KPMG

Cyber Resilience

Protecting your business

kpmg.ie

#CyberResilience

Contents

Introduction

Michael Daughton
Partner

John Poole
Partner

Bernard O'Hara
Director

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 $450 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 UK 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.

Business in Northern Ireland will not be immune – it is essential that each company consider its exposure to cyber attack, and take proportionate mitigating steps.

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.

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.

Cyber Risk - What should a Board focus on?

Cyber incidents affecting a number of high profile organisations including the NHS, Talk Talk, and Equifax have highlighted the vulnerability of large, technology dependent organisations to malicious attacks.

Such attacks demonstrate that, even where significant levels of resources are available for cyber defences, no organisation is immune from an attack when a determined criminal is at play. The response to a cyber incident, can be critical in ensuring business continuity and maintaining public trust (whilst protecting the company's reputation and underlying business), in the event of an attack.

SMEs are increasingly becoming targets for cyber attackers. Recent research by Zurich Insurance found that 875,000 SMEs across the UK had been affected by a cyber-attack in the 12 months to July 2017. Over 20% of companies affected estimated that the attacks have cost them more than £10,000, whilst 10% believed the attack had cost them more than £50,000.

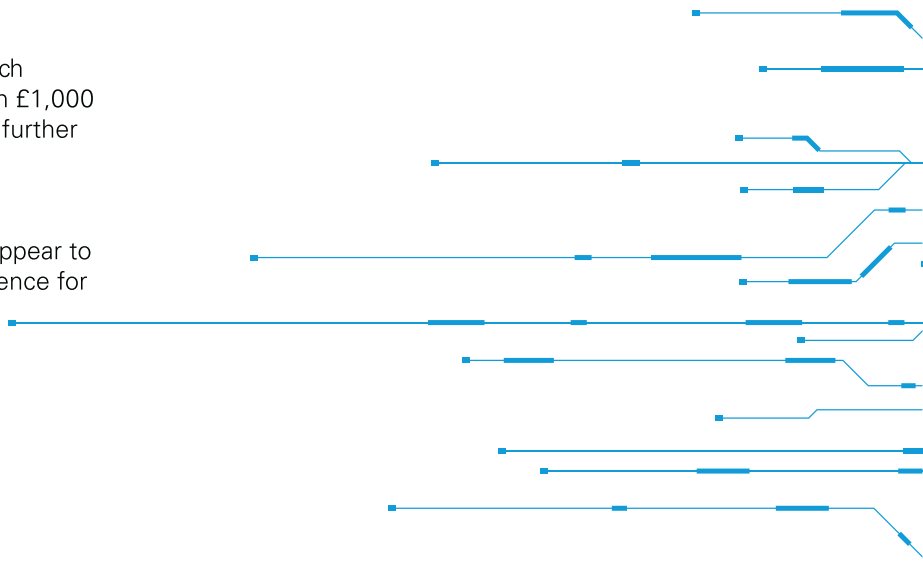
The motivation for such attacks may be financial, reputational or purely malicious. KPMG's most recent CEO Outlook – 'Disrupt and Grow', which surveyed CEOs both globally and locally, indicated that cyber risk continues to move up the agenda for Company Executives, operating across all sectors and scales – however, the lack of visibility in corporate risk registers indicates more focus is required on the pro-active management of cyber risk for local business, here in Northern Ireland.

Alarmingly, of 1,046 SMEs surveyed in the Zurich research, 49% expected to spend no more than £1,000 in the coming year on cyber defences, whilst a further 22% did not have an amount of spend in mind.

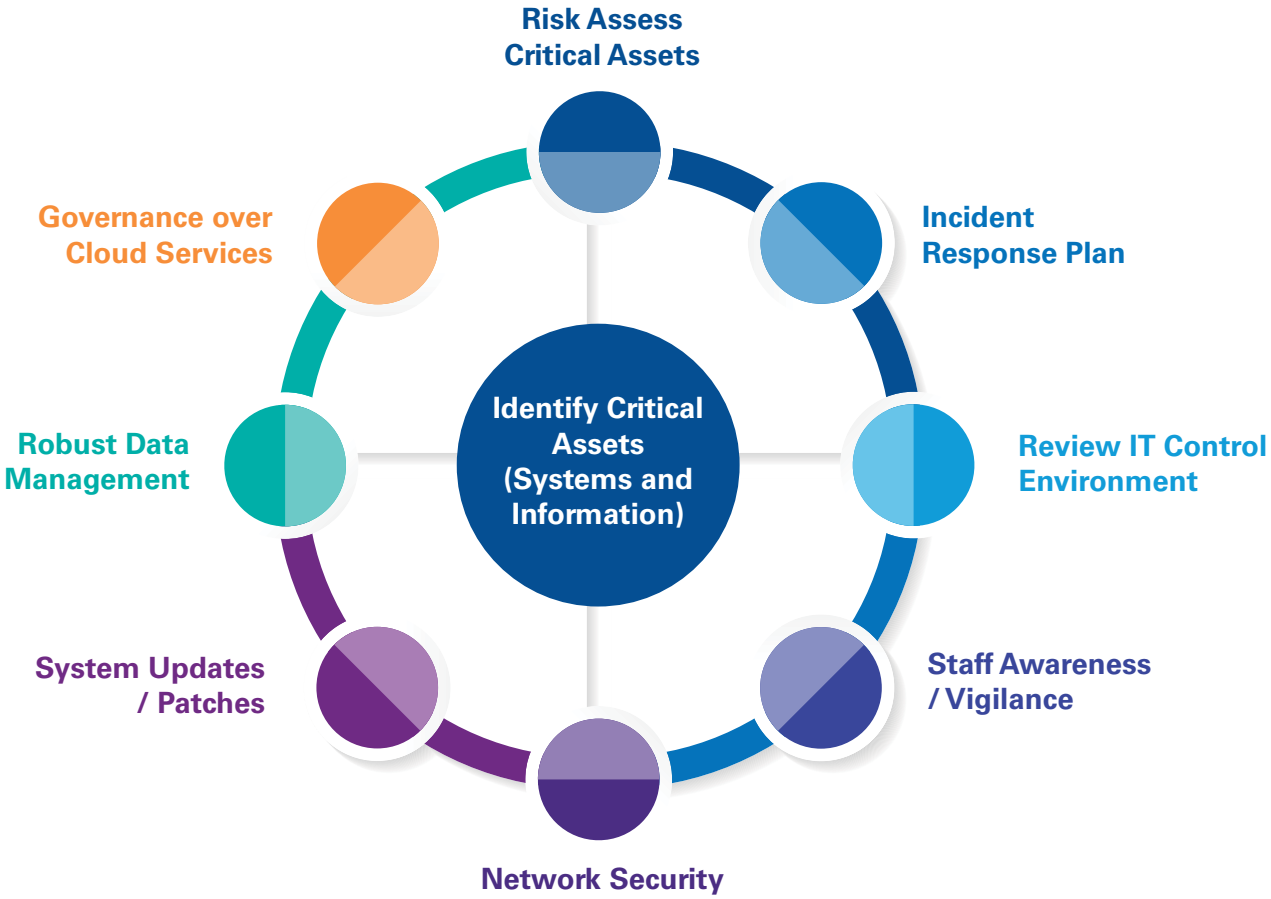
This would appear to suggest that, despite the increasing risk of cyber-attack, there does not appear to be a correlating increase in spend on cyber defence for SMEs. This may be because the Board does not believe an attack is likely, or will have a significant impact on their business, or they may see cyber defence as requiring technical solutions, which will likely prove costly.

Whilst it is true that unlimited resources could be spent on technical cyber defences, even this (as noted above) would not guarantee protection. The National Audit Office ('NAO') report into the WannaCry ransomware attack (which affected the NHS in 2017, and many other public and private organisations) made it clear that a series of management failings greatly increased the organisation's vulnerability to cyber-attack.

From a Board perspective, it is important to de-mystify the concept of "cyber risk," and how it relates specifically to their organisation. One size will not fit all, however every company, regardless of size, can take steps to help identify and respond to an incident. Expensive technical support, or software based solutions, are only part of the answer and organisations of all sizes can take steps to help identify and respond to the risks posed to their assets from both cyber criminals and non-malicious actions – centred around people, process and technology.



Practical steps which a Board can take to help support cyber resilience



As a starting point, Board members should consider the following areas of focus – a number of steps can be taken with minimal incremental cost, beginning with a cyber focused risk assessment:

1. Identify critical assets – both key systems and information assets – It is essential to understand what we are trying to protect and make investment decisions on cyber defence based upon the most critical assets.

2. Risk assessment – a risk assessment will help to understand how the threats to our assets are currently managed and identify/prioritise further mitigating actions, whilst ensuring ongoing focus on the issue at Board level. For key systems and information assets, consider the arrangements in place over access; backup; technical support; business continuity and protection against attack. Consider who might be interested in disrupting these systems, or stealing your data. An informed risk assessment will help build effective defences.

3. Incident response - consider how critical identified key systems are to your business and, in the event of an attack or disruption, how quickly you would seek to restore them – critical systems should be prioritised. Develop (and test) an incident response plan, which can be enacted in the event of an attack. This will help to ensure that the appropriate personnel (within the organisation and outsourced technical support) are quickly engaged, and that priority is given to isolation (and restoration) of key systems.

4. Review your own IT control environment – from maintaining up to date policies and procedures; through to regularly reviewing access and user rights to the network and key applications. Consider limiting the use of removable media – all laptops and removable media should be encrypted and regularly scanned for malware.

5. Staff awareness - staff are a critical element of cyber defence, particularly in relation to attempts at cyber fraud or theft, phishing, data theft or corruption

or transmitting malware. Ensure that they understand corporate policies covering acceptable and secure use of IT equipment. Encourage them to think twice before opening an unsolicited email attachment, or acting upon unusual requests (even if they appear to be from senior management) .

6. Network security – seek support from IT specialists to ensure robust network access protocols (including user/device authentication) and defence, such as firewall, antivirus and anti-malware. All systems and networks should be continuously monitored for unusual activity or attempted/actual attacks.

7. System updates and security patches – ensure that system software updates and security patches are processed as they become available. These are often issued by software providers to address known vulnerabilities or threats. Cyber attackers often exploit known system vulnerabilities, therefore timely application of system updates is essential.

8. Data management – cyber attacks often target company data, either to corrupt it, steal it, or demand a ransom. The General Data Protection Regulation ('GDPR'), (effective May 2018), will heighten the importance of robust data management and place a significant additional burden on companies in relation to any personal data they hold. All companies should take stock of their data management policies, procedures and processes (and indeed, only hold essential data), and reinforce controls to ensure secure data storage.

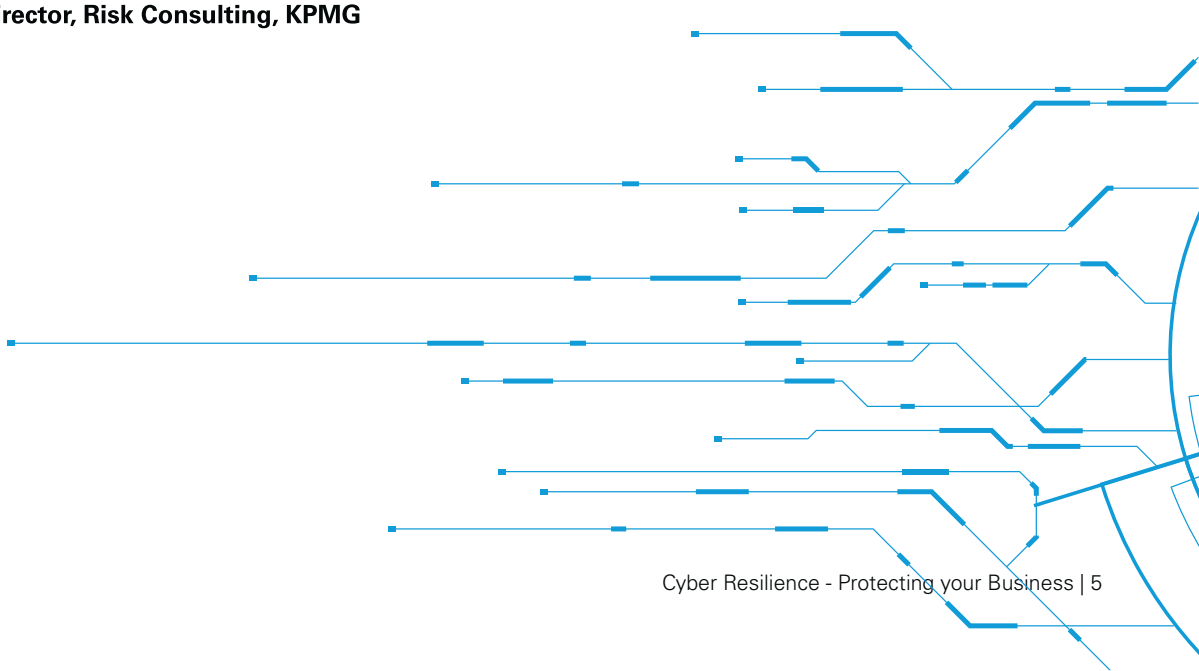
9. Governance over cloud based services – many companies are choosing to outsource their systems and data to third parties. Whilst this has many potential benefits, care should be taken to obtain assurance from third party providers (with their obligations being embedded within contracts), particularly with regard to business continuity, security of systems and data, and timely reporting of any attempted security attacks.

The areas of focus set out above are consistent with the approach suggested by the National Cyber Security Centre ('NCSC') (www.ncsc.gov.uk) in their '10 Steps to Cyber Security'. The NCSC was set up in 2016 by the UK Government to provide advice and support for the public and private sectors on how to avoid computer security threats and their website contains extensive support and guidance.

The threat from cyber attack is a real one and should be addressed proactively by all organisations reliant on IT systems. SMEs are not immune.

Boards should recognise that cyber defence is not just about technology spend – focus also on improving staff awareness and strengthening IT related processes (particularly around incident response and business continuity). Be ready and able for the challenge – it could come sooner than you think.

Bernard O'Hara, Director, Risk Consulting, KPMG



Developing a Proactive Cyber Defence Programme

On 25 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.

The GDPR will also come into force in Northern Ireland and the UK in May 2018 because the UK will still be a member state at this time. Furthermore, the UK has released its own draft Data Protection Bill, which aims to incorporate the GDPR and provide continuity throughout the Brexit process. The UK is aiming to implement this Bill in May 2018 and it will have to be read alongside the GDPR until Brexit is completed.

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.

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.

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 not tested until an incident occurs

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: Incident response tools are inadequate, unmanaged, untested or underutilised

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 UK 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 - Prepare, Withstand and Recover

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

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

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 motivation behind cybercrime includes disruption, positioning in the world cyber order and more likely a simple return on investment.

According to Verizon, which analysed 42,068 incidents and 1,935 breaches from 65 organisations in 84 countries; 51 percent of breaches involved organised criminal groups.

When you add in nation state actors, hacktivists and disruptive "script kiddies," sometimes hiding under cover of each other's labels, then you have the main actors in the cyber theatre of war.

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 has no relevance, if the price is right.

A Distributed Denial of Service (DDoS) attack can be procured for as little as US$7 per hour, with the costs of mitigation estimated at over $100,000 per hour. Incredibly, this makes the cost of performing an attack similar to that of going to see a movie.

The cost of defence has escalated over time, as organisations deploy multiple layered solutions to plug the security gaps without reconsidering the appropriateness of the solution and the true risk posed to their digital assets. Spending on cyber security now outpaces operational IT at a ratio of seven to one, an unsustainable strategy. Firms are coming under pressure to contain their burgeoning cyber security budgets, and manpower intensive compliance processes are beginning to give way to continuous testing and controls monitoring.

The six main European Institutes of Internal Audit in their "Risk in Focus: Hot topics in Internal Audit" report listed Cybercrime, General Data Protection Regulation (GDPR) and emerging technology as three of their top four risks in 2018.

Embracing emerging technology, and adopting services such as Cloud, allowing us to innovate and transform business, necessitates the treatment of cyber security as an essential business operation. The challenge is transforming our cyber security posture from a basic one to a more mature model, whilst doing so in a timeframe that avoids obsolescence. Increased delivery of services via digital channels will require that security by design and default is a core concept in transforming business, in a rapidly changing environment.

Almost half of the CEOs consulted (48 percent) in Northern Ireland and 56 percent of CEOs consulted in the Republic of Ireland by KPMG believe they need to do more to combat cyber security 'fatigue' in their organisation.

The apparent failure to explicitly identify and manage risks around cyber security, whilst noting the need to embrace emerging technology, might suggest a potential misdirection of effort, and resources, when dealing with the risks and opportunities around the application of technology within the business environment.

In our CEO Outlook 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, whilst everyone is waiting on the General Data Protection Regulation ('GDPR') to arrive on 25th May, new cyber-attack vectors have been identified in the form of hardware based attacks commonly known as Meltdown and Spectre, where core processing chips are used to access sensitive data, bypassing traditional controls.

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 tax 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 approach is focussed on the people, process and technology aspects within the cyber ecosystem.

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

Cyber resilience is focused upon 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 purely technical measures. By building an end-to-end understanding of cyber risks and threats, and aligning them to business objectives, cyber resilient businesses are able to take the appropriate measures to protect their digital assets and maximise the opportunities available online.

Cyber resilience also creates opportunities to increase the security awareness of staff, therefore reducing their riskier behavioural elements and creating a clear line of sight between business objectives, when set out in a Digital Strategy and Cyber Security implementation.

All very good, but how can we 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 GDPR, in force within the EU from 25th May 2018, will mandate this approach to information asset management in relation to all personally identifiable information.

The process for achieving cyber resilience can be best thought of within a framework containing five pillars: identify, protect, detect, respond, and recover. You can evaluate each pillar against your organisation's cyber security strategy to 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.

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.

The model is consistent with the EU Directive on Network Information Security (NIS) and by the UK National Cyber Security Centre (NCSC) in their '10 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 utilised by KPMG, in developing and delivering our Certificate in Cyber Security, which is delivered through Chartered Accountants Ireland.

The UK NCSC 10 Steps approach endorses the key enablers of a cyber resilient organisation and is available on their website ncsc.gov.uk. 'Disrupt and grow – The Irish CEO Outlook 2017' is currently available at kpmg.ie. The Risk in Focus: Hot Topics for Internal Audit 2018 is available via the Chartered Institute of Internal Auditors - UK and Ireland website.

Tony Hughes, Associate Director,
Risk Consulting, KPMG

The five pillars of cyber resilience

The General Data Protection Regulation from a Cyber-Security Perspective

> **"We will build in Britain a cyber strike capability so we can strike back in cyber space against enemies who attack us, putting cyber alongside land, sea, air and space as a mainstream military activity."**
>
> **- Philip Hammond (Chancellor of the Exchequer)**

Since the transposition of the 1995 Data Protection Directive into UK law, rapid technological developments and advancements have brought a plethora of new challenges for data protection. These changes have fundamentally changed even the most routine of business processes with the scale of data sharing and collection increasing dramatically. New technologies and innovations now allow companies and public authorities to use personal data on an unprecedented scale and in many new ways in order to pursue their activities. In addition to this, society in general are also increasingly making their personal information available publicly through multiple social media channels; channels which were never envisaged by the 1995 Directive. This societal evolution, together with the onset of the Digital Age, has necessitated the need for a stronger, more coherent data protection framework. As stated in the UK's National Cyber Security Strategy 2016-2021:

"Information and communication technologies have evolved over the last two decades ... [this] rapid evolution of the cyber landscape will constantly throw up new challenges as technology evolves and our adversaries act to exploit it ... cyber attacks are growing more frequent, sophisticated and damaging when they succeed."[1]

The European economy thrives on the free flow of information across borders using the latest technological innovations. However with new technology comes new (and significant) risks especially as organisations are becoming increasingly 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. Indeed the World Economic Forum, in its Global Risks Report 2017 cited cyber-crime among the highest of all global risks in terms of impact and likelihood of occurrence:

"Perhaps because of the increasing ubiquity of innovative technology, respondents to the Global Risk Perception Survey (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]

In 2017, Juniper Research put the annual cost of the global cybercriminal economy at approx. US$2tn. In 2013, Viviane Reding, then Vice-President of the European Commission, said:

[1] HM Government, National Cyber Security Strategy 2016–2021, para.2.1. Available at https://www.gov.uk/government/uploads/system/ uploads/attachment_data/ file/567242/national_cyber_security_strategy_2016.pdf
[2] World Economic Forum, Global Risks Report 2017. Available at http://www3.weforum.org/docs/GRR17_Report_web.pdf

"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."[3]

Westminster has also recognised the importance of trust in both the public and private sectors:

"The transformation brought about by this digitalisation creates new dependencies. Our economy, the administration of government and the provision of essential services now rely on the integrity of cyberspace and on the infrastructure, systems and data which underpin it. A loss of trust in that integrity would jeopardise the benefits of this technological revolution."[4]

The General Data Protection Regulation

At the date of writing this article, there are just 125 days remaining until the General Data Protection Regulation (the GDPR) enters into force on a European-wide basis. This will mean that the current legal regime applicable in the UK, the Data Protection Act 1998 ("DPA"), will be repealed and replaced in its entirety by the GDPR. In addition to this, the UK has until May 2018 to transpose the EU Directive on Security of Network and Information Systems 2016/1148 (the NIS Directive) into English 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 and is discussed further below.

From a macro-perspective, the GPDR will introduce many significant changes to data protection law in the UK which will include strengthened conditions for consent, a broader territorial scope, new breach notification requirements, the right to be forgotten, new rights of access and significant financial penalties. However, for the purposes of this article, we will focus on those changes that will have the most significant impact on the world of cyber-security.

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 it has to be said that the GDPR is more prescriptive than the 1995 Directive (which left a significant amount of 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 program of technical measures will fit all organisations.

"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."

[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-com mission-vice- president-reding/
[4] HM Government, National Cyber Security Strategy 2016–2021, para.2.2. Available at https://www.gov.uk/government/uploads/system/uploads/ attachment_data/ file/567242/national_cyber_security_strategy_2016.pdf

To delve into 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 programs 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 of 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. Frameworks such as these 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.

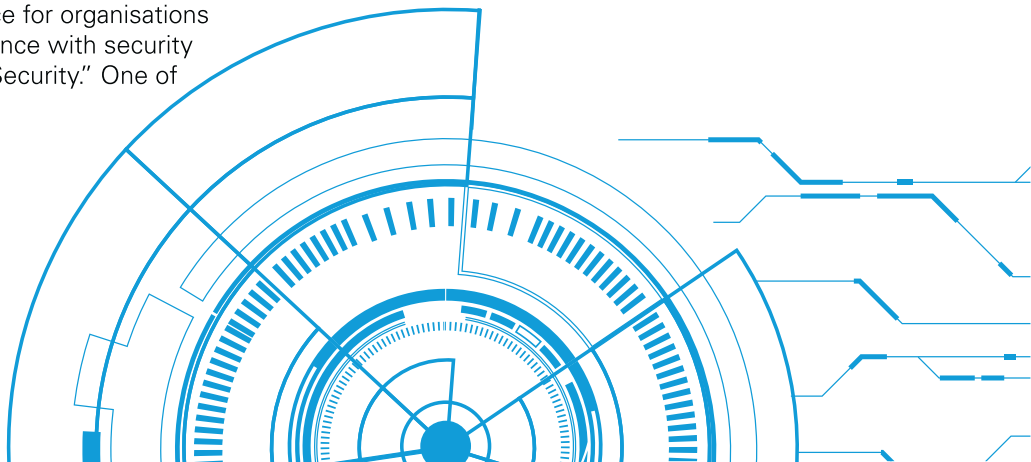
Authoritative Guidance

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 DPA, the Information Commissioner's Office has emphasised that there is no "one-size fits all" solution to information security and whilst any measures used do not have to be "state-of-the-art", they should be appropriate relative to the risks faced by an organisation and should be regularly reviewed as technology advances. The National Cyber Security Centre ("NCSC") has also 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 south, Ireland's 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 including:

- physical access controls to secure entry and exit, alarm systems and restricted access to server rooms;
- unique identifiers (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 controls 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.



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 Centre for the Protection of National Infrastructure in the UK. The CIS Security Controls are very closely aligned to the NCSC's "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 minimize 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 Directive is essentially 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 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, whist 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:

1. 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
2. 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:

1. 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);

2. 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;

3. 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

4.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:

1. preventive measures designed to guard against cyber-breaches;

2. raising awareness of the organisational and individual data protection obligations; and

3. 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 4% 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 by the UK Information Commissioner's Office (just under the maximum £500,000 fine). Under GDPR however, if that attack happened again, one cyber security expert touted a figure of 182 times that:

"TalkTalk should count themselves lucky this has happened now and not once GDPR is in play. If TalkTalk had been given the maximum fine, it would be looking at a bill of £73m."[5]

Similarly, Carphone Warehouse was recently fined £400,000 by the ICO for failing to have adequate technical security measures in place to protect customer personal data resulting in the unauthorised access to the personal data of over 3 million customers and 1,000 employees. An ICO review exposed inadequacies in the organisation's technical security measures including out-of-date elements of the software in use on the systems affected and the failure to carry out routine security testing. There were also inadequate measures in place to identify and purge historic data.

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. Cybersecurity 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 cybersecurity frameworks offering end-to-end protection with antiviruses, malware tools and firewalls in place and up and running. The financial and reputational consequences of failing to do so may be dire.

2017 was one of the biggest years in history for high-profile data breaches and 2018 will be no different. The first data breach in the post-GDPR world will set an example for the rest of Europe both in terms of thresholds for access control measures and the administrative fines. 2018 will likely also be the year when artificial intelligence really gets into its stride in terms of cyber security (building on the launch of "Watson for Cybersecurity" by IBM in 2017 which transformed the cyber security industry). Combining such AI technology with human intelligence, trained up in data protection compliance and underpinned by proper, implemented technical and organisational measures designed to protect personal data from attack, can be an effective proxy to reduce cyber-risks. 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."[6]

Gordon Wade, Associate Director, Legal Services, KPMG

[5] Rob Cotton, Chief Executive, NCC Group quoted in an article in the Financial Times (Bond, "TalkTalk hit with record fine over cyber attack" (Wednesday, 6 October 2016) Financial Times)

[6] 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/

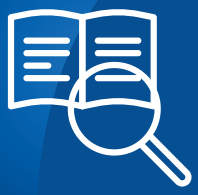
How KPMG Can Help

KPMG's Cyber Security Services see the world from the client's perspective, bringing a business context to cybersecurity for all levels of the organisation, from the boardroom to the back office.

Our service offering is focused on helping our clients transform their security function into business–enabling platforms so they can understand, prioritise, and manage their cybersecurity risks, take control of uncertainty, increase agility, and convert risk into advantage.

Business as usual | **Prebreach** | **Postbreach**

Strategy and Governance



Helping clients understand how best to align their cyber agenda with their dynamic business and compliance priorities

- **Cyber Security Strategy**
- **Target Operating Model Development**
- **Third Party Security Risk Management**
- **Business Continuity Planning**
- **Cyber Maturity Assessment**
- **Compliance/Framework Gap Assessment**
- **Privacy Management / GDPR**

Transformation

Helping clients build and improve their programmes and processes, supported by the right organisation and technology, to improve their cyber agenda

- **Identity and Access Management**
- **Digital Services**
- **Security Governance, Risk and Compliance (GRC)**
- **Analytics**
- **Asset Protection**
- **Security Program Delivery**

Cyber Defence

Helping clients maintain their cyber agenda as their business and technology prorgrammes evolve by providing greater visibility and understanding of changing risks

- **Technical Assessments**
- **Security Testing**
- **Application Security**
- **Security Operations Advisory**
- **Security Analytics**
- **Intelligence-Led Threat Assessment**

Cyber Response

Helping clients effectively and efficiently respond to cyber incidents and conduct forensic analysis and detailed investigations

- **Forensic Readiness**
- **Incident Response**
- **Breach Management**
- **Return to business as usual**

Contacts

Michael Daughton
Partner
Risk Consulting

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

John Poole
Partner
Audit & Assurance

t: +44 28 9089 3854
m: +44 78 7969 3854
e: john.poole@kpmg.ie

William O'Brien
Director
Forensic Technology

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

Bernard O'Hara
Director
Risk Consulting

t: +44 28 9089 3725
m: +44 79 1959 1326
e: bernard.ohara@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
Associate Director
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: January 2018. (3528)