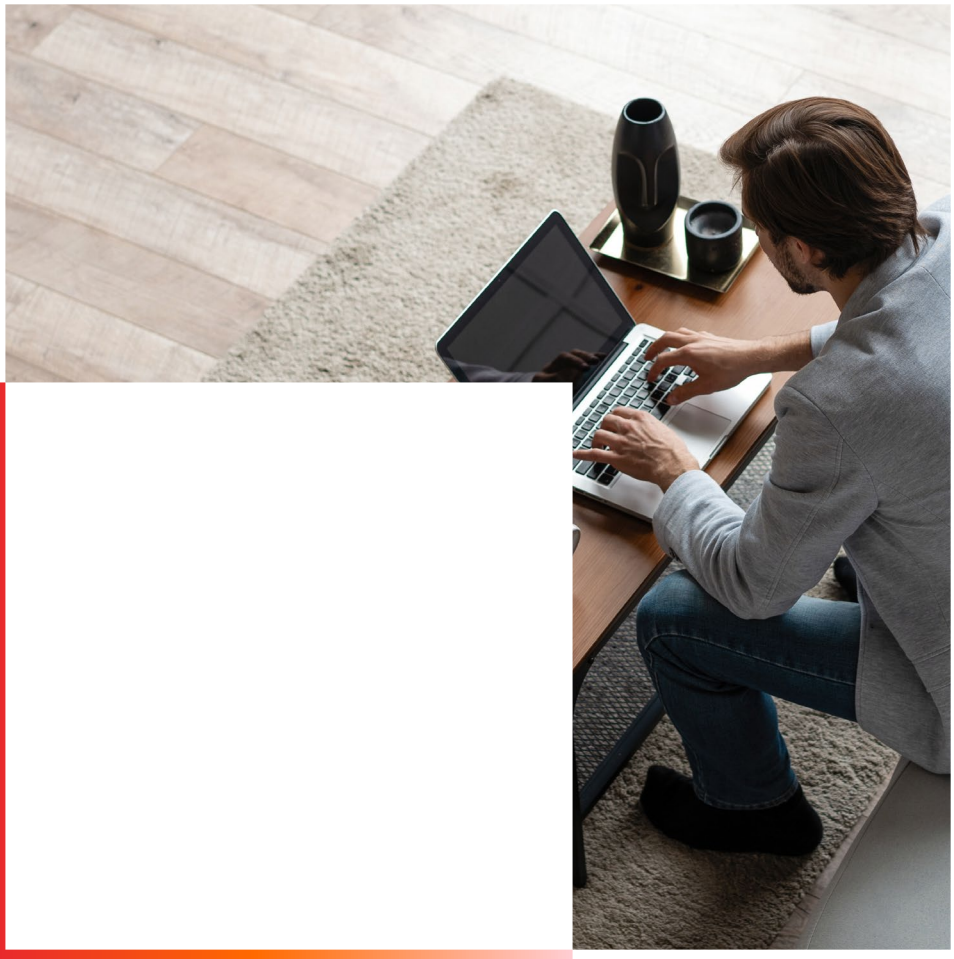


Cyber security

CGI's Digital Forensics and Incident Response (DFIR) Service

Contents

CGI's Digital Forensics and Incident Response (DFIR) team can provide an advanced level of security resilience that organisations simply cannot achieve alone.

Cyber security is part of everything we do

CGI's Digital Forensics and Incident Response (DFIR) Service.

Incident response (IR) is more than just the actions taken immediately following a cyber security compromise, attack, or breach. IR is also about raising your capability to deal with such an incident, and so improving the speed with which your business recovers.

Digital Forensic (DF) investigations can range between providing straightforward security assurance to answering specific questions. Targeted investigations can provide answers about a wide variety of issues, from a suspicious URL to when and where your critical data has gone and who moved it.

CGI's Digital Forensics and Incident Response (DFIR) team can provide an advanced level of security resilience that organisations simply cannot achieve alone. With the latest in DF hardware and software plus skilled and qualified personnel, our service offers the highest standards of forensic investigations. Our experts can provide support and evidence for an internal HR matter or in support of an IR matter that's being undertaken by CGI or a third party.

Benefits

- Minimise the impact of cyber-attacks and understand how they happened.
- Ensure peace of mind and quality assurance thanks to CREST accreditation.
- Choose from flexible service levels that suit your needs.
- Benefit from 24/7 assistance with rapid response.
- Enable your business to respond and upskill with insights and advice from industry leaders.
- Receive dedicated support from an assigned Service Delivery Manager who will make sure any issues are addressed.
- Protect your 'corporate credibility' with an enhanced security posture.

Why you need to take action

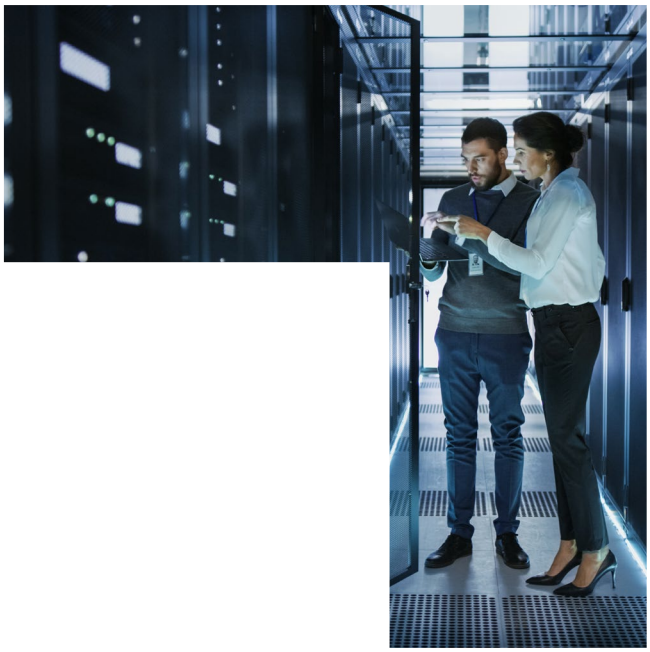
Understanding why cyber-attacks happen and building resilience to them can be complex and extremely challenging without the right expertise or knowledge, but it is absolutely vital for security. Increasingly organisations are finding they need external support in order to deal with attacks and prevent them from happening again.

Take for example two incidents which happened to two unconnected businesses at the same time, involving the CVE-2019-19781, a remote code execution vulnerability found on unpatched Citrix servers. Following the publishing of a proof-of-concept code which showed how to exploit the vulnerability, there were breaches around the globe. CGI stepped in to help these two publicly listed companies. Although dealing with both incidents in parallel was easier due to the shared vulnerability, it was still a significant result to remediate both incidents and have normal services back up and running within 48 hours. Imagine if this had been your business but you had been operating alone.

In fact, not all engagements result in finding a 'bad guy'. A number of recent engagements have resulted in there being no supporting evidence of a bad actor, yet we were able to attribute system anomalies that had all the hallmarks of a malicious actor. This included the apparent exfiltration of over 20GB of data from a UK government department. On detailed examination of the device and network logs, it was actually data coming into the network from a badly configured server being used for legitimate purposes.

In another matter, a major UK construction firm reported an unauthorised, remote third-party was controlling two of its laptops. Examination of the devices showed this not to be the case and attributed the mouse movements and unexplained document access to badly configured driver updates.

Without external support, businesses can struggle to identify where an attack is coming from and who the attacker is – leaving them with unanswered questions and vulnerabilities which make it impossible to resolve incidents or build future resilience.



Following the publishing of a proof-of-concept code which showed how to exploit the vulnerability, there were breaches around the globe.

Our approach

Our DFIR team maintain knowledge of current threats through various channels including the CiSP (Cyber Security Information Sharing Partnership) programme run by the National Cyber Security Centre (NCSC) as well as our own, in house, Cyber Threat Intelligence (CTI) team.

Our experts use a range of licenced and open-source software to support their work. The net result is that we are already on a forward footing when you request assistance.

Although the DFIR team is tool agnostic, we use endpoint detection and response (EDR) solutions which perform a variety of essential tasks, helping defend your network, speed up incident response and provide an excellent framework from which to assess your network's security stance.

At all stages of a DF examination the evidence produced is treated as if the matter was being progressed through the courts of law, ensuring compliance with legal obligations under GDPR and the Human Rights Act. Evidence and exhibits are subjected to stringent Chain of Custody controls and investigations are conducted with the tried and tested ACPO Principles of Forensic Investigation.

Our experts use a range of licenced and open-source software to support their work. The net result is that we are already on a forward footing when you request assistance.

Dependent on the service you choose, you will receive contact from the DFIR team in as little as 30 minutes from your initial call.

For IR engagements the DFIR team align to the CREST CSIR process. In 2020 CGI Security Operations received CREST Accreditation for its cyber security IR service. Within this methodology are **three key stages** when reacting to a cyber-attack:

Prepare

During an onboarding workshop, we will study your existing DF and IR systems and procedures and familiarise ourselves with your network and environment. We will also make suggestions for possible improvements to help you become even better prepared for any eventual cyber security incident. After this we will organise a follow-up workshop to provide you with clear metrics on how your IR stance has improved over the term.

Respond

As soon as you inform us of a breach our response action is triggered and, depending on the retainer level selected, our IR team will immediately start work to identify the exact nature and extent of the incident. We will then issue guidance on how to contain the incident in order to minimise disruption. Following containment, we work quickly to ensure the restoration of your systems - returning your business not just to a pre-incident state of operations, but a more secure state.

Follow up

Following the resolution of the incident, we provide an in-depth and detailed report. In our follow-up meetings we focus on how to prevent such a problem arising again, plus details of how the response to the incident can be improved to become more efficient and effective. In some ways, this is the most important element of the IR model as it feeds back and informs the “Prepare” phase with the most critical and relevant intelligence generated by an attack on your systems.

Why 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 hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

CGI's DF service is staffed by ex-law enforcement and military personnel. With experience in high profile fraud, malware, APT and international investigations, the team has an extensive background in sensitive and complex digital forensic investigations.

CGI Security Operations are a significant supplier to the Government, providing protective monitoring services from one of our UK Security Operations Centres to organisations including: The Ministry of Justice, The Crown Prosecution Service, Central Government, The Ministry of Defence, and also local authorities such as Edinburgh and Glasgow City Councils and Greater London clients.

Offering CREST accredited, 24/7 onsite or remote response to your cyber security incidents, CGI provide a level of technical expertise and support suitable for your business needs. Whether providing in-depth DF examination of devices in support of an investigation or a full IR managed service which takes full ownership of the incident, there will be a solution for your requirement.

Without external support, businesses can struggle to identify where an attack is coming from and who the attacker is.

Choose a level of service that suits you

An initial consultation with your CGI Cyber representative will allow you to fully explore which service tier is most suitable to your organisation.

The service has been designed to allow the customer a choice and our experts will cover the key areas and benefits against each of the options detailed below.

Baseline:

Retainer Level: **Small**

- Initial IR maturity assessment during on-boarding workshop.
- 180 hours Per Annum (2 days per month) remote IR and IRM service.
- 8x5 remote coverage of DFIR work.

Enhanced:

Retainer Level: **Medium**

- Initial IR maturity assessment during on-boarding workshop.
- 270 hours Per Annum (3 days per month) remote IR and IRM service.
- Cyber Security Training – Security Awareness training at client premises.
- IR Planning – Assisting the client in IR preparations: framework creation, playbook writing and process improvements.
- 24x7 remote on-call response for DFIR work.

Advanced:

Retainer Level: **Large**

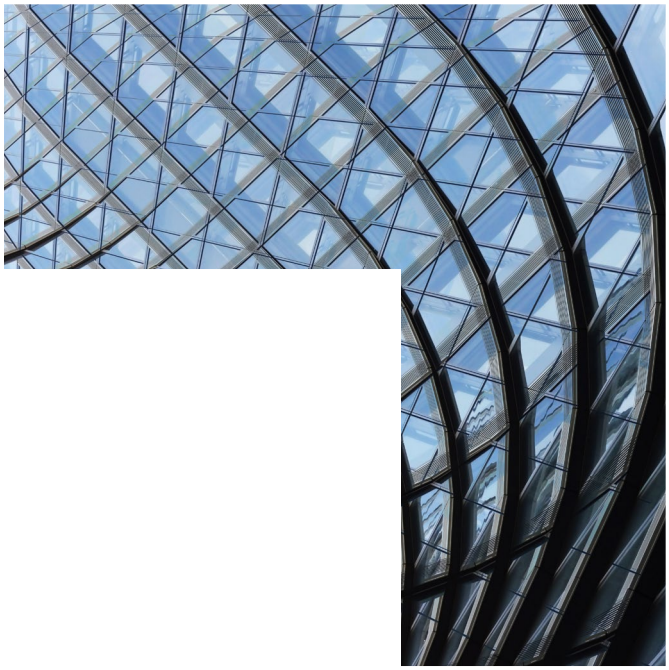
- Initial IR maturity assessment during on-boarding workshop.
- 360 hours Per Annum (4 days per month) remote and onsite IR and IRM service.
- Cyber Security Training - Security Awareness training at client premises.
- IR Planning – Assisting the client in IR preparations: framework creation, playbook writing and process improvements.
- Cyber Incident Simulation – Training delivered at client premises.
- 24x7 remote on-call response for DFIR work with on-site capability.

Digital Forensic (DF) investigations can range between providing straightforward security assurance to answering specific questions. Targeted investigations can provide answers about a wide variety of issues, from a suspicious URL to when and where your critical data has gone and who moved it.

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 82,000 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