

Cyber Intelligence Centre (CIC)

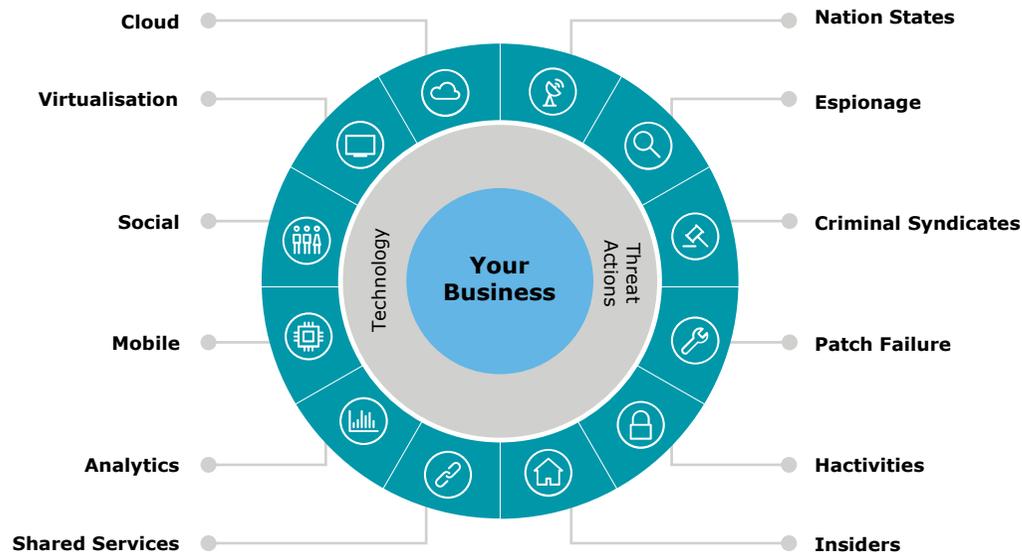
The Deloitte Cyber Intelligence Centre (CIC) combines deep cyber intelligence with broad business intelligence to deliver relevant, tailored, and actionable insights to inform business decision-making.

The CIC fuses a number of services together to provide our clients with a truly tailored service that enables them to fully understand their cyber risks and adopt proportionate responses in an increasingly digital and interconnected business environment. We do this by providing them with improved visibility of threats and assets, based on highly relevant intelligence that reflects their specific business, market, and industry context.

Based on a shared service delivery model, it is architected on a high-performance cloud-based analysis platform and is backed by world-class professional services expertise. We also continually invest in R&D, platforms, and people. This ensures our clients are able to stay secure in a rapidly evolving threat landscape, while avoiding spiralling costs and investment requirements. All client data is stored and disposed of in a manner that is consistent with the ISO 27001 standard. Clients can define storage and disposal methods within SLAs and the information is protected in our cloud platform through the use of our information protection tool.

Alongside our threat intelligence services, our global, 24x7 Cyber response team, informed by zero-day threat intelligence, delivers proactive incident response, fast and decisive remediation, and holistic crisis management support. This helps clients reduce the business impact of incidents, limit brand damage, and lower the risk of repeat occurrences.

Balance risk and reward in a dynamic cyber landscape



CIC – Mission, Capabilities, and Goals



Our mission

- Provide a client-centric cyber security platform that is based on understanding our client's business.

Our capability

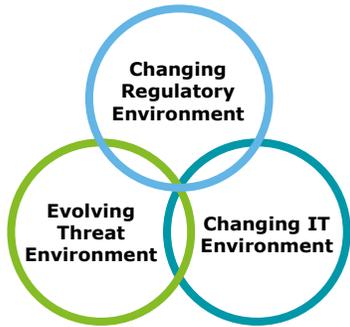
- Global Capability: We bring Deloitte's global network to every client.
- Global Research: We harness the strength of our global research team.
- Risk focus: Deloitte's approach understands the unique nature of cyber threat monitoring based on business context and applicable threats.

Our goals

- Performance: We drive for excellence through verifiable processes, metrics, and measures.
- Solutions based: We provide a solutions-based service.
- Quality: We strive for the utmost quality.
- Transparency: We earn our client's confidence and trust through execution and transparency.

Key Differentiators

- Standardized solutions delivery
- Experience with industry-proven methodologies and tools
- Vendor-neutral and tool-neutral solutions
- Cutting edge vulnerability research capabilities
- Breadth of experiences strategy, assessment, architecture, design and implementation of security solutions.
- Ability to address core security solutions and key elements using root cause analysis
- Consistent and controlled approach
- Adaptive, consultative, risk-based solution
- Clear articulation of business and technical risk



What is New with Cyber Security?

The business and IT environment is changing.

- New business models—cloud, mobile, big data, Internet of Things
- Enterprise IT environment disrupted—BYOD & “rogue IT”
- Regulatory changes, state & country laws, industry regulation, emerging NIST standards

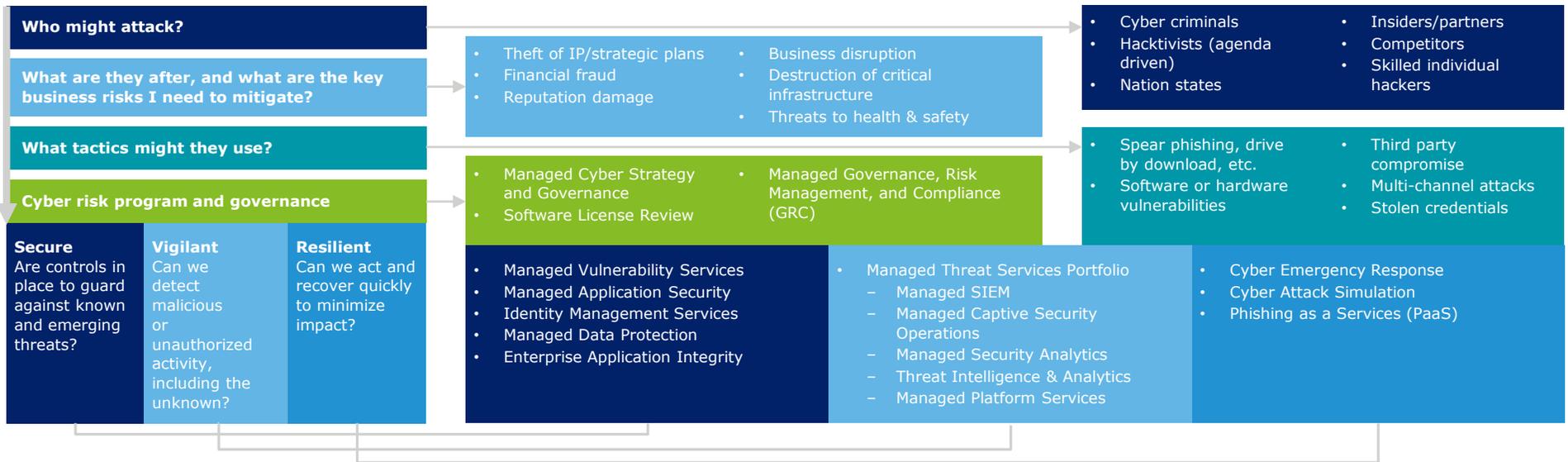
Leading to new, persistent, evolving risks

- More frequent, sophisticated, and malicious attacks
- Wide range of motives: economic, campaigns, Hactivists
- Hackers already inside the organization
- Data easily available and it’s money
- C-Suite, Board, and key staff are sitting targets

Clients are struggling to keep pace

- Risks are evolving faster than clients can react
- Need to transform how they think about Cyber Security
- Companies, large and small, do not have in-house skills
- Greater need for comprehensive, enterprise solutions
- Boards and Management are struggling how to “measure” cyber risk

It starts by understanding who might attack, why, and how..



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material and the information contained herein prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP) is intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or 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 material.

Contacts

Rohit Mahajan

President, Risk Advisory

Email: rmahajan@deloitte.com

Gaurav Shukla

Partner, Risk Advisory

Email: shuklagaurav@deloitte.com

Anand Tiwari

Partner, Risk Advisory

Email: anandtiwari@deloitte.com