

Cyber Security and the Digital Led University

- An Advisory Services PoV



Our range of cyber security services will meet any potential needs of your university, and can be implemented as individual modules to fit with your existing services, or provided as a fully managed service.

Threat actors targeting universities



Access brokers – seek to gain access to the university network and then sell access on to other attackers.



Nation state actors – seek to steal intellectual property and research.



Resources specialists – a number of groups seeking to gain access to university resources to sell on to other students.



Opportunity attackers – often seek out organisations that are running vulnerable software that they can exploit.



Insider threat – students or staff with legitimate access to the network either knowingly or unknowingly causing damage or removing data.

Infection vectors

Recent attacks against university sectors identify the following as key vectors for infection used by threat actors:



Remote access – attacker makes use of RDP or VPN vulnerabilities.



Phishing – used to install malicious software or harvest user credentials.



Poor security practices – weak passwords, lack of multifactor authentication and other poor practices.



Unpatched software – vulnerabilities within legitimate software targeted in order to gain a foothold.

The cyber threat

The higher education sector has always faced a greater cyber security challenge than most other industries; this is due to the very nature in which universities need to operate:

- Freedom of information is essential
- Large, accessible networks
- A wealth of confidential data held
- Prevalence of bring your own device usage
- Support requirements outside of academic terms
- Internet of things (IoT) and access to lab equipment, machinery, printers, etc. (all operational technology)
- Students studying cyber skills may even practice in-house.



“Ransomware attacks can have a devastating impact on organisations with victims requiring a significant amount of recovery time to reinstate critical services.” - NCSC 2021

- At least 6 UK universities succumbed to significant ransomware attacks in 2021.
- The average recovery cost from ransomware is estimated to be £2 million, but is likely more.
- Ransomware is increasingly used to target our universities.
- In the last year, attacks resulting in compromised data occurred 101 times, up from just 15 incidents five years ago.
- National Cyber Security Council (NCSC) data highlights increases in ransomware attacks on the UK education sector during August-September 2020, and again in February, May and June 2021.

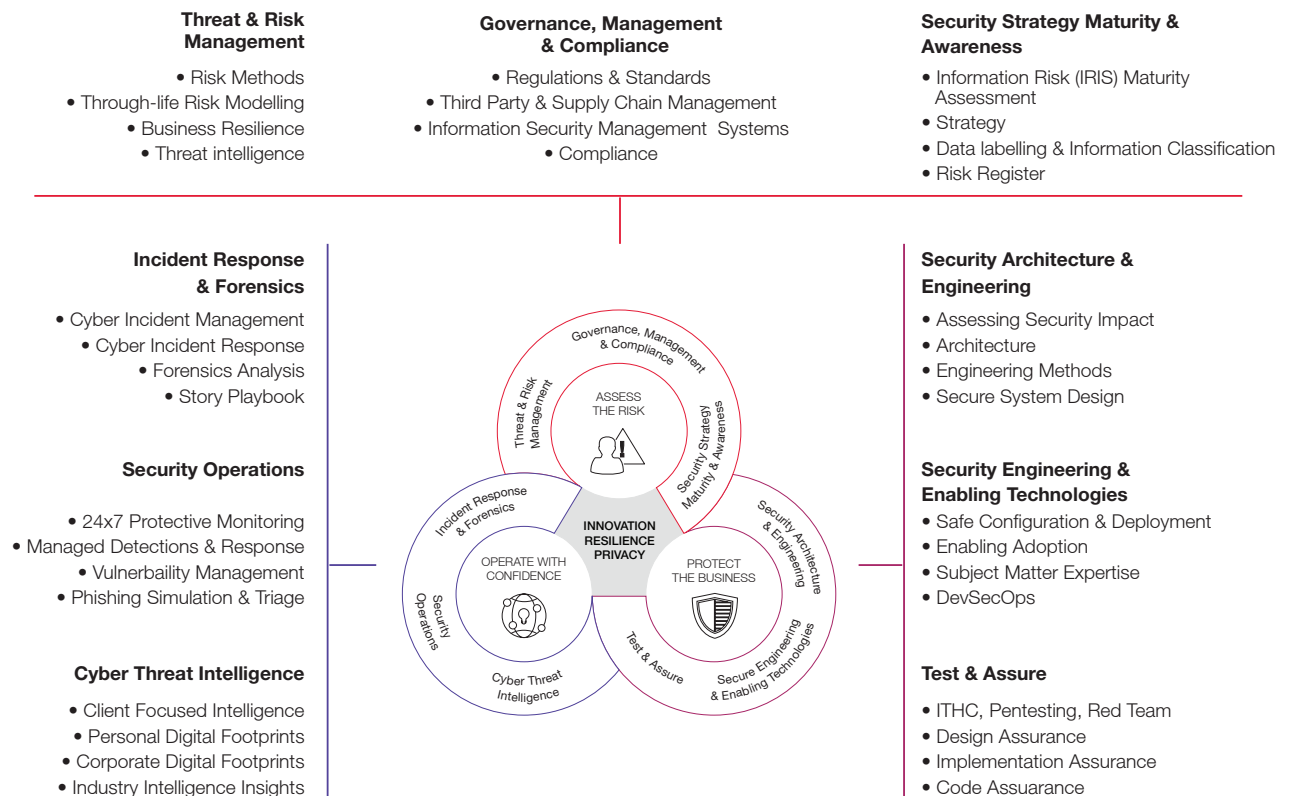
Recent unprecedented world events have only made academic life more challenging, with the rapid need to develop remote working methods that enabled academic personnel and students to continue operating safely through these difficult times.

Our integrated cyber security services

Our proven range of cyber security services are available to meet all of the potential needs of your university. These can be implemented as individual modules to fit in with existing established services, as replacements to areas of concern, or as a fully managed service to free up existing resources for other important activities.

CGI Cyber Security Services

Cyber security is part of everything we do.



Security operations centre (SOC)



An internally managed SOC can work well for very large campuses, nevertheless, they require a lot of funding and are a challenge to operate in a climate where universities face increasing cyber attacks and ever-changing vulnerabilities, alongside skill shortages.

When setting up and running a SOC, you must consider:

- People - retaining key staff, maintaining and updating skillsets, managing the headcount required to operate 24x7x365, morale, stress management, holiday, sick and training cover, etc.
- Systems - latest technologies and tools, hardware and software refresh, log management, patch management and ticketing.

- Processes - change control, process and procedure, threat intelligence, incident management and conforming to regulations, etc.
- Cost - controlling moving budget requirements, no economy of scale, salary changes.
- Other - scalability and flexibility, limited trend analysis as only dealing with a single environment and not multiple customers.

So setting up and maintaining a SOC is no easy task! For this reason, 64% of SOC's are outsourced to specialist partners like CGI.

Our SecOps services

Protective monitoring

- CGI's most comprehensive, hands-on service
- Our analysts monitor security events and alerts from your environment in order to identify malicious activities and attacks
- 3 service tiers to meet your requirements, dependent on your risk profile and the device counts within your network.

Analyst as a service

- CGI's most efficient protective monitoring service, often referred to as the "eyes on glass"
- Simple to integrate via your SIEM or via cloud-based products
- On-premise or cloud options
- 3 service tiers to meet your requirements.

Cyber threat intelligence

- CGI's CTI provides the most current intelligence on existing and future threat vectors
- Threat workshops and bespoke threat reporting
- 3 service tiers that can extend services to CDFA and dynamic malware analysis.

Phishing defence service

- CGI's phishing defence provides awareness training and a rapid reporting function for simulated campaign emails
- Learning management system included across all 3 tiers
- Malware analysis
- Search and remove malware inside an organisation.

Digital forensics and incident response

- DFIR is our OpSec's incident response service based on a retainer pricing model
- Retainer-based option allows for days to be called off each month, with on-site resource available
- Digital forensics is available as a stand-alone service and can support internal systems.

Vulnerability management

- This offering is via a 4 stage process: network discovery, scan of environment, reporting and remediation support
- Custom and standard reports
- 3 service tiers to meet your requirements.

Helping to mitigate your risks

Managing security risks in an increasingly connected and open academic environment demands an insights-driven, integrated security approach. We help you exploit technologies to deliver value quickly and securely.

Our digital risk management advisory services include:

- Integrated risk management - managing risks and linking near real-time source data to risk assessments, supported by custom visualisations for unique user needs.
- Cyber transformation service framework - using a programmatic approach to provide a holistic view of security risks and maturity that enables you to balance, scale, prioritise and justify your security investments.
- Privacy and compliance assessment - including privacy impact, privacy risk, health assessments and recommendations.
- Supply chain resilience and risk assessment - assessing the confidentiality, integrity and availability of university suppliers and their services, recommending an approach for managing them.
- Cyber security crisis preparedness - using our library of up-to-date crisis scenarios and crisis simulations to help you prepare for crises before they happen.



Why CGI?

We hold all of the certifications you would expect from a leading cyber security partner:

- +82,000 members, +400 locations, +40 countries – we are one of the largest IT, cyber and business consulting services organisations globally.
- +190 IP-based solutions.
- 95% projects on-time, on-budget.
- 9.3/10 client satisfaction score.
- 9 SOC's worldwide, 2 of which are UK-dedicated, managing public and private sector clients including universities.
- In the UK alone, we have +250 cyber security professionals covering a broad skillset.
- We develop and operate a security program supported by a comprehensive enterprise security management framework.
- We define technical and organisational measures that form a minimum security baseline.
- Our 5 star SDI accredited service desk provides our clients with the support they need, when they need it.





About CGI

Insights you can act on

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.

For more information

enquiry.uk@cgi.com

cgi.com/uk

