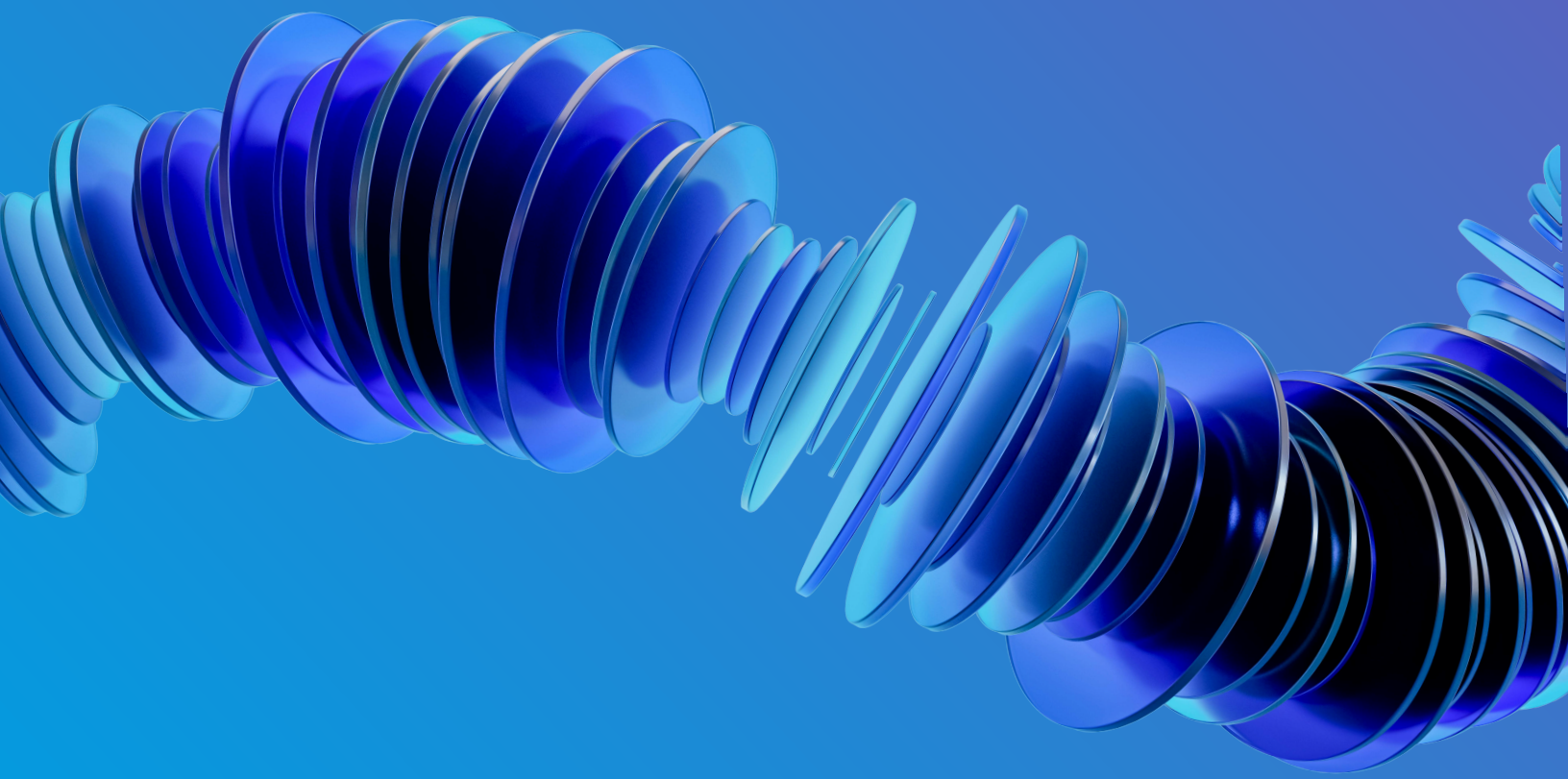
Mercer

welcome to brighter

Cybersecurity checklist for DC plan sponsors

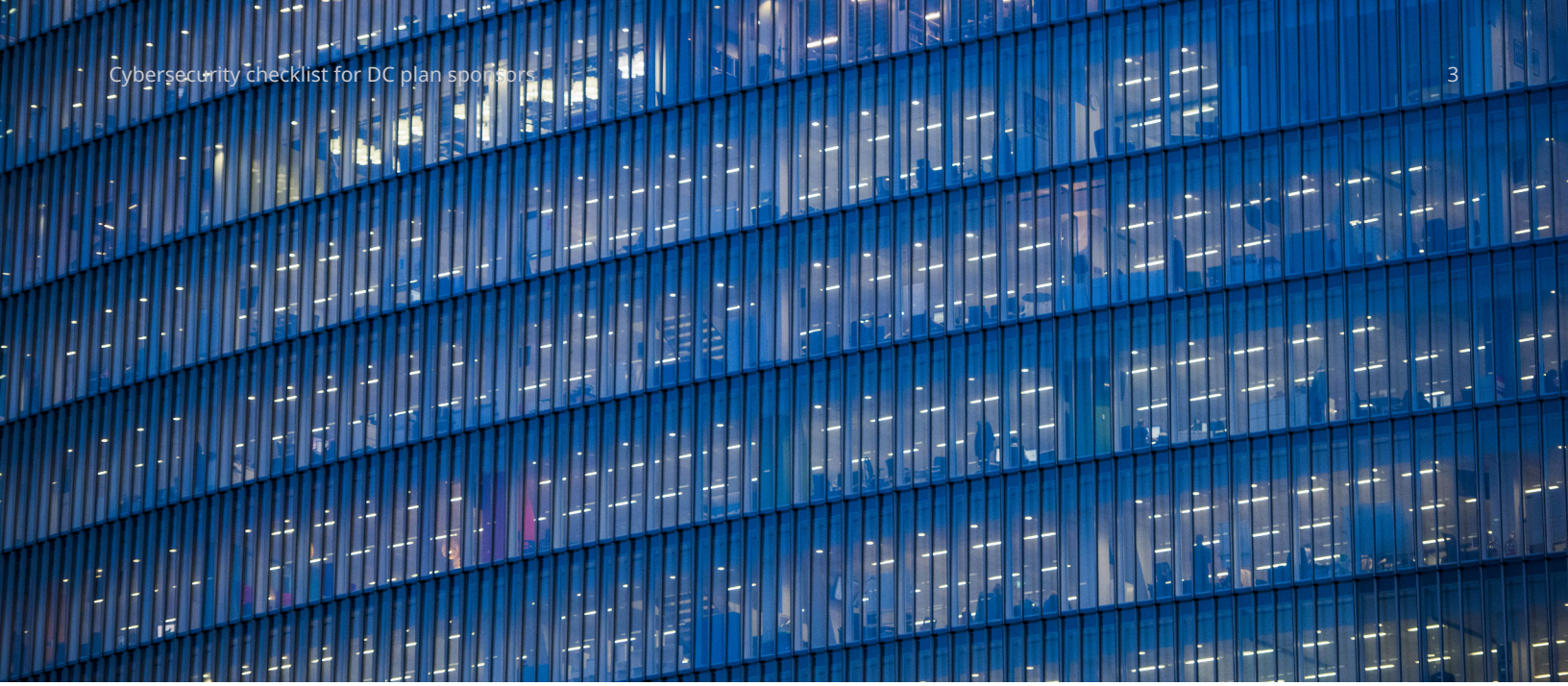


Retirement plans can be a tempting target for cyber-criminals due to the large amount of assets they hold and the personal data they store on participants. For retirement plan sponsors, having inadequate security controls can lead to the loss or unauthorized disclosure of Personal Identifiable Information (PII) or plan asset data — or worse, the theft of retirement savings of individual participants.

The FBI Internet Crime Complaint Center received close to 860,000 total cybersecurity complaints in 2024; the losses reported due to investment scams remain the most of any crime type, with losses rising from $4.6 billion in 2023 to $6.5 billion in 2024[1].

With the Employee Retirement Income Security Act (ERISA) requiring plan fiduciaries to take appropriate precautions to mitigate risk from both internal and external cybersecurity threats, we have established a cybersecurity checklist for DC plan sponsors to help establish and maintain their monitoring and communication efforts.

1. Source: FBI Internet Crime Complaint Center (IC3), 2024 Internet Crime Report



Consider establishing a policy regarding cybersecurity monitoring or amend the committee charter. This can help define the oversight that will be conducted and the responsible parties within the organization. To ensure accountability and effectiveness, the committee should agree to perform and document specific actions related to cybersecurity monitoring. It is also important to regularly review this policy and committee charter.

Regularly communicate with participants regarding Department of Labor's cybersecurity program's best practices[2] for protecting their accounts from cyber threats and fraud. This should include enrollment communication and annual communications specifically tailored to this topic. Use your recordkeeper to expand your messaging and document your efforts. For years, sponsors have directed participants to take a "set it and forget it" approach to their accounts, but active participants are more likely to identify a one-off breach of an account on a timely basis.

Review the annual audit report issued on your recordkeeper's systems and processes to make sure any shortcomings affecting your plan are identified and addressed. To the extent that committee or internal company resources do not have expertise in this area, engage with an external resource to support the review process. Monitor recurring or significant issues to determine whether to take action on finding an alternative provider. Document audit activity within sponsor and committee records.

2. Source: U.S. Department of Labor, Employee Benefits Security Administration. (n.d.). Cybersecurity best practices for retirement plans. https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf

Flag any third parties or advisors that have access to your plan's PII or participant financial information through the recordkeeper and determine what ongoing review of their practices should be conducted. Many recordkeepers outsource statement mailings or communications support that can require the sharing of participant data with third parties.

Understand your recordkeeper's fraud policy, and request at least annual updates to see if any changes have been made. Although most recordkeepers are willing to make participants whole for losses incurred through no fault of the participant, some have begun to add stipulations regarding actions that the participant (or the sponsor) must take to be eligible. Confirm that the recordkeeper's fraud policy extends to any contracted third parties.

Review the contract with the recordkeeper to help ensure it aligns with your organization's expectations on:

a. Use of participant data, particularly regarding services outside the qualified plan
b. Financial commitments to reimburse participants if account breaches occur and duration of such commitments
c. Timely notifications to you as plan sponsor regarding data security or fraud activity impacting your participants or systems
d. Oversight of third parties contracted by the recordkeeper
e. Level of support provided for the annual review of cyber practices and corresponding service level agreements

Engage an external expert to assist with contract review to ensure industry standards are being considered.

Conduct annual meetings between the recordkeeper and the committee regarding cybersecurity and include internal experts. Share with the committee materials prepared internally or externally reviewing the recordkeeper's capabilities, and reflect the due diligence undertaken in meeting minutes.

When evaluating alternative recordkeepers, include cybersecurity and fraud prevention questions in any requests for proposal issued, and consider responses to those questions in the evaluation and selection process. To the extent that external parties are part of the service delivery (external custodians, partners for nonqualified plan services, etc.), confirm that all organizations are evaluated.

Use interim fee benchmarking projects to gather insight into marketplace practices and negotiate contractual changes or service enhancements where appropriate. Staying informed about market changes is essential to ensure that the incumbent remains up-to-date and, ideally, a market leader.

Engage internal IT or external DC plan specialist resources to review recordkeeper capabilities and contractual commitments. Recognizing that IT professionals do not necessarily have expertise in DC plan administration, consider whether an education session for the IT team would be helpful.

Plan sponsors must prioritize the implementation of effective security protocols to mitigate the ever-evolving threat of cyberattacks. Remaining vigilant, continuously monitoring for vulnerabilities, and updating security measures are critical steps in safeguarding participants' assets and personal information. In a rapidly changing digital environment, proactive and comprehensive cybersecurity strategies are essential for ensuring the long-term security and integrity of retirement plans.

Contact us

Contact us to discuss this cybersecurity checklist in more detail or explore how we can help you assess the cybersecurity strategy for your DC plan.