Construction Industry

Cybersecurity Threat Assessment

The cybersecurity threat assessment is designed to quickly identify the potential vulnerabilities that could be exploited by the most common cybersecurity threats.

Business owners and executives need information technology to simply work and be resilient to support the business. Ransomware, data breaches, and fraudulent wire transfers are expensive distractions that can divert focus. Wipfli's Cybersecurity Threat Assessment is designed to provide you with insight into where your company has elevated risk related to the most common cyber threats to the construction industry.

This assessment focuses on the following critical areas of your business:

- External hack/unauthorized access to network
- Ransomware (malware)
- Unauthorized funds transfer
- Business email compromise (BEC)
- Business interruption

Approach

We use a combination of targeted control tests and interviews to determine the level of risk associated with each threat and provide prioritized recommendations to reduce the probably or impact of each threat. We use the following data inputs to prepare the threat analysis report:

- Scan of internet perimeter to identify known vulnerabilities
- Rapid scorecard to assess vulnerabilities discoverable on open source intelligence (OSINT)
- Email phishing campaign to identify "phish-prone" employees and user awareness
- Password cracking test to identify weak passwords
- Email compromise report showing email and passwords that have involved in a disclosed data breach.
- Microsoft Secure Score (if applicable) to assess security posture on Microsoft 365
- One (1) hour interview with client and IT service provider to assess security practices (if applicable)

Outcomes

Wipfli will analyze the results from each of the tests and interviews to prepare a comprehensive Threat Scenario Risk Profile along with prioritized recommendations so that you can make informed decisions on how to manage risk.