FACING REALITY

CYBERSECURITY IN 2025

NAVIGATING EMERGING THREATS, GEOPOLITICAL RISKS, AND INDUSTRY CHALLENGES

THE IMPACT OF EMERGING TECHNOLOGIES

The Impact of AI & ML on Risk Management

New technologies like AI and ML are reshaping industries, with 66% of organizations expecting AI to boost threat detection.

(CrowdStrike, 2024; Gartner, 2024).

AI: A DOUBLE-EDGED SWORD

- AI is hailed as the future of cybersecurity, with 66% of organizations expecting it to enhance threat detection in 2025.
- Leaders must ensure AI tools are securely deployed. Only 37% of organizations have processes in place to assess AI security.

(CrowdStrike, 2024)

NAVIGATING INTERNATIONAL RISKS

Geopolitical Tensions

U.S.-China tensions are escalating cybersecurity challenges, with Trump’s stance against Chinese cyber activities highlighting urgency.

Expanding Threats

Cybercriminals and state-sponsored hackers are using advanced tactics to exploit cloud and supply chain vulnerabilities, escalating the risk.

Regulatory Challenges

Organizations struggle to comply with evolving cybersecurity regulations, exacerbating risks as businesses try to balance security with compliance.

(CrowdStrike, 2024; Gartner, 2024; Treene & Liptak, 2025; Newman & Greenberg, 2025; Collier, 2025); World Economic Forum, 2025.

THE SUPPLY CHAIN VULNERABILITY

The Expanding Scope of Cyber Risks

Cyber risks extend beyond organizations to vendors, suppliers, and partners. Supply chain complexity increases vulnerabilities, weakening operational security.

Key Barriers to Cyber Resilience

54% of organizations cite supply chain interdependencies as the greatest barrier to cyber resilience, stressing the need for better protection.

(CrowdStrike, 2024; Gartner, 2024)

WORKFORCE SHORTAGE

Skills Gap

Two-thirds of organizations face a critical shortage of cybersecurity professionals, leaving them vulnerable to sophisticated attacks.

Building a Workforce

Invest in employee upskilling, partner with educational institutions, and cultivate a strong cybersecurity culture.

(World Economic Forum, 2025)

FROM PROTECTION TO PROACTIVE RESILIENCE

Rising Risk

As technology adoption grows, so do the risks and challenges businesses face.

New Focus

Shifting from protection to resilience is key for ensuring long-term business continuity.

Proactive Approach

Security has evolved from basic protection to a critical element of business continuity. As cyber risks increase, resilient security measures ensure operational success and protect against ever-evolving threats in dynamic digital and geopolitical environments.

(World Economic Forum, 2025; Gartner, 2024)

Securing the Path Forward

Cybersecurity in 2025 requires businesses to address evolving risks and integrate resilience. Proactive strategies and continuous adaptation will ensure stability and success in the face of rising global threats.

REFERENCES

Collier, K. (2025, January 18). China's hackers have run wild during the Biden administration. Can Trump rein them in? NBC News. https://www.nbcnews.com/tech/security/trump-faces-unprecedented-cyber-challenges-chinese-hackers-rcna186423

CrowdStrike. (2024). CrowdStrike 2024 Global Threat Report. CrowdStrike, Inc. https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

Gartner. (2024, January). Top 9 trends in cybersecurity for 2024: Optimizing for resilience and performance. Gartner, Inc. https://emt.gartnerweb.com/ngw/globalassets/en/cybersecurity/documents/top-trends-in-cybersecurity-for-2024.pdf

Newman, L. H., & Greenberg, A. (2025, January 18). Security news this week: US names one of the hackers allegedly behind massive Salt Typhoon breaches. Wired. https://www.wired.com/story/us-names-one-of-the-hackers-allegedly-behind-massive-salt-typhoon-breaches/

World Economic Forum. (2025, January 13). Global Cybersecurity Outlook 2025 – Navigating through rising cyber complexities. World Economic Forum. https://www.weforum.org/press/2025/01/global-cybersecurity-outlook-2025-navigating-through-rising-cyber-complexities/