

# MANAGING DEFECTIONS

HOW CAN FIRMS MINIMISE THE DAMAGE OF TEAM DEFECTIONS? MANAGING DIRECTOR JULIAN PARKER OF DIGITAL RISK SPECIALIST STROZ FRIEDBERG REVEALS HIS INSIGHTS AND EXPERIENCES

## FIVE THINGS YOU WILL LEARN FROM THIS MASTERCLASS:

- 1 When to pay attention to rumours
- 2 The importance of an effective investigation
- 3 The forensic trails that normal users leave behind
- 4 How to find the contacts they try to hide
- 5 The importance of a weak link

Mass defections are relatively rare and, understandably, hard to cover up. More common, in our experience, is the smaller team defection. In this, several workers conspire to move together, trying to hide this from their employer until they are successfully ensconced elsewhere.

### Bad things come in threes

The heading above is borne out of our experience of hundreds of these smaller team defections, or 'bad leaver' cases. I am not sure exactly why this should be, but often we seem to end up examining three people's computers and data. Sometimes all three have left, sometimes they are split between those gone and



left behind. Either way, three it often is. Perhaps it needs more than two people to make up their minds for what is, after all, a difficult decision. Just moving on can be hard, but to do so and to break the rules at the same time is doubly so.

Not everyone breaks the rules, of course, but then we are only instructed when rule-breaking is suspected – which happens more often than you might think. As with fraud investigations, our experience dictates that a business's

awareness of and readiness against a threat (in this instance to the theft of its data and/or staff) is directly linked to actual experience of such an event. Similarly, the skill and guile which a defecting team uses to access and remove data and coordinate their departure, normally directly reflects whether they have done so before or whether the business they are leaving has suffered such an event before and, if so, how it reacted.

**“While logs of user activity and access are both very useful and important, it is always evidentially more compelling to locate actual forensic proof on a user’s PC as corroboration.”**



Where a business has had no experience of such matters, it is common to find that data is poorly controlled. This is especially true in smaller firms where the IT function is limited or sometimes outsourced: logs are not always maintained and controls sometimes not even activated. We have direct experience of investigations in which distraught clients insist that access logs will prove their case, only for us to find that the logging in question was never activated.

Such gaps in the corporate defence are not always the fault of IT either – in many investigations, it transpires that IT were never instructed to worry about these issues and consequently only did what they were told. Even where access to data and the internet is controlled, the nature of the controls vary from incredibly helpful to quite the opposite.

For example, a log may prove that a company machine accessed a particular website, but not what was viewed, or that a user accessed a particular folder of company documents, but not what they did with them. In such cases, computer forensics is the only resort of the technical investigator.

#### **Investigating defection**

In a defection investigation, there are two key elements to determine:



#### **THE WEAKEST LINK**

In a memorable case, it only became apparent to the firm that a team was defecting when the last leaver approached his manager to resign. During the interview he let slip that he was joining the three previous leavers. This last person was the most technical, but the least highly paid. The investigative strategy was to put pressure on him, as the weakest link.

The manager called him back in for a heart-to-heart chat, in which he voiced his concern that the employee was leaving a secure established firm for a new one with no track record or work. This last point hit home; within minutes the employee was in contact with his co-conspirators on the outside reflecting this concern, the words of his manager ringing in his ears. The fact that he did so from the office allowed the investigators to capture the conversation, in which he was told not to worry as all the business was already in place (they had diverted it before they left)!

Evidence is not always so simple to come by, but the point of the story above is crucial. By their very nature, team defections involve more than one person, but it only takes one person to be the weak link. The danger of this weak link for the conspirators is that they cannot control what that person does (and probably do not realise this either).

We have investigated defections in which the top echelons are incredibly careful about what they say and do, and where they say it (in their electronic communications), only for us to find that a lower echelon person takes no notice of the secret instruction, or does not understand it, and effectively blows the gaffe on everyone else. In such a case, for example, we have been able to retrieve an email from this person that contains the plan and the instruction to keep it secret and the list of those it was sent to.

In another case, the new employer of the defecting team dropped them all in the mire – this time by asking a secretary to follow up on some detail. She used the defector’s current work email by accident.

1. data – whether the defectors have accessed and taken data they were not entitled to, and
2. people – the nature of the defection, i.e., whether they (or others) are in breach of their obligations in how they have conspired to leave together.

The investigative landscape for these elements is normally overlapping – that is to say, the places we would look for proof of either elements are similar and sometimes the same. So how might an investigation into defection unfold?

Firstly, it depends on the start point – that is the point at which the employer

becomes aware of the problem (or potential problem). Start points vary widely, from finding out on a Monday morning that a particular team fails to turn up for work (unbelievable but true), to a slight rumour that something is about to happen. One client was very interested (wisely, it turned out) in rumour, but only if he heard it from three different sources (which he felt gave it weight). When we investigated one such rumour it turned out that three key directors were planning to walk off with their business unit.

From an investigative standpoint, the best time at which to start gathering evidence is before the perpetrators realise they might be investigated. Therefore, catching a defection before it takes place is normally best and most likely to produce quick and usable results. When the defection process is partly complete and there are still potential defectors in place at the employer, this also allows for good evidential gathering, not only from investigating what has happened, but also potentially from monitoring the actions of those still on the inside (see box: 'The weakest link').

#### Forensic trail

In terms of technical, computer forensic investigation of a potential defection, our first question will always be the same; "why are we here?" This may sound obvious, but the point of asking is to find out by which route the client firm knows or suspects it has a problem. This will normally highlight personalities into which we can begin an investigation (whether they have left or not). It will also often provide clues to go on, such as names of outside parties or a new company, which can be used in a forensic search. It may also highlight certain data that is likely to have been compromised.

The digital forensic investigation will then look to work with the client firm and its IT function (if it has one), to determine where key data is held, how people access it, what controls are in place and what they can record, how people can communicate (internally and externally), how they can copy data and what devices the key personalities have (both company owned and personal).



**“Even highly computer literate users have little idea of the traces their actions leave behind.”**

From the answers to this we will be able to determine where to look and what we are likely to find.

For example, in a recent case the data was centrally held and tightly secured with logs of all access by user name. The logs showed a particular user accessing files which they had no legitimate reason to be accessing, just before they left. The files later turned up in a third party's possession. The log evidence, combined with some small forensic traces of the files on the individual's PC, was sufficient to conclude the investigation. And herein lies an important point – whilst logs of user activity and access are both very useful and important, it is always evidentially more compelling to locate actual forensic proof on a user's PC as corroboration.

This is where real computer forensics comes into play. If a user can access the internet, plug in a memory stick, copy files to it, send webmail, burn DVDs and print documents, then they can leave a forensic trail for the experienced investigator to follow. Moreover, even highly computer literate users have little idea of the traces their actions leave behind.

Imagine the surprise on one lawyer's face when the senior partner confronted him with a copy of a Hotmail email he sent from the PC in his office. The fact that it was to a headhunter was not the issue – the issue was that it confirmed the lawyer was already working for the

prospective new employer and had been caught moonlighting!

#### Mobile records

Forensic investigations will also look for data from mobile devices, especially now that these can access the internet – but there are complications with these devices, including the fact that many employees have a work-owned one and a private one, which can only be accessed by order or agreement. The forensic investigation of mobile devices is variable; each different handset will behave differently, store different amounts of data, in different ways and places – thus making it a very 'hit and miss' affair to investigate them.

Whilst I have seen one crucial text recovered from a work mobile (which read "I just hope they don't find the disks in your top drawer"), more often than not, mobile devices are very much secondary to desktops and laptops in terms of investigative usefulness (BlackBerry emails are most easily retrieved from the server rather than the handset, for instance).

One interesting thought on mobile devices, however: some devices will retain data that identifies where they are at particular times – which could be very interesting in terms of defection cases. Imagine being able to determine that a user is actually in the vicinity of a competitor's building when they are meant to be with a client.



#### CHECKLIST: SECURITY PROTOCOLS

- If your firm has ever suffered from defections before, consider what you did, what lessons were learnt and whether they have been acted upon.
- Check where your data is located and stored and who can access what information.
- Check what controls there are over your data – IT will be able to explain what these are, how they work, and what kind of information they capture – are these controls likely to be effective and will they produce useful information if called upon? (Forensic investigators will be able to assist in this judgement).
- Check what devices people have, and which ones belong to the firm – how enabled are these devices (can the users access the internet, copy to USB, DVD etc)? Does your IT control regime allow you to know who has what and where it goes? (Think of laptops being passed to new users after a defector has left – would you be able to find this laptop later for analysis?)
- Keep an ear to the ground – rumours are often the precursor to an actual event, and timely intervention is always better than a costly cure.
- On suspicion or knowledge of defection, ensure that appropriate plans to capture investigative data exist. This includes the forensic/evidential capture of PCs, laptops and other devices for subsequent investigation, as well as logs and backups of key information such as emails.
- Don't forget to switch off remote access for those who have left – if they can come back in they often will to look for key data, thinking you have stopped worrying about them and their access.
- Let people know this is your data! Remind employees with a well-drafted computer usage policy what they are and are not allowed to do – a solid investigation also helps to reinforce this policy.

#### Protecting data

In light of the above, what is the best way to protect a business against the theft of its data? In reality, protection of data is always a compromise between total security and the needs of the business and users to be able to operate effectively. For example, the

best way to prevent network attacks is to be offline, but that is not practical. Users need access to data, and often to be able to save it, copy it, take it home to work on, take it abroad and so on. Thus the decisions about how it is controlled need to be sensible ones that don't make their lives more

difficult (one sure way to encourage team defections!).

A good IT team will advise on sensible security measures, including the monitoring and control of access to data. They can also advise on 'locking down' desktops and laptops, i.e., limiting the ways in which users can copy data via their PCs. Some businesses have USB ports and CD/DVD services on their PCs blocked so that nothing can be copied via them.

All these measures are out there to be implemented. But before any are considered, an audit is advisable to determine what type of information exists and where. Once the scope, sensitivity and location of corporate information is understood, then the threat to it can be assessed, and sensible precautionary measures discussed and implemented.

**“If a team leaves – breaching all manner of covenants in the process – proving their wrongdoing and bogging them down with investigation and litigation is a huge impediment, not only to them personally, but to the new firm trying to employ them.”**

Lastly, as with fraud investigation, the best discouragement for future potential wrongdoers is a robust investigation. If a team leaves – breaching all manner of covenants in the process – proving their wrongdoing and bogging them down with investigation and litigation is a huge impediment, not only to them personally, but to the new firm trying to employ them.

In one extreme case, the scale of the breaches was so overwhelming that the managing partner thought the best course of action would be a 'fireside chat' with his counterpart at the firm the defectors were going to. His counterpart was so shocked at the seriousness of the breaches, and at the realisation that he would ultimately inherit staff with the capability for such action and disloyalty, that he stopped the move in its tracks! mp

– **JPARKER@STROZFRIEDBERG.COM**