AICPA

Employee Benefit Plan
Audit Quality Center

Cybersecurity and employee benefit plans: Questions and answers

These questions and answers were prepared by the EBPAQC to help plan auditors understand cybersecurity risk in employee benefit plans, and to discuss cybersecurity risk, responsibilities, preparedness, and response with plan clients.

1. How are employee benefit plans at risk for cyber-attacks?

Employee benefit plans, like all other organizations and individuals, are vulnerable to cyber-attacks and thus exposed to risks relating to privacy, security, and fraud. Retirement, savings, and health and welfare plans are attractive targets for hackers seeking access to plan assets and participant and beneficiary personal information. Factors that contribute to cyber risk in plans include:

- The electronic environment in which they operate. Electronic benefit plan information is especially susceptible to cyber-attacks because it includes large amounts of sensitive employee information that is shared with multiple third parties, including outsourced service organizations that also maintain and electronically share sensitive employee and asset information.
- Benefit plans often fall outside the scope of a sponsor organization's cybersecurity planning with regard to ongoing business activities.
- Employee benefit plans are not regulated for cybersecurity purposes, as are certain other businesses that handle personal information.

- Plan sponsors and administrators may have a false sense that anti-virus and anti-spam software adequately protect them from these risks.
- Plan sponsors and administrators may have a false sense that their service organization SOC 1 reports address cyber risks at the service organization.

2. What plan information and assets are at risk from a cyber-attack?

Plan sponsors, administrators, and service providers maintain electronic information that may be particularly vulnerable to cyber-attacks, including:

- "Personally identifiable information" (PII) such as social security numbers, dates of birth, and email addresses. PII has significant value to cybercriminals because it is permanently associated with an individual (unlike a credit card account number, PII cannot be easily "cancelled") and therefore can be misused over a longer period of time.
- Participant enrollment data, individual account balances, direct deposit information, compensation, and other financial information. A hacker could also target individual accounts online to gain the ability to request loans and distributions, and access participant and/or sponsor contributions.
- "Electronic protected health information" (EPHI), which includes information about health status, provision of healthcare, or payment for health care that can be linked to a specific individual, that is produced, saved, transferred or received in an electronic form. Similar to PII, EPHI does not expire, and stolen information can be used to acquire prescription drugs, receive medical care, falsify insurance claims, file fraudulent tax returns, open credit accounts, obtain official government-issued documents such as passports and driver's licenses, and even create new identities.

3. What are the potential consequences of a cyber-attack?

The consequences of a cybersecurity breach can be substantial for plan sponsors, service providers, participants, and beneficiaries.

- Significant costs may be incurred in detecting the extent of the break-in, investigating and managing the incident response, recovering data, and restoring system integrity.
- The theft of certain PII and breach of online security over plan assets and records can lead to monetary losses to participants, beneficiaries, the plan, the plan sponsor, and service providers.
- Cybersecurity breaches may result in operational disruption and damage to a sponsor's and administrator's reputation.
- Plan fiduciaries potentially could be found to be responsible for a fiduciary breach and required to restore losses to the plan participants and beneficiaries.
- A cybersecurity breach of EPHI in a health plan could result in potential violations of the Health Insurance Portability and Accountability Act (HIPAA) and subject the plan sponsor and service providers to fines or monetary settlements.

4. What are examples of cyber threats to benefit plans?

Plans and service providers have fallen victim to cyber schemes to steal participant data, make fraudulent transfers of participant assets (through direct transfers and fraudulent plan loans), and ransomware attacks. Some examples of cyber threats to benefit plans include:

"Phishing" techniques to deceitfully obtain logon credentials and passwords to gain access to online participant account information and request distributions or loans, redirect benefits to another account, or create fraudulent health claims.

- An email, purported to be from the plan sponsor's top executive, was sent to the human resources (HR) department requesting sensitive employee data. HR responded by sending the information before realizing it was a "spear phishing" or "whaling" email from an outside party.

- A phishing scheme was successfully carried out at a plan recordkeeper. As a result, participant accounts were breached and unauthorized distributions were made from those accounts.

Socially engineered malware, when an end-user is tricked into running a Trojan horse program, often from a website they trust and visit frequently. The otherwise innocent website is temporarily compromised to deliver malware instead of the normal website coding.

- A plan sponsor's internal IT department discovered malware on 50 computers. One participant account was breached and an improper distribution occurred before the Malware was discovered.

- In November 2016, the Department of Health and Human Services (HHS) announced a settlement with a large university for potential violations of HIPAA. Following a malware infection targeting the university's employee health care plan, the university agreed to pay $650,000 in penalties and to comply with the requirements of a corrective action plan. The breach exposed the private health information of 1,500 people. An HHS investigation revealed that the university had failed to accurately assess the risk of malware infection and adopt procedures to secure its data.

Cyber criminals using employees' personal information and setting up web profiles that allow them to take out loans from individual participant accounts.

- In June 2016, more than 90 deferred-compensation retirement accounts of a city's municipal employees were breached. Hackers obtained the personal information of plan participants and used it to set up online profiles on the plan custodian's web platform; the hackers accessed personal information and withdrew loans from 58 accounts. Reports estimate that the city lost about $2.6 million. The city returned funds taken from participant accounts and offered credit monitoring services to account holders.

- A service provider received an unusual number of distribution requests for one of their plan clients. The requests were vetted through the established process and denied because they were determined to be unauthorized.

Ransomware attacks in which cyber criminals encrypt and seize an entire hard drive, only releasing it in exchange for a ransom.

- In July 2016, a cyberattack targeted a grocery workers union pension plan. Hackers took control of the pension plan's computer servers and demanded a ransom in digital currency (three bitcoins, or about $2,000). "At risk" data included employee names, birthdates, Social Security numbers and bank information. The union refused to pay the ransom and turned to its backup system. While there was no evidence that hackers accessed sensitive information, the union offered plan participants 12 months of credit monitoring and identity theft restoration services.

Loss or theft of mobile devices, laptops, and flash drives with personal data, and personal information transmitted via unsecured email or portals

- A CD-ROM and laptop that contained private data of 30,000 plan participants and beneficiaries were stolen from the vehicle of an employee of a plan sponsor. Notification, credit monitoring, and insurance costs were approximately $200,000.

5. What responsibilities do plan fiduciaries, including those charged with governance, have for protecting plan information from cyber-attacks and responding to breaches?

Plan administrators and those charged with governance have an ERISA fiduciary duty with respect to the management of the plan, including implementing processes and controls to restrict access to a plan's systems, applications and data, including third-party records and other sensitive information. ERISA Section 404 requires benefit plan sponsors and other fiduciaries to administer their plans for the exclusive benefit of plan participants and beneficiaries, and with the "care, skill, prudence, and diligence under the circumstances that a prudent person acting in a like capacity and familiar with such matters would use." DOL Reg. §2520.104b-1(c) and DOL Technical Release No. 2011-03 and 2011-03R impose obligations to ensure that electronic systems protect the confidentiality of personal information.

As part of their ERISA duty to monitor plan service providers, plan sponsors must understand how their service providers store and protect the participant data they handle (see Question 8 below for special considerations when a service provider is used).

It is unclear whether state privacy and cyber laws are pre-empted by ERISA as it relates to benefit plan data. As such, fiduciaries should consider state statutes in determining their responsibilities for cyber security.

According to the DOL ERISA Advisory Council report, *Cybersecurity Considerations for Benefit Plans* (November 2016), (2016 DOL Advisory Council Cybersecurity Report), if (or more likely, when) a cybersecurity breach occurs, plan sponsors should have a plan in place for addressing the breach. The DOL Advisory Council Cybersecurity Report recommends:

- The plan should establish procedures for how the sponsor, likely working with its service providers, will communicate with plan participants who may be anxious about the breach and protecting their data.
- Sponsors should also have a process for determining how a breach will be corrected and what remedies will be used.
- Sponsors should document both their overall process for responding to cybersecurity breaches and any steps they take in correcting an actual breach. This documentation will help show that they acted prudently in the face of the breach.
- The Advisory Council stressed the need for plan sponsors to thoroughly vet their service providers and to negotiate contract provisions to lower or mitigate the costs of correcting a possible cyberattack on a plan.
- Finally, the Advisory Council encouraged plan sponsors to review and understand the limitations of their business insurance coverage, and consider cyber insurance to address possible coverage gaps. (The 2016 DOL Advisory Council Cybersecurity Report includes a detailed discussion of cyber insurance.)

6. What is the plan auditor's responsibility for evaluating cybersecurity risk and controls in an audit of a plan's financial statements?

The auditor's responsibilities with respect to cybersecurity matters in a financial statement audit are outlined in the Center for Audit Quality (CAQ) *Alert #2014-03, Cybersecurity and the External Audit*. The CAQ Alert notes the following:

> "Cybersecurity risks and controls are within the scope of the financial statement auditor's concern only to the extent they could impact financial statements and company assets to a material extent. Auditing standards require the financial statement auditor to obtain an understanding of how the company uses IT and the impact of IT on the financial statements. Financial statement auditors also are required to obtain an understanding of the extent of the company's automated controls as they relate to financial reporting, including the IT general controls that are important to the effective operation of automated controls, and the reliability of data and reports used in the audit that were produced by the company.
>
> In assessing the risks of material misstatement to the financial statements—including IT risks resulting from unauthorized access and unauthorized use or disposition of company assets—financial statement auditors are required to take into account their understanding of the company's IT systems and controls. If information about a material breach is identified, the financial statement auditor would need to consider the impact on financial reporting, including disclosures, and the impact on ICFR.
>
> The financial statement auditor uses a top-down approach to the audit of ICFR to select the controls to test. A top-down approach begins at the financial statement level and with the auditor's understanding of the overall risks to ICFR. The financial statement auditor then focuses on entity-level controls and works down to significant accounts and disclosures and their relevant assertions. This approach directs the financial statement auditor's attention to accounts, disclosures, and assertions that present a reasonable possibility of material misstatement to the financial statements, including related disclosures.
>
> Systems and data that are within the scope of most audits usually are a subset of the totality of systems and data used by companies to support their overall business operations. The auditor's focus is on access and changes to systems and data that could impact the financial statements and unauthorized use and disposition of assets; that is, matters within the defined boundary of ICFR.
>
> A company's overall IT platform includes systems and related data that not only address financial reporting needs, but also operational and compliance needs of the entire organization. The financial statement auditor's primary focus is on the controls and systems that are in the closest proximity to the application data of interest to the financial statement and ICFR audit—that is, systems and applications that house financial statement-related data. It is important to note that cyber incidents usually first occur through the perimeter and internal network layers, which tend to be further removed from the application, database, and operating systems that are typically included in access control testing of systems that affect the financial statements."

In a plan environment, even when a breach of participant information occurs, it may have no direct effect on the plan's financial statements. This might happen when, for example, participant information was breached but there were no plan assets lost because no participant accounts were accessed. In such situations, the breach would need to be considered, but because there is no effect on financial reporting, the auditor's response may be minimal. The CAQ Alert includes general information for auditors and should not be relied upon as being definitive or all inclusive. Auditors should refer to the rules, standards, guidance, and other resources in their entirety, and to carefully evaluate which requirements apply in each specific situation.

7. Are there additional cybersecurity considerations when plan administration is performed by a third-party service provider?

Many plan sponsors use third-party service providers such as plan administrators, actuaries, auditors, trustees, insurers and consultants for plan management and administration. These providers collect and maintain sensitive employee data, such as Social Security numbers, addresses, dates of birth, account balance information, beneficiary information and bank account details to meet their responsibilities and deliver services. Certain service providers also maintain systems that allow employees to initiate transactions online, such as obtaining loans and/or account withdrawals. Consequently, a cybersecurity breach within a service provider could result in participants' identities, personal information, or plan assets being compromised.

Plan sponsors should have discussions with the plan's third-party service providers regarding policies and procedures relating to data security, including passwords, use of social media, document retention, internet privacy, and other relevant issues. Plan sponsors should also understand the providers' procedures for breach notification, including any obligations they may have to notify participants or governmental authorities. Plan sponsors can obtain this information through discussions with those providers and by reviewing the service provider agreements.

The 2016 DOL Advisory Council Cybersecurity Report includes a list of questions regarding the protection of data that may be helpful to plan administrators when contracting with, and evaluating, service providers.

8. Does a SOC® 1 report address a plan's internal control over cybersecurity controls and risk?

For plans that utilize service organizations for most (or all) of their electronic records and investment transactions, a common misconception may be that those plans have relatively little cybersecurity risk if the service organization's SOC 1 report identifies no issues. However, a SOC 1 report addresses only a plan's internal control over financial reporting; it does *not* address broader entity cybersecurity controls and risk.

A SOC 2 report, however, specifically addresses the cybersecurity controls and risks in the system used by the service organization to provide such services to the plan. The report may also address controls relevant to the service organization's ability to maintain the confidentiality or privacy of the information processed by the system. (A SOC 2 report can address any or all of the categories in the AICPA's trust services criteria, including security, availability, processing integrity, confidentiality, or privacy.) As such, a SOC 2 report can help plan management assess and manage risks associated with outsourcing a function to a service organization by providing information about the effectiveness of controls at the service organization and how those controls integrate with the plan's controls. SOC 2 examinations are performed by independent CPAs in accordance with AICPA Guide SOC 2® *Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*

(SOC 2 guide). Read *Understanding How Users of Service Organizations Would Make Use of a SOC for Service Organizations SOC 2® Report* to better understand how a SOC 2 report may be useful to managing the plan's cybersecurity risks.

In addition, the AICPA *SOC for Cybersecurity* is a new risk framework that establishes common criteria and guidelines for communicating about an organization's cybersecurity risk management program. It enables plan management to report on the plan's cybersecurity management program to external stakeholders with the credibility associated with an independent examination report. Read more about the SOC for Cybersecurity guidance.

9. Are there resources available to help plans address their cybersecurity risks?

The 2016 DOL Advisory Council Cybersecurity Report included information for plan sponsors and fiduciaries to utilize when developing a cybersecurity strategy and program. A *cybersecurity risk management program* is a set of policies, processes, and controls put into place by management to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented. The report emphasized that when implementing a cybersecurity risk management strategy, plan sponsors should remember that one size does not fit all—the sponsor's approach will depend on its own circumstances, balancing the need to protect plan participant data and the sponsor's own business needs.

The AICPA has developed a Cybersecurity Resource Center that provides tools and information that plan sponsors can use to address cybersecurity risks.

10. What are effective practices and policies to protect against cyber-attacks?

The 2016 DOL Advisory Council Cybersecurity Report identified four major areas for effective practices and policies.

1. Data management – Protect and control data.
2. Technology management – Maintain up to date technology.
3. Service provider management – Perform due diligence on plan data security of service providers.
4. People issues – Properly train and manage personnel.

The Report includes information for plan sponsors to assist them in establishing a cybersecurity strategy for employee benefit plans and contracting with service providers, as well as a list of resources for plan sponsors and service providers that addresses considerations for managing EBP cybersecurity risks.

11. What resources are available to help plan management determine the adequacy of the plan's cybersecurity risk management strategy and program, and communicate that to plan fiduciaries and third parties?

The AICPA has developed an entity-level cybersecurity reporting framework through which organizations can communicate useful information about their cybersecurity risk management program to a broad range of stakeholders, including boards of directors, senior management, investors, and others. The AICPA cybersecurity risk management framework creates opportunities for:

- Plan management to describe the plan's cybersecurity risk management program.
- CPAs to perform a consulting engagement to help plan management develop a description of the plan's cybersecurity risk management program to provide to the board and other internal parties who are interested in that information.
- CPAs to perform a consulting engagement known as a "readiness assessment" to help plan management identify where the plan's cybersecurity processes and controls may need to be shored up.

In addition, the AICPA has introduced SOC for Cybersecurity, which:

- Enables CPAs to examine and report on a plan's cybersecurity risk management program.
- Results in the issuance of a general use cybersecurity report designed to meet the needs of a variety of potential users. The CPA provides an opinion on:
  - management's description of the entity's cybersecurity risk management program, and
  - the effectiveness of controls within that program to achieve the entity's cybersecurity objectives.

For auditors who wish to assist their plan clients in this area, the AICPA has developed an interactive training and self-paced learning program, the Cybersecurity Fundamentals for Finance and Accounting Professionals Certificate, which addresses terminology used and the appropriate questions to ask; applying the security mindset to daily work; the potential risks and opportunities in developing or evaluating cybersecurity risk management programs; and the importance and impact of cybersecurity risks on an organization, including relevant aspects of the AICPA's new cybersecurity risk management reporting framework. Two additional learning programs, Cybersecurity Advisory Services Certificate and Cybersecurity Attest Services Certificate, are offered at various times and locations—information is available at the AICPA Store.

* * * * * * * * * * * * * * * *