



PCI – Qualified Forensic Investigator

A significant data compromise that becomes newsworthy places a company brand and reputation at significant risk. The ultimate result can be the demise of companies, which has occurred in both Europe and the USA once the trust of customers has been lost.

A data compromise, if you are unfortunate to suffer one, potentially involves all key parts of your organisation and in the first few days an organisation's ability to continue with business as usual (BAU) is under threat. For these reasons, it is crucial for all organisations to have a fully developed Incident Response Plan (IRP) that is tested at least annually, which is one of the requirements of PCI DSS.

IRM is a Qualified Forensics Investigator approved by both VISA and MasterCard. As such, IRM is able to assist merchants with digital forensics investigations and incident response following security breaches.

Evidence gleaned from a forensics investigation can help pinpoint the root cause of a compromise, in addition to accurately identifying the possible scope of data that has been lost. IRM is also able to provide advice about how best to manage security incidents and what steps to take to contain any security breach without compromising the chain of evidence.

A QFI Investigation will help establish:

- How the perpetrators gained access to the various systems
- What was breached and exactly what information was viewed/accessed
- Who was involved in the compromise
- A timeline for the compromise
- What remediation work would be required to prevent reoccurrence
- Whether the organisation was compliant with the relevant standard(s) at the time of the compromise, which will affect liability
- A chain of evidence in the event that law enforcement authorities become involved.

The quality of any forensic investigation is dependent on detailed server logs being securely stored and those logs providing sufficient detail at a level which captures what each individual user has accessed on any system. It will also be dependent on the cooperation of any third party service providers.

About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.

Information Assurance
Risk Mitigation
Business Resilience
Compliance

