

Defending your organisation against digital security threats



Our cyber security expertise

- protecting assets, preventing attacks, and effectively responding to breaches.

No organisation is immune to cyber threat, but our cyber security specialists will help you reinforce your technical defences and ensure your response to potential attacks will be effective. We'll help you identify and fill critical capability gaps and understand the risks from human, physical, and technical perspectives so you can manage them appropriately and strengthen your security.

1

SECURITY TESTING

Security testing enables our clients to understand vulnerabilities that are relevant to the threats they face, and the work required to address them. We offer a range of CREST-registered intrusive and non-intrusive testing services to evaluate systems, policies and people, and prioritise plans. Our services can be tailored precisely to meet your requirements.

Our security testing services include:

- Penetration testing vulnerability assessments
- Build and configuration reviews
- Red Team testing
- Social engineering/phishing assessments
- IT Health Checks

They are conducted by experienced practitioners, certified to the exacting standards that the UK Government and industry require from their advisers, testers, accreditors, and auditors.

2

INCIDENT RESPONSE

While cyber-attacks and data breaches may be outside of your control, how your organisation responds to, and recovers from them is. Effective planning means an effective response; minimising the impact of a cyber-attack on your operations, reputation and bottom line.

Our Incident Response services include:

- Proactive prevention and preparation
- Reactive emergency response
- Consultancy around strengthening security measures
- Consultancy on developing in-house detection and response capability

We offer a UK Government-approved incident response service to give our clients ongoing assurance, including in support of insurance obligations.

3

INFORMATION ASSURANCE

Our experienced and qualified team of consultants will help you develop information security management systems, achieve compliance against international and national standards (such as ISO 27001, PCI DSS and the health sector's DSPT), and comply with relevant data protection legislation.

Our consultants tailor their approach to each business that they work with, ensuring any new processes that you choose to implement blend effortlessly with your existing business model. We believe that information security should work for you, not the other way around.

4

MATURITY ASSESSMENTS

We work at Board level to identify security gaps and risks to critical assets and then build security strategies, mitigation measures and investment plans. Using our Cyber Security Maturity Model, our consultants analyse your organisation's cyber security and compliance requirements to establish the effectiveness of current security measures. They also use the model to evaluate whether the current position aligns with organisational maturity targets based upon risk appetite, stakeholder expectations, and regulatory/legal requirements. Understanding your position highlights areas for improvement and facilitates investment prioritisation to keep your data and reputation safe.

How our clients use our services

Holistic Incident Response

We'll ensure you have considered every aspect of your Incident Response because we understand that a technical response only solves one part of the puzzle. We help our clients undertake proactive measures like security testing, maturity modelling, and facilitated exercises to ensure they are adequately prepared. We'll provide peace of mind with our Incident Response and digital forensic services, which aim to get systems back online as soon as possible to limit disruption. Finally, we will develop a comprehensive understanding of your organisation's vulnerabilities to help you protect against future threats. This may come in the form of an assessment to ensure all vulnerabilities have been remediated, such as

- Our Cyber Security Maturity Model
- The identification and implementation of an appropriate Information Security Management System
- Security testing

Supply Chain Security

Many of the world's largest cyber-attacks have been enabled by compromised suppliers. Accordingly, GDPR, NISD and most insurance policies demand management of supply chain security. We help organisations of all sizes to find practical, low-cost ways to categorise and improve their supply chain cyber security to the standard required to manage the risk each supplier represents.

Adherence to Regulatory Requirements

The risks of non-compliance with regulatory requirements, such as the NIS Directive or GDPR, can be both financial and reputational. Our clients come to us to ensure they are implementing compliant controls that aren't unnecessarily disruptive or expensive. We work with our clients to help them embed proportionate controls that enable, not disable operations.



Why choose PGI?

Every business is different; size, scope, complexity, structure, and sector all impact the security measures required for your level of risk. PGI can deliver the security solution that best suits your business because:

- We take a tailored approach with all our clients to ensure we understand all relevant aspects of the business we are working with and what is already in place. We use that as a framework before suggesting the most pragmatic route to achieving compliance.
- Our intelligence-led approach helps prioritise the work and allows cost-effective planning.
- We have in-depth experience in supporting a wide range of national and global organisations to identify and implement pragmatic solutions to the cyber threat.
- We are technology-agnostic, which means we can also provide impartial advice on products and deliver the most effective and affordable service possible for your needs and budget.
- Our team of cyber security specialists are qualified to the highest national and international standards. They are selected from relevant backgrounds to deliver world-class cyber security consultancy and services, including;
 - intelligence
 - security
 - law enforcement
 - multinational corporations
 - critical infrastructure protection