CYBERRESILIENCE
DIGITAL RESILIENCE FOR SMES

SME Cyber Resilience

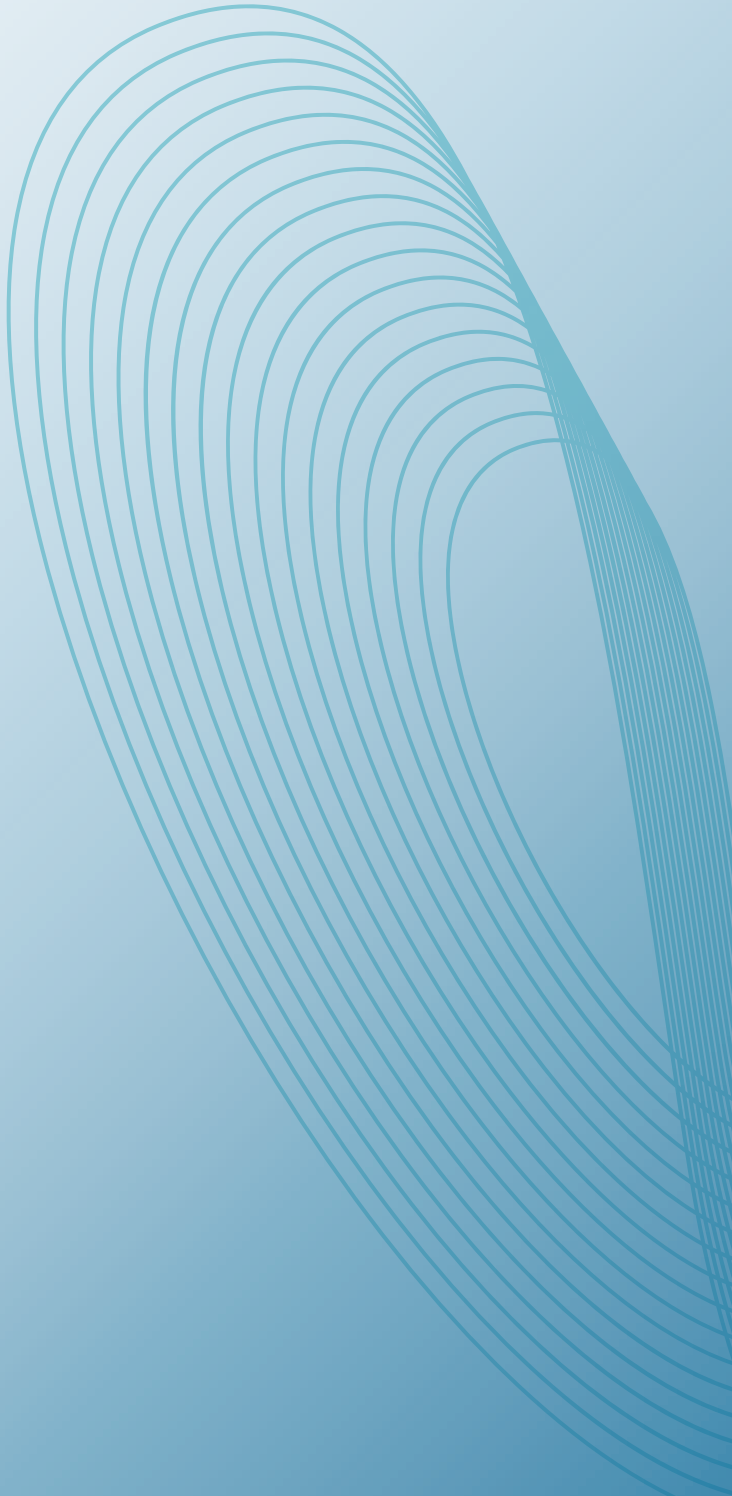
State of the Sector

2025

NATIONAL CHALLENGE FUND
From Ingenuity to Research and Solutions
Rialtas na hÉireann
Government of Ireland
Taighde Éireann
Research Ireland
Maoinithe ag an Aontas Eorpach
Funded by the European Union

This report was published by Munster Technological University (MTU) 'Digital Resilience for SMEs' Research Team in collaboration with the National Cyber Security Centre (NCSC). It was funded under the National Challenge Fund, established as part of the National Recovery and Resilience Plan (NRRP), and supported by the EU Recovery and Resilience Facility through Taighde Éireann.

Funding was provided by Research Ireland Digital for Resilience Challenge Grant Number 22/NCF/DR/11210G



Executive Summary

Ireland's small and medium enterprises (SMEs) face a critical cyber resilience gap. SMEs account for 99.8% of all enterprises in Ireland and employ over 2.29 million people, representing 67.9% of total employment (based on the latest CSO 2022 figures). This cyber resilience assessment reveals that the majority of SMEs remain underprepared for modern cyber threats.

Drawing on data from 894 enterprises across 11 sectors, this assessment reveals the current state of cyber resilience across Irish SMEs.

1. Cyber Resilience Levels Are Critically Low

- 78% of SMEs fall into the 'Low' or 'Very Low' Cyber Resilience Category.
- Only 6% achieve a 'High' or 'Very High' score.
- Micro Businesses are the most at risk (81% deemed 'Low' & 'Very Low' compared to 45% of Medium Businesses in the same categories).

This suggests that the most prevalent business types (Small and Micro) are also the least equipped to withstand or recover from a cyber incident.

2. Sector-by-Sector Resilience Reveals Unexpected Findings

Across 11 sectors analysed, no industry achieves a Cyber Resilience score of 6/10 or higher, suggesting widespread vulnerabilities.

Notable insights include:

- The Information, Communications and Technology (ICT) sector ranks highest at 5.7 out of 10, yet this is not considered a 'strong' threshold.
- Healthcare ranks the lowest at 3.3 out of 10, despite being one of the most regulated and targeted sectors.

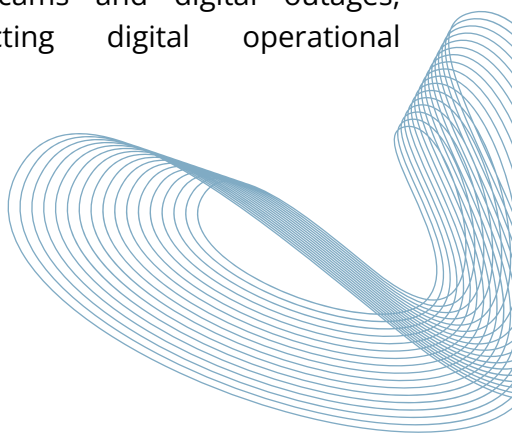
Notably, sectors handling highly sensitive data do not perform noticeably better than less regulated sectors in this study.

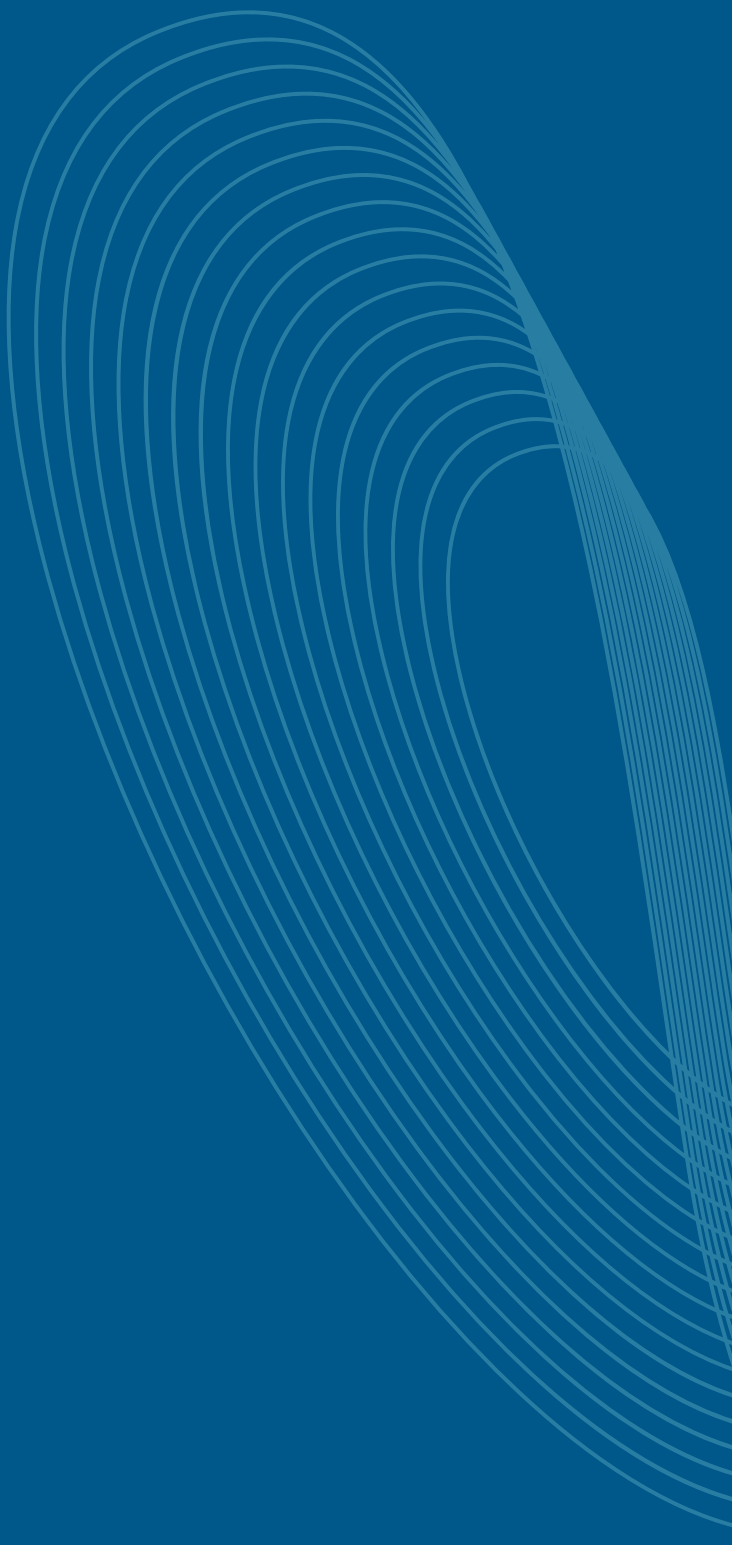
3. Critical Weaknesses Are Consistent Across SMEs

The most common areas of deficiency identified include:

- Data Backups
- Multi-Factor Authentication
- Incident Response Planning
- Cybersecurity Training
- VPN Usage
- Business Continuity Planning

These gaps significantly increase both the likelihood and the impact of cyber incidents, cyber-enabled scams and digital outages, seriously affecting digital operational resilience.





Introduction

Ireland's small and medium-sized enterprises (SMEs) form the backbone of the national economy, representing 99.8% of all enterprises and contributing over €53 billion in gross value added annually. SMEs are classified by employee size: Micro (1-9 employees), Small (10-49 employees), and Medium (50-249 employees). The most recent CSO data from 2022 shows SMEs employed 2.29 million people, representing 67.9% of total employment in Ireland.

Despite the importance of SMEs to the Irish economy, most Irish SMEs lack sufficient cyber resilience, leaving them exposed to cyber threats that could compromise individual businesses and disrupt entire supply chains and sectors.

When an SME experiences a cyber incident, the consequences often extend well beyond the business itself. Supply chain partners may also lose access to vital services, and customer data could be compromised. In the worst-case scenarios, the business might be forced to shut down entirely.

With 78% of Irish SMEs falling into the 'Low' or 'Very Low' categories of cyber resilience, the vast majority of small businesses remain poorly prepared to withstand or recover from a cyber incident.

A Comprehensive National Cyber Resilience Assessment

This report presents the findings of a comprehensive cyber resilience assessment of Irish SMEs, based on data collected from 894 enterprises across 11 sectors. Using the Cyber Fundamentals Framework, resilience was assessed across six essential functions: *Govern, Identify, Protect, Detect, Respond, and Recover.*

About The Cyber Fundamentals Framework

The CyberFundamentals (CyFun) framework is a recognised, structured, voluntary tool to help entities align with cybersecurity best practices and is based on the NIST Cybersecurity Framework v2.0.

1. **Govern:** Determine how cybersecurity risk management strategy, risk appetite, and policy are established, communicated, and monitored.

2. **Identify:** Understanding organisational risks, assets, and vulnerabilities.

3. **Protect**: Implementing controls to prevent cybersecurity incidents.

4. **Detect:** Developing capabilities to recognise and respond to threats.

5. **Respond:** Establishing incident response and mitigation procedures.

6. **Recover:** Ensuring business continuity and resilience following incidents.

Drawing on detailed resilience assessments across multiple sectors and business sizes, this report identifies the critical gaps in Irish SME cyber resilience and recommends specific interventions to address them.

Irish SME Cyber Resilience

The Cyber Resilience Level assesses how effectively an organisation can withstand, respond to, and recover from cyber-attacks or digital disruptions.

This assessment evaluated 894 Irish SMEs using the Cyber Fundamentals framework, assessing their security measures across 6 core functions. Each business then received a Cyber Resilience score from 0 to 10, reflecting the proportion of recommended security actions completed.

Based on their scores, the SMEs were classified into 5 resilience categories, from 'Very Low' (minimal security measures) to 'Very High', reflecting strong security implementation and the capacity to prevent, withstand, and recover from potential cyber-attacks.

SMEs with lower cyber resilience levels face greater business risks, including a higher likelihood of damaging cyberattacks, longer recovery periods, and increased financial risks.

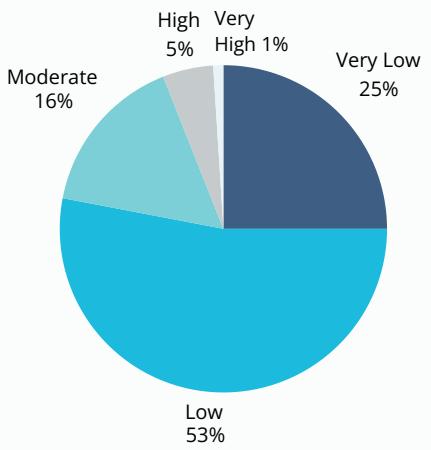
Cyber Resilience Levels

Survey findings show that 78% of SMEs fall into the 'Low' or 'Very Low' Cyber Resilience categories, indicating significant vulnerabilities across the sector. Only a small proportion demonstrate strong resilience, with 5% achieving a 'High' ranking and just 1% reaching a 'Very High' level.

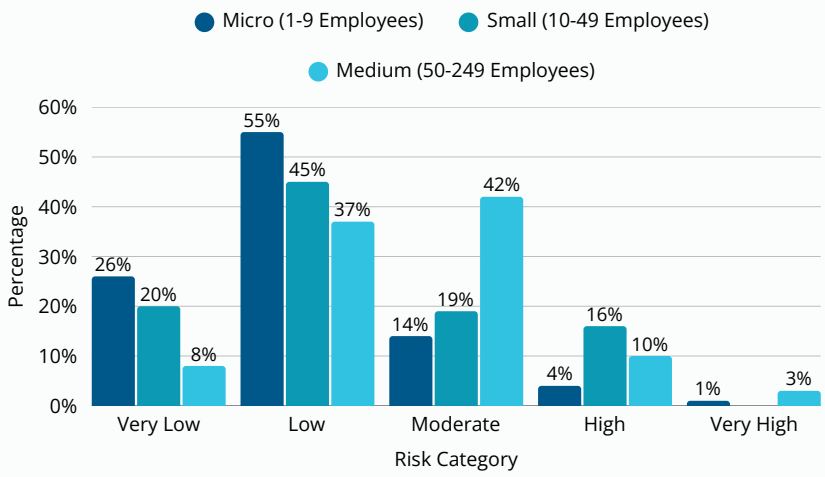
Cyber Resilience by SME Size

Analysis reveals that Micro SMEs exhibit significantly lower cyber resilience levels than Small and Medium SMEs. Specifically, 81% of Micro SMEs fall into the 'Low' or 'Very Low' Cyber Resilience categories, compared to 45% of Medium enterprises.

Cyber Resilience Levels



Cyber Resilience by SME Size



Top Cyber Resilience Weaknesses for Irish SMEs

Analysis identifies 10 key areas where Irish SMEs consistently underperform. These weaknesses greatly increase vulnerability to cyber incidents. Addressing even a few of these gaps can significantly improve an SME's resilience.

1. Data Backups

Only 26% have an automated data backup process in place.

2. Multi-Factor Authentication

Only 39% have multi-factor authentication on all business-critical applications.

3. Cyber Incident Response Plan

Just 22% have a Cyber Incident Response Plan or a tested plan.

4. Cybersecurity Training

Only 26 percent have trained in the last year. 40% have never trained.

5. Continuity Planning

Only 35% have a Business Continuity plan in place.

6. Password Policy

Only 38% enforce minimum password length requirements.

7. Cybersecurity Policy

Just 12% have a documented cybersecurity policy.

8. Network Security

Only 30% have an individual assigned to manage network security.

9. Software Updates

Just 39% have automatic software updates enabled.

10. Secure Communications

Only 24% use a VPN (virtual private network) when working remotely.

SME Cyber Resilience by Sector Type

Analysis of SME cyber resilience by sector type reveals significant disparities in preparedness across different industry sectors within Ireland. This data highlights both the most and least resilient sectors concerning cyber risk management.

Crucially, no sector achieves an average score of 6 or higher out of 10, indicating a widespread opportunity for improved cyber resilience. The healthcare sector records the lowest average Cyber Resilience Score among Irish SMEs, at a concerning 3.3 out of 10. This statistic is of particular concern given that, according to the World Economic Forum in 2023, the healthcare industry has sustained the most expensive data breaches globally of any sector for thirteen consecutive years.

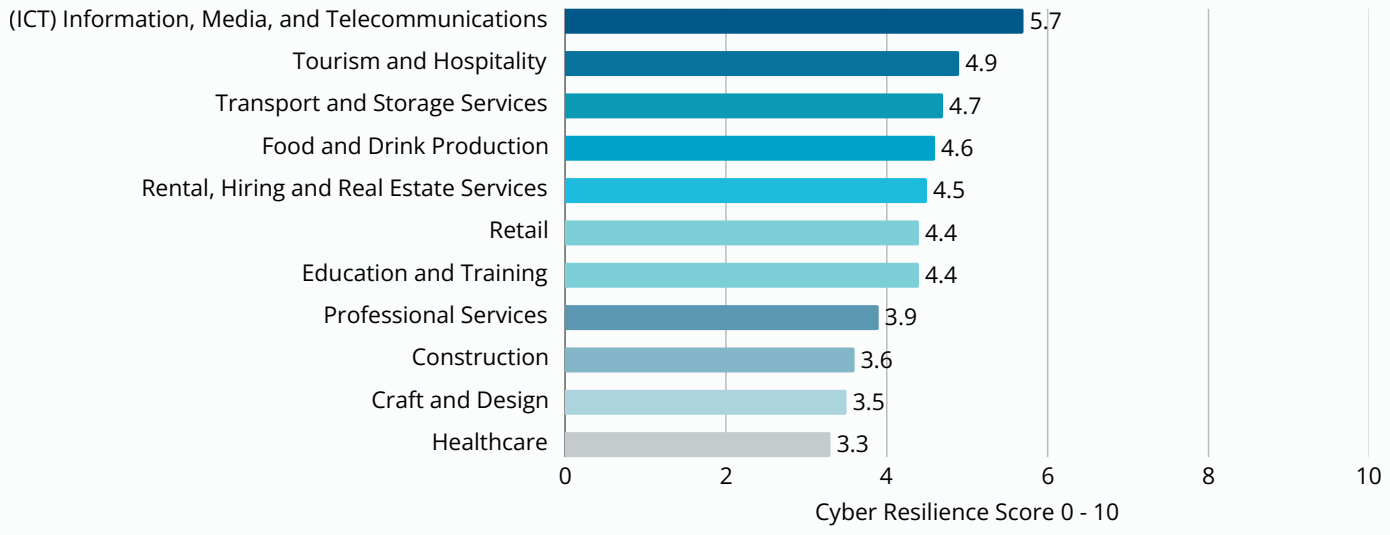
Conversely, the ICT sector demonstrates the highest cyber resilience among those surveyed, with an average score of 5.7 out of 10. While this is substantially higher than the next-best score of 4.9 out of 10 for Tourism and Hospitality, it still highlights significant room for improvement, especially given the industry's inherent digital risks and reliance on technology.

While the Information, Media and Telecommunications sector (ICT) leads the ranking, the overall spread between sectors is relatively narrow (2.4 points), indicating that heightened cyber resilience risk is a challenge shared broadly across Irish SMEs rather than concentrated within a few industry sectors.

Interestingly, sectors that routinely process larger volumes of sensitive personal or financial data, such as Healthcare and Professional Services, do not outperform less regulated industries. This highlights a potential gap between information security compliance requirements and real-world operational cyber resilience.

The graph below provides the average resilience score for each sector (scored out of 10):

Average Cyber Resilience Score by Sector



Alignment to the Cyber Fundamentals Framework

Govern

Determining how an organisation's cybersecurity risk management strategy, risk appetite, and policy are established, communicated, and monitored.

63% of businesses rely solely on the SME Owner for cybersecurity responsibility, often without dedicated expertise.

11% of SMEs lack clarity on who holds responsibility for the cybersecurity of their business.

67% of SMEs either never engage in training or participate only on an ad hoc basis.

86% operate without a tested Business Continuity Plan, leaving them vulnerable to prolonged disruptions.

Identify

Understanding organisational risks, assets, and vulnerabilities.

75% of SMEs lack an up-to-date hardware inventory, creating significant blind spots in the handling of business information across various devices.

74% fail to maintain an up-to-date inventory of software in use, increasing vulnerability to unpatched systems and unauthorised applications.

18% of SMEs are covered by cyber insurance, leaving the vast majority financially exposed to the cost of cyber incident management.

This widespread absence of comprehensive asset identification leaves many SMEs unable to effectively monitor, manage, or secure their digital landscape.

Protect

Implementing controls to prevent cybersecurity incidents.

74% of businesses have not implemented Multi-Factor Authentication (MFA) across all their business-critical applications.

69% of SMEs operate without automated backup solutions. Furthermore, even among those with a backup schedule, only 32% test their backups more than once a year, severely compromising recovery capabilities.

24% of remote workers use a Virtual Private Network (VPN) when accessing business applications, leaving 76% of the remote workforce potentially exposing company data to heightened risk outside secure networks.

27% of SMEs remain unaware of the cybersecurity benefits that a VPN provides, indicating a knowledge gap in remote work security.

Detect

Developing capabilities to recognise and respond to threats.

77% of businesses have antivirus software installed on their devices, yet only 51% ensure it is fully enabled across all workplace devices, highlighting a substantial gap in consistent protection.

27% of SMEs have no antivirus software deployed at all, leaving their entire infrastructure completely exposed to malware, ransomware, and other cyber threats.

63% of small and medium-sized enterprises (SMEs) do not enable automatic software updates, leaving their systems vulnerable to known, exploitable vulnerabilities.

67% of businesses lack a designated person or third party responsible for maintaining network security, indicating a critical absence of dedicated oversight for threat detection and prevention.

Respond

Establishing incident response and mitigation procedures.

67% of small and medium-sized Enterprises (SMEs) lack a formal Cyber Incident Response Plan, highlighting a crucial gap in their capacity to effectively manage and mitigate the impact of cyber incidents.

36% Of the SMEs that have implemented a Cyber Incident Response Plan, only 36% have ever tested it, significantly reducing the plan's practical usefulness.

67% of businesses also operate without a documented Cybersecurity Policy, resulting in fragmented security practices and unclear guidelines for personnel.

The widespread absence of planning means that employers and employees are often unprepared, leading to confusion or delayed action when faced with an incident.

Recover

Ensuring business continuity and resilience following incidents.

77% of organisations do not currently keep immutable data backups, a critical oversight given their importance in mitigating the impact of ransomware attacks.

58% of businesses lack website backups, leaving sales channels highly vulnerable to severe disruption in the event of a cyber incident.

17% of businesses protect their cloud data with a dedicated cloud backup service, meaning 83% are leaving vital information at risk of loss or compromise.

Collectively, these deficiencies highlight a widespread absence of robust recovery strategies, significantly prolonging potential downtime and financial losses following a cyber event.

The Way Forward...

Although the findings reveal significant gaps in the cyber resilience of Irish SMEs, every organisation that completed the assessment received tailored support through a customised action plan.

These plans highlight practical, prioritised steps that can meaningfully strengthen cyber resilience. A full version of the cyber resilience assessment and tailored recommendations will be available on the NCSC website in 2026.

Furthermore, with the NCSC's implementation of Cyber Fundamentals, organisations will gain access to a structured, three-tier model for risk-based cybersecurity analysis, supported by an optional certification pathway.

The Irish National Cyber Security Centre's co-ownership of the Cyber Fundamentals Framework, designed with a structured six-domain approach (Govern, Identify, Protect, Detect, Respond, and Recover), provides Irish SMEs with clear, actionable guidance aligned with internationally proven best practice.

Embedding Cyber Resilience

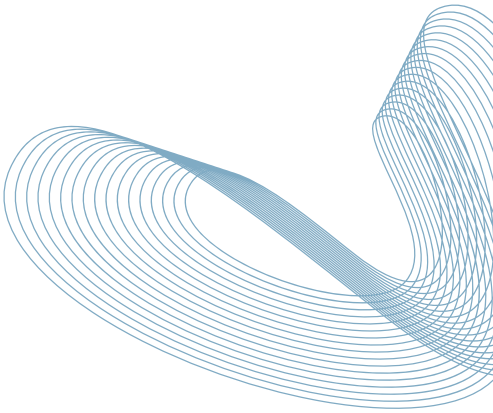
Examining the resilience of Irish SMEs provides crucial insight into the operational risks facing businesses today.

This understanding highlights several opportunities to strengthen support for this pivotal sector, including:

- Enabling industry bodies to deliver tailored, sector-specific cybersecurity training to their members.
- Embedding cybersecurity requirements across all digitalisation funding streams, including those for web development and AI enablement.
- Clarifying supply chain cybersecurity expectations and supporting SMEs within supply chains through transparent, consistent guidance.
- Promoting cybersecurity as a continuous business risk that warrants prioritisation to safeguard organisational health.
- Advancing research into the cybersecurity and business implications facing Irish enterprises to ensure sustained national resilience.

Irish SMEs face a significant national-level cyber resilience gap. This research highlights both the scale of vulnerability across the sector and the practical, achievable opportunities to strengthen cybersecurity.

A transparent understanding of the sector's current posture enables meaningful action at organisational, industry, and national levels. By confronting these challenges directly and building on the insights presented here, Ireland's SME sector is well-positioned to enhance its overall cyber resilience in the years ahead.



Methodology & Sector Representation

Methodology

The data in this report was collected by the Munster Technological University Cybersecurity Research Group under Ethics Approval Number MTU-HREC-MR-24-007.

The Cyber Resilience for SMEs project is a collaboration between Munster Technological University (MTU) and the Irish National Cyber Security Centre (NCSC). All research and data collection was conducted by MTU, not the NCSC.

The data was gathered from 894 organisations that completed the Resilience Assessment Tool on cyberresilience.ie during 2024-2025.

Responses were self-reported and anonymous, with no independent auditing. The tool was promoted through radio and LinkedIn ads.

The Resilience Assessment Tool generates a bespoke cyberresilience score for each SME upon completion. This score reflects an organisation's operational profile and the cybersecurity measures it has implemented. To ensure accurate and impactful evaluation, actions that are more critical to fostering cyber resilience are assigned a greater weighting, consequently having a more significant influence on the overall score.

The weighting of actions was developed in consultation with a panel of 30 Irish cybersecurity experts. This approach fundamentally prioritises an organisation's capacity for continuous operation and recovery in the event of a cyber disruption, rather than on the implementation of purely technical cybersecurity measures.

The Cyber Resilience Score, on a scale of 0 to 10, indicates how many of the suggested cybersecurity actions an SME has implemented. It is used to demonstrate the proportion of potential cybersecurity actions that SMEs have actually implemented.

A score of 0 indicates no relevant cybersecurity actions have been taken, while a score of 10 represents the full implementation of all recommended measures to secure the business.

Sector Representation

The distribution of SMEs represented in the sample data closely mirrors the real-world sectoral distribution (per CSO statistics 2022). The sample dataset is predominantly composed of microenterprises (88%), closely aligning with the CSO sectoral analysis (92.3%). Small enterprises account for 7.5% in the sample and 6.3% in the CSO data, while medium enterprises account for 4.5% and 1.2% in the CSO data, respectively.

Resilience Assessment Dataset

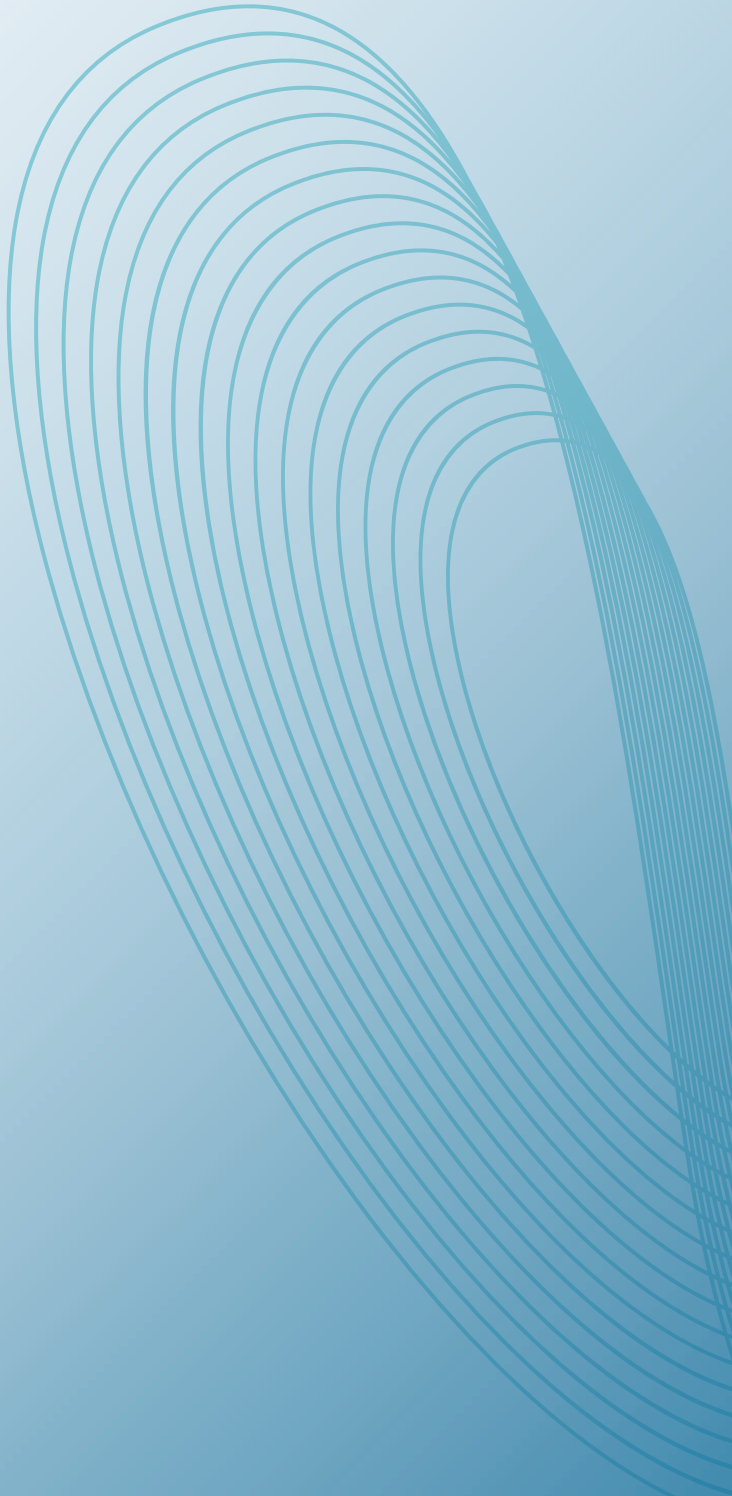
SME Size	%
Micro	88%
Small	7.5%
Medium	4.5%

Central Statistics Office Data (2022)

SME Size	%
Micro	92.6%
Small	6.1%
Medium	1.1%

The Cyber Security Research and Innovation Group at Munster Technological University specialises in critical infrastructure resilience, cyber governance, risk and compliance, human-centred cybersecurity and quantum information security. This research was led by the Cyber Governance, Risk and Compliance strand in collaboration with the National Cyber Security Centre of Ireland.

We would like to thank the 271 SME owners who contributed to the co-creation of the risk assessment tool, and the 894 SMEs who used the tool to take the first step towards improving the resilience of their businesses.



CYBERRESILIENCE
DIGITAL RESILIENCE FOR SMES

NATIONAL CHALLENGE FUND
From Ingenuity to Research and Solutions

Rialtas na hÉireann
Government of Ireland

Taighde Éireann
Research Ireland

Maoinithe ag an Aontas Eorpach
Funded by the European Union