Cyber Security – DOL Tips for Retirement Plans

John R. Reidy, President

Pension Technology Group

PENSION
TECHNOLOGY
GROUP

Hiring a Service Provider for your Pension Fund

- Pension funds rely on many different service providers to assist in various aspects of the fund's initiatives.

- These service providers have access to and maintain vital information pertaining to the pension fund.
  - Membership Personal Information
  - Pension Fund Finances

- Pension funds should require that their service providers follow strong cyber security practices.

- Common security practices can be measured and validated.

Presentation Goals

- Identify common security protocols and practices.
- Describe the validation reports that are designed to document the effectiveness of these security practices.
- Provide questions that Pension Trustees can ask of their service providers regarding their security practices.
- Help establish guidelines that pension funds can use to ensure that they are kept current with documenting their due diligence pertaining to the security practices of their service providers.

SOC Reports

- SOC Reports are Service Organization Reports that demonstrate that company/organization is following best practice and standards.
- A company will hire a third party to examine various aspects of their own operations.
- These reports are typically released annually.
- Pension Fund Auditors often request these reports during Audits.
- It is important for Pension Funds to gain an understanding of when each of their service providers reports are released.
- Bridge Letters can be provided to cover the time gaps between reports.
- These reports should be treated as confidential and are not for public dissemination.

Difference between 1/SOC, 2/SOC, 3/SOC & SOC for Cybersecurity

- **SOC 1 Reports** typically focus on outsourced services performed by service organizations that relate to financial reporting.

- **SOC 2 Reports** focus on operational risks associated with outsourcing outside of financial reporting.

- **SOC 2 Reports** are based on the Trust Services Criteria.
  - Security
  - Availability
  - Processing integrity
  - Confidentiality/Privacy

- **SOC 3 Reports** (SysTrust/WebTrust) cover areas similar to SOC 2 but not as comprehensive. Typically used for marketing purposes.

- **SOC for Cybersecurity** is a new report created by American Institute of Public Accounts (AICPA) that focuses mostly on an organizations enterprise wide cyber-security risk program.

Penetration Tests

- Penetration Tests (PEN Test) is the practice of testing a computer system, network, or web application to identify security vulnerabilities that a hacker might exploit to cause harm.
- PEN Tests are simulated attacks on a system performed by an independent third party.
- PEN Tests target the server where the target data is being stored.
- PEN Tests will result in a detailed report that details strengths and weaknesses of a technical environment.
- PEN Tests help companies to evaluate and measure their security infrastructure.
- PEN Test are not inexpensive but should be performed annually and or after any modifications of technical environment.

Web Application Firewall Grading

- Web Application Firewall (WAF) tests are designed to measure the effectiveness of the firewall that is securing the application.
- WAF Tests are not the same as Penetration Tests.
- WAF's are the first level of defense for the application.
- WAF's can be programmed to block traffic from specific originations/locations.
- WAF Testing reports result in an A-F Grading System.

Vulnerability Scans

- Vulnerability scans are regular/consistent scans of the firewall and application.
- Vulnerability scans are not as intense as PEN/WAF Tests.
- Vulnerability scans can be performed on a more regular/consistent basis. (Weekly/Monthly)
- Vulnerability scans are designed to measure the software application against the evolving landscape of cyber threats.
- Vulnerability scans test against the latest industry specific threats.
- Notification of a High/Medium threat should motivate the software provider to reconfigure the environment accordingly.
- PEN/WAF Test on new environment should be executed.

Disaster Recovery Plans

- A Disaster Recovery Plan is a formalized document that details how an organization will recover from a disruptive event.
- Organizations should establish a Recovery Point Objective (RPO) that identifies how long systems can be down without causing catastrophic impact to the business.
- Recovery Time Objectives (RTO) is the organization’s expectations of how long it would take to become operational after a disruptive event.
- Disaster Recovery Plans should be executed and tested to ensure that both the RPO and RTO expectations are met.
- Results of these tests can be documented and kept on file.
- A Disaster Recovery Plan is a formalized document that describes in detail how an organization will from a disruptive event.

Insurance Policies

- Inquire with your vendors about their Insurance Policies
- Do their policies cover losses caused by cyber or identity threat breaches
- Professional Liability/Errors and Omissions Coverage
- Obtain a copy of your vendors Certificate of Insurance on an Annual Basis.

Cyber Breach Incident Reports

- Ask your vendors if they have ever experienced a data breach
- If your vendor has experienced a data breach request an Incident Report about the Breach
- Incident Reports will document how the vendor responded to incident.
- Did the vendor notify the appropriate parties?
- Did the vendor investigate the incident?
- Did the Vendor fix the issue?
- What operational changes were instituted to mitigate future risks.

Presentation Recap

- Ask your vendors for the following documents:
- SOC Report
- Penetration Test/Web Application Grading Reports
- Vulnerability Scan Reports
- Disaster Recovery Tests
- Insurance Coverage Documents
- Cyber Incident Reports