Andrew Sheldon examines the challenge for providers of digital triage solutions and how they are helping to limit cyber crime

TAKING THE FIGHT TO CYBER CRIMINALS

The rise of cyber crime is, even in a climate of political upheaval and social realignment, still a headline grabber on a regular basis – and with the kind of statistics available, that's hardly surprising. For example, in the kind of personal scam barely known five years ago, dating fraud increased by 10 percent from 2014 to 2015 and now accounts for around £33million a year in the UK alone. In one astonishing case a newly divorced mother signed over £1.6million in a matter of weeks. Victim support organisations such as Scam Survivors estimate that 90 percent of members on some dating sites are scammed and there have been extreme cases where the victims have taken their own lives.

A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office entitled *The Cost Of Cyber Crime* (published in 2011) put the cost to the UK economy at £27billion and growing. And it's not an issue confined to our shores. The NCA's National Cyber Crime Unit is taking on the global nature of the problem via involvement in the Joint Cyber Crime Action Taskforce at Europol in The Hague. Hackers are indiscriminate in targeting global financial and payment systems and despite warnings about malware, organisations in private and public sectors will continue to fall prey to their activities. For its part, UK Government has become so concerned with the size of the problem that it has appealed for volunteers to investigate cyber crime as part of a new Policy and Criminal Justice Bill.

In September 2015, the then Home Secretary Theresa May said: "We want… to free up officers' time to focus on the jobs only they can carry out. At the same time, we want to encourage those with skills in particular demand, such as those with specialist IT or accounting skills, to work alongside police officers to investigate cyber or financial crime and help officers and staff fight crime more easily".

In my view what's needed is for professional providers to master the art of digital forensic triage and then deliver solutions to those already involved in the process in a form they can readily deploy with a minimum amount of training.

What might be a more realistic approach would be to recruit from the substantial ranks of recently retired police officers, many of who have first-hand experience of the value and use of digital forensics, all of which are well versed in the business of fighting crime.

A further source of relevant talent is the well-trained and knowledgeable IT support technicians working in major corporates who, through their organisations' Social Responsibility Policy, could be seconded for regular, short periods or on-demand (using an Uber-type model) to support officers in meeting key operational needs.

There are innumerable case studies from around the globe where specialist providers work with specialist crime teams that know their requirements, understand the criminal fraternity they are dealing with and can provide informed feedback on the speed and efficiency of the systems they're using. The answer is to empower the front-line officers themselves so that neither time-poor specialist officers nor well-meaning amateurs need to get involved.

The experience of Thames Valley Police provides a perfect example. Thames Valley Police introduced digital triage technology in its Forensic Investigation Unit a year ago and is already yielding some impressive process improvements. The system collects targeted data or conducts full forensic images from removable media such as hard-disk drives, USB sticks and memory cards. Delivering a flexible digital triage solution for in-the-field activities, the system uses standard removable USB devices as 'collectors', allowing many targets to be processed at once.

Principal CSI Clare Heron manages the digital triage project at the unit's headquarters in Oxford and acknowledges how the introduction of this new technology is proving a valuable aid in helping them to service some of the strategic directives outlined in the force's Delivery Plan.

"For us, the key objective to ensure public confidence and victim satisfaction remain high has to be based on adopting new and innovative approaches to transforming our service. A key part of the Delivery Plan is developing the role of our Crime Scene Investigators (CSI) to further support the activities of our High Tech Crime Unit (HTCU), create higher efficiencies in case management and ultimately reduce the impact around high-tech crime.

©Getty Images

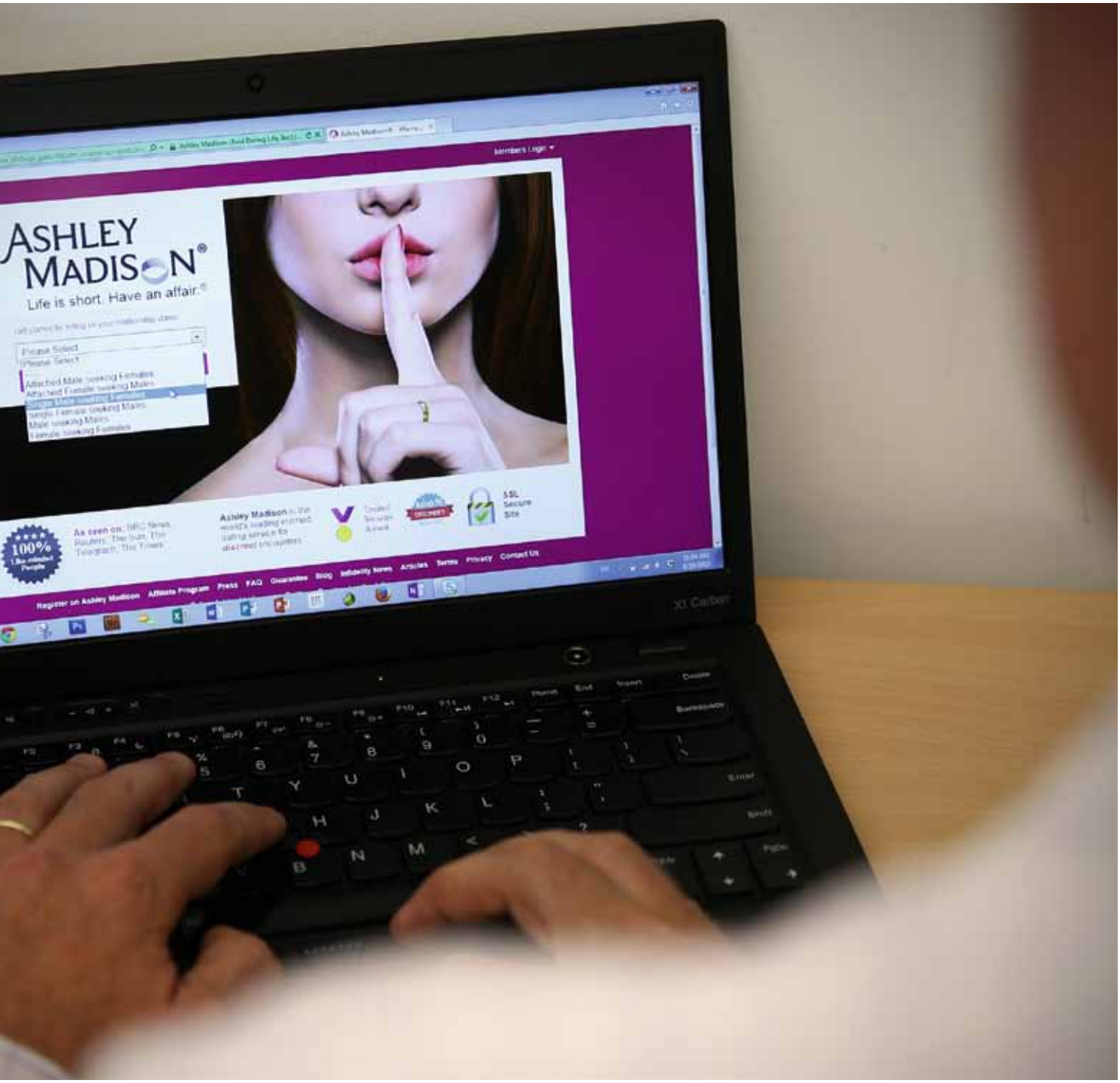
"While it's still relatively new for them, the intuitiveness of this system has meant that the 10 front-line officers trained in its use have been able to quickly adapt to taking on more responsibility at the crime scene and making important decisions on the outcome of examined data."

Designed for use by non-technical investigators, it allows front-line police and other enforcement officers to rapidly preserve and automatically examine data stored on computers, servers and mass storage devices. Using standard, accepted forensic techniques it preserves and protects original data while creating full forensic images or collecting targeted files.

Using a combination of desktop devices, the team of trained officers from Thames Valley Police's Forensic Investigation Unit now plays an active role in rapidly identifying and retrieving evidence from devices at the scene of a crime involving child sexual exploitation, illicit drug supply and other fraudulent crimes requiring the capture of illicit imagery.

In allowing target data to be quickly identified without needing to be taken from the scene for examination by specialist units, the force streamlines the asset retrieval process and ensures the efficient and speedy processing of evidence. As well as freeing up more of HTCU's time to deal with a backlog of cases and enabling them to move on to 'live' cases more quickly, this also offers a speedier resolution for those

Fraud on dating websites now accounts for around £33million a year



TAKING THE FIGHT TO CYBER CRIMINALS

individuals under investigation.

The early successes achieved by Thames Valley Police in Berkshire and Buckinghamshire have influenced the decision to extend the roll out across the entire force to include Oxfordshire, with the force planning to train at least 50 percent of their CSIs on the system in the near future.

This kind of success is available to all, but like all other aspects of policing it requires a professional approach. By contrast, there is considerable danger in allowing digital forensic triage to be carried out in haste or in ignorance. While most organisations in both the public and private sectors have disaster recovery plans in place, many of these are not entirely fit for purpose, resulting in actions being taken on digital systems that undermine the objectives and success of the response. Typically, the kind of events that will require forensic examination include: E-Discovery and E-Disclosure, investigations into inappropriate systems use resulting in policy breaches, support of civil litigation or employment law activities, data loss or compromise of statutory information security obligations and investigations into criminal activity such as fraud, theft, hacking and malware.

And of course the landscape is not static. Most organisations are affected by a series of market dynamics and continuing advances in technology require monitoring and reaction. Like all systems, incident response procedures need to constantly evolve; in dealing with the criminal fraternity this includes responding to the changing tactics and methods of law breaking that go on.

Ideally, regular reviews need to take place covering current human resourcing, current digital security, disaster recovery and contingencies, policies and procedures and analysis and review of historical incident responses and outcomes.

Reassuringly, the highly specialised proprietary software and hardware that is available, when used by front-line officers who have been through basic training, offers the capability to mix information from parts of the net and interrogate the full range of digital devices used by criminals. This gives crime fighters all the weapons needed to advance quickly to producing evidence-quality data. These techniques extend from abuse of corporate systems and misuse of intellectual property to the most serious cases of people trafficking and child abuse.

In 2015 the Office for National Statistics figures included data on cyber crime for the first time, with the crime rate for England and Wales soaring to more than 11.6 million offences as a result. An estimated 5.1 million online fraud incidents and 2.5 million cyber-crime offences were contained in the figures, and these were in stark contrast to a fall in the underlying crime rate, which was down by 8 percent on the previous year.

The Office for National Statistics Head of Crime, John Flatley, states: "It has been argued that crime has not actually fallen but changed, moving to newer forms of crime". It is against this backdrop that closer co-operation between those who develop forensic triage technology and those charged with protecting the public and the corporate community from the effects of cyber crime is made.

Empowering front-line officers to carry out what has previously been the preserve of specialists proliferates the power of forensic triage, significantly increases the chance of successful prosecutions and helps reduce case backlog.

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.

Evidence Talks' digital triage technology is helping Thames Valley Police to develop the role of its Crime Scene Investigators