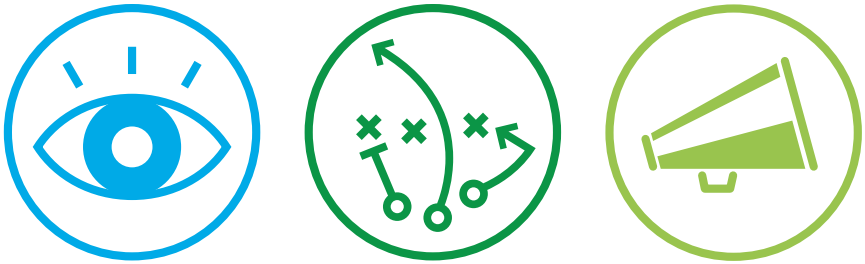
Deloitte.

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.

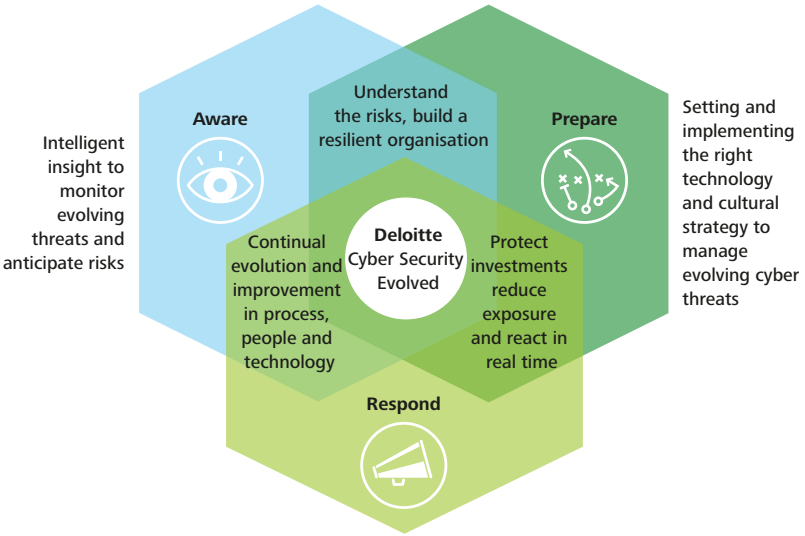
The rapid pace of change in technology has provided huge opportunities for organisations to develop new models, services and products. But while the digital revolution has evolved the way we do business, it has also created a sophisticated and complex set of security issues. Assets that were once physically protected are accessible online; customer channels are vulnerable to disruption; criminals have new opportunities for theft and fraud.

Business value is becoming more and more dependent on always-on, always-connected systems. Exposure to cyber threats increases as businesses embrace the digital world. The challenge is to understand what is going on in the digital landscape, what it means, and what to do about it.

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.

The most resilient businesses are those that are always aware of the latest risks, have prepared their organisations to be robust and are able to respond swiftly and effectively to mitigate new risks.

In managing these critical elements of cyber security we can help ensure that our clients continue to take advantage of the benefits of digital business.



Contacts

Mark Carter
Partner, Security & Resilience
+41 (0)58 279 73 80
markjcarter@deloitte.ch

Klaus Julisch
Senior Manager, Security & Resilience
+41 (0)58 279 62 31
kjulisch@deloitte.ch

Lance McGrath
Senior Manager, Security & Resilience
+41 (0)58 279 64 67
lamcgrath@deloitte.ch

Or to find out more visit **http://www.deloitte.com/ch/security**

Designed and produced by The Creative Studio at Deloitte, Zurich. 30450A