FLEXENTIAL

Cyber Defense **Program**

Systematically reduce IT risk and materially improve cybersecurity defenses

Internal cybersecurity teams face an expanding threat landscape and increasing attacks, including rampant ransomware attacks. To successfully defend, detect and respond, security organizations must proactively and systematically manage and mitigate risk and continuously fortify their environments against more attack surfaces and constantly shifting threat vectors.

Flexential's Cyber Defense Program combines cybersecurity and risk management best practices and standards to address these challenges in a recurring quarterly engagement. Our Professional Services' cybersecurity and risk team partners with your team to assess the security of your environment through penetration testing, ransomware defense readiness, incident response testing and risk assessment.

We deliver reports with specific, prioritized, actionable recommendations to improve your cybersecurity posture and reduce risk. The Cyber Defense Program enables and educates your team to programmatically apply risk and cybersecurity best practices that increase defense-in-depth by improving detection capabilities, strengthening response capabilities, and managing IT risks.

Deliverables include a comprehensive IT risk profile with identification of the most critical risks and data-based prioritizations for which mitigation actions to take and in which sequence. The program includes comprehensive assessments of environment architecture, preventative controls, and IT risks.

External Penetration Test

Objective: To find perimeter weaknesses and provide detailed remediation guidance to strengthen defenses

- Our certified penetration testers scan the dark web and then attempt to breach your external infrastructure.

Ransomware Defense Readiness

Objective: To ensure there are defenses, response capabilities and recovery capabilities in-house before a ransomware incident occurs

- Our team will understand your business, compliance, and regulatory needs and deep dive into environment architecture to uncover weaknesses
- We provide detailed, actionable and prioritized guidance to remediate weaknesses and strengthen defenses

Incident Response Tabletop

Objective: Build a more mature incident response (IR) program and a more knowledgeable and prepared staff

- We email phish your organization to test threat awareness
- We conduct incident scenario tabletop exercises to discover gaps and educate internal staff
- We document gaps and prioritize remediation recommendations to improve IR plans and policies

Risk Assessment

Objective: Understand IT risks by likelihood and impact, and know corresponding remediation actions

- We identify and document known and unknown IT risks, compensating controls, information assets, threat sources, events, and vulnerabilities.
- Deliverable includes detailed, actionable, and prioritized guidance to remediate risks

Deliverables

- Quarterly reports with detailed, actionable, and prioritized recommendations
- Presentations of findings with discussion of recommendations
- Knowledge transfer to security and risk teams
- Technical guidance for remediation of identified risks
- Executive summary of identified risks to share with IT and executive leadership
- Risk ratings for identified threats

Problems we solve

- Unknown and unaddressed risks
- Ad-hoc or reactive security approaches
- IT teams that are unsure of where to start
- Uncertainty on why and how to prioritize actions
- Lack of cybersecurity or compliance knowledge
- Insufficient tools and training
- Annual compliance requirements, such as HIPAA, PCI, ISO, and SOC 2

Outcomes we create

- Increased cyber defenses
- Know what to do and in which sequence to improve cybersecurity
- Increased IT staff preparedness and knowledge
- Visibility and documentation of business-impacting risks
- Alignment of risk reduction activities with business needs
- Confidence in meeting customer or regulatory requirements