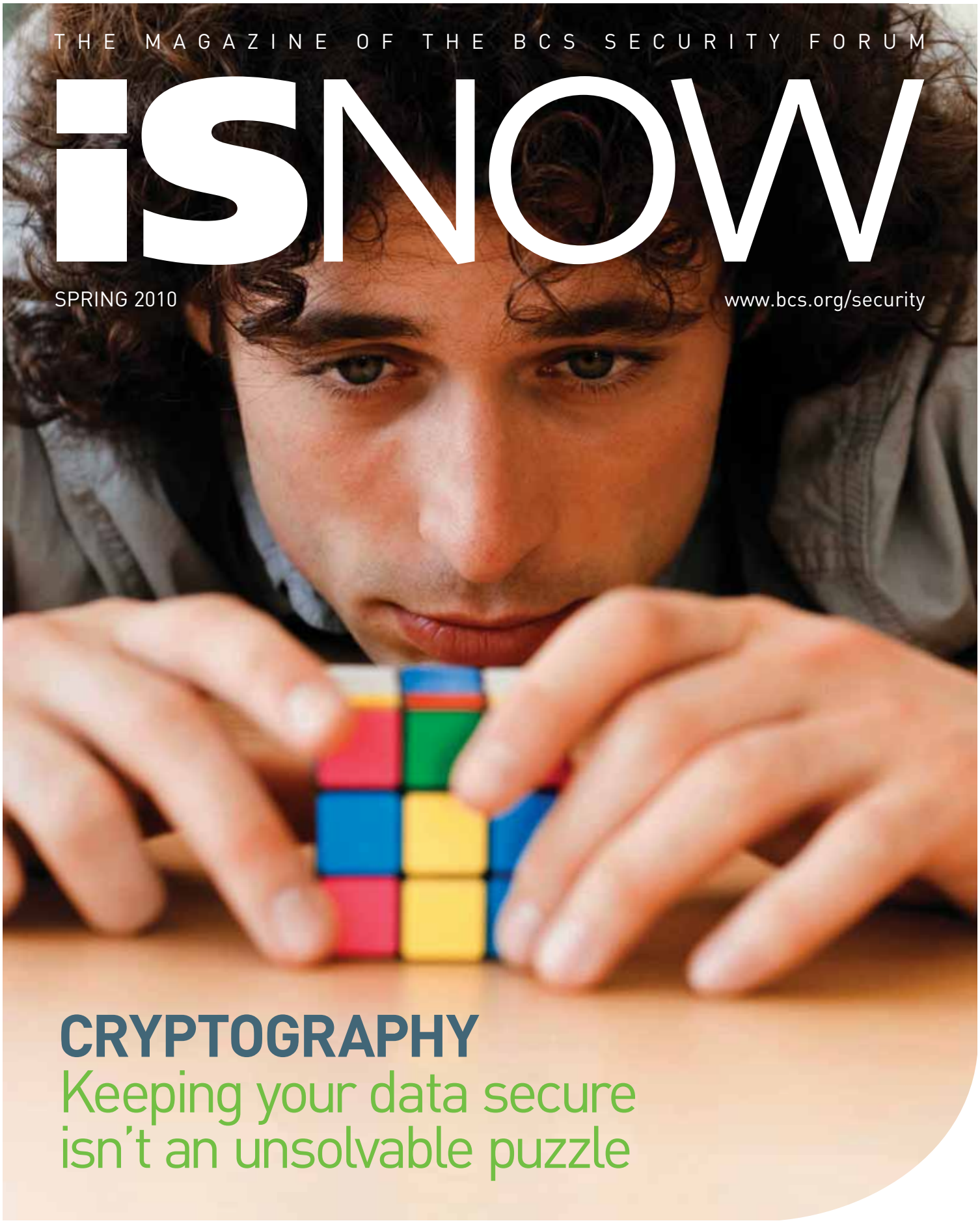
THE MAGAZINE OF THE BCS SECURITY FORUM

# iSNOW

SPRING 2010

www.bcs.org/security



## CRYPTOGRAPHY

## Keeping your data secure isn't an unsolvable puzzle

bcs The Chartered Institute for IT

# 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

**EDITORIAL TEAM**
**Henry Tucker** Editor
**Brian Runciman** Managing Editor

**PRODUCTION TEAM**
**Florence Leroy** Production Manager
**Marc Arbuckle** Graphic Designer
**David Williams** Graphic Design Assistant

**Advertising**
E catherine@atalink.co.uk
T +44 (0) 20 7074 7921

**Keep in touch**
Contributions are welcome for consideration.
Please email: editorialteam@hq.bcs.org.uk

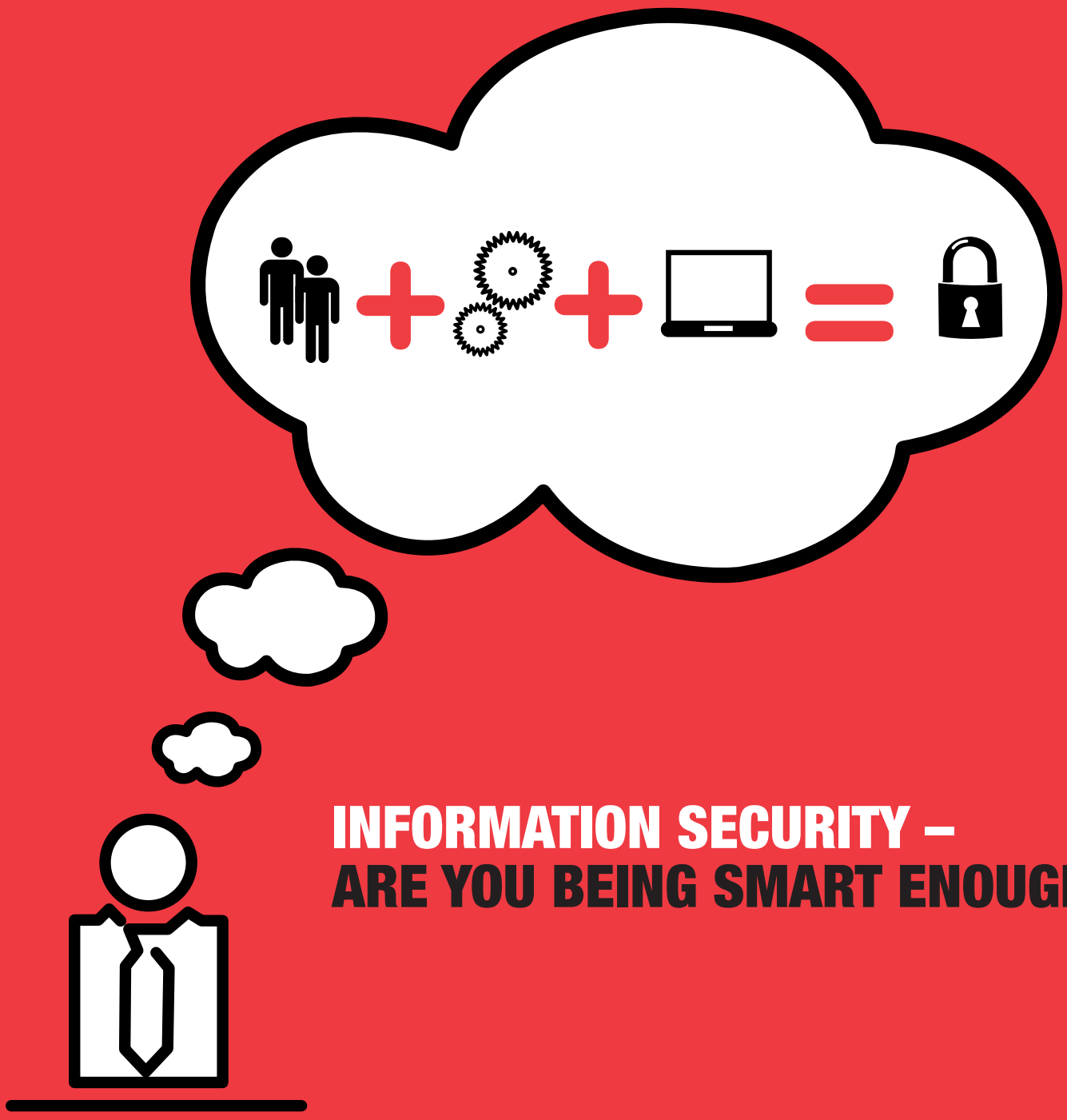
***ISNOW*** is the quarterly magazine of BCS Security Forum, incorporating the Information Security Specialist Group. It can also be viewed online at:
**www.bcs.org/isnow**



Printed in the UK by Interprint, Swindon, Wiltshire.
ISSN 1752-2455. Volume 4, Part 3.

**The British Informatics Society Limited**
First Floor, Block D, North Star House, North Star Avenue, Swindon, SN2 1FA, UK.
T +44 (0)1793 417 424
F +44 (0)1793 417 444
**www.bcs.org/contact**
Incorporated by Royal Charter 1984.

## CRYPTOGRAPHY



# INFORMATION SECURITY – ARE YOU BEING SMART ENOUGH?

Working smarter has never been so important and security so crucial when it comes to safeguarding and growing your business.

- Smart spending to justify and get value from budgets
- Smart optimization of your technology, processes and resources
- Smart people – education, training and awareness

**Register free* to attend now at:**

**www.infosec.co.uk**

**CELEBRATING 15 YEARS AT THE HEART OF THE INDUSTRY**
**EUROPE'S NO.1 INFORMATION SECURITY EVENT**

**27 – 29 April 2010**

**Earls Court**

**London | UK**

Organised by:

Reed Exhibitions®

infosecurity® EUROPE

* Register free before 23rd April at 5pm. Onsite registration £20.

# ROBUST DEFENCES

**ISSG Chairman Gareth Niblett says that when it comes to choosing a cryptography solution you need to make sure it is fit-for-purpose.**

Cryptography now protects most organisations' laptops, drives, removable media and communications, yet effective use of such technological solutions requires much more than selecting a vendor and implementing a product. Thought needs to be put in to how key recovery, data loss prevention, monitoring and audit work.

Cryptographic algorithms should be subjected to extensive peer review before being considered as robust and this process alone can take years, and then the new algorithm needs to be implemented - hopefully before the old one is irrevocably broken in some way. The false protection of 'security through obscurity' was destroyed recently when a number of GSM mobile encryption algorithms were broken.

Not only do crypto algorithms need to be robust, but they must translate effectively into implementation in a cryptographic module. The need for this was demonstrated recently when some USB memory sticks, validated to FIPS 140-2, and therefore approved to hold low-level classified data, were discovered to have a serious flaw that allowed ready access to the data.

There has been a lot of research into anonymous untraceable electronic cash and the cryptographic underpinnings required for it and things like coin divisibility, blind signatures, offline convertibility and to prevent double spending. Although there may be concerns about allowing such things, surely this is simply trying to replicate how cash works today?

Encryption techniques will continue to move forwards, fighting against the brains of mathematicians and the brawn of computing power; the emergence of elliptical curve cryptography (ECC) and quantum cryptography is already on the horizon, with more esoteric solutions to come.

**Gareth Niblett is chairman of the Information Security Specialist Group (ISSG).** www.bcs-issg.org.uk

## FURTHER INFORMATION

**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

# MOUNTAINS and molehills

**It started out as something that no military body would be without, now cryptography is something that businesses large and small should have in their armoury so says Paul Ducklin, Head of Technology, Asia Pacific, Sophos.**

Even in 2010, the word cryptography still carries a strong whiff of derring-do. It brings to mind secret agents deep behind enemy lines, tapping out brief Morse code messages on long-wave radios, knowing that to be caught with a transmitter would mean certain death. It conjures up smoky images of polyglot code breakers working through the night in leaky and improbably uncomfortable military huts, desperate to unscramble the latest enemy communications to protect their comrades on the battlefield.

Indeed, the historical connection between cryptography and affairs of state, military and diplomatic, had the result that until the late 1990s, many jurisdictions regulated cryptography in the same way as munitions. In some countries, a certificate to own a firearm, such as a shotgun or a handgun, was

easier to acquire than permission to trade in encryption software.

Until 1994, cryptographic regulations for the Western bloc were devised by CoCom, the Coordinating Committee for Multilateral Export Controls. Since 1996, CoCom's lists of restricted technologies have been replaced by the Wassenaar Arrangement, the Basic Document of which, at just 112 pages, must be considered a masterpiece of brevity by an international committee of its sort.

**Cryptography had turned into a mountain**

Ironically, the strict regulation of encryption software exported from the USA didn't prevent encryption from becoming a popular sales feature in software produced there. And since the USA is the largest and most influential, if not always the most innovative, of software markets, this led to a strange outcome.

Software vendors included encryption features, but deliberately nobbled them, ensuring that they would be crackable by the authorities and thus unsuitable for use in military or diplomatic environments. Products with weakened encryption could therefore be sold worldwide, but with an unfortunate side-effect: a false sense of security for business users and consumers.

Early web browsers, for example, supported only 40-bit SSL encryption, at least in their so-called International Editions. This deliberate limitation permitted the software to be sold into and out of most countries, neatly avoiding the legal mountain of export regulations.

But even in the 1990s, 40-bit symmetric encryption was an insufficient foundation for security. With 40 bits of key (a bit is a binary digit), there are 2^40 possible encryption keys. That's about one million million keys - a massive amount to a human, but a relatively small total to a computer, even one from the 1990s.

By 1998, a specialised computer to crack 56-bit DES keys by brute force in just a day (a task nearly 100,000 times bigger than cracking 40-bit keys) had been built for US$250,000. By 2006, the same job could be handled in under a week for just US$10,000. To such devices, cracking 40-bit keys is the work of seconds.

**Cryptography had turned into a molehill**

Fortunately, things have improved greatly on the legal front. Online business would never have taken off had they remained limited to 40-bit SSL encryption. The general deregulation of top-quality encryption tools for private and commercial purposes worldwide has been an important factor in the growth of web-enabled commerce.

Unfortunately, many web-enabled businesses haven't taken the advantage one might reasonably expect of this highly beneficial change.

For example, webmail services were slow to adopt SSL by default, because of the extra overhead in encrypting email traffic. It seems they preferred customer numbers over customer security. Similarly, some web hosting companies still allow their users to upload new content using FTP, in which usernames and passwords are exchanged in clear text, instead of mandating the use of SFTP, FTP's secure cousin.

Many businesses allow employees out on the road with unencrypted laptops stuffed with sensitive data, or transfer personal data between departments or divisions on unencrypted storage devices. Presumably they are gambling that their laptops won't number amongst the 12,000 lost each week at US airports, or that their backup CDs containing information on 25,000,000 individuals won't vanish in transit.

As a result, possibly the greatest irony in the mountain-or-molehill history of cryptography is unfolding right now. Some jurisdictions already have, and many others soon will, apply regulations which specifically require encryption when personally identifiable information is at stake.

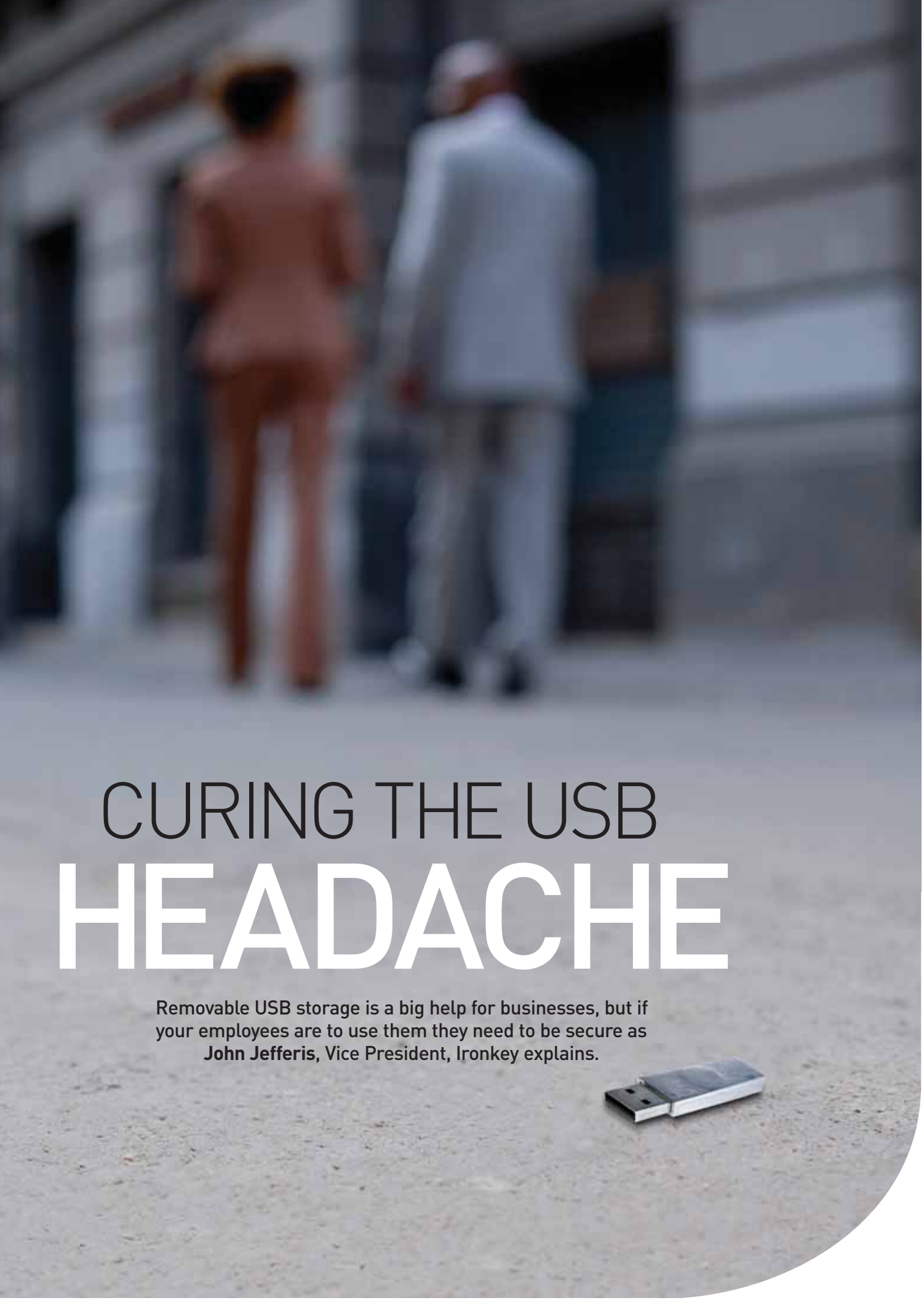
This will move us from a digital world in which encryption was considered a sacred military cow into one in which encryption will become a mandatory business practice.

It seems a pity that many organisations which keep personal data, especially when they hold onto it for their own commercial advantage, need to be compelled by law to look after it as simple decency suggests they ought, but if laws are what it takes, then we shall be bound to support them.

So if you still get nothing more than a whiff of derring-do when the word 'cryptography' is mentioned, you probably ought to wake up. It's 2010, not 1940.

So if you still get nothing more than a whiff of derring-do when the word ' cryptography' is mentioned, you probably ought to wake up. It's 2010, not 1940.

**For more security articles go online to** www.bcs.org/articles



# CURING THE USB HEADACHE

Removable USB storage is a big help for businesses, but if your employees are to use them they need to be secure as **John Jefferis**, Vice President, Ironkey explains.

USB drives, or memory sticks as they are sometimes referred to, are immensely popular and increasingly selected as the weapon of choice by employees looking for flexibility of their working environment. Having proved invaluable in increasing productivity they are easy to use, regardless of the user's technical ability, and able to carry millions of pages of data. The scenarios where they bring benefits are numerous, for example working from home, working on location at a client site, those using multiple computers, when travelling they can provide a means to back up your laptop, transfer information between your portable devices, and share data with customers at conferences or exhibitions, to name just a few. However, a word to the wise - this productivity comes at a cost higher than the original price tag.

These dream devices are proving an absolute nightmare for IT managers as they struggle to ensure the data they carry is secure. A standard DVD-data-sized (4GB) key fob drive can be bought online for less than £10 and from high-street retailers for little more. Coupled with the fact that a growing number of mobile phones and MP3 players are now starting to reach this level of storage capacity - and come with standard or mini-USB connectors, and you begin to understand the scale of the problem.

One serious risk is that of their being lost or stolen, as highlighted in an annual national independent study conducted by the Ponemon Institute into 'Trends in Insider Compliance with Data Security Policies'. In its most recent study (published June 2009) it discovered that 43 per cent of respondents admit to having lost or had stolen a portable data-bearing device. Another increasingly apparent issue is that of spreading viruses and malware. This was aptly illustrated by Ealing Council who revealed in September that it was forced to cut internet and phone links to preserve 'core systems and data' when a worker plugged an infected memory stick into a computer in May 2009. The sophisticated virus spread rapidly, with further shutdowns required when the network was re-infected twice the next week, with all terminals having to be rebuilt or replaced. The council is faced with a £501,000 bill for the emergency recovery and in lost revenue but it is feared the final cost could top £1.1 million if a new computer security system is needed. This is not an isolated incident and, in fact, was virtually the same as that suffered by Manchester City Council in February.

However, both of these risks can be counterbalanced by defining an effective IT security strategy. Here's how:

**Step 1: ban staff from using unprotected sticks and uncontrolled devices**
In the first instance, companies should bar staff using 'vanilla; (i.e. unprotected) USB sticks onto company premises, or use them on work-at-home PCs, if company data is involved.

**Step 2: give them something they can use**
Employees want to use them so remove the allure of USB sticks and provide an authorised corporate secure, encrypted, USB storage device. Increased productivity should compensate for the initial outlay and using a pooling system will help keep a lid on costs. By definition secure means a USB stick with a degree of security intelligence built into it such as encryption by default. This intelligence is quite benign and sensible, typically including on-board anti-malware and virus software - updated across the internet each time the device gains access.

**Step 3: induction**
If you don't already have a staff induction course, you need one, as all sorts of company legislation needs to be explained to new employees, as well as temporary workers from agencies. An important part of the process is to familiarise all employees with security policies. It is worth stating that any amendments to the security policy, and any other policies for that matter, should be communicated to existing employees with a method for tracking those that have been made aware of the change - ignorance shouldn't be used as a defence.

**Step 4: education versus draconian**
Rather than 'because I said so', all mandates should include an educational element so as not to be viewed as a pointless exercise created by those who 'don't understand how we work'. Explaining the reasoning behind rules will often gain employees support as they can follow the impetus behind the instruction rather than simply wishing to circumnavigate the obstruction.

**Step 5: identify what's out there**
It's vital to use on-network/IT resource technology that analyses new devices as they are hooked up to the company system and lock out any unauthorised device. No exceptions, even for the MD.

**Step 6: manage centrally**
All devices should be involved in a remote portable device scheme, whereby portable devices are updated with IT security policies and checked for general well-being as they connect to the company IT resource - directly, or across the internet. A reputable IT security system will include the remote management and tracking of secure intelligent flash drives, and also include the ability to recover content, reset a password and re-deploy or destroy data on a device as and when required. It's often this remote control facility that proves a serious lifesaver for staff and management, as USB sticks and portable storage devices can throw a wobbly.

43 per cent of respondents admit to having lost or had stolen a portable data-bearing device.

**Step 7: back up**
Finally, you'd be surprised how many people rely on these devices yet fail to take a back-up - even though their desktop or laptop PC is backed up automatically and regularly.

In an ideal world, all staff would understand the need for IT security, and backups for that matter, but life's too short, and some staff, let's face it, have other priorities in life. They, and we, are only human after all. This is where an effective IT security strategy that utilises automated security management of portable storage devices, as well as other on-network resources, is so critical. Good management software operates unobtrusively in the background.

We can't all be super-tech-savvy like Tom Cruise in Mission Impossible, but we can use our IT resources sensibly and comply with best practice, without having to worry about it. That's what differentiates a good IT security strategy from an effective one.

**For more security articles go online to:**
www.bcs.org/articles

**With all manner of data now at risk from loss or attack the sensible option is to lock down as much as possible with encryption according to Alex Campbell from DeLoitte.**

# LOCKING DOWN DATA

More and more organisations make an increasing amount of their data available to their customers, employees and suppliers over a wide range of channels. Real time access to data brings significant advantages; it allows an organisation's customers to access their personal data and perform various types of online transactions (e.g. banking payments). It also gives employees instant access to information, which can lead to better decision making and ultimately a more efficient operational environment. And for external suppliers, in many instances, the exchange of sensitive customer data with the parent organisation can help improve the overall customer experience.

However, as the communication channels and data recipients increase, so does the potential for attackers to exploit these channels and obtain unauthorised access to the data.

Cryptography plays a central role in protecting sensitive data from such attacks. This protection may take several forms.

**Local encryption**

Cryptography in its most basic form can be used to encrypt sensitive data stored locally (e.g. on user laptops) or centrally (i.e. in databases) so that even if attackers manage to get access to the storage device, the data is unreadable without obtaining the corresponding cryptographic keys (or passwords) to decrypt it.

For database encryption, there are several technology approaches to consider. Most database vendors have developed their own utilities that support whole or partial database encryption. These are typically shipped with the database software allowing the administrators to activate and configure encryption according to their security requirements and policies. An alternative approach is based on the data being encrypted at the application side before it is transferred to the database, thus also ensuring that the data is protected while in transit between the two

components as well as when stored within the database.

Additionally, many third party hardware products are available that can be used to encrypt all data before it reaches the database. As most of these products have been designed for this purpose, the impact of encryption on the overall system's performance is significantly reduced compared to other options (but will come at a cost). Organisations deciding on the best database encryption option for them, need to carefully consider a number of criteria, such as the amount of data that requires encryption (as the database will most likely contain a combination of sensitive and non-sensitive data), the acceptable level of performance degradation due to the encryption/decryption function and how the chosen solution best fits into their organisation's storage architecture (i.e. integration requirements differ based on standalone database vs. storage area network (SAN)).

For data stored locally, there has been a proliferation of laptop encryption technologies in the marketplace designed to provide whole disk encryption (as opposed to encryption of individual folders or disk partitions). Significant steps have been made in rolling out such enterprise solutions in recent years as organisations are slowly realising the potential impact of data leakage incidents. From a reputational point of view this can be substantial as we have seen from many recent examples of such events becoming front page news. There could also be a potentially financial impact if sensitive data gets in the hands of organised crime as well as the possibility of a regulatory fine following an incident due to lack of suitable security controls.

Another area where cryptography is used is for establishing secure communication sessions between remote data requestors and central repositories (i.e. databases). This can be achieved by performing a cryptographic function, often referred to as a 'handshake', between the two parties to authenticate each other and allow them to establish a trust relationship.

**Key sharing**

One of the fundamental challenges associated with establishing such sessions between two geographically remote entities is the ability to share a cryptographic key that will enable the subsequent protection of the session. The use of asymmetric (also known as public-key) cryptography addresses this problem to a large extent by eliminating the need to send 'secret' keys over unsecured channels, although to ensure there is adequate trust in the association of an entity with a public key there is a further requirement for the use of digital certificates. This certificate will enable the mathematical binding between the key and the key holder (which can be an individual user, system or website), which is fundamental for authentication and non-repudiation purposes (i.e. to eliminate the key holder denying use of his/her key at a future date).

As the communication channels and data recipients increase, so does the potential for attackers to exploit these channels and obtain unauthorised access to the data. Cryptography plays a central role in protecting sensitive data.

It is clear there is a considerable level of complexity that needs to be overcome in order to effectively apply certain cryptographic principles to authentication and data encryption. In most systems, however, the use of cryptography is transparent to the end user as the complexities of key exchanges and encryption algorithms are hidden beneath the application layer (e.g. SSL protocol, which enables secure website sessions via https, is based on public-key cryptography).

It is clear that the protection of an organisation's data must not rely solely on cryptographic controls such as the ones described above. Although cryptography implementations provide a strong layer of security, to be successful they must be driven by an overall security governance approach with clear objectives and policies across multiple layers of security.

This approach must also be supported by a security awareness campaign to communicate to all employees the importance of safeguarding their organisation's data. However, if these controls fail and sensitive data gets in the wrong hands either via a stolen laptop, a CD that is left on a train, or via a hacker successfully penetrating into the organisation's inner network, then cryptography is often the last line of defence.

**For more security articles go online to** www.bcs.org/articles

# THE HUMAN **FACTOR**

**With the ubiquitous use of laptops and handheld devices, a secure physical environment, while requisite, is no longer sufficient says Stephen Midgley, from Absolute Software Corp.**

As we enter a new decade, IT departments are faced with a proverbial perfect storm when it comes to securing data. Departments are dealing with reduced operating budgets resulting in them having to do more with less. There is a growing movement from various levels of government to regulate the security of data, such as the recent announcement by the UK Ministry of Justice that the Information Commissioner's Office (ICO) would have the power to fine organisations up to £500,000 for serious breaches of data protection principles. The European Council has approved a data breach notification rule for Europe's telecommunications firms. This amendment to a EU Directive will force telcos to inform customers if they lose their data. The growing enactment of regulatory legislation related to the securing of data will force the hand of corporations to establish necessary processes to ensure the integrity of data. To not do so could result in them being subject to significant negative financial and reputational repercussions if a data breach were to occur. According to the Ponemon Institute, the average cost of a data breach to an organisation in the UK is £1.7 million, while in Germany it is €2.41 million.



Along with reduced operating budgets and growing government legislation, the general public has become acutely aware (and concerned) about the security of their personal data as the instances of lapses in data security continue to increase. In fact, according to the ICO, the number of recorded data breaches in the UK increased by nearly 65 per cent last year over the previous year.

**Lost laptops**

And finally, there is the growing mobility of the workforce – from people travelling with their data to people telecommuting from their homes. According to the Ponemon Institute, over 3,500 laptops go missing every week in European airports. That's one laptop every three minutes. While mobility creates business opportunities, it has accelerated the use of corporate owned devices outside of the traditional workplace. Especially as more and more employees work from home offices. The result is the creation of a information perimeter outside of the traditional enterprise perimeter.

This perfect storm therefore begs the perfect question for any IT department: how do you secure data that you cannot track?

Encryption has, for some time, been the de facto standard in securing data and is one of the most important security tools in the defence of data. While it is an important part of any approach to data security, encryption alone is not enough. It does not enable IT to track the data and it does not provide any details as to what type of information was stored on the missing or stolen laptop. In fact when an encrypted laptop goes missing, all IT really knows is they have a laptop with potentially damaging information in the public domain with no means of retrieving the data. And, according to the latest research from the Ponemon Institute, there is no guarantee that encryption was set up properly on the device in question. Surveying non-IT business managers in the UK, it was found that 66 per cent of them either wrote down their password on a private document, such as a post-it note or shared it with other individuals in case the password was forgotten.

IT departments, in this mobile environment, require more than encryption to securely track, manage and protect their data. What they need is a layered approach to security that enables them to track data on and off the local area network and provide them with various options to access the data in case a laptop does go missing, instead of being left wondering if the encryption was disabled. In order to be effective, encryption requires organisations and users to take appropriate steps to make sure sensitive and confidential information is protected as much as possible

**The human factor**

As shown in research conducted by the Ponemon Institute and sponsored by Absolute Software on The Human Factor in Laptop Encryption, a cultural divide exists between non-IT business managers and IT practitioners when it comes to security. Too often IT is being bypassed, losing control, yet they remain accountable for data security and ensuring performance, integrity, availability and compliance of that data. It was found that a high percentage of employees surveyed in business functions (referred to as business managers) were not taking such precautionary steps as using complex passwords, not sharing passwords, keeping their laptop physically safe when traveling or locking their laptops to their desks to protect sensitive and confidential data. Further, many respondents believe that encrypted solutions make it unnecessary to take other security measures.

In contrast, their colleagues in IT and IT security functions (referred to as IT security practitioners) are diligent in taking all or most precautionary steps to safeguard the sensitive and confidential information on their laptops. They believe encryption is an important security tool, but believe it is critical to follow certain procedures to ensure that data is protected if a laptop is lost or stolen.

The following are some of the most salient findings:

- 86 per cent of IT security practitioners report that someone in their organisation has had a laptop lost or stolen and 61 per cent report that it resulted in a data breach. Only 45 per cent report that the organisation was able to prove the contents were encrypted.

- 59 per cent of business managers surveyed strongly agree and agree that encryption stops cyber criminals from stealing data on laptops versus 46 per cent of IT security practitioners who strongly agree or agree.

- 53 per cent of business managers have disengaged their laptop's encryption solution and 43 per cent admit this is in violation of their company's security policy.

**For more security articles go online to:**
www.bcs.org/articles

# ARE WE OVERREACTING?

Although cybercrime is a big threat to individuals and businesses this is just one of the threats that are out there says **Bill Roth** from LogLogic CMO.

Thanks to tough economic times (and the resulting hit on our wallets) and a generous dollop of fear-mongering from the media and opportunistic profiteers, we've all become myopically obsessed with cyber-crime. This is not entirely a bad thing. Unless you've been living under a rock, everyone knows that technology has created unimaginable opportunity for resourceful crooks. The pitfall is in our myopia. We've become so obsessed with cybercrime – a petty offence in the grand scheme of things – that we've overlooked the bigger picture.

A recent *New York Times* article reminded us of a conspicuously under-reported digital security threat: Cyberterrorism. Dennis Blair, the Director of National Intelligence (the uber-agency which houses the CIA), made the following comment in an appearance before the U.S. Congress:

'Malicious cyberactivity is occurring on an unprecedented scale with extraordinary sophistication.'

U.S. Secretary of State Hillary Clinton also recently shed light on the critical nature of this global issue when she urged NATO members to 'modernise and strengthen' their alliance to combat cyber-terrorism which has created a climate in which conventional weapons (i.e. missiles and bombers) are 'no longer sufficient to keep Europe and the US safe.

**Over hype**

A number of competitors (nominally in the log management market) are shamelessly hyping the dangers of cybercrime to degrees that border on the irresponsible. Yes, it is true that we need to be aware of hackers who want to steal our data. But in reality, true systems security is reliant on people, products and processes; it's not just about one single product which will solve all the world's security problems.

The fact of the matter is that bad things happen. You will be hacked. You may have already been hacked and not know it. A rational organisation will do three things.

**Fight off attacks**

First, put up the best defences you can. Second, implement the best people processes you can. Finally, be ready to clean up and perform forensics when you do get hacked, because one way or another, it will happen.

But the tools do exist to prevent, or at least discover when these types of attacks occur. The core assets IT environments can leverage are the mountains of log files that modern systems generate (but often ignore).

As has been noted by Mark Nicolett of Gartner, the best place to start is with log management. In his report, 'How to Implement SIEM Technology', Nicolett recommends the following starting place for building out what he calls a 'Security Information and Event Management' infrastructure:

Deploy a log management infrastructure. In most cases, the project team should implement log management functions before event management capabilities.

A number of competitors (nominally in the log management market) are shamelessly hyping the dangers of cybercrime to degrees that border on the irresponsible.

**Not in it for the money**

These are important reminders that all cyber-threats are not strictly for money and are certainly not all commercial. In fact, there is good reason to believe that the largest increase in systems security vulnerabilities will occur as a result of political, not criminal, activity. The good news is that most IT environments already have most (but not all) of the tools to deal with this emergent threat.

In discussing this issue, it is important to first have a decent working definition of politics. Politics is the creation, distribution and maintenance of power across some group of people. In this case, as we have seen with the alleged Chinese attacks on Google, the struggle is over the power of information.

This new brand of digital threat takes advantage of a weakness in the hierarchy of law. Most of what we're exposed to is either civil law (like lawsuits, generally) or criminal law (the kind we need police to enforce). This new form of exploit, however, runs up against international law. While I am not a lawyer, the principal issues with international law are that it is both ill-defined and expensive (or impossible) to enforce.

If the increased nature of the geopolitical cyber-threat is indeed true, it says something about the current, often hysterical, narrative floating around the industry about cybercrime. I have to admit, it is getting some traction in the media, as a cybercrime story even appeared on NPR's Fresh Air show.

**Fundamental elements**

The reason Gartner recommends log management is that real visibility and control of your IT environment starts with the fundamental elements of what is really happening in and around your systems...the logs. Logs and their log messages are the core of building true visibility in your systems. The Greek philosopher Demosthenes calls the smallest, indivisible bit of matter atomos, or atomic. Log messages are the atoms of IT visibility in that they form the core of what elements are visible in any environment. Everything else builds on that, including security event management, and event management in general. And from this base, a whole new class of threats can be dealt with and managed. This includes the new class of state-sponsored threats which go way beyond the current narrative around cybercrime.

**For further information please visit:**
www.bcs.org/security

# **DATA PROTECTION** AND THE ICO

**Charlotte Walker-Osborn,** Partner, and **Jennifer Liddicoat,** Solicitor, Technology Group, Eversheds LLP, discuss the ICO's application of new powers to issue monetary penalties.

The Information Commissioner's Office (ICO) has confirmed its new powers to issue monetary penalties under section 55C(1) of the Data Protection Act 1998 (DPA). The new powers are due to come into force on 6 April and the penalties may be as high as £500,000. The ICO considers this new power key to its enforcement strategy and hopes the sanction will act as a powerful deterrent to organisations flouting, overlooking or being careless with data protection compliance.

The new powers apply to the provisions of the DPA but not the Privacy and Electronic Communications (EC Directive) Regulations 2003. Specifically, if a data controller has seriously contravened one or more of the data protection principles, in circumstances where it is likely to cause substantial damage or distress, this power may be considered. However, the legislation requires the breach to be deliberate or to be such that the data controller must have known, or ought to have known, that there was a risk that the contravention would occur but still failed to take reasonable steps to prevent it.

Some examples have been provided by the ICO on how it will interpret this new power. For example, many a manager will shiver at the application of 'know or ought to have known', thinking of a situation where their IT department has told the management team that laptop encryption is needed but it hasn't been implemented and a security breach subsequently occurs. Likewise, 'deliberately' collecting data for one purpose and then using it for another – a common and often unintentional theme where organisations try to maximise return on marketing databases. Data controllers may take some comfort that the ICO has confirmed that it only intends to use its new power 'in the most serious situations'.

Whilst it may have been security breaches that triggered the introduction of the penalty, it is important to note that its application is not limited to that category of breach. Other examples could arise from failure to keep records up-to-date: substantial damage could occur if an incorrect job reference is given or if a job application is declined because of information obtained from an unlawful source.

Further, the individual doesn't have to suffer just financial loss. Distress to the individual is relevant too, even if their concerns (e.g. publication of lost heath records) do not materialise. This is an important consideration where, historically, most have focused purely on financial impact.

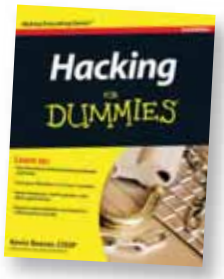
The penalties apply across all sectors, however, the ICO proposes to take account of the sector in which the organisation operates and 'the size, financial and other resources of the data controller' before making its decision. The ICO has confirmed that it doesn't intend to impose 'undue financial hardship on an otherwise responsible data controller'. The amount of penalties may vary widely, depending upon the circumstances.

The organisations under investigation will receive a notice of intent about penalty notices, in response to which the data controller may make representations to persuade the ICO to withdraw or reduce the penalty. The ICO may then use other enforcement powers or issue a formal penalty notice. There is also a right of appeal to the Tribunals Service, which may be against the notice as a whole, its amount or any variation of it by the ICO.

The new power is likely to be used most against organisations deemed to have sufficient resources to comply if they choose to, and which should have known better. The process of becoming compliant and continuing compliance obviously carries a resource cost and for those subject to the greater fining powers of other regulators such as the Financial Services Authority (FSA), the deterrent impact may not be as great as the ICO might like in order to sufficiently incentivise compliance. That said, deliberate non-compliance is likely to be viewed harshly. Publicly well-known organisations are also much more vulnerable, due to the media coverage that will be generated if they are selected for enforcement, giving the ICO publicity about its new power and its intention to use it.

# BOOK REVIEWS

**Hacking for Dummies**
(3rd Edition)
*Kevin Beaver*
Wiley
ISBN 9780470550939
**£21.99**




**8/10**

Now in its third edition, Hacking for Dummies is easy to read, the presentation is clear and uncluttered, it caters for a variety of audiences and it covers breadth rather than depth. The author presents not only the methods of attacks, but how to defend against them and also prevent them from happening in the first place. Hence this is an ethical hacking book.

Although the author does provide a brief health warning at the beginning of the book, and occasionally in chapters, this cannot be underestimated. Details of several tools and URLs are provided, but be warned that downloading and using the tools could harm your computer and those connected to it, particularly if used incorrectly. Your virus software is also likely to complain.

If using the tools at work, make sure you get permission from management as well as network and system administrators. Also, do not be tempted to go too far; by using the tools you could potentially have unauthorised access to systems and information.

The chapters progress from the basics of physical hacking to hacking networks, operating systems, including Windows 7 in this third edition, and applications, such as email, IM, VoIP, websites and databases. Since this is a book about ethical hacking, reporting results, prioritisation and counter measures are also discussed. There is the occasional case study to graphically reinforce the key points raised.

As with many dummies books, depth is lacking. For example, in the chapter covering password security, the basics of passwords are covered, along with a brief discussion on the tools and techniques that can be used to obtain or hack a password, but there is no detail on how to get access to the password file you are trying to hack.

If you have no or very limited experience of ethical hacking then this is the book for you. The best way to get the most out of it is to download and use the tools, but there are risks in doing so!

***Mehmet Hurer MBCS, CITP, CEng***

**Cloud Security and Privacy:** An Enterprise Perspective on Risks and Compliance
*Tim Mather, Subra Kumaraswamy, Shahed Latif*
O'Reilly
ISBN 9780596802769
**£26.99**


**9/10**

The concepts of cloud, security and privacy are not obvious bed-fellows and, as this is a key concern for both individuals and corporate users, it was only a matter of time before some books were published on the topic; and this book may well turn out to be one of the better ones, in my opinion.

The comprehensive depth of coverage provided by the authors makes this book a ready resource for those individuals or organisations that are serious about understanding security and the cloud.

It starts out with a contextual overview of the cloud, its position in the evolutionary timeline of the information age, which is then followed by an explanation of the SPI (i.e. software, platform and infrastructure) framework for cloud computing services, which neatly translates into the various services that are available.

Based on this foundation, the book then goes on to explore how and why security, privacy and the ability to cater for audit and compliance requirements are such hot topics, especially as they are also key barriers to adoption of cloud services in the enterprise.

The authors also provide much needed guidance on what to look for (and what to expect) from the typical CSP, and they also provide a listing of example CSPs and their service offerings. This level of coverage creates an almost encyclopedic view of the titular topics of cloud security and privacy.

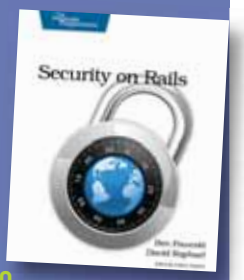
Unfortunately, it is not a straight forward read and readers unfamiliar with the enterprise security domain may well have to refer back to earlier sections in the book. Also the wide coverage means that it is not necessarily detailed enough for implementation decisions, without further information, but it does a good job of providing appropriate sources of reference for these anyway.

It is a great source of information on a hot topic and the combined experience and expertise of the authors brings credibility and added value.

***Jude Umeh, FBCS, CITP***

# BOOK OF THE MONTH

**Security on Rails**
*Ben Poweski, David Raphael*
The Pragmatic Bookshelf
ISBN 9781934356487
**£26.99**




**9/10**

The intended reader for this book is the professional web developer, with the book providing large amounts of example code illustrating both the correct and incorrect ways to do things.

The reader is assumed to have a good knowledge of web application development with Ruby, but no knowledge of application security or penetration testing is assumed.

The book begins with a very good introduction to and explanation of web application security issues, a large part of which can be applied equally well to other languages and environments once the developer understands the underlying issues.

This is followed by an explanation of how to test for security issues and which issues to test for. Coverage in this section is a bit light, as might be expected, but gets the main points across. No great criticism can be directed at this as proper, comprehensive security testing would require a full book on its own.

Different security issues are dealt with in turn by using an example application containing security issues that the reader fixes while working through the book. This method works very well, helping the reader to understand how the issues arise, why they are a risk and how to fix them.

Input validation is dealt with to illustrate how to protect against XSS, SQL injection and CSRF, followed by chapters dealing with authentication, authorisation and cryptography.

Full explanations are given showing how to locate the errors as well as fix them and by the end of the book the reader should have a much greater understanding of how to implement web application security and how to build more robust applications.

***Nick Dunn***

# SECRECY, FRIEND OF FOE?

**'Who goes there?' is the classic challenge of the sentry guarding the perimeter of the camp. A typical physical security barrier, but what happens when we cannot see the potential threat, or even know if our perimeter has been compromised? John Mitchell has some suggestions.**

Logical security is the obvious answer, but this itself requires us to have the ability of making the invisible visible. Conversely, if we want to keep something secret we need the ability to not only detect the invisible threat, but also to prevent our secrets from being 'lit up' by the enemy.

Keeping things secret is not only the domain of the military. We civilians are legally required to keep personal data secret and our organisation probably has things that are commercially sensitive that it would like to keep to itself. However, it is not only law abiding citizens that like to keep things secret; the criminals often have a greater desire to do so.

**Authorised access**

So security is a two-edged sword, with one side wanting to keep things secret and the other side wanting to find out what is being hidden. Interestingly, the Computer Misuse Act may be used against the good guys as well as the bad. If I legitimately want to see what you have electronically concealed, then I need to be certain that I am not opening myself to an accusation of 'unauthorised access', or worse still 'unauthorised modification'. The criminals do not care anyway, so the Act is only a deterrent to the law abiding.

I was asked to check a hard drive for some compromising material. First, I had to be sure that the drive was owned by my client company and not the user of the device. Second, I had to check that the firm had a policy that the equipment should only be used for the firm's business and that they had warned staff that the firm reserved the right to read all the traffic and data. Finally, to be sure to be sure, I required a clear, written request and authority from the company to examine the data. Then it became interesting.

The firm believed that the employee concerned was downloading pornography from the internet, but there was no indication of pornographic images on the drive. The computer was not locked down so the user could load any software that they liked. A trawl of the programs on the machine revealed one called Invisible Secrets. I knew that this software allowed the hiding of data inside image files so I had a good idea that there was some steganography involved in keeping things hidden. But where? The firm was in the graphic design business so there were upwards of 10,000 images on the hard drive, but which one(s), if any, held the invisible secret(s)?

I had already found some password protected word-processed files, which I had accessed quite easily with some commercially available software because the password was a dictionary word, but now it was find the needle in a haystack time. I tried writing a script to automatically open Invisible Secrets, access an image file to see if it asked for a passphrase (which would indicate something hidden) and if not, then cycle to the next file. This did not work because of the interrupts involved so it was back to a more prosaic approach. My assistant noticed that the suspect's cubicle contained numerous pictures of exotic cars so she suggested first searching images of that type. Bingo! The fifth file I opened using Invisible Secrets asked for the pass phrase. Fortunately, our suspect had been lazy and the pass phrase was the same password that we had previously unmasked from the word documents.

**Unbreakable encryption**

The moral here is that the bad guys need to keep secrets too and they have very powerful tools available to them. Asymmetric encryption, as provided by PGP, is currently unbreakable without the secret key and the legislation embedded in the Regulation of Investigatory Powers Act for the disclosure of a key demands a derisory two years in prison. Compare this with 15 years for making a paedophilic image, 10 - 15 years for money laundering and breaching the Proceeds of Crime and the Terrorism Acts. I know which one I would rather confess to!

**For more information visit:**
www.bcs.org/security

# Beam them up, Scotty

## Don't klingon to your servers.

If you are still buying in-house servers and managing them yourselves, it's time to see the new way of computing – computing as a service from Rackspace.

Free your business from the hassle of in-house server management, benefit from the flexibility and scalability of pay-per-use hosting solutions.

Choose a better way to manage your computing resources. Choose Rackspace Hosting, choose Fanatical Support®!

Find out more at www.rackspace.co.uk/nomoreservers


Managed Hosting • Cloud Hosting • Email & Apps
www.rackspace.co.uk 0800 988 0100

rackspace HOSTING