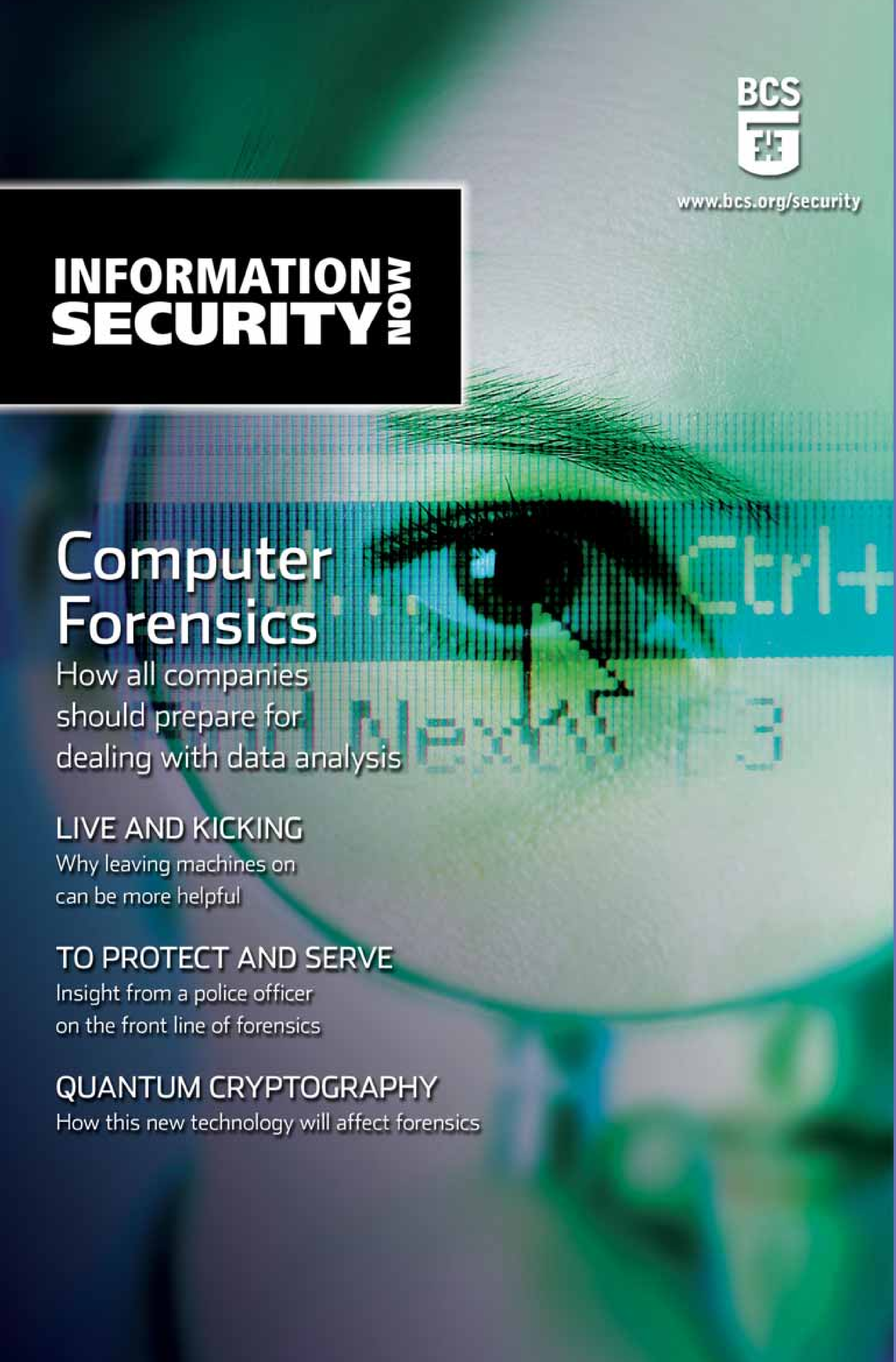
WINTER 2009

BCS
www.bcs.org/security

INFORMATION SECURITY NOW



Computer Forensics

How all companies should prepare for dealing with data analysis

LIVE AND KICKING

Why leaving machines on can be more helpful

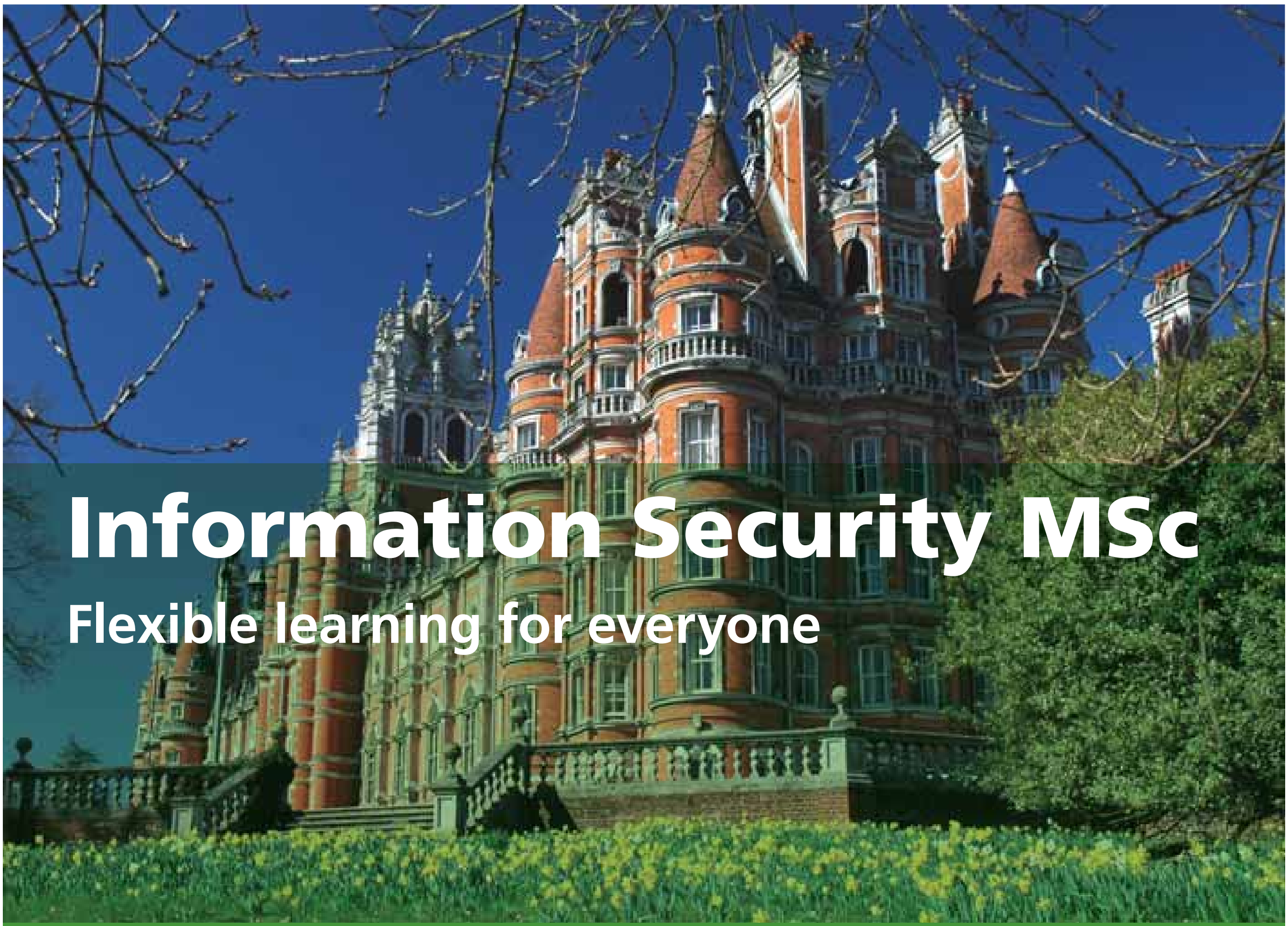
TO PROTECT AND SERVE

Insight from a police officer on the front line of forensics

QUANTUM CRYPTOGRAPHY

How this new technology will affect forensics

SUPPORTED BY THE BCS INFORMATION SECURITY SPECIALIST GROUP



Information Security MSc

Flexible learning for everyone

We have extended the way in which Royal Holloway's internationally recognised MSc is offered.

- **CPD/CPE Modules:** Most MSc modules are now available as stand-alone courses of one week's duration (Block Mode). These modules may be taken with or without an examination.

As a result the MSc now has the following traditional delivery modes:

Full-time, one year, on campus; **Part-time**, two years, on campus; **Block Mode**, two years, on or off campus; **Distance Learning**, up to four years via the Virtual Learning Environment.

The introduction of CPD modules has enabled us to introduce even more flexibility into our methods of delivery.

- **Latest innovation** – 'Mix and Match' degree programmes. It is now possible to obtain the MSc by accumulating modules by any delivery method listed above (maximum period seven years).
- **Postgraduate Diploma** – each module is also available in condensed mode and taught as a one, two or three-day training course offered by QCC Training Ltd. Students may follow a structured programme of these courses and then undertake an MSc level project to obtain the Postgraduate Diploma in Information Security.

Royal Holloway
University of London

Information Security Group
www.isg.rhul.ac.uk
p.stoner@rhul.ac.uk
z.ciechanowicz@rhul.ac.uk
T: 01784 443101

ISNOW is the quarterly magazine of the BCS Security Forum, incorporating the Information Security Specialist Group. It can also be viewed online at: **www.bcs.org/security/isnow**

EDITORIAL TEAM
Henry Tucker Editor
Brian Runciman Managing editor

DESIGN TEAM
Marc Arbuckle Art editor
David Williams Graphic assistant

Registered Charity No 292786.
The opinions expressed herein are not necessarily those of BCS or the organisations employing the authors.

Printed in the UK by:
Inter Print, Swindon, Wiltshire.
ISSN 1752-2455. Volume 3, number 2.

The British Computer Society
First Floor, Block D, North Star House,
North Star Avenue, Swindon SN2 1FA, UK
tel +44 (0)1793 417 417;
fax +44 (0)1793 417 444;
www.bcs.org
Incorporated by Royal Charter 1984.

ISNOW | ISSG PERSPECTIVE

Gareth Niblett, chairman of the ISSG, says forensics is something all companies need to address.

Digital forensics is an area overlooked by many companies – until needed. When required it can touch upon many business areas, including IT, HR and legal. Proper planning can help ensure that it is effective when called upon.

Forensic readiness

Companies should have a formal forensic readiness plan in place, so that when an incident occurs the correct skills, processes and technology are available to ensure proper collection of reliable evidence. This may require external resources being brought in to perform activities beyond, say, seizure or quarantining of a system or storage medium. It may also be sensible to limit untrained internal technical resources from engaging in digital forensics. They may overcompensate for having 'permitted an incident to occur' by being overly eager to respond and investigate, usually in a non-forensically sound manner. This would then undermine any disciplinary and legal proceedings. As with any incident response and investigation, all those involved need to be skilled and knowledgeable practitioners in their field and follow clear procedures, such as the CPNI First Responder's Guide and the ACPO Good Practice Guide for Computer-Based Electronic Evidence.

Future forensics

I expect issues to develop with increasingly smart mobile devices, cloud, Web 2.0 services and storage, encryption and anti-forensics tools. Emerging techniques such as live and remote forensics will continue to develop to try and keep up with the bad guys.

ISNOW | CONTENTS

FURTHER INFORMATION

Information Security Specialist Group: www.bcs-issg.org.uk
Information Risk Management and Assurance Specialist Group: www.bcs.org/groups/irma **BCS Security Portal:** www.bcs.org/security
***ISNOW* online:** www.bcs.org/forum/isnow

Data loss, liability, reputation and mitigation of risk

Charlotte Walker-Osborn, partner; Phil Sherell, partner; Vin Bange, associate, Commercial Technology Group, Eversheds LLP examine the thorny problem of keeping data in check.

Continuing on from my last article which looked at data protection and security breaches, this piece touches upon data loss more generally. With an increasing number of security breaches hitting the headlines, there is, unsurprisingly, a growing awareness amongst regulators and the public alike of data security issues.

The risks to businesses of being involved in a data loss incident are high. Criminal sanctions under the Data Protection Act are well established, but other regulators like the Financial Services Authority (FSA) are also willing to flex their enforcement muscles. In the last three years, the FSA has levied substantial fines against several of its members for security breaches.

Bad publicity is another potentially lethal sanction. A recent study by Ponemon showed that 31 per cent of respondents terminated their relationship with an organisation on receiving notification of a breach of data security.

Finally, where third party suppliers are dealing with data, security breaches can lead to termination of their contract and liability for losses incurred.

Mitigating legal risk

Arrangements under which third party suppliers handle customer data should provide for clear lines of responsibility. It is ultimately the data controller's responsibility to ensure that its suppliers treat data carefully, but the supplier will also require their assistance to minimise damage if a breach should occur.

The services contract should:

- clearly spell out each party's responsibilities - security measures should be specific and clearly identified (i.e. within a security schedule) and should be achievable;
- set out some basic controls in the event of a data loss or breach – the parties should co-operate to prevent further damage;
- have indemnity and termination provisions, which specifically address the issue and the consequences of data loss on the supplier's part; and
- very importantly, contain specific provisions for press statements to be mutually agreed so that neither party can depict the other as the scapegoat.

Practical steps

All businesses should have robust data security measures. In particular:

- human and operational controls to ensure effective training for all staff who handle the customer data so staff clearly understand what their responsibilities are;
- technical measures, which must be robust and backed up by an audit trail to demonstrate that they are tested and effective for the specific data and contractual requirements.

Reputational damage

Instant and intense media scrutiny can be expected in the event of data loss so businesses should plan in advance how the situation will be handled. You will need to establish the exact facts very quickly and present a coherent explanation showing that you are in control. If there is doubt as to what has happened, you are entitled to prevent the media pointing the finger until the facts are clear.

Be careful about blaming a third party – check whether you are contractually entitled to do so and consider the risk should you be wrong.

If it is clearly your fault, a prompt public apology combined with a clear explanation as to how you will mitigate any damage caused may be the most effective way of defusing the situation. Whilst writing, I should mention the long-awaited changes to the Computer Misuse Act have finally come into force.

Please note that the information provided is for general information purposes only and should not be relied upon as a detailed legal source.

Encryption: the first and last line of defence

Our privacy is under constant threat. Whether it is through malware, hacking or theft, the loss of sensitive data can be very damaging for both businesses and individuals. Michael Marzy, CEO of Steganos, explains how encryption is the best way to ensure private files stay private.

Privacy is important. Most of us store files on our home and business computers that we wouldn't want others to have unrestricted access to. Addresses, phone numbers, bank details, pictures and video – any of these things could cause problems in the wrong hands. And with portable devices being so, well, portable, and hackers and malware assaulting users from the internet, the wrong hands could quite easily gain access. But there is a proven defence against all these threats – encryption.

The British government lost 29 million personal records over 12 months. The Daily Mail lost a laptop containing thousands of staff records in July this year. A manager was recently fired from Colchester University Hospital after a PC containing unprotected patient records was swiped from his car. 2007 and 2008 have been defined by data loss, and the media have been overflowing with stories about large organisations and the government making basic privacy mistakes and failing to encrypt valuable files. But smaller businesses and home users often make similar errors themselves – they may not make the headlines, but these incidents can be just as damaging.

The strength of laptops, USB sticks, CDs et al is also their greatest weakness, they are easy to lose and they are easy to steal. I am consistently surprised that even with all these high profile data losses making the front page of the papers, people still maintain a very blasé attitude to privacy and believe that password protection is sufficient to protect their valuable data. It isn't. Password protection is notoriously easy to break.

The most effective way to protect important information is to encrypt it. Encryption transforms files so that they are unreadable to all but the owner of the decryption key. Many modern encryption solutions use the Advanced Encryption Standard (AES), a secure and highly regarded encryption algorithm. In fact, the US government considers this type of encryption to be suitable for TOP SECRET classified files, the highest level of secrecy there is. These solutions are inexpensive and widely available whether it is for a global enterprise, small business or home user. It is good practice, both personally and professionally, to encrypt all valuable information on a portable device. That way, if a user's critical information is stolen, the thief will be unable to make any use of it whatsoever.

Of course it is not only hardware loss that threatens users' data. The internet is rife with threats that can allow outside eyes to access a hapless victim's sensitive files. Malware is one such threat – with some threats allowing thieves access to the files stored on the victim's computer. If a user downloads the wrong file, or visits a contaminated website, they may find their computer infested with this malicious software. Even worse, they may not even know. Internet security software generally does an excellent job of protecting users against the majority of these threats, but with new threats emerging daily, it is best to err on the side of caution and encrypt the files that are particularly sensitive. That way, if malicious code does manage to bypass internet security, the information has an extra layer of defence and privacy can be ensured.

If sensitive information is no longer required, the best way to protect it is to delete it. However, when files are deleted from a hard drive they leave traces that can be reconstructed by thieves and hackers. By encrypting the files before deletion, the remnants that remain on the drive will remain encrypted and remain inaccessible should they be reconstructed.

In this way, encryption protects your privacy, even when the files are gone. Another way to ensure that the deleted files are safe is to use a file shredder. File shredders work by overwriting the deleted information with another piece of data. The software also removes any links to other sensitive files that may remain in the data, so as to fully ensure privacy. This method is often used by military organisations to protect their deleted data. The United States Department of Defence, for example, overwrites sensitive files a minimum of three times in order to ensure no access to deleted files is possible.

Good encryption gives users both a first and last line of defence, protecting them against threats to their privacy. Isn't it time more people started doing that?

Keeping it live

Sometimes you can get hold of more data to carry out computer forensics if you don't turn off the machine, but live forensics isn't without its challenges. Henry Tucker spoke to Andy Clark from live forensics company Detica.

Andy started by explaining the difference between live forensics and standard forensics. Historically a lot of computer forensics and information systems forensics has been from a dead PC, Andy said.

'One attends a scene of an incident, turns the machines off and takes them away and takes the hard drive out and then looks to see what's on them.'

The reality is that in the current environment, where all sorts of different applications can be running and data can be protected in different ways, just taking a dead machine and recovering the data does not necessarily mean that you get everything that is relevant. So increasingly, and in particular with people using encryption on their hard drives, capturing data live is necessary, which is what Andy's company does.

By accessing the machine when it is on, Andy's team obtain a whole raft of things including: access to protected file systems, access to what is happening online, such as online chat, IRC chat, which ports are open, what applications are running and what remote services are being accessed. It is a much more comprehensive approach than the simple expedient of looking at a dead computer.

How they go about live forensics is also different from standard forensics. The life cycle for forensics is comprehensive and it starts as soon as somebody thinks they have a problem. Detica is engaged in the early intelligence gathering phase and they advise people on how they can look at the data to establish whether or not they have a genuine cause to go and conduct an investigation.

This stage is very important, says Andy, as there are a lot of people who need to be involved, such as HR, because companies need to ensure that their policies and their practice statements are correct and that the investigation can proceed. Legal counsel will also need to be involved and Andy says that his team is there to help advise people to look at their architecture, see how data is segregated, and see from where data can be collected evidentially.

Once they have done this, and established that there is proper cause for them to proceed, only then do they go and support the actual collection of that data. Having said that though his team don't just turn up. There is a lot of sensitivity to what is being done and so they will always liaise carefully with the client to find out when is the best time for it to be done, when they can minimise the personnel impact, and also how they can minimise the business impact.

'You need to remember, people are innocent until proven guilty. So in the event that there is an investigation under way, it needs to be done sensitively and completely in line with the business. The last thing you want to do is to stop the business,' said Andy.

This is particularly so if the data which needs to be examined is on the main corporate server. It is obvious, said Andy, that the server would be turned off with standard forensics but with live forensics you don't need to, so it has less impact on the business. Andy and his team do get data from servers, but also from remote access devices and individuals machines.

When it comes to actually getting the data off, how they go about it is all decided in the planning stage. Andy says that they ask 'who do we believe is engaged in this?'

If they, and the company that has hired them, believe that it is an individual working alone then the process is relatively straightforward. In the event that it is a little more complex, and they all believe that there are a group of people working in conspiracy, then the planning stage is a lot more complex and so they have to manufacture a mechanism by which they minimise the chance of tipping people off. This can be via a cover story, but it varies.

In order to then get to the data, more often than not they have to go and sit down at the suspect's PC. When they do this Andy says that they dress appropriately and they try to blend in to the environment. Andy says that this is just one example of why, at the early stages of planning, all the right people are involved.

'This is not techies wearing their underpants on the outside of their trousers, flying in and saying "the forensics team are here." This is very much working together and in partnership with the business,' said Andy.

Sometimes though it isn't always possible to sit at a PC and get the data off. There are mechanisms to get to it over the network but, according to Andy, that involves pre-deploying forensic software on to the target machine. If you can do that, then you can get access to the machine without sitting there and pull the data back forensically and remotely.

As well as having access to running processes and any active ports, plus the data that is moving through them, by using live forensics you do get more data from a machine than if it had been turned off. You also get attached network drives, you get attached services, so you get everything that is currently going on.

Although accessing data from a PC or server might sound easier with live forensics than typical standard forensics, it is not without its own challenges.

'You need to understand about the target before you get there, and you need to fully understand the operating system. Live forensics is challenging to do and you need to understand firstly what OS the person is running. That's not just "is it XP or 2000 or Vista?" You need to know whether it is XP 32 or XP 64. Different tools are required for different operating systems, so pre-knowledge of the target is vital because you don't want to have to spend a very long time doing this work by doing things that are handcrafted. What you would like to do is run a series of scripts that are pre-prepared.'

Despite the obvious complex nature of the task, many of the tools that Andy and his team use are open source, free and openly available. He has a word of caution though as the tools don't always work as they are supposed to.

'We actually spend a lot of time developing, testing, modifying, testing again and qualifying tools to collect data in a live environment. So although there are quite a lot of live forensics tools available that people can go and get from open source, don't expect them all to work.'

The notion that free software can be used by professionals may sound odd, however, it is the application of the software that makes the service that Detica provides stand out.

'The software is good enough for professionals, once you have validated and checked them,' says Andy. 'Forensics is not rocket science. It is the thorough application of proper procedure and practice in order to preserve, investigate and present evidence. Now having said that it is not rocket science, it is not the sort of thing that you just want to practice or that people ought to be doing for themselves - because in this way it is not rocket science. But all of the stuff that goes on behind this is all about being a forensics professional and ensuring that you do things in a way that is provably correct and is impartial and expert. The method in which we use the tools, the protocols and procedures that we use to follow and the way that we present our evidence is all designed to satisfy the requirements of evidence in court if necessary.'

One of the biggest challenges to all forms of forensics is encryption. However, sometimes in these situations live forensics has added benefits.

'In one case the subject was using an encryption package and in order for us to be able to understand the contents of their hard drive we needed to look at the subject's machine while it was on, and we were not expecting the subject to be cooperative. So in those circumstances, in the event that the machine had been taken away dead, they might not have given up their passwords.'

Taking less time

It would have involved a substantial amount of work to gain access to the data that was previously encrypted. So by doing live forensics they reduced the amount of work dramatically, which in turn cuts the time taken to get to court or the time to produce the evidence properly. It reduces the time taken in the vast majority of Andy's cases. Once the data is presented, most people decide that if there is a solid case to answer and it is clear, they will plead early and save the public purse a great deal of money. The alternative would be to take a dead machine and spend a substantial amount of time attempting to recover the data with less chance of success than if it is done live.

Having said all that, doing live forensics doesn't mean that it takes less time for them to do their job.

'If you're looking at a dead machine and there is nothing there you can get at, it will take you less time to discover that there is nothing there. However, had it been live it would have taken you longer to look at, but you would have got a lot of stuff. So it is not a simple answer. it is all about the planning.'

Following on from this, Andy says that there is something really important to bear in mind when thinking about calling in his team.

'If there was one message here, it is really vital to engage with forensic professionals early, don't think that because you have seen CSI, you know everything there is to know about this and say "the guys in IS have already had a look at it." This is fatal. This happens to us on a regular basis and it happened to me just recently. Someone phoned in with what was quite clearly, potentially, a very solid case. And when they said "yes, our IT people have already had a look at it and we've established this, we've recovered some files already and done this", we just put our head in our hands because we realised that they had contaminated all of the material that would otherwise have been relevant. And they had basically walked away with their own case.

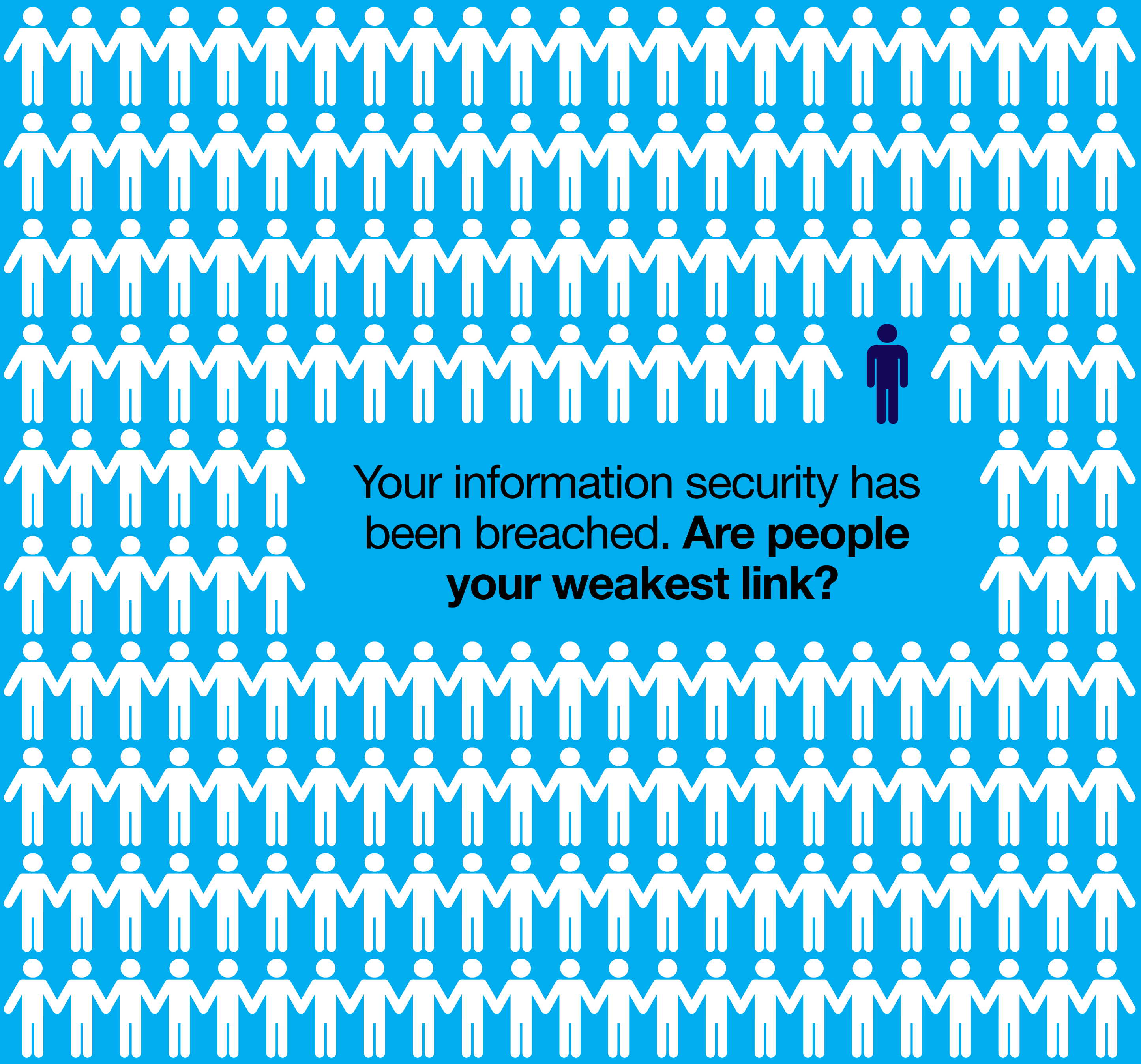
'The first thing IT departments need to assume is that there is going to be a problem at some point. So what they ought to do is to have some sort of digital incident readiness review that starts with the question "What would we do at that point?" Let me give you an example of when we have done these reviews in the past. Somebody will say "well, the first thing we are going to do is to check their email." And I would say "can you do that?" and they would say "yes, it is easy, we will just go and look at the exchange server."

'And I said, "no what does the policy say about your rights to inspect individual's emails?", "I don't know" is the typical response and they then go and read the policy. The digital incident readiness reviews start from the very beginning to say what actually exists within the organisation's acceptable use policy, HR procedures and so on as to what we can do. And then, as part of that, we give people a digital incident checklist that says: these are the people you need to phone, these are the people that need to be in play, and the first thing that happens is that we will have a teleconference to say we believe there is an incident let's get everyone on the phone very quickly and establish what needs to be done.'

One of the problems with computer forensics is that people assume that it is mainly done with technical people and as soon as they are called in, the IT team gets excited and everyone wants to be involved. In reality, Andy says that everybody needs to stop, take stock and call his team in.

Added to this he said: 'Now we may not be the people who are doing everything at this stage but we are certainly going to be advising people in the IT department as to what they ought to be doing. So we will say, for example, "can we disconnect that server without affecting the business?", "what's the state of backup data?". We are giving professional advice rom a forensics standpoint.'

For further details visit: www.detica.com


Your information security has been breached. **Are people your weakest link?**

Information Security - Combining effective technology and informed people.

Attend Infosecurity Europe 2009 and…

- Increase information security awareness amongst your employees and suppliers by attending the free education programme
- Meet over 300 of the top technology, service and solution suppliers in the industry

Visit Infosecurity Europe, Europe's No.1 information security event.

New venue for 2009!

28-30 April 2009
Earls Court
London | UK

Register for FREE ENTRY
at www.infosec.co.uk

Reed Exhibitions®

infosecurity® EUROPE

TO PROTECT AND SERVE

Paul Wright is a detective sergeant with the City of London Police. He was previously seconded to the National Hi-Tech Crime Unit as an operational team leader and as a career detective he has spent the last 10 of his 25 years service specialising in internet, network and forensic investigations, at a local, national and international level. Henry Tucker spoke to him about his work.

Since January 2004 Paul has been in charge of the Hi-Tech Crime Team in the City of London. In this role he is responsible for the day to day running of the team and for the implementation of the forces outreach programme to the financial sector.

This e-crime strategy involves giving presentations to a wide range of business organisations and at the same time actively encourages the flow of information between the private sector and law enforcement regarding hi-tech and e-crime.Along with a number of IT and computer forensic qualifications, he holds a master of science in professional computing, is an associate of the Institute of Information Security Professionals, and is also a regular lecturer on computer forensics, hi-tech and e-crime at a number of universities and colleges.

What is your workload like? And what is your role in managing that workload?

All over the globe more and more instances of hi-tech and e-crime are being investigated by law enforcement agencies and other investigative bodies. Along with this increase in workload has come the realisation that crimes involving computers; either as the target of offending, or as one of a range of tools, or the principal tool used in the commission of offences, are technically difficult to investigate and raise many practical problems. One of my main roles is to solve those problems and anticipate as many of them as I possible can.

What challenges are there now? And where strategically can we respond to these in the future?
There are major challenges facing the world of information security, incident response and computer forensics in how best to understand and deal with the complex and dynamic developments in the ever-evolving world of the internet and digital information. If we do not invest in the skills necessary to police this ever-changing environment, we will have to contend with playing catch-up in understanding how new technologies are associated with traditional and new crimes.

As a forensic science we need to continually seek cost effective ways in which to deal with digital and electronic investigations involving IT abuse and hi-tech crimes. To achieve this we need to commit to training that allows for regular updates, commit to adequate funding and combine it with a commitment to quality.

There is also a need to acknowledge the importance of the work, whilst at the same time trying to get others to understand the issues and difficulties associated with it.

In your experience, are criminals becoming better informed about computer forensics procedures? How will these skills be used criminally in the future?
Organised crime and criminals do not stand still and the history of crime trends shows how they have transcended different crimes.

Now we have offences like counterfeit pharmaceuticals and e-fraud being committed via the internet:

1 kilo of active ingredient $70, makes 14,000 tablets. These are then sold for $10 a tablet which will make $140,000

In addition they are becoming aware the cyber-criminals, more than any other global crime gangs are becoming faster and more flexibility in ways to deal with data compromise challenges and avoiding the existing rules, regulations and legislation. It can, and is, perpetrated from anywhere in the world against any computer.

Therefore criminals do attempt to camouflage their methodology but not necessarily because they have become aware of forensic procedures. Those that advocate such awareness tend to have the tools, but not the know-how or the inclination to use them. However, I do believe that this trend will change, but the changes will vary in speed dependent on the type of abuse or crime.

The future, as well as the awareness and use of anti-forensic tools, I see more and more computer literate criminals being sent to prison, in particular hackers and paedophiles, a number of whom have a very good knowledge in the use of sophisticated computer and internet techniques. The upper echelons of the criminal fraternity will exploit these skills to their own ends, for example the drug dealer who wants an untraceable and anonymous communication network.

What is the most rewarding part of your job? What aspect of your job do you find most challenging?
Beside the rescuing of children from harm, the most rewarding part is trying to establish multidisciplinary partnerships between academia, industry and law enforcement, in order that we can work together on emerging problems within ecommerce, e-discovery, e-crime prevention, hi-tech and IT enabled abuse.

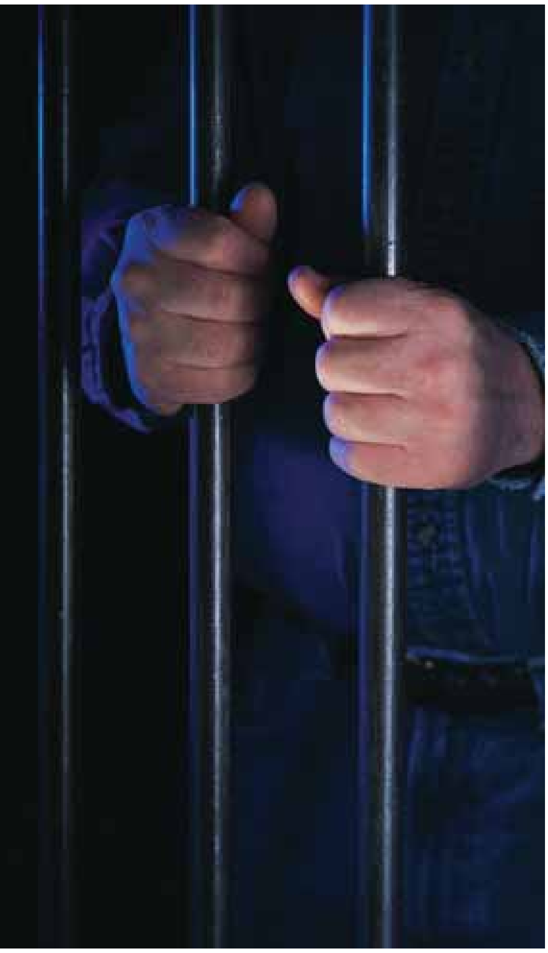
Trying to ensure that any such combined effort produces results, such as developing research into technologies and tools, to creating a repository for electronic crime and cyber forensics technical papers. As well as me, there are national institutions and agencies around the globe that are trying to do the same.

The most challenging aspect is getting organisations to understand where they are exposed in relation to incident response and forensic procedures. It is very hard to get an IT administrator to think like an offender, and have him or her keep pace with them.

If we were able to put such infrastructures in place I believe we would all be able to further our knowledge and investigative skills with regard to IT abuse, and in particular hi-tech crimes and the hi-tech criminal.

Encouraging others to establish these foundation stones, along with the thought of legal and financial sanctions, may motivate and cause them to consider the establishment of things like e-crime units, e-crime laboratories and public-private partnerships; especially the later as history shows us that they do work.

What particular aspects of computer crime legislation do you feel could be improved?
Hi-tech crime is committed across cyberspace and does not stop at national



borders. More than with any other large-scale crime, the swiftness and flexibility of hi-tech crime leaves our existing rules of regulation and legislation outdated.

Such crimes can be perpetrated from anywhere in the world against any computer and I believe that efficient action to combat it is necessary at not only a local level but also at an international level.

Legislation in most countries has fallen behind; it needs to maintain the same speed of change as Moore's Law. The international legal systems have gone some way to achieving the sixth principle established by G8, commonly known as 'quick freeze, slow thaw'. However the detection and punishment of hi-tech crime is highly likely to remain problematic.

This type of crime is perceived to suffer from an increased tendency to 'legislative dependence'; in other words a long period of time elapsing between innovations in criminal enterprise and the response of the state and law enforcement agencies. Technology, and as a result digital crime, develops and changes very rapidly and it takes years for legislation to be enacted, by which time the crime and criminal will have developed a different form of modus operandi.

As a consequence there are those, including me, who say that many digital crimes and criminals cannot be dealt with appropriately under current legislation and unfortunately this is not likely to change in the near future.

What advice would you give to someone who has just started a career in computer forensics? What qualities do you look for in new colleagues?
What is clear, as a forensic examiner in the public or the private sector is that the procedures, techniques, and guidelines are equally applicable to the collection and examination of digital evidence in internal, civil and criminal investigations. In addition, the emerging case law and regulatory requirements have produced the need for all to preserve data 'by the book'. This, and the speed with which technology is advancing have far reaching implications for the forensic examiner. It also emphasises the need to assume that evidential data should be dealt with as if it were criminal, and the need to keep up to date with emerging techniques and technologies. As for qualities, I look for someone who combines attention to detail and patience with innovative and practical thinking.

As many computers and servers now have huge amounts of storage, what issues does this set you and your team?
As a unit we are seeing that there is an ever-increasing growth in demand for forensic computer evidence recovery. In addition to the number of conventional desktop computers now in circulation there are also a wide variety of computer storage media available.

The force is unique in that the majority of the computer crime workload is fraud based and as a consequence it involves large and complicated networks and servers. Added to this is the growth in storage space available on hard drives and this capacity continues to grow. It is predicted that within two years home computers will have the capacity to store more data than some of the current City of London Police servers. Capacity means longer retrieval and analysis times.

To quantify this in the future the force has now established aims, objectives and performance indicators, all of which will benefit the direction our investigative strategies take. For example the performance indicators will help present the real workload in terms of the total gigabytes searched, rather than the number of computers submitted for examination each quarter.

> **It is predicted that within two years home computers will have the capacity to store more data than some of the current City of London Police servers.**

What are the pressing issues for the future?
There is a major problem facing the City of London Police (CoLP) in how best to understand and deal with the complex and dynamic developments in the ever-evolving world of the internet and digital information. If we do not as a force invest in the skills necessary to police this ever-changing environment, we will have to contend with playing 'catch-up' in understanding new technologies associated with a range of traditional crimes.

As a force we believe that we are able to give a cost effective way in which to deal with digital and electronic investigations involving hi-tech crimes, especially in relation to those that impact on the financial sector.

To achieve this we commit to training that allows for regular updates, commit to adequate funding and combine it with a commitment to quality, and at the same time we acknowledge the importance of the work, whilst doing this we also endeavour to understand the issues and difficulties associated with it.

As a result we benefit from a valuable tool for investigations and a very cost effective way of achieving good results, whilst being seen to adopt an innovative approach to intelligence analysis and the capacity to deal with the quick and instant changes that occur in the digital world. Myself and others fully advocate that officers should not be prevented from investigating because of outdated technology and lack of forethought.

More information at:
www.cityoflondon.police.uk

A matter of time

The defence lawyers usually ask the wrong question. They usually want to know if I can confirm that certain things the prosecution say that they found on a computer actually do exist. The answer is invariably yes, but what they should be asking is: how did it get there, is it likely that the accused knew it was there and very, very importantly, when did it get there?

The importance of accurate time determination is often a crucial part of the forensic computing evidence chain. If it got there before the accused owned the computer then it is unlikely that he knew it was there. If the last accessed date is when the accused did not have access to the computer, then it is unlikely that he accessed the file concerned. But unless the timestamp is accurate all the above are cast into doubt.

Most timestamps are produced from the computer's internal clock, or from the clock of another computer that the file may have been transferred from. Many computer clocks are adjusted for the local time zone of the country that the computer usually sits in, but laptops travel the world and we need to know if the time zone adjustment was made. The potential for accidental or deliberate manipulation of the time/stamp is huge, so the best form of confirmation evidence is from something outside of the target machine. Perhaps a transaction on a credit card issuer's machine, or a PayPal invoice. However, in many cases these are not available so it is back to the tedious task of creating a timeline of the events on the target computer. Emails may provide the appropriate mechanism, after all, the reply to an email can hardly occur before the initial message is sent and the reply will have been generated on a different computer and possibly transferred over the internet. Examination of the headers can prove the hypothesis that the target computer's clock was accurate at the time of the email exchange. But was it always so? The creation of a time-line may be tedious, but it can reveal inconsistencies in timestamp evidence.

One of my cases involved a 'missing 17 minutes' hypothesis that when proven totally destroyed the other side's case. In another, the prosecution's case that the accused had accessed 31 websites was jeopardised when a time-line showed the sheer implausibility of a person accessing a website every six seconds in just the three minutes and 11 seconds that the prosecution's internet history revealed. The prosecution's case had been put forward without a timeline and thus without realising that they were potentially claiming that the accused had the fastest fingers and most speedy internet connection in the whole world.

Different systems operating in different time zones also present problems. Trying to show a jury that an ATM receipt produced in a British high street showing a British Summer Time timestamp is the same transaction as recorded in Mountain Standard Time on the credit card's computer in the USA, is fraught with difficulty (and some amusement when observing the baffled looks of the 12 good people on the receiving end of the explanation).

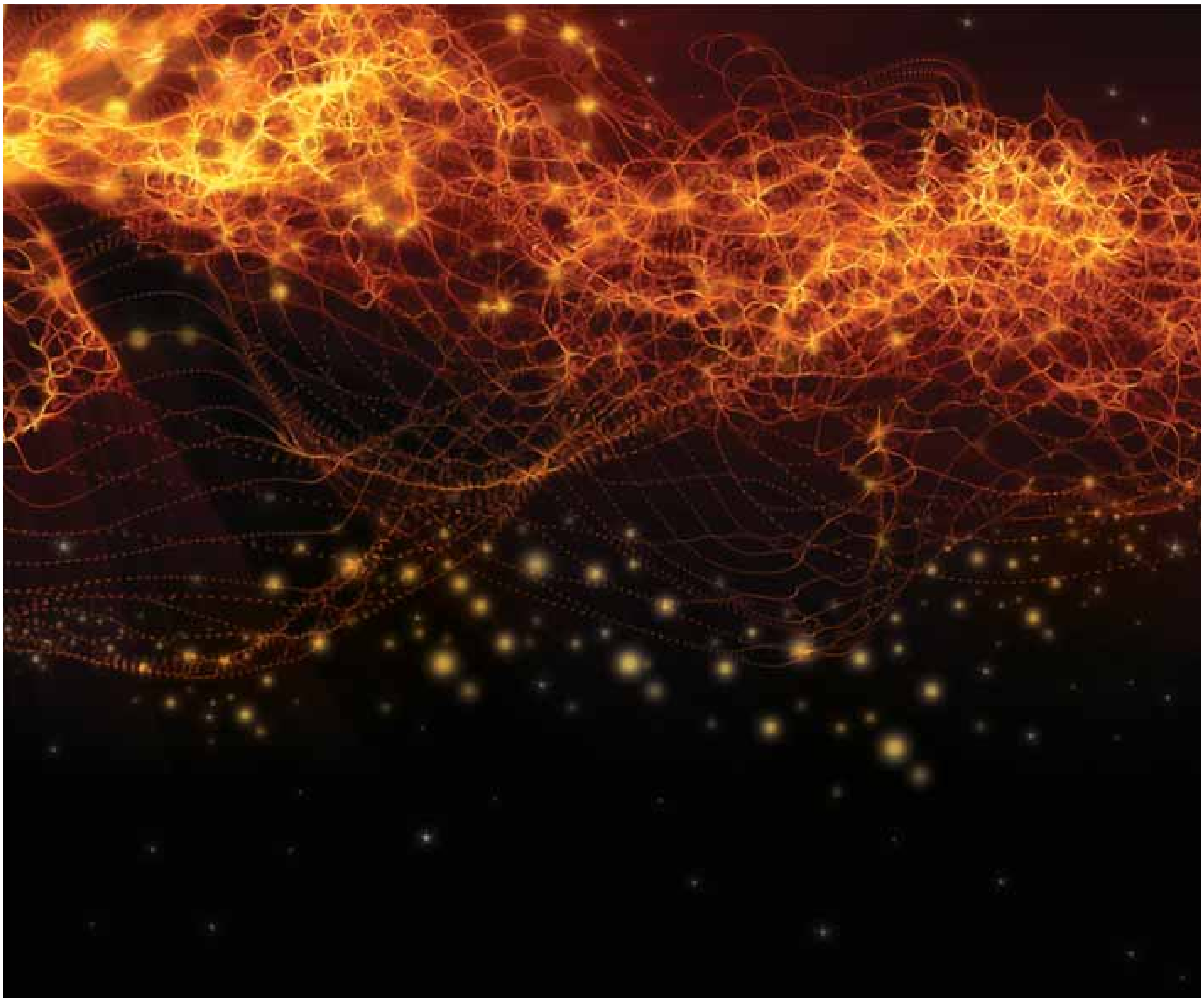
The documentation of timestamps created by software, whether it be base or application, is woefully inadequate and the forensic investigator often has to experiment in order to ascertain what is being recorded. This is especially true where timestamps have been recovered from deleted records. In some cases timestamps are recorded differently in what are basically the same files. Take the internet history file for example. Yes, but which one? The internet history file exists as a daily, weekly and full-history file, yet each records the time somewhat differently.

When looking in the full history file records are stamped with the time zone setting as the base, whereas the daily file takes daylight saving time (if initiated) as its base point. What other applications do is almost anyone's guess, hence the need for experimentation before offering an opinion.

Many pieces of evidence recovered during a forensic examination of a computer are partial fragments recovered from either a cache, or from the slack space between records. These often contain no time stamp information at all and so answering my originally suggested questions will depend on the existence of circumstantial evidence. This may be in the form of an invoice showing that the machine was purchased new on a certain date and has only been used by a single person, ergo it was 'them that did it'. It is then up to the jury to determine if this is sufficiently beyond reasonable doubt to convict.

We urgently need more information on timestamp formats, how the data is obtained and how it is recorded. This a research project which could be conducted internationally and continuously into the future. Is there a British university out there willing to initiate a project and is the BCS willing to provide the seed capital to get it started? Please let me know.

John is managing director of LHS Business Control, a corporate governance consultancy.
john@lhscontrol.com
www.lhscontrol.com



A quantum of cryptography

Cryptography can be the bane of any forensics professional but it is also a legitimate tool for businesses. Tom Graham, an associate at law firm Nabarro looks at quantum cryptography from a legal point of view.

The recent demonstration by the organisation Secure Communication Based on Quantum Cryptography (SECOQC) of a secure computer network protected by unbreakable quantum cryptography has been hailed as a major step along the road to perfect privacy. This news will have been met with no small measure of relief by businesses that have either already fallen victim to or are vulnerable to cybercrime. It will also have been welcomed by public bodies keen to avoid more highly publicised losses of sensitive data.

You could be forgiven for thinking that we are now leaving the age of public key infrastructures and pretty good privacy and entering a new era of unbreakable encryption. However, is this new and exciting technology likely to catch on in the way the SECOQC hope? This article looks at some of the legal issues that may influence the wider adoption of quantum encryption.

How does quantum cryptography work?

It is worth pointing out at the outset of any explanation of quantum cryptography that Niels Bohr, one of the fathers of quantum mechanics, has observed that 'anyone who says that they can contemplate quantum mechanics without becoming dizzy has not understood the concept in the least.' The principles are so counter-intuitive that it is hard for our rational minds to accept. Even Einstein had trouble, consistently rejecting quantum theory and famously arguing that 'God does not play dice'.

Therefore, as a rational lawyer, it is probably wise to limit any explanation to the following: quantum cryptography is based on the strange behaviour of light particles called ‘photons’. This strange behaviour has two consequences. First, it is impossible (according to Heisenberg's uncertainty principle) to measure every aspect of the photons' behaviour accurately. Secondly, and crucially, it is impossible to measure the photons without risking altering the properties you are measuring. Therefore, any third party seeking to eavesdrop on a communication protected by quantum cryptography cannot do so without being discovered. The SECOQC system is designed to shut down without being compromised when it detects an eavesdropper.

Quantum cryptography and conventional cryptography both rely on a secure key. The difference is that conventional cryptography relies on complicated mathematical functions to protect the secret key.

These mathematical functions are theoretically not impossible to break given sufficient time and computer processing power. However, the key created by quantum cryptography relies on the fundamental laws of physics and therefore, based on our current understanding, it cannot be broken.

Will quantum cryptography catch on?

Quantum theory, in addition to offering perfect secrecy, may render conventional encryption obsolete in another way. Quantum computing provides far greater processing power than conventional computing and so could eventually provide the kind of processing power necessary to crack the complicated mathematical functions on which conventional encryption relies. As long ago as February 2007 a US company D-Wave demonstrated what it called the ‘world’s first commercial quantum computer’. **http://tinyurl.com/5z8qhh**

Organisations may decide that as conventional encryption’s days seem to be numbered, upgrading to quantum cryptography is only a matter of time. However, are things as clear cut as that? As SECOQC accepts in its white paper - **www.secoqc.net** - promoting the use of quantum cryptography, no regulation currently expressly mandates the use of quantum cryptography.

Under English law, the Privacy and Electronic Communications Regulations 2003 (implementing EU Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector) and the Data Protection Act 1998 both talk about the use of appropriate technical measures to ensure an appropriate level of security, without specifying any particular method, or even the most technologically advanced method. In the case of the Data Protection Act, the appropriate level of security must be assessed in light of considerations such as:

- the state of technological development;
- the cost of implementing any measures;
- the harm that might result from unauthorised or unlawful processing; and
- the nature of the data to be protected.

Clearly for some companies or public bodies quantum cryptography may be difficult to ignore, particularly if the cost comes down over time. For example, because of the sensitive nature of the data they handle or because of the serious consequences of a security breach, either for the data subject or for the data processor.

But some existing regulations governing communications may ironically lead governments to limit the take-up of quantum cryptography. For example, in the UK, the Regulation of Investigatory Powers Act 2000 regulates the circumstances in which UK authorities can obtain access to encrypted information and communications. Since the nature of quantum cryptography precludes covert eavesdropping even by governments, this presents a problem for the state.

It may therefore decide, far from mandating the use of quantum cryptography, to seek to restrict its use to all but the most essential sectors of society.

Unbreakable encryption = unbreakable secrecy?

Having access to unbreakable encryption is not the same thing as having access to a foolproof system for protecting confidential information. Clearly data has no value unless it can be accessed and interpreted by the individuals sending and receiving it. Once data is recorded in human memories it loses the protection afforded it by quantum cryptography.

The recent case of Magical Marking Limited and another v Sean Holly and others [2008] All ER (D) 153 (Oct) provides an example of why human involvement will always create a weak link in otherwise secure data storage and communication systems.

In this case, when former business partners fell out, one of the estranged partners excluded the other from the premises of the company. However, the excluded partner enlisted the help of an IT consultant with knowledge of the company’s systems. He then attended the company premises with the IT consultant in the knowledge that the company's directors would not be present. He was therefore able to gain access to the company's IT system, copy all the material contained there (including confidential and copyrighted materials) and then change all the relevant passwords so that no one else could access them. Quantum cryptography provides no obvious solution to the problem of inside jobs where those with access to secure systems willingly abuse their position.

We don't know whether the use of quantum cryptography will become as widespread as conventional encryption. The decision for or against it will partly be driven by government regulation, either requiring or restricting its use and partly by company’s own risk assessments. Those companies who identify the interception of communications in transit as a particular risk are probably the most likely to conclude that quantum cryptography would provide a significant benefit. On the other hand, those who identify employee access as the most significant weakness in their systems are likely to reach a different conclusion.

These kinds of considerations may in any case one day be overtaken by regulation. If governments for reasons of national security take a restrictive approach towards the use of quantum encryption then its use may be prohibited in all but a few key sectors.

> **Even Einstein had trouble, consistently rejecting quantum theory and famously arguing that ‘God does not play dice’.**

Forensic readiness plans

Andy Henry, head of forensics at Portcullis asks, what are forensic readiness plans and is it time to think about getting one?

The Cabinet Office report on data handing procedures in government, issued in June 2008, details a number of mandatory minimum measures on data handling across government. One of these mandatory requirements is for the creation of a forensics readiness plan (FRP). Up until this report was issued, the forensics readiness plan was mainly a recommendation and never really given much attention. This requirement is intended for government systems and those organisations and agencies connected to them, though surely, it won't be long before compliance ensures that the private sector follows suit?

Most organisations will have already addressed the various disaster recovery and incident response issues that may arise from time to time and have a variable impact on the business. Possible mitigation for these issues may include such things as off-site backups, off-site hot spares or even complete remote clustered systems. All of which are designed to keep the business running or provide effective and speedy recovery in the event of a serious incident or disaster.

Some incidents that affect the business may not always be regarded as disasters but merely security incidents, either from an external source or perhaps even from an employee. Nevertheless, each incident has to be addressed in some way and an investigation launched if the incident is of sufficient severity.

In the event of such an incident, the corporate incident response plan will be put into action and potential virtual teams from across the organisation will meet and the investigation will proceed.

Incidents are wide, varied and can range from a server crash, denial of service or breach of company IT usage policies to even a power failure in the main data centre. The primary responsibility of any incident response from IT support personnel is to get the degraded system back up and running as quickly as possible. However, these actions although performed for the good of the business may actually be contrary to the requirements for an effective investigation.There are many types of incidents that may require some form of forensic investigation, and naturally, the collection of evidence. Where is that evidence going to come from, who is going to collect it and how is it going to be handled? Detailing the procedures in how to handle an incident should be well documented in the incident response plan. This plan is just that, responding to an incident, always after the event.

What about planning for that inevitable incident? Not planning what will be done after the event, but preparing the systems, procedures and staff to identify, preserve and store the data pertaining to that incident, long before it happens. This is the forensics readiness plan, pre-preparing for the post-incident investigation.

If the organisation has no forensic readiness plan in place, incident responders and subsequent forensic investigators are going to take some time examining systems for potential evidence, collating that information and proceeding with their examination and investigation.

In this case, the investigation will tend to take longer, cost more and may not provide for the best possible outcome. If however, there is a forensic readiness plan in place, those systems that are a potential source of evidence will have been previously identified, a collection and monitoring policy will already have been designed and implemented, response staff roles and responsibilities will already have been detailed. Evidence handling and storage procedures will have been written and prior arrangements with law enforcement and/or a specialist forensics company will have been made. This plan is going to save the organisation a considerable amount of time, resources and money, and could provide for a better and more comprehensive investigation outcome.

> **Incidents are wide, varied and can range from a server crash, denial of service or breach of company IT usage policies to even a power failure in the main data centre.**

The forensic readiness plan is not a piece of vendor-ware that is installed and forgotten, it is the culmination of a ground up look at the corporate business function and how that function is supported by its IT infrastructure. In turn, the FRP when implemented properly, could be used to support those business functions during any legal or tribunal proceedings.

The basic function of the FRP is to enable the effective collection of potential evidence long before the incident, and minimise the cost of the subsequent investigation of a security incident. It should be designed and implemented with the business in mind, and as part of a risk assessment, in conjunction with the global security policy and incident response plan.

A joint approach to forensic readiness planning is the key, as the forensic investigator knows what sort of evidence he is looking for during an investigation, the IT security manager or systems administrator is best placed to know where that potential evidence resides in the systems under his control and the data or risk owner will be best placed to decide which are critical assets and the risks associated with them.

The FRP will accurately describe a number of data sources, what potential evidence is available from them, and how it is to be collected and stored. The data sources will include IT assets including server logs, desktop workstations, network devices, and any security applications that may have a logging capability. It is not simply a case of implementing a global collection and logging policy. This would be costly, complex and most certainly an overkill approach. It is first necessary to identify under the risk assessment which system are critical assets, what is the likely threat, and the cost to the business should those systems be compromised.

The forensic readiness plan once implemented will need to be maintained, tested and updated if necessary. Systems change, staff turnover can be quite significant and in order to provide the best possible evidence during an investigation, the plan will need to be examined after any incidents to ensure that it is still fit for purpose and satisfies the requirements to have it in the first place. So in this current climate of expensive e-disclosure, litigation and intellectual property claims, now is the time to take a look at your corporate information security procedures and if you don't have a forensics readiness plan in place, then perhaps you should seriously think about the development and implementation of one.

FORTHCOMING | EVENTS

BCS ISSG legal day 2009

23 January 2009
Royal Air Force Club, Piccadilly, London.
The legal day will bring you up to date with key legal changes and news which may impact on the IT/IS professional's business.

BCS ISSG annual conference

26 - 27 March 2009
Venue TBC.
The annual conference is our premier event, and this year's theme will be 'data leakage and data loss - the new frontier'.

BCS ISSG annual general meeting

13 May 2009
Logica offices, Kings Place, London.
Every year we hold a free event in conjunction with our annual general meeting, usually at the premises of a major supplier of information security products.

Note: *There is no admission charge for this event, which is restricted to ISSG members only.*

IRMA events

Handling computer-related incidents in the workplace

5 February 2009. 17.00 for a 17.30 start
BCS London Office.
Speaker: Jan Collie.

Software auditing

14 February 2009.
17.00 for a 17.30 start
BCS London Office.
Speaker: John Mitchell.

Radio-frequency identification (RFID)

1 April 2009. 17.00 for a 17.30 start
BCS London Office .
Speaker: Ken Munro.

Large scale and complex fraud: the digital forensics approach and AGM

27 May 2009. 17.00 for a 17.30 start
BCS London Office.
Speaker: Keith Foggon.

Payment Card Industry (PCI) Data Security Standard (DSS)

1 July 2009. 17.00 for 17.30 start
BCS London Office.

Whitelist - the BCS security podcast

Whitelist is a fortnightly podcast discussing the latest security issues. Put together by the team behind the oddIT podcast it also includes expert analysis from leading industry figures.

Highlights from recent episodes...

Episode 16

When it comes to data losses it appears that the stories will never end. In one case a man bought a PC on eBay and then found that it had account details on its hard drive. The PC had been sold on by the bank's IT provider and the data hadn't been removed.

Added to this, levels of malware don't appear to be dropping either. In fact, in July 2008 the amount of files detected was twice as much as previous years and this wasn't a blip either.

Naughty admins

IT administrators have a lot of responsibility and according to a recent survey some of them are more than happy to take information that is available to them when they leave the jobs. It just goes to show that you should always be careful as to who has access to your systems.

Bank bungling

Customer's relations with banks is rarely smooth and it certainly wasn't for one Lloyds TSB customer whose chosen password for telephone banking was changed by a member of staff as it was seen to be insulting. It just goes to show that you should always choose your passwords wisely.

Episode 17

Following on from this we take a look a new way of logging in to your PC or authorising financial transactions. It's called GrIDsure and uses a simple five by five numbered grid and so all you have to remember is your pattern and not a five digit number.

Lack of data trust

It seems that all the recent data losses are starting to have an effect on people. According to a recent survey 89 per cent of people want companies that lose data to be prosecuted and four out of five don't trust companies with their data.

Hacking leads to divorce

Finally a Japanese woman has been arrested for hacking into her virtual husband's computer after she divorced him in the online game Maple Story.

To get whitelist go to www.bcs.org/podcasts or subscribe using iTunes.

UCL

M.Sc. in Information Security Management

UCL's MSc in Information Security Management is an advanced programme for Computer Science, Electrical Engineering and Science graduates who wish to pursue a rewarding and remunerative career at advanced levels of Information Security Management.

Modules

- Applied Cryptography
- Artificial Intelligence and Neural Networks
- Computer Graphics
- Computer Security II
- Crime Science and Detection
- Cryptography I
- Database Systems
- Digital Rights Management
- Examples of Security Management
- Financial Institutions and Markets **(the number of places may be limited)**
- Information Security Management
- Introduction to Cryptography and Network Security
- New Ventures Business
- People and Security
- Project Management
- Risk and Contingency Planning
- Software Engineering
- Systems Requirements Engineering
- Understanding Crime (subject to approval by UCL)

The programme is directed and supervised by Professor Ingemar Cox and Dr. Nicolas Courtois

Location

Students can enrol at either UCL's main Bloomsbury Campus or UCL's Adastral Park Campus in Martlesham Suffolk/ Most modules are available at Adastral park with live interactive video conferencing to and from Bloomsbury,

Contact Information:

Brian Riley 01473 829 067

http:// isecmgmt.adastral.ucl.ac.uk

UNIVERSITY OF
OXFORD

part-time study

network security
trusted computing
systems design
security processes
people and security

msc in software and systems security

www.softeng.ox.ac.uk/security