Bloomberg Law

Pension & Benefits Daily™

Record Keeping

View From Groom: Cybersecurity as It Relates to Retirement Plan Data

BY JENNIFER E. ELLER AND ALLISON A. ITAMI

Cybersecurity related articles dominate the front pages of newspapers on a weekly basis. Incidents ranging from the recent Equifax breach to the breach of the federal government's Office of Personnel Management files are high profile examples of widespread data breaches. Other cyber threats include ransomware attacks that restrict access to data until a ransom is paid and phishing attempts to have individuals disclose security information voluntarily.

Cybersecurity can be loosely defined as the preventative techniques used to protect the integrity of networks, programs and data from attack, damage, or unauthorized access. While few of these headlines relate to ERISA retirement plans, it may be only a matter of time before they do.

In fact, Bloomberg BNA reported on an ERISA related ransomware attack in November 2016 that demanded approximately $2,000 worth of bitcoins be paid for the release of computer servers. While the ransom was ultimately not paid in this case, it may be just the first of the reported cybersecurity incidents directly impacting retirement plans.

Jennifer E. Eller (jeller@groom.com) is the co-head of Groom Law Group's Fiduciary Practice Group. She advises financial institutions on the design and delivery of products and services to the retirement plan marketplace, and advises large corporate and public plan sponsors on all aspects of ERISA fiduciary compliance.

Allison A. Itami (aitami@groom.com) is an associate in the Fiduciary Practice Group at Groom Law Group where she advises employers and service providers on employee benefit programs. Her practice focuses primarily on federal laws such as ERISA and the Internal Revenue Code, and the ways in which state laws affect benefit plans.

Data as a Plan Asset

Data provided by participants and beneficiaries to retirement plan record keepers and service providers often includes significant personal identifying information. In the wrong hands, this information can create serious identity theft issues for plan participants and beneficiaries.

Importantly, courts have found that plan data is an asset of the plan under ERISA. Under section 404 of ERISA, a plan's fiduciaries must discharge their duties with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims. Therefore, arguably, as it becomes prevalent for other ERISA fiduciaries to use procedures to secure online plan data from cyberattacks, as a matter of prudence, an ERISA fiduciary should also implement such procedures.

The trend certainly seems to be that ERISA fiduciaries are actively seeking advice regarding cybersecurity related duties and have implemented, are in the process of implementing, or are starting to consider the protection of plan data vis a vis cyberattacks.

Guidance Related to ERISA Plans

Given the apparent need for fiduciaries to consider a prudent process for protecting plan data, where should a fiduciary turn for guidance? The 2016 Advisory Council on Employee Welfare and Pension Benefit Plans prepared a report, ''Cybersecurity Considerations for Benefit Plans'', which suggested that plan sponsors and fiduciaries consider a framework upon which to base their cybersecurity risk management strategy.

The 2016 Council identified several key components of a cybersecurity strategy, including:

■ Describing a process to identify risks;

■ Developing a program to protect data that could be at risk;

■ Stating how breaches will be detected. Security penetration testing may be helpful in determining vulnerability;

■ Establishing a response plan for security breaches in order to minimize damage.

Likewise, the SPARK Institute developed ''standards to help record keepers communicate, to plan consultants, clients and prospects, the full capabilities of their cybersecurity systems.'' These were recently issued at the end of September 2017 with the intent that they be used to facilitate conversations between providers and sponsors regarding cybersecurity systems and are comprised of six recommendations and sixteen control objectives.

Guidance From Alternative Sources

Plan fiduciaries may also look to other sources for assistance in developing cybersecurity risk management procedures for their plans. For example, there is guidance from the American Institute of CPAs and from a multitude of state privacy laws, including from Massachusetts with the Standards for the Protection of Personal Information of Residents of the Commonwealth.

1) The American Institute of CPAs SOC The American Institute of CPAs (AICPA) has developed a framework for organizations to use in connection with their cybersecurity risk management programs. The framework includes a Systems and Organizations Controls (SOC) component and guidance that the AICPA states ''can help senior management, boards of directors, analysts, investors and business partners gain a better understanding of organizations' efforts''. The SOC guidance helps to articulate key concepts and terms to effectively describe cybersecurity risk management programs. AICPA also states that it will be issuing future guidance that is intended for use at the supply chain level.

2) Standards for the Protection of Personal Information of Residents of the Commonwealth While many states have their own privacy laws, the Massachusetts statute covers financial account information and provides a list of action items covered entities, such as employers, should take and provides a list of electronic security related items that must be included in its written information security program. Specifically these include:

(1) Secure user authentication protocols including:

(a) control of user IDs and other identifiers;

(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

(c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

(d) restricting access to active users and active user accounts only; and

(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(2) Secure access control measures that:

(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and

(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;

(5) Encryption of all personal information stored on laptops or other portable devices;

(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.'' 201 CMR 17.04.

Liability Protection and Insurance

1) Inventory & Review One of the first steps in liability protection should be an inventory of the plan data. Is it all necessary to the operation of the plan? Who has access to it? The next logical step is to review service provider contracts to determine what notice provisions each provider has with respect to data breaches and the liability associated with such breaches. Do the contracts address cybersecurity readiness? Once the plan fiduciary is able to identify the plan data owned by the plan, the scope of third party provider protection and exposure that is related to the operation of the plan, he or she will be in the best position to determine the best next steps for protecting plan data and limiting liability.

2) SAFETY Act The Support Anti-terrorism by Fostering Effective Technologies Act of 2002 or SAFETY Act is aimed at preventing liability concerns from impeding the dissemination of technologies and products that could save lives and limit harm to Americans in the event of an act of terrorism by limiting third party liability related to those technologies. The Department of Homeland Security (DHS) runs the SAFETY Act program and interprets harm to cover financial harm. It covers software, services, and intellectual property, including information technology. The list of approval technologies ranges from a safety procedure at an NFL stadium to cybersecurity consulting services and testing technology.

  ISSN

Purchasing or utilizing SAFETY Act certified or designated technologies and services may provide fiduciaries with comfort due to the DHS vetting. The SAFETY Act also provides an exclusive federal cause of action for losses arising out of the performance of the certified technology and DHS interprets this to mean claims may only be brought against the seller of the technology. Conceivably this could eliminate claims against the plan fiduciaries, but it is unclear what the result of the interaction between the SAFETY Act liability limitation and ERISA pre-emption would be.

3) Insurance Plan fiduciaries should be sure to review their insurance contracts. Fiduciary insurance is typically triggered when a lawsuit is filed, while cyberinsurance is often triggered by a data breach. Knowing what coverage is available, and when, under plan specific or company-wide insurance is important.

Conclusion

As cybersecurity threats increase, so should plan fiduciary efforts to combat these threats. Fiduciaries can work with service providers to strengthen existing protections and can work internally to create and document procedures that demonstrate prudent process.