In today’s technological world, no person or organization is immune from the threat of a cyberattack. Hacking now occurs with alarming frequency as cybercriminals have targeted corporations, websites, health insurance companies, banks, law firms and others. Employee pension and welfare plans are among the victims of cyberattacks. In the recent past, several employee benefit plans sponsored by private employers and boards of trustees, as well as public employee plans sponsored by municipalities, have become victims of malware infection, ransomware attacks and the electronic theft of plan data and funds.

Indeed, employee benefit plans may be particularly enticing targets to cybercriminals, since these plans typically maintain sensitive participant- and plan-related information that they share with third parties providing administrative and other necessary services to the plans. These plans often do not maintain sophisticated cybersecurity protections. In fact, the Federal Bureau of Investigation (FBI) has stated that health care data is “uniquely at risk” because the information is highly valuable to hackers who can use it to file false medical claims, obtain

Employee benefit plans maintain sensitive information and are among those at risk for cyberattacks. This article looks at potential legal liabilities for plan sponsors and plan fiduciaries related to data breaches.

by Neal S. Schelberg and Miriam S. Dubin
prescription drugs and steal plan participants’ identities. Moreover, as an increasing number of plans have transitioned from paper to electronic methods of storing participant and plan data and information, the threat of such information being hacked, intercepted or inadvertently exposed has significantly increased.

On January 24, 2017, the 2016 ERISA Advisory Council published the final report of its working group on cybersecurity protections for benefit plans. The report offers guidance to the Secretary of Labor and the employee benefit plan community on the risks associated with securing plan data and recommends protective measures that plans may take to increase cybersecurity. This article provides an overview of the cyberthreats facing benefit plans and explores the potential legal liability that plan sponsors and plan fiduciaries may incur from a cyberbreach of plan data.

Background

Several recent high-profile cyberattacks on benefit plans have made it abundantly clear that guidance was sorely lacking in this area. For example, in July 2016, an unidentified hacker gained access to a multiemployer pension plan, took control of one of its computer servers and demanded a ransom payment of three bitcoins (approximately $2,000) to unfreeze it. The plan did not pay the ransom, instead enlisting a third-party forensic analyst to investigate the breach. The plan relied on a backup server until the breach was eliminated. An investigation revealed that the hacker had gained access to the server one week prior to the attack. The breach potentially exposed the personal data of more than 18,000 participants, including employee names, dates of birth, bank account information and Social Security numbers. As a precaution, the trustees offered participants one year of credit-monitoring services.

In another example, one month before the ransomware attack on the pension plan, the deferred compensation accounts of municipal employees in Chicago were breached by an unidentified hacker or group of hackers. The hacker(s) accessed secured personal information, created web profiles and withdrew loans from the retirement accounts. The fraudulent loans reportedly totaled more than $2.5 million. A total of 91 accounts were breached, and money was withdrawn from 58 of those accounts. The company that administers Chicago’s deferred compensation plan noticed suspicious activity and quickly notified the account holders and the federal authorities. The City of Chicago, as the plan sponsor, returned the funds to the breached accounts, and the plan administrator offered two years of credit-monitoring services to the affected employees.

These attacks are not limited to the retirement or deferred compensation plan context. As previously discussed, the FBI has noted that health care plan data is of particular interest to hackers because it often includes personally identifiable information such as names, birth dates, credit card numbers and medical records, which can be sold on black markets for a considerable profit. Moreover, the former section chief of the FBI Cyber Security Division in Washington, John Riggi, has noted that the health care industry is “less mature” in its cybersecurity capabilities and, therefore, is more susceptible to attack than the financial or retail industries.

The FBI issued a private industry notice in 2014 to select health care industry employers, warning that the industry was particularly vulnerable because of the “mandatory transition from paper to electronic health records, lax cybersecurity standards, and a higher financial payout for medical records in the black market.” The notice further predicted that cyberactors will increase intrusions against health care systems.

Under state and federal law, a breach of health plan information may result in a significant fine or penalty. For example, in November 2016, the Depart-
ment of Health and Human Services (HHS) announced that it was settling potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules with the University of Massachusetts Amherst. The university agreed to pay $650,000 and comply with a corrective action plan. One of the university’s workstations was infected with a malware program that exposed hackers to the electronic protected health information (ePHI) of more than 1,500 individuals. HHS investigated the incident and concluded that the university failed to identify all of its health care components and, therefore, did not implement HIPAA procedures at the breached center.

Another similar settlement, totaling $42.2 million, was announced by HHS on January 18, 2017 in connection with violations that stemmed from a stolen pen drive (a data storage device) that was left unattended in the IT department of an underwriter of disability insurance and group health insurance plans. The pen drive contained ePHI of more than 2,000 individuals.

These breaches underscore the severity of the risk that sensitive data or plan asset information may fall into the wrong hands. Not only must plans be concerned about deliberate data breaches, but they should be aware of the possibility that plan or participant information may be inadvertently exposed as a result of the sharing of data with multiple third parties, including administrators and other service providers. To address these risks, as explained by the report, it is critical that plan sponsors and fiduciaries develop cyber-risk management strategies that serve to protect their plans from these threats.

2016 ERISA Advisory Council Report

The report begins with the important premise that cyber-risks cannot be eliminated, but they can be managed, stating “[it is] not a question of if, but a question of when a breach will occur.” No individual, organization or industry is immune from cyberattacks, including employee benefit plans. The purpose of the report is to help plan sponsors, administrators, service providers and fiduciaries develop feasible cybersecurity strategies to minimize these risks. The report states that it is not intended to be prescriptive or a checklist but rather aims to generally enhance and broaden awareness of cybersecurity considerations for benefit plans.

The report encourages plans to establish a customized cybersecurity strategy and carefully contract with service providers on these matters. Furthermore, plans should establish policies for protecting data—such as data retention, training, reporting, testing and data updating processes—as well as a procedure to recover data and restore systems in the event a breach does occur. The report further recommends that plan sponsors, fiduciaries and service providers consider purchasing cyberliability insurance.

In this regard, Segal Select Insurance, a major provider of insurance products to Taft-Hartley plans, explained in a bulletin that multiemployer plan administrators and trustees often are unsure if cybersecurity insurance is necessary where the plan engages outside service providers. However, the report suggests that plan fiduciaries have an obligation to safeguard participant data that cannot be outsourced, and it states explicitly that plans should consider the need for not only “third-party” cyberliability coverage that is triggered by a lawsuit for a cyberbreach but also for “first-party” insurance coverage that triggers coverage at the first sign of a cyberbreach of a plan’s computer systems.

Although the report offers helpful recommendations for establishing and maintaining a cybersecurity risk management program for benefit plans, it is important to note that there is no comprehensive federal law (including the Employee Retirement Income Security Act (ERISA)) that governs a plan sponsor’s or fiduciary’s responsibility for implementing cybersecurity measures to protect plan or participant data. Of course, HIPAA provides some limited guidance on data privacy and security for plan sponsors. However, this guidance applies only to health plans and not to other types of welfare or pension plans.

In the absence of comprehensive legal authority, plan sponsors and fiduciaries do not have clear guidance or direction in determining whether and when strategies are needed to secure plan data. However, in light of the ERISA Advisory Council’s well-founded concerns regarding the susceptibility of benefit plans to cyberthreats, a compelling question that plan fiduciaries should be asking themselves is whether they have a fiduciary duty under ERISA to implement cybersecurity safeguards.

The report explicitly states that the council is aware of the possibility that the implementation of cyberprotections may be characterized as an ERISA fiduciary duty but that it would not offer an opinion on the matter because it was beyond the scope of the study. As noted above, the report also explained that there is no comprehensive federal law requir-
ing plans to implement cybersecurity protections.13 Also, in the report, the council stated that it was beyond the scope of its study to address whether state privacy laws are preempted by ERISA and therefore inapplicable to benefit plans.

Those important issues remain open legal questions, which can be unsettling for plans and fiduciaries as there is little guidance in this area, and the ultimate determination of these issues has the potential to greatly impact the benefit plan community. Consider, for example, if state privacy laws are found to be applicable to benefit plans and whether protecting plan data is within a trustee’s fiduciary duty under ERISA.

The Federal Bureau of Investigation has proposed approaches for benefit plans to address cyberthreats, including establishing a “culture of information security” and backing up and storing plan data off-network.

takeaways

• Employee benefit plans are enticing targets for cyberattacks because of the sensitive information they maintain and share with third-party vendors.
• A recent ERISA Advisory Council report encourages plans to establish a customized cybersecurity strategy.
• Because there is no comprehensive federal law governing their duty to implement cybersecurity measures or protect plan and participant data, plan sponsors and fiduciaries lack clear guidance to determine whether and when strategies are needed to secure plan data.
• Important unanswered questions include whether state privacy laws are applicable to benefit plans and whether protecting plan data is within a trustee’s fiduciary duty under ERISA.
• The Federal Bureau of Investigation has proposed approaches for benefit plans to address cyberthreats, including establishing a “culture of information security” and backing up and storing plan data off-network.

that even a single breach can expose a plan to substantial penalties, costs and expenses.14

Because of these factors and others, and due to the obligations imposed on plan fiduciaries under ERISA to act "with the care, skill, prudence, and diligence . . . that a prudent man acting in a like capacity and familiar with such matters would use,”15 those asserting a fiduciary obligation maintain that the U.S. Department of Labor or a federal court could conclude that the failure of trustees to implement reasonable measures to protect plan and participant data constitutes a breach of fiduciary duty under ERISA.

Outside of the benefits context, the report highlights steps that the banking and financial services industries have taken on matters of cybersecurity. The report lists several frameworks for protecting data that have been successful in those industries, along with detailed recommendations for developing effective strategies and procedures in the benefit plan context.

In addition to the strategies offered in the report, the FBI has also proposed to plan sponsors and fiduciaries various approaches to address cyberthreats. The FBI explained that plans should establish a “culture of information security” that emanates from the top of an organization down to the staff. The FBI also suggested that plans should back up and store data off-network to effectively segregate and quarantine the backup from cyberbreach.16

Finally, the FBI has stated that planning for a breach by having reporting and security procedures in place can considerably minimize a plan’s costs and exposure if and when a breach actually does occur.
Conclusion

The information systems maintained by employee benefit plans are susceptible to offensive, malicious attacks that can expose sensitive and confidential plan and participant data. Through the report, the ERISA Advisory Council has raised awareness of these issues and has offered important guidance on strategies that plan fiduciaries should consider implementing to mitigate these threats. However, the report is limited in that it does not provide guidance on critical legal questions relating to ERISA fiduciary obligations, ERISA preemption of state privacy laws, and other legal issues regarding the responsibility to implement cybersecurity measures.

Inevitably, benefit plans will continue to be targeted by cybercriminals who are encouraged by lax cybersecurity measures and motivated by black market prices for participant data. Given the potential significant harm to the plan and its participants of a data breach, plan sponsors and fiduciaries should take proactive steps to mitigate these risks by adopting customized security measures for their plans and exploring the purchase of cyberliability insurance.

Endnotes

1. A cyberattack is an offensive maneuver employed by individuals, groups, organizations or nation-states that targets computer information systems, infrastructures, computer network and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters or destroys a specified target by hacking into a susceptible system. See Tom C. W. Lin, "Financial Weapons of War," University of Minnesota Law Review, Volume 100, Issue 4, 1377 (2016). See also Robert Galvin, chief technology officer, The Port Authority of New York and New Jersey, Testimony for Joint Subcommittee Hearing, "Enhancing Preparedness and Response Capabilities to Address Cyber Threats" (May 24, 2016).


3. Advisory Council on Employee Welfare and Pension Benefit Plans, known as the ERISA Advisory Council. The duties of the council are to advise the secretary and submit recommendations regarding the secretary’s functions under the Employee Retirement Income Security Act (ERISA). See ERISA Section 512.


6. Ibid.

7. Ibid.

8. The U.S. Department of Health and Human Services notes that the settlement amount is reflective of the fact that the university operated at a financial loss in 2015.


11. The report states: "As noted in the 2011 Council report, there continues to be no comprehensive federal law governing cybersecurity for benefit plan service providers. There are laws that govern the financial industry’s use of financial information . . . [but] these laws, however, do not apply directly to benefit plans or the sensitive individual data held in conjunction with those plans." Moreover, the report explains that "[m]ost states have laws that address the protection of PII and PHI in some form but, like federal laws, these laws generally apply to health plans, and not to other welfare benefit plans or to pension plans." The report further suggests that plan sponsors might look to HIPAA or other existing cybersecurity frameworks for guidance on navigating cyber-risks in the pension and welfare plan context. See report at pp. 7-8.

12. In this regard, the report states: "[T]he 2016 Council is not opining on whether cybersecurity is a fiduciary or settlor function or what should be acceptable fiduciary conduct with respect to cybersecurity for benefit plans. This issue was not within the scope of the 2016 Council’s work and we did not hear testimony or receive commentary on the issue sufficient to reach any conclusions or recommendations." Id. at p. 16.

13. For a summary of the report’s account on the lack of state and federal laws directly addressing cybersecurity protections for pension and welfare plans, see infra note 11.

14. The report notes that the cost of a cyberattack includes detecting the extent of the breach, recovering exposed data and restoring the systems, in addition to any fines or penalties that may be imposed on the plan. See report at p. 1.

15. ERISA Section 404(a)(1)(B).


Neal S. Schelberg is a partner in Proskauer Rose’s New York office, where he practices in the employee benefits and ERISA litigation areas. He is an active volunteer for the International Foundation as a committee member and chair, a frequent speaker at educational programs and contributing author to the Trustee Handbook: A Guide to Labor-Management Employee Benefit Plans, Seventh Edition, and many other International Foundation publications. Schelberg is a former chair of the Advisory Council on Employee Welfare and Pension Benefit Plans. He is a graduate of the Hofstra University School of Law and the Georgetown University Law Center.

Miriam S. Dubin is a law clerk in the labor and employment law department and a member of the employee benefits, executive compensation group at Proskauer Rose’s New York office. She has a B.A. degree from Yeshiva University and a law degree from the Benjamin N. Cardozo School of Law.