

# Build a viable global response

A remote forensic solution has many benefits, as long as it does not compromise security or business operations, says **Andrew Sheldon**

**T**he number of investigations requiring a digital forensic response continues to grow, driven by a dramatic rise in the number of internal and external threats.

The key to successful forensic intervention is a combination of specialist skills and speed of response. No matter if the incident is desktop abuse, eDisclosure, theft of intellectual property or hacking, you need to protect the evidence and get forensic investigation skills on site quickly.

In organisations with multiple geographic risk locations, the traditional approach has been to send a specialist from a central forensic team – a time-consuming and costly process. Alternatively, the evidential items are shipped to a forensic facility – a process fraught with security and evidential continuity issues.

Existing solutions tend to access targeted systems via the corporate network. This means there must be connectivity to the suspect machines, which usually involves installing a “client” application on every machine first. Alternatively, some systems allow a server to push a client to the suspect machine remotely.

Imaging a remote disk over a network can be done – but at what cost to network performance? It is for this reason that most large-scale enterprises still prefer to mobilise a forensics team to the site of an incident, even though this is a costly and time-consuming procedure. A viable remote forensics solution should avoid this.

In order for organisations with a dispersed IT population to react faster and smarter to digital incidents within a forensically sound environment, the skills and technologies need to be located



**The incident response team should be able to gain secure access at any time from anywhere – even wireless”**

where the risks are. This means each risk site needs to either have the skills and equipment on-site or they need the ability for the central forensic skills to reach and use forensic tools via a network.

Remote forensic solutions should therefore obey a number of basic principles:

1. You shouldn't need to learn a new forensic package to respond remotely. An

ideal solution should allow you to remotely deploy any of the tools your forensic specialists are familiar with.

2. A viable solution should enable response to both networked and non-networked digital media – an urgent forensic response might be needed when your critical system has gone offline or has been damaged.

3. Remote response should not impact the normal operation of the networks. If you need to take a forensic image of a remote workstation hard disk, pulling that volume of data over a corporate network could have a significant impact.

4. Security and confidentiality of business data should be maintained at all times – and creating a forensic image over a transnational network may not be permitted from some legal jurisdictions.

5. The presence of the remote forensics solution should never allow business security to be compromised.

6. The incident response team should be able to gain secure access at any time from anywhere via a secure, authenticated-access network – even wireless.

By meeting all the above principles, an economic remote forensic solution can be deployed quickly with maximum security, efficiency and flexibility while producing minimal impact on business operations.

Likewise, organisations facing geographically dispersed risk or those wishing to offer a global forensic service to their customers can significantly reduce setup and ongoing response costs while providing a faster and more flexible service.

*Andrew Sheldon, managing director  
Evidence Talks, MSc in forensic computing*