Andrew Sheldon says that after a breach to first-line security it's vital that you act quickly and smartly to minimise the damage

WHAT TO DO IN THE EVENT OF A CYBER SECURITY

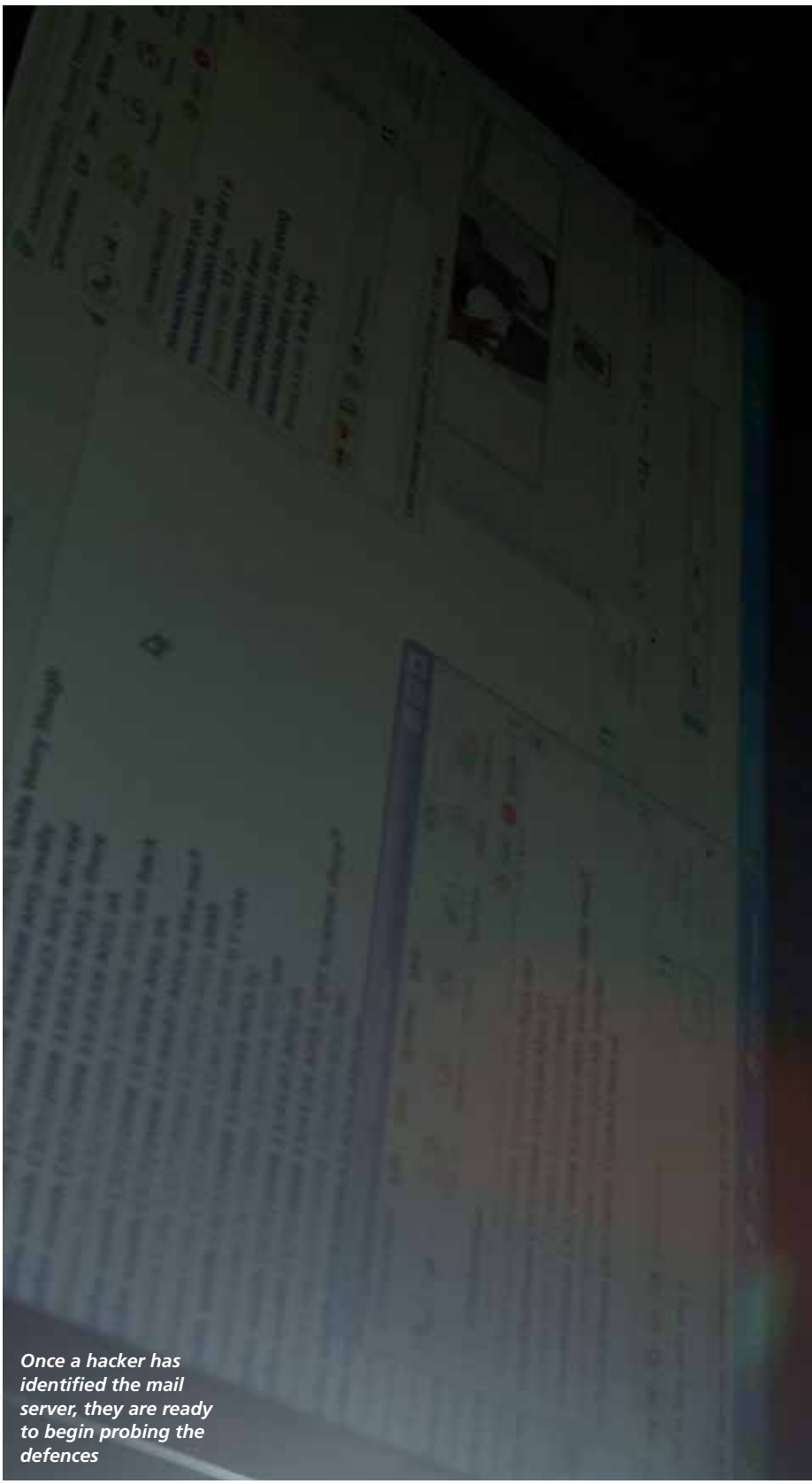
In matters affecting corporate finances and reputation, the role of cyber security in the prevention, detection and investigation of malfeasance is generally well understood. However, in a world where the ability of super-smart hackers and determined criminals to subvert the systems of a business is continually evolving, the hand-in-glove capabilities of digital forensics argue strongly for greater attention.

The world of the cyber offence can be divided into four basic motives – money, kudos, facilitation and vengeance. Although it's become something of a media cliché, it's certainly true that in darkened bedrooms across the globe, there are people whose entire self-esteem is driven by the ability to outwit IT defences – and generally the bigger the target, the more enticing the challenge. Then there are the self-appointed crusaders that have the corporate world in their sights, seeking to change the way the world works. Finally, there are the out-and-out criminals, intent on cheating, defrauding and stealing from commercial operations of all types and sizes.

Hackers and criminals are often smart people. Once they've got something as simple as a URL, they will start to investigate the digital boundaries and weaknesses of an organisation. As soon as they have identified the mail server, the web server, perhaps even the FTP server, they are ready to begin probing the defences. While cyber security offers protection, detection and to a certain extent investigation of these, digital forensics should be called upon at the earliest possible stage after the event, picking apart the attack, identifying what's been done or lost, creating new protocols to shore up the weaknesses and pinpointing the source and identity of the attacker. Digital forensics will enable you to rapidly see the extent of the damage and whether attacks are continuing.

Let's examine a typical 'route' of attack. Someone in the organisation receives an email, purporting to be from the Chairman, with a PDF attached. When it's opened the PDF has malicious content. It might open up what's called a 'back door' or a 'listener' and broadcast the IP address to the attacker. At that point the attacker can start to look at that PC and using the information they find on it can 'swivel' the attack sideways to other devices and resources within the network. Potentially, all sales, marketing, finance, technical, procurement, logistics and other data is now vulnerable.

As soon as an alarm is raised, probably at the



©Getty Images

Once a hacker has identified the mail server, they are ready to begin probing the defences

BREACH

router or server, digital forensics takes over to pinpoint the source of the attack and what data has been divulged. Evidence on the device or devices in question will be preserved, further spread of the problem prevented and a fix can be made, maybe via applying patches to vulnerabilities in the operating system that the organisation uses.

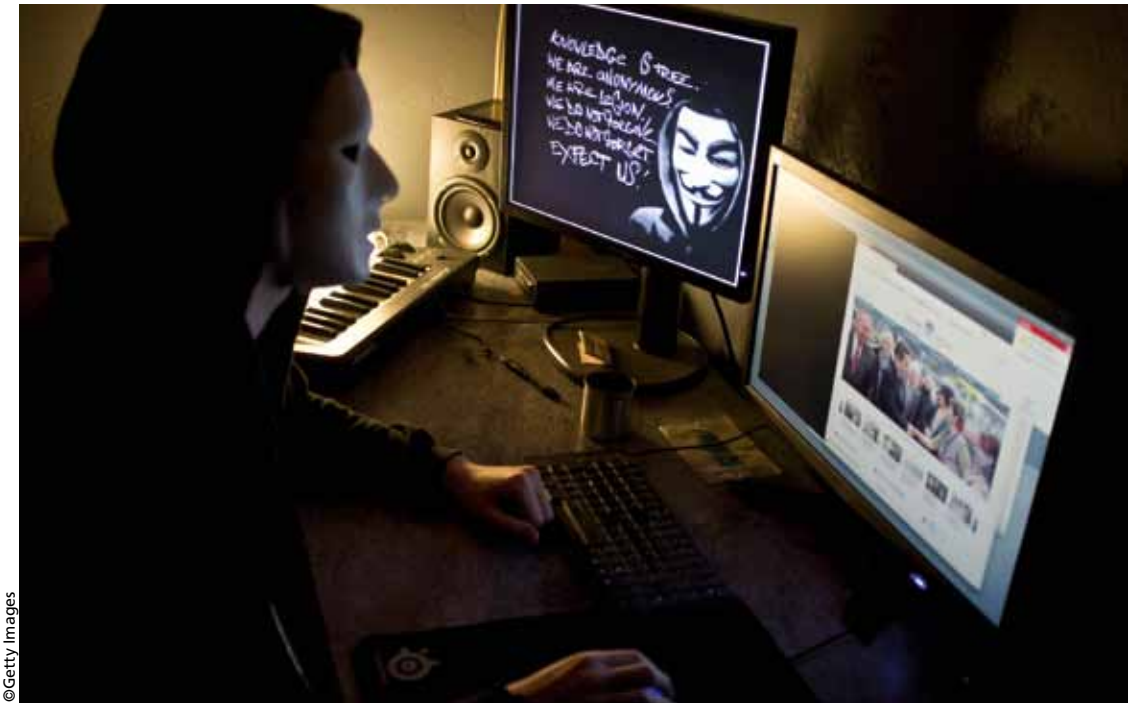
Whatever the motivation of an attack, the effect on corporate wellbeing can be devastating. Once breached, cyber defences will not repair themselves. Then it becomes necessary to detect, recover and, wherever possible, act to prevent re-occurrence. Nor should matters stop there. Cyber crime is not victimless and must be subject to investigation and prosecution wherever possible. Rapid identification of activity source is the quickest route to remedial action and potentially recovery of funds and reputation. Smart forensic techniques will do this and allow you to analyse, report on and apply the evidence you've found.

The tools, training and techniques now exist to support governance and compliance officers in many aspects of this work, including payment stream analysis, travel and entertainment expenses, payroll, financial mis-management, bribery and corruption and capital projects. Digital triage systems now allow non-technical investigators to produce results to evidential standards based on the recovery of live and deleted files, volatile memory and comprehensive file information from Windows, Apple or Linux-based machines as well as mobile phones and tablets.

Understanding what is available and what its capabilities should be is an easy fix. There are training courses which, in a matter of a couple of days, will give non-technical staff a sound working knowledge of digital forensics and in particular the power of digital triage. This is an important, low-cost first step for professionals because when a cyber attack happens, the best-intentioned responses can actually cause massive damage to evidence at source, impede your ability to stop the problem and make it impossible to deal with those that are responsible. Smart use of digital forensics will make corporate response more efficient, less damaging to evidence data and more likely to achieve satisfactory redress.

With the power of digital forensics, it's possible to fight back, and here's a heartening case. In India, a business was bemused by the fraudulent loss of a million dollars worth of sales to a competitor. Spotting the mobile number of one of their own

WHAT TO DO IN THE EVENT OF A CYBER SECURITY BREACH



©Getty Images

Hackers and criminals have a variety of different motives for accessing and utilising different companies' data

junior employees on the rival's website they used digital triage tools to examine the manager's computer, finding and dealing with the source of the problem. The fraud was stopped in its tracks.

To put some objective context on the size of the problem, a recent report published by the Center for Strategic and International Studies calculated that the cost of cyber crime to the global economy is around $445 billion every year, with damage to business from theft of intellectual property exceeding $160 billion due to hacking. An Ernst & Young report in 2014 stated that 80 percent of an enterprise's digitised information resides in individual hard drives and personal files, with the consequent increase in risk.

There are, however, simple protocols that can be adopted to minimise the danger. One such is to always retrieve the company's laptops and mobile devices used by key staff that leave rather than merely handing them over to their replacements. Prior to re-issuing the computer, simply remove and store the hard drive in a secure place 'just in case' it is needed as evidence of wrongdoing at a later date.

In a report by Overill, Silomon and Roscoe published by Elsevier in 2013, it was pointed out that the London Metropolitan Police Service Digital Electronics and Forensics service was receiving more than 38,000 digital devices to be examined per annum. "Not untypically" the report went on "these devices will have a storage capacity of gigabytes or terabytes". The sheer volume and power of digital capability available to fraudsters is immense, and companies must be in a position to fight back. In the UK many police forces and government organisations such as the DWP are turning to digital forensics as a first line of response. For private organisations this is both a signpost and a reassurance – digital forensics evidence is strongly endorsed by the forces of law and order and accepted as standard evidence for criminal prosecutions.

A further step forward in the ability of organisations to deal with unwanted cyber activity has been taken with the relatively recent emergence of highly portable forensic triage tools, which enable staff even with relatively low technical skills to carry out quite sophisticated investigation and analytical work. Such devices temporarily turn a standard PC or Apple Mac into a powerful forensic intelligence appliance and being eminently portable, enable investigation work in the office or at any remote site. Crucially, this avoids the need to outsource specialist forensic services, which can be very expensive.

These same tools and techniques are being rapidly adopted by law enforcement and security agencies. A recent Home Office report published in March 2016 called for a national approach to forensic science delivery in the criminal justice system. I'd like to draw your attention in particular to the paragraph in the report which points out the dynamic nature of the digital technology employed against the corporate world.

The report states: "The rapid growth and development of digital technology creates unique challenges; from the sheer quantity of digital data, to new forms of encryption and the increasing use of cloud storage". It also points out that: "The average British household now owns 7.4 digitally enabled devices".

Faced with this burgeoning volume of digital activity, it is not surprising that the criminal and the disaffected have become more savvy and more relentless in their practices.

The good news, however, is that a suitably trained and equipped corporate team using digital triage techniques has the power to investigate, identify, analyse and respond to breaches of the security wall and protect the long-term interests of the business.

Andrew Sheldon MSc is chief technical officer at Evidence Talks. Founder and innovator of the technology, which drives the company's products and services, Andrew has 37 years of experience in IT, 23 years of which has been focused in Forensic Computing and he was one of the first to gain a Masters degree in the discipline.