



Internal Response Teams versus External Consultants - A Decision Matrix

Edward Wilding, DGI

Management is continually under pressure to cut costs and save money. As a result, there have been many instances where 'in-house' IT departments have been tasked with the investigation of suspected fraud and computer misuse or the preservation and analysis of computer evidence. Few IT professionals have been trained in evidence processing, forensic procedures or courtroom procedure.

Some of the bigger companies and other large organizations have trained 'in-house' computer forensic teams and other specialist computer investigators. There may be compelling reasons to establish and maintain such a capability, but the decision to do so should be made only after careful consideration.

One of the key considerations in determining the economic feasibility of an 'in house' forensic response team will be the number of investigations that any organization will conduct in an average year that require computer evidential processing or specialist forensic assistance. The following table itemises the 'pros', and 'cons' of developing an in-house forensic response team or contracting an external consultant.

Figure 1. Internal Response Teams versus External Consultants - A Decision Matrix

Internal and External Resources			
In-house Forensic team		External Forensic Expert	
Pros	Cons	Pros	Cons
Will be familiar with the organization's systems, processes and operations.	Experience is generally limited only to those investigations conducted within the organization.	Extensive, broad experience of many different types of investigation in different commercial environments. The external consultant will have a knowledge of a wide range of operating systems, processors, networks, configurations and devices, encountered in a variety of circumstances.	Will not be conversant with 'in house' systems or processes, the organizational culture, structure or operations. This may impede the analysis of any information recovered, and may slow the progress of the investigation. The external consultant will necessarily need a period of acclimatisation.
The team will be familiar with the organization's culture, management style and structure.	The team's investigative function may be widely known and understood and its members' identities will be known. This awareness amongst the workforce may affect the team's operations.	The identity of the external team will not be known and there may be greater latitude for covert investigations, undercover or pretext operations.	Unknown individuals are more likely to arouse suspicion if discovered on-site accessing systems or conducting other covert activities. Cover stories need to be credible and properly supported.
Financed internally using paid employees.	Will require training and the provision of equipment and software which will need regular updating.	There is no ongoing overhead - the consultant arrives with the emergency and departs upon its resolution.	Expensive. Forensic consultants typically charge £1,000 a day.
Can deploy as and when required.	There will be a commensurate dilution of focus on core business activities to which staff are principally attached. This is particularly relevant should the team become engaged in prolonged civil proceedings, or criminal prosecutions requiring extensive case preparation and attendance at court.	Commercial forensic teams should be able to deploy anywhere in the world within 24-hours notice.	A qualified practitioner may be unavailable due to other commitments when most urgently needed. This is particularly true of independent consultants and "one-man bands". Some companies offer a retainer, although this is rare.
The team can be assembled from a broad skill set, knowledge base and experience.	There is a risk that the team comprise only IT specialists and will lack the broader knowledge necessary to complete an investigation. Difficult to maintain, equip and train in a state of readiness and as a cohesive unit.	The best independent forensic investigators have a profound working knowledge of corporate fraud and business risk and should add value beyond the strict parameters of the computer or IT environment.	Many computer forensic practitioners are technically adept but have little experience of fraud investigation, business risk or commercial malpractice.

Internal and External Resources

In-house Forensic team

External Forensic Expert

Pros

Cons

Pros

Cons

Basic procedures and techniques can be regularly disseminated throughout the team.

Experience and knowledge is forfeited through departures and people changing job roles, both internally and externally. This can lead to inconsistency.

The best consultants will remain consistent in their chosen profession and will amass considerable experience accordingly.

There are lots of so-called 'experts' offering consultancy services. The forensic and investigations industry is not regulated nor does it offer professional qualifications. There is a risk of contracting a 'dilettante' or 'wannabe' sleuth who will use the opportunity to learn the basics on your ticket.

There will normally be good lines of communication within the team.

There is a risk that the team may become insular and will fail to correspond with experts external to the organization. This can lead to blinkered, out-dated attitudes and approaches

The forensic investigator will normally be involved in the relevant professional associations and will regularly exchange information and ideas with the wider forensic community.

The investigator's level of knowledge will be dependent on his commitment and experience. This varies enormously between individuals and companies.

The team should have an innate understanding of what is possible, permissible and acceptable within the organization.

There is a risk that individual members of the team may be subjective in their approach due to personal allegiances or prejudices towards their fellow employees. There also is a risk that the team inadvertently (or intentionally) might leak sensitive information to unauthorized members of staff.

The independent consultant has no vested interest in the matters or the people that are being investigated and is highly unlikely to compromise the investigation. This professional detachment should promote objectivity and reason.

The independent consultant may not know salient facts, background information, gossip or hearsay which might help sharpen the focus of the enquiry, clarify matters or define alternative lines of investigation.

There will be a clear chain of command and allocation of responsibility within the team.

If the team is subjugated in the wider chain of command, there is a risk that it or its individual members may be subjected to management intimidation, interference or coercion should its findings be considered unpalatable. There is also the ever present risk of political infighting that is always a possibility in large organizations.

The independent investigator is apolitical and unlikely to be influenced by infighting, or pressurised by coercion. It is relatively easy to control the independent investigator, who is bound by confidentiality and must yield to management decisions.

If the independent investigator reports to corrupt management, or is dependent on the blessing of compromised individuals it is probable that the investigation will be disabled, impeded or aborted.

The team will normally show a strong allegiance and heightened loyalty to its employer and will act with dedication and commitment and in the organization's interest.

Members of the team may be required to give evidence under cross examination which may result in the disclosure of information, methods and practices which their employer would rather remain generally unknown.

The independent expert is more likely to be perceived by a court or tribunal as impartial even though he is in the pay of his client. Most forensic practitioners undertake defence and prosecution work. This provides them with experience of the criminal prosecution process and the strengths and weaknesses of any evidence submitted into proceedings.

There is a remote risk that the independent investigator will lack passion because the people and processes being examined are of no direct interest to him.

It is unlikely that the team will have significant or regular experience of presenting evidence in court, or of the legal process. The team may be perceived as lacking independence. Evidence produced by the team may be considered less probative and its testimony may be contested as biased.

The independent consultant will normally have considerable experience of the court process and legal matters because solicitors will comprise a significant proportion of his client base. Many forensic experts are registered as expert witnesses.

Many consultants do not have court experience. A poor performance when giving testimony or under cross examination can seriously impact upon a verdict.

There is a cross-cultivation of skills and knowledge within the team.

Key members of staff engaged in ongoing proceedings or prosecutions may leave the organization.

The contract should state that the consultant or consultancy engaged will commit itself to the formal conclusion of the investigation.

There is a risk that the organization becomes dependent on the testimony and evidence of an individual expert and has no backup in the event that this person is indisposed.