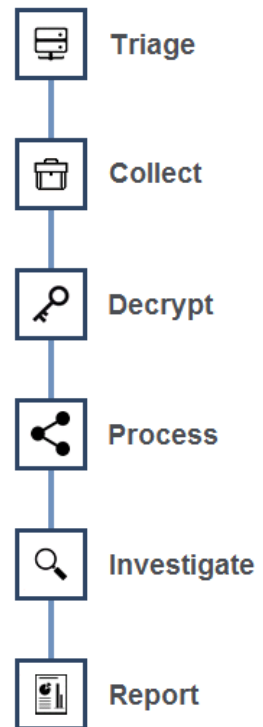# Security Incident Response and Cyber Forensics

Kaon SecurITy specialise in the human factors side of information security and provide services to a range of Local Government, Central Government and Commercial Enterprises in Australia and New Zealand. In our history we have worked to develop long term relationships with our clients and built a level of trust that is key to ensuring they keep their systems, data and people secure.

The company is acknowledged for its regional leadership in helping organisations improve their security posture. A typical engagement entails developing a strategic and holistic view of Information Governance and IT Security leading to programmatic improvement. Tactical advice is also readily on hand as the dynamic nature of technology means a "set and forget" approach to IT Security has limited effectiveness.

Information technology is an integral part of all enterprise operations so our consultants are well versed in communicating in the right terms to people at all levels within an organisation on topics including risk, assurance, governance and IT operations.

- Triage
- Collect
- Decrypt
- Process
- Investigate
- Report

www.kaonsecurity.com.au
www.kaonsecurity.co.nz

Overview

Very few businesses can function without the use of technology in today's world. Our increasing digital connectivity has brought many business benefits, however this connectivity and other advancements in technology has also opened up an opportunity for people to engage in malicious behaviour making Cybercrime a big business.

It is now common place to hear of organisations being hacked, dealing with Ransomware demands or battling a Distributed Denial of Service (DDoS) attack. Whilst many organisations have endeavored to mitigate against threats and attacks, the attackers are proving to be well organised and quick to exploit all manner of vulnerabilities.

Kaon SecurITy can quickly react to a cyber attack to initially combat it and limit the damage to your organisation. Thereafter our consultants can conduct an investigation to understand the cause of an attack and assist you put in place countermeasures to mitigate the risk of further possible incidents.

Cyber Forensics

The hyper connected digital world presents some unique challenges for any organisation that needs to investigate issues concerning data breaches, malware outbreaks e.g. ransomware, or the misuse of organisational systems and data, that potentially could lead to legal and employment action. The use of mobile technology, adoption of Cloud services, increased levels of virtualised systems, combined with the ongoing use of traditional or legacy computer platforms, means many investigations are becoming more complex.

Kaon SecurITy are here to assist Senior Executives and Management Teams with these types of challenging and complex issues.

We follow a forensic investigation strategy using six stages to identify the existence of digital evidence, to secure it and then interpret that evidence.

- Triage
- Data Collection – capture, search and secure at site after an incident
- Decryption and examination of data
- Process and interpret the data
- Investigate including interviews of witnesses and suspects
- Data reporting

The basic objective of conducting forensic investigations is either to identify anomalies in order to avoid further breaches or to collect supporting evidence for employment or legal proceedings. Ordinarily investigations follow a defined approach, however in order for findings to be admissible in court during legal proceedings, investigation methods must follow strict legal guidelines.

To undertake comprehensive and legally acceptable cyber forensic investigations requires suitably qualified experts with adequate knowledge of IT technologies, cyber laws, LGOIMA, litigation, compliance, forensically sound investigation techniques and proven industry experience. A qualified expert investigator from Kaon SecurITy can go to the extent of triaging a significant volume of evidence, system logs and security best-practice in order to assist an organisation clear up matters after a data breach and recommend how to mitigate further breaches.

Incident Response and Cyber Forensics Service

Kaon SecurITy have established a capability to provide incident response and cyber forensics services that utilise the Guidance Software Encase Forensic platform to conduct investigations.

This platform is supported by specialist hardware – F.R.E.D – or Forensic Recovery of Evidence Device – these systems are capable of handling the most challenging computer case having being designed specifically for both the rapid acquisition and examination of computer evidence.

The combined software/hardware capability allows us to –
- Acquire data from the widest variety of device types including over 25 different types of mobile devices such as smartphones, tablets, and GPS.
- Complete a comprehensive, forensically sound investigation.
- Produce extensive reports on findings while maintaining the evidence integrity.

The services are performed by our analysts who are certified to internationally recognised standards - Cyber Forensic Professional – European Union (CCFP-EU) and Computer Hacking Forensic Investigator (CHFI V8.0).

Our core service offering
- Data collection and preservation
- Internal and/or external incident response
- Forensic analysis and data analytics