DATA SHEET | Cyber Forensic Investigative Services

What Is Cyber Forensics?

Cyber (or digital) forensics is an electronic discovery technique used to determine, reveal and preserve technical criminal evidence in a way that is suitable for presentation in the court of law.

Cybercrime Fast Facts

- ✓ South Africa has the *third-highest* number of *cybercrime victims* worldwide – the country loses an estimated R2.2bn a year to cyber-attacks
- ✓ South Africa ranks *sixth* on the list of *most-targeted countries for cyberattacks*, with the greatest concentration of affected businesses scoring the highest rank of 300+ (extreme exposure) on the Cyber Exposure Index
- ✓ *Cybercrime* ranks as the second most frequently reported type of fraud and is recognised as the *most disruptive and serious economic crime* expected to impact firms in the next two years
- ✓ Over the next five years, economic *loss* due to cybercrime is predicted to *reach $5.2 trillion*
- ✓ 58% of cybercrime targets small businesses, with the global cost of cybercrime standing at $600 billion in 2018.

**Source World Economic Forum, Verizon Data Breach Investigations Report, South African Banking Risk Information Centre, PwC 2018 Global Economic Crime Survey*

Working with Cerebus

Cerebus Cyber Forensics keeps abreast of the everchanging cyber environment and threats. By partnering with Cerebus Cyber Forensics, you are assured of your readiness before, during and after an attack.

We provide organisations with peace of mind when navigating the complexity of digital incidents, such as fraud, theft and industrial espionage.

We aim to establish the following:

- ✓ Details of the incident including the data that was compromised and the time of the incident
- ✓ Motive(s)
- ✓ Uncovering the responsible person(s)
- ✓ Weakness in the cybersecurity system that led to the attack.

Digital Investigation

Preserving digital evidence that is critical to the event is of the utmost importance. With a focus on authentication and chain of custody preservation, our technical team uses court-tested and defensible techniques for collecting and preserving information. We analyse the available data so that accurate conclusions can be drawn regarding the fundamental cause of the event.

Expert Testimony

Cerebus Cyber Forensics' team have vast experience with collecting and identifying digital evidence, as well as with interpreting and presenting this information for litigation. Findings are documented in an *expert report* crafted by highly experienced computer forensic professionals with world-class pedigrees, certifications and significant court testimony experience.

Our Assurance

- ✓ Full visibility of increased threat in current cybersecurity system
- ✓ Incident response and remediation
- ✓ Identify and traces paths of Advanced Persistent Threats (APT)
- ✓ Investigate motives for attack
- ✓ Expert report admissible in a court of law
- ✓ ISO certified lab
- ✓ Ethical conduct ensuring complete confidentiality and sensitivity.

Stages of The Investigation

Identification

In the identification phase, potentially responsive electronic documents are identified for further examination and review.

Preservation

A duty to preserve begins as soon as there is reasonable anticipation of litigation. During preservation, data that is identified as pertinent to the case, is placed in a legal hold. This ensures that the data cannot be tampered with or destroyed.

Collection

Data collection is the process of extracting potentially relevant information from its native source.

Processing

The processing phase involves preparing the collected information. This is typically performed by specialised software, and can include the extraction of text and metadata, removing of duplicates, performing keyword searches and converting files.

Review

The review typically involves the evaluation of the identified and processed information for relevance.

Production

The data that is identified as relevant must be produced for use as potential evidence. e-discovery rules and procedures will address how these documents must be produced.

Services

Fraud investigations

Employment disputes

Intellectual Property theft investigations

Data breach or any other such suspicious activity

Cyber audits

Real-time asset tracking