asureti

Cybersecurity Maturity Assessment

Case Study

National Wholesale Building Material Distributor

Midwest, United States

This company offers a complete range of products and services for both the public and private sectors and operates across the United States. Each of their 60 offices offers preventive maintenance programs and emergency service capabilities 24 hours a day, 7 days a week, 365 days a year.

Key figures:

- Serving over 1 million commercial and residential customers.
- Over 3,000 employees, and 1,700 service vehicles.
- Over $1 billion revenue in 2023.

asureti

The Challenge

As part of their objectives to protect their systems and data, this organization wanted to review their current information security program and their ability to protect critical data, processes, and associated assets. Our assessment allowed the organization to clearly understand their security risk management maturity, confirm alignment with regulatory and compliance obligations, and prioritize areas for improvement.

Potential Low Maturity Cybersecurity Risks

Increased Vulnerability to Attacks

Increased susceptibility to cyberattacks, such as malware, phishing, and ransomware.

Legal Action & Financial Losses

Increased exposure to substantial legal actions, litigation, and the costs associated with data breaches.

Reputational Damage

Potential loss of customer trust, business opportunities, and competitive advantage.

asureti

Our Approach

We utilized the National Institute of Standards and Technology (NIST) Cyber Security Framework 2.0 (CSF) as a baseline to identify strengths and weaknesses in the company's current security program. This process included interviews with key stakeholders, documentation reviews, and analysis of current state operations as outlined in the following steps:

1. **Performed an enterprise-wide review** of the company's current security program and their ability to protect critical business units, processes, and associated information assets.

2. **Identifed program strengths and opportunities** for improvement to increase the overall maturity of the security program.

3. **Provided prioritized recommendations** related to identified risks that allow the company to increase its desired security posture and reduce risk exposure.

4. **Identifed areas** where resources can be used to maximize investments while reducing risk to the organization.

asureti

Our Analysis: Program Strengths

Employee Expertise and Longevity: Skilled cybersecurity professionals in place with extensive institutional knowledge.

Senior Management Support: Commitment from senior management for funding and prioritization of security initiatives.

Technical Measures: Examples included effective use of VLANs and Multi-Factor Authentication (MFA) enhancing network segmentation and account security.

Field Connectivity and Logging: Secure field devices adequately deployed and extensive system logging in place for detecting and analyzing security events.

Our Analysis: Gaps Identified

Program Governance: We recommended improvements in documentation and communication of cybersecurity policies and standards, as well as updated training programs.

Security Monitoring: We identified recommendations for their security monitoring process and use of logging tools for enhanced threat detection and response.

Vulnerability Management: We recommended strengthening vulnerability management programs through updates to secure coding practices and patching processes.

Resource Allocation and Documentation: We noted that limited resources sometimes resulted in delayed remediation, insufficient incident response plans, and incomplete documentation of systems architecture and dependencies.

Business Continuity and Data Management: We identified incomplete governance of continuity programs, inconsistent data retention and destruction standards, and lack of integrated risk management processes.

Project Recap

The maturity assessment of this company's security program involved reviewing current practices, identifying strengths and weaknesses, and providing a maturity summary with actionable recommendations.

Our findings emphasized the need for improved documentation and governance, as well as the importance of prioritizing data security and compliance to align employee actions with desired program practices.

The recommendations we presented guided the improvement and maturing of the company's security program and operations efforts. Working with Asureti allowed this company to be in a better position to avoid risks of data breaches and compliance failures, and address regulatory and customer inquiries more effectively.

asureti

Similar Challenge?

Book a discovery call

Email

info@asureti.com

asureti