enveedo

RISK SCORECARD REPORT

Prepared on: **November 2024**

Risk Scorecard

The Risk Scorecard, derived from a high-level assessment, **provides an initial overview of potential security vulnerabilities**. It serves as a valuable first step, pinpointing areas of heightened risk that warrant a more in-depth analysis.

The Enveedo platform builds upon these findings, delivering detailed assessments and actionable insights.

Organizations can prioritize immediate concerns, while also crafting a robust, long-term security strategy.

Enveedo's data-driven approach empowers users to not only identify weaknesses, but also tailor remediation efforts to their specific needs. This proactive stance ensures that security measures continuously evolve, keeping pace with emerging threats and business goals — fostering a resilient, adaptive security posture.

Risk Scorecard

5

CRITICAL LIKELIHOOD

Risk List:

01. Application Vulnerabilities
02. Artificial Intelligence & Autonomous Systems
03. Data Leakage
04. Distributed Denial of Service (DDoS)

Minimal to no controls are in place, making the risk highly probable and almost certain to occur.

3

HIGH LIKELIHOOD

Risk List:

01. Governance
02. Human Error
03. Insider Threat
04. Network Vulnerabilities

Many controls are ineffective or missing, leading to an increased likelihood of the risk materializing.

4

MEDIUM LIKELIHOOD

Risk List:

01. Privileged Misuse
02. Ransomware
03. Security Culture
04. Social Engineering (Pishing)

Some controls may be partially effective or missing, creating opportunities for improvement and a moderate chance of risk occurrence.

2

LOW LIKELIHOOD

Risk List:

01. System Intrusion
02. Third-Party Risk

Most controls are effective and well-implemented, reducing the likelihood of the risk significantly but not entirely.

1

LOWEST LIKELIHOOD

Risk List:

01. Unpatched Software

Controls are highly effective and fully implemented, making the likelihood of risk occurrence very minimal.

Risk Scorecard

CRITICAL LIKELIHOOD

Application Vulnerabilities

Weaknesses in software applications that can be exploited by attackers, often due to coding flaws or unpatched issues, potentially leading to unauthorized access, data breaches, or service disruptions.

Top Mitigating Controls

- Secure Coding Practices
- Web Application Firewall
- Penetration Testing
- Vulnerability Management

CRITICAL LIKELIHOOD

Artificial Intelligence & Autonomous Systems

AI and autonomous systems can introduce legal and reputational risks, including bias, discrimination, and decision-making errors, which could negatively impact operations or safety.

Top Mitigating Controls

- Algorithm Audits
- Access Control
- Incident Response Plan
- Cybersecurity Policies

CRITICAL LIKELIHOOD

Data Leakage

Unauthorized or accidental exposure of sensitive data to external parties, potentially leading to financial loss, reputational damage, or legal consequences.

Top Mitigating Controls

- Data Loss Prevention
- Encryption
- Conditional Access
- Cybersecurity Policies

CRITICAL LIKELIHOOD

Distributed Denial of Service (DDoS)

A large volume of traffic disrupts system or network availability, leading to downtime and operational losses. DDoS attacks can overwhelm systems, affecting service reliability and causing financial damage.

Top Mitigating Controls

- DDoS Protection
- Next-Gen Firewall
- Load Balancing
- Security Operations Center
- Cyber Insurance Policy with Ransomware Coverage

CRITICAL LIKELIHOOD

Governance

Weak governance can lead to legal and financial penalties due to poor policies and oversight, resulting in security risks, compliance violations, and operational failures.

Top Mitigating Controls

- Governance Framework
- Compliance Management
- Regular Audits
- Policy Enforcement

HIGH LIKELIHOOD

Human Error

Mistakes caused by human actions, such as misconfigurations or negligence, can lead to security breaches, system outages, or data loss, resulting in operational and financial impacts.

Top Mitigating Controls

- Policy Enforcement
- Security Simulation & Awareness Training
- Backup and Recovery
- Incident Response Plan
- Crown Jewels Analysis

HIGH LIKELIHOOD

Insider Threat

A current or former employee or partner abuses access to sensitive information, leading to data theft, sabotage, or system disruption for personal or malicious reasons.

Top Mitigating Controls

- User Monitoring
- Access Reviews
- Background Checks
- Security Simulation & Awareness Training
- Privileged Access Management

HIGH LIKELIHOOD

Network Vulnerabilities

Flaws in network configurations or protocols, which can be exploited to gain unauthorized access or cause data breaches, increasing security risks for the organization.

Top Mitigating Controls

- Next-Gen Firewall
- Vulnerability Management
- Network Segmentation
- Patch/Device Management

Risk Scorecard

MEDIUM LIKELIHOOD

Privileged Misuse

Unauthorized or inappropriate use of elevated access can lead to data breaches, service disruption, and reputational damage, whether through intentional or negligent actions.

Top Mitigating Controls

- Role Based Access Control
- Privileged Access Management
- User Monitoring
- Access Audits

MEDIUM LIKELIHOOD

Ransomware

Malicious software encrypts files or locks systems until a ransom is paid, causing operational disruption, data loss, or financial harm due to downtime or payment demands.

Top Mitigating Controls

- Backup and Recovery
- Intrusion Detection/Prevention System
- Endpoint Protection
- Security Simulation & Awareness Training
- Cyber Insurance Policy with Ransomware Coverage

MEDIUM LIKELIHOOD

Security Culture

A lack of awareness or commitment to security policies among staff can lead to weak defenses, increased vulnerabilities, and higher risks of breaches or data loss.

Top Mitigating Controls

- Data Loss Prevention
- Encryption
- Conditional Access
- Cybersecurity Policies

MEDIUM LIKELIHOOD

Social Engineering (Pishing)

Attackers manipulate individuals into divulging sensitive information or granting access, using tactics like phishing or impersonation, leading to potential security breaches.

Top Mitigating Controls

- DDoS Protection
- Next-Gen Firewall
- Load Balancing
- Security Operations Center
- Cyber Insurance Policy with Ransomware Coverage

LOW LIKELIHOOD

System Intrusion

Unauthorized access to systems by attackers seeking to steal, corrupt, or misuse data, potentially causing financial and operational damage due to security failures.

Top Mitigating Controls

- Intrusion Detection/Prevention System
- Endpoint Protection
- Security Operations Center
- Conditional Access
- Access Control
- Next-Gen Firewall
- Cyber Insurance Policy with Ransomware Coverage

LOW LIKELIHOOD

Third-Party Risk

Risks posed by external vendors or partners due to inadequate security measures or vulnerabilities, leading to potential breaches or system compromises.

Top Mitigating Controls

- Crown Jewels Analysis
- Vendor Risk Management
- Due Diligence
- Incident Response Plan
- Continuous Monitoring
- IT Asset Inventory

LOWEST LIKELIHOOD

Unpatched Software

Software vulnerabilities left unpatched expose systems to potential exploits, increasing the risk of breaches, data theft, or operational disruptions.

Top Mitigating Controls

- Patch/Device Management
- Vulnerability Management
- IT Asset Inventory
- Endpoint Protection
- Crown Jewels Analysis


enveedo