Cyber security

Digital Customer Experience

Digital Employee Experience

Digital Insight

Internet of Things

Payments

IP Solutions

Cyber Security

Cloud

CGI

Contents

Cyber Security

Securing organisations in a digital world

Organisations have invested time and effort in IT computer security over the last 40 years, in fact for as long as network computers have existed. However, the term cyber security is a more recent one, and reflects the changing nature of information security in a digitally interconnected world.

The rapid advance of digital technologies is undoubtedly driving this transformation. But more fundamentally, organisations have been unwittingly taking on risk—making use of networked information, digitalising their businesses—and leaving themselves vulnerable to attack.

There are many factors that have turned traditional IT security on its head:

- Industrial-scale cyber espionage, which targets information, undertaken by criminal gangs and state-sponsored espionage.
- The "militarisation" of cyber space, as nations start to treat cyber space as another military domain and act to build offensive capability and safeguard national critical infrastructure.
- The rise of "hacktivism", with activists taking on corporates and public institutions by defacing their websites or disrupting their online services.
- Organised cyber crime that now makes more money from a variety of illegal online activities, acting with impunity as national police forces struggle to respond on an international stage.
- Growing dependency on the Internet as businesses and governments move their services online, closing down traditional ways of engaging with citizens and customers.

Clearly, a great deal has changed since the first worm was created at Cornell in 1988. In fact, in 2011, a single attack on the Sony PlayStation network cost the organisation as much as USD 170 million. Today, the losses created by a single cyber attack are unprecedented.

With the risks and impacts associated with cyber attacks becoming more visible, the awareness of cyber security has also grown significantly. During our in-person interviews with 962 senior clients in 2015, 64% of clients identified their level of cyber risk as being either high or very high.

As a security specialist, CGI has been part of this evolving journey within our clients' organisations. We understand how cyber security plays a crucial role in facilitating those enabling technologies that transform a modern business into a digital organisation.

40%

of clients recognise cyber security threats as their top

IT priority of 2015.

Source:
CGI client interviews, conducted in 2015

64%

of clients recognise their level of

cyber risk

to be high or very high.

Source:
CGI client interviews, conducted in 2015

Business **drivers**

In our face-to-face client interviews, 40% of organisations ranked cyber security as their top IT priority for the year. There are several factors driving the increased business interest in cyber security.

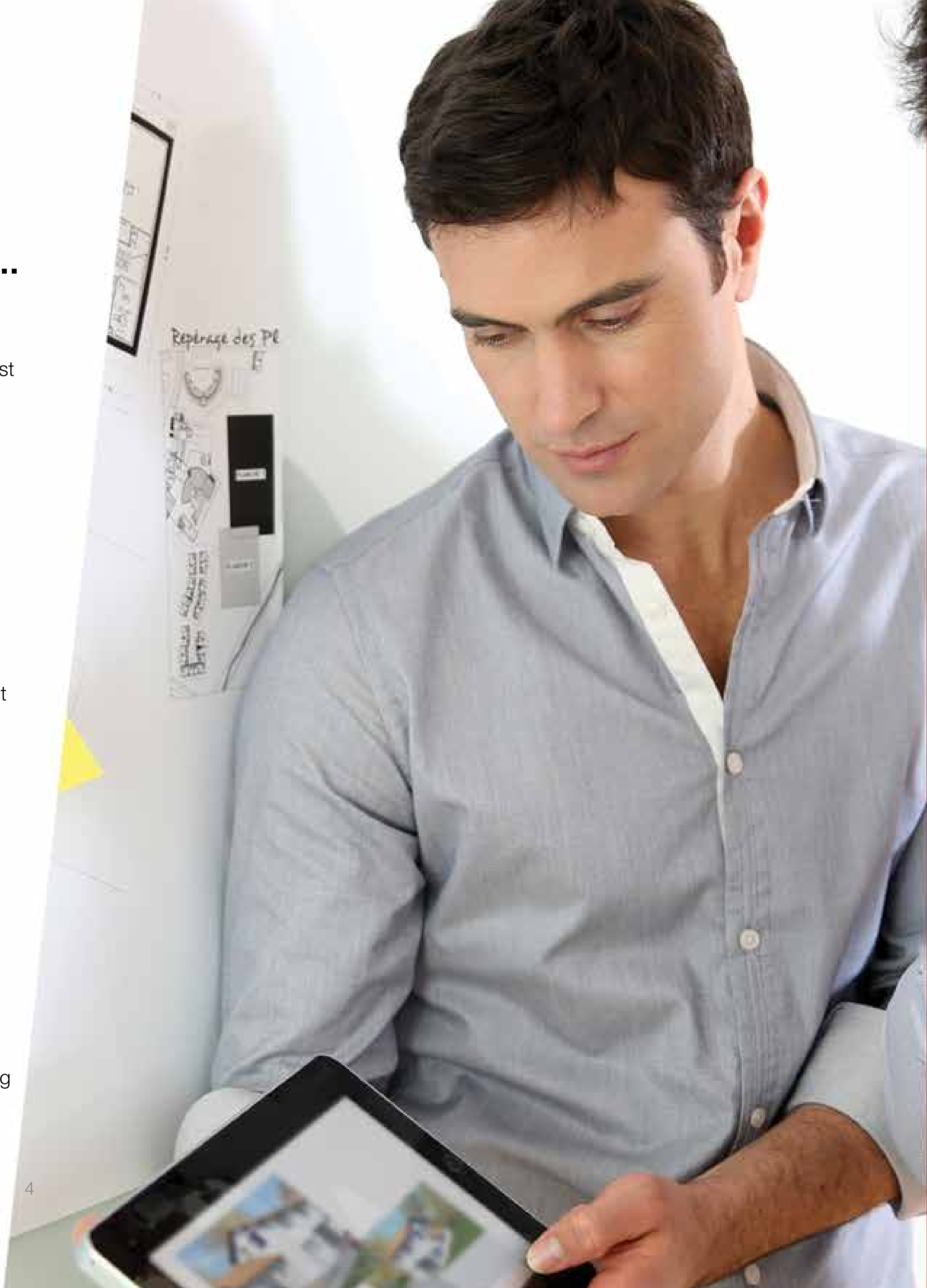
- **Digital transformation**
  In the last decade, it has become imperative for organisations to digitalise their businesses. They have become dependent on their digital infrastructure, without necessarily even being aware of this. The security of such infrastructure is a fundamental prerequisite for successful digital organisations.

- **Compliance**
  With regulatory authorities becoming more stringent and far-reaching, it becomes crucial for organisations to be able to monitor and protect the use of sensitive information, whether in the form of payments records or personal information about clients and staff.

- **Specialist skills shortages**
  The skills and know-how required to detect sophisticated cyber attackers are hard to find and in high demand. Increasingly organisations are turning to 3rd party teams to access the expertise they need.

- **Digital customer experience**
  In the digitally-enabled enterprise, a secure environment plays a crucial role in creating a memorable consumer experience and gaining customers' confidence. The rising use of mobile technologies has driven innovation in security, protecting services provided by these means.

- **Privacy and data protection**
  Government regulation is also creating stronger obligations on organisations holding personal data and making citizens and customers more aware of their loss of privacy via the Internet. Again, security of such data is both a legal and a moral obligation.



Technology enablers

- **Digitalisation**
  The increasing digitalisation of information within businesses has made it imperative for organisations to consider the new security vulnerabilities introduced by mobile and cloud technologies, by virtual employees and by the new channels to consumers.

- **Explosion of the Internet of Things**
  It is estimated that the Internet of Things will reach an installed base of 25 billion objects by 2020 (Source: Gartner, 2014)[1]. Inevitably, the rise in "connected" objects is directly responsible for new types of vulnerabilities and attacks.

- **Mobility**
  As more individuals use mobile devices to connect to the digital world, the proliferation of these devices raises new challenges for cyber security.

- **Cloud**
  With a rising numbers of businesses moving into the cloud and an increasing number of cloud services becoming interconnected and interoperable, users are starting to worry about how to assure the security of the cloud.

- **Big data**
  While advances in predictive analytics have made it possible to analyse customer information to extract unforeseen business insights, it is also becoming increasingly crucial for this data to remain secure and private. Handling huge datasets, which represent aggregates of multiple different sources, is one of the most striking security challenges of the next 10 years.

- **Sophisticated malware and cyber attacks**
  Analysts predict that the level and sophistication of attacks will only increase over the next 10 years.

[1] Gartner, P. Middleton, T. Koslowski and A. McIntyre, Forecast Analysis: Internet of Things, Endpoints and Associated Services, Worldwide, 2014 Update, 02 December 2014

Delivering the solution

CGI offers consultancy, solutions and managed services that enable our clients to assess the risk, protect their business and operate with confidence.

Our services help organisations:

- **Assess and mitigate the risk:** Risk and vulnerability assessments, information handling, data protection, regulatory compliance, insider threat analysis, threat trends, board-level awareness, education and cultural change, response and recovery planning, security audit, security policy, procedures and processes, and information security management systems.
- **Protect their business:** Secure systems engineering, securing new technologies, penetration testing, identity and access management, biometrics (including Eligo IP) , system test and evaluation including Common Criteria, CESG's Tailored Assurance Scheme (CTAS), Commercial Product Assurance (CPA) and CESG Assured Services (CAS), crypto management.
- **Operate with confidence:** Protective monitoring, Security Incident Event Monitoring (SIEM), security appliance management, incident response, advanced threat investigation services and threat intelligence analysis.

Cyber security as a business enabler

At CGI, we recognise that cyber security is an enabler for anything that a client wants to achieve. We build cyber security into a business strategy that drives competitive advantage, efficiency and growth by securing:

- New technologies—cloud, Internet of Things and mobile platforms.
- New ways of working—collaboration, mobile workforce and automation.
- Increasingly agile and globalised supply chains.
- Innovative, creative and collaborative business environments to attract the best talent.
- Organisations' compliance obligations.

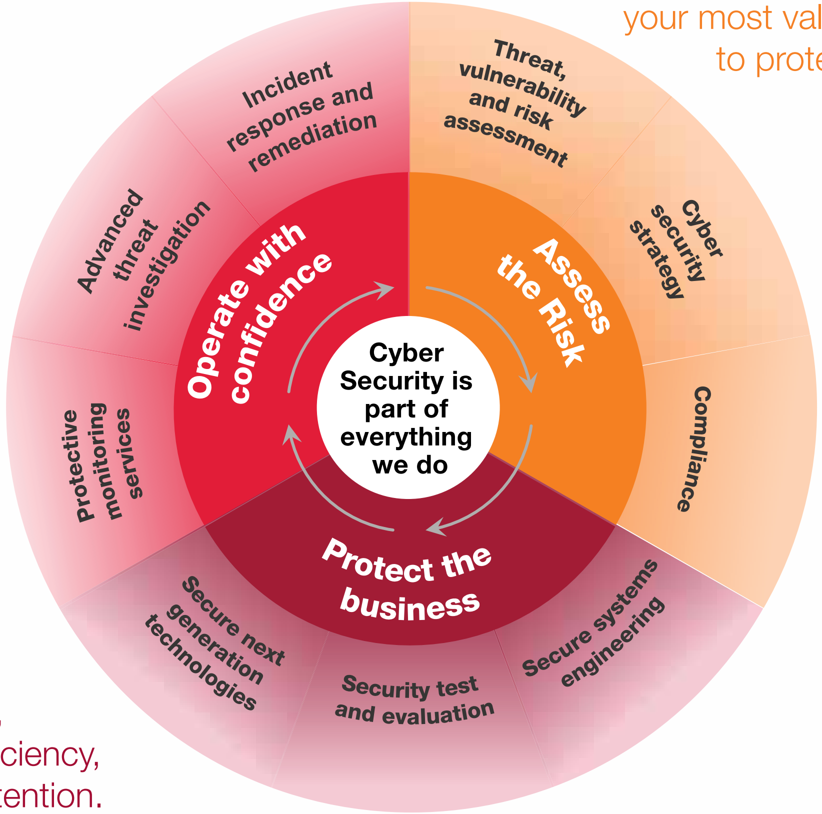
CGI's **approach**

Swift response to get an organisation operating after a cyber attack.

Protection against advanced and sophisticated cyber threats. Finding attacks that penetrated standard security defences.

Round-the-clock, end-to-end protection against cyber attacks and prompt action when events are detected.

Securing new technologies and ways of working (e.g. Internet of Things, mobile platforms, cloud, automation). Supporting agility, efficiency, cost savings, growth and talent retention.


Cyber Security is part of everything we do
Operate with confidence
Assess the Risk
Protect the business
Incident response and remediation
Threat, vulnerability and risk assessment
Cyber security strategy
Compliance
Secure systems engineering
Security test and evaluation
Secure next generation technologies
Protective monitoring services
Advanced threat investigation

Understanding the risks and vulnerabilities to your most valuable information. Learninging how to protect it at the right level of investment.

Creating and managing the organisation's cyber strategy, enabling business objectives, embedding security in businesses' processes and culture.

Ensuring compliance to standards such as Data Protection Act 1988, PCI DSS, ISO27001 and ISO22301.

Designing security into new complex systems, ensuring information is secure and only accessed by the right people.

Ethically hacking systems, networks and products to find vulnerabilities. Evaluating products and services for use in HMG UK systems, accredited to CTAS, CTA, CAS and Common Criteria.

Cyber security is a part of everything we do for our clients

In a digital world, customers will increasingly begin to perceive cyber security as an integral part of IT, outsourcing and business process services. They already demand a high level of competence in security from companies like CGI and this expectation is only likely to increase in the future.

Anticipating this, we ensure that cyber security is not just an add-on service for our client—it is an integral part of our IT strategy for every client.

How cyber security drives cultural transformation

CGI views cyber security as more than a technology solution. It’s a cultural change that covers:

- People.
- Processes.
- Technology.

For cyber security to succeed, all three elements must be addressed. Technologies must be used securely, processes must be designed to protect sensitive information and people must recognise that they have a fundamental role to play in ensuring security within their organisation.

Why **CGI?**

1 Deep expertise, backed by over 35 years of experience in supporting government and commercial clients as a trusted advisor on security.

2 Cyber experience across all market sectors, bringing expertise and insight from a wide variety of customer situations.

3 Experts who are respected as thought leaders—our approach to building secure systems was recognised by the UK's Institute of Risk Management and featured in its book Cyber Risk: Resources for Practitioners.

4 Close ties across trade bodies and government departments, including techUK and the CBI, help us to stay informed and influence emerging cyber security policy.

5 Global security evaluation expertise, with a commercial test and evaluation facility that has tested the products and services of over 25 global technology suppliers for 27 years.

6 Commitment to our customers, demonstrated by our clients' 100% success rate in achieving ISO 27001 accreditation.

CGI across the world

- Over 1,400 cyber security experts globally, who collaborate to share expertise, research, knowledge, capabilities and solutions.
- Three accredited security certification facilities in the US, UK and Canada.
- We have 3 Security Operations Centres globally.
- Our managed services support over 100 clients in 16 countries.

Examples of our **cyber security solutions**

- CGI has designed solutions for some of the world's most secure systems like Galileo – Europe's satellite navigation system, the UK's Police National Database and Ministry of Defence's Medical Information Capability programme.
- In the UK, our secure service will enable utility companies to access information on the energy usage of 53 million smart meters to be deployed from 2015.
- Our support has even enabled cyber security for the UK 2011 Census programme, assuring the privacy of 60 million citizens.
- We also continue to assess cyber risk for many of the UK's critical national infrastructure organisations.
- In the automobile industry, Volvo Car Group depends on CGI for security services.
- We also partner with Aon to provide cyber insurance risk assessment services for Finnish companies.
- CGI fights 75 million cyber attack incidents each day on military and intelligence networks.
- We have deployed and supported more than 9,000 biometrics systems and devices at over 100 worldwide locations, delivering more than four million biometrics enrolments each year for the US military.

Certified, secure cloud services

CGI offers secure cloud services through the UK's G-Cloud initiative, which helps public bodies quickly and simply select proven and flexible cloud-based IT services.

CGI was also the first large cloud provider to receive the US Federal Risk and Authorization Management Program (FedRAMPSM) cloud security certification, and one of the first to receive the Defense Information Systems Agency's (DISA) cloud security accreditation.

About **CGI**

Founded in 1976, CGI is a global IT and business process services provider delivering high-quality business consulting, systems integration and managed services. With 68,000 professionals in 40 countries, CGI has an industry-leading track record of delivering 95% of projects on time and within budget, aligning our teams with clients' business strategies to achieve top-to-bottom line results.

CGI

www.cgi-group.co.uk

Email: Cyber-enquires@cgi.com
Web: www.cgi-group.co.uk/systems-integration-services/cyber-security