withum

CASE STUDY

PROACTIVE CYBERSECURITY FOR MULTIEMPLOYER FUNDS

EXECUTIVE SUMMARY

A self-administered multiemployer fund engaged Withum's Cybersecurity team to evaluate its existing cybersecurity program. Withum conducted a thorough review of its written information security program, performed vulnerability scans, and executed both internal and external penetration tests. This comprehensive approach identified potential vulnerabilities and provided actionable recommendations for remediation. Withum also collaborated with the client to update its cybersecurity policies, ensuring compliance with the Department of Labor's (DOL) Cybersecurity Program Best Practices.

THE CLIENT

The client is a large self-administered multiemployer fund with a team of approximately 20 IT and Development Operations employees.

THE CHALLENGE

The client was concerned about potential vulnerabilities in its information security program that could be exploited by threat actors. It also wanted to ensure compliance with DOL guidelines.

THE APPROACH AND SOLUTION

- **Penetration and Vulnerability Testing:** Withum's team performed extensive vulnerability scans on the client's infrastructure. By leveraging these results, the team attempted to gain elevated privileges within the systems, successfully accessing admin-level data. This testing simulated potential hacker activities, allowing the client to address identified vulnerabilities and prevent unauthorized access. Withum conducted retests to confirm that all vulnerabilities were effectively mitigated.
- **Cybersecurity Program Review:** Withum reviewed the client's existing written cybersecurity policies and provided updated feedback to ensure compliance with DOL guidelines as well as provided working drafts of additional policies the fund could customize for their environment.

CASE BRIEF

CLIENT: A large self-administered multiemployer fund with a team of approximately 20 IT and Development Operations employees

CHALLENGE: Concerned about potential vulnerabilities and exploitation in its information security program

OUTCOME: Addressed vulnerabilities before any data breaches occurred along with detailed recommendations for system reconfiguration and enhanced security measures. Updated policies and reporting mechanisms to align with current DOL guidance

THE RESULTS

The testing revealed personal identity information (PII) related to the plan's participants, highlighting vulnerabilities that could potentially be exploited. Withum's timely intervention prevented external threat actors from accessing this sensitive data. The findings were shared with the client, along with detailed recommendations for system reconfiguration and enhanced security measures. Withum also assisted the client in updating its policies to align with DOL guidance, providing a comprehensive report of findings and actionable next steps. This assessment can be presented to the DOL during audits, providing assurance that a robust information security program is in place. Having written policies ensures continuity of security measures, even if key personnel leave the organization.

CONCLUSION

Through proactive cybersecurity measures, the fund was able to address vulnerabilities before any data breaches occurred. The updated policies and reporting mechanisms provide alignment with current DOL guidance. It is crucial to recognize that cybersecurity is an ongoing process. As threats evolve, continuous updates and annual third-party audits of security controls are essential to maintain effective protection.