KING’S KNIGHT GROUP

Mitigating risk in an uncertain world

CYBER SECURITY AND DIGITAL FORENSICS

Pro-active Management of Cyber Security Risks

The impact from cyber security risks can have a severe impact on a company’s share value, reputation and culture, and every organisation is a potential victim. Weaknesses in the approach to cyber security open opportunities for either targeted or un-targeted attacks.

If an organisation is targeted specifically, the attacker has a definite interest in the business information and activity. Groundwork for such an attack may take weeks or months of planning, establishing the best route in exploitation of the business and damaging systems, or obtaining restricted data such as client and personnel information. Targeted attacks include spyware, spear-phishing, a Trojan horse, worm malware and blended threats, the sending of emails to specific individuals that may contain attachments or a link to download malicious software, or deployment of a botnet to deliver a ‘Distributed Denial of Service’ (DDoS) attack.

We establish a governance framework that enables and supports a consistent approach to cyber security risk management across the entire organisation. We provide guidance at board level to review risks and understand new challenges and emerging threats to technology and systems security.

Guidance – A Dynamic Approach

When an organisation loses information, the causes are usually one of the following elements; human error, printed documentation, electronic devices such as laptops, tablets or memory sticks, and surveillance devices. We provide necessary guidance in the application of security controls to successfully address these risks, and how they are incorporated within an organisation’s overarching security strategies.

We offer pro-active security and pre-emptive defence concepts to create a complete strategic understanding of cyber-crime and possible future trends. This is achieved with relevant threat intelligence specific to an organisation, and the provision and regular testing of effective response countermeasures against cyber-crime.

Whilst hackers are frequently in the news, it is a company’s personnel and other insiders that pose the largest threat to keeping a company’s information secure. The mitigation of information risks being reduced from employees, printed documentation and information technology systems, is achieved by refining existing access control procedures, system privileges and enhancing need to know policies. We assist in developing and managing these procedures, and also provide appropriate awareness training relevant to the role of employees, demonstrating a company’s commitment to cyber security and promoting a strong risk management culture.

CYBER SECURITY AND DIGITAL FORENSICS

Integrated into a comprehensive information security programme, our team also provides forensic analysts who are able to extract evidence from systems, enabling us to identify and focus on security concerns, to help improve our client's resilience and business continuity.

Red Teaming

We provide confidential adversary strategy based reviews using controlled and realistic processes for assessment and security testing purposes. A key benefit is to enhance appropriate decision making in respect of information technology, and ensure a security led approach with both immediate and long term organisational strategies.

Digital Forensics

Computer and internet related crime leaves trails of digital evidence, and whether the crime is cyber-bullying, drug trafficking, fraud, unauthorised sharing of confidential information, corporate espionage or acts of terrorism, we are able to critically follow the electronic trail and recover information. We implement this by analysing data and retaining evidence in its original form, enabling our findings to be admissible in a court of law.

For evidence to be admissible, it must be reliable and not prejudicial. Therefore, admissibility is our primary concern at every stage of computer forensic examinations. Our guidelines in this respect are as per the Association of Chief Police Officers Good Practice Guide for Digital Evidence and Good Practice Guide for Computer-Based Electronic Evidence.

Any computer may be constituted as a 'scene of a crime', i.e. with hacking or denial of service attacks, or hold evidence such as emails, internet history, documents or other files that may be relevant to crimes. In addition to the content, the metadata associated to these files is also of interest to an investigation team. Metadata details a chain of information relating to devices including; the location and time of creating, viewing, downloading, copying or amending, and printing of documents, emails and websites, and which user will have carried out such actions.

We provide bespoke protective security solutions to governments, corporate clients and individuals worldwide.
For further information in respect of our services, products or training, please contact us on:
E: info@kingsknightgroup.com
T: +44 (0) 1403 800 234
Your enquiry will be dealt with in total confidentiality.

www.kingsknightgroup.com