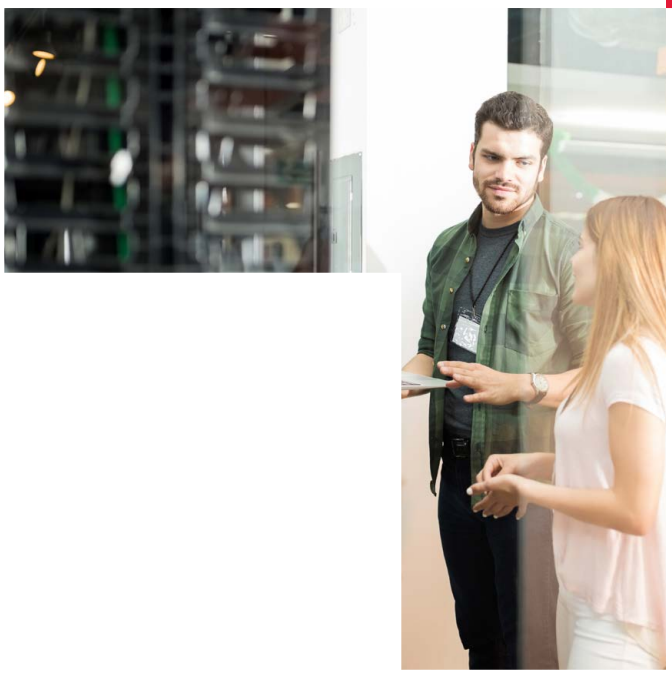
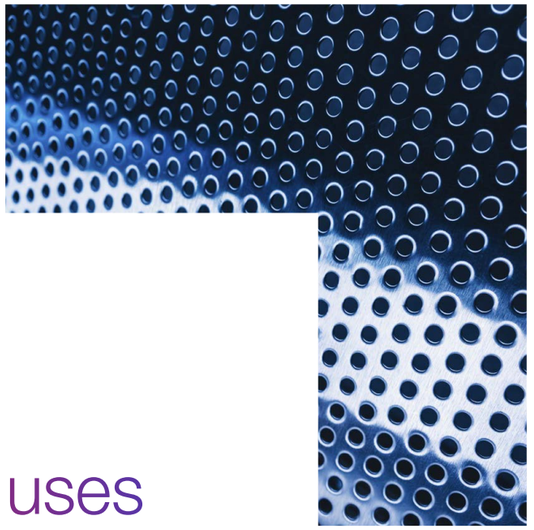


Penetration testing services

CGI's operational security division

Contents

In today's fast-paced world, keeping business and IT systems up to date and operational is a constant challenge.



Penetration testing uses simulated cyber-attacks to evaluate systems.

By subjecting them to external internet attacks and by considering potential insider threats, the tester checks for exploitable vulnerabilities.

In today's fast-paced world, keeping business and IT systems up to date and operational is a constant challenge. Cyber security threats continue to increase, so it is vital that any changes to systems include the correct security controls. For over 19 years we have security tested our clients' systems, ensuring business leaders can be confident that their organisations remain secure.

By using our penetration testing services to perform IT Health Checks at regular intervals, our clients stay one step ahead of potential attackers. Their IT systems can safely grow within their organisation without being open to attack.

Benefits of an IT health check

Identifies specific weaknesses in security that might leave an organisation vulnerable to attack.

Provides clear recommendations for vulnerability mitigation.

Delivers mitigation activity tailored to an organisation's systems and what it requires from them.

Supports a proactive security posture and confidence in the security of systems.

Penetration testing services

Why you need to take action

The vast majority of organisations depend on IT systems to operate effectively and competitively in this digital age.

These systems need frequent updates, and even small changes can introduce new vulnerabilities. Developers may work hard to ensure that their systems run effectively and that they have incorporated all necessary security controls; however, these security controls are not always evaluated to see if they have been implemented correctly or are fit for purpose. Most vulnerabilities are only discovered once they have been exploited, leaving the organisation open to regulatory fines, financial and reputational damage or theft of business-critical information or intellectual property.

How CGI's penetration testing service works

Our approach to your IT Health Check provides a thorough, objective and independent service while maintaining the flexibility to test a wide range of IT systems. We will carry out an initial evaluation and recommend the types of testing that are most appropriate for your situation. **These could include:**

Remote penetration testing

Using remote access to carry out a full range of tests. Remote testing uses cloud-based technology to assess your attack surfaces and security controls.

Testing Industrial Control Systems (ICS)

Specific testing to check your ICS security configurations to make sure they are correctly implemented and fit for purpose.

Testing telecommunications systems

Specific testing of your security configurations, including 'black box' provisions by operators, to make sure they are correctly implemented and fit for purpose.

Phishing simulation

Phishing simulations replicate techniques used by malicious individuals attempting to gain access to sensitive information, and help you understand the risks that phishing poses to your business.

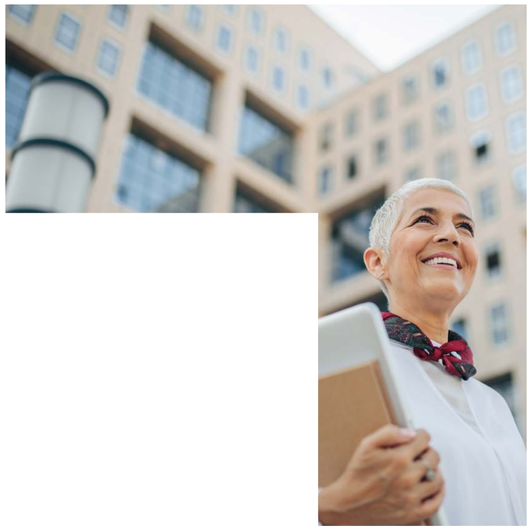
A red team engagement

Red teaming is a full-scope, multi-layered attack simulation designed to measure how well your people, networks, applications and physical security controls can withstand an attack from a real-life adversary.

Most vulnerabilities are only discovered once they have been exploited, leaving the organisation open to regulatory fines, financial and reputational damage.

Remote penetration testing

Although remote penetration testing is not a new concept, the need for it has grown in recent years thanks to the wide adoption of cloud services and technology such as software-defined networking. Remote engagements are ideal for situations where the cloud suppliers' physical infrastructure cannot be accessed.



More recently, the lockdown measures adopted by many countries in response to the coronavirus pandemic has made remote penetration testing, even on traditional in-house infrastructure, a necessity. Plus, organisations supporting home working have opened up their internal network boundaries to include their employees' home networks. This increases the attack surface of the organisation and means that good security hygiene and practices are more important than ever.

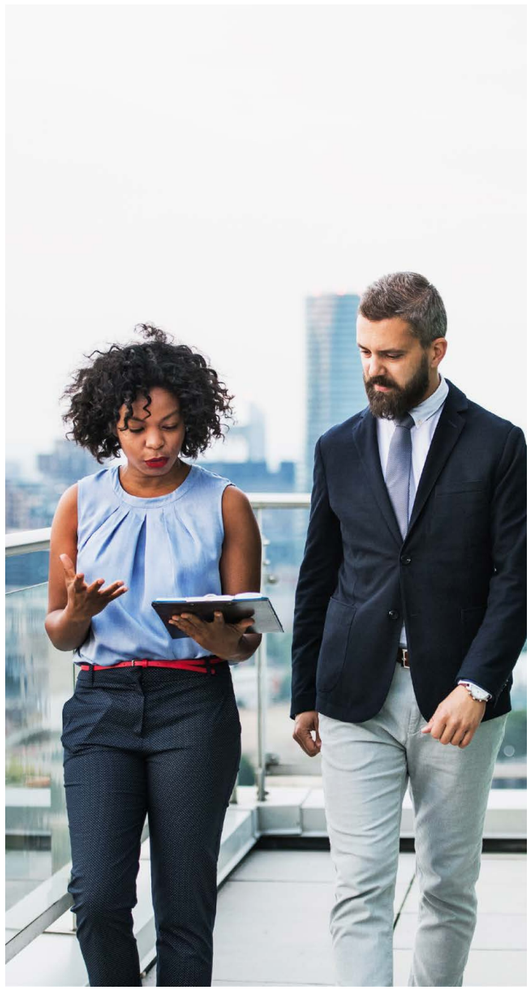
Organisations supporting home working have opened up their internal network boundaries to include their employees' home networks.

How CGI's remote penetration service works

Our remote penetration testing solution is flexible, adaptable and will be integrated fully into your environment. We understand that there is no 'one size fits all' solution, we offer a number of different VPN setups. This ensures we can always choose the connectivity set up best suited to your environment and the boundary security measures implemented by your organisation.

	Type of VPN	
	Existing client VPN	**CGI Pen Test VPN**
Hardware appliance	✔	✔
Virtual machine	✔	✔

Our VPN infrastructure is designed and configured in line with the guidance published by the National Cyber Security Centre (NCSC), following NCSC's VPN best practice recommendations, advice, policies, protocol recommendations and cryptography requirements. It uses proven technology and is secured by multi-factor authentication.

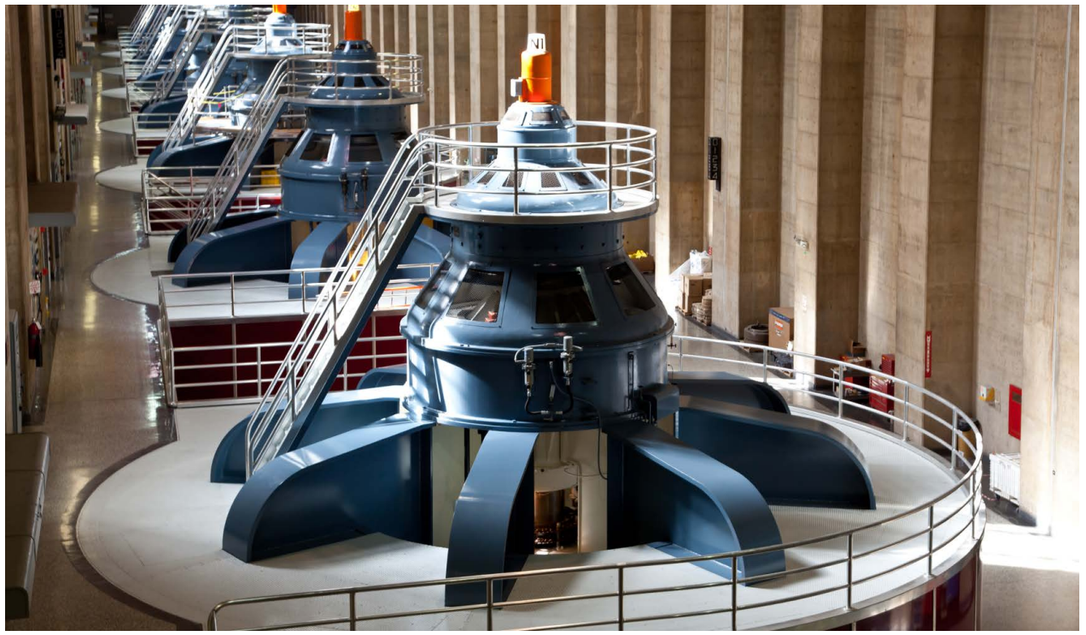


Testing Industrial Control Systems (ICS)

Heavy industry organisations control and maintain complex and critical infrastructure throughout the UK, serving multiple industries within the public and private sectors. Innovation within this industry is fast paced, so the ability to operate efficiently, effectively and, most of all, safely, is essential.

Industrial Control Systems allow you to monitor and adjust your operations to ensure your systems run effectively and safely, with all necessary security controls in place. However, many protocols and processes used within ICS are created with weak configurations and are not always tested to make sure they have been implemented correctly, and that they are fit for purpose.

Frequently, equipment that is known to be insecure, is inadvertently connected to wider organisational networks, significantly increasing the risk to ICS components. It is also recognised that ICS equipment is known to not prioritise security, which can lead to multiple vulnerabilities. This can leave the organisation open to safety breaches, regulatory fines, financial and reputational damage or theft of business-critical information or intellectual property.



How CGI's ICS testing service works

We provide a thorough, objective and independent service that has the flexibility to test a wide range of IT systems safely. The following are a sample of the operational technology and ICS that may be tested as part of the assessment:

- Authentication, authorisation, and accounting functions (AAA)
- Software defined networks (SDN)
- Programmable logic controllers (PLC)
- Data historians
- Human-machine interface (HMI)
- Remote terminal units (RTU)
- Supervisory control and data acquisition (SCADA) and distributed control system (DCS) systems
- ICS specific and proprietary protocols.

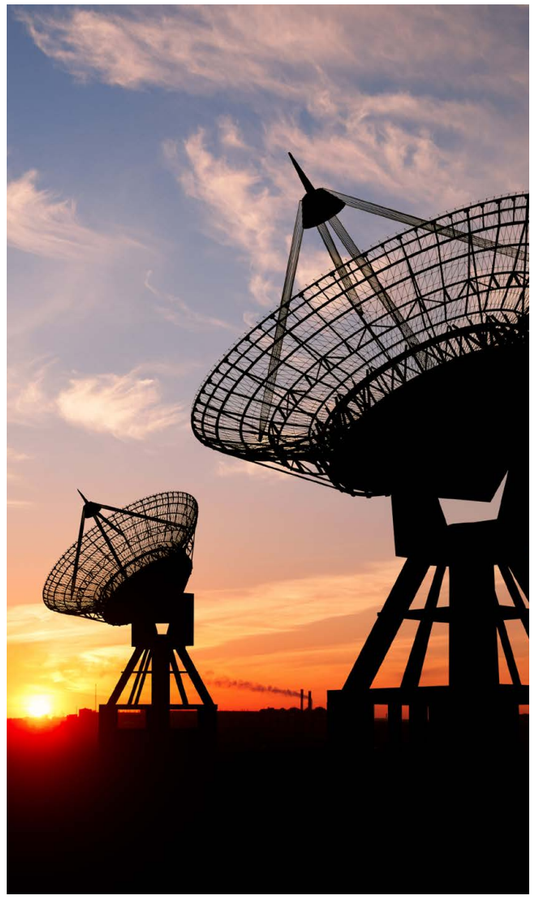
Many protocols and processes used within ICS are created with weak configurations and are not always tested to make sure they have been implemented correctly.

Testing telecommunications systems

Telecommunications organisations construct and maintain significant, complex and critical infrastructure globally, serving multiple industries within the public and private sectors. Innovation within the telecoms industry is fast paced, so the ability to operate efficiently and effectively with a competitive edge is essential.

Telecommunication operators work hard to make sure that their systems run effectively and that the necessary security controls are incorporated. However, many organisations, for business or technical reasons, do not always examine whether these security controls have been implemented correctly or are fit for purpose. Especially in the case of 'black-box' implementations; these are delivered and expected to function securely, but this is rarely the case in practice.

We provide a thorough, objective and independent service that has the flexibility to test a wide range of IT systems safely.



How CGI's telecommunications testing service works

We provide a thorough, objective and independent service that has the flexibility to test a wide range of IT systems safely. The following are a sample of telecommunications infrastructure that may be tested as part of the assessment:

- Authentication, authorisation and accounting functions (AAA)
- Software defined networks (SDN)
- Network function virtualisation (NFV/VNF)
- Evolved packet core (EPC)
- IP multimedia subsystems (IMS)
- Telecoms messaging service (SMPP/UCP)
- Operations support systems (OSS)
- Subscriber data management (SDM)
- Signalling transport (SIGTRAN)
- Telecoms specific and proprietary protocols.

Phishing simulation

You have probably received phishing emails. They often disguise themselves, making it look as though they have come from a trusted sender and typically contain a malicious attachment or a link directing you to a website that captures your information.

Not all phishing attacks are opportunistic; attackers also target individuals who have access to the business information they want, or whose access they can use to achieve their goals. This may involve a period of information gathering to craft a message that the recipient is likely to act upon. This technique, known as spear-phishing, has been successfully used in several large-scale breaches in recent years and has grown in sophistication over time. It can be extremely difficult, even for a seasoned security professional, to determine whether a well-crafted spear phishing message is legitimate or not.

Phishing is a growing threat and widely available free tools mean even attackers with little skill can penetrate sophisticated network defences.

How CGI's phishing simulation works

We replicate the steps that a malicious attacker would take. This tests the response of your staff, locating weaknesses so you can set up a remediation plan that will put you in a better position to keep your data secure, should your business or staff be targeted.

Our consultants will work with you to tailor our phishing service to your needs, generating the information that will allow you to make informed decisions.

We will create a bespoke solution on our dedicated penetration testing platform to ensure a reliable test that delivers relevant results.

Any data we capture related to your business will be stored and handled with care. The testing information we gather is stored securely using industry-standard encryption technologies combined with strong access controls.

At the end of the simulation, we will provide you with a report containing a detailed analysis of the data we have obtained so you can grasp the risks to your business. This will include a list of respondents, their IP addresses, the date and time of the response, the type of device used and other metrics.

We can perform three types of simulated phishing attack against your business:

Level 1

Low sophistication campaign

- Simulating an opportunistic, low-skilled attacker.
- Using an email that is easily identifiable as a phishing attack. This will typically contain spelling mistakes, grammatical errors, or formatting issues.
- It will contain a link that directs the user to a landing page informing them how to detect phishing attacks.

Level 2

Mid-level sophistication campaign

- Simulating a deliberate, but hastily designed, attack by a mid-skilled attacker.
- Typically, the email will be less identifiable as a phishing email. It will imitate your corporate mailshots, using email addresses which, at a glance, somewhat resemble your corporate domain.
- We will send it using a dedicated infrastructure set up to high standards to help fool automated scanning tools.

Level 3

High sophistication campaign

- Simulating a premeditated, planned and orchestrated attack by a highly skilled attacker.
- It will be able to capture credentials and other sensitive information through a variety of techniques.
- We can create and deliver customised executable attachments.

Red team engagements

A red team engagement is typically most valuable when you have a firm understanding of your security posture, potentially through discrete penetration tests. It provides insight into the overall interconnectivity of your systems and how broader security mechanisms and policy protections can be circumnavigated, in a way that regular assessments do not.

Red team engagements are an important part of the assurance process, helping you to understand existing risks and how a malicious user could exploit them. They are not a direct substitute for regular penetration testing or an IT Health Check (ITHC). In fact, they are best used in tandem with other assessments because an ITHC assures a particular system or network, but a red team engagement takes a less detailed view of specific infrastructure or systems. Instead, it takes a holistic view of the attack avenues available to a malicious actor and the extent to which those avenues can be exploited.

What happens in a red team engagement?

Red teaming does not have a 'one size fits all' approach. Red team activities include:

- Complete network enumeration.
- Infiltration of your enterprise network to determine if it is possible to further access the targeted networks/hosts.
- Infiltration of your network through simulated third-party links or infrastructure with direct connectivity to the target network.

Red team engagements are, by necessity, broad in scope, but you will achieve the most useful outputs by establishing a narrow set of objectives and then remaining flexible about how these are achieved. Your objectives can range from exploring specific systems, to specific activities and/or focusing on the avenues highlighted as most at risk.

Generally, our primary objectives for red team engagements are:

- To demonstrate that a given objective is either achievable or unachievable within the time allocated at the point of testing.
- To provide clear recommendations for vulnerability mitigation that are both straightforward to implement and tailored to the required functionality of the system under test.
- To help you understand the security posture of particular sections of your infrastructure.
- To evade detection, by circumventing security controls and interacting with the target systems in ways that could be considered normal usage. That is not to say exploitation does not take place, but it is weighed against the prospect of our activities being flagged.

An important part of the assurance process, helping you to understand existing risks and how a malicious user could exploit them.

How CGI's Red Teaming Service works

Our initial approach is orientated around scoping. This involves identifying target networks or hosts, assimilating the risks belonging to those networks, and formulating objectives for the engagement.

During scoping, we consider:

- Target networks and hosts
- Potential methodologies, e.g., physical security, phishing, open-source intelligence
- The bounds of operation, including out of scope items and methodologies
- The objectives of the engagement
- Levels of interaction with the blue team (if required)
- Specific infrastructure requirements necessary for the engagement to start, e.g., domain registration for phishing.

Once scoping is completed and you have accepted our proposal, we will put together your red team to match the requirements identified by scoping and introduce them to you. The team will include a primary point of contact to coordinate with you, provide regular progress updates, and request permission for certain activities of specific concern (e.g., affecting a system that is considered or believed to be of particular sensitivity).

We always bear in mind we are red team testing in a live environment and that it is critical that your systems remain stable. We restrict activities that often cause disruption, such as Man-in-the-Middle attacks, to specific targets (unless the risk is understood to be negligible). Our methodologies are shaped by years of experience and closely relate to the MITRE ATT&CK guidelines.

Naturally, all our security testing is carried out within the law. In the UK, this means that we comply with the provisions of (among other acts of law) the Computer Misuse Act, the Data Protection Act and the European Convention on Human Rights. In general, these articles of law require us to obtain specific, preferably written, permission to test IT systems from their owners and the owners of the data that resides on, or is carried by, them.

A red team engagement in action

Objective

To conduct an adversary simulation against an organisation's corporate network and users, with their central payment system as the overall target.

Preparation

Our technical team worked closely with the client to determine key targets and to formulate the likely objectives of a malicious actor.

Process

We began the engagement by gathering the publicly available footprint of the network and its userbase, using a combination of open-source intelligence and physical reconnaissance to determine any weak links that stood out.

We acquired a target list and made phishing attempts that included custom payloads, to connect back to our bespoke, UK-based command and control network. This was successful, and we made connections to client machines via CGI owned and registered domains (designed to mask suspect outbound traffic). Once we had an initial foothold, we started enumerating the enterprise, identifying attack paths to key targets from our positions.

One of the hosts we accessed was a SYSTEM-owned service that used Dynamic Link Libraries. We were able to modify these by devising shellcode and injecting it into the legitimate file. The service was configured to run automatically on start-up, so it was a waiting game until the payload was invoked and we achieved privilege escalation. We found local administrator passwords were being reused and confirmed this by using our new level of access to pass its NT hash, leveraged from the Security Account Manager database.

On a broader level, we used a range of different attack methods to allow us lateral movement to gain access to different systems so we could achieve our key objectives. One of these methods involved leveraging the Kerberos network authentication protocol that uses tickets to identify communicating nodes securely. The system was using service accounts associated with Service Principle Names, meaning that these tickets could be requested from the domain controller on its behalf. Loading these tickets into memory on the compromised systems allowed us to travel further through the networks.

As we drew closer to our intended targets, we had to devise increasingly intricate methods to protect our penetration efforts and remain undetected. We identified a high-value database target with a weakness; we found a blind SQL injection vulnerability on a front-end web application where Boolean responses can be deduced by exploiting expected output via unexpected means. Even though obfuscation techniques had been applied on the database, we created an application to exfiltrate the data.

The algorithm within our application was designed to run through the maximum possible permutations based on the previous output of the blind SQL injection vulnerability. This was done to increase efficiency, reduce network load, evade detection and counter the obfuscation techniques applied within the database. We increased efficiency further by changing the query methods into lightweight, non-intrusive, parallel processes where each Boolean response determines the next phase of the injection. The parallelism was also extended to the logic used for data exfiltration.

Results

Our successful penetration meant that any data held in the database could be freely altered without detection (including addition, deletion and modification). We could also revert the database back to a previous state to conceal malicious activity, and we could exfiltrate data at a large scale.

Once we had compromised the key targets, we used the remaining time of the engagement to locate different attack paths while creating more and more noise to test detection rates, as neither the initial intrusion or database enumeration was detected.

With our objectives complete, we produced a full report along with comprehensive executive and technical summaries. At the client's request, we delivered a wash-up presentation to key parties which the participants noted as being very beneficial in helping them to understand the outcome.

Our methodologies are shaped by years of experience and closely relate to the MITRE ATT&CK guidelines.

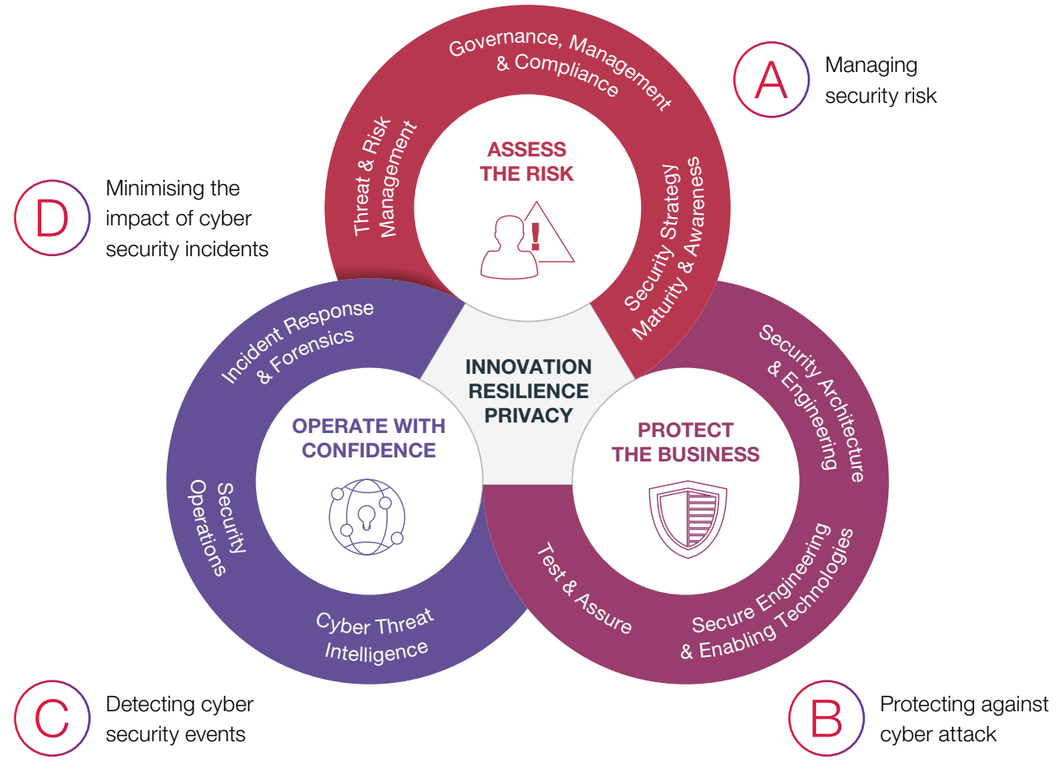
Why CGI

We have long lasting relationships with our clients, and this gives us detailed and unparalleled insight into the risks they face, allowing us to deliver effective solutions. We've been working for defence, government and international commercial clients for over 35 years, ensuring their business-critical systems and services are secure.

As a founding member of the NCSC CHECK Scheme, we have one of the longest established histories in the UK of providing IT Health Checks and penetration testing services to multinational and government organisations.

Our team holds qualifications by CREST, Tiger and Offensive Security. We offer a broad range of testing methods, which are normally combined to provide the balance of testing each individual client needs.

Cyber security wheel



In today’s fast-paced world, keeping business and IT systems up to date and operational is a constant challenge. Cyber security threats continue to increase, so it is vital that any changes to systems include the correct security controls.

Make an enquiry

If you know who your contact point is within CGI, then simply reach out to discuss the options best suited to your requirement.

For general enquiries, please email: **cyber.enquiry.uk@cgi.com**

About CGI

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industries in 400 locations worldwide, our 77,000 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

Our commitment: Insights you can act on.

For more information, visit cgi.com/uk/cyber-security or email us at cyber.enquiry.uk@cgi.com

CGI