CYBER SECURITY & RANSOMWARE ATTACKS

John R. Reidy

PENSION TECHNOLOGY GROUP

Consider -

Is your fund

at risk for a cyber attack?

able to pay a ransom?

Does your fund have

a Cyber Security Plan?

Business Continuity Management?

Recent Breach

Exploited vulnerabilities in the application used to securely transfer encrypted files

Public pension system in at least 10 states impacted

Multiple record keepers affected

Many impacted through a prominent service provider

Recent Breach

- DOL made it clear it is the plan sponsor's fiduciary duty to assess its service provider
- Expectations of plan sponsors and vendors spelled out in guidance
  - What questions were asked of service providers?
  - What process was used to hire them?
  - Was the cybersecurity posture evaluated as part of the hiring process?

In this session, we will:

- Review DOL's Cybersecurity Guidelines
- Detail reports pension funds should request from their vendors.
- Discuss specific internal controls to protect membership data and assets.
- Identify Common Points of Vulnerability

DOL Guidance

Cybersecurity Program Best Practices

Hiring a Service Provider

Online Security Tips

Best Practices

- Formal Cybersecurity Plan
- Annual Risk Assessments
- Audit Security Controls
- Define Security Roles/Responsibilities
- Strong Access Controls
- Audit Cloud Hosting
- Periodic Cybersecurity Training

Best Practices (cont'd)

- Implement Secure Systems Development Life Cycle (SLDC)
- Business Continuity Management Plan
- Encrypt Sensitive Data – Stored/ Transit
- Implement Strong Technical Controls
- Incident Response Plan

Service Providers

When Hiring:

1. Request detailed information
2. Assess how they validate security practices
3. Evaluate Track Record
4. Review insurance policies
5. How will/did provider respond from incident?

Service Providers Contracts

Contracts should include:

i. Regular Security Reporting
ii. Provisions pertaining to information sharing
iii. Notification of Cyber Breaches
iv. Record Retention compliance
v. Insurance coverage

Security Validations

- SOC Reports (Bridge Letters)
  - SOC 1 is for financial reporting
  - SOC 2 is for security framework (organizational & operational)
- Penetration Testing Reports
- Web Application Firewall Grading Reports
- Disaster Recovery Test Reports (RPO & RTO times)
- Vulnerability Scans (Daily)

Online Security Tips

- Monitor Your Online Account
- Strong Passwords
- Multifactor Authentication
- Updated Personal Contact Info
- Close/Delete Unused Accounts
- Be Wary of Free Wi-Fi

Online Security Tips

- Beware of Phishing Attacks
- Use Antivirus Software
- Keep Applications Current
- Know How to Report Incidents
- FBI/ Homeland Security Sites

Methods of Attack

- Malware
- Phishing
- Vishing
- Ransomware
- Social Engineering

Ransomware Is Spiking

- Working Remotely has caused large spikes
- In the last 2 quarters of 2022, there were 155 million cases world-wide
- 381 attacks against US organizations in 2022; average ransom demand of $4.15M
- 43% of all global attacks were in United States
- Attacks have become very sophisticated
- Many organizations are attacked more than once

To Pay or Not to Pay

- How sensitive is the information?
- Do you have back-ups of critical data?
- What are your RPO and RTO times?
- What is cost of refusing to comply?
- Legal issues associated with attack

Social Engineering

Email

Phone

Indirect Contact

Cyber Liability Insurance might not cover

What Can You Do?

- Develop a Cyber Security Plan
- Use Multi Factor Authentication
- Encrypt Data and Passwords
- Remote Back-up
- Train and Test Staff
- Board Meeting Minutes – don’t disclose to much
- Verify Not Trust
- Test Your Systems
- Cyber Insurance Policy

Session Recap:

DOL Guidelines are a good path to follow

Review your pension funds vulnerable points

Request proper documentation from vendors

Adopt proper policies and procedures to protect your fund

Questions?