Cybersecurity Framework for Multi-Employer Plan Trustees

Presented at the 40th Annual National Labor & Management Conference
February 20, 2017

Elizabeth Rogers | rogersel@gtlaw.com | 512-320-7256
Jeffrey Mamorsky | mamorskyj@gtlaw.com | 212-801-9336
Why Should Plan Fiduciaries be Concerned with Creating a Cybersecurity Framework?

- **U.S. avg cost of breach**: $6.5 mm ($5.8 mm)
- **World avg cost of breach**: $3.8 mm ($3.5 mm)
Do Multi-Employer Plan ("MEP") Trustees Have a Duty to Protect Plan Participant Data from these Risks?

All companies, organizations and associations have a duty to protect;

- Non-Public Financial Information (NPFI)
- Personal Identifiable Information (PII)

But many MEP Trustees generally do not have any of the following:

- employees computers cabinets
- web PII safes or vaults
- NPFI office
- no information about the employers, employees or retirees.
July 2016 - Ransomware Demand Hits UFCW Local 655 Food Employers Joint Pension Plan

> The plan is a multi-employer defined benefit plan that had assets of approximately $569 million at the end of 2015.

> Hacker took control of one of the Local 655 plan’s servers and demanded ransom in order for the server to work again.

> Ransom not paid because all information was on a backup server.

> Participants’ names, dates of birth, Social Security numbers and bank account information.

> Union offered credit monitoring and identity protection services to its members for 12 months without cost.
The Risk

Summary of Expert Testimony Provided in a Report by the 2016 ERISA Advisory Council to the Honorable Thomas E. Perez, United States Secretary of Labor, November 10, 2016:

- Cyber threats are a daily headline
- Benefit plans and their service providers are at risk
- Cyber criminals buy and sell data
- Not a question of IF, only a question of WHEN
- Common risks include identity theft, privacy breaches, theft of assets, and HIPAA breaches/fines
- The cost of a breach—detecting the extent, recovering the data, and restoring the system—can be substantial
All of the Personal and Financial Information Assets are Processed by Third Parties

ERISA Fiduciary Duty to Prudently Select and Monitor Third Party Service Providers

MEP Trustees

- Recordkeeper (service provider)
- TPA (service provider)
- Actuary (service provider)
- Custodian (service provider)
- CPA/Attorney (service provider)
Does the “Prudent Expert” Duty Require MEP Trustees to Protect the Information Assets of the Plan?

> ERISA’s “Prudent Expert” Rule

- A Plan Fiduciary must:
  - discharge his or her duties
  - with the care, skill and diligence
  - that would be exercised by a reasonably prudent person
  - who is familiar with such matters.
Prudent Expert Duty to Create Cybersecurity Framework

> Plan administration involves data sharing and asset movements among multiple parties

> Need **strong cyber controls**

> Plan sponsors, administrators and service providers must have a strategy to:

  – **Manage data and assets** to minimize exposure to the cyber threats now and in the future; and

  – **Respond and recover** should a breach occur.

> Trending support for liability

  – **Fortune 1000**: Claims of fiduciary duty breach against directors in **class action data breach** lawsuits

  – **Insurance industry**: NAIC Model Cybersecurity Law

  – **Banking Industry**: NYDFS Regs & ANPR by Big 3 Regulators
While you can't entirely avoid these risks, you can be prepared.

MEP Trustees, administrators and service providers must have a strategy to:

- Minimize exposure to current and future cyber threats, and
- Respond and recover if a breach occurs.
Cybersecurity Risk Management Framework

> MEP Trustees have policies and procedures for their plan investments, conflicts and expenses
  - Also need to have policies that protect their plans’ and participants’ data or assets

> Establish a Cybersecurity Risk Management Framework
  - One size does not fit all—your strategy will depend on your plan, size, resources, expertise, data, assets
  - What are the potential risks? What is the potential exposure?
  - Start by identifying and prioritizing what data are most critical to protect, who has it and what the possible threats may be
Risk Management of Third Party Service Providers and Administrators

- Service providers who access and process plan data may be at risk for a data security breach (for example, a third party administrator, record-keeper)

- Vendor selection due diligence
  - Before contracting with a provider, ask:
    - Does the provider have a comprehensive and understandable cybersecurity program?
    - What are the elements of the program?
    - How will plan(s) data be maintained and protected?
    - Will the data be encrypted at rest, in transit, and on devices
Already Existing Third Party Relationships

- Extend Cybersecurity Risk Framework to Third Parties via a Information and Privacy Cybersecurity Addendum
  - Robust definitions of key terms like Confidential Information, Authorized Persons/Employees, Data Security Breach, Costs
  - Require a series of critical information cybersecurity practices for the protection of plan participant data
  - Provide for strict breach reporting guidelines
  - Demand generous indemnification and/or cyberliability insurance
  - Restrict limitation of liability
Duty to Monitor Third Party Compliance with Cybersecurity Best Practices

> Request copies of written results//summaries of annual information security audits and SOC I and II reports

> Annually request evidence of and review of cybersecurity liability insurance to determine adequacy of limits and terms of coverage
Key Cybersecurity Framework Considerations

> Administration of the Framework
  
  – Allocate Cybersecurity Responsibility to MEP Trustee
  
  – MEP Cybersecurity Trustee Appoints Cybersecurity Officer (normally Fund Administrator assisted by Cyber Counsel)
  
  – MEP Cybersecurity Trustee and Cybersecurity Officer Create Checklist for Annual Reporting to Board of Trustees
    
    ▪ Record due diligence in writing
    
    ▪ Regularly, and at least annually, provide updates to the Board of Trustees and Plan Participants
    
    ▪ Include updates as part of the Minutes
Key Cybersecurity Framework Considerations

> Consider Purchase of Cybersecurity Liability Insurance

- Complete Application with outside counsel to protect and preserve the Attorney-Client Privilege of information that may be considered or included
- Proper valuation of the amount of coverage
- Review terms of coverage and exclusion carefully
  - Ransomeware only officially considered a breach by the OCR in the context of PHI
  - Add ransomeware as an included “data security breach”

- Who is covered?
  - Not all carriers have caught up with the need for Plans to purchase coverage
Key Takeaways

• Assume your data is at risk—an attack will happen
• Be prepared with a Cybersecurity Compliance Framework
• Customize your Framework for your plan, assets, data, risks, resources
• If you do not have expertise, get it
• Ensure vendor contracts include requirement for cybersecurity compliance
• Regularly fulfill duty to monitor
• Create a Chief Cybersecurity Compliance Officer
• Consider cyber insurance
Q & A

THANK YOU