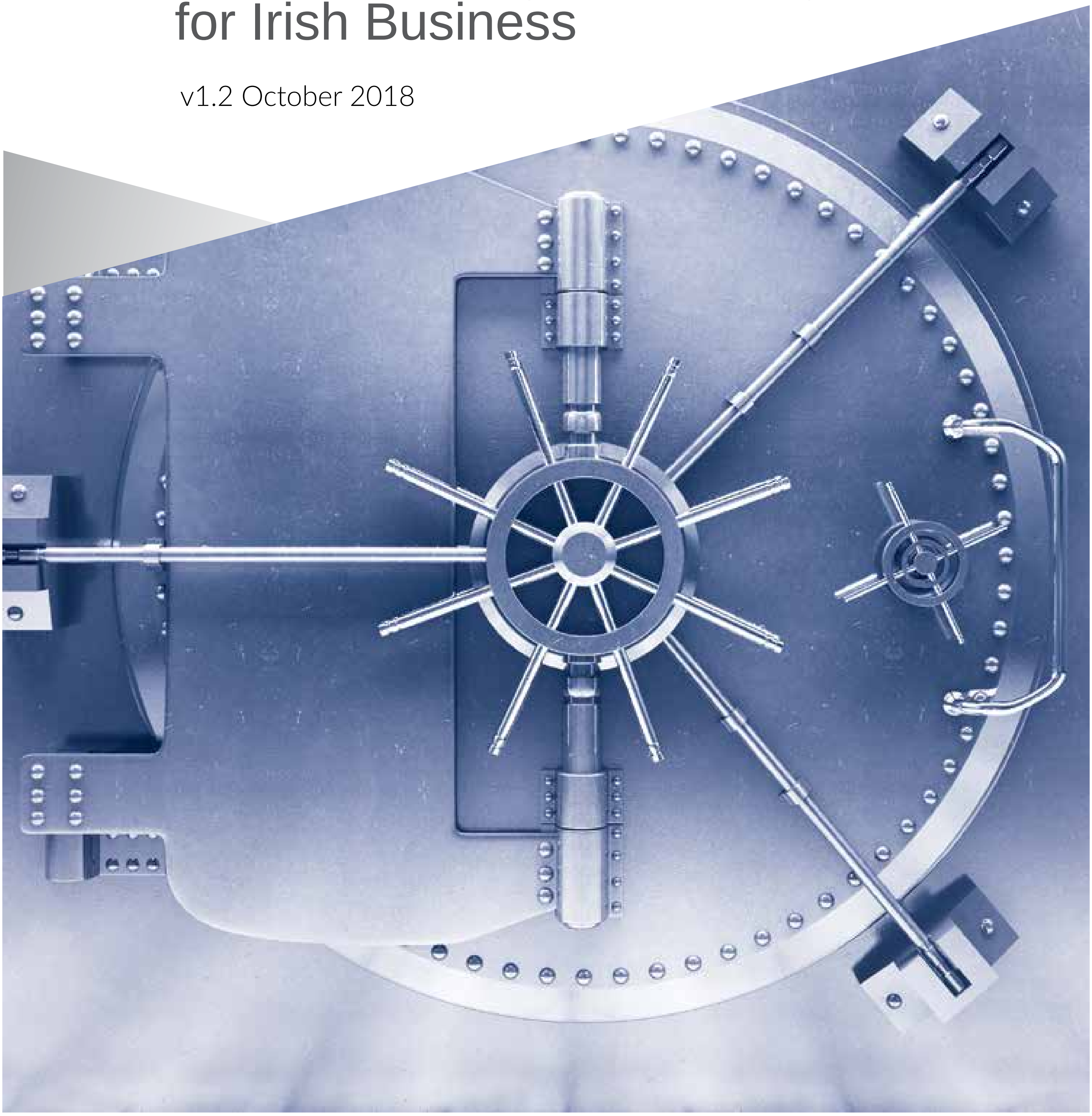
Rialtas na hÉireann
Government of Ireland

12 Steps to Cyber Security

Guidance on Cyber Security for Irish Business

v1.2 October 2018



> “Cyber risk is now one of the most commonly talked about topics as the impact of cybercrimes reaches an all-time high.”

Background

The race to a digital world, and the inherent connectivity of people, devices and organisations, has opened up a whole new playing field of cyber risk. We now have an irreversible reliance on technology in all aspects of our lives and the line between personal and business use continues to blur – we're all in the cloud, whether we like it or not!

Businesses are focusing their strategy on new digital channels to maintain a competitive edge, while consumer-driven Internet of Things (IoT) developments create brand new benefits and risks for digital citizens, including connected cars, medical devices, critical infrastructure, and even smart cities. Hardly a day goes by without reports of another high-profile cyberattack hitting the headlines.

Cyber risk is now one of the most commonly talked about topics as the impact of cybercrimes reaches an all-time high. There are high expectations from institutions, markets, regulators and the public for organisations to protect themselves and their customers at all costs.

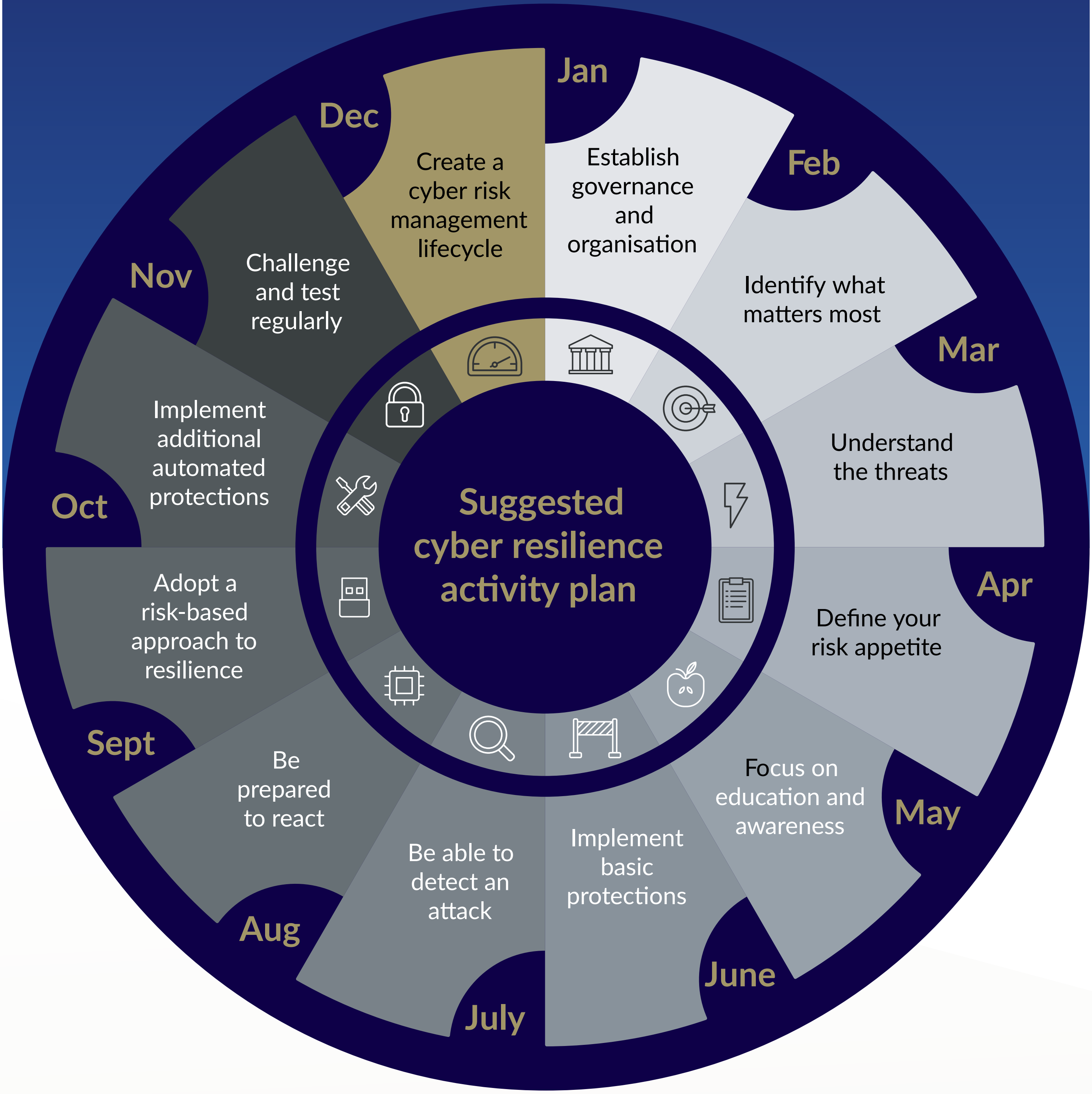
No industry has been spared, with high-impact attacks reported across a broad range of sectors. Cybercrime is now a greater source of revenue for organised crime than drug or arms trafficking. This is big, global business and cyber threats will therefore continue to multiply and evolve rapidly.

Cyberattacks make headlines on a daily basis. It's no longer a question of if your company will be breached, or even when, it's likely to have happened already. The real question is whether you will know and are you prepared?

Overview

This guidance is intended to be used by businesses as a suggested activity plan which may be undertaken on a month-by-month basis over a suggested 12 month period to improve cyber resilience.

Each of the areas may then be revisited in subsequent year's cycle to continuously improve the area in order to keep pace with external developments and standard practice in protecting the business from cyber threats.



Suggested cyber resilience activity plan

Jan: Establish governance and organisation

Feb: Identify what matters most

Mar: Understand the threats

Apr: Define your risk appetite

May: Focus on education and awareness

June: Implement basic protections

July: Be able to detect an attack

Aug: Be prepared to react

Sept: Adopt a risk-based approach to resilience

Oct: Implement additional automated protections

Nov: Challenge and test regularly

Dec: Create a cyber risk management lifecycle

1. Establish governance and organisation

Start by understanding key business drivers and obtaining senior management support for a robust cyber security programme. This is followed by establishing roles and responsibilities, agreeing your strategy, developing policies and standards, and enabling reporting.

2. Identify what matters most

Map business objectives/products/services to supporting people, processes, technology and data infrastructure, and rank by criticality to your business. This includes the ecosystem/supply chain which you operate within, both 3rd parties who supply you and those that you supply.

3. Understand the threats

Understand who might want to attack you, why, and how they might go about carrying out such an attack in order to allow you to focus your efforts on how to respond to the most likely threats.

4. Define your risk appetite

Start to understand what the most likely cyberattacks could cost your business through simplified cyber risk quantification coupled with a cyber risk management framework, which forms part of your overall operational risk management processes. This includes setting your risk appetite and reporting mechanisms to ensure you operate within it.

5. Focus on education and awareness

Establish an education and awareness programme, ensuring all of your employees, contractors and third parties can identify a cyberattack and are aware of the role they play in defending your business against threat actors.

6. Implement basic protections

Secure your business at the technology level by deploying basic protections including secure configuration, patch management, firewalls, anti-malware, removable media controls, remote access controls, and encryption. Establish a Vulnerability Management (VM) programme which manages vulnerabilities from identification through to remediation. Establish an effective Identity and Access Management (IAM) programme to control access to your information. Focus on data protection and privacy (technical and compliance) as well as managing third parties who have access to/ control of your data.

7. Be able to detect an attack

Establish a security monitoring capability which can detect an attack through monitoring activity at various levels within your business. Depending on your industry and available resources, this could be a basic system whereby an alert is generated and emailed when suspicious activity is detected on a firewall, through to a 24*7*365 Security Operations Centre monitoring networks, operating systems, applications and end users.

8. Be prepared to react

Establish a formal cyber incident management team who have been trained in and are following a documented plan, which is tested at least annually.

9. Adopt a risk-based approach to resilience

Establish recovery plans (including comprehensive backups) for all processes and supporting technologies in line with their criticality to the survival of the business.

10. Implement additional automated protections

Start to mature existing capabilities (e.g. automate VM and IAM processes using specialist technology), in addition to implementing complimentary capabilities/technologies such as Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Web Application Firewalls (WAF) and Data Loss Prevention (DLP) systems.

11. Challenge and test regularly

Carry out a cyber incident simulation exercise to test your executive management's ability to manage the response to a significant cyberattack. Carry out an initial red team exercise (essentially a planned attack, carried out by professional ethical hackers) to test your technical ability to detect and respond to sophisticated attacks.

12. Create a cyber risk management lifecycle

Reflect on all areas of your cyber risk management programme and identify areas for ongoing improvement, repeating risk assessments on a regular basis, and considering compliance with relevant regulations.

Practical considerations

All organisations are different and therefore they will necessarily manage cyber risks differently. Some practical considerations include:

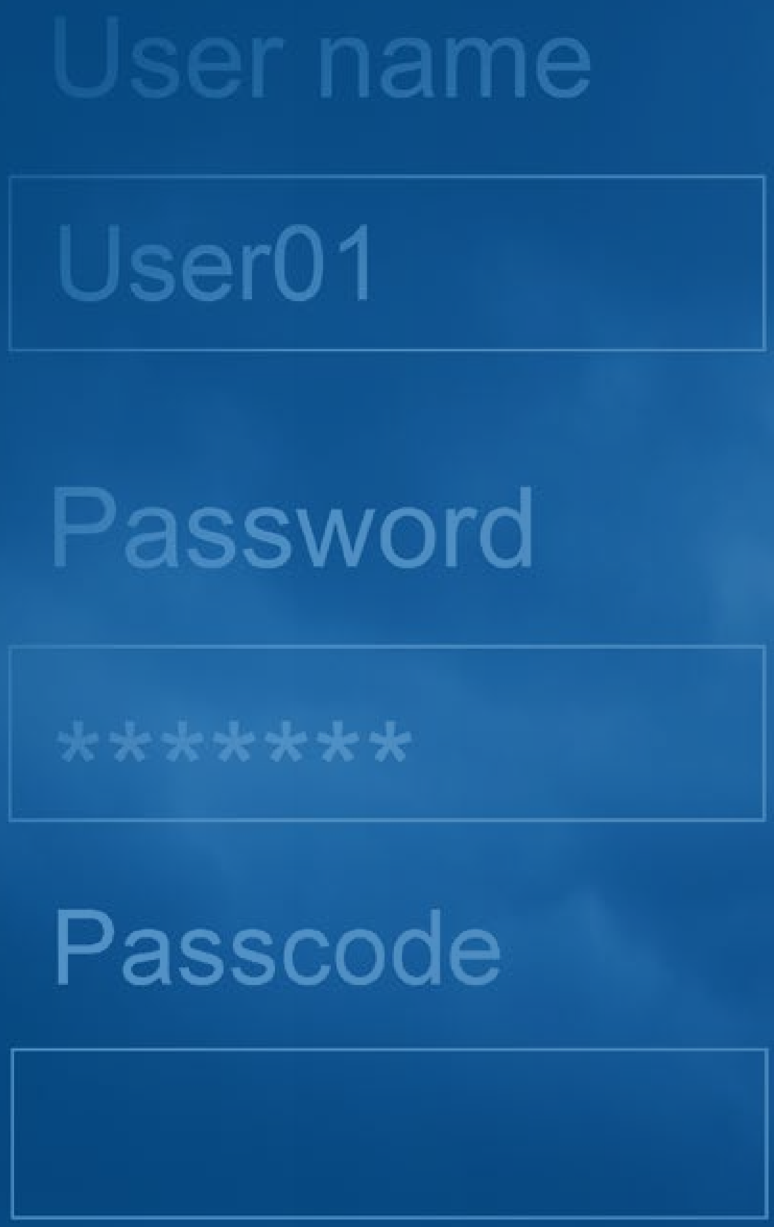
- **The size and complexity of the team required will vary significantly, from small businesses where all responsibility will be borne by one person, to larger businesses who may have one or more people working under each of the areas outlined in this guidance.**
- **The level of capability required will also vary greatly based on the size and complexity of the business and the level of risk it faces and is willing to accept.**
- **Organisation structure and service delivery models will influence security controls and applicability by region, service sustainability goals, hosted or on-premise models and data retention methods. No single standard will apply to all organisations - awareness and consideration of multiple measurable standards will be required to ensure best fit for each organisation.**
- **While technology is typically an important component of any suite of cyber security defences, people with the relevant skills to implement processes and technology are vital. Organisations should consider people first and then focus on what open source and commercial technologies are available to support.**
- **While it is suggested that organisations consider each of these 12 steps on a month by month basis, it is expected that many of the steps will take significantly more than a month to complete.**

These 12 steps provide an overview of suggested steps an organisation may take to improve its ability to prevent, detect and respond to cyberattacks. It comprises of high-level guidance and does not intend to be comprehensive in nature. Organisations should take steps to ensure they apply appropriate cyber security controls based on their risk appetite and not solely rely on the suggested guidance here.

While this document provides guidance across all areas of cyber risk management, smaller businesses, or those at the very early stages of addressing cyber risks, may choose to focus on implementing basic protections (step 6) as their first step. This might include implementing boundary firewalls, secure configuration, patch management, malware protection, encryption and access controls.
These essentials are a minimum baseline for any organisation.

> **“Organisations should take steps to ensure they apply appropriate cyber security controls.”**

“Understanding what and where your digital assets are is an important first step in protecting them.”



Detailed guidance

1. Establish governance and organisation

Any successful programme requires clear governance, defined roles and responsibilities and the support of the most senior management of an organisation. Given the critical impact a cyber-breach can have on an organisation, this is necessarily required for the successful management of cyber risks.

Steps which organisations should consider include:

- **Understand the key business drivers, plans and strategy.**
- **Obtain the support of senior management for a robust cyber security programme to protect the business and help it enable its objectives.**
- **Establish roles and responsibilities (including education and experience standards for key cyber security personnel).**
- **Establish a cyber risk management group which includes all relevant stakeholders.**
- **Develop your cyber risk management strategy.**
- **Establish policy and standards frameworks.**
- **Develop/adopt policies and standards (policies include all areas in this guidance, such as end-user security policy, data protection policy, malware protection policy, remote access policy, etc.), as well as a programme to monitor/measure compliance.**
- **Establish metrics to gather information which enables reporting at both a technical and executive level across all aspects of your cyber risk management programme.**

2. Identify what matters most

Understanding what and where your digital assets are is an important first step in protecting them. After all, if you don't know what you have and where it is, how can you even start to protect it?

Steps which organisations should consider include:

- **Map business objectives/products/services/processes to supporting people, processes, technology (including applications, middleware, major platform and network infrastructure) and data flows (paying particular attention to what information is most important and where it flows). This should include all third parties who manage systems/data on your behalf (also a good time to review contracts/SLA's to ensure they cover cyber risk).**
- **Establish a comprehensive technology asset management programme which includes all of the assets above and ranks/classifies them by criticality to your business in a centralised asset inventory. Note: It may be possible to leverage work already completed for Business Continuity Planning (BCP) and/or Disaster Recovery (DR), as these also need to understand key assets in order to plan for more traditional threats (see step 9)**

3. Understand the threats

Threat actors (cyber criminals, malicious insiders, etc.) vary in capability and sophistication, whilst also constantly changing depending on the value of the prize they seek to exploit. Depending on the nature of your industry, the ecosystem which you operate and the digital assets your business holds, you will be of interest to one or more threat actors. Learning as much as is practical about them is an important step in defending against them.

Steps which organisations should consider include:

- **Establish a Cyber Threat Intelligence (CTI) capability which enables you to identify (through intelligence sources/feeds) and understand the top 5-10 threat actors and likely attack scenarios (these are your key cyber risks) and record them in a risk register.**
- **Understand who the attackers are and what motivates them to attack you (e.g. money, ideology, competitive advantage, etc.).**
- **Understand, in detail, how they might attack you – this typically involves mapping the attack lifecycle for the most likely attacks (e.g. ransomware, fraud, website defacement, etc.).**
- **Use this understanding to focus your efforts on how to best protect the digital assets at risk and your ability to detect and respond to the most likely attack scenarios.**
- **Repeat this risk assessment process on a regular basis to help inform and direct your cyber risk management programme.**
- **Take an active part in industry forums where threat intelligence is shared.**

4. Define your risk appetite

With an understanding of what you have, who might attack you, what they might be after and how they might go about it, the next step is to estimate what the most critical scenarios, if realised, might cost your business. Without a firm understanding of what the risk exposure is in terms of monetary value, it can be very difficult to gauge the right level of investment to reduce your risk. Breaches of regulatory requirements should also be considered here.

Steps which organisations should consider include:

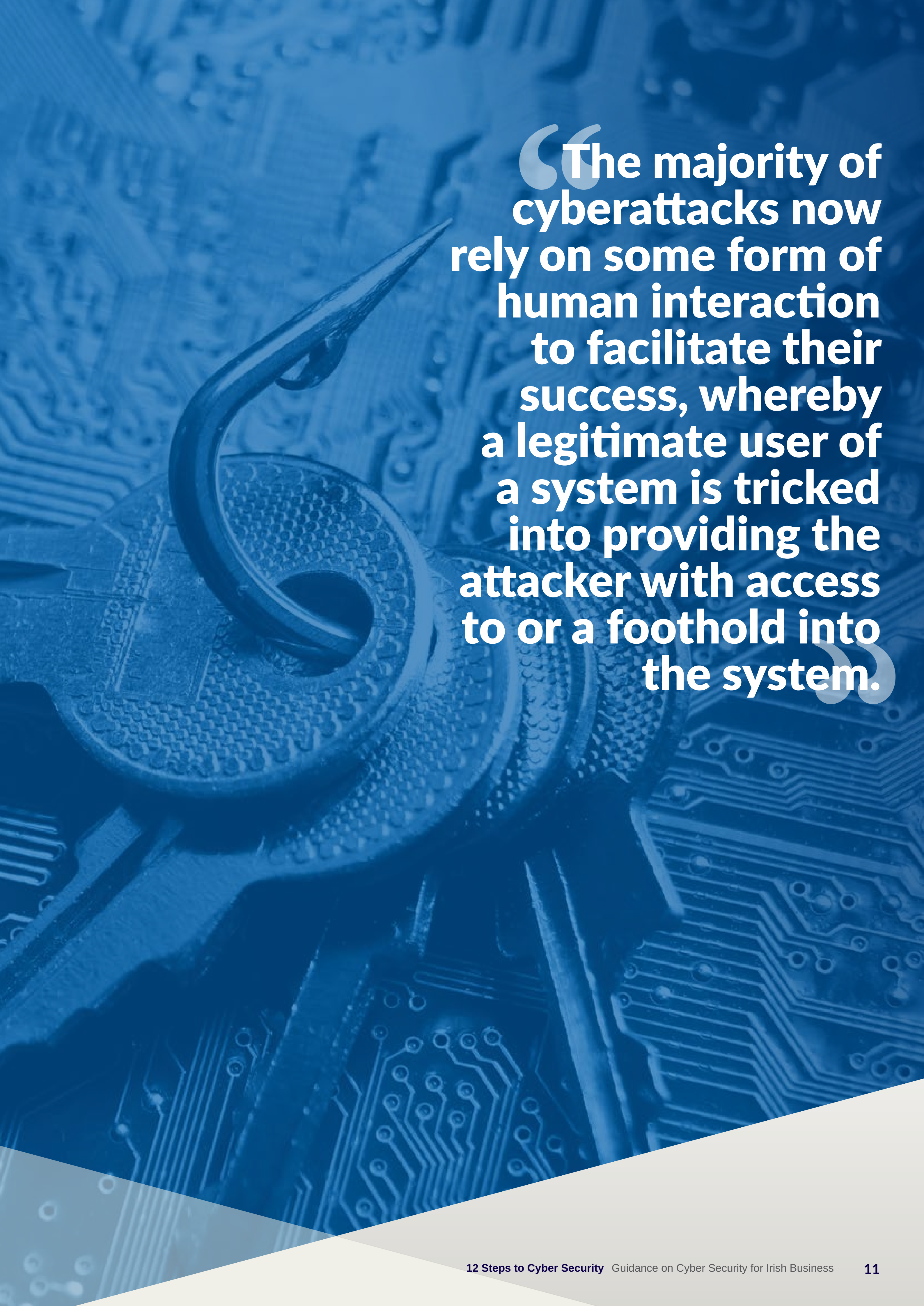
- **Establish a cyber risk management framework which forms part of your overall operational risk management processes.**
- **Use cyber risk quantification to estimate what each of your likely cyberattack scenarios might cost you if the scenarios were realised (often a range of costs is calculated).**
- **Document your cyber risk appetite (knowing the cost of defending risks is critical to determining which risks must be mitigated and which may be allowed to occur) and have senior management approve, ensuring that all stakeholders are aware of and comfortable with the risk to the business, and use this to focus resources accordingly.**
- **For risks which are outside of your appetite, consider activities to reduce (typically through additional controls), avoid (change your business plan/strategy), transfer (typically through cyber insurance), or accept (do nothing but recognise the potential need for business recovery/ resolution).**

5. Focus on education and awareness

The majority of cyberattacks now rely on some form of human interaction to facilitate their success, typically early in the attack lifecycle, whereby a legitimate user of a system is tricked into providing the attacker with access to or a foothold into the system. This comes in many forms of 'social engineering' such as phishing emails, phone calls, and physically bypassing security controls to get into a data centre. Your system users are your first, and most critical line of detection, defence and response.

Steps which organisations should consider include:

- **Establish an education and awareness programme, including at induction and at regular intervals annually (including news-flash alerts during attacks to help prevent the attack spreading).**
- **Extend the programme to include bespoke training for high-risk users, such as executives and those with privileged systems or information access.**
- **Empower and encourage staff to critically evaluate requests and ensure there is a clear channel for suspicious requests to be reported.**
- **Consider contractors and third parties who have access to/control of your systems and data.**



> "The majority of cyberattacks now rely on some form of human interaction to facilitate their success, whereby a legitimate user of a system is tricked into providing the attacker with access to or a foothold into the system."

6. Implement basic protections

In a large number of cases, cyber criminals are able to exploit vulnerabilities due to a lack of basic protections. Most exploits require an IT system which has not been kept up to date with security patches and/or has an out-of-date Malware protection system in place. Implementing basic protections can significantly reduce the risk of becoming a victim of a successful cyberattack, especially at the hands of an unsophisticated cyber-criminal who is only capable of exploiting basic vulnerabilities.

Steps which organisations should consider are spread across five key areas:

Implement technology security protections

- Enable a comprehensive configuration and patch management programme which ensures that systems are patched within an established and agreed timeline based on severity and risk to the business (for example on at least a weekly basis for externally facing systems, with internally facing systems patched on at least a monthly basis).
- Establish basic perimeter and network security through the use of firewalls, internet proxies and network segmentation (to separate untrusted areas such as the Internet demilitarised zone (DMZ) from those internal areas hosting high value systems and information).
- Establish comprehensive anti-malware protection, both at the host (on every computer, server, mobile device, etc.) and network level (at email/web gateways, etc.) – make sure it's updated in real-time and then proactively scan for malware in real-time and on a regular scheduled basis (daily/weekly).
- Establish removable media controls, whereby use of removable media (such as USB keys) is restricted, enforces encryption and is scanned for malware on each use.
- Adopt secure configurations for all of your technologies - lock down operating systems and software to only provide the services required, thus reducing the attack surface.
- Establish remote access/remote working controls, including secure access to systems and controls on the devices which may be used to access your systems (they should be at least as secure as those directly connected to your systems).
- Establish a data security programme, which focuses on how data is stored and secured in your organisation. This involves mapping of data locations and flows at step two above, and then focusing on how it is protected at every step in its lifecycle. This includes access controls (see IAM below) as well as using encryption. At a minimum, sensitive data should be encrypted in transit over untrusted networks like the Internet (using encrypted containers and/ or encrypted communications channels) and consideration should be given to encryption at rest. Full disk encryption should be used on all mobile devices, such as laptops and removable media (USB keys).
- If you develop your own software or engage a third party to do so on your behalf, ensure that they incorporate security through the whole Systems Development Lifecycle (SDLC) from initial design through to deployment. This can save significant resources by eliminating risks very early in the process.

Vulnerabilities are weaknesses in a system which can be exploited by an attacker to gain unauthorised access to that system. They come in many forms and are typically only discovered long after a system has been deployed. New vulnerabilities are discovered every day, so it's vital to continually assess your systems to see what vulnerabilities exist.

- Organisations should establish a comprehensive Vulnerability Management programme to firstly search for and identify vulnerabilities and then manage them through qualification (how will they impact my systems?) and treatment (can we apply a configuration change or security patch to remediate them?).
- A centralised reporting capability is required to track the risks posed by vulnerabilities as well as showing progress in treating them. Vulnerability Identification (VI) should encompass both automated and manual discovery methods, from automated scanning through to manual penetration testing and social engineering exercises

Establish an Identity and Access Management programme starting with a centralised identity store and a robust process to manage access to all systems from initially granting access through modification and eventual revocation of access. Basic features include:

- Adopt the principle of least privilege – only give people access to what they need to do their job, and no more.
- Manage privileged user access – only specifically trained and vetted individuals should have access to administer systems and consideration should be given to using separate access controls (such as tokens) for such access.
- Focus on critical systems first - Establish controls around access to sensitive data and financial systems.
- Determine the best method and level of authentication for your organisation – this may be usernames and passwords for non-sensitive systems, through to multi-factor tokens for sensitive systems (recommended for remote access).
- Where passwords are in use, they should be of sufficient length and complexity to make them very difficult to guess (even by artificial intelligent systems used to guess millions of passwords a second) – they should be changed on a regular basis, particularly for business critical systems.
- Establish a process to regularly review who has access to what – verify that access is still required or revoke it if it's not.

Personal data held internally (such as employee records) as well as customer/third party data (such as customer names and addresses) is regulated by the Data Protection Act 2018 and/or the EU General Data Protection Regulation (GDPR). Organisations that hold personal data should consider the privacy impact of their business processes and their supporting systems and data, and establish an effective privacy programme to ensure you are compliant with relevant regulations.

During step two ('Identify what matters most'), establish and record details of all of your processes, systems and data which might be managed by a third party. Establish a third party management programme, utilising a central register of third parties who have access to/control of your systems/data, which has been prioritised by risk/criticality, and ensure that appropriate due diligence has been performed on these parties to ensure they manage your data with at least the same level of security that you do. This includes cloud hosting/systems providers, which many businesses outsource large portions of their technology systems to.

7. Be able to detect an attack

It is accepted that most organisations will be attacked, if they have not been already. Threat actors are many and sophisticated, and dedicated attackers have a high chance of breaching your defences given enough time and persistence. Detecting that you are under attack is the first prerequisite to enabling any form of response.

Steps which organisations should consider include:

- **Decide which activities on your systems should be logged and how long those logs should be retained for – maintaining comprehensive audit trails through activity logging is key to being able to monitor them and/or establish what happened when a successful attack occurs.**
  - Basic logging includes access (login/logout), remote access, connections by third parties, (failed) attempts to access your systems, alerts from anti-Malware systems, and internet access. Monitoring is entirely dependent on the depth and quality of the activities being logged, which of course brings with it requirements for secure storage of logs and a clear retention policy/process.
  - More advanced/complete/thorough logging can include activities inside specific applications (such as accessing sensitive data and/or committing financial transactions), connection attempts within your systems, and Intrusion Prevention/ Detection systems (IP/DS). This enables better correlations to be made informing towards root cause of past events and building knowledge to protect for future instances.
- **Once logging capabilities have been established the next step is to monitor the logs for suspicious behaviour – this includes the people, processes and technology required to detect an attack through monitoring network (perimeter, host and traffic in transit), operating systems, applications and user accounts.**
  - Basic monitoring might be as simple as an alert being emailed to an IT administrator from critical systems when a certain activity is detected (e.g. more than three failed login attempts on a critical system, or Malware detected on a laptop).
  - A Security Operations Centre (SOC) is typically deployed for larger and/or higher risk organisations, whereby a dedicated team monitors networks, operating systems, applications and end users on a continuous basis.

> “Detecting that you are under attack is the first prerequisite to enabling any form of response.”

8. Be prepared to react

Attacks will occur, therefore having a capability to respond is crucial. Organisations who are well-prepared and rehearsed for this eventuality will typically experience a greatly reduced impact.

Steps which organisations should consider include:

- **Establish an incident response and investigations capability including a formal team, who have been trained in and are following a documented plan, which is tested at least annually.**
- **Such a plan includes how an incident will be identified/detected, categorisation and classification of the incident, how it will be contained, how the root cause will be investigated and how the organisation will recover from the incident.**
- **Plans should include all stakeholders, such as business owners, legal, HR, PR/communications/ marketing, risk/compliance, IT/incident management as well as any 3rd parties which you might rely upon for capability you don't have in-house (e.g. technical forensics, legal, communications, etc.)**
- **Plans should include considerations for gathering evidence, reporting to relevant law enforcement agencies, and recording/reporting on incidents in general.**
- **For regulated entities (financial, data protection, etc.) - understand your notification obligations under the relevant regulations, such as the GDPR, Central Bank rules, and the Network and Information Security Directive (NISD).**

9. Adopt a risk-based approach to resilience

Resilience is about the ability of an organisation to recover from disruption, including those caused by cyberattacks. When the inevitable cyberattack does occur and damage and/or disruption is inflicted, an organisation's ability to recover quickly will be the key to its survival.

Steps which organisations should consider include:

- **Establish a team who are responsible for Business Continuity Planning (BCP – also known as Disaster Recovery or DR), who have been trained in and are following a documented plan, which is tested on a regular basis (typically at least annually).**
- **Establish recovery plans (including comprehensive backups) for all business processes and their supporting technology systems, along with agreed time to recovery which is line with the criticality of the systems.**

> “Attacks will occur, having a capability to respond is crucial.”

10. Implement additional automated protections

Step six provided guidance in relation to basic protections which an organisation might consider implementing to defend against threat actors. Once these have been implemented, along with the ability to detect and react, organisations should consider additional protections to further reduce the risk of cyberattacks. These should be considered in line with steps three and four, so that additional protections are focused on reducing the greatest risks further.

Steps which organisations should consider include:

- **The basic protections outlined at step six above may be matured focusing on broader coverage across all systems and functional business areas.**
- **Additional technologies, such as Intrusion Prevention Systems, Intrusion Detection Systems, Web Application Firewalls and Data Loss Prevention systems will provide enhanced capabilities.**
- **Technologies which support IAM and VM, and in particular the centralisation and automation of IAM and VM processes will deliver efficiencies and cost savings. Consideration should be given to establishing a formal role/function which considers security architecture in all aspects of your organisation's IT programme. It is particularly important for organisations who develop software/systems that security is embedded at all stages throughout the Systems Development Lifecycle.**
- **A cyber risk reporting programme may be established/improved to include regular reporting both within IT and cyber security, and also to business units and senior management.**

11. Challenge and test regularly

Once an organisation is comfortable that they should be able to protect against, detect and react to their currently understood cyber threats, the next step is to test that capability in order to gain some assurance that controls are effective.

Steps which organisations should consider include:

- **If not completed as part of step eight ('be prepared to react'), organisations should carry out cyber incident simulation exercises at least annually to test the ability of the organisation to respond to a cyberattack – these should be carried out at the executive and tactical response team levels.**
- **Red Team exercises should be carried out at least annually to test the technical ability of an organisation to defend, detect and respond to sophisticated attackers.**
- **Pro-active hunting of threat actors who may already be in your systems should be carried out on a regular basis.**
- **The ability of your entire workforce to identify, detect and respond to threat actors should be tested at least annually through social engineering exercises (such as phishing exercises) – this will help to reinforce your education and awareness programme.**

Note: Standard VI activities such as routine penetration testing and security reviews of new systems/applications will form part of your VM programme. The activities outlined at this step are designed to test your ability to defend, detect and respond to threat actors, rather than identify vulnerabilities which they might exploit. It is likely that new vulnerabilities will also be identified as part of these activities, and should be fed into your VM programme.

12. Create a cyber risk management lifecycle

Cyber risks will continue to evolve, along with an organisation's exposure to the risks. Establishing a cyber risk management lifecycle is essential for effective ongoing management of cyber risks, while making the task part of business as usual.

Steps which organisations should consider include:

- **Reflect on all areas of your cyber risk management programme and identify areas for ongoing improvement based on the results of step eleven.**
- **Repeat steps three and four above at least annually and/or as cyber threats change, and/or as your organisation evolves.**

National Cyber Security Centre

Email: certreport@dccae.gov.ie
Website: www.ncsc.gov.ie
Address: 29-31 Adelaide Road, Dublin, D02 X285

Rialtas na hÉireann
Government of Ireland