FORTRESS
SECURITY RISK MANAGEMENT
A Division of **MCPc**

TECHNICAL TESTING

No one is immune to cyber-attacks.

Technical testing by Fortress SRM identifies vulnerabilities early on and proactively prevents attacks.

PENETRATION TESTING

KEY BENEFITS

- Identify security risks: our security experts identify the information assets at risk
- Identify test readiness: depending on your maturity, our testing services help address your security
- Meet compliance: experienced testers understand compliance requirements
- Improve security: obtain a prioritized list of actionable items to address

VULNERABILITIES ASSESSMENT

KEY BENEFITS

- Internal and External validation of exploitable vulnerabilities following internationally accredited methodologies
- Assessment paths that mimic the approach of real-life attackers in a controlled manner
- An analysis of root cause to help critique existing practices and inform future decisions
- The formation of clear, actionable and prioritized recommendations that once implemented will reduce the likelihood of an incident
- Support for informed decision making capable of improving the organizations susceptibility to malicious and accidental exploits

WIRELESS ASSESSMENT

Fortress SRM will conduct configuration review, technical testing, and scanning for rogue access point detection. For Payment Card Industry (PCI) data environments covered within scope, this testing may be used to satisfy relevant Data Security Standard requirements. We will passively monitor the wireless network to determine weaknesses first, and then, if necessary, actively attack the network to gain access by breaking encryption keys or bypassing other security measures. Results of the test may include, as appropriate:

- Wi-Fi signal leakage security design flaws
- Encryption keys (IVEP/WPA)
- Rogue access points analysis of defensive measures

PHISHING SIMULATION

Fortress SRM will facilitate phishing tests to assess our customers' risk exposure to phishing and weak security behaviors. These risks are often introduced to an organization by its employees, agents, and contractors. The objective is to validate user security awareness.

In these tests, customers can choose from a list of possible phishing attacks that vary in complexity and extent of data harvesting. With every click of a links in the emails, the perpetrating user will receive a brief message notifying them of the test along with a security awareness video. Once the test emails have been sent, all results will be compiled by our team and presented to the client.