2025 - Top 10 Cybersecurity Threats

Executive Version

Protecting your organization from emerging cyber threats is essential to safeguarding revenue, reputation, and customer trust.

This executive overview spotlights the most critical threats on our radar and the strategic actions required to reduce risk and ensure resilience.

EVA TECHNOLOGIES®

ENTERPRISE
VULNERABILITY
ASSESSMENT &
AVOIDANCE TECHNOLOGY

Key Threats & Business Impact

Top threats taken from the current TOP 10 which can be consulted in the full document: EVA_2025-Top10_CybersecurityThreats_vDetailled

1

Advanced AI-Powered Phishing and Social Engineering

Business Impact: High risk of data breaches, financial fraud, and reputational harm through convincing, AI-driven impersonations and manipulative tactics.

2

Unresolved Vulnerabilities and Obsolete Systems

Business Impact: Increased exposure to breaches and operational failures due to unpatched systems; can lead to significant downtime, legal liabilities, and costly recovery efforts.

3

AI and Machine Learning Integration

Business Impact: Unmonitored and misuse of AI tools can expose sensitive data or undermine critical processes and introduce unreliable decision-making as AI can produce misleading outcomes through hallucinations and other inaccuracies.
AI can be tricked into producing false results which remain a risk for enterprises.

4

Resiliency and Backup Solutions

Business Impact: Insufficiently tested or compromised backup systems can prolong downtime, escalate costs and force ransom payments, undermining business continuity and elevating financial risks.

5

Internal Threats and Inadequate Asset Management

Business Impact: Insider abuse (intentional or accidental) and improper assets inventory can open security gaps, leading to unauthorized data access, compliance failures, disrupt business operation and reputational harm.

Solution Ideas

Below are key approaches to address the identified threats and strengthen overall cybersecurity. Only a tailored roadmap can produce optimal results, consider consulting with our specialists.

1 Employee Training & Awareness

Educate all levels of staff on phishing recognition, secure data handling, and reporting mechanisms.

2 Multi-Factor Authentication Everywhere

Secure access points with MFA, particularly for critical systems and privileged accounts.

3 Continuous Monitoring

Actively monitoring security bulletins to ensure timely updates and robust security controls.

4 Asset Management

Maintain an accurate inventory of all devices and applications to ensure timely updates and consistent security controls.

5 Critical Patching & System Updates

Regularly update software and replace outdated systems to reduce exposure to vulnerabilities.

6 AI Governance & Secure Integration

Implement robust AI policies and monitoring protocols to protect AI-driven processes.

7 Vendor & Third-Party Risk Management

Strengthen contract requirements, security screenings, and oversight of external service providers.

8 Network Segmentation & Access Control

Isolate critical systems, apply strict access policies, and monitor for abnormal activity to contain breaches.

9 Enhanced Backup & Recovery Validation

Test restoration processes, store backups in secure, isolated environments, and ensure both are vetted by a security expert for quick and reliable recovery.

10 Sustained Security Culture

Encourage leadership sponsorship, frequent awareness campaigns, and ongoing evaluations to foster continuous improvement.

For details on these and other advantageous solutions, please see the full document.

Risks of Inaction

Data Breaches

Unauthorized access to sensitive information can lead to severe financial and reputational damage.

Operational Disruptions

Downtime impacts productivity and can halt critical services, affecting overall business operations.

Data Extortion

Threat actors may demand payments in exchange for stolen or withheld data, leading to financial and operational strain.

Financial Losses

Includes direct costs from theft, fraud, or ransom payments, as well as indirect costs like legal fees, lost clients and increased insurance premiums.

Reputational Damage

Loss of customer trust and negative media coverage can hinder long-term success and market position.

Infrastructure Vulnerabilities

Obsolete systems and inadequate security controls create more entry points for attackers, increasing the risk of successful breaches.

Regulatory Non-Compliance

Breaches can lead to fines and legal actions under laws like GDPR, HIPAA, and PIPEDA, impacting both financial and legal standing.

Business Partnerships

Relationships with business partners and stakeholders can suffer, potentially leading to loss of partnerships and trust.

For details on these risks and more, please see the full document: EVA_2025-Top10_CybersecurityThreats_vDetailled

Call to Action & Next Steps

1

Establish Executive Buy-in

Secure commitment from leadership to prioritize cybersecurity initiatives across the organization.

2

Increase Cybersecurity Budget

Allocate additional resources to implement advanced security concepts, technologies and acquire skilled assistance.

3

Develop a Comprehensive Security Roadmap

Create a detailed plan outlining security improvements over the next 12-24 months, strive for continuous measurable improvement

4

Implement Regular Security Assessments

Conduct periodic security evaluations and penetration tests to maintain alignment of your security roadmap.

Your business objectives are at the core of our approach.
At EVA Technologies, we optimize CyberSecurity to empower your success using a refined tailored approach.

Looking to improve your cybersecurity, we're here to help!

Get moving towards improved maturity in the security of your enterprise with one easy step, talk with an expert. Reach out to us at **info@eva-technologies.com**.

For more information on our cybersecurity solutions, visit **https://eva-technologies.com**