ansec
an Outsource Group Company

The importance of Digital Forensics in the cyber security and audit world

With the increasing frequency of cyber threat due to the reliance organisations now place on IT, digital forensics has become an important part of the cyber security and audit world.

Expedited by the global pandemic, today data is stored on a wide range of digital devices, making it increasingly easy for hackers planning a cyber-attack.

The term forensics has been used for many years and has its origins in the Latin word *forensis,* meaning *"pertaining to the forum",* or as we now refer to it, the *courts*. Cyber crimes are not easy to investigate because the crime scene exists in the digital world. Digital forensics is a branch of cybersecurity which focuses on the recovery and investigation of material found in digital devices. It is the process of identifying, preserving, analysing, and documenting digital evidence to a standard that can be presented as evidence in court, if required.

This can include civil cases, employment tribunals and even internal disciplinary hearings. A common factor is that all hearings will require evidence to be produced to the highest possible standard before it can become admissible.

An often missed point is that digital forensics can also be used as an audit tool to independently assure controls are effective before an incident occurs; for example, checking that group policies are in place through reviewing a randomly selected sample of the organisation's end point devices (phones, laptops etc.).

In a digital forensic process, the type and location of data may not be known or fully understood. It could involve the recovery and analysis of deleted or hidden data and the analysis of artifacts from inaccessible areas of the file system which need to be interpreted by the expert and ultimately presented and explained to the court. This will often require an opinion to be given, which in a court will require the person providing the evidence to be considered an expert in their field.

Businesses seeking digital forensics services need to act fast to ensure the digital evidence is preserved for the investigation process. One of the most common issues in digital forensics is that an organisation will request an investigation into something that happened months prior, only to discover that their software licencing only retains log files for one month or that logs have been overwritten before being backed up to a secure location. It is not uncommon to find that computers have been in regular use since the alleged incident or even that they have been wiped and reallocated to another member of staff. This can often have a negative impact on the outcome of the investigation.

An unwanted incident can lead to a wide range of issues including insurance claims and legal matters. Therefore, having a forensic readiness plan in place can assist your organisation in its response to any incident by ensuring that vital digital evidence is collected, preserved and protected by competent staff using approved methods. Having a forensic readiness plan can also minimise the costs of investigations, block the opportunity of cyber threat and show due diligence and good corporate governance as well as determining the next logical steps your business needs to take to ensure your cybersecurity. Indeed, many government departments and agencies are now required to have a forensic readiness policy in place, as the government security policy framework states that, *“well-tested plans, policies and procedures will reduce organisations’ vulnerability to security incidents”*.

Effective leadership is a critical component of good security and accountability. It is ANSEC’s recommendation that the leadership team in any organisation should give serious consideration to the implementation of a forensic readiness policy if they have not already done so.

While many organisations are currently aware of the need for business continuity plans, they should also consider the need for a forensic readiness plan to minimise the potential issues that could arise and to ensure that digital evidence is gathered appropriately and treated with due care.

Equally, audit teams should consider whether testing a random sample of devices will provide additional assurance and potentially assist in the prevention of an incident in the first place.

Background

ANSEC have provided digital forensic services within the UK, Ireland and Europe for over 10 years with a team of experienced investigators. For more information contact:

Peter Leitch

ansec

Founding Partner | ANSEC IA Limited | Direct: +44 (0) 28 9448 2901 | Mobile: +44 (0) 7760282156 | Email: Peter.leitch@ansecia.com

Offices: Antrim | Belfast | Cookstown | Dublin | Edinburgh

An Outsource Group Company, 4, Plasketts Close, Kilbegs Business Park, Antrim, County Antrim, BT41 4LY. ANSEC IA Limited is registered in Northern Ireland. Registration Number: NI 064909.