CCL GROUP

protecting
responding
investigating

Internal Investigation

Case study

The case

Internal investigation into the conduct of a number of members of a sales team who it alleged had been stealing high value stock and selling it on for private gain. The potential losses were in the region of £5m.

The requirement was to forensically collect any email data stored locally on the individuals' laptops. The company's email policy limited employees to 100MB mailboxes meaning that a culture evolved of employees archiving email locally to their laptops and desktops.

The client was unwilling to undertake an overt exercise, as at this stage, there was no way to independently confirm the veracity of the allegations. In addition, they were unable to collate a definitive list of suspects and were concerned that an overt investigation would tip off other individuals involved in the activity, who would then have the opportunity to cover their tracks.

What CCL did

CCL deployed a remote forensic toolset onto the client's network, and covertly deployed servlets onto the individuals' laptops and desktops. This allowed our forensic analysts to remotely access data stored on these devices without the knowledge of the users.

Given the severity of the allegations, and that the client was considering pursuing criminal charges, the entire process had to be defensible. ACPO guidelines were followed and contemporaneous notes were kept.

Over a number of months email data was acquired from all of the suspects' laptops. This data was aggregated into an investigation platform where it was keyword searched.

The Outcome

The investigation revealed that individuals from the sales team had been stealing stock and that several individuals from various areas of the business were also involved in the fraud.

The individuals had developed a practice of appending additional stock items onto large value orders at 0 value. The customer would often not notice that these had been added on, as the total of the order was unchanged. The warehouse staff would then ship the items as they were present on approved invoices. At a later date, one of the sales team would phone the client and inform them that an item had been shipped in error and would arrange collection of this item. The collected item would never make it back to the warehouse.

The analysis of email was able to uncover not just the method employed, but also evidence of the practice, including emails referencing occurrences and modified invoices submitted for approval.

Digital forensic Services

- Digital investigations advice
- Computer forensics
- Mobile device forensics
- Data recovery
- CCTV forensics

Other CCL Services

- Search orders
- Cell site analysis
- Social media data collection
- E-Disclosure

CCL Solutions Group Ltd

Office Address: 36 Cygnet Court, Timothy's Bridge Road,
Stratford-upon-Avon, Warwickshire, CV37 9NW

t. 01789 261 200 f. 01789 262 525 e. info@cclgroupltd.com
www.cclgroupltd.com