Benefit Plan Cybersecurity Considerations: A Recordkeeper and Plan Perspective

Timothy Rouse, David Levine, Allison Itami, and Benjamin Taylor

December 2018

PRC WP2018-16
Pension Research Council Working Paper
Pension Research Council
The Wharton School, University of Pennsylvania
3620 Locust Walk, 3000 SH-DH
Philadelphia, PA 19104-6302
Tel.: 215.573.3414 Fax: 215.573.3418
Email: prc@wharton.upenn.edu
http://www.pensionresearchcouncil.org

Benefit Plan Cybersecurity Considerations: A Recordkeeper and Plan Perspective

Timothy Rouse, David Levine, Allison Itami, and Benjamin Taylor

Abstract

The U.S. has no comprehensive national law governing cybersecurity and no uniform framework for measuring the effectiveness of protections, though retirement plan record keepers maintain the personally identifiable information on millions of workers, collecting names, birth dates, social security numbers, and beneficiaries. Plan sponsors frequently engage consultants and attorneys to help them secure sensitive data, but more work is necessary to engage a larger discussion around this issue. The SPARK Institute has outlined a flexible approach for an independent third-party reporting of cyber security capabilities with several key control objectives.

Keywords: Cybersecurity, Personally Identifiable Information (PII), benefit plans, data security, robo-advisor

Timothy Rouse
SPARK Institute

David Levine
Groom Law Group

Allison Itami
Groom Law Group

Benjamin Taylor
Callan Consulting

Plan sponsors and fiduciaries[1] have traditionally relied on advisers—from attorneys to accountants to benefit consultants—to help guide decisions with respect to their retirement plans. For decades, a cornerstone of this assistance has been making recommendations about retirement plan investment portfolios. With the rise of both defined contribution (DC) plans and cyberattacks on financial institutions, a number of plan sponsors and their advisers have started to focus more time and resources on the security of their plan data, including the participant information held by service providers.

As plan sponsors and their advisers ask these providers more questions about cybersecurity, resistance to answering those inquiries has also risen. Service providers recognize the right of plan sponsors to confirm their participants' data is protected but fear the information, if distributed, could help cybercriminals breach systems.

Government regulators continue to grapple with how to develop workable regulatory structures. Rules by nature limit how providers can operate, which in turn helps cybercriminals focus their efforts at undermining those regulations. The United States Department of Labor (DOL) and the Employee Retirement Income Security Act of 1974 (ERISA) Advisory Council have, consistent with the flexibility adopted in other parts of ERISA, not required one single approach to ensure cybersecurity. States too have entered the cybersecurity discussion but, given ERISA preemption standards and the multistate nature of many retirement plans, face many challenges in imposing their own requirements upon ERISA plans.

The retirement industry itself has begun to develop its own solutions by working with all stakeholders—service providers of all shapes and sizes as well as plan sponsors. In this chapter, we present a solution for the challenge of verifying the cybersecurity capabilities of providers without revealing information that could help cybercriminals. The potential solution we present in

this paper relies on attestations provided by trusted third parties to audit the providers with a consistent set of standards. Since it is not a regulated solution, this approach is flexible enough to allow industry members to use whatever data security frameworks they feel are most appropriate for their organizations. Yet while providers are free under this potential solution to use frameworks of their choosing, the reporting of the controls used and how these controls were tested is designed to fit a uniform basic framework.

This chapter discusses the development, the components, and the communications process for this uniform basic framework, incorporating the perspectives of an investment consultant, a data security professional, and two lawyers. Retirement plans commonly employ advisers to assist with fiduciary oversight tasks such as selecting funds, benchmarking fees, and choosing third-party vendors such as recordkeepers, trustees, and custodians. These advisers include investment consulting firms, accountants, attorneys, and other industry experts. The vendor selection process is often led by investment consulting firms. The core competencies of these consulting firms are typically services such as asset allocation, capital market research, investment manager selection, monitoring, and other affiliated services. For many of these firms, the optimal approach to conducting vendor due diligence on complex administrative tasks has been to rely on third parties—whether auditors, attorneys, or other services—to verify the accuracy and thoroughness of the vendor's procedures. As DC plans have grown to be a larger part of the marketplace, these consulting firms shifted focus from defined benefit (DB) to DC services, and that shift included developing the ability to select and monitor recordkeepers and custodians.

Until now, firms conducting most of the vendor search and due diligence services in the marketplace have not had a primary focus on matters such as cybersecurity. Yet a handful of

leading-edge firms has been developing ways to help plan sponsors evaluate the cybersecurity protocols of their service providers.

At present, there is no consensus within the industry regarding which cybersecurity framework constitutes a 'best practice' approach. Additionally, the major frameworks address the matter slightly differently, and the implementation of each framework introduces additional variability.

The process of assessing security is further complicated by a destructive information cycle. Recordkeepers have significant incentives to reveal only a limited amount of information about their cyber defenses, because hackers can learn from extensive revelations to adapt their methods and avoid detection. This means that recordkeepers often rationally respond with only limited information about cyberattacks. This, in turn, causes some plan sponsors and consultants to react with renewed vigor in their efforts to confirm the adequacy of defenses, which can lead to either frustration or to recordkeepers complying with the requests, weakening their defenses.

There is significant room to improve the measurement of security within the vendor community, and later sections of this chapter will address the efforts SPARK and the ERISA Advisory Council, among others, have made in that direction. Ultimately, it is clear that the lack of cybersecurity expertise in the adviser community, the need for plan sponsors to protect participant data, and the lack of a uniform standard or process for third-party audits of cybersecurity measures, all call for a solution. That solution will ultimately very likely include an industry standard that permits third-party audit.

Existing Regulatory Structure

Gramm Leach Bliley. The 'Safeguard Rule' of the Gramm-Leach-Bliley Act of 1999 (GLBA) requires that covered U.S. financial institutions safeguard sensitive data (15 U.S.C. 6801). Businesses that are significantly engaged in providing financial products or services, such as banks and brokers, are covered financial institutions that must safeguard customers' personal information. This personal information includes nonpublic information that is personally identifiable financial information (known as National Provider Identifier, or NPI) collected by the financial institution. Items such as names, social security numbers, debt and payment history, and account numbers can be NPI when provided by the customer to the financial institution.

According to the law, the goal of the Safeguard Rule is to:

> Ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. (5 U.S.C. 6801(b)).

It establishes standards relating to physical, technical, and administrative information safeguards. It also requires a written information security program that contains certain basic elements, has a continuous life-cycle, and is subject to revision as experience warrants.

The written plan must include (16 C.F.R. § 314):

(1) The appointment of a person responsible for coordinating the program;
(2) Identification of reasonably foreseeable internal and external risks, and an assessment of the sufficiency of any safeguards against those risks in these areas:
    a. Employee training and management
    b. Information systems, including information processing, storage, transmission and disposal, network software and design
    c. Detection, prevention, and response to attacks, intrusions, or other systems failures
(3) The procedure for designing, implementing, and testing of information safeguards
(4) Protocols for overseeing service providers capable of maintaining appropriate safeguards

(5) Rules for evaluating and adjusting the security program to react to any material business changes.

Under the Safeguard Rule, it is interesting to note, there is no obligation for a financial institution to disclose its information security program.

Title V privacy. Under GLBA's 'Privacy Rule,' financial institutions in possession of NPI must also provide customers with notices regarding the use of their NPI and give them the opportunity to opt out of sharing that data with unaffiliated third parties, unless subject to an exception (15 U.S.C. § 6802).

Prudent protections. ERISA imposes a standard of care on plan fiduciaries. One becomes a plan fiduciary either by being named as such, or through actions that result in the exercise of discretionary authority or control with respect to the management of a plan or its assets; providing investment advice for compensation; or having discretionary authority or responsibility in the administration of a plan (ERISA § 3(21)).

Fiduciaries are subject to the prudent expert standard of care and owe a duty of loyalty to the plan participants. A prudent expert acts with the care, skill, and diligence that the circumstances call for a person of like character and like aims to use. Fiduciaries must discharge their duties solely in the interest of plan participants and beneficiaries for the exclusive purpose of providing benefits to those participants and beneficiaries (ERISA § 404).

ERISA also requires that plan assets be held in trust by one or more trustees and that the indicia of ownership of such assets be held within the jurisdiction of the district courts of the United States (ERISA §§ 403 and 404).

Undeniably, the monetary assets of the participant accounts are plan assets and a fiduciary must undertake prudent steps to protect them from theft, including theft by means of a cyberbreach. However, unlike the HIPAA rules (45 C.F.R. 160, 162, and 164) that apply to health care data for

ERISA-covered health care plans, there is no clear ERISA regulatory scheme governing the protection of financial information in retirement plans.

Whether a failure to protect retirement-related financial data results in a fiduciary breach turns on whether the financial data is considered a plan asset. If it is a plan asset, then failure to take prudent steps to prevent its loss or misuse likely results in a fiduciary breach.

Several different tests could be applied to determine whether plan data is a plan asset, although none have been applied by a court directly to personal financial data. It has been the DOL's position that 'the assets of a plan generally are to be identified on the basis of ordinary notions of property rights under non-ERISA law' (DOL Adv. Op. 92-02A (Jan 17, 1992)). Courts have applied other tests such as whether the data have any value and whether the assets were viewed or treated as plan assets (*Patient Advocates, LLC v. Prysunka*, 316 F. Supp. 2d 46, 49 (D. Me. 2004)). In *Acosta v. Pacific Enterprises,* the court said that

> [i]n order to determine whether a particular item constitutes an 'asset of the plan,' it is necessary to determine whether the item in question may be used to the benefit (financial or otherwise) of the fiduciary at the expense of the plan participants or beneficiaries (950 F.2d 611, 620 (9th Cir.1990)).

Another court found that plan assets must have some sort of inherent value, be capable of the assignment of value, or otherwise be subject to market forces (*Grindstaff v. Green*, 133 F.3d 416, 423, 425 (6th Cir. 1998)).

The need to protect the privacy of certain participant information has been directly addressed by the USDOL. For example, information relating to participant actions related to employer securities is briefly touched upon in the context of ERISA section 404(c). Additionally, the concept of securing private participant information in connection with a retirement plan is also raised by DOL Technical Release No. 2011-03 addressing certain electronic disclosures.

Given the focus on the value of personal data in our society, a conservative approach is to treat plan participant financial data as being a plan asset and take prudent steps to protect it as such.

International regulations. The European Union General Data Protection Regulation (GDPR) is the foremost set of European rules on information privacy,[2] with requirements applying as of May 2018. 'Data subjects' are persons that provide their individual information to companies, if they are identifiable from that information. Personal data includes financial data. These data subjects have rights under the GDPR with regard to companies that 'process' the data. Processing data has a very broad definition that includes collection and storage. There are core principles that apply to the companies that possess the data including: lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. These principles encompass many of the goals found in the separate privacy laws in the United States, but they are combined into a single scheme that is applicable much more broadly than any current U.S. law. Under the GDPR, data subjects have many rights, including the right to be 'forgotten,' or erased from a company's data; the right to portability of the data; and the right not to be profiled if this has legal effects on the data subject.

The GDPR imposes many rules on the companies that act as a data controller and data processer regarding the safeguarding of personal data aimed towards achieving the core principles. These range from required contractual provisions to notifications of a breach.

This regulatory scheme is acknowledged as being one of, if not the most, comprehensive data protection regimes in the world. The GDPR has some extraterritorial implications applying to data from Europeans outside of Europe that are less likely to apply to a U.S.-based retirement plan, but potentially could apply.

Regulatory Directions

There is no comprehensive federal regulatory scheme governing cybersecurity for retirement plans in the US. Likewise, there is no comprehensive federal scheme that covers their service providers, as not all are subject to GLBA. ERISA is silent on data protection in the form of electronic records, and the US courts have not yet decided whether managing cybersecurity risk is a fiduciary function. Many providers that service the retirement market are covered by federal rules based on their industry. However, these same retirement plan service providers often cross several different industries, making compliance more of a patchwork.

To address these gaps, some states have started to create their own laws which typically address breach notifications and private rights of action for any unauthorized disclosures of protected personal information. While several state attorneys general have been active in enforcing these laws in cyberbreach cases, a state-by-state framework remains a patchwork solution.

ERISA Advisory Council. Despite a lack of federal regulation, the DOL and the ERISA Advisory Council (2016) recently recommended that the DOL communicate to the employee benefits community the cybersecurity risks and potential approaches for managing those risks (ERISA 2016). The ERISA Advisory Council's proposal to the DOL included guidance for plan sponsors on how to evaluate cyber-risks for their benefit plans, requiring them to: understand the plan's data; know the different security frameworks used to protect data; build an adaptive cybersecurity process that includes implementation and monitoring, testing and updating, reporting, training, controlling access, data retention and destruction, and third-party risk management. Additionally, the guidance required these sponsors to: customize a strategy to fit the unique needs of the plan sponsor; balance the plan sponsor's threats based on size, complexity, and risk exposure; and address state law considerations.

While ERISA does not outline specific rules for protecting data, the DOL did recognize the risks associated with electronic communications of plan information. For instance, in Regulation Section 2520.104b-1(c), the DOL addressed electronic distribution of plan information to participants, by saying that plan administrators must take appropriate measures to 'protect the confidentiality of personal information relating to the individual's accounts and benefits.' These measures were designed to prevent unauthorized receipt of information or access to such information by individuals other than the intended user. Additionally, DOL Technical Release No. 2011-03 addressed participant information available on administrators' websites and required the plan administrator to take appropriate and necessary measures reasonably calculated to ensure that the electronic delivery system protects the confidentiality of all personal information. How best to achieve the confidentiality of personal information relating to individuals' accounts and benefits is not well defined.

Despite the ERISA Advisory Council's recommendations on how to evaluate risks, important questions remain unanswered. For example, is cybersecurity an ERISA fiduciary responsibility? If so, does ERISA preempt state cybersecurity laws? Plan sponsors and service providers already take seriously their responsibilities to protect participant data, but where are the lines of responsibilities and accountability in the event of a breach?

Other Legal Considerations

For some plans, such as state and local government-sponsored plans, ERISA and its preemption do not apply. Moreover, even for ERISA-covered plans, it is not clear that state privacy or cybersecurity statutes would be preempted by ERISA.

Governmental plans. Many governmental plans, especially on the state level, have adopted ERISA statutory language nearly word-for-word. For example, retirement systems in numerous states such as the District of Columbia, Illinois, and Ohio, have used substantially the same language as ERISA to govern state plans (7 DCMR 15; 40 ILCS 5/; ORC145.01). Most of these plans will look to how an ERISA plan or an ERISA service provider would address the same situation, in order to determine what actions and remedies are appropriate. A court would also do the same in these jurisdictions. In other jurisdictions, the fiduciary concepts are similar to ERISA even when the statutory language is different, and courts are again likely to look to ERISA precedent.

State statutes. While ERISA was intended to prevent a patchwork of state law requirements from applying to the same plan, it is not clear that personal privacy and cybersecurity statutes would be preempted by ERISA. Clearly ERISA predates the widespread use of the internet and the general awareness of cyberthreats. The lack of comprehensive financial privacy protections in ERISA could lead courts to determine that no ERISA preemption occurs with respect to state protections. A majority of states have statutes regarding privacy, cybersecurity, financial information, or all of the above. For example, Massachusetts has its 'Standards for the Protection of Personal Information of Residents of the Commonwealth' (201 CMR 17.04). A written information security program is required for entities including employers that maintain personally identifiable financial information about a Massachusetts resident. Statutes and regulations such as those adopted by Massachusetts can provide plan sponsors, fiduciaries, and service providers with additional reference points for constructing their own cybersecurity protocols for retirement plans.

Another prominent example is the New York Department of Financial Services regulation, considered to be one of the most comprehensive cyber-security regulations at the state level.

Entitled Cybersecurity Requirements for Financial Services Companies, the ruling was promulgated in 2017 and covers financial services companies operating under a license or certification issued under the New York Banking, Insurance, or Financial Services laws (23 NYCRR 500). It aims to set certain minimum standards for cyber-security programs that keep pace with technological advances, while promoting the protection of customer information. It requires involvement from senior level management to file an annual statement of compliance with the New York Department of Financial Services. While there are staged deadlines, compliance generally requires having a cyber-security program, policies, penetration testing, an incident recovery plan, risk assessment, encryption of non-public information, and training and monitoring (*Id.*).

Cybersecurity breach examples. Cyberbreaches have become an unfortunate part of commerce today. Whenever and wherever value has been stored, thieves have always tried to take it. The motives remain the same, but the methods and means of stealing have adapted to where and how we store value. The United States is by far the number one target, followed by the United Kingdom (Tech World 2017). Some of the most infamous breaches of the last several years have exposed millions and in a few cases, billions of individuals to identity theft. Well-known cases include:

(1) Uber: Over 57 million customers and drivers had their names, emails, and phone numbers stolen in 2016;

(2) Target: In 2013, the firm's customers had their names, credit/debit card numbers, expiration dates, and card values stolen. The theft involved over 70 million retail customer accounts. Investigations showed the thieves entered the retailer's systems through a third-party refrigeration company hired by Target to help renovate some stores; and

(3) Equifax: This firm's 2017 breach is one of the most serious ever because it included the names, social security numbers, dates of birth, and addresses for more than 143 million.

Cyberattacks tend to fall into several general categories which information security officers use to identify countermeasures and solutions based on the different types of attacks:

Phishing. Hackers pose as a trusted vendor or third party and request data, often providing a link for victims to enter personal data. While phishing emails have gotten much more sophisticated in recent years, consumers have also become more sophisticated. Many consumers verify such requests directly with their financial institutions before clicking on links or providing information. Nevertheless, a vulnerable population and a favorite target for hackers are the elderly. To combat these attacks, most companies stress to clients that they will not ask for personal information via email, and tell them that if they receive such a request they should report it immediately to the firm.

Malware. This term includes several cyberthreats such as trojans, viruses, and worms. In simple terms it refers to any code with malicious intent that typically steals or destroys data or locks a computer. Recordkeepers protect against such attacks through firewalls that catch malware programs before they get into a system, or by educating employees not to click on suspicious links or download attachments from unknown senders. This is sometimes done by deploying robust and updated firewalls, which prevent the transfer of large data files over the network to weed out attachments that may contain malware. It is also important to continually ensure all computer operating systems are updated and use the most recent security programs.

Rouge Software. This is a newer type of malware that masquerades as legitimate security software. The criminal designs the software to make pop-up windows and alerts that look authentic. Once a user downloads the new security software, the corrupt software is downloaded to the user's

computer. An organization's information technology practices can help prevent these attacks with updated firewalls or trusted anti-virus or anti-spyware software.

Password Attacks. These happen when a thief gains access to a customer's account by cracking the user's password. This type of attack is often simple and does not usually require any type of malicious code or software. Hackers use software to guess passwords by comparing various word combinations against a dictionary file. Recordkeepers typically require their clients to use sophisticated passwords that include a combination of letters, numbers, and special characters, as well as limiting the number of failed login attempts.

Denial-of-Service (DoS) Attacks. A DoS attack disrupts the service to a network. Attackers will send a high volume of data requests to a network until it becomes overloaded and can no longer function. Attackers typically use several means of attack, but the most common is the distributed-denial-of-service (DDoS) attack: this involves the attacker using multiple computers to send the traffic or data to overload the system. Often computer users do not even realize that their computers have been hijacked. Many of these types of attacks are not intended to steal data or money, but to protest something. Although recordkeepers are not typically the targets of these types of attacks, they help prevent them by monitoring security as well as data flows to identify any unusual or threatening spikes in traffic before these become a problem. DoS attacks can also be accomplished by physically cutting cables or disconnecting servers, which is why firms also protect their physical properties and systems.

'Man in the Middle' (MITM). Sophisticated hackers will often impersonate an organization's login page or endpoint. From here they will ask the client for online information. For example, if you are banking online, the man in the middle would communicate with you by impersonating your bank, and communicate with the bank by impersonating you. The man in the middle would then

receive all the information transferred between both parties, which could include sensitive data such as bank accounts and personal information. Recordkeepers and other financial firms usually require clients to use only encrypted access points.

Drive-By Downloads. Through malware on a legitimate website or detachable drive, a program is downloaded to a user's system just by visiting the site or connecting to the target's system. Typically, a small snippet of code is downloaded to the user's system and that code then reaches out to another computer to get the rest of the program. It often exploits vulnerabilities in the user's operating system or in other programs. Some thieves have even labeled thumb drives with 'payroll' and dropped them in an organization's parking lot. The intent is for an unsuspecting employee to pick up the thumb drive and connect it to a secure computer. Once that happens, the malware code is released. Organizations protect against these attacks in various ways such as education, strict rules against use of detachable drives, and restrictions on web browsing.

Data Security Best Practices

The Data Security Oversight Board (DSOB) of Spark Institute has developed standards to help recordkeepers communicate the full capabilities of their cybersecurity systems to plan sponsors, consultants, and others. These standards are not intended to provide a recommended level of cyber protection or guarantee against a data breach or loss. Instead, these standards are intended to help establish a uniform communications tool to assist plan sponsors and service providers in properly assessing and comparing retirement plan vendors.

Plan sponsors and their consultants generally understand that recordkeepers need to maintain a level of secrecy around the products and processes used to secure client data. Conversely, recordkeepers know that clients and prospects have legitimate needs to understand

how their data are protected. These standards establish a base of communication between recordkeepers and sponsors using independent third-party audits of cybersecurity controls. With this tool, vendors can properly validate the robust nature of their cybersecurity systems and provide assurances to clients and prospects that their systems are protected against hackers.

A firm's overall data security capabilities identify recommended control objectives in 16 areas critical to data security as defined by SPARK. The resulting audit reports identify the primary applications and processing systems that support the services offered. Recordkeepers and service providers can report their results in two ways. First, they can generate a Service Organization Control (SOC 2) report, conducted under the AICPA audit standards. This focuses on controls at a firm relevant to security, availability, processing integrity, confidentiality, or privacy (AICPA 2017). Second, they can produce an Agreed Upon Procedures (AUP) report, in which an auditor is contracted to issue a report or findings based on specific agreed-upon procedures with the client applied to cybersecurity controls for use by specified parties (AICPA – AT-C Section 215).[3]

Section III of the SOC 2 or the cover page of an AUP would be used to address which systems are within the scope of the audit and which are not. The scope of these audits includes anywhere customer or plan-provided NPI or Personally Identifiable Information (PII) is processed or stored. PII is defined as (US Department of Labor 2017, n.p.):

> Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors) … Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

NPI is defined as (Federal Trade Commission 2002, 4-5):

> Any information an individual gives you to get a financial product or service (for example, name, address, income, social security number, or other information on an application); Any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or Any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

The detailed control objectives section of the auditor's report must include each control objective, the test procedures, and the results. The format for this report should follow a format similar to that outlined in Table 1.

Table 1 here

Table 2 here

How cybersecurity testing results are reported can differ in several ways. First, firms can choose to perform an AUP engagement. This is one in which an auditor is engaged to issue a report and findings based on specific agreed-upon procedures that apply to certain subject matters for use by specified parties. In this case, the specified parties would typically be a client plan sponsor that requires independent proof of cybersecurity capabilities. Under AICPA guidelines, the specified parties determine the procedures they believe appropriate to be used by the auditor. This creates a slight challenge when using the SPARK Industry Best Practices, since these 16 categories and the controls aligned to these categories by the recordkeeper must be accepted as appropriate by the client. Client acceptance of the procedures can take several forms and be a formal letter or a simple email.[4]

A SOC 2, or Service Organization Control report 2, addresses a firm's controls related to operations, availability, security, processing integrity, confidentiality, and privacy. The report follows the five AICPA Trust Services principles and includes detailed descriptions of the auditor's test of controls and results.

The Role of an ERISA Attorney

While investment consultants often play a lead role, ERISA attorneys are regularly deeply involved in the Request for Proposal (RFP) process when a retirement plan puts services out to bid and in the response to such requests. By understanding the SPARK Best Practices prior to entering into the RFP process, the ERISA attorney can facilitate communication between the parties. ERISA attorneys for recordkeeping institutions can use this knowledge to respond to RFPs that may, at first, not necessarily focus on cybersecurity in a coherent manner. By providing thoughtful responses and information to an RFP request, the ERISA attorney can focus plan sponsors on the items most appropriate for a benefit plan. While procurement and technology personnel are adept at cybersecurity as it relates to the plan sponsor's business, the ERISA attorney will be able to provide guidance regarding norms for benefit plans, which will help align a plan fiduciary's behavior with that of other prudent experts in similar circumstances in keeping with ERISA's standard of care. By facilitating understanding of the standards and practices, an informed ERISA attorney can help the benefit plan seek and obtain cybersecurity protection appropriate for particular needs of a retirement plan, while also reducing liability exposure for the plan's fiduciary.

The Road Ahead for Cyber Security and Employee Benefits

Plan sponsor next steps. Plan sponsors will need to quickly educate themselves about the benefit plan cybersecurity environment. This could involve a presentation to plan sponsor personnel with responsibility for a retirement plan, or by attending a conference for human resource professionals regarding plan cybersecurity. Awareness of the issue can help obtain buy-in to expend resources so as not to lag behind other plan stewards. Education can also help set realistic expectations,

because total prevention is not achievable, and total outsourcing of cybersecurity is also unlikely. With these fundamentals established, a plan sponsor can begin or further a productive endeavor towards retirement plan data security that meets the applicable fiduciary standards.

Moreover, plan fiduciaries might consider going on a 'data diet' to reduce the amount of retirement plan information shared among the plan, the plan sponsor, and service providers. Like any diet, the first step is to identify what data are currently being collected, produced, retained, and shared. From there, it is likely that a plan sponsor may be able to identify excess at each of these stages. As part of this process, plan sponsors might evaluate whether each recipient truly requires the full scope of data being shared to accomplish the task at hand, and if not, whether there is an operationally efficient manner to reduce the creation, transfer, and storage of excess data. By reducing the data at play, a plan sponsor can limit the plan's exposure to a cybersecurity attack. Of course, the degree to which a plan sponsor will have leverage to modify existing practices is likely to depend on the size and assets of its plan.

ERISA does not mandate a written cybersecurity or financial information policy, and there is no one-size-fits-all approach that must be taken. Instead, a plan sponsor must act prudently. The easiest way to show that a plan sponsor has followed a prudent process is to document that process. Creating any prescriptive document beyond those required by ERISA can carry significant challenges and risks, so cybersecurity documents should focus on process items rather than attempting to lay out any hard and fast rules.

Cybersecurity incidents or breaches involving plan sponsors are a question of when, not if. Therefore, plan sponsors might also consider a response-and-recovery plan. The timing of the development of such a plan can vary widely—from proactively or after-the-fact. Fiduciary insurance is typically triggered when a lawsuit is filed or regulatory investigation is commenced

(or sometimes when a regulator asserts a deficiency), while cyber insurance is often triggered by a data breach. This means that while existing fiduciary insurance may help after a lawsuit is filed, but prior to that point, the plan and/or plan sponsor may be responsible for the costs and mechanics associated with a breach (depending on the terms of the insurance policy). These include finding, hiring, and paying for experts to assess the scope of the breach and develop a mitigation plan, as well as finding the capacity to notify and respond to participant inquiries regarding an incident.

Plan sponsors may wish to seek specific cyber insurance policies or riders to existing policies (some of which are available in the market today) to cover the employee benefit plan(s). Policies that provide benefits upon a breach can offer assistance in locating the appropriate personnel to address each step of the process, from determining the scope of the breach, to notifying the appropriate individuals or entities, to providing resources to mitigate, or making whole any damages suffered as a result of the breach, such as identity monitoring or replacing stolen assets. Plan sponsors will also wish to consider how to evaluate and update their plan-related cybersecurity approach on a periodic basis.

Conclusion

The cybersecurity environment for retirement plans is undergoing significant evolution, and this evolution is likely going to continue to accelerate. While the precise fiduciary obligations of plan sponsors with respect to plan and participant information are not yet clearly defined, it is clear that multiple efforts are underway to define those obligations, and to respond to the increasing need to strengthen protections. Presently, the SEC, the DOL, multiple states, and key industry organizations like SPARK are working to regulate cybersecurity and develop increased protections.

As these efforts proceed, it is essential that plan sponsors work together with their vendors, including recordkeepers, consultants, accountants and attorneys to put in place adequate safeguards. For these safeguards to be successful, it will also be essential to develop common practices for conducting due diligence with respect to these safeguards while also avoiding disclosures that may help malicious actors. The SPARK standards, applied via a SOC2 or AUP, can serve as an essential starting point and provide the opportunity to receive assurance of industry-vetted practices via a trusted third party. Plan sponsors may also benefit from careful review of their insurance coverages with respect to cybersecurity, as there is a wide range of available protections including common gaps with respect to when policies are triggered or what they provide.

References

AICPA (2017). *AT-C Section 215: Agreed-Upon Procedures Engagements.* Association of International Certified Professional Accountants. https://www.aicpa.org/research/standards/auditattest/downloadabledocuments/at-c-00215.pdf

ERISA Advisory Council (ERISA) (2016). *Cybersecurity Considerations for Benefit Plans*. Report to the Honorable Thomas E. Perez, United States Secretary of Labor. https://www.dol.gov/sites/default/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf

Federal Trade Commission (2002). *How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*. Washington, DC: FTC. https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf

The SPARK Institute (2017). 'Industry Best Practice Data Security Reporting.' *SPARK Institute Release 1.0*. September 20. http://www.sparkinstitute.org/pdf/SPARK%20Data%20Security%20Industry%20Best%20Practice%20Standards%209-2017.pdf

Tech World (2017). 'The Most Infamous Data Breaches.' *Tech World*. December 6: https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

US Department of Labor (2017). *Guidance on the Protection of Personal Identifiable Information.* https://www.dol.gov/general/ppii

Endnotes

[1] This chapter refers to 'plan sponsors' as including both plan sponsors and plan fiduciaries. Although there are important lines between plan sponsor 'settlor' advice and fiduciary activities, for ease of communication we have used the term 'plan sponsor' throughout.

[2] Regulation (EU) 2016/679 (General Regulation of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC 25).

[3] Under AICPA standards, an AUP is only to be used by the parties that agreed to the procedures. Any AUP that is used over again for new clients would first require that client to accept the original agreed upon procedures.

[4] A self-assessment using the SPARK Institute's Cyber Security Best Practices is only a stopgap process to help aid in industry adoption. Recordkeeping firms can use the SPARK 16 Cyber Security Categories and report their controls and test results without third-party attestation, but only until they can contract with their audit firms to do independent reporting.

Table 6.1. Sample Format: SPARK Data Security Report

Controls	Test Procedures	Results
Each control tested is defined and aligned to one of SPARK's 16 key areas of security focus.	Test parameters: Define what was tested and how test was performed.	Summarize test results (i.e., no exceptions noted or exception noted and provide details).

Source: The SPARK Institute (2017).

Table 6.2. Spark Institute 16 Control Objectives for Communicating Cybersecurity Capabilities

Control Objective	Description	Sample Controls[a]
(1) Risk Assessment and Treatment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	*Technology risk assessments are completed.*
(2) Security Policy	Organizational information security policy is established.	*Security policies are approved and communicated.*
(3) Organizational Security	Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.	*A CISO or ISO has been assigned.*
(4) Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	*IT application records are maintained in a formal system of record.*
(5) Human Resource Security	The organization's personnel and partners are suitable for the roles they are considered for, are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	*Personnel are subject to initial and periodic background checks*
(6) Physical and Environmental Security	Physical access to assets is managed and protected.	*Data centers are secured 24x7x365 with on-site physical security controls.*
(7) Communications and Operations Management	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	*Networks and systems include standard data security tools such as firewalls, antivirus, intrusion detection, and patch management.*
(8) Access Control	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	*Unique, complex passwords are assigned to all employees.*
(9) Information Systems Acquisition Development	A system development life cycle (SDLC) to manage systems is implemented; a vulnerability management plan is developed and	*Regular penetration tests are conducted on customer-facing applications.*

	implemented, and vulnerability scans are performed.	
(10) Incident and Event Communications Management	Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events.	*Cyber incident procedures are documented and routinely tested.*
(11) Business Resiliency	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	*The organization maintains and tests BCP and DR plans.*
(12) Compliance	Legal requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	*Policies and procedures are in place to enforce applicable privacy obligation.*
(13) Mobile	A formal policy shall be in place and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.	*A mobile policy is approved and enforced.*
(14) Encryption	Data-at-rest and data-in-transit are protected.	*External transmissions are encrypted using FIPS-approved algorithms.*
(15) Supplier Risk	Ensure protection of the organization's assets that is accessible by suppliers.	*Suppliers are subject to periodic security reviews.*
(16) Cloud Security	Ensure protection of the organization's assets that are stored or processed in cloud environments	*Cloud providers are subject to periodic security reviews or can provide independent security assessments of their environment.*

Notes:
[a] For illustrative purposes only; not intended to be a list of controls.

Source: The SPARK Institute (2017).