Calvetti Ferguson

CYBER SECURITY ASSESSMENT

The Calvetti Ferguson cyber security assessment is a detailed look into your IT environment and is normally completed in a few weeks. The cyber security assessment gives management a helpful glimpse into how to handle common risks in the company's IT environment.

When an organization's vulnerabilities are exploited, they become susceptible to data loss, identity theft, unauthorized access to network resources, systems, and resources, and implementation of malware that can lead to ransom attacks, stolen information, and other destructive actions.

Our clients receive valuable insight into areas where they might be carrying significant risks, a preliminary evaluation of the quality of controls in place, and detailed recommendations to help their organization improve.

The cyber security assessment is designed to assist organizations in:

- Understanding their current security posture
- Assessing their exposure to common vulnerabilities and threats
- Making a preliminary evaluation as to the current design of controls in place

Our cyber security assessment is customizable and scalable to accommodate organizations of all sizes, complexities, and industries. The assessment is primarily focused on the following areas:

- IT Governance
- Logical and physical security
- Change management
- IT operations
- Problem management
- Asset management
- Incident response
- Business continuity
- Disaster recovery
- Third-party risk management

WHAT DOES THE CHECK UP FOCUS ON?

A Calvetti Ferguson cyber security assessment, is the first step to determining the current state of risk and compliance and generating a prioritized plan for reducing risk, staying compliant, and appropriately protecting sensitive information.

Phase 1

- Documentation of all hosts, OS, and applications
- Capturing of network architecture, including, open ports, protocols, and services
- Internal and external vulnerability scans for assessing the IT infrastructure

Phase 2

- Documentation review of existing IT, cyber security, and physical security policies
- Interviews with key stakeholders to discuss observations
- Creation of a list of prioritized recommendations for improving the overall security posture

Phase 3

- Presentation of findings
- Development of security program roadmap

WHAT IS THE PROCESS?

As part of the check-up, we will conduct a thorough search on the dark web to identify any potential compromises linked to your internet domain. This search will help us gain valuable information about the origin and nature of compromised data, including personal information or stolen account passwords.