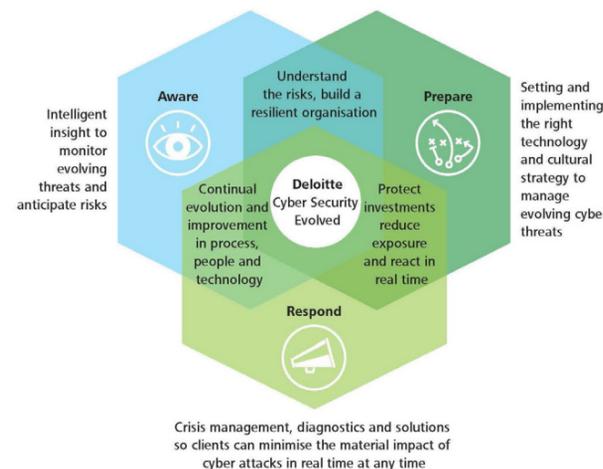


"We recognise that every organisation is different. Our flexible, pragmatic and independent approach to managing cyber security means that we work with you, from network to boardroom, to address the constantly changing threats."

Colm McDonnell, Partner, Risk Advisory Services

Cyber Security	Information Privacy & protection	Identity & Access Management	Digital Forensics & e-Discovery	Resilience & Preparedness	Focused Services
Defend against and limit the impact of a cyber attack	Protect sensitive information and ensure compliance with regulations	Control access to information in a borderless environment	Recovery, analysis and advisory on digital investigations and analysis engagements	Anticipate, plan and prepare for predictable and worst case scenarios	Protect people and infrastructure
<ul style="list-style-type: none"> <li>Security Strategy &amp; transformations</li> <li>Cyber Preparedness</li> <li>Vulnerability &amp; Pen Testing Assessment</li> <li>Web Application Assessments</li> </ul>	<ul style="list-style-type: none"> <li>Data Privacy &amp; Data Protection</li> <li>PCI DSS</li> <li>Info Protection Technology</li> <li>Cryptography &amp; PKI</li> <li>Third Party Security</li> </ul>	<ul style="list-style-type: none"> <li>Access Certification</li> <li>User Life cycle Management</li> <li>Cloud Identity &amp; Federation</li> <li>Privileged Access Management</li> <li>Information Rights Management</li> </ul>	<ul style="list-style-type: none"> <li>Digital Forensics</li> <li>E-Discovery</li> <li>Litigation Support</li> <li>Incident &amp; Crisis Response</li> <li>Forensic Capability Partnership</li> </ul>	<ul style="list-style-type: none"> <li>Business Continuity</li> <li>Disaster Recovery</li> <li>Key Supply Chain Reviews</li> <li>Incident &amp; Crisis Response Management</li> <li>Forensic Capability Partnership</li> </ul>	<ul style="list-style-type: none"> <li>Cloud Computing</li> <li>Policies &amp; Standards Development</li> <li>Information Security Best Practice</li> <li>Mobile Computing &amp; Smart Devices</li> </ul>



For more information please contact:



**Colm McDonnell**  
 Partner, Risk Advisory Services  
 T: +353 (0)1 417 2348  
 E: cmcdonnell@deloitte.ie



**Jacky Fox**  
 Cyber & IT Forensic Lead  
 Risk Advisory Services  
 T: +353 (0)1 417 2208  
 E: jacfox@deloitte.ie

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/ie/about](http://www.deloitte.com/ie/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

With nearly 2,000 people in Ireland, Deloitte provide audit, tax, consulting, and corporate finance to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. With over 210,000 professionals globally, Deloitte is committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, Deloitte Global Services Limited, Deloitte Global Services Holdings Limited, the Deloitte Touche Tohmatsu Verein, any of their member firms, or any of the foregoing's affiliates (collectively the "Deloitte Network") are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

## Contacts

Dublin  
 Deloitte  
 Deloitte & Touche House  
 Earlsfort Terrace Dublin 2  
 T: +353 1 417 2200  
 F: +353 1 417 2300

Cork  
 Deloitte  
 No.6 Lapp's Quay  
 Cork  
 T: +353 21 490 7000  
 F: +353 21 490 7001

Limerick  
 Deloitte  
 Deloitte & Touche House  
 Charlotte Quay Limerick  
 T: +353 61 435500  
 F: +353 61 418310

[www.deloitte.com/ie](http://www.deloitte.com/ie)

# Deloitte.

## Cyber Security Evolved



# Aware



Cyber threats are many, varied and always evolving

Being aware is “knowing what is going on so you can figure out what to do”. The challenge is to know which cyber threats are relevant to your organisation and to anticipate what the next threats will be and where they will come from.

Deloitte’s cyber aware capability gives organisations situational awareness of the cyber threats facing them. Whether the threats come from insiders, from organised cyber criminals, from hacktivists or from sophisticated attackers using innovative techniques, our services help organisations to understand the threats, how they affect their business and how to deal with them.

**Cyber intelligence:** Our cyber intelligence centre draws on real time security intelligence from our strategic partners in the security industry, from our own platforms and tools, and from our clients’ own systems. Our operational security experts analyse, contextualise and integrate these diverse feeds with our unparalleled understanding of business processes and risks to give our clients enriched situational awareness and pragmatic actionable information to address threats as they arise.

**Managed security assessments:** Our dedicated team of security penetration testing experts can carry out a range of system security assessments. From light touch vulnerability assessment through to controlled yet relentless attacks on an entire organisation’s systems and processes, we can identify where there are weaknesses, what impact they might have on business value and help you manage the risks in a pragmatic and business-focused way.

**Managed security services:** Deloitte’s cyber intelligence centre enables businesses to extend and enhance their own security operations capability by leveraging our and our strategic partners’ security experts.

We can help you to defend the greatest threats and mitigate the greatest risks by building a dynamic real time view of your threat profile.

- Understand the cyber threats that are relevant to your organisation.
- Assess your systems to uncover weaknesses and angles for attack.
- Anticipate what the next threats will be.
- Identify where the next threats will come from.

# Prepare



Making sure you have the capability and skills

Although the technical defences against a cyber attack must be built by IT, a breach of those defences can have far reaching business consequences. Identifying the business risks and deciding how and when cyber issues should be escalated are the starting points in developing an effective, coordinated business response.

Protecting information assets in an always-on and always-connected world is of critical importance to the sustainability and competitiveness of businesses today. Effective security is the difference between success and failure; between understanding and ignorance; between compliance and non-compliance; between winning and losing.

Deloitte’s cyber prepare capability helps organisations to set and implement the right technology and cultural strategies to manage evolving cyber threats. Our tailored services range from understanding cyber risks and crisis management to cyber simulation and encouraging responsible behavioural change.

**Cyber preparedness:** Our cyber preparedness capability helps businesses to understand their true cyber risks. We test cyber crisis management procedures in controlled but realistic scenarios rather than use hypothetical plans. We pressure test cyber incident management strategies so that hidden errors, false assumptions, gaps in plans and unrealistic expectations are exposed and resolved before live deployment.

**Cyber simulation:** Our skilled practitioners have a track record of delivering strategic cyber simulations and crisis management exercises based on proven methodologies.

**Behavioural change:** Our training programme educates and raises awareness on cyber risks across your organisation.

With a planned, coordinated and tested capability to respond against the persistent threat of attack, you can better protect your staff, assets, customers and value. We can help you minimise disruption by:

- Understanding your risks and developing mitigation plans.
- Defining the roles, responsibilities and procedures.
- Communicating clear escalation paths as well as devolved authority to respond.
- Undertaking simulations and training to support your staff.

# Respond



Supporting you from network to boardroom

When a breach occurs the response must be fast, thorough and decisive. Immediate action is required on several fronts. The nature of the breach must be established and the losses and damage understood. Further attacks must be prevented by urgent action while a longer-term solution is found.

Management and security teams are judged on their ability to respond. Slow or ineffective response can mean reputational damage, decreases in share value and potentially lead to litigation costs or further attacks.

Deloitte’s cyber response services have been designed to provide organisations with access to the skills, experience and knowledge that are needed during times of crisis. We work to help manage your response, investigate and understand the root causes behind the incident and put remediation plans in place.

**Cyber incident response:** Effective cyber incident response requires flexibility and the ability to make decisions, often with incomplete information to control the incident and manage the risk. Our approach blends deep technical skills, crisis management expertise and business intelligence to deliver a complete service, when and where organisations need it most.

**Crisis Management:** Our cyber crisis management team works with an organisation to quickly define roles and responsibilities, complete a risk and impact assessment and agree response work streams and strategies.

**Cyber Forensics:** Specialist teams can assist you to conduct technical root cause assessment, breach analysis and forensic investigation.

We are trusted to deliver scalable crisis management, incident response and forensic services to minimise the impact of cyber attacks. We can help:

- Deploy our specialist teams on the ground, fast, where you need them.
- Provide flexible support, integration or complete management of your response.
- Manage an incident in a proportionate and informed way.
- Prepare for the inevitable by developing and testing your incident response plans.