KPMG

Cyber Resilience

Protecting your business

kpmg.ie

#CyberResilience

Contents

Introduction

Michael Daughton
Partner
Risk Consulting

Ensuring that you are as prepared as possible for a cyber event is no longer optional – it has become a strategic imperative for all business leaders.

Over the past few decades technology, and particularly the internet, has provided a remarkable platform for business growth and innovation. It has disrupted long-standing industries, killed off established brands, allowed new players to emerge and it has transformed the way business is conducted.

This has created huge opportunities for new ideas and fresh thinking – but it has brought with it many risks as well, particularly as companies become more interconnected and reliant on complex IT systems.

Globally, cybercrime is now estimated to cost businesses €330 billion a year and cyber risks are among the top issues businesses have to consider when it comes to their resilience and continuity planning. In the past year both the Irish Government and the World Economic Forum have cited cybercrime among the highest of all global risks in terms of impact and likelihood of occurrence.

New legislation such as the General Data Protection Regulation (GDPR) places an even greater responsibility on businesses to be cyber aware, with significant penalties for non-compliance.

This report outlines some of the most common cyber risks encountered, frequently made mistakes in dealing with cyber events, insights on how your business can become more cyber resilient, and finally an overview of the legal landscape, in particular, recent legislative changes that all businesses need to act upon.

I hope that you find this report to be a valuable guide in developing your businesses cyber security policies and we look forward to providing you with regular updates on the cyber issues you need to consider to protect your business.

Michael Daughton

Michael Daughton

Cyber - Am I a Target?

Instances of high-profile cyber-attacks seem to be proliferating all the time. Amongst the factors driving this particular risk is the fact that attacker capabilities are growing, the connectivity of devices is mushrooming, the reliance on third parties and supply chains is growing and cost issues can mean IT resources are under pressure.

This can result in a 'readiness gap' in which the threat is increasing while companies' preparedness struggles to keep up. Every institution needs to be able to detect and respond to cyber security threats, but with information processes about threats, risks and solutions tending to be dominated by technological buzz words, there is often a sense of mystery around what cyber security means for senior management.

Why should I be concerned, I have nothing of interest or value?

Although many organisations think this way, every organisation is a potential victim. All organisations have something of value that is worth something to others. If you openly demonstrate weaknesses in your approach to cyber security by failing to implement basic controls, you will experience some form of cyber-attack.

The cyber-attacks that frequently dominate the headlines can distort how businesses perceive the risks associated with cyber. There is a natural tendency to focus on the unusual or memorable, but this doesn't always reflect the reality of the cyber risks facing companies every day.

So who is interested in attacking me?

- Cyber criminals interested in making money through fraud or from the sale of valuable information for use in identity theft and extortion.
- Nation State Actors, interested in gaining an economic advantage for their countries and its commercial interests.
- Hackers who find interfering with computer systems an enjoyable challenge.
- Hacktivists who wish to attack companies for political or ideological motives.
- Employees, ex-employees or those who have legitimate access, who can cause damage or loss either by accidental or deliberate misuse of assets.

Your organisation does not have to be specifically targeted to become a victim. Un-targeted attacks are also common. These attacks indiscriminately infect as many devices, services or users as possible. Methods of infection include phishing emails, ransomware and visiting a website that has itself been compromised to infect visitors.

Developing a Proactive Cyber Defence Programme

In May 2018, the new EU General Data Protection Regulation ("GDPR") will come into force. The GDPR contains a number of new protections for EU data subjects and threatens significant fines and penalties for non-compliant data controllers and processors. Fines for non-compliance can be up to 4 percent of an organisation's global turnover or €20 million, whichever is higher.

One of the material changes impacting data controllers under the GDPR relates to the mandatory notification of data breaches to the relevant supervisory authority. Under the GDPR, a "personal data breach" is "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*" Notice must be provided to the relevant supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it." If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay. These new obligations are integral to the principles of accountability and transparency that run through the GDPR.

Types of personal data breach:

Insider leak: a trusted individual with privileged access steals data.

Loss or theft: usb drives, laptops, computers, smartphones, files, and other physical properties are lost or stolen.

Unintended disclosure: through mistakes or negligence, sensitive data is exposed.

A data breach or other sort of cyber event is not just an issue for those whose data could be affected, it can also cause significant reputational damage for an organisation and impact both consumer and investor confidence. This is forcing companies that handle EU citizens' data to undertake major operational reform, one of these operational reforms will be in relation to how an organisation handles incident response and breach notification.

Incident response describes the process by which an organisation handles an incident, such as, a data breach or cyberattack, including the way the organisation attempts to manage the consequences of the attack or breach.

Shining a spotlight on the ten common incident response mistakes can help organisations determine if their incident response plans / teams are capable of solving, rather than exacerbating, their security problems.

Top 10 Incident Response Mistakes

#1: Plans are not tailored to the organisation

Many organisations implement boilerplate incident response plans that itemise, in extensive detail, every step that should be taken to investigate a potential incident. While this may feel thorough and reassuring, it can often overcomplicate response procedures and slow down or work against investigations. Off-the-shelf plans are often outdated and ineffective against evolving threats and changing technology.

Advice: Establish policies, processes, and procedures that are tailored to your culture, environment, response personnel, and most importantly, business objectives. Documentation should be concise, and should evolve constantly to remain current with both data protection trends as well as shifts in business objectives.

#2: Plans are only used in real-world incidents

In information security, planning only goes so far. Organisations create comprehensive incident response plans but sometimes do not test them until a real event occurs, only to find they fail at the first step. Additionally, many organisations view creating an incident response plan as a one-time event as opposed to an evolving process. As a result, plans have incorrect information regarding tools and people, or detailed steps that do not work or are out of order.

Advice: Put plans into action with regular frequency before a real incident occurs similar to the way fire drills and business continuity plans are performed and tested. Lack of exercising an incident response plan could result in increased response time, confusion, and worst of all, a data breach.

#3: Teams are unable to communicate with the right people in the right way

As many IT security organisations are characterised by segmented functions such as vulnerability scanning, patching, and system administration, it can be a major challenge to find, coordinate and communicate with the key parties involved when responding to an incident.

Advice: A centralised communication dashboard, where the incident response team can post details about the current investigation can help limit the disruptions of constant e-mail messaging, which can overwhelm inboxes and lead to missed messages or conflicting information. Additionally, this dashboard system can be configured to limit access or add people as needed, without sending duplicative e-mails.

#4: Teams lack skills, are wrong-sized, or mismanaged

All organisations face challenges when it comes to choosing the right personnel to staff the incident response team. With limited security budgets, small organisations may assign incident response duties to system and network administrators, who possess technical knowledge and historical understanding of how systems operate, but no experience making business-impacting decisions amid a crisis or breach. On the other hand, large organisations may struggle to allocate the most efficient number of resources to the incident response team, assuming more personnel equals greater capability. This can lead to overlapping efforts.

Advice: Closely evaluate the need for additional training or internal recruiting assistance to help foster the proper level of experience on the incident response team. In addition, strong leaders who oversee the team should clearly define roles and responsibilities, promote greater collaboration, and improve communication both within, and beyond, the team.

#5: Helpdesk activities can destroy critical evidence

From strange computer behaviour to frequent account lockouts to multiple antivirus alerts, computer issues that may signal a malicious code infection are often first reported to the helpdesk. If helpdesk staff members are not well versed in the needs of incident responders, their work to fix user issues may destroy valuable evidence. For example, installing software, running antivirus or cleaning tools, or adjusting system settings can overwrite information that may be invaluable to incident responders. Piecing together the chain of events can be impossible, especially if the initial actions were not documented. Organisations who use subcontractors as their IT helpdesk should make sure their helpdesk staff are aware of the indicators that need the involvement of the incident response team.

Advice: If helpdesk staff members suspect a user issue may be caused by malicious code, they should firstly notify their incident response team. Once the incident response team is notified they may want to capture a memory image of the system prior to making any other changes. The helpdesk should also be trained to document their activities in case their actions become part of an investigation.

#6: Plans are only used in real-world incidents

Organisations may see that their incident investigation and remediation processes experience unexpected delays, or even grind to a halt, if the tools teams rely on to unearth information about affected systems and people are mismanaged or misused. Even the latest and greatest technology solution can fail to provide a consistent, reliable output without proper planning, investment, and maintenance.

Advice: Maintain an inventory of tools in a centralised location and establish processes to help ensure timely licence renewal and functional component upgrades. Team members should be trained across the entire tool set on an ongoing basis. Finally, tools should be regularly assessed to determine if they can address the most current threats.

#7: Data pertinent to an incident is not readily available

When information containing the relevant details of an attack does not exist or is not readily available, there is a negative effect throughout the incident response process. Ultimately, the incident response team struggles to assess the impact, contain the damage, and communicate effectively to management.

Advice: Organisations need to understand what data sources they have, what data they are capable of producing, and how they manage their data. Engaging technology owners and evaluating the asset management system are both good ways to uncover the full range of potential data sources. In addition, the incident response team should identify signalling events (e.g., failed authentication, logs purged, interactive log-on, etc.) that could provide contextual information about an incident, and establish processes for assembling, storing, and making sense of this data.

#8: There is no "intelligence" in the threat intelligence provided to incident responders

Threat intelligence (TI) is a buzz-worthy topic in IT security; and threat intelligence products are flying off the shelves, but many organisations find that purchasing all available threat feeds does not result in complete threat detection. Often, incident responders are overwhelmed with file names, IP addresses and other indicators, but given little or no context as to how these indicators may affect their organisation.

Advice: Integrate threat intelligence into incident response and actively work with your TI vendor to assess if the intelligence is actionable and valuable for your organisation.

#9: The incident response team lacks authority and visibility in the organisation

Internal conflicts can work against the incident response team's efforts, waylay the response process, and prevent timely incident resolution. It is rare that incident response teams operate with the ultimate authority to make the business changes to secure the organisation. Rather, they must escalate issues to management to receive the necessary traction, sometimes as incidents worsen.

Advice: Management must fully support the incident response team, its mission, and its activities during an investigation. Incident response should be communicated and marketed as a service that maintains the integrity of the organisation, not as the group that creates more work. Additionally, the incident response team should engage other teams to nominate a primary contact to facilitate participation in the incident response process.

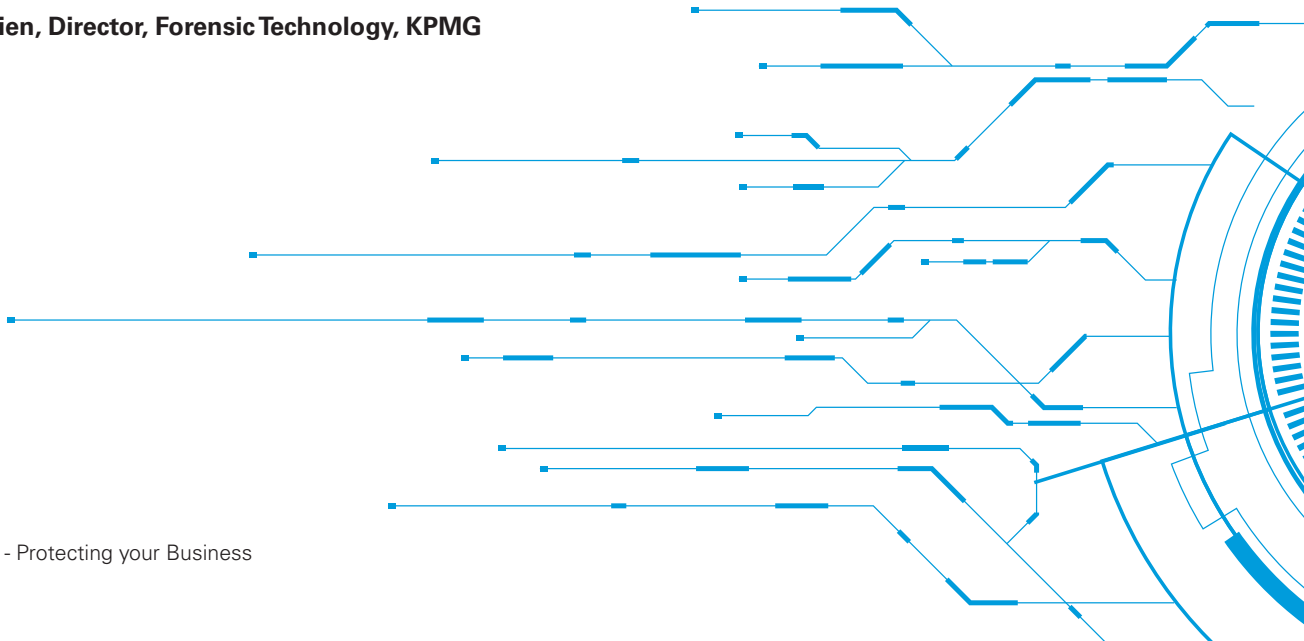
#10: Users are unaware of their role in the security posture of the organisation

Exploiting users is one of the most common, and easiest, ways that criminals compromise organisations. Finding a vulnerability that gives an attacker full access to a network can be a lot of work, but crafting an e-mail message that convinces a user to run malware is extremely easy. Unfortunately, educating users about threats only goes so far.

Advice: The security management team should continuously educate users not only about common exploitation practices, but also about information security's role within the organisation. By doing so, users can be active participants in security. They will know where to turn to and trust the process, rather than attempt to solve security problems on their own by installing untrusted tools and potentially causing greater problems across the network.

The operational reform that many organisations are forced to address as part of their GDPR obligations and readiness programmes should be viewed as an opportunity to develop a proactive and comprehensive cyber incident response programme. With the growing cyber threat that is part and parcel of modern day business, such programmes are a critical element of information security. Addressing these common incident response mistakes will ultimately strengthen your incident response plans / teams and mitigate your risk of failing to notify the supervisory authority of a "personal data breach" under the GDPR within the designated 72 hour period.

William O'Brien, Director, Forensic Technology, KPMG



Cyber Resilience - the New Hero in Information Security?

Globally, just over two in five CEOs say they feel prepared for a cyber event, up from one in four last year. In the Republic of Ireland, almost nine out of ten CEOs feel fully prepared for a cyber event whilst a significantly lower one in five (20 percent) express similar attitudes in Northern Ireland, according to the 2017 KPMG Irish CEO Outlook Report.

With spending on cyber security expected to top the US$113 billion mark by 2020 and reports of data loss making the headlines daily, why in the age of mature cyber security products do large scale breaches continue to happen?

Evolving risk

Cyber criminals are employing tools of an increasing complexity and deploying them in an ever more sophisticated manner using the same enterprise levels of artificial intelligence and machine learning solutions that security professionals aspire to possess. The emergence of super strength encryption on readily available communication apps and the layered security model of the "dark web," hosting online stores for criminal goods and services means that the potential for detection has decreased dramatically.

The prevalence of point and click cyber weapons, loaded with an array of ransomware, phishing and denial of service botnets, easily obtained on the dark web has created a lucrative "gun for hire" marketplace on the internet. Distance, time of day or innocence of the target have no relevance if the fee is paid.

A collective of nation state actors, organised criminals, hacktivists and so called "script kiddies," sometimes hiding under cover of each other's labels are the main actors in this cyber theatre of war.

This cyber arms race comes at a much higher cost to the defender as most of the capability of the attacker is either stolen or bought to order, not learned or developed in the traditional way that mainstream cyber security professionals have evolved whilst deploying multiple solutions to plug the security gaps.

"This cyber arms race comes at a much higher cost to the defender."

Risk & Innovation

Cybercrime is consistently listed as a top concern of CEOs worldwide but in Ireland it does not explicitly feature, despite emerging technology appearing as the number five risk. How can we separate the risk of emerging technology, allowing us to innovate and transform business yet not consider the security risks as an essential business operation? Over half of CEOs (56 percent) in the Republic of Ireland and almost the same (48 percent) in Northern Ireland believe they need to do more to combat cyber security 'fatigue' in their organisation.

In the report Safra Catz, CEO of multinational computer technology company Oracle says, "The hit that wipes you out is the one that comes from the side, so you need to keep an eye on all directions."

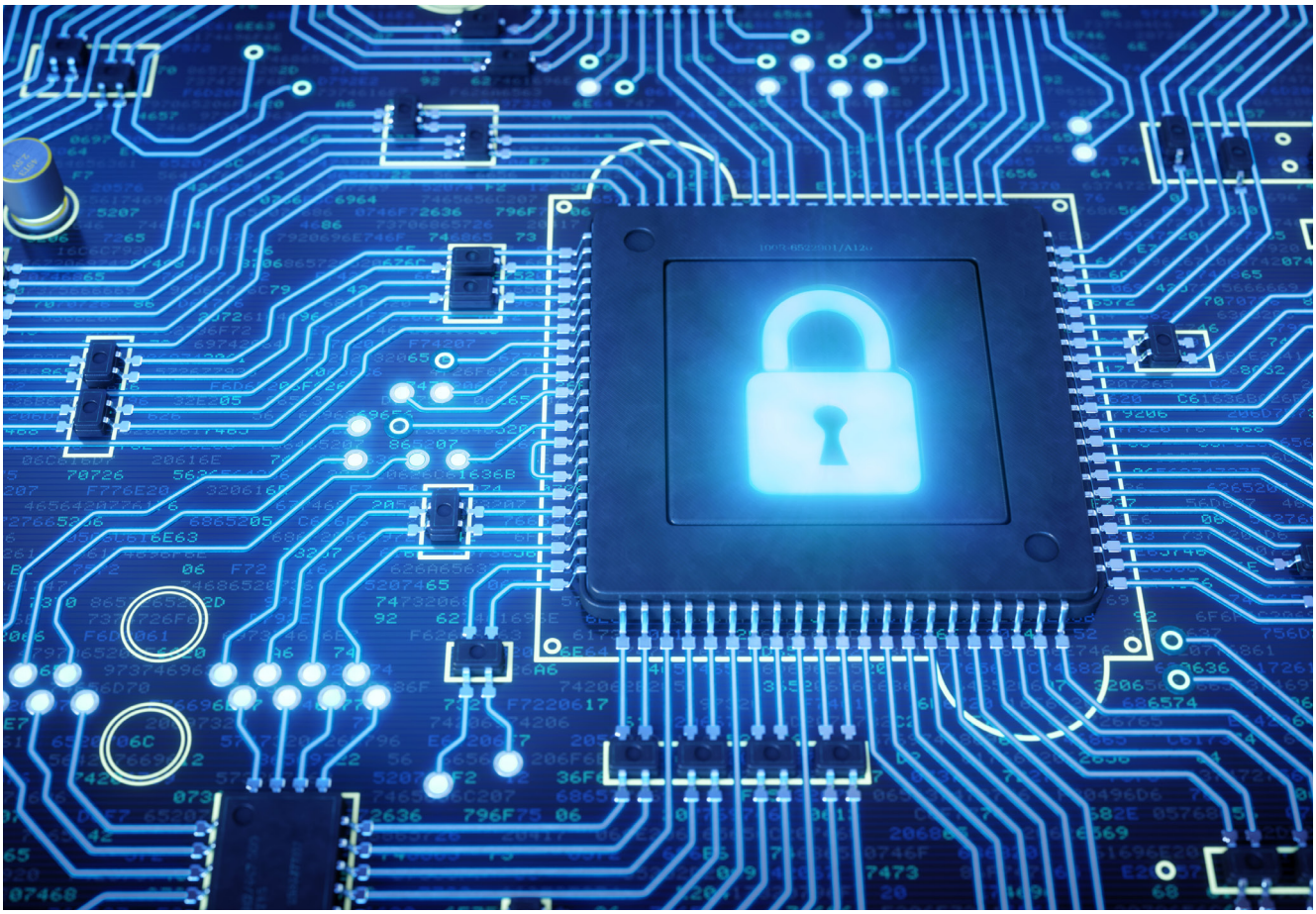
Wise words, and with this in mind it is possible that the current approach to securing our technology has not fully lived up to expectations and that no magic bullet or box exists to solve the end to end multidirectional attack vectors employed with ever-more efficiency and effectiveness by the modern cyber criminal.

Cyber security professionals have repeated the "defence in depth" mantra for well over a decade, and the current theme is focused on the people, process and technology aspects within the cyber ecosystem.

Evolving from those traditional models is a new way of considering the overall approach to securing our assets designed to reduce the risk of a "hit" whichever direction it comes from, this approach is called cyber resilience.

Cyber resilience is being able to prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events in the online world. Cyber security is a key element of being resilient, but cyber resilient organisations recognise that operating safely online goes far beyond just technical measures. By building an end to end understanding of cyber risks and threats, and aligning them to business objectives, they are able to take the appropriate measures to protect their assets and maximise the opportunities available online.

Cyber resilience also creates opportunities to increase the security awareness of staff therefore reducing their riskier behaviour elements; and creates a clearer line of sight between business objectives, when set out in a digital strategy and cyber security implementation.



How can I implement cyber resilience in practice?

Cyber resilience is by its nature a process of continual refinement and relies on organisations understanding the quantity, sensitivity and location of the assets they are trying to protect. The new General Data Protection Regulation (GDPR) in force from May 2018 will mandate this approach to information asset management on all personally identifying citizen data.

The process for achieving cyber resilience can be best thought of as a framework with five pillars: identify, protect, detect, respond, and recover. You can evaluate each pillar of your organisation's cyber security strategy, reduce the risk of adopting a static security posture in an ever-evolving threat landscape; and ensure that business rules continue to be applied in the way they were designed, via the use of technology.

For example, looking at the pillars for identify, protect and detect, the use of vulnerability assessments can expose weaknesses that exist and countermeasures can be deployed early to mitigate the risk. By evaluating the risk posed by each weakness identified and addressing the weaknesses that are most critical, you should be able to improve your preparedness for an attack. With each scheduled cycle of assessments, the security strategy is re-evaluated, and since every organisation has unique systems and different security needs, the results of each series of assessments is measured against the current threat environment and the acceptable risk level for the organisation, rather than a relatively generic series of standards and checklists.

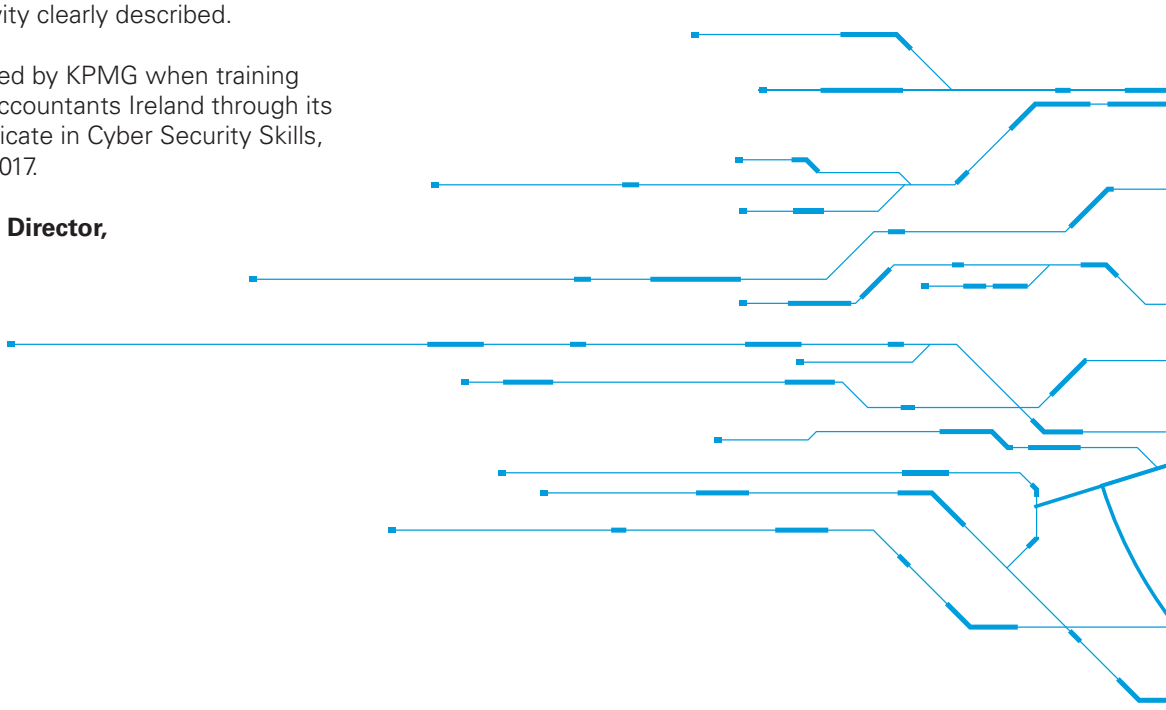
This approach is confirmed by the National Cyber Security Centre (NCSC) for Ireland who are launching a 12 Steps to Cyber Security approach, employing a number of key building blocks proportionate to all sizes of organisation, with an end to end continual assessment of each activity clearly described.

It is also the approach used by KPMG when training members of Chartered Accountants Ireland through its recently developed Certificate in Cyber Security Skills, launched in September 2017.

Tony Hughes, Associate Director, Risk Consulting, KPMG

> **"The hit that wipes you out is the one that comes from the side, so you need to keep an eye on all directions."**
>
> **Safra Catz, CEO, Oracle**

> **"Every organisation has unique systems and different security needs."**



The General Data Protection Regulation and Cyber Security

> **"People ask me all the time, 'What keeps you up at night?' And I say, 'Spicy Mexican food, weapons of mass destruction, and cyber-attacks."**
>
> **Dutch Ruppersberger (U.S Congress Representative)**

Since the transposition of the 1995 Data Protection Directive into Irish law, rapid technological developments have brought a series of new challenges for data protection. This has fundamentally changed even the most routine of business processes with the scale of data sharing and collection increasing dramatically. New technologies and innovations allow companies and public authorities to use personal data on an unprecedented scale. Individuals are also increasingly making personal information available publicly through social media channels which were never envisaged by the 1995 Directive. This evolution has necessitated the need for a stronger, more coherent data protection framework. As stated in Ireland's National Cyber Security Strategy 2015-2017, the "evolution of attack vectors and threats has resulted in previous network security technologies becoming less effective and the adoption of a defence in depth approach."

The European economy thrives on the free flow of information across borders using the latest technology. However with new technology comes new risks especially as organisations become more interconnected and reliant on complex IT systems. In business, this translates into increased exposure for organisations to the risk of cyber-attacks and greater risks for data to be lost, stolen, corrupted or accessed. Whilst technological progress has seen the development of highly intelligent security measures to protect information from attack, the converse has also occurred in that cyber-attacks have, as a result, become more sophisticated, frequent, targeted and difficult to detect. Both the World Economic Forum, in its Global Risks Report 2017, and the Irish Government's 2016 National Risk Assessment cited cyber-crime among the highest of all global risks in terms of impact and likelihood of occurrence. According to the 2016 National Risk Assessment:

"A specific risk for the public service is theft or compromising of data collected by the public service which would reduce confidence in public service administration and the use of technology for public services. There are also pressing risks for businesses and individuals, including the loss or theft of personal or business information, or even the destruction of property."

In its Global Risks Report 2017, the World Economic Forum state that:

"Perhaps because of the increasing ubiquity of innovative technology, respondents to the GRPS have tended not to include technological risks among the most impactful or the most likely to occur … The year 2014 was the first in which two technological risks made it into the evolving risk matrix, and this year, although only one is included ("massive incident of data fraud/theft"), another ("large-scale cyberattacks") came sixth in the list of risks most likely to occur in the next 10 years."[2]

[1]Department of the Taoiseach, National Risk Assessment 2016: Overview of Strategic Risks. Available at *http://www.taoiseach.gov.ie/eng/Publications/Publications_2016/2016_National_Risk_Assessment.pdf* at p.40.

[2]World Economic Forum, Global Risks Report 2017. Available at *http://www3.weforum.org/docs/GRR17_Report_web.pdf*

In 2013, Europol put the annual value of the global cybercriminal economy at approx. US$1tn.
In that same year, Viviane Reding, Vice-President of the European Commission, said:

"Personal data has become a highly valuable asset. The market for analysis of large sets of data is growing by 40% per year worldwide. The currency of this new digital economy is data and in many cases personal data. But the free flow of any currency depends on a precious commodity: Trust. It is only when consumers can 'trust' that their data is well protected that they will continue to entrust businesses and authorities with it by buying online and accepting new product developments and services. And trust is waning."

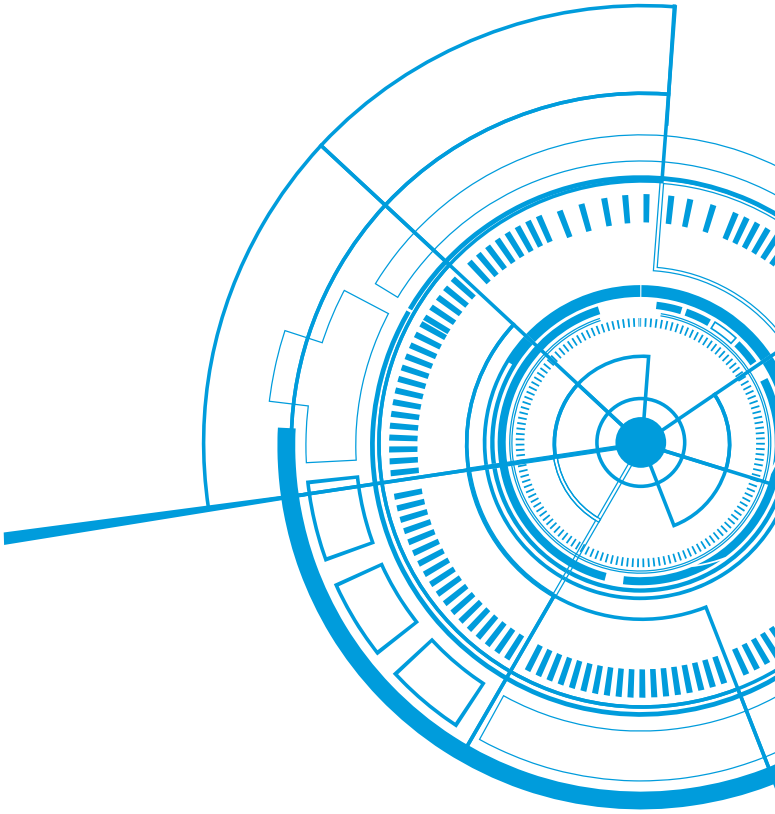
The General Data Protection Regulation

In May 2018, the General Data Protection Regulation (the GDPR) enters into force on a European-wide basis, meaning the current legal regime in Ireland, the Data Protection Acts 1988 & 2003 (the DPAs), will be repealed and replaced in their entirety by the GDPR. In addition to this, Ireland has until May 2018 to transpose the EU Directive on Security of Network and Information Systems 2016/1148 (the NIS Directive) into Irish law. The NIS Directive is aimed at harmonising cyber-security regulation among EU Member States and at the establishment of an EU-wide system of sharing and exchanging information between EU Member States.

From a macro-perspective, the GPDR will introduce many significant changes to data protection law in Ireland which will include:

- strengthened conditions for consent
- a broader territorial scope
- new breach notification requirements
- the right to be forgotten
- new rights of access
- significant financial penalties

From a cyber security perspective, the GDPR will have a substantial impact on data processing operations and contains a complex regime of measures companies must take to protect personal data. However, whilst the GDPR provides detailed guidance on the appointment of a data protection officer and the maintenance of detailed documentation to prove compliance, it is surprisingly light on the topic of data security. Indeed the GDPR does not pronounce on any precise technology that must be used to secure data. Of the 99 articles contained in GDPR, only three relate to data security – and even at that two of these relate to notification of data breaches. The result is 20 lines of guidance as to what data security measures will be mandated or expected under the GDPR. Whilst the GDPR is more prescriptive than the 1995 Directive, which left more discretion to the data controller in terms of the technical and organisational measures to be implemented in the controller's particular context, the net effect of the GDPR is very similar - the primary requirement is that the controller / processor must ensure the security of the personal data that they process. However, it goes without saying that no single programme of technical measures will fit all organisations.



[3]Viviane Reding, "The EU's Data Protection rules and Cyber Security Strategy: two sides of the same coin" (2013) Speech at the United Nations 2013. Available at *http://eu-un.europa.eu/the-eus-data-protection-rules-and-cyber-security-strategy-two-sides-of-the-same-coin-%C2%96-speech-by-eu-commission-vice-president-reding/*

Looking in more detail at the GDPR, Article 32 says that personal data must be processed in such a way that ensures the security of that data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by implementing appropriate technical or organisational measures. Depending on the nature of the processing, such security measures may include:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and / or
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

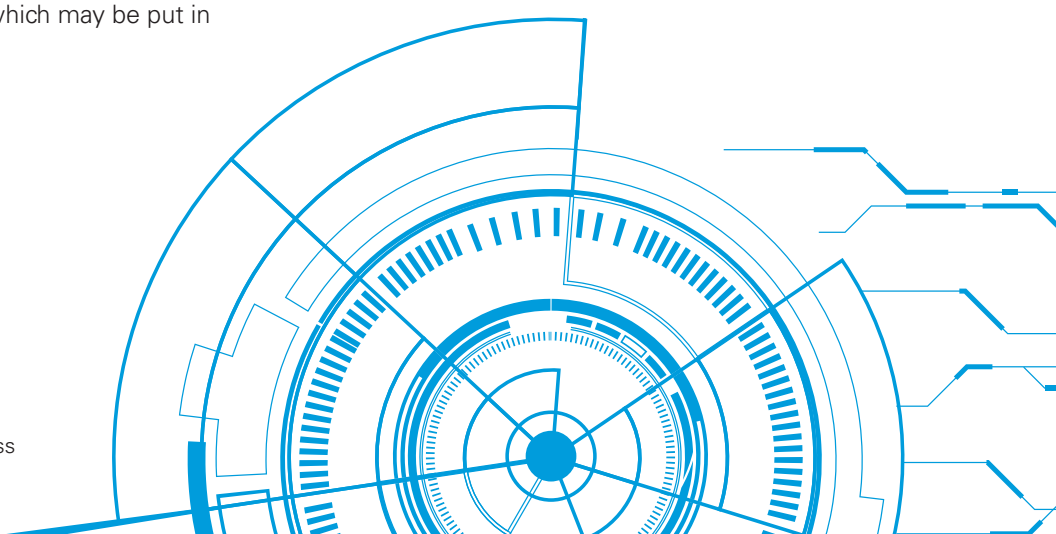
Article 32 represents a clear nod to a risk-based approach to cybersecurity. Risk-based security programmes are designed to provide an evaluative framework according to which threats to, and the vulnerability of, data may be prioritised. Such threats and risks are then evaluated in light of the likelihood a cyber-attack occurring combined with any economic or reputational impact that the attack may have. The result of the evaluation will in turn determine the significance attributed to each risk. These frameworks can be very useful to organisations for enhancing their cyber defences in certain areas and also for re-thinking other levels of cyber-security in areas which perhaps may not require elaborate and costly security controls which may inhibit business performance.

Authoritative Guidance

The GDPR calls on data controllers and processors to look to existing best practices and recommendations for guidance on types of data security measures available. In respect of the DPAs, the Office of the Data Protection Commissioner has issued guidance recommending that the types of security measures envisaged by data protection law which may be put in place to include:

- physical access controls to secure entry and exit, alarm systems and restricted access to server rooms;
- computer users should have a unique identifier (such as a password, passphrase, smart card or other token) to allow access to personal data;
- automatic screen savers to lock unattended computers;
- at least a 256 bit whole disk encryption to encode stored information;
- antivirus software, firewalls and software patches;
- use and access to data controls which allow only access to specific personal data that employees are authorised to use. These controls should include safeguards to prevent reading, copying, modifying or removing personal data without authorisation using a user account management system;
- data transmission controls ensuring that personal data cannot be read, copied, modified or removed without authorisation during transmission. Measures include using data transfer logs, encrypting data and control remote server access;
- data input control to verify who inputs data into processing system thus creating an audit trail; and
- availability control mechanisms such as backups and disaster recovery plans to ensure data is protected from accidental destruction or loss.

Source: Office of the Data Protection Commissioner



Further afield, the UK's National Cyber Security Centre published actionable guidance for organisations to achieve cyber security and compliance with security obligations in its "10 Steps to Cyber Security." One of these 10 steps calls for monitoring to detect attacks, respond to attacks and account for activity:

"System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements."

Looking even further beyond our borders, the CIS Critical Security Controls for Effective Cyber Defense has been developed by the US Center for Internet Security with support and input from the UK's Centre for the Protection of National Infrastructure. The CIS Security Controls are very closely aligned to the "10 Steps". An example of the technical guidance in the Critical Security Controls is CSC 4 "Continuous Vulnerability Assessment and Remediation." It recommends that organisations "continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimise the window of opportunity for attackers."

The NIS Directive

The NIS Directive will provide measures to boost the overall level of cyber-security in the EU by imposing minimum harmonisation rules for Member States. The NIS is concerned with two types of entities (i) "essential service operators" within the energy, transport, banking, financial market infrastructure, health, drinking water, and digital infrastructure sectors, and (ii) "digital service providers," including entities such as online marketplaces, online search engines, and cloud computing service providers.

Interestingly, the inclusion at all of category (ii) in the NIS Directive was the source of considerable disagreement. Those against the inclusion were of the mind that cyber-attacks on digital service providers are not significant enough and therefore do not require additional regulation. In its final form, the NIS Directive includes digital service providers, but subjects them to less stringent regulation than essential service operators. For example, digital service providers must notify incidents having a "substantial impact," whereas operators of essential services are subject to the broader-ranging requirement of notifying any incident having a "significant impact".

In a similar vein to the GDPR, whilst technical and organisational measures are required to be implemented to ensure data security, no specific commercial information and communications technology product is specified in the NIS Directive. The NIS Directive requires digital service providers to:

- identify and take appropriate technical and organisational measures to manage the risks facing the security of the network and information systems used in offering services within the EU. Such measures must adhere to the "state of the art" and take into account the following elements: (i) security of systems and facilities; (ii) incident management; (iii) business continuity management; (iv) monitoring, auditing, and testing; and (v) compliance with international standards; and
- take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on services offered within the EU, with a view toward ensuring service continuity.

The objectives of the NIS Directive include:

- requiring Member States to increase their preparedness and have a minimum set of cyber security capabilities at regulatory and operational levels, encompassing national strategies, National Competent Authorities (NCAs) and national Computer Security Incident Response Teams (CSIRTs);
- establishing formal EU co-operation arrangements at both strategic and operational levels, namely a co-operation group and a CSIRT network, between the Member States to improve mutual collaboration on cyber security;

- requiring identified operators of essential services (digital infrastructure, energy, transport, finance, health, water supply) to take appropriate and proportionate technical and organisational measures to manage security risks, to report serious incidents to NCAs and to comply with instructed requirements of NCAs; and
- requiring digital service providers (online/e-commerce marketplaces, online search engines, cloud computing services) to take appropriate and proportionate technical and organisational measures to manage security risks, to report particular incidents to NCAs and to comply with requirements of NCAs.

Post-May 2018, data controllers and processors may find themselves simultaneously subject to both the NIS Directive and the GDPR. A significant distinction, however, can be made with regard to the type of data protected under the NIS Directive and the GDPR. While the GDPR applies only to personal data, the NIS Directive covers any type of data at all. In addition, the NIS Directive encompasses not only data breaches but also any "incidents" that could affect the security of digital service provider networks and impact the provision of service.

Conclusion

Combining the data protection principles embodied in the GDPR with an effective cyber-security policy can act as a catalyst to reduce cyber threats. Organisations need to integrate the two by placing emphasis internally on:

- preventive measures designed to guard against cyber-breaches;
- raising awareness of the organisational and individual data protection obligations; and
- distributing responsibility for those obligations amongst all levels in the organisation.

Those organisations who fall within the scope of GDPR will face a potential fine of 2% of global revenue for a failure to implement appropriate technical or organisational measures to protect personal data from cyber-attacks. It is for this reason that the GDPR will arguably raise the benchmark of the quality of cybersecurity controls because of the impact it will have where organisations get it wrong. For example, when the TalkTalk cyber breach occurred in the UK in October 2015, TalkTalk were fined £400,000 (approx.. €455,000) by the UK Information Commissioner's Office. Under GDPR however, if that attack happened again, they could face a potential penalty of millions, if not tens of millions, of Euro.

As the scale, sophistication and complexity of cyber-attacks continue to grow, organisations must remain vigilant and seek to implement appropriate technical or organisational measures, processes and policies to best protect the personal data they process and maintain compliance with the GDPR. Cyber security and the GDPR complement one another and have the same common denominator – the protection and management of data. When the GDPR gains force of law on 25 May 2018, data controllers and processors will need to have effective cyber security frameworks offering end-to-end protection using antivirus, malware tools and firewalls in place and up and running. The financial and reputational consequences of failing to do so may be dire.

As Viviane Reding said in 2013:

"A modern set of data protection rules and greater cyber-security resilience will contribute to more people using more online services which directly translates into growth for the companies. People will also be more confident to entrust their data to public administrations. This is the first way in which data protection rules and cyber-security measures are complementary."[4]

Gordon Wade, Manager, Legal Services, KPMG

"In October 2015, TalkTalk were fined £400,000 (approx.. €455,000) by the UK Information Commissioner's Office. Under GDPR however, if that attack happened again, they could face a potential penalty of millions, if not tens of millions, of Euro."

[4]Viviane Reding, "The EU's Data Protection rules and Cyber Security Strategy: two sides of the same coin" (2013) Speech at the United Nations 2013. Available at *http://eu-un.europa.eu/the-eus-data-protection-rules-and-cyber-security-strategy-two-sides-of-the-same-coin-%C2%96-speech-by-eu-commission-vice-president-reding/*

How KPMG Can Help

KPMG's unrivalled experience of large transformational change projects means we understand the challenges facing you in becoming cyber resilient and can assist you in addressing these challenges. KPMG can offer you a full range of services to suit your specific cyber security needs.

Risk Consulting

- ☑ Data Protection Risk, Process and Control Assessment
- ☑ Information Security Controls
- ☑ Cyber Security

Forensic Services

- ☑ Data Discovery
- ☑ Forensic Technology Experts
- ☑ Cyber Incident Response
- ☑ Cyber Incident Readiness / Planning

Legal Services

- ☑ Data Protection Obligations
- ☑ Technical and Organisational Security Measures
- ☑ Data Breach Reporting
- ☑ Privacy, Data Protection and Cyber Security Policies

Contacts

Michael Daughton
Partner
Risk Consulting

t: +353 1 410 2965
m: +353 87 744 2965
e: michael.daughton@kpmg.ie

William O'Brien
Director
Forensic Technology

t: +353 1 700 4119
m: +353 87 050 4119
e: william.obrien@kpmg.ie

Tony Hughes
Associate Director
Risk Consulting

t: +353 1 700 4229
m: +353 87 050 4229
e: tony.hughes@kpmg.ie

Gordon Wade
Manager
Legal Services

t: +353 1 700 4806
m: +353 87 050 4806
e: gordon.wade@kpmg.ie

kpmg.ie

Produced by: KPMG's Creative Services. Publication Date: September 2017. (3093)