PRACTICE NOTE

THOMSON REUTERS
PRACTICAL LAW™

Best Practices for ERISA Fiduciary Responsibilities and Cybersecurity for Retirement Plans

by Michelle Capezza, Mintz, with Practical Law Employee Benefits & Executive Compensation

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/W-026-7320**
Request a free trial and demonstration at: **us.practicallaw.tr.com/about/freetrial**

A Practice Note discussing cybersecurity best practices for retirement plans to address fiduciaries responsibilities imposed by the Employee Retirement Income Security Act of 1974 (ERISA).

The Employee Retirement Income Security Act (ERISA) imposes specific obligations on employers, individuals involved with retirement plans, and other entities, including special rules for fiduciaries as defined in ERISA Section 3(21) (29 U.S.C. § 1002(21)).

In today's world, most transactions involving retirement plans are conducted electronically, including maintaining and sharing data across multiple platforms. Data and personally identifiable information (PII) have become increasingly vulnerable to attack as information travels across employer and third-party systems. This increasing vulnerability is partially caused by advancements in:

- Plan administration.
- Technology.
- Online enrollment.
- Electronic access to account information.
- Electronic delivery of disclosures, including benefit statements.
- Benefit plan transaction processing (including self-certification of distributions).

Ongoing advancements in technology and the novel cybersecurity risks that those advancements bring create concerns for both:

- The security of employee data that is collected, transmitted, processed, and stored for employee benefit plans.
- The security of the assets in participant accounts.

Until recently, ERISA plan fiduciaries had no clear protocols to consider for protecting PII in retirement or other benefit plans despite its vulnerability to data breaches. However, on April 14, 2021, the US Department of Labor's Employee Benefits Security Administration (EBSA) issued its first formal cybersecurity best practices guidance for retirement plans (EBSA Cybersecurity Guidance). The EBSA Cybersecurity Guidance provides recommendations for:

- Plan sponsors.
- Fiduciaries.
- Recordkeepers.
- Service providers.
- Participants and beneficiaries.

The EBSA Cybersecurity Guidance:

- Is intended to help plan sponsors and fiduciaries to prudently select a service provider with strong cybersecurity practices and monitor them.
- Assists plan fiduciaries and record-keepers in their responsibilities to manage cybersecurity risks.
- Offers plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss.

The EBSA Cybersecurity Guidance is in the form of tips with suggested best practices to consider, and it is the first formal declaration from EBSA that ERISA plan fiduciaries are at least obligated to ensure proper mitigation of cybersecurity risk (see Legal Update, DOL Issues Cybersecurity Guidance for ERISA Retirement Plans).

This Note provides guidance for plan fiduciaries of retirement plans to develop prudent policies and procedures to mitigate cybersecurity risks and secure information and data. For a basic framework plan fiduciaries must consider for their responsibility to protect PII and data, see Practice Note, Cybersecurity and ERISA Fiduciary Responsibilities for Retirement Plans.

Fiduciary Challenges

Understanding ERISA fiduciary obligations to protect against employee benefit plan participant data breaches presents a challenge because of:

- The movement toward developing federal cybersecurity legislation.
- Varying state laws on data privacy, security, and data breach notification requirements.
- Scrutiny over financial institutions and their compliance with laws designed to protect PII.
- The increasing importance of HIPAA and HITECH compliance in the wake of health plan data breaches.
- Emerging litigation.

Fiduciaries must meet a prudence standard when discharging duties solely in the interest of plan participants and beneficiaries. Fiduciaries must:

- Act prudently in responding to a breach of their plan participants' protected health information (PHI) and PII.
- Consider developing prudent policies and procedures for handling, collection, transmission, security, and storage of all PII, data, and PHI.
- Consider developing third-party procedures and notification and remediation measures for breaches of their plan participants PHI and PII.

The EBSA Cybersecurity Guidance provides tips to assist fiduciaries in meeting their responsibilities under ERISA to prudently select and monitor service providers and determine those that have strong cybersecurity practices.

Establish Cybersecurity Policies

Plan fiduciaries must always carry out their duties with prudent procedures and processes. Development of best practices related to cybersecurity requires thought and insight and depends on the facts and circumstances.

Establishing an appropriate cybersecurity policy for retirement plans, including other benefit plans (Policy) is complicated because:

- This area is evolving and questions regarding ERISA preemption and conflicts with state and federal data privacy laws are not yet definitively addressed.
- Remediating financial harm to a participant might be difficult because the level of financial injury resulting from a data breach might not be immediate or easily quantifiable.

Further, prudent selection and monitoring of plan service providers that may handle PII requires critical due diligence of the third-party service provider's systems, data storage, and encryption security. Responsibilities to company personnel who handle the PII should also be prudently delegated.

Plan sponsors and fiduciaries should:

- Prepare and follow individualized Policies that suit their organization.
- Require third-party service providers to demonstrate compliance with Policies.

The plan sponsor and fiduciaries' Policies should:

- Address cybersecurity for benefit plan administration.
- Reflect that the organization's internal cybersecurity protocols which have been designed in compliance with applicable law.
- Address how external service providers will be evaluated.

The EBSA Cybersecurity Guidance includes Cybersecurity Program Best Practices (Cybersecurity Best Practices) that:

- Recordkeepers and other services providers responsible for plan-related IT systems and data should have in place.
- Plan sponsors and fiduciaries can incorporate into their own procedures and use as guideposts to select and monitor service providers.

The Policy should reflect the plan fiduciaries' actual processes and should exclude items that the organization does not follow. The practice of developing and following a prudent Policy enables plan sponsors and fiduciaries to:

- Act prudently.
- Mitigate cybersecurity risks and the risk of a breach of fiduciary duties.

Developing a Cybersecurity Policy

In developing these Policies, consider:

- Assembling a team, including clearly defining roles and responsibilities (see Assemble a Team).
- Identifying data (see Identify the Data).
- Data retention policies (see Data Retention Policy).

- Training employees handling data (see Train Employees Handling Data).
- Communicating with and educating employees (see Communicate with and Educate Employees).
- Remote working issues (see Remote Working Issues).
- Prudent standards for selecting and monitoring service providers (see Prudent Standards for Selecting and Monitoring Service Providers).

Assemble a Team

Given the complexities of understanding data systems and security controls, organizations must assemble a qualified team of individuals to ask the right questions and review and interpret the answers.

The team may include individuals from:

- HR.
- IT.
- Legal.
- Compliance.
- Risk management.
- Any organizational cybersecurity leaders.

The team should identify its areas of risk and define its protocols around:

- Benefit plan data collection.
- Transmittal.
- Processing.
- Storage.
- Encryption.
- Outsourcing.
- Breach notification and response.

These protocols should then be properly executed and updated to comply with changes in applicable laws.

Designated employee benefit plan fiduciaries should incorporate organizational protocols in an approved Policy as part of its fiduciary best practices for benefit plan governance. To the extent the organization has an already developed data and information security program as an employer, the existing program should be incorporated into benefit plan management and administration practices. If an organization does not have adequate in-house resources to develop these data and security programs, it should obtain qualified outside assistance.

Identify the Data

The plan sponsor and fiduciaries should know what participant and beneficiary information and data is collected, transmitted, processed, and stored. PII and data typically at issue include:

- Social Security numbers.
- Birth dates.
- Addresses.
- Beneficiary names.
- Financial information.
- Account information.

Organizations must define the types of employee data that they are handling and set parameters for its maintenance and security. The definition of PII can also vary under applicable state and other laws. Plan sponsors and fiduciaries should take these differing definitions into consideration when establishing procedures. Employee benefit plans store extensive amounts of PII for participants and beneficiaries. Various personnel and service providers may have access to the PII, making it vulnerable to data breaches.

Organizations should focus on limiting the amount of information they collect to categories that are crucial for the maintenance and administration of the plan. Depending on the type of benefit plan program, privacy and security may require vetting under different rules or through the use of different channels.

If the organization will make a retirement investment advice tool available to participants, plan fiduciaries should also perform due diligence on the tool and on the provider's privacy and security measures to protect PII.

Given the lack of uniform legal requirements in this area, plan sponsors and fiduciaries should:

- Be mindful of various applicable laws including state and local laws, and international laws, that may affect the collection, storage, and transmittal of PII.
- Understand that the definition of PII can vary depending on the jurisdiction in which the plan is administered or the participant is located.
- Be aware of:
  - the types of data collected from participants and beneficiaries;
  - the parties that are given access to the data;

- the types of data shared with outside plan service providers;
- ways to limit the amounts of data shared; and
- methods to protect the security of the data in different environments.

An organization's general information security program should already have identified data points and be in compliance with applicable laws. These should be followed for benefit plan purposes.

Data Retention Policy

In addition to collecting no more data than is absolutely necessary, plan fiduciaries and sponsors should ensure that data that is no longer needed by the organization or no longer required to be maintained by document retention laws is deleted.

Plan records typically must be retained for at least six years after the filing of a report (for example the Form 5500 created from those plan records). Records must be kept if they could be relevant for determining a participant's or a beneficiary's entitlement to a benefit, but the law does not provide a clear timeframe for retaining these types of records.

Record retention policies must:

- Be designed prudently.
- Consider the various requirements and statutes of limitations.
- Require secure archiving of data once a reasonable amount of time has elapsed (to eliminate some of the risk of hosting data on systems penetrable by hackers via the internet).

Organizations should keep only data that they need and adopt effective processes to discard unnecessary data (including back-up paper and electronic copies) and to reconcile procedures with applicable plan record-retention requirements.

Electronic documents are not easily deleted, and organizations may need to consult external service providers to achieve deletion of data. For example, even when a document is dragged and dropped into the recycle bin on a desktop, it may remain on the computer's hard drive or on the cloud drive that constantly backs up the data stored on the computer. Simply dragging and dropping a document into the recycle bin or hitting the delete button can leave metadata that contains an individual's personal email address, IP addresses, or other sensitive information contained within the document.

Plan sponsors and fiduciaries should know where PII is located in all of the organization's systems and understand the security levels of any cloud computing and remote data storage processes that are involved in plan administration, including how data is stored and protected. In addition, organizations should ensure that:

- Computer systems are updated, including prompt installation of software patches.
- Electronic threats are monitored to allow for effective responses.
- They give attention to the National Institute of Security & Technology guidelines on computer configuration use.
- They consider full disk encryption on laptops and external data storage devices that might hold PII or information on how to access it.
- A complete login for the network, firewalls, routers, and key software applications is implemented.
- The usage of portable devices and data storage devices that might hold PII or information on how to access those devices is limited or defined.

If plan records are maintained by third-party service providers or recordkeepers, plan sponsors should ensure that service agreements address:

- Secure access to the records.
- Proper transfer, retention, and destruction of records following termination of services.

Consultations with legal and IT departments and advisors can aid in determining:

- What information can be deleted.
- How information can be properly deleted.
- If information cannot be deleted but can be archived, how that information can be safely stored.

Train Employees Handling Data

The Cybersecurity Best Practices notes that employees are often an organization's weakest link for cybersecurity. In addition to evaluating whether service providers adhere to best practices on cybersecurity awareness training at least annually, plan sponsors and fiduciaries should train and educate their own employees and plan participants at least annually on cybersecurity issues.

Organizations should:

- Ensure that all personnel given access to employee data and PII are properly trained in safeguarding it, including securing the transmission of any data to third-party service providers.

- Consider identity theft a key topic of training, and focus on current trends to exploit unauthorized access to systems.
- Update training to reflect risks identified by the most recent risk assessment.
- Ensure that internal personnel who handle employee data are properly vetted.
- Ensure that proper measures are taken to protect against security breaches from within the company.
- Perform background checks on all individuals with access to PII.
- Ensure all personnel given access to employee data and PII are trained in data retention and destruction, social networking, social engineering, and litigation holds.
- Designate an individual to be in charge of privacy and security of PII.
- Implement and test contingency plans for use if a data breach occurs.
- Perform periodic risk assessments, maintain good controls, and be careful about which parties can override them.
- Train employees responsible for contract and vendor management to review privacy and security issues in vendor arrangements.
- Ensure that plan fiduciaries address how they intend to handle and respond to a data breach in the Policy.
- Designate and train individuals to respond to any benefits-related data breach and follow procedures for reporting breaches using the appropriate channels of the organization.
- Identify who must be notified at the company, what should be reported to third-party service providers (to coordinate remediation efforts), notification procedures, and related tasks.
- Be on the lookout for individuals falsely posing as authorized plan officials, fiduciaries, participants, or beneficiaries.

Communicate with and Educate Employees

Education is a key aspect of cybersecurity awareness and training. The EBSA Cybersecurity Guidance includes a checklist of Online Security Tips that can be provided to plan participants and beneficiaries to assist them in reducing the risk of fraud and loss to their retirement accounts. To communicate with and educate employees, plan sponsors and fiduciaries should:

- Share the Online Security Tips from EBSA with participants and beneficiaries.
- Inform employees about the importance of safeguarding their data at all times and how to manage their online accounts.
- Consider identity theft as a key education topic, and focus on current trends to exploit unauthorized access to systems.
- Warn against email and phishing scams.
- Encourage use of regularly updated passwords with a high level of security and multi-factor authentication.
- Advise participants and beneficiaries to monitor their accounts and maintain updated antivirus software on computers and mobile devices.
- Focus on security measures in place for plan distributions, loans, and withdrawals.
- Prepare communications that remind participants and beneficiaries to safeguard their own benefit information, account balances, health information, passwords, and PINs.
- Advise against placing too much personal information on social networking sites and reviewing sensitive data on public computers or kiosks.
- Educate participants on how to protect information by:
  - locking computers;
  - using anti-spam and antivirus tools;
  - hiding information from cameras;
  - setting up two-step authentication to access accounts;
  - shredding documents;
  - securely storing documents and addressing storage;
  - limiting device sharing;
  - being alert to phishing;
  - protecting and updating passwords and PINs; and
  - swiftly reporting identity theft and cybersecurity incidents to the appropriate authorities.

Determine whether to include specifics regarding these issues and the Policy in a plan document and summary plan description (SPD) so that they can be clearly communicated to and acknowledged by participants. Having clear language in a plan document and SPD about procedures participants must follow to access their accounts and protect their data can serve as an extra layer of protection against fiduciary breach claims. (See Summary Plan Description (SPD) Toolkit.)

Plan sponsors should also consider the viability of including arbitration provisions within their plan documents and the extent to which these arbitration provisions incorporate claims brought for cybersecurity breaches or mishaps. In *Dorman v. Charles Schwab Corp.*, the US Court of Appeals for the Ninth Circuit overturned precedent by holding that ERISA claims can be subject to mandatory individual arbitration (934 F.3d 1107 (9th Cir. Aug. 20, 2019)). In a companion case, the court upheld the plan's arbitration provisions and class action waivers (*Dorman v. Charles Schwab Corp.*, 780 F. App'x 510 (9th Cir. Aug. 20, 2019)).

A plan provision requiring arbitration also may include an ERISA Section 502(a)(2) claim brought on behalf of a plan, and class waiver language may also serve to limit the scope of a dispute to losses to an individual account. That being said, questions posed in *Smith v. Board of Directors of Triad Manufacturing Inc.* on appeal before the US Court of Appeals for the Seventh Circuit concern whether ERISA violations and ERISA 502(a)(2) claims can be arbitrated or whether they create impermissible waivers of participants rights to pursue statutory remedies and impermissible requirements on participants to arbitrate fiduciary breach claims (Appellate Brief, No. 20-2708 (7th Cir. Jan. 26, 2021)). It is unclear whether class action waivers for ERISA fiduciary breach claims will be enforceable, whether arbitration provisions in retirement plan documents are likely to proliferate, and whether they would be beneficial or burdensome if a cybersecurity breach case arises. (See Arbitration of Disputes for Retirement Plans Toolkit.)

Plan sponsors and fiduciaries should also determine whether any special notices or disclosures under state or other applicable law regarding the collection or use of participant data are required, especially if ERISA preemption has not been reconciled (for example, under the California Consumer Privacy Act or California Privacy Rights Act).

Remote Working Issues

When employees work from home, companies may face additional risk from employees who take shortcuts to ease working on personal devices or outside of the organization's regular environment. For example, employees may:

- Send emails or other documents that contain PHI or other PII to their personal email addresses, which then may be automatically uploaded to their cloud-storage accounts.
- Upload sensitive data to their personal electronic devices that are unsecured or otherwise poorly protected.
- Physically take sensitive information home, either printed in hard copy or on flash drives, which can be lost or negligently shown to other individuals in the employee's home.

Similarly, hackers have exploited the chaos surrounding the COVID-19 pandemic and the ongoing remote and hybrid work arrangements companies have by sending out phishing emails purporting to provide employees with vital company policy or coronavirus updates. These emails request personal or essential login information that can give the hackers opportunities to infiltrate the organization's networks and databases.

It is impossible to predict or protect against every type of cyberattack, but plan sponsors and fiduciaries can take special actions to educate remote workers to protect sensitive data related to benefit plans, such as:

- Sending out reminders to employees to be extra vigilant.
- Providing access to cybersecurity training or webinars so that employees are reminded how to identify phishing scams and similar online attacks.
- Continuing ongoing employee communication efforts (see Communicate with and Educate Employees).

Prudent Standards for Selecting and Monitoring Service Providers

The EBSA Cybersecurity Guidance includes tips for hiring a service provider with strong cybersecurity practices. Plan sponsors and fiduciaries should consider those tips and also:

- Establish cybersecurity guidelines for engaging, monitoring, and renewing service providers, such as:
  - confirming the provider's cybersecurity program, information security standards, and certifications;
  - reviewing how they encrypt and protect data;
  - understanding their breach notification procedures;
  - reviewing service organization control reports or similar reports about their privacy and security controls, levels of insurance, and scope of coverage for losses caused by cybersecurity and identity theft breaches; and
  - reviewing the scope of their assumption of liabilities.

- Evaluate the service provider's track record in the industry, including public information on information security incidents, litigation, and other legal proceedings related to the vendor's services.
- Request information regarding the service provider's processes and systems for addressing cybersecurity threats and protection of PII, as well as past data breaches.
- Ensure third-party provider subcontractors are held to the same standards as the service provider.
- Develop a record of diligence efforts undertaken to document the level of security of third-party service providers.
- Understand where data is stored and how it is secured and protected.
- Engage the expertise of company IT professionals and legal counsel to review the service agreement's provisions on data security, data storage, websites, right to review audit results, breach notification, and confidentiality, and develop parameters for compliance representations and indemnification requirements.
- Establish procedures for any IT security review of service provider systems, including requests for penetration tests to detect security risks, and identify the best people to speak with vendors (for example, IT professional to IT professional).
- Develop a list of due diligence questions to ask service providers for RFPs and contract renewals, and select those providers with demonstrated security programs.
- Understand whether the service provider uses agents or subcontractors to perform the services and the chain of security measures and indemnification.
- Understand how participants and third parties access data (for example, through online access or requests for retirement account distributions or transfers).
- Request that the service provider use enhanced measures for participants to access the information, such as two-step or even three-step authentication (if not already doing so).
- Consider having the service provider generate and issue complex usernames and passwords, as participants frequently use the same passwords and usernames across different websites.
- Consider setting up alerts for unusual behavior, and educate employees on the steps they can take to protect their benefit plan information.
- Communicate with service providers as partners in the effort to protect plan data. Maintain open lines of communication and report suspicious activity.
- Connect organizational IT professionals with service provider IT professionals to address issues.
- Ensure that service agreements address compliance with cybersecurity and information security standards, third-party audits, confidentiality of information, notification of cybersecurity breaches, compliance with applicable laws governing privacy and security of personal information, and insurance coverage.

Cybersecurity Program Best Practices

The EBSA Cybersecurity Guidance includes Cybersecurity Program Best Practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data and for plan fiduciaries making prudent decisions on the service providers they should hire. The Cybersecurity Program Best Practices state that responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks and indicates that service providers should be evaluated based on:

- Their formal, well-documented cybersecurity program.
- Their performance of prudent annual risk assessments.
- Reliable annual third-party audits of the organization's security controls.
- Management of their cybersecurity program by senior executives and qualified personnel with clearly defined and assigned information security roles and responsibilities.
- Their strong access control procedures for authentication and authorization to access IT systems and data.
- Ensuring that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.
- Their implementation of periodic cybersecurity awareness training.
- Their implementation and management of a secure system development life cycle (SDLC) program.
- Their effective business resiliency program.
- Their implementation of current, prudent standards for encryption keys, message authentication, and hashing

to protect the confidentiality and integrity of the data at rest or in transit.

- Their implementation of strong technical controls in accordance with best security practices.
- Their appropriate response to any past cybersecurity incidents.

The Cybersecurity Program Best Practices advise that a prudently designed cybersecurity program will protect the infrastructure, information systems, and the information in the systems from unauthorized access, use, or other malicious acts by enabling the organization to:

- Identify the risks to assets, information, and systems.
- Protect each of the necessary assets, data, and systems.
- Detect and respond to cybersecurity events.
- Recover from an event.
- Disclose the event if appropriate.
- Restore normal operations and services.

Plan sponsors and fiduciaries should familiarize themselves with the best practices for reviewing a service provider's cybersecurity program. Further details of these best practices, and additional considerations, include:

- Strong access control procedures (see Strong Access Control Procedures).
- Cloud computing security (see Cloud Computing Security).
- A secure system development life cycle program (see Secure System Development Life Cycle Program).
- A business resiliency program (see Business Resiliency Program).
- Strong technical controls (see Strong Technical Controls).
- Responsiveness to cybersecurity incidents or breaches (see Responsiveness to Cybersecurity Incidents or Breaches).
- Mobile app security (see Mobile App Security).

Strong Access Control Procedures

The Cybersecurity Program Best Practices includes the following best security practices for access control:

- Limit access to systems, assets, and associated facilities to authorized users, processes, devices, activities, and transactions.
- Limit access privileges based on the role of the individual and adherence to the need-to-access principle.
- Review access privileges at least every three months, and disable or delete accounts in accordance with the policy.
- Use unique and complex passwords for all employees.
- Use multi-factor authentication, especially to access internal networks from an external network, unless a documented exception exists based on the use of a similarly effective access control method.
- Implement policies, procedures, and controls to monitor the activity of authorized users and to detect unauthorized access, use of, or tampering with nonpublic information.
- Implement procedures to ensure that any sensitive information about a participant or beneficiary in the service provider's records matches the information that the plan maintains about the participant.
- Confirm the identity of the authorized recipient of funds.

Cloud Computing Security

The Cybersecurity Program Best Practices notes that cloud computing presents many unique security challenges since visibility and control over data is limited. Plan sponsors and fiduciaries must understand the security posture of the cloud service providers to make sound decisions on using the service. In this context, best practices include:

- Requiring a risk assessment of third-party service providers.
- Defining minimum cybersecurity practices for third-party service providers.
- Periodically assessing third-party service providers based on potential risks.
- Ensuring that guidelines and contractual protections address third-party service providers':
  - access control policies and procedures, including the use of multi-factor authentication;
  - encryption policies and procedures; and
  - notification protocol for a cybersecurity event that directly impacts a customer's information system or nonpublic information.

Secure System Development Life Cycle Program

The Cybersecurity Program Best Practices defines a secure SDLC program as one that ensures that security assurance activities, such as penetration testing, code review, and architecture analysis, are a part of system development. These best practices include:

- Procedures, guidelines, and standards that ensure that any in-house applications are developed securely with such protections as:
  - configuring system alerts to trigger when an individual's account information has been changed;
  - requiring additional validation if personal information has been changed before a request for a distribution from the plan account; and
  - requiring additional validation for distributions (other than a rollover) of the entire balance of a participant's account.
- Procedures for evaluating or testing the security of externally developed applications, including periodic reviews and updates.
- A vulnerability management plan, including regular vulnerability scans.
- Annual penetration tests (particularly for customer-facing applications).

Business Resiliency Program

The Cybersecurity Program Best Practices define business resilience as the ability of an organization to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and data.

The main components of a business resiliency program are a business continuity plan, disaster recovery plan, and incident response plan. An effective business resiliency program should:

- Reasonably define the internal processes for responding to a cybersecurity event or disaster.
- Reasonably define plan goals.
- Define the documentation and reporting requirements for cybersecurity events and responses.
- Clearly define and describe individual roles, responsibilities, and authority levels.
- Describe external and internal communications and information sharing, including protocols to notify plan sponsor and affected users if needed.
- Identify remediation plans for any identified weaknesses in information systems.
- Include after-action reports that discuss how plans will be evaluated and updated following a cybersecurity event or disaster.
- Be annually tested based on possible risk scenarios.

Strong Technical Controls

Technical security controls are implemented and executed by the information system through the hardware, software, or firmware aspects of the system. The Cybersecurity Program Best Practices for technical security include:

- Keeping up to date hardware, software and firmware models and versions.
- Maintaining vendor-supported firewalls, intrusion detection and prevention appliances or tools.
- Keeping current and regularly updated antivirus software.
- Maintaining routine patch management (preferably automated).
- Network segregation.
- System hardening.
- Backing up routine data (preferably automated).

Responsiveness to Cybersecurity Incidents or Breaches

When a cybersecurity breach or incident occurs, the Cybersecurity Program Best Practices advises that the following action should be taken to protect the plan and its participants:

- Inform law enforcement.
- Notify the appropriate insurer.
- Investigate the incident.
- Give affected plans and participants the information necessary to prevent and reduce injury.
- Honor any contractual or legal obligations for the breach, including complying with agreed upon notification requirements.
- Fix the problems that caused the breach to prevent its recurrence.

Mobile App Security

The security of mobile apps should also be reviewed since many new mobile apps allow plan participants to:

- Check account balances, contributions, and investment changes.
- Request loans or distributions.
- Receive alerts and educational information.
- Track financial and physical wellness and collect and convey this information to benefit plans.

Despite the convenience of mobile apps, their use provides yet another opportunity for data breaches or the actual theft of assets and benefit payments. Plan fiduciaries should ensure that the Policy sets out the protocols that should be followed when introducing apps into any benefits program.

Suggested RFP Considerations from the 2016 ERISA Advisory Council

When contracting with service providers for plan administration, organizations must give providers access to plan data, which may be a potential source of a breach. The optimal time to address cybersecurity with a service provider is during the RFP stage. When contracting with and evaluating service providers, the 2016 Council suggested raising the following types of inquiries with service providers:

- Whether the service provider has a comprehensive and understandable cybersecurity program.
- The elements of the service provider's cybersecurity program.
- How plan data will be maintained and protected.
- Whether the data will be encrypted at rest, in transit, and on devices and whether encryption is automated (rather than manual).
- If the service provider will assume liability for breaches.
- If the service provider will stipulate to permitted uses and restrictions on data use.
- Whether the service provider has acceptable protocols for notifying plan management if a breach happens.
- Whether the service provider will agree to provide regular reports and monitoring and what the reports and monitoring would include.
- Whether the service provider regularly submits to voluntary external reviews of their controls (such as System and Organization Controls (SOC) reports or a similar report or certification).
- The level and types of insurance coverage the service provider carries.
- The level of financial and fraud coverage that will protect participants from financial damage.
- Whether the service provider insists on protections in its agreements with subcontractors (if any).
- The controls the service provider has in place over physical assets that store sensitive data, including when these assets are retired or replaced (for example, servers, hard drives, mobile devices).
- The service provider's hiring and training practices (for example, background checks, screening practices, and cyber training of personnel).

Service Agreements

Under the organization's Policy, and EBSA's tips for hiring a service provider, the service agreement should address:

- Data privacy and security compliance.
- Third-party audits.
- Breach notification procedures.
- Liability.
- Indemnification provisions.
- Insurance coverage.

Plan fiduciaries should also:

- Request periodic updates from their service providers on the cybersecurity measures they follow and any new initiatives, which should be noted in meeting minutes.
- Ensure an emergency response game plan is in place that meets standards under applicable laws to communicate any data security breach to participants, beneficiaries, and appropriate authorities.
- Perform due diligence for any service tools or apps (some apps may have a combination of financial, retirement plan, and health plan tools, which may require review under a broader array of privacy laws, HIPAA, and state law requirements).
- Review and negotiate service agreements at the same level of detail as other service provider agreements.

Provisions to consider for a service agreement may include:

- **Data privacy addendum.** Benefit plan service provider service agreements should include provisions addressing cybersecurity for benefit plans, including any breach notification and remediation procedures. It is common to request that the agreement include a data privacy addendum. An addendum may be offered by the service provider to reflect its information security program, or a plan sponsor may have its own form to be reviewed and negotiated for inclusion in the agreement. The data privacy addendum should:
  - identify and define in the agreement (or appropriate exhibits incorporated by reference) the security protocols that will be used for plan transactions and

distribution requests (for example, encryption, two-step authentication); and

  - address compliance with applicable privacy and security laws and industry standards.

- **Indemnification.** Review and negotiate indemnification provisions to contractually address risk and the extent to which risk is redirected to third parties.
- **Limitations of liability.** Review limitations of liability to determine if they carve out caps to damages for cybersecurity breaches and seek to carve out caps as they may apply to cybersecurity breaches. At a minimum, negotiate away caps on costs for breach notification and remediation.
- **Use of data.** Define any limitations that should apply on use of participant data (for example, use solely for services defined in the agreement, the location of processing and storage, applicable data transfer restrictions). Define applicable law for offshore data storage (for example, follow US law to maintain data under applicable state requirements, regardless of where data is managed, unless a more stringent law applies).
- **Breach response plan.** Define how any data breach must be handled (for example, define data breach remediation and notification procedures, timelines, and which party pays costs). Negotiate the right to review breach communications before they are distributed to participants.
- **Right to audit and security program updates.** Establish parameters for auditing third-party systems, receiving SOC reports, and receiving security program updates. Negotiate the right to make any related requests based on an audit or review.
- **Customer guarantees.** If a service provider offers a customer guarantee, seek to have the guarantee should specifically be incorporated into the service agreement.
- **Agents and subcontractors.** Negotiate service agreement privacy and security terms that also apply to any service provider agents and subcontractors, including terms that address destruction of data.
- **Termination of services.** Factor cybersecurity considerations and related provisions into causes for termination, especially provisions addressing data transmission, storage, and destruction.
- **Vendor insurance.** Confirm limits that apply to the vendor's applicable cyber coverage, request a certificate of insurance, and define available coverage in the service agreement.

Cyber Insurance

Cybersecurity insurance has emerged in recent years and can offer various types of coverage, including coverage for certain disaster recovery and data breach response assistance, that can be triggered by a benefit plan for a security breach. Organizations should:

- Assess existing insurance and liability coverages to find out how cybersecurity insurance can fit within employee benefit plan insurance needs.
- Evaluate any cybersecurity insurance to ensure that it does not carve out and exclude needed coverage, and then make any appropriate adjustments.
- Determine available coverage from a service provider and its interplay with the plan sponsor's own coverage.

The 2016 Council's Report noted that many insurance carriers now offer cyber insurance policies to augment existing insurance protection. In addition to third-party damage and defense costs, cyber insurance policies may include first party coverage, which means that an insured does not have to wait for a third party to sue the plan. This type of coverage may:

- Apply to:
  - cyber extortion;
  - data recovery;
  - business interruption; or
  - bad actors preventing an organization from operating.
- Cover costs related to investigations and monitoring.

With this coverage, the plan can trigger coverage on a breach to obtain direct risk management and services, such as disaster recovery and response assistance. Third-party coverage is triggered by a lawsuit and may include:

- Forensic investigations.
- The cost of legal advice or specialists.
- The settlement of lawsuits.
- The cost of remediation.
- Regulatory liability.
- Media liability.
- Credit monitoring.
- Credit freezes.

The 2016 Council's Report advised that, when considering the role that insurance is to play in a cybersecurity risk management strategy, it is important to:

- Determine what is included and excluded from insurance policies already in place for a cyber breach.
- Consider how the coverage compares to the cyber risk assessment.
- Determine if the coverage limits are acceptable.
- Confirm whether policy terms and conditions of coverage can be complied with.
- Consider the types of protection needed (for example, protection for participants against financial damage if a breach occurs, first party coverage to offer material assistance to respond to and recover from a breach, and coverage of the costs related to required breach notification and penalties for failure to comply with breach notification laws).
- Determine whether to review multiple policies, as policies can vary among carriers.
- Understand what is and is not covered by an insurance policy.

Plan sponsors and fiduciaries should also keep records of any breach investigations and steps taken to remedy the breach. Plan sponsors and fiduciaries should review fiduciary liability insurance and consider the potential interplay with cybersecurity insurance. (See Practice Note, Insurance for ERISA Fiduciaries.)

ERISA Bond

With certain exceptions, ERISA plan fiduciaries and every person handling plan funds or property must be bonded. Plan officials are considered to handle funds if their duties or activities may cause funds or other property to be lost if the officials commit fraud or dishonesty, either alone or in collusion with others (for example, if they have duties related to the receipt, safekeeping, and disbursement of funds, relationships that involve access to funds or other property, or decision-making powers regarding funds or property that can give rise to the risk of loss).

Plan sponsors and fiduciaries should determine whether they can or should obtain ERISA bonds at levels that protect against theft of plan assets by a plan fiduciary or person handling plan funds or property via a cyber-crime. The underlying terms of any ERISA bond must be reviewed for exclusions for cybercrime by plan fiduciaries or others handling plan funds. (See Practice Notes, ERISA Bonding Requirements and Insurance for ERISA Fiduciaries.)