CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

MTU

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Cybersecurity Maturity Baselines of Irish Exporting SMEs

April 2026

Cyber Ireland / Munster Technological University

NCC
NATIONAL CYBERSECURITY COORDINATION AND DEVELOPMENT CENTRE
IRELAND

Rialtas na hEireann
Government of Ireland

Co-funded by the European Union

Funding note: This report was published by Cyber Ireland and Munster Technological University (MTU) in collaboration with the National Cyber Security Centre (NCSC), as part of the NCC-IE Cyber Community Project.

The project was supported by the NCC-IE, funded by the Government of Ireland and European Commission. It is co-funded by the European Union under the Digital Europe Programme, Project: 101127902 — NCC-IE — DIGITAL-ECCC-2022-CYBER-03.

EXECUTIVE SUMMARY

98 **IRISH EXPORT-FOCUSED SME'S ASSESSED**

TOP CYBERSECURITY WEAKNESS

1. **Govern:**
71% had no cybersecurity policy
66% no cybersecurity awareness training
79% did not assess third-party vendor risks

2. **Identify:**
85% had no vulnerability management processes
89% didn't conduct penetration testing

3. **Protect:**
99% had network security weaknesses
96% had major access control issues
99% had data security gaps
74% had cloud misconfigurations

4. **Detect:**
66% lacked an IDS / IPS

5. **Respond:**
70% had no incident response plan

6. **Recover:**
89% had backup weaknesses

TOP SME CYBERSECURITY SOLUTIONS REQUIRED

- Baseline cybersecurity governance packages
- Lightweight, SME friendly managed services
- Access & identity governance
- Network security modernisation
- Backup resilience services

RECOMMENDATIONS

- **SMEs:** Prioritise baseline cybersecurity requirements and follow guideance: Enable MFA, keep systems patched, test backups, and maintain updated devices.
- **Cybersecurity Providers:** Deliver SME-tailored services: Provide bundled and ongoing support that covers monitoring, patching, identity, cloud security, and vulnerability management.
- **For Government:** Promote dedicated cybersecurity resources for SMEs and use a standardised framework such as CyFun.

Rialtas na hEireann Government of Ireland
Co-funded by the European Union

Contents

Co-funded by the European Union

1. Introduction

Irish export-focused companies depend on digital systems to deliver their solutions internationally and remain competitive. Cybersecurity is critical for these companies to protect their organisation, solutions and customers. Investing in cybersecurity not only mitigates the risk of a cyber-attack, it also is a value-add and differentiator for companies selling internationally and part of global supply chains.

To support export-focused Small and Medium-sized Enterprises (SMEs), Enterprise Ireland (EI) and the National Cyber Security Centre (NCSC) launched the Cyber Security Review Grant and Cyber Improvement Grant.

The EI Cyber Security Review grant provided companies funding to conduct and independent review of their cybersecurity posture, identify vulnerabilities, and develop a clear roadmap to enhance security measures.

Cyber Ireland was tasked by the National Cybersecurity Coordination and Development Centre (NCC-IE) to assess Cybersecurity Maturity Baselines of export-focused Irish SMEs taking a sample of Irish SMEs who had completed the EI Cyber Review. This research aims to understand security practices and common vulnerabilities, which could be improved through targeted supports such as cybersecurity grants or ENISA support services. Furthermore, analysis of common cybersecurity frameworks and the standardised reporting templates used by cybersecurity consultants was conducted to support the improvement of the cybersecurity grants through Enterprise Ireland (Cyber Review Grant) and the National Cyber Security Centre (Cyber Improvement Grant).

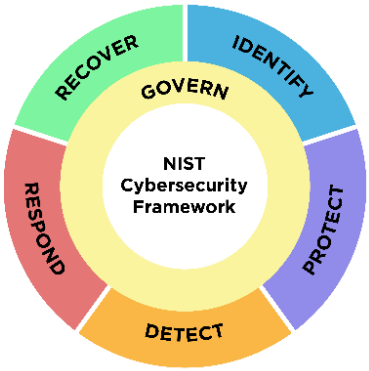
2. Methodology

This report presents the findings from an analysis of 98 anonymised cybersecurity assessment reports, conducted through the EI Cyber Review Grant. The vulnerability analysis was categorised into 10 domains, aligning with the NCSC Cybersecurity for small businesses guidance.

Certain limitations should be noted including that results reflect export-focused SMEs who applied for EI grant schemes, which may incur leading bias and are not representative of all Irish SMEs.

NCC IRELAND
Rialtas na hEireann Government of Ireland
Co-funded by the European Union

3. Top Cybersecurity Weaknesses in Irish SMEs



The top cybersecurity weaknesses in Irish SMEs are presented, aligned to Cyber Fundamentals (CyFun):

3.1 Govern – Policy and Oversight Gaps

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

Governance weaknesses were the most common and most severe:

- **71%** had *no cybersecurity policy*
- **70%** had no incident response plan
- **64%** had *no business continuity plan*
- **66%** provided *no cybersecurity awareness training*
- **79%** did **not** assess third party vendor risks
- Security responsibilities were often undefined or informal.
- Policies, where they existed, were inconsistent or outdated.

What this means for SMEs: Most SMEs lack the internal structures needed to enforce even basic cyber hygiene. Without policies, plans, or defined roles, technical controls are rarely maintained over time.

Co-funded by the European Union

3.2 Identify – Understanding Assets, Data and Risks

Understanding organisational risks, assets, and vulnerabilities.

SMEs struggle to understand what needs protection:

- **51%** no data classification place
- Limited or missing asset inventories (devices, cloud services, accounts)
- Weak visibility of third-party dependencies
- **85%** had no vulnerability management processes
- **89%** did not conduct penetration testing

What this means for SMEs: You cannot secure what you cannot see. Poor visibility results in unpatched systems, unmanaged cloud services, and blind spots that attackers exploit.

3.3 Protect – Technical Controls to Prevent Attacks

This category contained the largest number of technical weaknesses.

Network & Infrastructure

- **99%** had network security weaknesses
- **40%** had flat, unsegmented networks
- **27%** had no Virtual private network (VPN) for remote or third-party access
- Firewalls were misconfigured, outdated, or missing

Access & Identity

- 96% had major access control issues
- 70% had password weaknesses
- 69% had no or only partially implemented Multifactor Authentication (MFA)
- 35% had no access review process

Application & Data Security

- 58% had web application vulnerabilities
- 90% had data security gaps (no data classification, no encryption policy, no retention policy)
- Encryption was inconsistently applied

Rialtas na hEireann Government of Ireland
Co-funded by the European Union

Cloud Security

- **74%** had cloud misconfigurations
- Weak identity controls and inconsistent MFA identified.
- Overreliance on vendor defaults

What this means for SMEs: Even SMEs with MFA, cloud tools, and firewalls still had misconfigurations or partial implementations. Attackers most often exploit these basic lapses, not advanced weaknesses.

3.4 Detect – Monitoring, Alerts & Early Warning

Developing capabilities to recognise and respond to threats.

Across SMEs:

- 66% lacked an Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
- Little or no security monitoring in cloud platforms
- No centralised log collection
- No threat detection or alerting tools in place
- No vulnerability management processes

What this means for SMEs: Most SMEs are blind to security incidents until after damage is done. Detection capabilities are essential to prevent small incidents becoming major breaches.

3.5 Respond – Ability to Contain and Mitigate Incidents

Establishing incident response and mitigation procedures.

Response readiness was poor across SMEs:

- **70%** had *no incident response plan*
- Lacked defined response roles or communication procedures
- Lacked tabletop exercises or simulations
- No vendor or legal response contacts prepared
- No internal reporting or escalation mechanisms

Rialtas na hEireann Government of Ireland
Co-funded by the European Union

What this means for SMEs: Without a plan, incident response is slow, uncoordinated, and costly. Even a basic plan dramatically reduces impact and downtime.

3.6 Recover – Backups, Continuity & Resilience

Ensuring business continuity and resilience following incidents.

SMEs rely on backups, but most are not fully reliable:

- **89%** had backup weaknesses
  - **38%** never tested backups
  - **31%** had backup coverage gaps
  - **9%** had unencrypted backups
  - **3%** had *no backups at all*
- **64%** had *no business continuity plan*
- Backup storage often local-only or cloud-only (single point of failure)

What this means for SMEs: Backups often give a false sense of security. Unverified backups or poor recovery plans lead to long outages after ransomware or system failures.

4. Insights for Cybersecurity Companies

For cybersecurity providers, this research highlights clear areas of market need, where solutions and services are required:

1. **Baseline governance packages**
   - Policy development (cyber, access control, IRP, BCP)
   - Cybersecurity awareness programmes
   - Vendorrisk frameworks

2. **Lightweight, SME friendly managed services**
   - Managed patching
   - Managed detection & response (MDR)
   - Cloud configuration monitoring
   - Vulnerability management as a service

Rialtas na hEireann Government of Ireland
Co-funded by the European Union

3. **Access & identity governance**
   - Role-Based Access Control (RBAC) design
   - MFA rollout and enforcement
   - Password and credential hygiene

4. **Network security modernisation**
   - Affordable segmentation solutions
   - Firewall review & documentation
   - Zerotrust remote access options

5. **Backup resilience services**
   - Backup testing and recovery simulations
   - Hybrid backup design
   - Encryption and retention policy development

5. Standardising Report Templates and Frameworks

The EI Cyber Review Report Template was applied by the cybersecurity consultants in approximately 85% of reports.

The most common cybersecurity frameworks used in reports were ISO 27001 (35%), followed by NIST CSF (23%), NIS2 (22%) and CIS Critical Security Controls (19%). However, 26% of reports did not mention any cybersecurity framework; furthermore, NIS2 is not a cybersecurity framework, rather a regulation that requires a cybersecurity framework to implement controls.

It is recommended that future cybersecurity grants from government utilise one standardised framework, such as CyFun. This allows for more consistent comparison and risk scoring, with clearer prioritised remediation roadmaps.

Rialtas na hEireann Government of Ireland
Co-funded by the European Union

6. Recommendations – A Collaborative Approach to SME Cyber Resilience

The report makes recommendations from the analysis to improve the delivery of cybersecurity grants and SMEs cyber resilience:

6.1 For SME's

1. **Prioritise the basics**: MFA, tested backups, patching, updated devices.
2. **Build governance foundations**: cybersecurity policies, incident response plans, and staff training matter as much as technical tools.
3. **Know your assets**: keep an inventory of devices, systems, and cloud services.
4. **Classify your data**: identify what information matters most and protect it accordingly.
5. **Treat cloud and third-party risks seriously**: misconfigurations and vendors are major sources of compromise.

For information on best practices in cybersecurity for SMEs, see the **NCSC's SME webpage**.

6.2 For Cybersecurity Providers

1. **Create SME tailored service bundles** addressing the most common gaps.
2. **Adopt and promote standardised frameworks and reporting,** such as CyFun.
3. **Support SMEs with continuous rather than one off services**, especially in monitoring, patching, identity, and cloud security.
4. **Help SMEs move from reactive to proactive security** through vulnerability management and governance.

6.3 For Government

1. **Provide dedicated cybersecurity resources** and guidelines for Irish SMEs, targeting the most common weakness identified, and communicated through a national awareness campaign.
2. **Provide an online cyber risk assessment tool** available for all SMEs to improve their cyber resilience.
3. Align future cybersecurity grants from government with one **standardised cybersecurity framework**, such as CyFun. This allows for more consistent comparison and risk scoring, with clearer prioritised remediation roadmaps.

Rialtas na hEireann Government of Ireland
Co-funded by the European Union

4. **Continue research on cybersecurity maturity baselines** to track trends over time and explore more comprehensive analysis with sector specific insights.

Overall, continued focus on these areas ensures that future initiatives deliver greater value and support companies in achieving cyber resilience.

Rialtas na hEireann
Government of Ireland
Co-funded by
the European Union

CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

MTU

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCC
NATIONAL CYBERSECURITY COORDINATION AND DEVELOPMENT CENTRE IRELAND

Rialtas na hEireann
Government of Ireland

Co-funded by the European Union