Cyber security and the Digital Led University

CGI higher education insights

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 universities 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 education sector is the most targeted industry in the world for cyber crime, with 79% of higher education organisations globally reporting they have been hit.

The higher education sector has always faced a greater cyber security challenge than most other iindustries. 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
- Funding struggles creating a lower level of resourcing and technology
- 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.

Combined, these act as weaknesses which are exploited and targeted by adversaries. And recent unprecedented world events have only made academic life more challenging, with the need to rapidly develop remote working methods to enable academic personnel and students to continue operating safely through difficult times.

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

- At least 5 UK higher education organisations have succumbed to significant ransomware attacks in 2023 (as of July).
- The average recovery cost from ransomware is estimated to be £2 million, but is likely more. For those organisations that can restore their data from backups, the average cost still remains high at an estimated £1.2 million.
- Ransomware is increasingly used to target our universities.
- Third party breaches create equal risk, with universities becoming the victims of ransomware attacks on occasions where their suppliers were the original targets.

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.

Threat & Risk Management

- Risk Methods
- Through-life Risk Modelling
- Business Resilience
- Threat Intelligence

Governance, Management & Compliance

- Regulations & Standards
- Third Party & Supply Chain Management
- Information Security Management Systems
- Compliance

Security Strategy, Maturity & Awareness

- Cyber Maturity Assessment
- Strategy
- Data Labelling & Information Classification
- Risk Register

Incident Response & Forensics

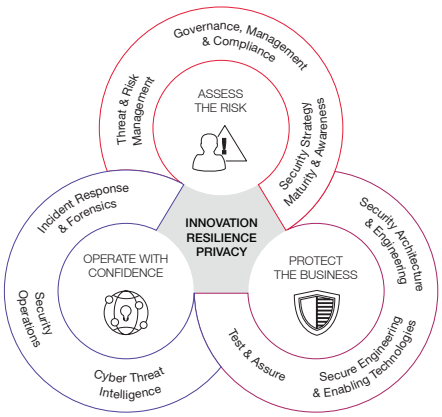
- Cyber Incident Management
- Cyber Incident Response
- Forensics Analysis
- Table Top Exercises

Security Operations

- 24x7 Protective Monitoring
- Managed Detections & Response
- Vulnerability Assessment
- Phishing Simulation & Triage

Cyber Threat Intelligence

- Client Focused Intelligence
- Vulnerability Prioritisation
- Brand Impersonation Detection
- Credential Leak Reporting



Security Architecture & Engineering

- Assessing Security Impact
- Architecture
- Engineering Methods
- Secure System Design

Security Engineering & Enabling Technologies

- Safe Configuration & Deployment
- Enabling Adoption
- Subject Matter Expertise
- DevSecOps

Test & Assure

- Penetration Testing, Red and Purple Teaming
- Design Assurance
- Implementation Assurance
- Code Assurance

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.
- 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, we recommend outsourcing your SOC to a specialist partner.

With cyber security as a managed service, you can rest assured that your SOC analysts are looking at all possible cyber issues and wider trends, not just those typically associated with the higher education industry.

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 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.

Phishing defence service

- CGI's phishing defence provides awareness training and a rapid reporting function for simulated campaign emails.
- 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 a 4 stage process: network discovery, scan of environment, reporting and remediation support.
- Custom and standard reports.

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.
- IT health check - a thorough, objective and independent service with the flexibility to test a wide range of IT systems. By using our penetration testing services to perform IT health checks at regular intervals, you'll stay one step ahead of potential attackers.

Why CGI?

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

- 91,500 members, +400 locations, +40 countries – we are one of the largest IT, cyber and business consulting services organisations globally.
- +170 IP-based solutions.
- 95% projects on-time, on-budget.
- 9.3/10 client satisfaction score.
- 9 SOCs worldwide, with a UK-based SOC 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

cgi.com/uk/higher-education