Services

Employee Benefits and Executive Compensation

Fiduciary Duties and Governance

Qualified Retirement Plans

Taft-Hartley Plans

Health and Welfare Plans

Government Plans

Higher Education

Employee Stock Ownership Programs (ESOPs)

Executive Compensation and Nonqualified Plans

ERISA and Benefits Litigation

College Savings and ABLE Plans

Mandatory Paid and Unpaid Leave

Audits and Investigations

U.S. Department of Labor Issues Cybersecurity Guidance for Plan Sponsors, Recordkeepers, and Plan Fiduciaries

The Internet continues to be an ever-more-prevalent part of our lives; 90% of people today complete some or all of their financial transactions online. However, as online financial transactions increase, so do internal and external security threats. Even a relatively small retirement plan can present an optimal target opportunity for criminals, given the amount of assets involved and the number of potential data sources (e.g., participants, insurers, plan administrators, custodians, trustees) and entry points (e.g., phones, laptops, servers). A single successful attack can be devastating.

ERISA requires plan fiduciaries to take appropriate precautions to mitigate these risks. Consequently, the Employee Benefits Security Administration division of the U.S. Department of Labor ("DOL") has, for the first time, released cybersecurity best practices to assist prudent plan sponsors, plan fiduciaries, and recordkeepers in protecting participant data. This guidance builds on the DOL's existing regulations concerning the electronic records of plan participants and beneficiaries. Because cybersecurity is likely to be an emerging enforcement focus for the DOL in coming years, this article highlights steps that plan sponsors can take to safeguard the retirement benefits and personal information of their plans' participants.

Cybersecurity Best Practices

According to the DOL's best practices guidance[1], responsible plan fiduciaries will take the following steps to mitigate their cybersecurity risks:

1. **Have a formal, well-documented cybersecurity program** that fully implements information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the system. Any adopted policies should be approved by senior leadership and reviewed at least annually.
2. **Conduct prudent risk assessments**, at least annually, that identify, estimate, and prioritize information system risks and describe how such risks will be mitigated or compartmentalized.
3. **Have a reliable, annual third-party audit of security controls** so that fiduciaries have a clear, unbiased report of existing risks, vulnerabilities, and weaknesses.

[1] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf

4. **Clearly define and assign information security roles and responsibilities.** Generally, the program will be managed at the senior executive level (e.g., CIO) and executed by qualified personnel.
5. **Have strong access control procedures**, which include authentication and authorization components.
6. **Ensure 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.**
7. **Conduct periodic cybersecurity awareness training** and update the training as needed to reflect risks from the most recent annual risk assessment.
8. **Implement and manage a secure system development life cycle ("SDLC") program**, including penetration testing, code review, and architecture analysis.
9. **Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.**
10. **Encrypt sensitive data, stored and in transit** by implementing the most current standards for use of encryption keys, message authentication and hashing.
11. **Implement strong technical controls in accordance with best *security* practices**, such as automatic updates, system hardening, routine backups, and use of antivirus software and firewalls.
12. **Appropriately respond to any past cybersecurity incidents** by adequately investigating the incident, informing law enforcement, insurers and affected participants, and fixing the problems that led to the breach.

Best Practices for Hiring Service Providers

Responsible plan fiduciaries have an obligation to ensure proper mitigation of *all* potential cybersecurity risks, including any cybersecurity risks from vendors or service providers that use or maintain participant data. Plan fiduciaries should hire service providers that follow strong cybersecurity practices.[2] Therefore, any prudent process for hiring service providers will include:

1. **Asking about the service provider's information** security standards, audit results, practices, and policies, including how these compare to the industry standards adopted by other financial institutions.
2. **Asking how a service provider validates its practices**, and what levels of security standards it has met and implemented. Vendor contracts should give plan fiduciaries the right to review audit results demonstrating compliance with the standards.
3. **Evaluating the service provider's track record in the industry**, including public information regarding information security incidents, other litigation, and legal proceedings related to vendor's services.
4. **Asking whether the service provider has experienced past security breaches**, what happened, and how the service provider responded.
5. **Confirming the service provider has insurance policies that would cover losses caused by cybersecurity and identity theft breaches** (including breaches caused by internal threats, such as misconduct by the service provider's own employees or contractors, and breaches caused by external threats, such as a third party hijacking a plan participant's account).

---

[2] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf

Contacts

John E. Schembari
Omaha
402.231.8886
john.schembari@kutakrock.com

Michelle M. Ueding
Omaha
402.661.8613
michelle.ueding@kutakrock.com

William C. McCartney
Irvine
949.852.5052
william.mccartney@kutakrock.com

P. Brian Bartels
Omaha
402.231.8897
brian.bartels@kutakrock.com

Cindy L. Davis
Minneapolis
612.334.5000
cindy.davis@kutakrock.com

Ruth Marcott
Minneapolis
612.334.5044
ruth.marcott@kutakrock.com

Jeffrey J. McGuire
Omaha
402.661.8647
jeffrey.mcguire@kutakrock.com

Sevawn Foster Holt
Little Rock
501.975.3120
sevawn.holt@kutakrock.com

John J. Westerhaus
Omaha
402.231.8830
john.westerhaus@kutakrock.com

Emily P. Dowdle
Omaha
402.661.8683
emily.dowdle@kutakrock.com

Robert J. Hannah
Omaha
402.661.8667
robert.hannah@kutakrock.com

Rachel A. Loscheider
Minneapolis
612.334.5011
rachel.loscheider@kutakrock.com

Emma L. Franklin
Omaha
402.231.8842
emma.franklin@kutakrock.com

When reviewing the contracts with a service provider, plan fiduciaries should verify that the contract requires *ongoing* compliance with cybersecurity and information security standards. Provisions that limit the service provider's responsibility for I.T. security breaches should be rejected. In addition, vendor contracts should include cybersecurity protections that protect the plan and its participants, such as insurance policies, information security reporting obligations, information sharing and confidentiality provisions, cybersecurity breach notification requirements, and record retention/destruction protocols.

In addition to the above, fiduciaries should consider securing cyber security insurance to cover their retirement plan. Some fiduciary liability insurance policies cover cyber incidents, but not all policies provide the same level of protection.

If you have questions about the cybersecurity guidance or the compliance obligations created by the guidance, please reach out to a member of the Kutak Rock Employee Benefits and Executive Compensation practice group.

Employee Benefits Security Administration
News Release (No. 21-358-NAT)