NAVIGATING NIS2:

THE GUIDE FOR IRISH SMES

BHConsulting
Cybersecurity & Data Protection

HUAWEI

FOREWORD

Huawei Ireland has commissioned independent information security expert Brian Honan to write this guide on how organisations within Ireland, and indeed elsewhere within the European Union, need to align their cybersecurity frameworks with the requirements of the latest EU Network InformationSecurity Directive (NIS2).

The current version of Network Information Security Directive (NIS) has been in place since 2016 and applies to organisations deemed to be part of the critical infrastructure of EU member states. The EU update of the NIS Directive came into force on January 16, 2023, and organisations have until 17 th October, 2024 to comply with the requirements of NIS2. This update will apply to a wider range of organisations than were included under the original NIS directive.

The purpose of this guide is to highlight, to those affected, what they need to have in place by 2024 toensure they are compliant with the requirements of the Directive.

ABOUT BRIAN HONAN, GUIDE AUTHOR

Brian is a highly experienced information security professional and one of Ireland's foremost experts in cybersecurity. Over his long-established career, he has managed and delivered information security projects and services to organisations of varying sizes, from SMEs to large and multinational companies.

Additionally, he has worked extensively with government departments both in Ireland and the UK and has provided advice to various Government security agencies, the European Network and Information Security Agency and the European Commission.

After more than 12 years in various management, operations and network roles, Brian founded BH Consulting in 2004. In 2013, Brian was appointed as a special advisor on internet security to Europol's European Cybercrime Centre (EC3). He has since established IRISSCON, the annual Irish Cybercrime conference in Ireland and is highly sought after as an expert commentator in the media on topics such as cybercrime and information security.

Brian regularly presents at industry conferences including RSA Conference (Europe and US), B-Sides London, Source Conferences, Cloud Security Summit, Infosec Europe and IDC IT Security Seminar. He is a member of the Information Systems Security Association, the Irish Computer Society and the Information Systems Audit and Control Association.

TABLE OF CONTENTS

CHAPTER

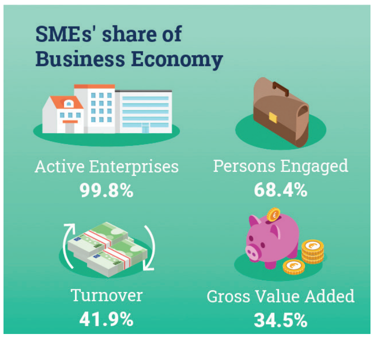
01 THE IMPORTANCE OF THE SME TO THE IRISH ECONOMY

1. THE IMPORTANCE OF THE SME
TO THE IRISH ECONOMY

Despite the headlines and attention often shown to the large multi-nationals that chose to locate their operations in Ireland, the driving force behind Ireland's economy are the many Small and Medium sized Enterprises (SMEs). According to the Irish Central Statistics Office's (CSO) "Business In Ireland Report"[1] of the active enterprises in Ireland in 2020, 99.8% are SMEs and those SMEs account for 68.4% of all people employed. The CSO also states that the SME sector in Ireland generates approximately 42% of all turnover in the business economy.

The definition of a SME is any organisation that employs less than 250 employees and has an annual turnover of less than €50 million euro. Within that definition there are further categories of small and micro businesses SME Characteristics.[2]

An Phríomh-Oifig Staidrimh
Central Statistics Office



COMPANY CATEGORY	STAFF HEADCOUNT	TURNOVER	BALANCE SHEET TOTAL
Medium-sized SME	< 250	≤ € 50 m	≤ € 43 m
Small SME	< 50	≤ € 10 m	≤ € 10 m
Micro SME	< 10	≤ € 2m	≤ € 2 m

While this dependency on the SME sector brings many societal, economic, and individual benefits, it also poses some risks. Recent years have seen significant challenges to the Irish economy and to Irish businesses, in particular to the SME sector. The COVID19 pandemic caused significant disruption to businesses, with organisations of all sizes and in all sectors having to rapidly adjust their business models in other to survive.

Post the COVID19 pandemic, businesses faced additional challenges in the lingering impact on the supply chain, and staffing shortages, resulting in significant increase in costs. The continued uncertainty around Brexit, as the United Kingdom left the European Union, also impacted on many of those Irish businesses who not only serve the UK market but also on those businesses who sourced supplies from, or through, the UK.

To exacerbate an already challenging business environment the illegal invasion of Ukraine by Russia, in 2022, caused a significant jump in the costs of energy, grain, and other materials resulting in a significant and rapid increase in the cost of living and, in turn, overall business costs.

Many Irish SMEs have proven to be resilient and adaptable to all these challenges and continue to provide services to their customers, and employment to their staff. Part of this resilience and adaptability has been in the willingness and openness by Irish SMEs to embrace digital technologies in order to improve efficiencies, reduce costs, and to reach new markets.

According to the CSO's "Information Society Statistics - Enterprises 2022"[3] Irish businesses rely heavily on internet and ICT services with 97% of Irish businesses utilising broadband and 49% of SMEs conducting online sales.

[1] https://www.cso.ie/en/releasesandpublications/ep/p-bii/businessinireland2020/smallandmediumenterprises/
[2] https://isme.ie/sme-facts-and-faqs/
[3] https://www.cso.ie/en/releasesandpublications/ep/p-isse/informationsocietystatistics-enterprises2022/

1.1 CYBERSECURITY IN IRELAND

In 2021 cybersecurity hit the headlines in Ireland in a major way resulting from a ransomware attack which took all the computer systems in the HSE[4] offline for several weeks, with some systems remaining offline for months. There have been other high profile attacks since then against organisations such as Munster Technology University (MTU)[5] and Virgin Media[6]. While attacks against large organisations generate headlines, cybercrime is increasingly a major risk against all organisations no matter what their size.

According to a survey published in February 2023 by AON[7] nearly **one in five companies in Ireland experienced a cyber attack in 2022**. These findings are reinforced by the insurance company Hiscox's Cyber Readiness Report[8] which highlights that **49% of Irish companies surveyed suffered a cyber attack in 2021** and 20% of those companies that were victims of a cyber attack say their solvency was threatened as a result of the attack.

1.2 CYBERSECURITY CHALLENGES FOR IRISH SMES

Criminals do not discriminate against victims based on their size. SMEs are often targeted by criminals as demonstrated by Grant Thornton's Cost of Cyber Crime Report 2022[9] which states that **one third of Irish small-and medium-size businesses were victims of cyber crime**. Criminals will target SMEs based on that company's profile or will target an SME simply based on who their customers are.

A common misconception is that cyber-attacks only affect large organisations, but this is not the case. Any enterprise, regardless of its size, can be vulnerable to cyber threats. SMEs are especially attractive targets for cybercriminals, who may perceive them as having weak cybersecurity measures and defences. Moreover, SMEs that serve larger organisations, may be exploited as a gateway to compromise the systems and data of their clients.

Criminals that are looking to compromise the systems of a large organisation, may not do so directly as that large organisation may have very robust cybersecurity measures in place. Instead, in order to breach the security of the target organisation the criminals may look to gain access via one or more of the suppliers into that organisations. We have seen examples of these type of attacks in recent years, such as the compromise of US government agencies' systems allegedly by the Russian government exploiting a weakness in the SolarWinds[10] software employed by those agencies. More recently Aer Lingus staff data[11] was compromised by criminals using a weakness in the MoveIT software employed by Aer Lingus's payroll sub-contractor. The HSE suffered another data breach due to the outsourcing of their recruitment process to the consulting firm EY[12]. EY employed the MoveIT software for transferring files between itself and its clients, resulting in data belonging to the HSE being compromised. Another Irish victim of the MoveIT breach was Dublin Airport who outsourced services to the insurer Aon[13].

New technologies offer many benefits for businesses including SMEs such as reducing costs, improving efficiencies, and providing better data to make management decisions. One such technology is Artificial Intelligence, otherwise known as AI. Artificial Intelligence can be employed by SMEs to assist improve customer service by providing 24x7 online chat bots to manage customer queries. AI can also be used to help analyse vast quantities of data to identify ways to improve an SME's product range or improve on its manufacturing processes. Other areas

[4] https://www.hse.ie/eng/services/news/media/pressrel/hse-publishes-independent-report-on-conti-cyber-attack.html
[5] https://www.irishtimes.com/crime-law/2023/02/14/munster-technological-university-cyberattack-the-work-of-sophisticated-ransomware-group/
[6] https://www.rte.ie/news/2023/0220/1357832-virgin-media-hack/
[7] Aon's Survey Finds One in Five Firms in Ireland Experienced a Cyber Attack Last Year | Aon
[8] Cyber Readiness | Hiscox Ireland
[9] https://www.grantthornton.ie/insights/publications/the-cost-of-cybercrime-2022/
[10] https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
[11] https://www.rte.ie/news/ireland/2023/0606/1387652-cyber-attack/
[12] https://www.rte.ie/news/2023/0609/1388385-hse-ey-cyberattack/
[13] https://www.siliconrepublic.com/enterprise/dublin-airport-employees-daa-cyberattack-moveit-hack-aon-clop

where AI can help SMEs is creating marketing content or presenting business data in a more constructive way to assist in better decision making. However, **AI can also present cybersecurity and data protection challenges which SMEs need to grapple with**. Any AI systems used by SMEs need to be implemented, maintained, and deployed in secure ways to ensure the maximum benefit is derived from them.

As can be seen, cybersecurity is becoming a business critical issue for SMEs and needs to be managed the same as any other business risk. However, while SMEs face the same threats from cybercriminals as large organisations, SMEs have different challenges than their larger counterparts.

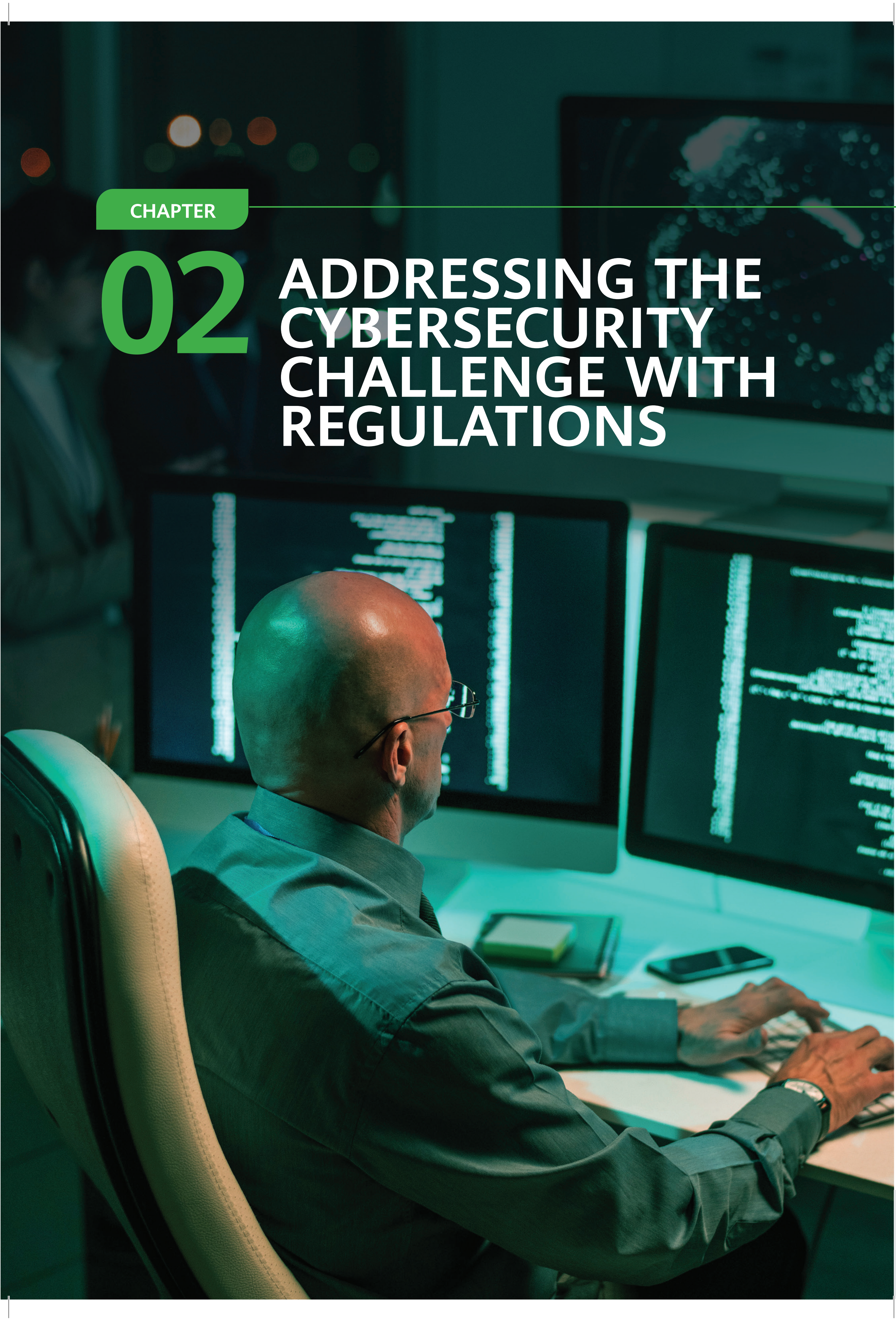
Some of the key challenges SMEs face relating to cybersecurity[14] are:

- Inadequate management support and commitment to cybersecurity. This often arises more often due to a lack of appreciation of the threats facing their business. However, it can lead to a lack of commitment to cybersecurity by SME management, which in turn leads to lack of budget and resources to improve cybersecurity.
- Low cybersecurity awareness among staff. Many people working in SMEs are not provided with appropriate levels of awareness training so that they can identify and respond to security threats, and also how to use technology in a safe and secure manner.
- Inappropriate security measures deployed to protect sensitive information. In many SMEs, there is not a structured approach to managing sensitive data with many people having unnecessary access to it.
- Many SMEs do not have a dedicated cybersecurity budget relying instead on their IT budget to include measures to secure their systems and data. **The Hiscox Cyber Readiness report[15] recommends that 22% of a company's overall ICT budget should be dedicated to cybersecurity measures**. However, often this is not the case and IT budgets only cover some basic measures such as anti-virus software.
- Most SMEs do not have access to cybersecurity specialists to provide them with guidance on the steps they need to take to secure their systems and data. Indeed, SMEs may often rely on external companies to provide them with support for their IT needs and in many cases this does not include specialist cybersecurity advisory services.
- While there are many guidelines published to help organisations secure their systems, many of these guidelines are aimed at larger organisations resulting in impractical or cost-prohibitive advice being given for SMEs to follow.
- A common challenge for SMEs is the use of personal devices, such as phones and laptops, and cloud services by employees to access and work on company data, which can leave companies with a security challenge. This is because personal devices are often not as secure as company-issued devices, and they may be more susceptible to malware or data breaches. Additionally, if employees store company data in the cloud, they may not be aware of the security or regulatory risks associated with doing so. This leaves a challenge for SMEs on how to secure that data and ensure it complies with its regulatory requirements such as the EU General Data Protection Regulation (GDPR).[16]

[14] https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes
[15]https://www.hiscox.ie/cyber-readiness
[16]https://www.dataprotection.ie/en/organisations/data-protection-basics

CHAPTER

02 ADDRESSING THE CYBERSECURITY CHALLENGE WITH REGULATIONS



2. ADDRESSING THE CYBERSECURITY **CHALLENGE WITH REGULATIONS**

Given the growing dependency on the internet and IT systems, cybersecurity is obviously a vital issue for all businesses. It is also a concern for Ireland at the national level and for the European Union as a whole. In particular, the EU and member state governments are worried about the detrimental impact should organisations which provide critical services at the EU or individual member states level become victims of a major cyber attack. As evidenced by the cyber attack against the HSE, these type of attacks can have significant impacts on the economy, reputation and resilience of a country.

To manage this significant risk, the EU has introduced an enhancement to its Network and Information Security (NIS) Directive[17]. The NIS2 (Network and Information Security Directive 2) is an updated version of the EU NIS Directive, adopted on **December 14, 2022,** which requires organisations that provide critical services, such as energy, transport, and financial services, to implement appropriate security measures to protect their systems and data from cyberattacks.

The NIS2 aims to improve the overall level of cybersecurity in the European Union by addressing the challenges that have emerged since the adoption of the original **NIS Directive in 2016**. These challenges include:

- the increasing sophistication of cyberattacks;
- the growing interconnectedness of critical infrastructure;
- the increasing use of cloud computing and other shared services.

The NIS2 makes a number of changes to the original NIS Directive, including:

- expanding the scope of the directive to cover more sectors and organisations.
- increasing the requirements for risk assessment and incident response.
- strengthening cooperation between organisations and national cybersecurity authorities.
- introducing a new certification scheme for cybersecurity products and services.

NIS2 came into force on January 16, 2023, and organisations have until the 17th of October, 2024 to comply with its requirements.[18]

The NIS2 is a significant piece of legislation that has the potential to make a real difference in the fight against cyberattacks. By requiring organisations to implement more stringent security measures and cooperate more effectively with national cybersecurity authorities, the NIS2 aims to create a more secure and resilient European Union.

Here are some of the key differences between the original NIS and the NIS2:

- The NIS2 expands the scope of the directive to cover more sectors and organisations. This includes organisations in the healthcare, water, and telecommunications sectors.
- The NIS2 increases the requirements for risk assessment and incident response. Organisations are now required to carry out more comprehensive risk assessments and to have more robust incident response plans in place.

[17] https://digital-strategy.ec.europa.eu/en/policies/NIS2-directive

[18] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

- The NIS2 strengthens cooperation between organisations and national cybersecurity authorities. This includes providing the European Union Agency for Cybersecurity (ENISA)[19] with an enhanced mandate and role which will allow it to provide additional supports to national cybersecurity authorities.

- The NIS2 introduces a new certification scheme for cybersecurity products and services. This scheme will help organisations to identify and purchase cybersecurity products and services that meet the highest standards of security.

Under NIS2 the list of industries covered is much longer than with NIS, which means that many Irish SMEs will need to determine if they are obligated to comply with the requirements of the NIS2 directive.

While most SMEs are exempt from NIS2, **it applies to businesses with more than 250 employees and an annual turnover of more than €50 million and/or an annual balance sheet above €43 million**, Irish SMEs could be impacted if they operate, or their clients operate, in areas such as digital services, communications, transport, or finance to name a few. The Irish government, and other member states, will classify entities that are "essential" (e.g., critical infrastructure operators, certain manufacturers) or "important" (e.g., digital services providers, managed services providers). While both groups must meet the same requirements, "essential" entities will face proactive supervision.

The NIS2 Directive applies to a wide range of businesses in Ireland as detailed in the Annex of NIS2[20].

Highly critical sectors:

These are businesses that provide critical services to society, such as;

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure
  - ICT service management (business-to-business)
- Public administration
- Space

Other Critical Sectors

- Postal and courier services
- Waste management
- Manufacture, production, and distribution of chemicals
- Production, processing, and distribution of food
- Manufacturing including:
  - Medical devices
  - Computers
  - Electronic and optical products
- Electrical equipment
  - Motor vehicles
  - Transport equipment
  - Machinery and equipment
  - Industrial Control Systems
- Digital providers
  - online marketplaces
  - online search engines
  - social networking services platforms)
- Research organisations

[19] https://www.enisa.europa.eu/

[20] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72172

For many SMEs, becoming compliant with the requirements of NIS2 may seem a major challenge. However, there are some simple, practical, and cost-effective approaches that they can take to address the challenge. NIS2, similar to many other EU cybersecurity and privacy regulations, is based on addressing cybersecurity risk within the organisation.

One way to demonstrate to a regulator that the SME organisation is taking appropriate steps to comply with NIS2 is to use existing cybersecurity risk-based frameworks and standards. For Irish SMEs the most common standards to consider would be the ISO 27001:2022 Information Security Standard[21,] currently there is no Irish cybersecurity standards but that may change in the future. The ISO 27001:2022 Information Security Standard is a very well regarded standard that is recognised internationally, however for some SMEs it may prove to be a costly solution.

In addition, the EU Cybersecurity Act[22] introduces an EU-wide cybersecurity certification framework[23] that companies providing IT products and services can choose to use to demonstrate the security of their products or service. Any Irish SMEs that produce or manufacture IT hardware, software, or cloud services should make themselves familiar with the above certification framework and consider certification. Those SMEs that are not manufacturing or producing any products or services should consider the benefit of purchasing certified products and services.

2.1 MANAGING CYBERSECURITY RISK

As highlighted, NIS2 is focused on the cybersecurity risks and it is critical that an SME impacted directly or indirectly by the directive has taken an appropriate approach to cybersecurity risk management.

Cybersecurity risk management is the process of identifying, understanding, and reducing the potential impacts of cyberattacks on your business. There are several different methodologies and tools that an SME can employ to help them manage cybersecurity risks, which ENISA has comprehensively covered[24].

The ENISA website has a dedicated area, called SecureSME[25] to help SMEs understand the various cost-effective ways they can secure their business.

Managing cybersecurity risks is key to complying with the requirements of NIS2 and its essential that SMEs conduct regular risk assessments to ensure that the appropriate security measures are in place.

[21] https://www.iso.org/standard/27001
[22] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
[23] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework
[24] https://www.enisa.europa.eu/topics/risk-management
[25] https://www.enisa.europa.eu/securesme#/

CHAPTER

03 THE IMPACT OF NIS2 ON IRISH SMES

3. THE IMPACT OF NIS2 **ON IRISH SMES**

The NIS2 Directive will impose new cybersecurity compliance requirements on SMEs that fall within its scope. These requirements will include:

- putting in place appropriate technical and organisational measures to protect their networks and systems from cyber threats.
- identifying and assessing their cyber risks.
- cooperating with competent authorities and other entities in the event of a cybersecurity incident.
- reporting significant cybersecurity incidents to the National Cyber Security Centre (NCSC)[26] which is Ireland's national Computer Emergency Response Team (CERT).

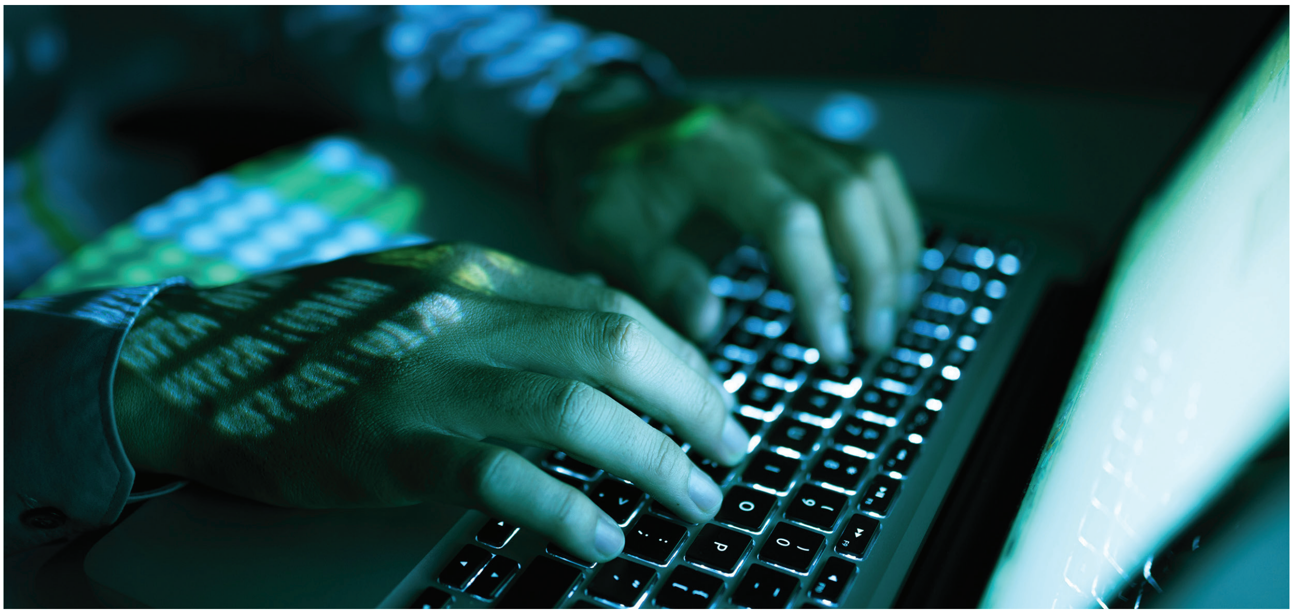
It should be noted that the NIS2 strengthens the enforcement and sanctions regime for non-compliance by introducing **fines of up to 2% of the annual turnover or €10 million (whichever is higher)** for essential entities, and up to 1.4% of the annual turnover or €7 million euros (whichever is higher) for important entities.

Regulators will be appointed by each member state which will ensure the requirements of NIS2 are being met by regulated entities. Within Ireland the current regulators under NIS are as follows:

REGULATORY BODY	REGULATED ENTITIES	CONTACT DETAILS
The National Cyber Security Centre (NCSC)	Digital Service Providers (DSPs)	www.ncsc.gov.ie nisdirective@dccae.gov.ie +353 1 6782333
The National Cyber Security Centre (NCSC)	Operators of Essential Services (OESs); • Energy, • Transport, • Health, • Drinking water supply and distribution, • Digital infrastructure	www.ncsc.gov.ie nisdirective@dccae.gov.ie
Central Bank of Ireland[27]	Banking and financial service providers	https://www.centralbank.ie/home fcpm@centralbank.ie +353 1 2244203

[26] https://ncsc.gov.ie/

[27] https://urldefense.com/v3/__https:/www.centralbank.ie/home__;!!DOxrgLBm!XCP8yWnK5A2aowAxfJ4-bIAjqJnf0z_hS2-mgRRAif2qFI-ZZWwWVLMxU5z0Ylq-2Mi5fxrnatrUGsaXrA$



It is not yet known if the current regulators will change with the transposition of NIS2 into Irish law.

Even if a small business is not directly subject to the NIS2 regulation, it may still be affected indirectly by NIS2. A new focus in NIS2 is that regulated entities must not only ensure the effectiveness of their own cybersecurity controls, they must also ensure that they conduct regular cybersecurity risk assessments of those businesses they rely on in their supply chain. This will mean regulated entities will be looking at their suppliers, and the suppliers to those suppliers, to provide assurances that those suppliers have effective cyber security controls in place. This will result in any SMEs that provide IT or other services to regulated entities will need to be able to demonstrate to their clients that they have appropriate cybersecurity measures in place.

This could lead to an increase in costs for directly and indirectly impacted Irish SMEs. A recent report from EY titled "The Future of Cybersecurity in Europe – Challenges related to the NIS2 Directive"[28] highlights that for SMEs to comply with the requirements of the NIS2 Directive there will be an increase in their ICT costs.

While any increase in costs in the current economic climate is a challenge for many SMEs, the increase in spending to comply with the requirements of NIS2 should not be viewed as a cost but rather as an investment. As discussed earlier, the current cyber threat landscape is very challenging with the likelihood that a successful cyber attack against an SME could pose significant challenges, up to and including going out of business

It should be noted that investing in cybersecurity improvements can also improve overall IT systems leading to improved outcomes in business processes, services, and reducing other costs. Many of the costs associated with cybersecurity can be included in investing in other areas of IT such as upgrading computer operating systems to the latest versions, migrating from on-premise applications to the cloud, and outsourcing some IT and cybersecurity functions to specialist providers.

> "For the new sectors or services, an increase of about 25% of ICT spending can be expected, while for the sectors and services already covered by the NIS Directive, an increase of ICT security spending of about 15%."

[28] https://www.ey.com/en_pl/law/the-future-of-cybersecurity-in-europe-NIS2-directive

CHAPTER

04 TEN STEPS FOR SMES TO IMPROVE CYBERSECURITY FOR NIS2

4. TEN STEPS FOR SMES TO IMPROVE **CYBERSECURITY FOR NIS2**

One of the main challenges for small businesses is to implement effective and affordable security measures that can protect their systems and data from cyberattacks. A main part of this challenge is that many SME owners and management may not have a thorough understanding of what needs to be done to improve the cybersecurity posture of their organisation. This lack of knowledge and confidence can lead to a lack of appropriate decision making or investing in solutions that may not actually resolve the challenges they face.

To help these business owners and managers the following are 10 useful and practical security steps that a SME could consider implementing:

STEP 1 - IDENTIFY WHAT YOU NEED TO PROTECT

One of the first steps in cybersecurity is to understand what it is you need to protect. If you do not know what data you have, the services that you rely on, the systems which are critical to your business, then it will be difficult to properly defend those assets. So the first step SMEs should consider is to identify all the key business assets that it relies on.

These assets can be grouped together into categories to make them easier to manage. The following are examples of some categories an SME could consider;

- Financial data
- Customer data
- Intellectual property
- IT systems
- Computer Devices
- Cloud Services
- Physical infrastructure

Once the assets have been identified the SME can then classify the assets by how important or critical they are to the business. This is to enable the SME to determine on what assets to focus their time, resources, and investment in to securing.

STEP 2 – CONDUCT A RISK ASSESSMENT

After identifying and classifying its key asset, it would be useful for the SME to conduct a risk assessment in order to determine what risks could potentially impact on the assets. These risks could range from data being hacked, to computers being infected with ransomware or other computer viruses, to systems going offline due to a cyberattack, or unencrypted devices being stolen or lost.

A risk assessment is critical to eenable the SME improve its cybersecurity posture by:

- Identifying and prioritising key cybersecurity risks. This is important because not all risks are created equal. Some risks are more likely to occur than others, and some risks can have a more significant impact on the business should they materialise. By prioritising its risks, the SME can focus resources on the most important areas.

- Enabling the development and implementation of a plan and controls to mitigate the risks. This plan can outline in what priority risks are managed, the resources required to manage those risks, who is responsible from implementing the controls and by when they should be implemented by.
- Demonstrating due diligence to customers, partners, and regulators that the SME is taking cybersecurity seriously and taking the appropriate steps and measures to address the risks.
- Ensuring management commitment to improving the company's cybersecurity posture.
- A cybersecurity risk assessment presents cybersecurity risks to management in the same way that other business risks are presented. This allows management to better appreciate and understand the risks associated with cybersecurity and to commit the appropriate resources and investment to address those risks.
- Improving the overall cybersecurity posture for the SME as conducting regular cybersecurity risk assessments can identify areas where cybersecurity can be improved.

By conducting a regular cybersecurity risk assessment, SMEs can take steps to protect themselves from cyber attacks and reduce the likelihood of a data breach.

STEP 3 – DEVELOP SECURITY POLICIES

While policies are not often viewed as a technical measure to prevent cyber attacks they play a vital role in improving cybersecurity for all types of organisations, including SMEs. Cybersecurity policies can lay out for both management and employees what is expected of them to protect the company from a cyber attack. Security policies typically cover all aspects of how employees should use the company's ICT environment, equipment, and services. This includes things like password management, email security, remote access, and various other areas.

It is important that these policies are clear, easy to understand, and to follow. The policies should be specific enough to cover all of the possible ways that an employee could compromise the company's security, but not so specific that they are difficult to remember or apply.

It is important that the cybersecurity policies also highlight the consequences an employee could face should they not adhere to the policies. This is important to deter employees from violating the it is important to regularly review, update, and communicate policies to employees, and that employees understand those policies. This is important to ensure that the policies are up to date and that employees are aware of them and understand them.

STEP 4 – IMPLEMENT BASIC CYBERSECURITY CONTROLS

Having identified its key assets, recognised the risks posed to those assets, and documented its policies on how those assets should be protected, it is important for the SME to consider what cybersecurity controls are required to protect the assets in question. Some of the basic cybersecurity controls should include the following:

- **Anti-virus software** – computer viruses are small computer programs often written by criminals to disrupt operations on an affected computer, to steal, corrupt, or wipe data from a computer, allow criminals to remotely access the computer and to run programs on it, or to even encrypt the data on a computer so that criminals can extort money to release that data. To prevent these computer viruses from installing and impacting on computers and systems special cybersecurity software called anti-virus software can be installed on the computers.

- **Implement firewalls** – computer and network firewalls enable a company to manage what traffic can enter and leave its networks and systems. When configured and managed properly, a firewall will only allow traffic authorised by the SME to travel through it. An effective firewall is similar to having security guards at the entrances to a building who check that those entering and leaving the building are authorised to do so.

- **Encryption** – Encryption is where data and information that can be read by humans is passed through an encryption solution which makes that data and information unreadable and inaccessible to humans. The only way to access and read the encrypted data is for someone to use the same encryptions solution and know the secret passphrase to unlock the data. Encryption is a very effective way to protect data and it makes it very difficult for unauthorised people to steal or view sensitive information, such as credit card numbers, passwords, or medical records.

- **Backup data and systems** – A backup is a copy of your important data that is stored on a separate device or location so that if your original data is lost, corrupted or even inaccessible due to ransomware, you can restore it from the backup. Backups are also important to enable the recovery from other disasters such as a computer system failure, a fire, a flood or a cyberattack. Ideally backups should be conducted at regular intervals and stored securely away from the systems and data that are being backed up. These backups could be carried out onto portable disks, tape, or to the cloud. As important as it is for the SME to conduct regular backups it should also periodically test that it can recover from its backups .

- **Password management** - This is a practice that involves creating and using strong passwords for accounts and devices, and storing them securely. Passwords are one of the most common ways for people to authenticate their identity and access resources online or offline. Password management can protect accounts and devices from being hacked or compromised by unauthorised parties who may guess or steal those passwords. It is recommended that SMEs ensure their staff know how to create strong passwords which are:

  - long,
  - complex,
  - unique for each account or device
  - avoid reusing them
  - use a password manager to store them safely.
  - Reset their password should they believe the password has been compromised[29].

- **Consider using Multi-factor authentication (MFA)** - This is a method that requires two or more pieces of evidence to verify a user's identity for them to access a system or application. Traditionally MFA is comprised of two or more for the following types of authentication:
    - something you know (such as a password or a PIN),
    - something you have (such as a phone, a swipe card, or a key),
    - something you are (such as a fingerprint, facial recognition, or retinal scan).

The majority of breaches relate to credentials being abused by criminals, mostly due to compromised passwords[30]. By having MFA in place the risk of such a compromise can be greatly reduced as the criminals need to compromise not just one form of authentication but the other forms that are also in place. SMEs should consider enabling multi-factor authentication for all computer systems and devices whenever possible, especially for those that contain sensitive data or grant high privileges.

STEP 5 – REGULARLY PATCH AND UPDATE COMPUTER SYSTEMS AND APPLICATIONS

Computer software can never be written in such a way that there are never any mistakes in the code for that computer software. Often, the software manufacturer will become aware, either by its own research or by external third parties, that there is an error in its software. These errors are better known as software bugs or software vulnerabilities. If not addressed these vulnerabilities can enable a criminal to break into the software. Instead of rewriting all the code for the software a manufacturer will write a small specific program, called a patch, to address the identified vulnerability. By keeping its software up to date with the latest patches, a SME can help to protect its computers from security threats.

At a high level a SME can implement a patch management process as follows:

- **Identifying patches:** The first step in patch management is to identify which patches are available for the installed software. This can be done by visiting the websites of the software vendors or by using a patch management tool.
- **Testing patches:** Once the patches have been identified, they should ideally be tested in a test environment before deploying them to your production systems. This will help to ensure that the patches do not cause any unexpected problems.
- **Deploying patches:** Once tested satisfactorily, the patches can then be deployed to the production systems. This can be done manually or automatically using a patch management tool.
- **Monitoring patches:** Once the patches have been deployed they should be monitored to make sure that they are working properly and that they have not caused any problems.

[29] https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
[30] https://www.verizon.com/business/resources/reports/dbir/

STEP 6 – CYBERSECURITY AWARENESS AND EDUCATION

Technical security controls can only go so far in protection systems from being attacked. An effective cybersecurity education and awareness program in place is essential for an SME to protect against cyberattacks. It is vital that staff are regularly reminded and informed of the latest cybersecurity threats, how they can identify those threats, and what they should do to prevent falling victim to them. An effective awareness program will empower staff with cybersecurity best practices, how to identify and avoid phishing emails, how to use strong passwords, and how to report suspicious activities.

STEP 7 – REGULARLY MONITOR NETWORK AND KEY SYSTEMS

Many modern operating systems and devices come with security logging and auditing available on them. Once these are enabled a lot of data is available to help detect and alert to a possible cyber attack. However, while this data is readily available it is essential that it is proactively monitored and reviewed for any signs of intrusion or compromise. This will enable the SME to respond quickly to any alerts or incidents. It can take specialised skills and systems to implement a successful cybersecurity monitoring solution. This can be done by the SME itself or alternatively it may prove to be more cost effective and efficient to outsource this activity to an external third party that specialises in this area.

STEP 8 – REPORT ANY SIGNIFICANT CYBER INCIDENTS

NIS2 sets out strict incident reporting requirements with tight deadlines. Any regulated entities are required to provide an initial early warning of any significant cyber incidents within 24 hours of becoming aware of the incident and a more detailed notification report must be sent to the relevant national authority, Central Bank of Ireland for financial entities and the NCSC for all others, within 72 hours of becoming aware of the incident.

Even if an SME does not come under the scope of the NIS2 Directive, if it is a supplier to an entity that is under the scope of the directive the SME should ensure that it can detect and report incidents in a timely manner to its customer.

It is therefore essential that SMEs develop comprehensive Incident Response plans that detail exactly how to respond to various cyber attacks, the roles and responsibilities for dealing with such an attack, and how to report the incident to the appropriate organisations and authorities.

SMEs should also regularly test their Incident Response plans to ensure they are appropriate for their needs and to identify any potential improvements that can be made to the plans.

STEP 9– REGULARLY REVIEW THE CYBER SECURITY MEASURES

As discussed earlier the cyber threat landscape is constantly evolving and the threats will change in line with that landscape. It is therefore essential that SMEs conduct regular reviews of their cybersecurity measures and adjust them according to the changing threat landscape and business needs.

STEP 10 – SEEK HELP

Complying with the NIS2 Directive can seem daunting to many SMEs. However, there is a lot of good practical advice available, often at no charge, that an SME should refer to when embarking on their cybersecurity journey. There are several excellent resources available that provide comprehensive and practical guidance to SMEs.

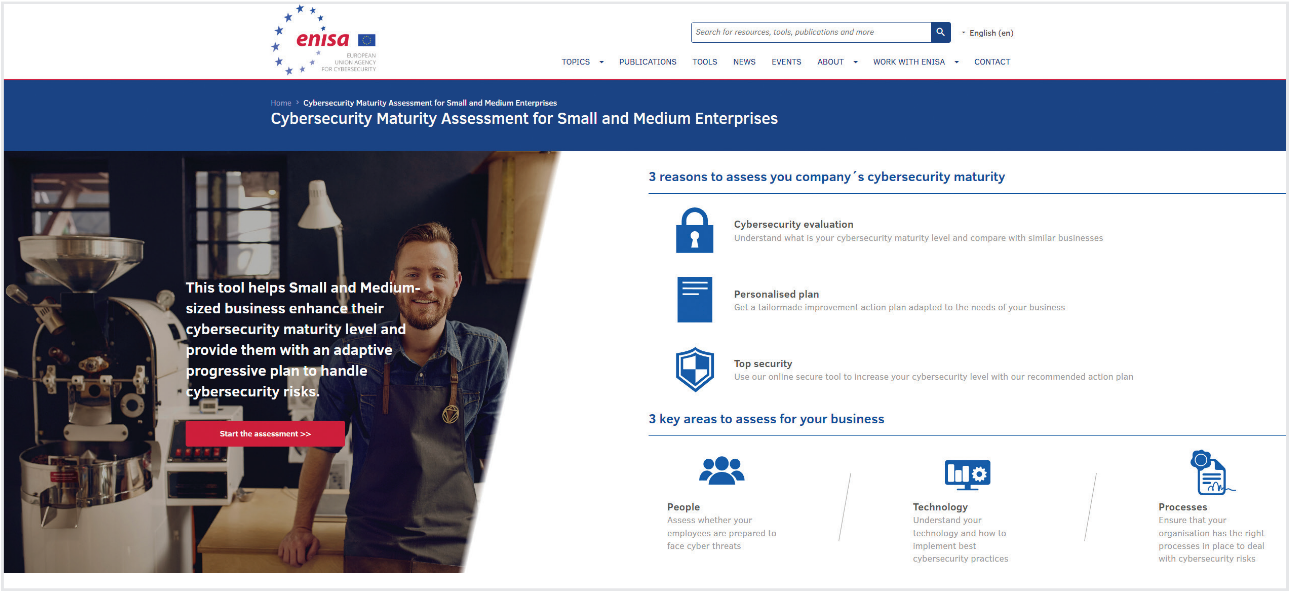
- The EU Agency for Cybersecurity (ENISA) has a comprehensive guide aimed at assisting SMEs to better improve their cybersecurity stance. The ENISA report "Cybersecurity for SMEs – Challenges and Recommendations" is available at https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

- Huawei provides an in-depth guide on cybersecurity for the SME in its study "Cybersecurity for European SMEs" https://www-file.huawei.com/-/media/corp2020/media-center/pdf/facts/papers/cybersecurity%20for%20european%20smes%20a%20huawei%20study.pdf?la=en

- The National Cyber Security Centre (NCSC) has a guide for Irish businesses to help them improve their cybersecurity. The NCSC's "12 Steps to Cyber Security – Guidance on Cyber Security for Irish Businesses" can be downloaded from https://ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf

The EU Agency for Cybersecurity (ENISA) also provides an online "Cybersecurity maturity assessment for small and medium enterprises" focused on the cybersecurity needs of SMEs. The online tool is a series of questions that the SME owner can respond to. Based on the answers provided, the tool will provide a series of recommendations the SME can implement to improve their cybersecurity.

31


enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
Search for resources, tools, publications and more
English (en)
TOPICS
PUBLICATIONS
TOOLS
NEWS
EVENTS
ABOUT
WORK WITH ENISA
CONTACT
Home › Cybersecurity Maturity Assessment for Small and Medium Enterprises
Start the assessment >>

Cybersecurity Maturity Assessment for Small and Medium Enterprises

This tool helps Small and Medium-sized business enhance their cybersecurity maturity level and provide them with an adaptive progressive plan to handle cybersecurity risks.

3 reasons to assess you company´s cybersecurity maturity

Cybersecurity evaluation
Understand what is your cybersecurity maturity level and compare with similar businesses

Personalised plan
Get a tailormade improvement action plan adapted to the needs of your business

Top security
Use our online secure tool to increase your cybersecurity level with our recommended action plan

3 key areas to assess for your business

People
Assess whether your employees are prepared to face cyber threats

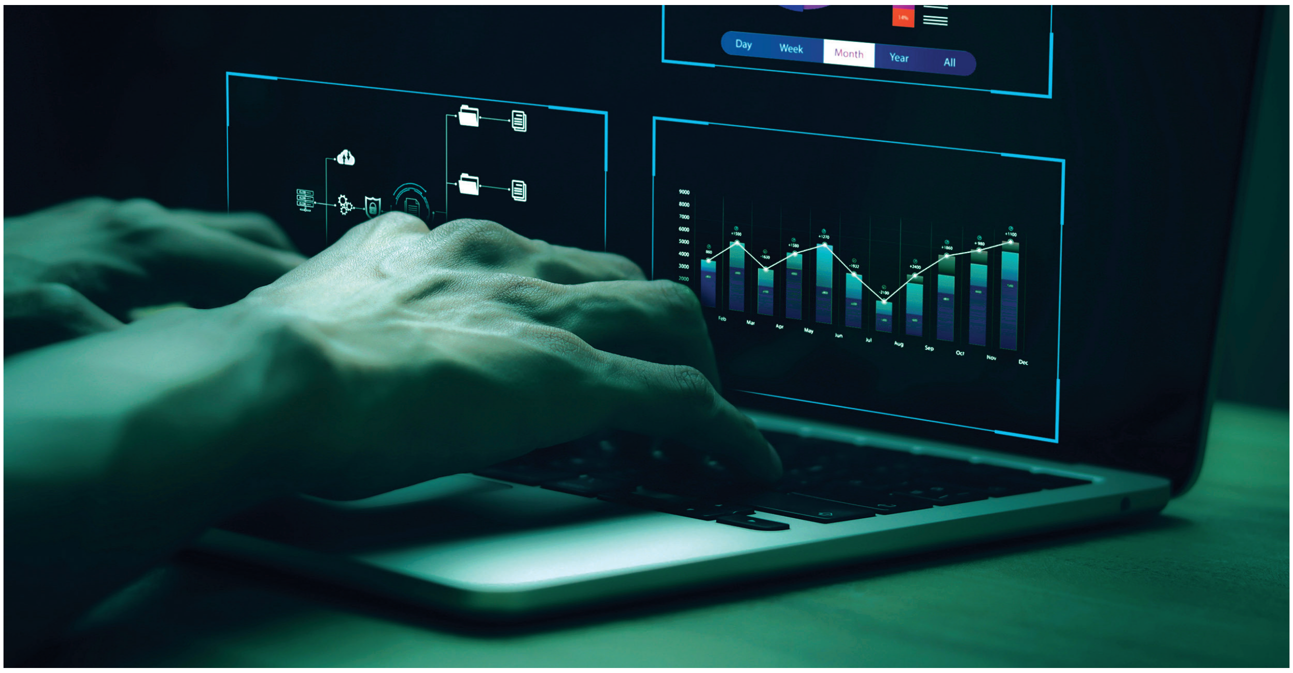
Technology
Understand your technology and how to implement best cybersecurity practices

Processes
Ensure that your organisation has the right processes in place to deal with cybersecurity risks

Alternatively, should the above guides prove not to be appropriate or applicable to an SME there are many specialist IT and cybersecurity advisory firms available that can provide recommendations and solutions.

CONCLUSION

The NIS2 Directive is a way for the EU to ensure all critical services that EU businesses and citizens rely on for their day-to-day lives are appropriately protected from cyber attacks. Even if NIS2 does not impact an SME directly or indirectly through its supply chain, it cannot escape the fact that cybersecurity is fast becoming one of the main business risks facing many SMEs today. Any SME that wishes to remain competitive while reducing its risk profile needs to take cybersecurity seriously. This guide provides the initial building blocks that SMEs can build their cyber defences upon and comply with the NIS2 Directive and many other directives and regulations that will come along.



[28] https://www.ey.com/en_pl/law/the-future-of-cybersecurity-in-europe-NIS2-directive

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.