FORTRESS
SECURITY RISK MANAGEMENT

Service Brief

Cybersecurity-as-a-Service

Dramatically improves an organization's cyber maturity and response capability, affordably.

The development of an Incident Response Program has significant value in protecting an organization from cyberattack. As a monthly subscription program, the Fortress SRM Cybersecurity-as-a-Service Program offers a truly comprehensive, phased, and affordable way to clearly assess an organization's cyber maturity, develop a security plan around identified vulnerabilities, prioritize immediate actions to take to address critical risks, establish the cyber response team, and practice what to do in the event of a cyberattack.

PROGRAM ELEMENTS:

Cybersecurity Program Maturity Assessment

An in-depth security program assessment is measured against best practice cybersecurity frameworks: ISO27001, NIST, or one of the CIS Top 20 frameworks based on industry or company preference.

Governance, Risk, & Compliance Management

Fortress SRM uses specialized Governance, Risk and Compliance (GRC) software that allows for efficient building, management, and reporting of the Client's chosen security framework. This software allows for continual monitoring and updating of Client progress in addressing gaps, allowing for a real time view of the Client's maturity posture.

Development of Security Program Documentation

The purpose of an Incident Response Program is to define a high-level incident response management structure for any cybersecurity incident. The program, as defined by an Incident Response Policy and Management Plan, is used to set response expectations and define general communication processes for managing security incidents, which helps minimize the impact and scope of the incident on the organization.

Defining standard incident handling protocols reduces ambiguity and helps keep stakeholders accountable and aware of the incident. It is expected that while the Incident Response Policy may require occasional edits, the Management Plan will be regularly reviewed, evaluated, and updated as part of the Client's on-going security program. This also involves the appropriate training of resources expected to respond to security incidents, as well as the training of general employees and the understanding of their security responsibilities.

Quarterly Security Briefings

To stay current with the latest threats and review the processes and procedures in the plan, quarterly briefings are a critical aspect to get the organization to have "muscle memory" of the incident response plan and procedures.

Incident Runbooks

The development of an Incident Runbook (or Playbook) will allow the Client to plan for and define specific responses to common cyber incidents. The key to success in responding to and remediating a cyber incident is to not only document processes, roles and responsibilities as will be done in the Incident Runbook, but to practice these documented procedures in the form of a simulated incident.

Attack Simulations – Tabletop Exercises

Fortress SRM will provide Tabletop Exercises to correspond with the chosen Runbooks. In these live simulations, Fortress SRM will present the Client with a simulated incident. These exercises will bring together all players on the Incident Response team to identify gaps in response, improve the plan and policies, practice the technical and managerial responses, review the coordination and communication structure, and identify new threats and risks.

Incident Response

The high-level activities Fortress SRM will perform during an investigation (if an attack were to occur) consist of the following:

- **Assess:**
  Gain an understanding of the current situation.
- **Client Objectives:**
  Define objectives that are practical and achievable. The goal will be to identify data loss, recover from the event, determine the attack vector, identify the attacker, or some combination.
- **Analyze:**
  Based on the evidence that is available and the Client's objectives, Fortress SRM will draw on skills that range from forensic imaging to malware and log analysis to determine the attack vector, establish a timeline of activity and identify the extent of the compromise.
- **Provide Direction:**
  During each investigation, Fortress SRM will work with Client management to provide status reports that communicate findings.
- **Remediation Plan:**
  Remediation plans vary depending on the extent of the compromise, the size of the organization, and the tactics/objectives of the attacker. As part of an investigation, Fortress SRM will deliver a comprehensive remediation plan and assist with the implementation.
- **Reporting:**
  Fortress SRM will provide a detailed investigative report at the end of every engagement that seeks to address the needs of multiple audiences including senior management, technical staff, third party regulators, insurers and litigators.

Incident Response Service Level Agreement (SLA)

- An Incident Commander will respond to a Client request or emergency assistance within four (4) hours.
- If the Client requests on-site assistance in the continental U.S., Fortress SRM will make a reasonable effort to arrive on-site within twenty-four (24) hours. Response time outside the continental U.S. is subject to travel carrier and visa availability. Fortress SRM will make commercially reasonable efforts to respond to Client travel requests.
- The traditional $15,000.00 incident declaration fee will be waived for Cyber-as-a-Service Clients.
- In the event of a cyber incident, Client will receive discounted rates.

Penetration Tests

Fortress SRM penetration tests are threat-centric, emulating a variety of threats based on the tactics, techniques, and procedures outlined in the MITRE ATT&CK framework. A threat-centric penetration test validates security measures, prioritizes vulnerabilities, and highlights the impact and probability of a cyber-attacks.

All of our team members are Certified Ethical Hackers accredited by the EC Council and are continually working to expand their skills on a variety of tools and tactics.

Fortress SRM Penetration Tests are modeled after the industry recognized PTES methodology, NIST SP 800-115, the MITRE ATT&CK framework, and the OWASP Web Application Penetration Checklist.

Security Awareness Training

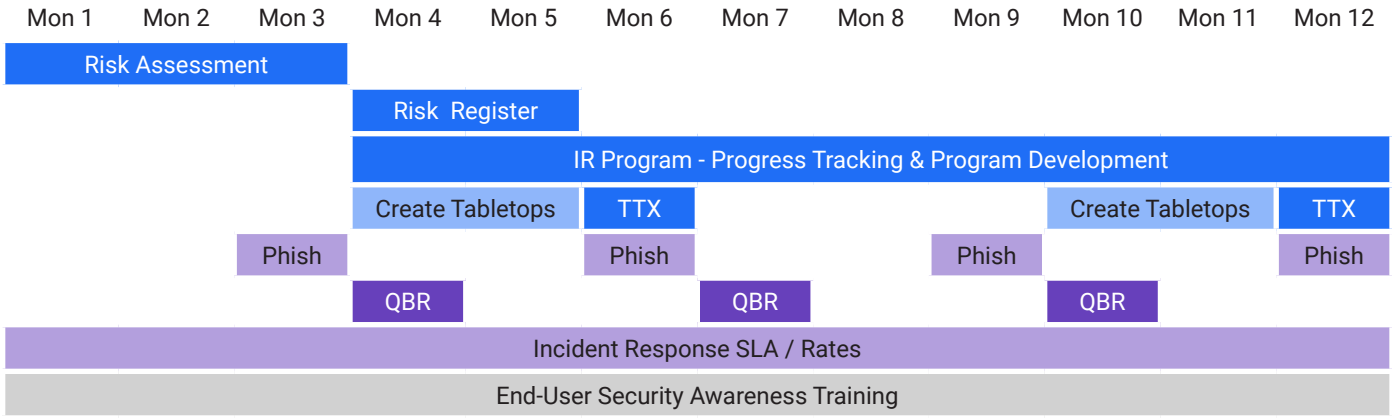
No matter how strong a company's technical controls, the end-user will pose a perpetual risk to the organization. While it is impossible to eliminate this threat entirely, Fortress SRM aims to drastically reduce end-user risk through targeted and tangible security awareness training and testing. This awareness training program consists of hands-on user training on common security issues (to be chosen by the Client) integrated in the Client's existing Learning Management System (LMS) or our hosted LMS site, as well as frequent phishing campaigns.

These phishing campaigns are designed to assess the Client's risk exposure to phishing and other exploits of weak security behaviors. Fortress SRM and the Client will agree upon appropriate levels of complexity and content from a collection of prepared (and common, real-life) templates, as well as the content delivered to end-users when a link is followed, or an attachment is downloaded in the simulated phishing email.

Program Development Deliverables

The development phase of a cybersecurity program involves an understanding and assessment of the threat environment and associated risks to the Client's business. Fortress SRM will provide a strategy for improving the Client organization's cyber maturity. This program development will be aimed at the creation or editing of policies and procedures along with the establishment and/or assistance of governance-oriented entities within the organization.

Example of a typical implementation schedule:



OUTCOMES:

- Risk Assessment mapped to selected framework (ISO, NIST, CIS Top 20, etc.)
- Risk Register
- Governance, Risk, and Compliance Software
- Progress Tracking of Identified Gaps
- Incident Response Policy and Management Plan
- Incident Runbooks x2
- Tabletop Exercises x2
- Vulnerability Assessments x4
- Penetration Test x1
- End-User Security Awareness Training
  - Tailored LMS-Integrated Training and Phishing Scenarios x4 (quarterly)
- Incident Response Support, Service Level Agreement, and Reduced Rates

BENEFITS:

- ✓ Dramatically improves cyber maturity
- ✓ Minimizes business disruption in the event of an attack by speeding recovery
- ✓ Helps ensure operational continuity
- ✓ Mitigates financial, data, operational, compliance, and reputation risk
- ✓ Affordable, monthly subscription