



## Client

Private multinational company

## Project Background

This client receives significant revenue through on-line activities and had gone through a PCI DSS accreditation process. They also have regular external vulnerability assessment scans performed by a third-party.

A system administrator discovered a server had unexpectedly crashed. An internal investigation led the client to understand that a security breach had occurred in an Internet-connected web cluster. This compromise had involved over ten servers in different network and involving different technologies.

The client needed to understand the scope of the breach and any data that had been obtained. This would then allow appropriate regulatory authorities to be notified.

IRM was originally approached to provide specialist forensic resources to assist the internal investigative staff.

## IRM's Approach

IRM sought to work closely with the internal client staff who had been investigating the breach to date. IRM provided specialist hardware and software for imaging of affected servers and analysis.

As servers were delivered back to the client office IRM imaged the disks in a forensically sound manner such that any evidence on the disks would not be compromised should a police investigation occur. IRM performed keyword searches across the files from the servers, including those that had been previously deleted.

Potential malicious or non-standard activity on servers was documented and reviewed with internal staff to determine those actions that were business as usual or otherwise legitimately performed by internal system administrators. The resulting evidence was integrated into a timeline of the attack and further systems identified that may also have been compromised.

Non-standard software on the compromised systems was assessed to determine its function, method of operation and communication with other systems. Privilege escalation exploits, Trojans and backdoors were identified that communicated with overseas IP addresses. One such external IP address was subsequently imaged and found to contain card holder data and customer database information.

### FAST FACTS

#### Geography

- ▶ UK

#### Challenges

- ▶ Identify the scope of breach
- ▶ Identify source of attacks and data obtained
- ▶ Identify if card holder data had been compromised

#### Solutions

- ▶ Incident Response
- ▶ Digital Forensics

#### Results

- ▶ A detailed timeline of the breach
- ▶ A report detailing the approach used to gain unauthorised access to systems, software and data

**Information Assurance**

**Risk Mitigation**

**Business Resilience**

**Compliance**





### What IRM delivered

IRM produced regular reports detailing evidence identified, other systems to be assessed that may have been accessed during the breach, potential keywords that could be used in searching other systems and IP addresses of external systems accessed during the breach or used by malicious software for external communication.

A detailed timeline of the breach was co-developed with internal staff allowing events to be cross-checked and verified.

A formal report was provided detailing the systems assessed, analysis performed, the approach used by the external attackers to gain internal access to systems, software components used and a summary of the critical events in the security breach. The report was drafted such that it could be presented to the Board or to external authorities such as the Information Commissioner's Office.

### Benefits to the Client

IRM provided expertise and specialist hardware/software to aid the internal security team in analysis of the security breach. The provision of such resources allowed the creation of a detailed picture of the breach to be created significantly faster than with internal resources only. This speed was required by the Board to determine potential media responses and disclosures to external authorities. IRM's approach to analysis was such that evidence could be relied upon forensically in court.

### What the Client did next

Appropriate disclosures were made to external authorities and the local police force. The discovery that card data had been compromised required that an independent QFI investigation be performed for PCI purposes. IRM did not participate in this having worked with the internal team during the earlier phases of the investigation.

A review of information security policies and processes across the organisation was initiated to prevent future security breaches.

**Information Assurance**  
**Risk Mitigation**  
**Business Resilience**  
**Compliance**

