Defensible

Defensible Risk Assessment Methodology

An effective approach to managing information security risk includes evaluating the root causes of historical data breaches. While the specific vulnerabilities, attack techniques, and circumstances involved in a given data breach are often unique, a common pattern of direct technical and indirect policy or governance-related root causes can invariably be established.

Defensible's risk assessment methodology utilizes the seven technical root causes and three governance root causes as reference points when evaluating the current state of our client's information security program.

DATA BREACH ROOT CAUSES

DIRECT

1. Unencrypted data
2. Phishing
3. Malware & Ransomware
4. Third-party compromise
5. Software vulnerability
6. Inadvertent mistakes
7. Credential theft

INDIRECT

1. Lack of prioritization
2. Underinvestment
3. Poor execution

The five Information Security risk management functions, as defined by the NIST Cyber Security Framework, enables Defensible to evaluate the effectiveness of our client's security risk management program.

Identify: Develop an understanding of your environment to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect: Develop and implement the appropriate safeguards to limit or contain the impact of a potential cybersecurity event.

Detect: Implement the appropriate measures to quickly identify cybersecurity events.

Respond: Develop and apply a detailed response plan to take action if a cybersecurity incident is detected.

Recover: Develop and implement activities to restore any capabilities or services that were impaired due to a cybersecurity event.

Defensible's Unique Approach to Risk Assessments

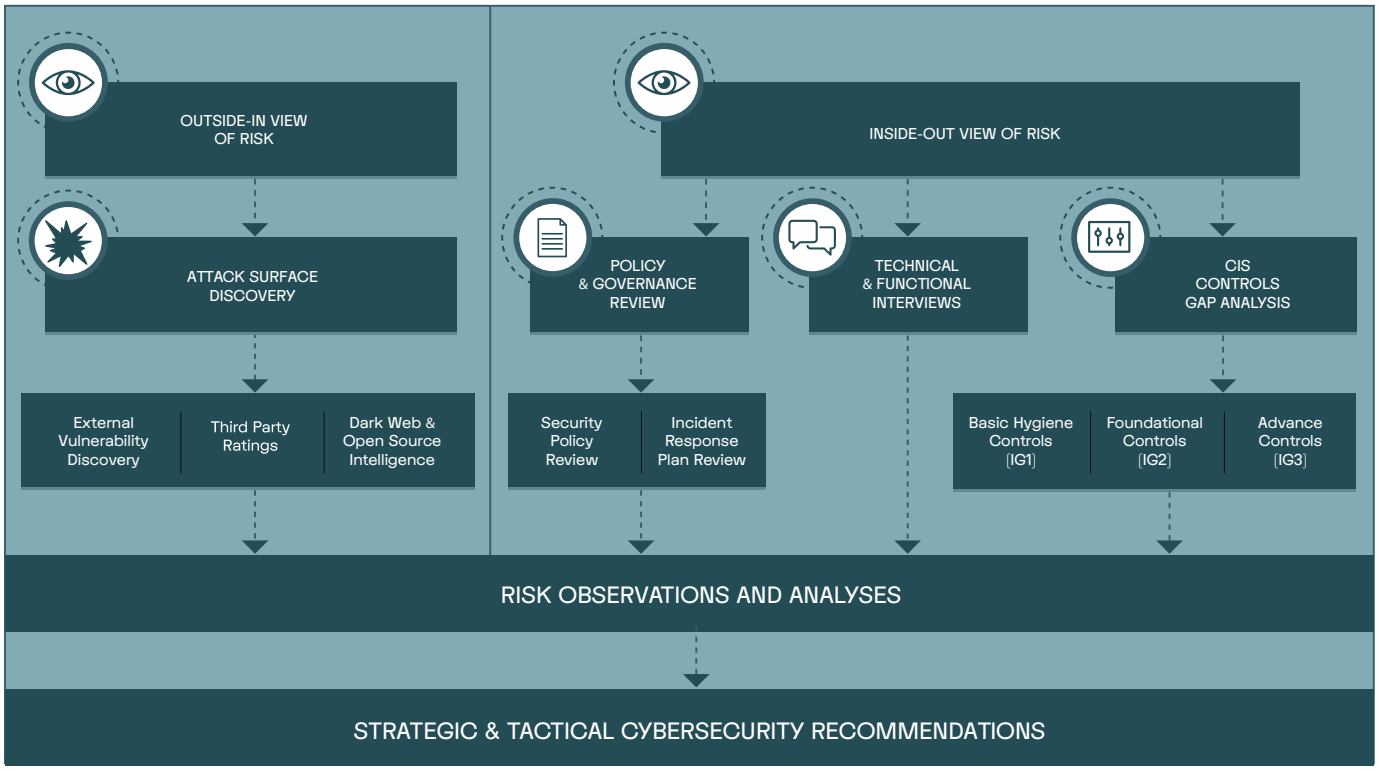
Defensible examines security risk from two perspectives – the outside in and the inside out. This approach allows us to identify patterns of information security risk relative to a client's information security program and provide tactical and strategic recommendations on security risk management.

External Risk Perspective

From the outside in, or external view of risk, Defensible utilizes publicly available information and data from several external sources to establish and define an attack surface that would be accessible to a bad actor.

Internal Risk Perspective

From the inside out or internal view of risk, Defensible evaluates a client's information security policies, business and technical operations, and the controls or safeguards that the organization implements to protect, detect, and respond to cybersecurity incidents and attacks.



What to Expect During a Risk Assessment

Attack Surface Discovery: Our team utilizes publicly available information, open-source intelligence (OSINT), and vulnerability scanning techniques to identify weaknesses and potential attack vectors.

CIS Controls Assessment: We utilize the CIS Controls from the Center for Internet Security as a quick and cost-effective method for identifying gaps in the information security program and establishing a reasonable, affordable, and defensible security roadmap.

Policy and Governance Review: Defensible consultants collect baseline information and documentation on the client's current security environment, including all relevant policies, standards, guidelines, procedures, and technical documentation.

Technical and Functional Interviews: We conduct interviews with key stakeholders in each of the client's core operational or functional areas identified as critical to managing risk and sustaining business operations.

Arm Your Organization with Defensible

Assess: Proactively evaluate your organization's ability to effectively prevent, detect, and respond to cyber threats and receive tactical and actionable recommendations to improve processes, technologies, and overall security posture.

Remediate: Address and fix security incidents quickly, effectively, and at scale with comprehensive incident response including investigation, remediation, and new technology deployments.

Manage: Outsource the systematic approach to managing your organization's security needs by having us oversee the company's network and information system security on a continuous, retainer-based basis.

Get Started With Defensible
www.defensible.tech