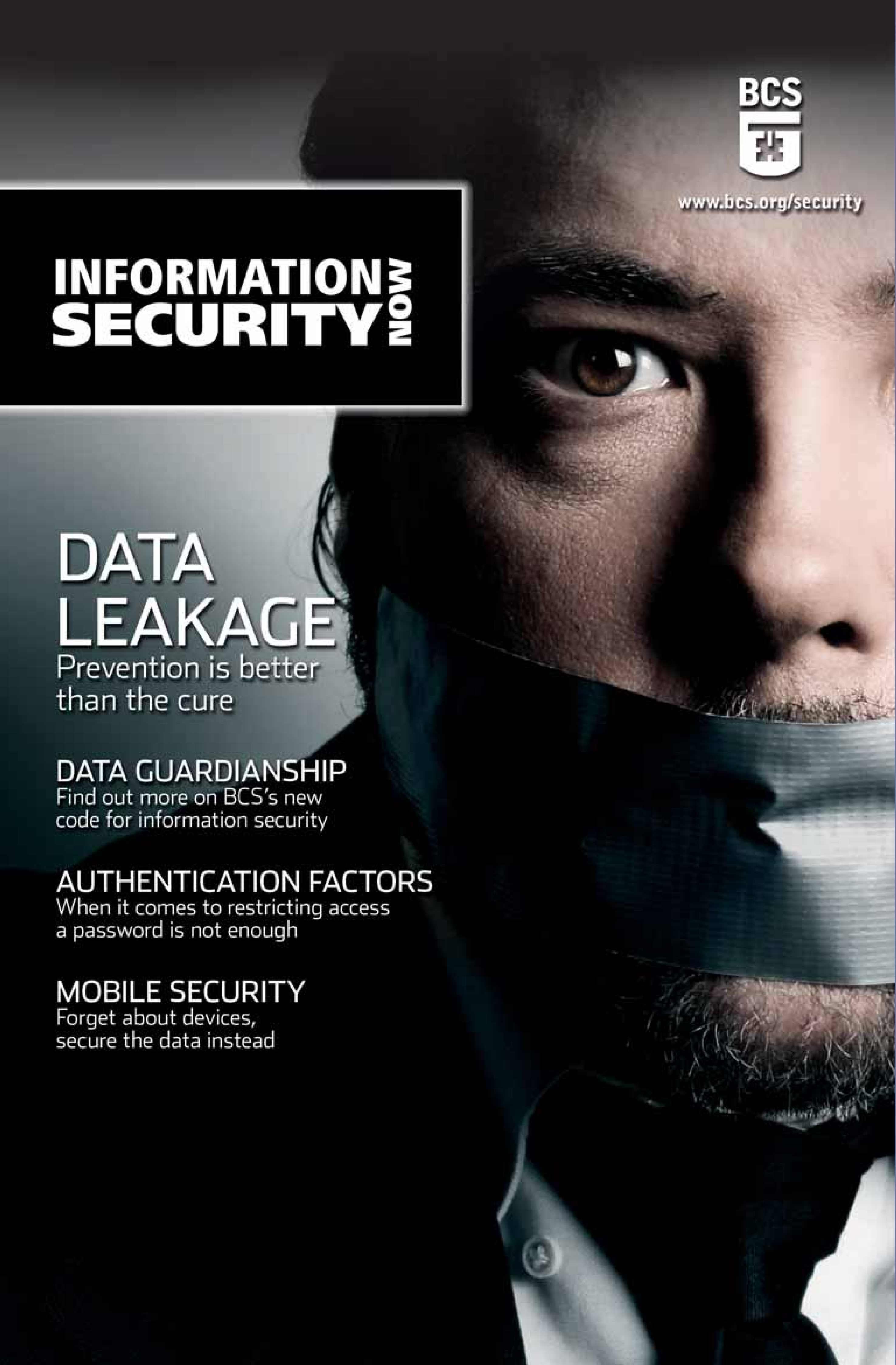
SUMMER 2009

BCS

www.bcs.org/security

INFORMATION SECURITY NOW



DATA LEAKAGE

Prevention is better than the cure

DATA GUARDIANSHIP

Find out more on BCS's new code for information security

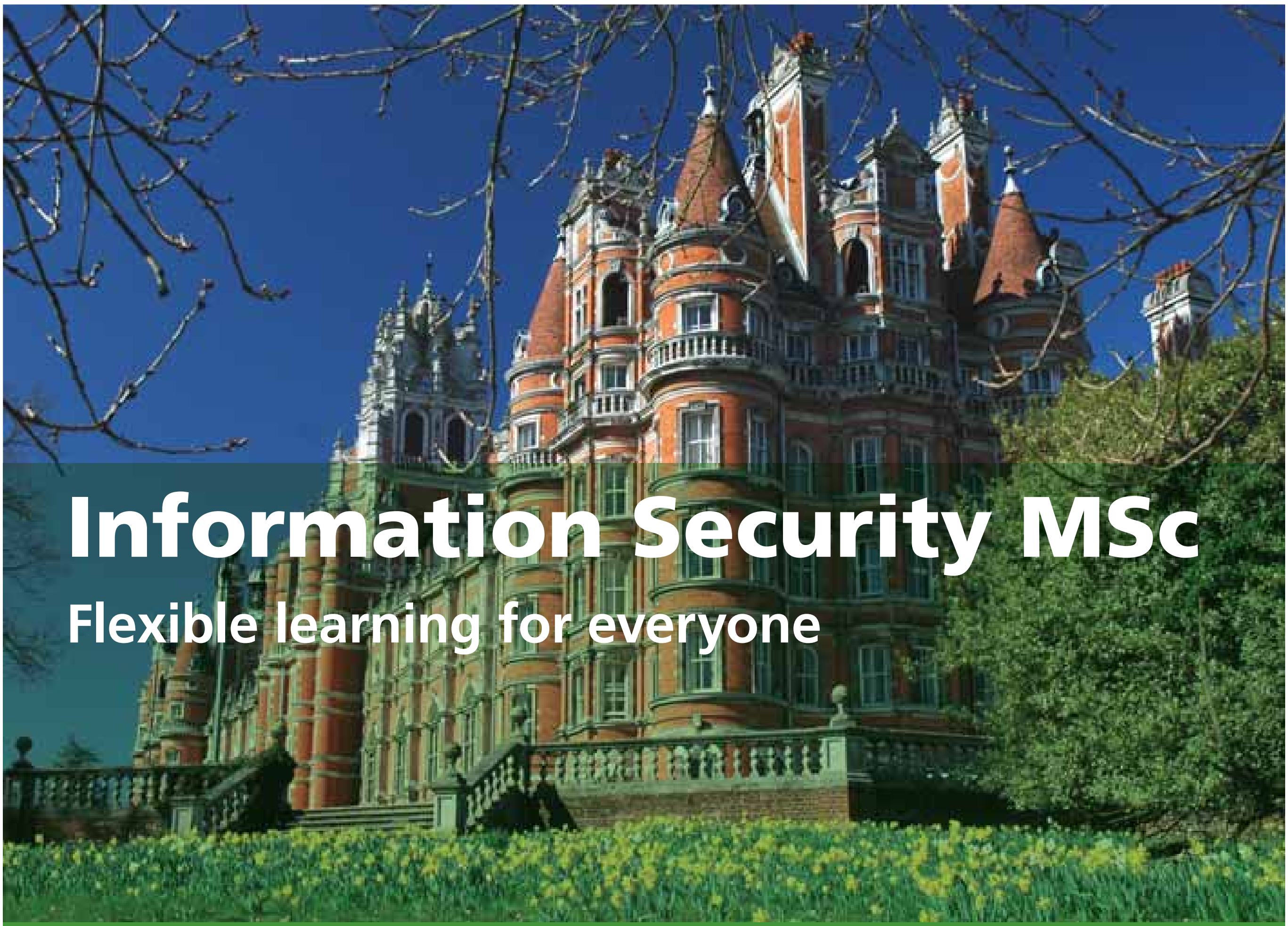
AUTHENTICATION FACTORS

When it comes to restricting access a password is not enough

MOBILE SECURITY

Forget about devices, secure the data instead

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 Great Britain by:
Inter Print, Swindon, Wiltshire.
ISSN 1752-2455. Volume 3, number 4.

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 there are steps every company should take to prevent data leakage.

Data loss prevention should be less about deploying the latest technology that claims unrivalled capabilities in securing all the data you value, rather it should be about having the right data policies, procedures in place, along with suitably educated and motivated people, who can act as your data guardians. The lack of universal technical control will always leave gaps for data to be deliberately exfiltrated or accidently exposed, but without comprehensive and effective data policies and procedures, and the people to support and enforce it, technology cannot provide a solution to your data management ills. It is key that data procedures cover at least, how the organisation assigns a value to its data and information, i.e. values its assets; how it categorises and marks data, in relation to its value or sensitivity and how it assigns rules for handling data throughout its whole lifecycle, especially for personal information. In a recession, the impact of the loss of corporate or customer data can be amplified and leave your organisation more vulnerable to disaster than before. The actual, or suspected, loss of information should be covered by your organisation's incident response or business continuity plan.

People can be shocked and concerned when media-friendly volumes of data are lost or exposed, even though only a tiny proportion may directly relate to or affect them, yet they volunteer personal information to near strangers when using the internet and think very little about the implications of doing so. With their photos, blogs, CVs, social networks, and contributions to online discussions individuals can provide the greatest insight and intrusion into their online and real world lives, and also the lives of their friends and family who may not have consented to their information being shared so openly. Maybe each internet connection should come with a health/wealth warning.

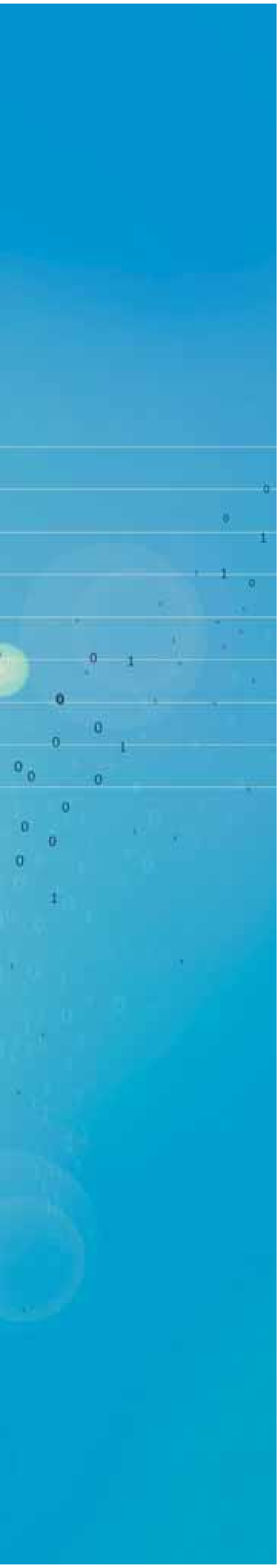
ISNOW | CONTENTS

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**

Securing personal data

On 1 June 2009 BCS, in partnership with ISAF, launched the Personal Data Guardianship Code (www.bcs.org/datacode) as part of an effort to change the culture of organisations towards the handling of personal data. Louise Bennett, Chair of the BCS Security Forum explains.



The Code is intended to help organisations and the people in them who handle personal data understand their individual responsibilities. It promotes best practice and provides common sense guidance for board members and all data handlers. It also explains the rights and responsibilities of the data subject.

The BCS is now asking all members to bring the Code to the attention of the responsible person (that is the senior person who is accountable for the purpose and manner in which personal data is collected, processed, stored and disposed of) in their organisation to see how the Code can assist in improving data guardianship at their place of work.

The BCS would like all members to report back to Liz Long (liz.long@hq.cs.org.uk) about how the Code has helped change attitudes to data guardianship where they work. The next phase of the BCS campaign on this vital topic will be to report back with anecdotes and measured improvements on the ground resulting from the initiative.

Culture shift

We hope that the Code will help change behaviour and cultures. Most specifically we want board members to quiz those responsible for databases with challenges like: ‘Show me the audit trail proving that we have deleted all copies of personal data after twelve months.’

We want ministers and civil servants to think about personal data from the individual citizen’s perspective. We hope they will soon be asking: 'If we link these databases will it help the public or just make our administration easier? This is because one of the great problems is that much of the government’s thinking about e-government has been about how it will improve internal efficiency, not about its responsibilities to its citizens for personal data security and privacy, and the impact on individuals if they fail to look after data properly. We want people to query: ‘will our administration actually be better or cheaper if the data in these linked databases is inaccurate or the linkages are incorrect?’

> **We want every employee to think before they take their laptop home: ‘I have got staff records in my laptop. Would it hurt them if my laptop was stolen?’**

Clean data

We want people to be certain they have asked: ‘have we included what it will cost to clean the data in the project?’ This is because so-called dirty data, that is data which is wrong, inaccurate or out of date, is a major problem, particularly when compounded by data sharing.

We want everyone who inputs data to become aware of the consequences of their errors. For example, a nurse should always be thinking: ‘did she say her postcode was 8HP or 8PH? If I get it wrong the heart attack may go on the wrong record.’

We want every employee to think before they take their laptop home: ‘I have got staff records in my laptop. Would it hurt them if my laptop was stolen?’

Employees should not just be thinking: ‘would losing the data mean I lost my job, or my employer’s reputation took a hammering?’ We want the culture to change so people think twice, and think again before they take personal data on portable devices outside the office.

Finally we want everyone – you, me, our parents, our children to think: ‘I only want to buy a ticket so why do they want to know my ethnic origin, gender, marital status?’

Good reason

If we are not asked for and do not give out personal data without a good reason for the transaction we are involved in we will all be much safer and there will be less to be lost. We all have to remember that personal data disclosed in a face to face conversation is not the same as personal data submitted and recorded electronically, because once data is held electronically it is so easy for it to be used, re-used, shared out of context, copied and abused.

We all have to recognise that in the information age individuals and organisations can leak data that has the potential to do ourselves and others harm. Our electronically held personal data no longer has what academics call ‘practical obscurity’. In the past, practical obscurity existed because of the extreme difficulty of retrieving data when it was kept in dusty archives.

Even when people have been searching for it, like the copies of John Osborne’s early plays, it has been hard to find. Now, eventually, those plays have been found after 60 years in the censor’s archives, even though the author wanted them consigned to the scrapheap.

Once personal data is in the electronic environment it persists, it is not going to go away. We should all limit the volume to the minimum and guard it jealously. Most of us will not want those embarrassing Facebook entries or You Tube clips around after 10, 20, 30 years, but they will be.

The BCS hope that you and your organisations will find the Personal Data Guardianship Code valuable in changing attitudes and in helping to produce a culture where protecting personal data is second nature to us all. Please let us know your experiences using it.

Doubling the authentication factor

In a battle to combat online identity theft, phishing and other online fraud whereby the only defence against attackers is a password, organisations are adding extra layers of security at all levels to protect valuable assets using two-factor authentication. Yurong Lin, CEO of Deepnet Security investigates this added layer of security.

Authentication ensures the person accessing data, whether it be via a virtual private network (VPN) connection, remote desktop, email application (Outlook Web Access, Outlook Anywhere) or an online shopping portal, is who they claim they are and that they are authorised to access the data. Traditional authentication systems include only one level of authentication such as passwords.

Identity theft in the UK costs businesses on average £1.2bn according to research from the Home Office, fuelling the government's decision to push identity cards in a battle against the growing number of online identity crimes. Organisations are faced with a similar problem, whereby uninvited users are able to penetrate security and access corporate data, and of course the age-old problem of users logging on under another person's identity.Two-factor authentication adds stronger security as users need to authenticate themselves with extra credentials in addition to their passwords. Two-factor authentication requires two out of the following three factors: something you know (e.g. password or PIN), something you have (e.g. security token, mobile phone or USB stick), something you are (e.g. fingerprint or iris recognition). However, selecting an appropriate two-factor authentication system can be difficult and expensive, as there are many products on the market that provide different types of technologies. A unified authentication is a single platform that integrates all types of user credentials and authentication methods, enabling organisations to deploy strong authentication across all types of applications, such as remote access, internet access and mobile applications, for all groups of users such as employers, contractors and business partners. A unified authentication system is, therefore, more user-friendly, cost-effective and future-proof. In a bid to tackle card-not-present fraud (CNP), Visa recently announced the availability of the EMUE card, a credit card powered with a LCD display and mini-keypad that generates one-time passwords for account logon and online transaction.

Impact of regulation

Regulation is fuelling the uptake of two-factor authentication, with many organisations using the technology to replace insecure passwords and secure assets in addition to meeting regulatory compliance such as HIPAA, Sarbanes-Oxley and FSA. The most recent regulatory pressure by the government is the Code of Connection (CoCo) standards, which will define the future of communications between local and central government. The regulation requires local authorities to implement rigorous security processes and IT controls, as well as provide secure access to data through multi-factor authentication.

The CoCo deadline has recently been extended to 30 September 2009 and it is apparent that councils are going to face a real threat of ID theft and loss of network connection to central government departments if they don't comply by this date.

Whilst councils are looking for a quick fix to the problem, it is clear that there is a lack of knowledge around the topic, which is holding them back and causing widespread confusion of what is required and who to turn to for a solution.

Achieving CoCo compliance isn't a quick job. There are many different areas, which councils must comply with. Five key areas represent the biggest challenge for councils: securing remote devices, developing secure processes, managing software centrally, managing a cultural change and maintaining ongoing compliance.

For remote devices to be CoCo compliant they must be secure, encrypted and only given access to the network through a secure virtual private network (VPN) using two-factor authentication. The simplest way to achieve this is to provide a unified authentication platform to prohibit unauthorised access to government networks, without the need to increase password complexity. Greater complexity invariably means users forget their passwords, and need to call the IT help desk for a rest, or put them at risk by writing them down.

Authentication approaches

The unified approach

Unified authentication provides a multi-factor authentication service on a single platform, which enables strong authentication for different types of applications and different groups of users, using different types of authentication methods. Organisations can achieve a lower total cost of ownership (TCO) with unified authentication than using a traditional two-factor authentication system.

Hardware tokens

The most common form of the 'something you have authentication' are hardware tokens: dedicated electronic devices that generate one-time passwords.

Software tokens

Similar to hardware tokens, a software token is a new generation of devices that can create a online-time password. Instead of using dedicate, expensive hardware devices, software tokens use the device that users already have, such as mobile phones, computers, and USB sticks.

Virtual tokens

Virtual tokens do not require an additional physical device. Common implementations of virtual tokens employ technologies such as secure cookie, user online profiles and IP locations. Virtual tokens can also refer to technologies that use user's computer devices as the authentication tokens.

Biometric tokens

Users can authenticate via physical biometrics such as fingerprint or iris recognition and enter a PIN or password to gain access to data. However, this type of authentication is only suitable in physical access applications. For online applications, behavioural biometrics such as keystroke dynamics and voice recognition are more appropriate and cost-effective, as they do not require an additional hardware scanner.

Digital certificates

A digital certificate is a PKI solution for enabling the enhanced user identification and access controls. Digital certificates are often stored in computers, but can also be stored on smart cards or USB sticks for use when travelling

Compliance and lowering TCO

Different applications require different levels of security, hence users possessing varied forms of security protection. Achieving the right balance of authentication security without compromising the user experience or the bottom line has always been a challenging task for organisations. Therefore, a single platform with multiple authentication methods can provide peace-of-mind and is also cost-effective, in addition to providing strong protection of assets.

Achieving compliance through two-factor authentication can appear complex and confusing, but organisations must address CoCo head on now by reviewing security processes, so that they are not burying their head in the sand and have enough time to implement any necessary changes before the deadlines arrives.

Further information
www.deepnetsecurity.com

Closing the transfer window

Data is today's business currency: most organisations' success is closely associated with their ability to move, change, manipulate and use data to manage and run their operations. As a result, data is increasingly vulnerable to loss or theft, with accidental and malicious security breaches increasingly common, says Dr Paul Steiner, Managing Director, Accellion.

Organisations can mitigate these kinds of risks by integrating secure, file transfer capabilities as a core business process. In all aspects of business, the transition of data from a physical to digital format has been rapid and widespread. Once organisations exchanged folders, paper and CDs, now they send electronic files online, containing a huge range of information items in various formats. Communication, data, correspondence, images, texts and archives are now digital assets which are created and maintained electronically; making life easier and data transportation faster and more accurate.

Whilst the switch to digital information has improved the speed and efficiency of business communication, it has highlighted concerns about the security of data transfer. The value, confidentiality and importance of data in a digital format is exactly the same as physical data; yet many organisations still don't fully comprehend the need to store and secure digital assets with the same protection given to physical assets. The rise of global corporate networks combined with mobile and remote working has given many more employees access to vast amounts of data which they can view, change and transfer around the world from a PC, laptop or even mobile phone.

Whilst few would argue against the business benefits of such developments, many now view them as a double edged sword: if it's easier to access and transfer data, then it's easier for hackers and unauthorised employees to do the same. There is a growing awareness that many organisations have not invested sufficiently in a robust business process to transfer data securely.

When files go missing

The consequences of inadequately managed file transfer can be severe: over the past 18 months, the UK's Information Commissioners Office (ICO) has highlighted more than 275 data breaches across different markets. The most high profile case was undoubtedly the government's loss of CDs containing personal information on 25 million recipients of Child Benefit. Similarly, the Ministry of Defence lost a laptop containing 600,000 records of UK residents interested in joining the armed forces, whilst Virgin Media and Marks & Spencer were ordered to encrypt portable mobile devices and laptops following serious data security breaches.

UK regulation is also driving organisations to look closely at transferring data more securely. The

Financial Services Authority's (FSA) can now fine organisations that fail to manage client data securely. Since 2007, several high-profile financial institutions have been fined, notably Norwich Union whose failure to manage customer data adequately resulted in a £1.26 million penalty. Local authorities and their partners must now adhere to Code of Connection (CoCo) Compliance. This outlines the security controls that must be in place before they can connect to the government's national communications infrastructure. Retailing is increasingly governed by the Payment Card Industry's (PCI) Data Security Standards (DSS) which sets out the degree of data security required from card issuers and handlers and how they should use, process, transfer and store data.

Additionally, whilst UK companies are not directly subject to US regulations such as Sarbanes-Oxley, the Securities & Exchange Act (SEC), Health Insurance Portability and Accountability Act (HIPAA) and Food & Drug Administration (FDA) laws, the legislations' emphasis on accountability, audit, control and care of data, has made many UK organisations reassess their digital asset management.

The new challenge

Whilst email has become the de facto standard for digital communication, it has some significant disadvantages when transferring files, particularly large ones. Initially, email was designed as electronic mail, not as a means of transferring large amounts of data around networks or across the internet. As a result, servers became overloaded and there is an adverse affect on the performance of messaging systems.

To address this and speed the movement of large files, many organisations have deployed FTP servers. But, FTP was designed when the security was much less of a concern. As a result, the same username and password is often shared among multiple users, representing a potential and significant security breach. Additionally, simple FTP cannot provide audit trails which meet today's compliance and audit legislation. Enhanced FTP systems (such as SFTP, FTPS and EFTP) offer genuine improvements over conventional FTP, but need specialist programs installed on users' desktops; adding overheads for IT departments and inconvenience for users.

Data management over FTP can also be problematic: once files are uploaded into FTP directories they need to be deleted manually, so they are rarely removed. The result is a set of directories containing hundreds of files, with little information about when they should be deleted. This creates a valuable digital asset which is left unprotected for extended periods and is accessed easily by unauthorised users.

A new business process

Traditional solutions like FTP and email now struggle as adequate business tools for secure and large file transfers. But this doesn't become apparent until some something goes wrong and security is compromised. With data confidentiality such an important issue, organisations need to consider a dedicated solution which offers embedded security. Data encryption is essential, and systems should be capable of authenticating the recipient and managing each file and account lifecycle automatically. This would mean that no confidential information is left exposed and no unauthorised user access takes place.

Technologies that manage file transfer have emerged to meet the need for on-demand and automated, multi-office enterprise, secure file transfer. These robust systems send and receive data securely with folders up to 50GB. Highly secure, these solutions fully encrypt all files and control access to each document, eliminating the risk of data breaches.

The resulting audit trails meet the security and compliance standards of Sarbanes-Oxley and most other regulatory requirements. Extremely easy to use, they can be installed in next to no time and have minimal impact on IT resources. From their desktops, users are often unaware of the deployment, beyond a small email type icon.

For instance, many users in different sectors have benefitted from these solutions' speed and simplicity. Construction companies have found it ideal for transferring large files containing blue prints and building specifications. TV production companies have found that such solutions have allowed them to transfer large video files between staff, production studios and international broadcasters quickly and easily. As well as cutting production times, the solution also safeguard the secrecy of new episodes of TV programmes. Many organisations including advertising agencies, law firms, universities, insurance brokers and medical research have similarly implemented such solutions to transfer files faster and more securely.

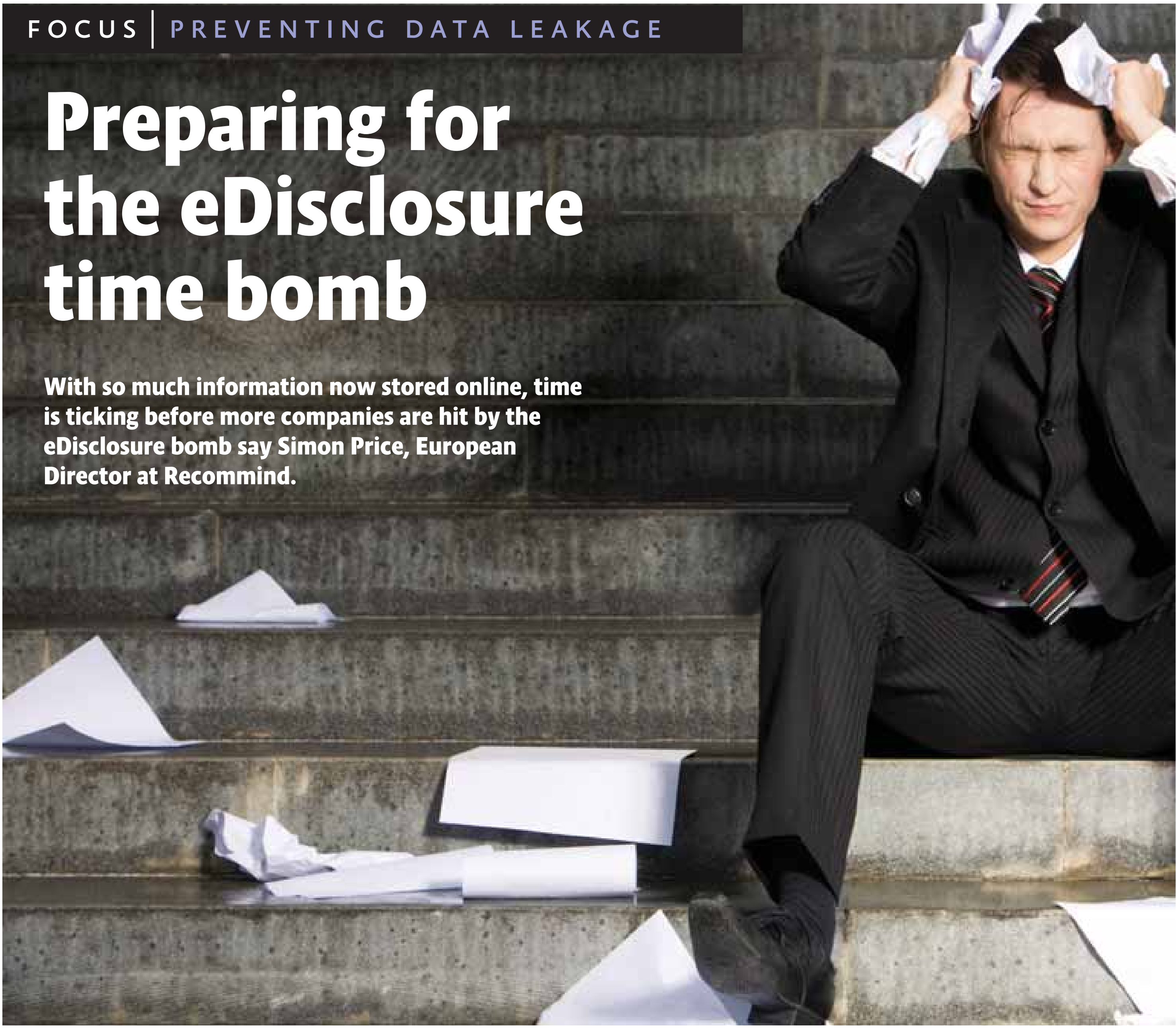
Important but hidden

As organisations become more reliant on information for their success, so their ability to move data securely and effectively from one location to another becomes paramount. Managed secure file transfer solutions allow organisations to achieve this in a cost effective and unobtrusive way. As such, secure file transfer will become a core business process used by world-leading organisations to run, maintain and manage their operations.

Further information
www.accellion.com

Preparing for the eDisclosure time bomb

With so much information now stored online, time is ticking before more companies are hit by the eDisclosure bomb say Simon Price, European Director at Recommind.



As businesses communicate and share information in more ways than ever before, whether by email, instant messaging (IM), blogging, and social networks such as Twitter, Facebook and LinkedIn, the amount of electronically stored information (ESI) is skyrocketing to record highs. While storing this information is always a concern, securing and making the information searchable is now the more challenging issue. This is becoming even more of a concern as the regulatory and legislative environments become more stringent, giving rise to an increase in requests for the production of ESI in response to regulatory inquiry, internal investigations or litigation, which are collectively referred to as eDisclosure requests.

There has been a significant backlash against the lax regulatory environment of the past few years, most recently marked by the record-breaking 1.06bn Euro (£950m) fine handed to Intel by the European Commission for anti-competitive practices. With the continuing tough economic conditions and even more regulation on its way, eDisclosure related investigations, prosecutions and fines are likely to become more common. While US organisations have always been subject to greater scrutiny and are therefore more familiar with the concept of eDisclosure (called eDiscovery in the US) and the challenges it can present, UK businesses are not ready to deal with this increase.

However, eDisclosure is a global issue and companies around the world need to be prepared. In the UK, almost 50 per cent of companies have experienced an increase in eDisclosure requests compared to last year, but IT directors still do not fully grasp its importance, rating it as their lowest priority below information security, email archiving and rolling out productivity-related tools. In line with this, more than two thirds of these organisations dedicate less than five per cent of their IT budget to provisioning and preparing for eDisclosure.

Fundamental for compliance

In fact, eDisclosure should not be viewed as an option but should rather be fundamental to a company's entire information management, compliance and risk mitigation programmes. The risk of damage to a business from compliance lapses and failure to meet disclosure demands is on a similar scale to, if not

greater than, that of IT security challenges such as data privacy breaches. An oversight could have severe repercussions and leave businesses highly vulnerable to the consequences associated with information risk - including breach of compliance, reputational damage, and loss of stakeholder and customer/client confidence - all of which have the potential to cripple a company.

Managing the wealth of data

To combat this, companies need to take a proactive approach. If not, responding to an investigation will be an expensive and extremely time-consuming endeavour due to the sheer volume of ESI that needs to be identified, collected, reviewed and analysed. To put this in context, regulatory inquiries often result in the production of more than one terabyte of data (the equivalent of 75 million pages) and the costs involved with review can therefore exceed the amount at issue if a company is not prepared.

Companies are also often required to respond within a day due to the regulator's demands, but also to try and negate the internal risk of data destruction and alteration. In addition, any oversights can incur severe sanctions and even bigger bills. For example, the US Office of Federal Housing Oversight responded to a third party subpoena related to the case of Fannie Mae and Freddie Mac, and in the process incurred USD $6M in electronic discovery expenses which equated to nine per cent of the agency's entire annual budget.

To avoid this risk, companies should invest in solutions that can automatically categorise, index, access, preserve, delete and collect relevant ESI in any form.

Since these challenges are similar to those presented by email and knowledge management, the use of sophisticated search technologies which enable organisations to effectively and securely manage all of their data can help achieve similar results in risk management.

For example, when a discovery demand is filed, concept search greatly increases the efficiency of any review as it will locate all information related to a pre-defined issue, rather than relying on inefficient keyword search that would either miss relevant data and/or bring up a sea of clearly irrelevant documents containing a particular search term.

The effective management of this wealth of ESI will not only automate the eDisclosure process and improve a company's ability to respond to eDisclosure demands, but it will also allow companies to improve productivity and efficiency by providing staff with access to all the information they need for their daily jobs. This is particularly key in the current financial climate where less staff are being stretched to fulfil more roles as processes are streamlined. Despite this, most UK organisations are using out-dated, legacy search and data management tools which do not meet the sophisticated information needs of the staff and are not capable of searching data in different formats and from diverse locations. The result is that staff waste valuable time trying to locate the documents and information they need. In fact, a quarter of UK businesses admit that their employees typically spend more than half a day a week on this task. For a company with 1,000 employees, this equates to upwards of £50,000 worth of lost time a week or £2,600,000 a year.

The role of security in search

Many companies are concerned that by providing staff with access to all the information they may require they will inadvertently open up Pandora's Box and risk sensitive information being compromised.

However, search solutions do not need to come at the expense of the security of the information. Effective search can actually reduce this risk by providing information to employees based on their roles. By implementing strict policies such as these to safeguard information, businesses can ensure that confidential data is only accessible by those who are authorised to access it.

Through the tagging and categorisation of information, it is possible to carefully define what information can be searched and by whom. This will help organisations remain compliant with data regulations, and will also make it much easier and quicker to collate the relevant information when an eDisclosure demand is received.

Not only can effective search solutions help organisations prepare for eDisclosure and secure their data by enforcing authorisation policies, it can also help monitor illegal financial activity - cited by IT directors as the main reason for the recent increase in eDisclosure requests. By providing an audit trail for employee actions, it can enable organisations to trace illegal financial activity and irregularities. The explosion of ESI volumes, types and sources has made it more difficult to effectively control and protect information, making it harder for businesses to deal with eDisclosure requests. Companies need to provision for the new regulatory environment, which is proving to be intolerant of those organisations that cannot effectively identify data that is requested and produce it promptly.

By incorporating sophisticated search and eDisclosure technologies into a company's IT security strategy, businesses can effectively avoid the costly and severe repercussions of unmanageable eDisclosure requests when they hit.

Further information
www.recommind.com

The data loss cocktail - anytime, anywhere

With mobile computing advancing at a pace the focus has generally been on securing the devices. Nick Garlick, Managing Director, Nebulas Solutions Group, says that this is wrong and companies should focus on securing the data instead.

The growth rate of mobile computing, underpinned by the proliferation of smart phones, BlackBerrys, public Wi-Fi hot spots and high speed internet access in homes, shows no signs of abating. Many enterprises have simply replaced desktop PCs with laptops, and USB flash drives are now standard for transferring large amounts of data such as presentations.

The rapid advancement of mobile technology has collided with the rise of cloud computing, web 2.0 and now mobile 2.0 to produce a fundamental change in computing and working practices. Most of these changes have been to the benefit of employers as well as their employees and customers – improved customer response times being one example.

However, the very thing which has made web and mobile 2.0 so compelling has also proved to be their Achilles heel. Many employees have been seduced by the informality of a social networking site or chat room into revealing corporate or personal data that should have stayed firmly under wraps. Furthermore, the exploitation of the trust of the user – trust which is crucial for the functioning of social networks, blogs and micro blogs like Twitter (frequently accessed from mobile devices) has enabled hackers to pull off raids such as the SQL injection attacks that hit many organisations throughout 2008.

Headache inducing cocktail

This cocktail of criminals, unwitting employees and data accessible from any device, anywhere at any time of day has given many CIOs a major headache. Aggravating the problem is the fact that as the amount of data and devices have mushroomed, so have government and industry regulations relating to data control. Sarbanes Oxley, Basel II, and the Payment Card Industry Data Security Standard (PCI DSS) are just some of the regulations that businesses (depending on the nature of their business) have to demonstrate compliance with. However, despite the increasing stringency of this regulatory framework, the high profile data breaches just keep on coming.

In late 2007, HM Revenue and Customs lost the details of 25 million child benefit claimants in the post. In January of this year, a private company contracted to the Home Office lost a USB drive containing the names, addresses and release dates of 84,000 prisoners. In May, four separate NHS trusts were found in breach of the Data Protection Act 1988 by the Information Commissioner's Office. In one of these cases, the lost USB stick was encrypted, but the user had attached a post-it note to the drive containing the password details.

In the corporate world, the picture is little better. In 2007, it was revealed that over an 18-month period, criminals had stolen the debit card data of over 45 million customers of TJX, owners of the discount retailer TK Maxx. Other high profile organisations such as HSBC and Ernst & Young have also lost drives or laptops containing confidential customer information.

So why, despite the risk of public censure and the knowledge that their brand and credibility could be seriously and permanently affected, do organisations continue to lose data?

Many security specialists believe that the answer lies in the approach that organisations take to data security. Many organisations make the mistake of focusing on the device rather than the data. The scenario often found in public and private sector, is that hardware may be managed by one individual and security by another. Given the extensive and complicated nature of these challenges, it may be time to modify this approach.

Company-wide policy

The first step to a data focused approach is to formulate a company-wide policy on data security, perhaps as a part of an acceptable use policy (AUP). The stringency of the policy will vary according to the organisation but Nebulas Solutions believes that policy should not be so draconian that users' immediate reaction is to try and circumvent it.

A policy to regulate the number of different devices used within an organisation seems sensible. A move to ban all use of USB sticks does not. All employees should sign up this policy, which should be regularly reviewed and updated and be easily accessible to staff. Pinning a copy in the kitchen and leaving it untouched for three years simply won't suffice.

The drawing up and communication of an internet acceptable use policy is pointless, unless it is also enforced. There are a variety of tools available for the enforcement of data security. The first is encryption. Relying on passwords to protect the data held on mobile devices is not a sufficiently robust approach. Drives can be removed and placed in another system and the data easily read. Implementing mobile device encryption tools to protect data at rest and in motion on laptops and other mobile devices should be a fundamental part of the enforcement process. Disk encryption and encryption for data being shared between users for most mobile devices is available from a variety of vendors including PGP, McAfee and Check Point. Encryption is a very useful weapon in the data security war but it isn't a silver bullet, at least not in its present state. Security researchers have found ways around disk encryption including a cold-boot attack which was showcased at the Usenix Security Conference in July 2008. Whilst a cold-boot attack requires physical access to a machine it allows the attacker to copy the RAM contents including encryption keys. This is possible because RAM data fades gradually after power is cut and this process takes anything from a few seconds to a few minutes. This period can be extended by keeping the chip physically cool, giving an attacker plenty of time to read the contents.

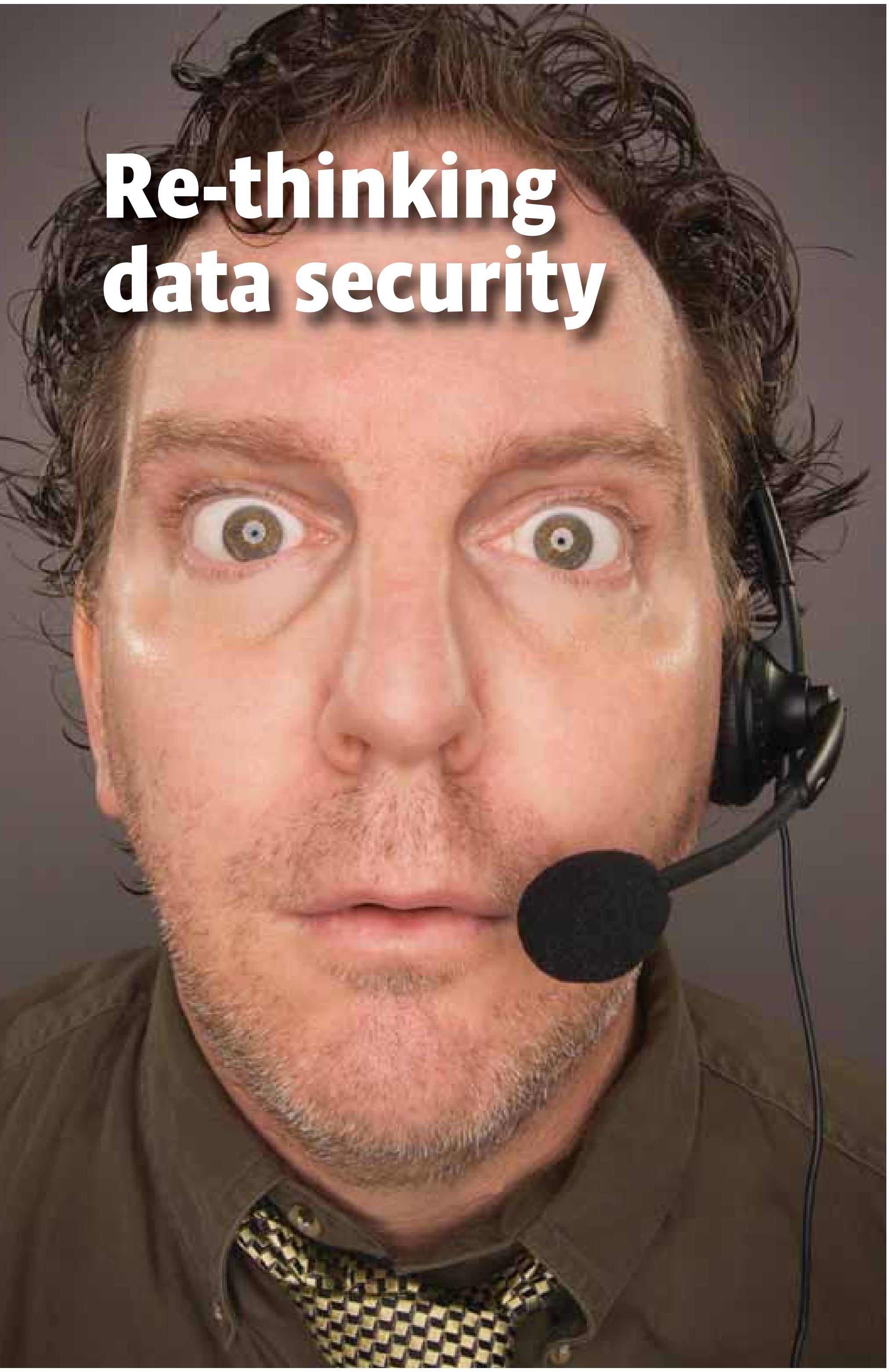
Cold boot

The cold-boot attack brings into sharp focus the fact that the most sensible option for mobile data security enforcement is simply to not allow data to reside on personal devices at all. Most users would struggle to come up with adequate reasons why the majority of information on their laptop or PDA shouldn't be stored on a central server – backed-up and secure. In reality, such a stringent policy is unlikely to win favour with employees, so companies should make sure that data leak prevention (DLP) forms a key part of any data security policy enforcement.

DLP allows organisations to see exactly where key, confidential information is stored, how it is used, and they can both monitor and prevent data from leaving the network boundary. Policies can be set which prevent confidential files being copied or downloaded to local drives, USBs, DVDs or other media devices. A DLP solution will also play a part in the education process by displaying on-screen messages to users about the need to protect such important data.

Organisations considering their mobile security need to develop a clear strategy which focuses on safeguarding the data, rather than the multiple devices where it's stored, transferred and used. Implementing a three-prong strategy based on policy, education and enforcement will significantly reduce the likelihood of any organisation becoming another casualty of data loss.

Further information
www.nebulassolutions.com



Re-thinking data security

Over the last 12 months, the UK media has been awash with stories of security breaches, whether they are accidental such as lost memory sticks or are perpetrated with more malicious intent. As a result, IT departments are coming under increasing pressure to safeguard the protection of data that could be misused if it fell into the wrong hands, reports Brett Feldon, General Manager EMEA at VeCommerce.

Unfortunately fraud is an escalating problem and according to the latest figures from the UK's fraud prevention service CIFAS cases are up by 15 per cent. There have also been suggestions that in a downturn this is likely to get worse as economic pressures increase.

Not only can such incidents cause embarrassment and damage to your brand, they can also result in substantial financial losses if the data is exploited. To put it into perspective, on the black market, for example, credit card numbers sell for between 7p and £17, and, with the average limit on cards at around £2,800, this represents a highly lucrative business for organised crime. But it isn't just credit card details that need to be protected, passwords, PINs and other personal details can be manipulated for financial gain. So what are the challenges for protecting sensitive data and what loopholes exist that can result in potential leaks?

Understanding the impact that data breaches can have is well documented in the press, but finding methods to minimise them is more tricky. The inherent problem is society's huge reliance on passwords and PINs, whether it's to access information on a computer network, the ability to identify yourself on the phone or to make online transactions. The critical flaw in this thinking is that when personal data is acquired through non-legitimate means it's like giving a fraudster an open cheque book. With the rise of the internet the situation has been exacerbated because many financial transactions are carried out remotely and it's easier for someone's identity to be impersonated using personal details.

For those that manage data security it is of course possible to encrypt information, restrict access to certain personnel and ensure that your network is protected against hackers, viruses and even terrorist threats, but what about when the threat is closer to home? Insider fraud is growing and concepts such as social engineering whereby staff extract information from those that don't appreciate the value of the knowledge they are giving away are becoming more common. The UK's largest data theft so far online when job hunting site Monster, became victim to hackers managing to gain access to the personal details of four and half million people registered on monster.co.uk – is an example of where social engineering could make the impact of a breach even more serious. Although the stolen information didn't include social security numbers or financial data, it did contain user IDs, passwords, email address and so on, all of which could easily be used by fraudsters to trick individuals into revealing more data.

Vulnerable areas

There are certain parts of an operation where it is more difficult to restrict access to personal information and these become soft targets for would be fraudsters. Take for example any organisation that runs a contact centre and is in daily contact with customers. How many times have you parted with highly confidential information over the phone if you want to prove your identity or want to make a purchase using a credit card? The irony is that most of us don't think twice about imparting this kind of information but would be horrified if we mislaid our credit card – but are the two really any different? In fact the former should be more worrying because not only do they have your credit card details they also have all the information they need such as registered name and address to go on a spending spree. Contact centre workers are privy to confidential information that is given to them. There is also the possibility they could download sensitive information using techniques such as iPod slurping or with the use of other devices such as memory sticks. There is already evidence that these type of workers, some of which are casual staff, are also being planted by criminal gangs or are bribed into giving up customer data.

Stripping the power of sensitive data

But imagine what would happen if the contact centre insisted on a form of identification that could not be stolen, replicated or borrowed? Could reducing the dependence on personal information be the key to beating fraud by making personal information almost redundant and therefore worthless to thieves? Voice biometrics is a technology that is promising to change the attitudes towards how we identify people. In a contact centre environment, for example, replacing personal information with a individual's voice to verify their identity would strip the power of sensitive data and remove one of the most powerful weapons in a criminal's arsenal.

The beauty of this approach is that is also improves convenience for the customer. They don't have to remember passwords/PINs and they can carry their method of identification wherever they go without the risk of it being stolen.

For those that manage data security it is of course possible to encrypt information, restrict access to certain personnel

Voice biometrics?

The deployment of voice biometrics is relatively straightforward. Firstly a customer needs to enrol onto the system to register their voice print. This is surprisingly simple given the level of technology involved, and on average it takes less than two minutes for an individual user to enrol their voice, based on a specific text such as name and account number. The system then measures many aspects of the user's voice, such as the shape of the vocal tract, and stores this voice print in a secure manner. The next time they call in they can simply say their details: if their voice matches the voice print stored on file, then the person is given the authorisation to access an account, transfer money and so on. This whole operation takes less than 30 seconds and the agent taking the call has no knowledge of the caller's private information, therefore eliminating a further security risk associated with call centre operatives.

The way voiceprints are stored is also significant. While there is no feasible means of reverse engineering a voiceprint, careful implementation of the voiceprint storage system is required to address data security concerns. The specific issues differ from organisation to organisation, but typically include items such as rendering the voiceprint data anonymous, encryption of database tables and communications, and the physical security of the system.

Removing temptation

Changing the method by which people are identified on the phone also means that the exposure of personal data to contact centre staff becomes less frequent. The data is no longer required as a matter of course inside that contact centre, and so access can be restricted to a small, trusted and vetted set of personnel. This further limits the possibility of data from one contact centre being used to attack a different organisation that uses similar information to verify identity. So whereas normally a large proportion of employees might have access to personal details held on a CRM database available on the corporate network, with the introduction of voice biometrics, access to the system that stores the voiceprints would be limited to a much smaller set of staff who need such information. One of the first industries to take an interest in the technology is banking, where many institutions are currently evaluating how they can use it to protect both their customers and themselves from the ramifications of data theft. Of course, the financial services sector is also being pushed by the threats of hefty fines such as the one imposed by the FSA last year on BNP Paribas Private Bank which was penalised £350,000 for weaknesses in systems and controls that enabled an employee to transfer £14m out of clients' accounts.

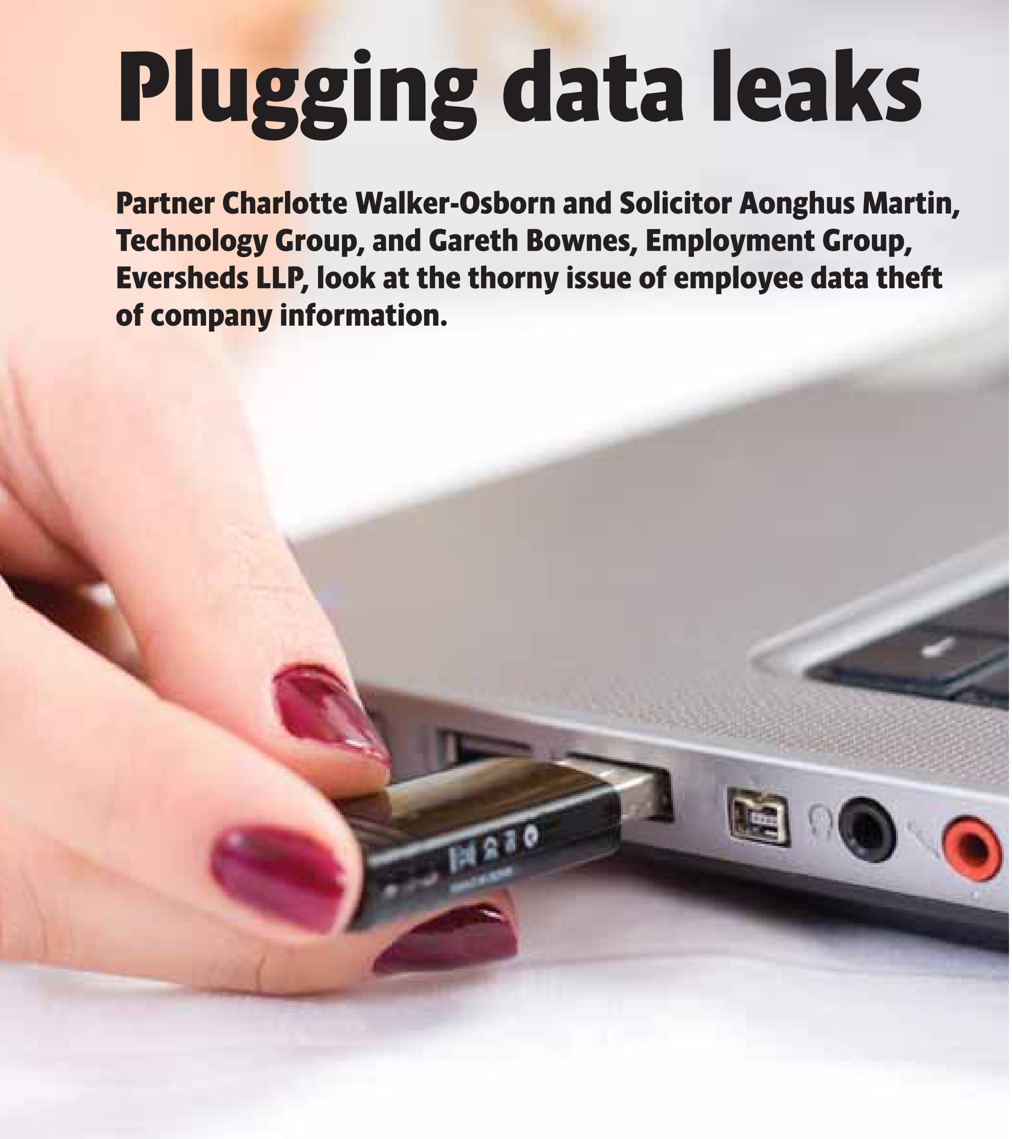
But it isn't just banks that should be considering this technology. Any organisation that maintains large customer databases that retain confidential information can benefit. In the last month we witnessed the largest increase in the UK, with recruitment site Monster.com and, in the, US Heartland Security suggesting the problem is getting worse not better. In the past there have been concerns over the viability of such a technology, but with over a decade in development it is now proving itself in the commercial world.

In other parts of the globe, Australia in particular, it is being embraced by a large percentage of the population who view it as a more convenient and safer means of identification which can prevent fraud. With this shifting mindset voice biometrics represents a new way forward in security. Not only does it reduce crime but it also makes the data held on networks less attractive. The implications of introducing such a technology will certainly make life easier for the IT department.

For more information
www.vecommerce.com

Plugging data leaks

Partner Charlotte Walker-Osborn and Solicitor Aonghus Martin, Technology Group, and Gareth Bownes, Employment Group, Eversheds LLP, look at the thorny issue of employee data theft of company information.



The widespread use of portable storage devices and networking websites has made it easier for employees to remove confidential or copyright protected company data. This removal has been exacerbated by the current economic climate. Below are some steps that employers should consider taking in order to reduce the risks of such data leakage:

- strictly prohibit the downloading of data, other than for legitimate business reasons, as stated in the IT policy;
- restrict access to sensitive data to a need to know basis, e.g. with password protection or tiered-access to sensitive data;
- consider whether ports for portable storage devices should be disabled (if pragmatic);
- review and seek legal advice on restrictive covenants in employment contracts to ensure that they are adequate and enforceable.

If an employer believes that an existing employee has committed a serious breach of its IT or employment policy, it should conduct a full investigation before taking disciplinary action, even if there has been an obvious breach. This will reduce the risk of an unfair dismissal claim, as the employer needs to show that it had a genuine belief in the employee's guilt; has carried out a reasonable investigation and that the dismissal was 'within the band of reasonable responses'. The (IT) policies must clearly cover the alleged misuse; have been properly communicated to employees; and have been applied in a consistent manner.

If an employer discovers that sensitive data has been downloaded by a former employee, it should look to obtain and preserve as much evidence as legally possible and, where necessary, engage forensic technology experts.

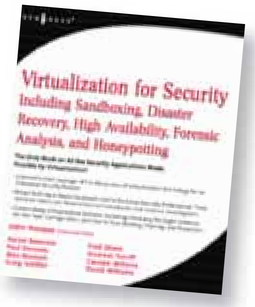
In terms of legal redress, there is no offence clearly aimed to cover only this type of employee breach. An employee who has inappropriately accessed or copied company information could be considered to have gained unauthorised access under Section 1 Computer Misuse Act 1990 depending on strict criteria having been met. If the data accessed by the employee is considered 'personal data' under the Data Protection Act 1998 (DPA) then the DPA will apply. Section 55 of the DPA, for example, makes it a criminal offence to disclose, obtain or procure the disclosure of personal information knowingly or recklessly without the consent of the date controller.

However, redress is usually sought through the civil courts, e.g. injunctions for breach of confidence to deliver up and prevent the use of confidential information or copyrighted information. Unless a search and seizure order is used to seize media containing confidential information/ copyrighted information then contact should be made with the former employee to seek an undertaking to deliver up and prevent the use of such information. If that is unsuccessful then you may need to apply for a court injunction, which can be expensive. The company may also have a claim for damages if it can prove that it has suffered loss, for example if the employee has diverted business from the company. Additionally, the former employee may be in breach of restrictive covenants in their employment contract. Having tightly drafted restrictive covenants, intellectual property and confidentiality provisions in the employment contract will make it much easier to obtain the requisite injunctions and restraining orders. Pragmatically, however, whether that former employee have monies to pay for any damages is another matter. In this way, prevention is clearly better than cure.

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

BOOK REVIEWS

Virtualization for Security: Including Sandboxing, Disaster recovery, High Availability, Forensic Analysis, and Honeypotting



John Hoopes

Syngress Press

ISBN: 13:978-1-59749-305-5

£29.99

Rating: 8/10

The aim of the book is to guide readers through the journey of using virtualisation for common everyday business issues, and how virtualisation can benefit and enhance the business operations economically, and practically.

Each contributing author in their own right is an 'expert' in their respective field, with John Hoopes acting as the overall technical editor. The book guides the reader through, for example, what is virtualisation, through to tasks such as building a honeypot, configuring a virtual machine, forensics etc. At the end of each chapter the book provides a brief summary of what the chapter contains with the key points, a solution fast track, and FAQs. These provide useful reference points for time pressed individuals. The book does provide a very good introduction, and all the essentials required for the set up, management, running and maintenance of a virtual machine, backed up with further references from the web for the reader requiring additional information. The book is also supplied with a unique electronic access code for the e-book version of the book, downloadable at no extra charge.

If you are after an in-depth technical reference book, then this is not for you. You need to be aware, that no formal standards in relation to virtualisation presently exist, and if you are operating at different security levels, then virtualisation in itself present its own issues in relation to security separation.

Adam Gostling MBCS CITP

Managing the Human Factor in Information Security: How to Win Over Staff and Influence Business Managers

David Lacey

Wiley

ISBN: 978-0-470-72199-5

£29.99

Rating: 8/10

David Lacey uses the first chapter of his book to set in context the human aspects of security. He does this through consideration of the impact of networks on the security of the enterprise and the problems that could arise following the emergence of social networking.

He continues by covering in detail the various security roles required in an organisation, together with the likely beliefs and opinions of stakeholders and others, regarding the security of information.

He devotes the next three chapters to the human weakness aspect together with an examination of major incidents, how they are managed and what can be learned from them.

This is followed by an examination of risk assessment and management and how this can play a large part in an effective information security strategy.

He then considers how to change people's attitudes and behaviour to security in the organisation and the related psychological factors before advising on the design of persistent and effective security management programs.

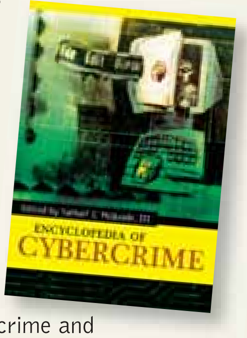
I found the book to be a well-written, varied and informative treatment of the subject. It has the potential to appeal to a wide range of business and technical readers alike.

I found the summary section at the end of each chapter particularly useful in reinforcing the main theme of each topic. I believe the book is only let down by Lacey's inadequate cross-referencing in the text to his sources of information.

Jim McGhie CEng MBCS CITP

Book of the month

Encyclopedia of Cybercrime



Samuel C. McQuade

Greenwood Press

ISBN: 978-0-313-33974-5

£41.95

Rating: 8/10

This book serves as a useful, concise and topical resource on cybercrime and related topics. In all there are just over 80 articles written by several authors, each summarised into about two pages, with references for suggested further reading. Topics included relate to terminology and definitions; types of attacks; computer abusers and cybercriminals; the underpinnings of cybercrime, social and economic impacts of cybercrime and many more.

The articles are concise, have been well written using non-technical terms and are, therefore, very easy to read.

Many articles include real cybercrime cases and names of notorious cybercriminals. Coverage is pretty complete, and include big names such as the Melissa and I love you worms, slammer and code red.

Further reference information is provided in the book, such as a chronology of selected cybercrime related events, further reading, relevant films and documentaries.

The only downside, as you would expect from a book authored in the US, is that it makes significant references to legislation, institutions and enforcement agencies in the US, includings US case studies justifying the need for legislation and agencies. This makes it difficult to relate to equivalent, if any, UK and European legislation and organisations.

Overall this is a well written and an easy to read book. It uses non-technical terms, making the book accessible to a broad spectrum of readers.

Mehmet Hurer MBCS CITP CEng

Governance is key

The key to the problem of data leakage can be laid squarely at the door of poor information security governance. As information security governance is a sub-set of IT governance, then the starting and finishing position rests with the CIO, says John Mitchell.

I am constantly amazed at CIOs who have no clear governance programme in place to ensure that their function can not only support current business objectives, but also help to extend the enterprise into the future. After all, IT departments only do two things: facilitate the development of new business solutions and deliver existing solutions to its clients.

In order to do these it must have a suitable organisational structure, excellent staff who are managed by appropriate policies, standards and procedures and a relevant way of measuring performance. So IT governance is all about putting a framework in place which enables the management of IT to meet business objectives with suitable success metrics.

Rather than reinvent the wheel each time it makes sense to pick up best practice from throughout the world and this is where the International Standards Organisation (ISO) comes in. As IT only do two things and as the way they deliver these things is pretty much the same regardless of language, culture, or technological maturity it seems an ideal candidate for a number of ISO standards.

There are now national and international standards for IT governance, software development, service delivery, information security and business continuity. Indeed the whole of IT is now covered by just five standards. The standards themselves have a standard format: part 1 is the code of practice and part 2 provides guidance on the implementation of part 1. All the standards require some sort of policy statement and as a policy is simply a statement of intent these should be concise and to the point. For example, there are only two possible security policies and as they are mutually exclusive your company can only adopt one of them.

The first states that everything is open to everyone unless specifically restricted, while the second states that everything is locked down unless specifically derestricted. The implementation of either of these policies then requires the adoption of appropriate standards and procedures requiring the identification of assets which are either to be restricted, or opened up and the allocation of appropriate privileges to the people.

Apart from the official standards there are a host of good practice out there which have been identified by ISACA – **www.isaca.org** and the IT Governance Institute (ITGI). These two organisations use a common umbrella open standard titled Control Objectives for IT (CobiT) which sits above the international and national standards and provides examples of good practice and measurement frameworks to enable organisations to implement good IT governance in an economical way.

As an assurance professional (auditor) I tend to use a fairly simple process to gauge the governance maturity of any IT function. This is based around the maturity model concept which was initially developed by the Software engineering Institute of Carnegie Mellon university and extended by ISACA to cover the major IT processes. Basically you can take any process and measure it on a scale of 0 through 5.

0 Nothing in place to manage the process
1 Initial consideration is given to process management
2 The process is repeatable, but depends on individuals for its success
3 The process is defined and documented
4 The process is managed and measurable
5 Yhe IT process is integrated with the business process.

You will notice that full compliance with any of the standards forces the IT function to level 4 as, not only is the process defined, but it is also measurable because all the standards require the collection and analysis of metrics to prove compliance. Some standards, ISO 27000 (information security) and ISO 20000 (service delivery) move the IT function to level 5 by integrating the IT processes with the business processes. ISACA has defined 34 common processes used by IT departments and provides a maturity scale definition for each one. This enables me, with IT and the business, to assess the function's maturity in the key areas.

It's then up to the business to decide whether they are satisfied with their current level, or would like to improve on it. ISACA also provides an anonymous benchmarking service. I was a bit shocked to find that the average for Information security was 2.8, which is below defined process. Worrying, isn't it?

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