SECUREYES
Infusing Security

Cybersecurity Posture

Evaluation Checklist 

Cybersecurity posture is not a single, monolithic value. It's a complex and multi-faceted concept that encompasses various aspects of an organization's security practices and readiness.

Use this checklist to align your cybersecurity strategy with business goals, emerging threats, and technological advancements; building resilience against an increasingly sophisticated threat landscape.

Benchmark and Evolve
Your CyberSecurity Posture.

Start Now

hello@secureyes.net www.secureyes.net

Cybersecurity Posture

Evaluation Checklist ☑

1. STRENGTHEN AI-DRIVEN THREAT DETECTION

- [ ] Ensure your security tools leverage AI and machine learning to detect anomalies and emerging threats faster.
- [ ] If not, implement AI-based threat detection systems capable of identifying patterns and anomalies in real-time.
- [ ] Use behavioral analytics to detect deviations in user behavior that may indicate insider threats or compromised credentials.
- [ ] Evaluate & Partner with vendors providing AI and machine learning-driven threat intelligence platforms to stay ahead of emerging attack vectors.

2. PREPARE FOR QUANTUM COMPUTING

- [ ] Conduct an audit of existing cryptographic systems to assess vulnerabilities to quantum decryption.
- [ ] Begin transitioning to post-quantum cryptography standards as recommended by NIST and other regulatory bodies.
- [ ] Monitor advancements in quantum computing through industry reports to stay informed about timelines and risks.

3. ADOPT A ZERO TRUST SECURITY MODEL

- [ ] Implement identity-based access controls, ensuring users, devices, and applications are verified every time they request access.
- [ ] Segment the network into micro-perimeters to limit lateral movement during a breach and to minimize the blast radius of potential breaches.
- [ ] Use multi-factor authentication (MFA) and strict role-based access controls (RBAC) to fortify access protocols.

Cybersecurity Posture

Evaluation Checklist ☑

4. ADDRESS SUPPLY CHAIN AND THIRD-PARTY RISKS

- [ ] Map & maintain a detailed inventory of all third-party vendors, including subcontractors, and categorize them based on risk levels using standardized frameworks.
- [ ] Use automated platforms like SE-TPTRAC to continuously monitor vendor compliance with security policies and standards.
- [ ] Conduct annual security audits for critical suppliers and include cybersecurity clauses in contracts.

5. SECURE IOT AND OPERATIONAL TECHNOLOGY (OT)

- [ ] Map all IoT and OT devices across your network to identify potential weak points.
- [ ] Apply network segmentation to isolate IoT devices from critical infrastructure.
- [ ] Apply endpoint protection and regular patching to mitigate vulnerabilities in connected devices.
- [ ] Regularly update device firmware and enable encrypted communication channels.

6. ENHANCE EMPLOYEE AWARENESS AND TRAINING

- [ ] Roll out customized & gamified cybersecurity training programs for all employees, focusing on phishing, social engineering, and insider threats to increase engagement and retention.
- [ ] Test employee vigilance using simulated phishing attacks and social engineering exercises.
- [ ] Train staff on new threats, including deepfake phishing and voice synthesis scams.

Cybersecurity Posture

Evaluation Checklist ☑

7. INTEGRATE THREAT SIMULATIONS

- [ ] Regularly run tabletop exercises and red-teaming scenarios to assess your readiness for high-impact cyber events.
- [ ] Test organizational response to ransomware and phishing attacks.

8. COMPLIANCE WITH EVOLVING DATA PRIVACY REGULATIONS

- [ ] Conduct a regulatory readiness assessment for frameworks such as GDPR, CCPA, and India's DPDP Act.
- [ ] Implement data discovery and classification tools to understand where sensitive data resides and how it's processed.
- [ ] Invest in tools to streamline compliance reporting and manage data access permissions with centralized dashboards and automated tracking.

9. BUILD A COMPREHENSIVE INCIDENT RESPONSE PLAN

- [ ] Develop scenario-based response playbooks tailored to ransomware, DDoS, insider threats, and nation-state attacks.
  Establish clear roles and responsibilities for incident response teams to ensure swift and effective actions.
- [ ] Maintain a cyber insurance policy that covers new-age threats like supply chain attacks.
- [ ] Partner with a managed cybersecurity service provider for 24/7 monitoring and rapid threat containment.

Cybersecurity Posture

Evaluation Checklist ☑

10. FORTIFY CLOUD AND HYBRID ENVIRONMENTS

- [ ] Deploy cloud-native security solutions that provide visibility and control over multi-cloud environments.
- [ ] Use cloud-native security tools to monitor and protect assets hosted across AWS, Azure, or Google Cloud.
- [ ] Implement encryption for data at rest and in transit to safeguard sensitive cloud-stored information.
- [ ] Enforce strict adherence to shared responsibility models for cloud security.

11. STRENGTHEN ENDPOINT SECURITY

- [ ] Deploy Endpoint Detection and Response (EDR) solutions to detect and mitigate endpoint threats proactively & in real time.
- [ ] Regularly update security patches and establish automated updates across devices.
- [ ] Monitor and restrict access for remote workers, emphasizing VPN usage and secure configurations.
- [ ] Establish strict BYOD (Bring Your Own Device) policies to minimize risks from employee devices.

12. ESTABLISH PROACTIVE MONITORING FOR ADVANCED PERSISTENT THREATS (APTS)

- [ ] Collaborate with threat intelligence vendors to stay updated on sector-specific APTs targeting your industry.
- [ ] Conduct red-teaming exercises to simulate attacks by nation-state actors and evaluate response efficiency.
- [ ] Ensure that all critical systems are equipped with deception technologies to mislead attackers.

Cybersecurity Posture

Evaluation Checklist ☑

13. SECURE DEVOPS PIPELINES

- [ ] Shift left on security by embedding security scans into CI/CD pipelines.
- [ ] Use tools like Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) to find and fix vulnerabilities during the development process.
- [ ] Conduct secure code reviews to ensure applications are resilient to attacks.

14. EXPAND METRICS FOR CYBER RISK MANAGEMENT

- [ ] Track advanced KPIs like Percentage of Patching Compliance, Time to Contain (TTC), and Impact per Incident.
- [ ] Use dashboards to automate reporting to track progress and communicate value to stakeholders & to provide real-time visibility into security posture and generate insights for decision-making.
- [ ] Quantify risks in monetary terms to articulate the importance of cybersecurity to non-technical stakeholders.

15. CYBERSECURITY IN MERGERS & ACQUISITIONS (IF ANY)

- [ ] Conduct cybersecurity due diligence to uncover vulnerabilities in acquired entities.
- [ ] Include post-acquisition integration plans for aligning security postures.

16. PHYSICAL SECURITY INTEGRATION

- [ ] Monitor for convergence between physical and digital threats, such as IoT-enabled surveillance systems being exploited as entry points.
- [ ] Train physical security teams to collaborate with cybersecurity units during incidents.

Cybersecurity Posture

Evaluation Checklist ☑

17. ADDRESSING SHADOW IT

- [ ] Identify and secure unauthorized devices and software being used by employees.
- [ ] Implement policies and tools to monitor and manage shadow IT activities.

18. LEGACY SYSTEM RISK MITIGATION

- [ ] Audit legacy systems for outdated protocols and vulnerabilities.
- [ ] Prioritize upgrades or isolation strategies for end-of-life infrastructure that cannot be replaced immediately.

19. INTEGRATING CYBERSECURITY INTO ESG INITIATIVES (ENVIRONMENTAL, SOCIAL, AND GOVERNANCE)

- [ ] Include cybersecurity metrics in ESG reporting to demonstrate organizational resilience.
- [ ] Collaborate with stakeholders to build trust by showcasing transparent security practices.

20. FOSTER BOARDROOM-LEVEL CYBER RISK DISCUSSIONS

- [ ] Regularly brief the board on your organization's cyber risk posture, key metrics, and major threats.
- [ ] Secure dedicated budgets for cybersecurity initiatives aligned with business objectives.

Cybersecurity Posture

Evaluation Checklist ✅

Thank you for completing the SecurEyes' Cybersecurity 2025 Checklist!

Your Score: [*Count the boxes you have checked*] = [ ]

The above result indicates your organization's current cybersecurity readiness.

What Your Score Means:

Below 30:

Your organization is in dire need of cybersecurity enhancement.

The current state of your security infrastructure exposes you to significant risks, including advanced threats, compliance violations, and data breaches.

Action Needed: Immediate expert consultation and strategic intervention are required to uplift your cybersecurity posture.

Cybersecurity Posture

Evaluation Checklist ✅

What Your Score Means:

30 to 40:

Your organization has achieved stability, but there is room for improvement.

While you may have addressed fundamental security measures, readiness for advanced and emerging threats remains a concern.

Action Needed: Strengthen existing frameworks and prepare for sophisticated threat vectors to ensure future resilience.

Above 40:

Your organization has demonstrated commendable efforts toward cybersecurity. You have a robust foundation and appear well-prepared to tackle upcoming challenges in 2025.

Action Needed: Continue fine-tuning strategies and adopting emerging technologies to stay ahead.

SECUREYES
Infusing Security

YOUR TRUSTED PARTNER FOR COMPREHENSIVE AI-POWERED CYBERSECURITY SOLUTIONS

Consulting & Advisory | Cybersecurity Products | Corporate Training & Upskilling

Are you ready to evolve your organization's cybersecurity posture?

Let's connect for a 30-minute discussion?

We'd like to explore how SecurEyes can support your journey toward a more secure digital future.

www.secureyes.net

hello@secureyes.net

IND +91 9939217654
IND +91 8041264078
UAE +971 50 8950797
USA +1 361 423 1683