2008-02
Who Should Do Your Forensics

Introduction:

While everyone with a systems administration account seems to think that they are forensics experts, the reality is quite different. Digital forensics is a specialty area fraught with special requirements and special pitfalls and should not be assumed to be covered by expertise in information security.

Why can't my security team do forensics?

Of course there are security teams that do forensics work, and some of them are very good at what they do. But most security teams are not forensics specialists and don't really know about the special requirements of forensic investigation or the specifics required to do a good job in the digital forensics area. There are some good reasons for this in most enterprises;

1. Forensics should be independent of the people who might be involved in any criminal activity. That means they cannot work for the CISO or the CEO or anyone else that might be under investigation.
2. The computer security folks are very busy keeping up with everyday security needs and don't have the time to dedicate day after day to the details of any specific investigation on an emergency basis.
3. The priorities of forensic investigation are often at odds with the priorities of business. The people doing the forensic work should not be focussed on the business issues, but rather the legal issues.
4. Forensics requires a lot of specialized training and expertise that is not needed by most computer security folks. The high investment in digital forensics experts is hard to justify for everyone in security.

OF course there are many exceptions and security team members do play a vital part in investigations, but the digital forensics area is usually separated and a smaller team that can be spared from every-day activities for the periods they need to spend working on legal matters.

Who should the forensics team work for?

I already identified that the forensics folks shouldn't work for anyone they might investigate, so who should the work for? In most enterprises, the answer is the Legal team, and most often, the Chief Counsel. Since essentially all investigations must involve the legal team in one way or another, and since there are very specific legal mandates for investigations and forensic matters, this makes sense.

If the legal team is somehow suspected in something in appropriate, then it is most common for the board or the CEO to contact outside counsel and have that outside counsel operate the investigation using their forensic experts.

Another key point in having the legal team operate the forensics effort is that this effort is intimately tied into the legal hold process, which is used to meet the records retention and disposition requirements, which are in turn imposed by legal mandates. It may create unnecessary and potentially problematic interactions for the legal department to have to work through other departments to support litigation.

Finally it may reduce attorney client confidentiality if the forensics team is not directly working for counsel. There may be additional overhead or risk associated with the multitude of roles for digital forensics experts, and keeping them within the office of the chief counsel makes any question of their role as part of the counsel's office harder to challenge.

How about outsourcing forensics?

These days many companies outsource anything and everything, but as a general rule, I don't favor outsourcing of most security functions. But for digital forensics, I make a broad exception.

Outsourcing digital forensics is certainly an option for companies that don't sustain enough legal work in this arena to justify internal expertise. The high degree of expertise and the high risks of mistakes combined with the relatively low volume of effort make outsourcing a reasonable alternative.

Of course the problem is that outside experts don't usually have as much knowledge of internal operations and therefore have a harder time in getting what they need quickly and efficiently.

However; their independence and the potential to get just the necessary expertise when needed is a real plus in this particular niche area. And their lack of internal knowledge may be a great benefit in legal matters where their selective exposure to information is often a benefit.

Conclusions:

Digital forensics is a highly specialized field that requires a specialized team. It does not belong within the normal corporate structure, but rather within the office of the chief counsel or an outside entity.

If there is inadequate internal forensic work to justify a skilled internal team of dedicated experts, outsourcing is a viable alternative in this narrow area.