Employee Benefits Security Administration – cybersecurity leading practices

Navigating the U.S. Department of Labor guidance

January 2022

EY
Building a better working world

Navigating the Department of Labor guidance on cybersecurity program leading practices

Insights and state of industry

- The Department of Labor (DOL) notes that as of 2018, there are approximately 140m plan participants with approximately US$9.3t in assets that are part of these plans.
- The industry continues to struggle with cybersecurity issues and fraud. The ability and methods for criminals to commit fraud has grown faster than the industry's ability to develop effective practices and controls to prevent and detect fraud.
- Organizations have become increasingly connected, and as a result, third, fourth and even fifth party relationships can impact the security of the first party (e.g., plan sponsors, fiduciaries).
- Identity-related theft and fraud, including familial fraud, have continued to strain the industry. A growing focus is being placed on strong, frequent and real-time identity verification across multiple interaction channels, and this requires a strong cybersecurity program to implement effectively.

What is the DOL's Employee Benefits Security Administration guidance?

In April 2021, the DOL announced new guidance for retirement plan sponsors, fiduciaries, record keepers, and plan participants on the leading practices for maintaining cybersecurity. The guidance spans three categories:

- Tips for hiring a service provider (SP)
- Cybersecurity program leading practices
- Online security tips for plan participants

Who should utilize the guidance?

The guidance is aimed at fiduciaries and plan sponsors regulated by the Employee Retirement Income Security Act (ERISA).

Why is this regulatory guidance important?

Regulatory leading practices signal what risks regulators are concerned about and the topics that will be part of their reviews. Given the number of plan participants and assets in these plans, the DOL sees this as an area of concern from an overall risk management perspective for the industry.

Next steps for fiduciaries, record keepers and plan sponsors:

1. For each of the guidance documents, the organization should understand if the organization is performing the leading practices, how well they are performing them, and note any gaps, both in design and degree of available documentation
2. Communicate cybersecurity awareness recommendations to plan participants as part of financial wellness education.
3. Consider whether i) fiduciary liability insurance covers cyber theft, ii) organizational cybersecurity insurance covers pension breaches and iii) service provider management program address cyber risk.
4. Understand how their cybersecurity and fraud programs are aligned and how they can be better designed to prevent and detect fraud.

Navigating the Department of Labor guidance on cybersecurity program leading practices

Leading practice No. 1: Tips for hiring a service provider (SP)

1. Look for a SP to follow a recognized standard for information security and third-party audit of cybersecurity.
2. Understand how a SP validates implement standards and seek right to audit contract provisions
3. Evaluate industry track record, including security incidents and other litigation.
4. Inquire about past breaches and how the SP has responded to those breaches
5. Determine if the SP has cyber insurance that would cover losses by cyber incidents including identity theft and breaches
6. Require ongoing cybersecurity compliance in contractual requirements. Include evaluations of limitations of liability, data sharing, breach notification, etc.

How Ernst & Young LLP (EY US) can help

- We can develop your third-party risk management program to enable the quantification of systemic third-party risk and decision-making tools to help manage this risk
- We can review processes used to evaluate SP risk and implement improvements that will enhance and maintain best practices
- We can implement supplier monitoring programs to actively measure risks
- We can review and enhance cybersecurity contractual requirements for service providers to better manage risk

Leading practice No. 2: cybersecurity program leading practices

1. Have a formal cybersecurity program
2. Conduct prudent annual risk assessments
3. Have a reliable annual third-party audit of security controls
4. Clearly define and assign information security roles and responsibilities
5. Have strong access control procedures
6. Ensure appropriate security reviews for data stored in the cloud or manager by a TPA
7. Deploy periodic cyber training
8. Deploy and manage a security system development lifecycle program (SDLC)
9. Have a cyber resiliency program
10. Encrypt sensitive data in transit and storage
11. Implement strong technical security controls
12. Appropriately respond to cyber incidents

How Ernst & Young LLP (EY US) can help

- We can enhance your cyber program to incorporate DOL cyber guidance tailored to your risk appetite, benefits market risks, and cyber threat trends.
- We can assist with your customer and digital identity program to manage fraud risk
- We can help to develop your cybersecurity resiliency program to protect and respond to ransomware and other resilience events
- We can improve your overall cybersecurity governance by collaborating with you to align measures with business strategy and risks.
- We can help to better integrate fraud and cybersecurity programs to better detect and prevent fraud.
- We can help to identify your high value assets and implement controls to better control access to your most valuable data.
- We can perform red/blue/purple team tests to understand how your cyber program is operating

Navigating the department of labor guidance on cybersecurity program leading practices

For more information on how Ernst & Young LLP can help, please contact:

Jami'h Rainer
Managing Director
Cybersecurity – Insurance

+1 571 565 8759
jamih.rainer@ey.com

Abhishek Madhok
Principal
Cybersecurity – Insurance

+1 732 516 5117
abhishek.madhok@ey.com

Natasha Wheatley
Managing Director
Cybersecurity Wealth & Asset Management

+1 617 375 1348
natasha.wheatley@ey.com

Steve Ingram
Managing Director
Cybersecurity Lead for Financial Services

+1 203 674 3541
steve.ingram@ey.com

Sheva Levy
Principal
People Advisory Service – Wealth and Asset Management

+1 216 583 8235
sheva.levy@ey.com

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

2201-3945816
US SCORE no. 15305-221US ED None

ey.com