Strategic Risk Insights is provided as a courtesy by the Strategic Consulting Group (SCG) and is intended to offer insights into relevant risks, threats, and vulnerabilities. The information contained in this document is provided "as is" and does not establish or imply any business relationship with SCG. Due to the evolving nature of risk, the value of this information may diminish after the publication date. SCG makes no guarantees regarding the accuracy, completeness, or timeliness of the content and cannot be held liable for any errors, omissions, or misinterpretations.

Strategic Risk Insights is designed to provide a high-level overview of emerging risks, threats, and vulnerabilities relevant to your organization. It should be used as an early awareness tool to inform strategic discussions, enhance risk management efforts, and support decision-making. While this report highlights key concerns, it is not a substitute for a comprehensive risk assessment. Organizations should conduct their own due diligence, validate findings against internal data, and consult subject matter experts as needed to develop appropriate mitigation strategies.

SUMMARY

As of January 2025, approximately 965 million devices still use the Windows 10 Operating System

As of **October 14, 2025**, Microsoft will officially end support for Windows 10, ceasing the provision of free software updates, security patches, and technical assistance. Organizations that continue to use Windows 10 beyond this date will face significant security, compliance, and operational risks due to the absence of critical security updates and vendor support.

To mitigate these risks, organizations should prioritize a transition to Windows 11 or another supported operating system. While Microsoft offers Extended Security Updates (ESU) for purchase starting in late 2024, these updates only provide temporary relief and should not be considered a long-term solution. Proactively upgrading to a supported OS is essential to maintaining security, regulatory compliance, and operational efficiency.

Prioritized InfoSec and Cybersecurity Threats, Risks, and Vulnerabilities

1. **Unpatched Vulnerabilities:** Any new security vulnerabilities discovered after October 14, 2025, will remain unpatched, making Windows 10 systems increasingly vulnerable to exploits, zero-day attacks, and unauthorized access.
2. **Increased Malware Threats:** Unsupported operating systems are prime targets for malware developers. Without security updates, the risk of ransomware infections, data breaches, and malware propagation rises significantly.
3. **Compliance and Legal Risks:** Many regulatory frameworks (e.g., GDPR, HIPAA, NIST, PCI DSS) require organizations to maintain up to date, supported software. Using an unsupported OS could result in compliance violations, leading to audits, fines, and reputational damage.
4. **Lack of Technical Support:** Microsoft will no longer provide technical assistance, leaving organizations without access to vendor support for troubleshooting, bug fixes, or security-related issues.
5. **Compatibility Challenges:** Over time, third-party applications, security tools, and enterprise software will stop supporting Windows 10, creating compatibility issues that could disrupt business operations and limit future software deployment options.

RISK LEVEL TIMELINE SUMMARY

The risk level rating in this report is presented using the **SCG Codified Risk Ranking** and **SCG Codified Risk Language**, ensuring a standardized and consistent approach risk language across the organization's enterprise to assessing threats, vulnerabilities, and potential impacts.

RISK LEVEL TIMELINE DETAILS

Risk Rating Before October 14, 2025:

Attack Vector	Level	Date
Early-stage compatibility issues, misconfigurations, social engineering (phishing), IT workload strain, operational inefficiencies.	**4: Moderate**	Before Oct 14, 2025

While Windows 10 remains supported, there is no immediate security risk. However, organizations may face early operational challenges in preparing for migration.

Key Risks:

- **Compatibility Concerns:** Some applications and enterprise environments may start optimizing for Windows 11, leading to early-stage compatibility issues.
- **Security Gaps in Long-Term Planning:** Organizations delaying upgrade decisions may face bottlenecks when the end-of-support date approaches.
- **Increased IT Workload:** IT teams will need to allocate time and resources for a well-planned transition, which could disrupt other priorities if left too late.

Risk Rating After November 14, 2025 (One Month Post-End-of-Life):

Attack Vector	Level	Date
Exploitation of unpatched vulnerabilities, ransomware, malware, phishing, regulatory non-compliance, vendor abandonment, expanded attack surface.	**6: Strong**	After Nov 14, 2025

The risk escalates significantly after Microsoft ceases security updates and technical support.

Key Risks:

- **Unpatched Vulnerabilities:** Any new security flaws discovered will remain unaddressed, exposing organizations to cyberattacks, including zero-day exploits.
- **Compliance & Regulatory Risk:** Companies bound by data protection regulations (e.g., GDPR, HIPAA) may be in violation if they continue running unsupported software, potentially leading to legal penalties.
- **Increased Attack Surface:** Unsupported operating systems are prime targets for attackers, increasing the likelihood of ransomware, phishing attacks, and malware infections.
- **Lack of Vendor Support:** Third-party software providers may stop supporting Windows 10, leading to operational inefficiencies and unexpected service disruptions.

Risk Rating (April 14, 2026 - Six Months Post-End-of-Life)

Attack Vector	Level	Date
Weaponized zero-day exploits, targeted ransomware, severe compliance breaches, system instability, increased IT costs, business continuity risks.	**7: Very Strong**	After April 14, 2026

By six months after end-of-life, the risk associated with running Windows 10 has escalated significantly. At this point, organizations that have not upgraded are facing increasing security, operational, and compliance challenges.

Key Risks:

- **Highly Exploitable Vulnerabilities:** With six months of unpatched security flaws, attackers have had time to develop exploits targeting Windows 10 systems. Exploits will be actively traded and weaponized in cybercriminal networks.
- **Growing Compliance Violations:** Regulatory bodies and industry standards (e.g., PCI DSS, HIPAA, NIST) will consider unsupported operating systems as security non-compliant, increasing the likelihood of fines, audits, and legal repercussions.
- **Ransomware and Malware Surge:** Threat actors will focus on Windows 10 vulnerabilities that remain unpatched, increasing the risk of malware infections, ransomware incidents, and data breaches.
- **Software Incompatibility and System Failures:** Vendors will begin phasing out support for Windows 10, leading to software updates and security patches that no longer function properly, causing operational disruptions.
- **Escalating IT Burden:** Organizations still using Windows 10 will require additional resources to mitigate security gaps, manually patch vulnerabilities, and implement workarounds, diverting critical resources from other IT and security initiatives.

Strategic Consulting Group Codified Risk Ranking Model

The SCG Codified Risk Ranking Model is a proprietary framework developed by Strategic Consulting Group (SCG) to provide a standardized approach to risk assessment and classification. SCG retains all intellectual property rights to this model, and any use of it requires proper attribution to SCG. Creating derivative works or modifications does not transfer ownership of the original model or its components.

Level	Name	Description
1	**Negligible**	Insignificant or no noticeable impact.
2	**Very Low**	Minor inconvenience with limited effect.
3	**Low**	Slight impact, typically manageable without significant resource allocation.
4	**Moderate**	Noticeable impact requiring moderate effort to address.
5	**Considerable**	Widespread impact with measurable disruption.
6	**Strong**	Significant impact requiring dedicated resources and attention.
7	**Very Strong**	High impact, affecting a considerable portion of stakeholders.
8	**Severe**	Extensive disruption, likely requiring organizational reprioritization.
9	**Destructive**	Major impact, with long-term consequences for core operations.
10	**Very Destructive**	Critical disruptions, threatening organizational stability.
11	**Devastating**	Near-catastrophic effects, with substantial and enduring impacts.
12	**Catastrophic**	Irreversible consequences with widespread societal or organizational failure.

ABOUT THE STRATEGIC CONSULTING GROUP

The Strategic Consulting Group (SCG) helps clients make better decisions in a fast-evolving environment. We specialize in Operational Excellence, Risk Management, Training, and Strategic Planning. With our expertise, clients can effectively navigate challenges such as misinformation, operational risks, competition, regulatory compliance, privacy, and information security, ensuring they remain adaptable and resilient. Our evidence-based approach empowers organizations to tackle complex issues and achieve sustainable success while staying ahead of industry trends, shifting client needs, and changing regulations.

Our clients make better decisions: wwwyscg.ca