ACME Cyber Security Program Review Results

ABSOLUTE PERFORMANCE

Risk Profile

Operating in the Financial Services industry, ACME faces several unique threats due to their access to liquid currency, sensitive data, and partner relationships.

With over 300 employees and over $25m in annual revenue, ACME would also be classified as a mid-sized company.

As a result of their market vertical and size, the Triton team estimates that they are a **Moderate to Highly Attractive Target for** attackers and should align their defense to a financially motivated attacker with **Organized Criminal** level capabilities.

Likely Attack Vectors

Business Email Compromise

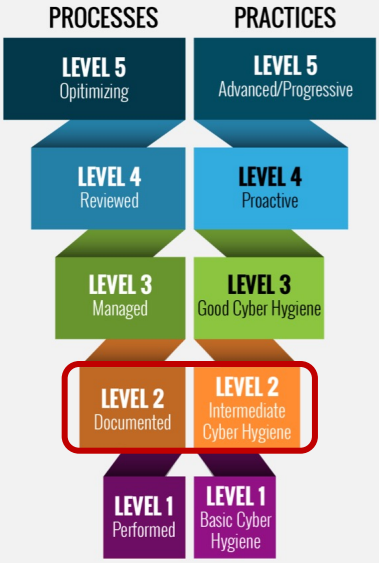
Attackers use a variety of techniques to compromise an employee email address. Once the email has been compromised, they may impersonate key stakeholders to persuade employees to transfer funds to an account controlled by the attacker.

Ransomware

Malware encrypts or destroys key data and systems. Then attackers demand a payment to restore access or not release sensitive data. According to Sophos, over 50% of financial services organizations were hit with a ransomware attack in 2022, making it one of the most targeted industries.

A high level Cyber Security Program Review with ACME Stakeholders was conducted on 5/19/23.

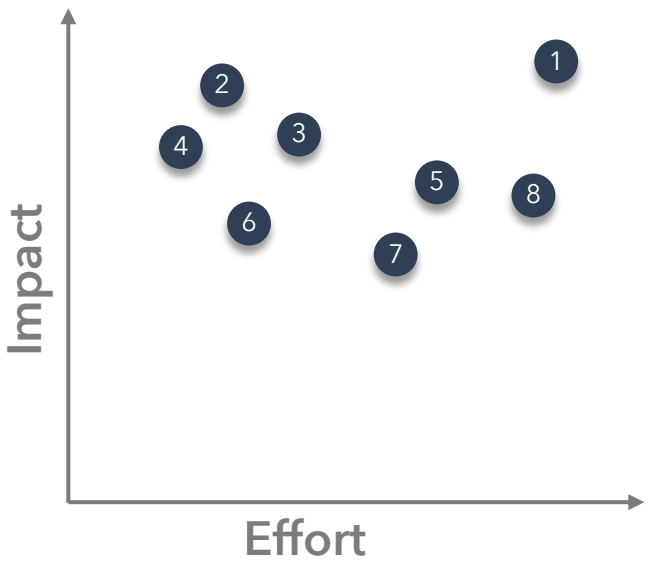
The review focused on the 5 Functions identified in the NIST CSF. Based on this review, the team worked with ACME to identify key controls and areas of possible improvement in their security posture.



Using the CMMC Maturity Model, the ACME's cyber program **was accessed** to be a **Level 2** maturity program.

Based on the initial review, many of the foundational building blocks of a robust security program appear to be in place, but additional focus may help enhance the effectiveness and efficiency of the controls. This may include expansion of current controls to provider broader cover across the environment.

ACME can enhance their security program through technical, procedural and strategic initiatives, several of which are shown below. Note that this is not a complete list.



1. MFA Enhancements
2. Risk Assessment and Security Strategy Review
3. SOC/SIEM Improvements & Tuning
4. Incident Response Planning
5. Vulnerability Scanning & Remediation
6. Vendor Monitoring
7. SOC/SIEM Device Onboarding
8. Network Segmentation