PICPA
Belong. Grow. Achieve.

Cybersecurity

Today's speaker

Richard Fischer

Certified Public Accountant

- Partner, Louis Plung & Company
- Audit & Assurance
- 30+ years of experience in Audits, Reviews, Compilations, and Internal Controls
- PICPA / AICPA
- Actively involved in PICPA and on committees including Employee Benefit Plans, Construction, Accounting & Auditing, and Peer Review

Objectives

- Common Cyber Threats
- Cyber Risk Management Strategies, Scaled Based on Sponsor and Plan Size, Type and Resources
- Cyber Breaches May Result in ERISA Violations for Plan Sponsors, Fiduciaries and Service Providers

Objectives

- What Plan Auditors Look For In Accessing Risks
- SOC 1 and SOC 2 Reports
- Insuring Against the Cybersecurity Risks in Fidelity Bonds, and Cybersecurity Insurance or Endorsements to Fiduciary Insurance Policies

Cybersecurity

- Krause and David McFarlane, a partner at the same firm, say that the courts will look to the plan sponsors and see if they fulfilled their fiduciary responsibilities under ERISA, and whether they took reasonable action to prevent phishing attempts.

Cybersecurity

- Even if the plan participants are not liable, they will see investment losses due to shortened time that the money can grow to its full potential. For retired workers, the effects of a cyberattack would be detrimental, the attorneys say.
- “It would be a real catastrophe if people fell prey to these types of attacks,” Krause says. “These are not people who are drawing a paycheck regularly.”

Cybersecurity

- In 2016 DOL raised concerns regarding cybersecurity.
- ESBA Chief Accountant Ian Dingwall encouraged plan administrators to evaluate the plan's cybersecurity governance, including serviced providers and their vendors

Cybersecurity

- ESBA's suggested steps in cybersecurity risk assessment process included:
  - Review written information security policies, including those regarding encryption
  - Conduct periodic audits to detect threats
  - Perform periodic testing of backup and recovery plans
  - Determine responsibility for losses, including adequacy of cybersecurity insurance coverage
  - Establish training policies to reinforce data security

Cybersecurity

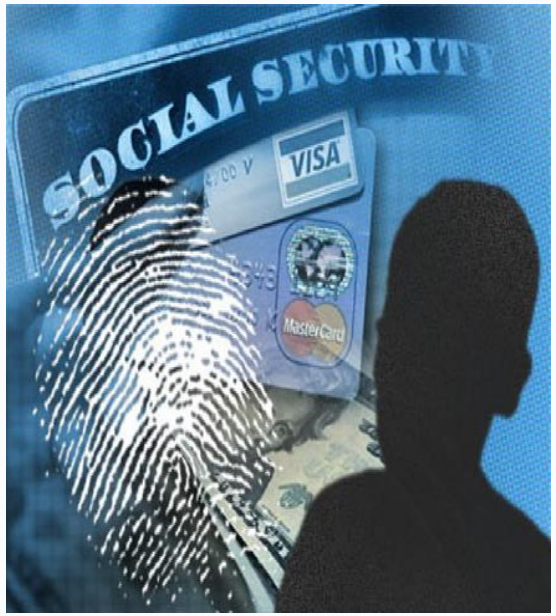
- November 2016 the Advisory Council on Employee Welfare and Pension Benefit Plans released their report Cybersecurity Considerations for Benefit Plans.
- Benefit plans often maintain and share sensitive employee data and asset information across multiple unrelated entities, such as TPAs, actuaries, auditors and trustees, as a part of the benefit plan administration. process.

Cybersecurity

- Develop procedures to protect personally identifiable information (PII)
- Anyone that comes in contact with PII has a role in protecting data.
- Larger employers are more likely to have the resources to obtain guidance on managing PII.
- Small and Mid-sized employers less likely to have resources to obtain this guidance.

Cybersecurity

- Service providers collect and maintain sensitive employee data to meet their responsibilities and deliver services.
- Data includes:
  - Social security numbers
  - Home address
  - Date of birth
  - Account balance information
  - Beneficiary information and bank account details



Cybersecurity

- Cybersecurity breach within a benefit plan could result in employees' identities, personal information or plan assets being compromised.
- Plan sponsors and fiduciaries may be challenged by limited resources, technical expertise and lack of clear standards

Claims of Breach of Fiduciary Duties Under ERISA

- Does ERISA fiduciary responsibilities include securing online plan data from cyberattacks in 401(k) and other retirement plans?
- Congress has not amended ERISA to address cybersecurity.
- DOL has not formally addressed cybersecurity in ERISA guidance or regulations.

Claims of Breach of Fiduciary Duties Under ERISA

- ERISA preemption may block state governments from regulating the data security of employee benefit plans, and no other federal regulatory scheme applies as directly to the issue of ERISA's duty of prudence.
- New DOL Electronic Disclosure Final Rules require that plan fiduciaries "take measures reasonably calculated to ensure that the website protects the confidentiality of personal information relating to any covered individual."

Claims of Breach of Fiduciary Duties Under ERISA

- Cybersecurity threat is so pervasive that lawmakers have asked GAO to examine the cybersecurity of the U.S. retirement systems.
- The Securities and Exchange Commission recommends that plan participants pick strong passwords and change them regularly, add biometric screenings and two-factor authentications, use caution with Wi-Fi connections and public computers, and opt-in for account alerts.
- Those suggestions won't help employees, however, if they think an alert about 401(k) misuse is coming from the plan sponsor instead of a hacker.

Claims of Breach of Fiduciary Duties Under ERISA

Steps Plan Sponsors may take to PII in exchanging information with record keepers and other service providers The Siegal Group recommends:

- Create an information security policy and an incident response plan.
- Review information being requested to ensure that only absolute minimum PII is requested, exchanged and used.
- Mandate use of encryption for data-at-rest and data-in-motion.
- Review and access record keepers' technology and security procedures.
- Set up and regularly review system.
- Maintain activity logs adequate levels of cyber liability protection.

See Aon's 2019 Cyber Security Risk Report

Service Organization Controls (SOC)

- A SOC 1 Report is a report on controls at a service organization which are relevant to user entities' internal control over financial reporting.

Service Organization Controls (SOC)

- An example of a service organization that may need a SOC 1 report is a company that provides payroll processing services to user entities.
- User entities that use the payroll processing company realize the material impact of payroll on their financial statements and request some independent assurance that their payroll is being handled in accordance with their expectations.

Service Organization Controls (SOC)

- A SOC 1 report provides user entities of the payroll processing company reasonable assurance that the internal controls of the payroll processing company are suitably designed (Type I report) or suitably designed and operating effectively (Type II report) to provide the payroll services.

Service Organization Controls (SOC)

- If you are hosting or processing other types of information for your clients that does not impact their financial reporting, then you may be asked for a SOC 2 audit report.
- In this instance, your clients are likely concerned whether you are handling their data in a secure way, and if it is available to them in the way you have contracted it to be.
- A SOC 2 report, similar to a SOC 1 report, evaluates internal controls, policies, and procedures.

Service Organization Controls (SOC)

- However, the difference is that a SOC 2 reports on controls that directly relate to the security, availability, processing integrity, confidentiality, and privacy at a service organization.
- These categories are known as the Trust Services Criteria and are the foundation of any SOC 2 audit engagement.

Service Organization Controls (SOC)

- Complementary user entity controls (CUECs) are an essential part of any SOC audit report.
- When contracting with a service organization, any user entity must accept that certain controls will remain among that entity's prescribed responsibilities.

Service Organization Controls (SOC)

- CUECs encompass all controls within a service organization's systematic processes that rely on the user entity for implementation and function.
- User entities are accountable for the performance of CUECs.
- And if a user entity does not consistently perform CUECs as stipulated, its affiliated service organizations may ultimately be unable to deliver contracted control objectives.

Service Organization Controls (SOC)

Examples of complimentary End User Controls

- **Security Monitoring** – User entities must monitor and update their own antivirus definition updates and security patches unless the service is included within a contracted Statement of Work with the service organization.
- **Physical Access** – It is the responsibility of user entities to notify the service organization in the event that physical access needs to be added, modified, or revoked for a user entity's employees.
- **Contingency Plan** – The service organization's contingency plan is applicable to its operations only. User entities are not covered by it and should develop their own contingency plan.

Service Organization Controls (SOC)

Some examples of organizations who may receive SOC 1 or SOC 2 reports include:

- Payroll processors
- Medical claims processors
- Loan servicing companies
- Data center companies

Actual Cases of Breaches in Cybersecurity

- Levanthal v MandMarblestone Group, LLC, Case No. 18-CV-2727 (E.D. Pa., filed 6/28/18).
- MMG was a consulting firm, Named Fiduciary and Plan Administrator.
- Nationwide was the custodian of the law firm's 401(k) Profit Sharing Plan.
- "Unknown criminals" obtained a copy of Levanthal's office email account. The form requested that the funds be sent to a bank account that did not belong to Plaintiff and had not previously been used by him. Over $400,000 was taken.

Actual Cases of Breaches in Cybersecurity

Levanthal v MandMarblestone Group, LLC, Case No. 18-CV-2727 (E.D. Pa., filed 6/28/18).

- Court found the MMG and Nationwide were fiduciaries – MMG was the "Named Fiduciary" and Nationwide exercised actual control over the assets. Court held that Levanthal sufficiently pled a breach of fiduciary duty when alleging that MMG and Nationwide failed to act prudently in failing to alert Levanthal or verify the requests when they saw the "peculiar nature" and high frequency of withdrawal requests that were to be distributed to a new bank account.
- In May 2020, court ruled that MMG and Nationwide may bring counterclaims against the law firm for contribution and indemnity based on allegations that plan sponsor was "careless" in its "computer/IT systems" and "employment policies" in permitting Levanthal to work remotely without adequate safeguards.

Actual Cases of Breaches in Cybersecurity

"Phishing" techniques to deceitfully obtain logon credentials and passwords to gain access to online participant account information and request distributions or loans, redirect benefits to another account, or create fraudulent health claims.

- An email, purported to be from the plan sponsor's top executive, was sent to the human resources (HR) department requesting sensitive employee data. HR responded by sending the information before realizing it was a "spear phishing" or "whaling" email from an outside party.
- A phishing scheme was successfully carried out at a plan recordkeeper. As a result, participant accounts were breached and unauthorized distributions were made from those accounts

Actual Cases of Breaches in Cybersecurity

"Socially engineered malware", when an end-user is tricked into running a Trojan horse program, often from a website they trust and visit frequently. The otherwise innocent website is temporarily compromised to deliver malware instead of the normal website coding.

A plan sponsor's internal IT department discovered malware on 50 computers. One participant account was breached and an improper distribution occurred before the Malware was discovered.

Actual Cases of Breaches in Cybersecurity

- “In November 2016, the Department of Health and Human Services (HHS) announced a settlement with a large university for potential violations of HIPAA.
- Following a malware infection targeting the university's employee health care plan, the university agreed to pay $650,000 in penalties and to comply with the requirements of a corrective action plan.
- The breach exposed the private health information of 1,500 people. An HHS investigation revealed that the university had failed to accurately assess the risk of malware infection and adopt procedures to secure its data.

Actual Cases of Breaches in Cybersecurity

Cyber criminals using employees' PII and setting up web profiles that allow them to take out loans from individual participant accounts.

- In June 2016, more than 90 deferred-compensation retirement accounts of a city's municipal employees were breached. Hackers obtained the personal information of plan participants and used it to set up online profiles on the plan custodian's web platform; the hackers accessed personal information and withdrew loans from 58 accounts.
- Reports estimate that the city lost about $2.6 million. The city returned funds taken from participant accounts and offered credit monitoring services to account holders.
- A service provider received an unusual number of distribution requests for one of their plan clients. The requests were vetted through the established process and denied because they were determined to be unauthorized.

Cyber Security

- In 2014 National Institute of Standards and Technology (“NIST”) develop a cybersecurity framework
- Framework has three parts.
  - Core
  - Implementation
  - Developing an organizational

Cyber Security

- Framework - Core
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

Cyber Security

- Framework - Core
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

Cybersecurity

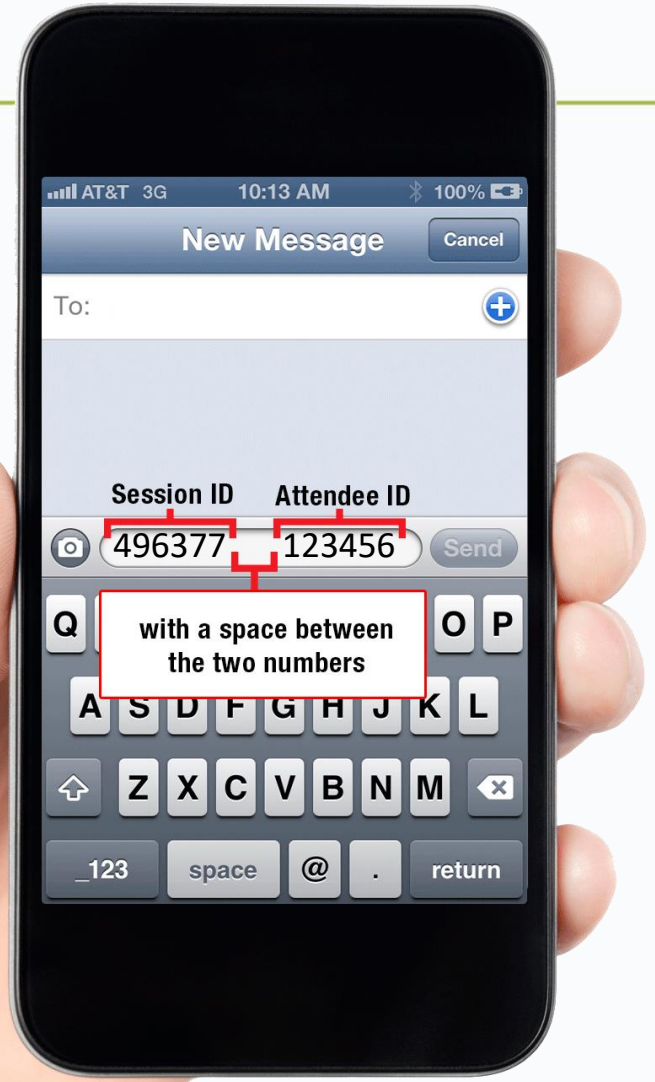
- Framework - Implementation – of a risk management program and assist organizations in understanding where they are with regard to implementation
  - Partial
  - Risk informed
  - Repeatable
  - Adaptive

Cybersecurity

- Framework - Developing an organizational profile
- Profile will use the functions, categories and subcategories outlined in the framework core along with business drivers and risk assessment to determine which is most important.
- Develop policies that address implementation and monitoring, testing and updating, reporting and training.

Cybersecurity

- According to Soha System's survey, 63% of breaches were traced to third-party vendors.
- Many organizations have long focused on building their own cybersecurity defenses.
- If an organization has failed to understand the controls of their vendor's cybersecurity defenses, it could exploit the organization.



To Claim CE for this meeting:

Text # 22333

Use session ID 48234 {space} and then your ASPPA ID#

(See sample of phone picture)

Please text within 48 hours of attendance