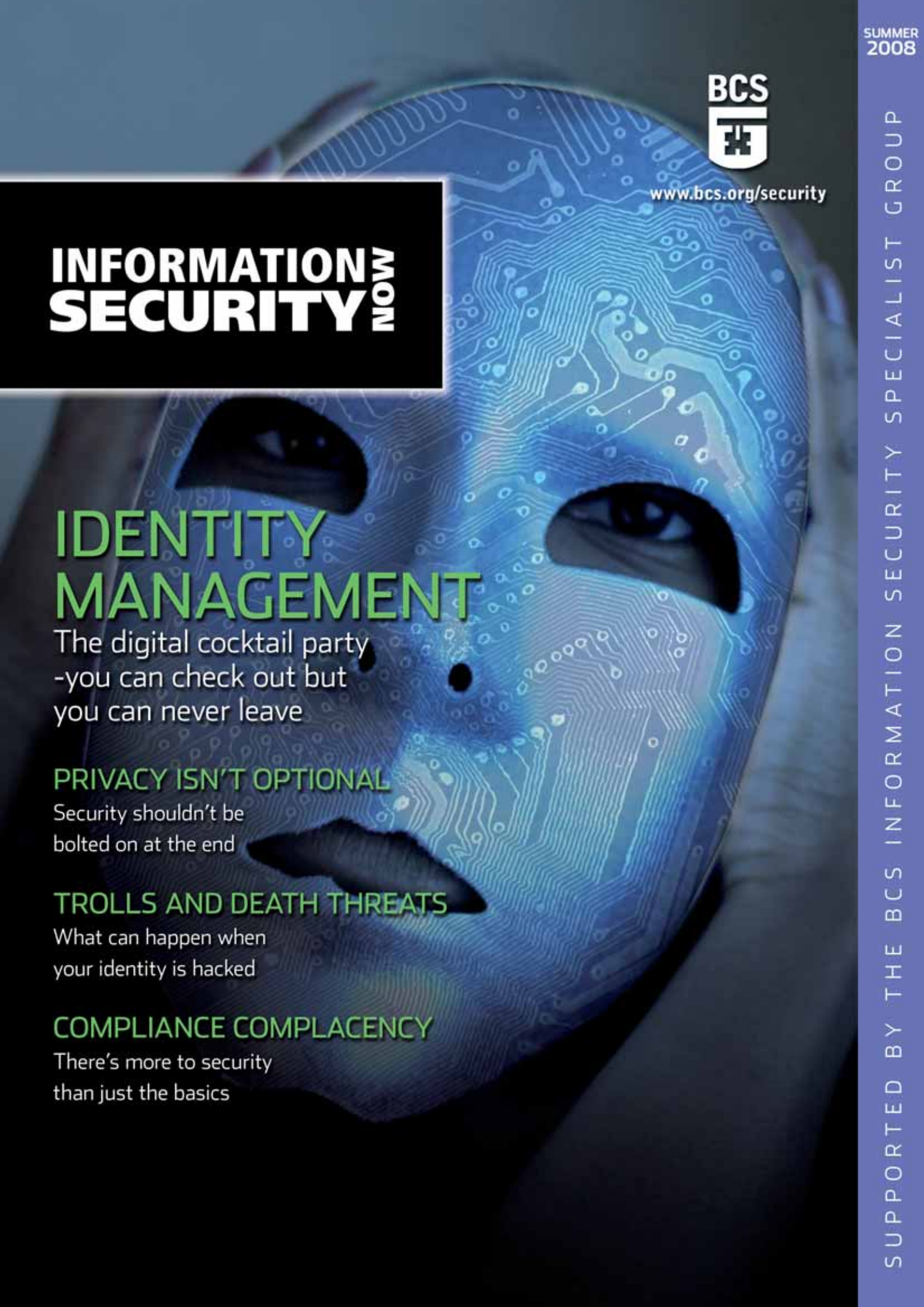


SUMMER 2008

BCS

www.bcs.org/security

INFORMATION SECURITY NOW

IDENTITY MANAGEMENT

The digital cocktail party -you can check out but you can never leave

PRIVACY ISN'T OPTIONAL

Security shouldn't be bolted on at the end

TROLLS AND DEATH THREATS

What can happen when your identity is hacked

COMPLIANCE COMPLACENCY

There's more to security than just the basics

SUPPORTED BY THE BCS INFORMATION SECURITY SPECIALIST GROUP

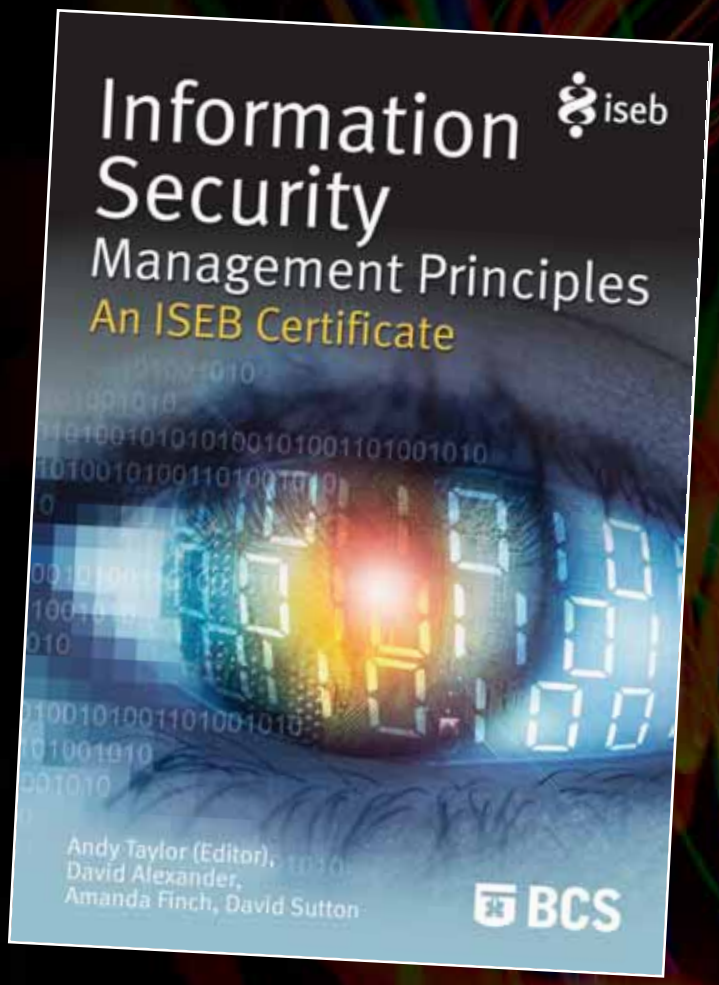
BOOKS08

www.bcs.org/books

INFORMATION SECURITY MANAGEMENT PRINCIPLES

ANDY TAYLOR (Editor), DAVID ALEXANDER, AMANDA FINCH, DAVID SUTTON

How safe is your information? Recent events show that commercial, personal and sensitive information is very hard to keep secure and technological solutions are not the only answer. Information security is largely a management issue and this book outlines the management principles for securing your data. It also acts as a textbook for the *ISEB Information Security Management Principles Certificate.*



Published: Sep 2008

www.bcs.org/books/informationsecurity

Price: **£24.95** 256pp

ISBN: 978-1-902505-90-9

Title ..... Initials ..... Surname .....

Delivery address .....

Telephone ..... Email .....

BCS membership number (if applicable) .....

I enclose a cheque ☐ made payable to 'The British Computer Society' or please charge my:

☐ Visa ☐ Mastercard ☐ Switch/Maestro ☐ American Express (please indicate)

Start date (Maestro/Switch only) ..... Issue number (Maestro/Switch only) .....

Expiry date ..... Card number .....

Name as it appears on card .....

I would like to order ☐ copies at £24.95/€39.95/$44.95 (please indicate)

I would like to order ☐ copies at £20 (BCS members' discount)

P&P: UK £2.75 for the first book, then 75p for each additional item. Europe €7.50 then €1.00 for each additional item. Rest of the World $24.00 then $2.00 for each additional item.

P&P ☐ Total ☐ Signature .....

BooksUpdate service: please mark this box to receive occasional emails about new titles and special offers on BCS publications (you can opt out from receiving these communications at any time). ☐

BCS

To order your book(s), please complete this form and send it to:
BCS Books, Turpin Distribution, Pegasus Drive, Stratton Business Park, Biggleswade, Bedfordshire, SG18 8TG, UK.
Fax: +44 (0)1767 601640
Tel: +44 (0)1767 604951
custserv@turpin-distribution.com
Also available in all good bookshops.

BCS is registered with the Information commissioner in accordance with the Data Protection Act 1998 and will only use the data provided to process your order and to contact you regarding the BooksUpdate Service if you have requested us to do so.

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

Printed in Great Britain by:
Inter Print, Swindon, Wiltshire.
ISSN 1752-2455. Volume 2, 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, asks how can we manage our identities.

Is your identity simply based on your DNA, or is it more ephemeral and flexible? Is it limited to what is on a card or in a database? Can your identity be stolen, or merely assumed? There is no black and white with identity, merely shades of grey.

Someone may have multiple 'identities', to suit particular purposes – e.g. banking, dating, online (public / private), acting – with legitimate or criminal intentions. On the other hand, government and business often need to uniquely identify the people they interact with. This does not predicate a universal identity, but multiple John Smith's have to be managed.

To authenticate someone's (claimed) identity, there are four common methods:

- something you know – e.g. password, PIN, mother's maiden name
- something you have – e.g. identification card, authentication token
- something you are assigned – e.g. name, NI/ NHS number, IP address
- something you are – e.g. fingerprint, retina, DNA, voice, signature

The risk of misidentification is managed through the appropriate selection and application of these authentication methods and their associated data. Generally, the more factors that are used the stronger the authentication and greater the accountability, but this needs to be balanced against usability and failure rates.

If you've managed to get beyond (mis)identification then there needs to be a link to a level of authorisation for each user. These rights need to be properly maintained for each role or user, as this is the second step in identity and access management.

ISNOW | CONTENTS

FURTHER INFORMATION

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

Data guardians

BCS organised a seminar in March with the ultimate aim of improving data guardianship in the public sector. A wide range of delegates from the public sector, learned societies, professional associations, charities and other independent bodies joined BCS for the seminar to work on a blueprint, to take to the government, that can help build trust in the use and sharing of data across the public sector.

During the seminar BCS presented the results of a public opinion survey. BCS also asked the audience to consider its proposed set of data guardianship principles – drawn up over the last year – in discussion groups. In addition, Richard Thomas, the Information Commissioner, gave a keynote address, and other experts in the field presented their views.

It was clear from the survey results that the British public are highly aware and also highly mistrustful of the whole issue of data guardianship. Ninety per cent of the 1,025 respondents were aware of the Data Protection Act, but 66 per cent said their trust in established institutions, such as government departments, had decreased in the light of recent data breaches. The survey also demonstrated that the public do care about accountability, visibility, consent, access and the stewardship of personal information that is collected about them.

These areas form the backbone of the BCS data guardianship principles, which were discussed in the seminar under three themes. Each theme was addressed, initially by presentations, followed by group discussions, held under the Chatham House Rule.

The array of recent IT-related security breaches, including the high profile loss of CDs containing family details by HMRC, has eroded public trust in the government's ability to keep data safe.

Theme one: data governance and accountability

As part of achieving accountability and winning public trust, participants felt that government departments ought to make data processes transparent and visible. The public also need to be able to interrogate and question the processes.

Other participants felt this should be taken a step further, arguing that accountability would only make a difference if it leads to a change in both individual and government behaviours. One way of changing behaviours is by introducing some form of redress, for example, via published audits and the concept of 'class actions' for complainants.

Another view was that achieving a change in behaviour is not best done via a legal process. Instead, government departments could be asked to demonstrate evidence of good processes. Routine governance reporting and audits would bring to light the effectiveness of what an organisation has in place to stop problems arising.

Participants considered how to engender the same public trust in data privacy when a citizen was interacting with a bureaucratic entity (such as a government department) as existed when they were interacting with a professional individual (such as a doctor). One possible solution would be for

organisations to make clear in their governance statements that data privacy and stewardship rested with named and trusted individuals. Another aspect of this was ensuring that everyone in an organisation understood the differences between accountability to their organisation and to 'data subjects' and that accountability to the latter was considered at least as important as the former.

There was general agreement that effective data governance and transparency would only be obtained if the top people commit to it and lead it. They must be given the authority to do so. There was a suspicion that data governance does not currently come under the remit of top leaders on the board, as it should.

Rebuilding public trust in government departments, via actions such as audits, would incur costs. However, savings made from introducing e-services should help fund them. In addition, costs from data losses would be avoided.

A large part of the costs of such losses to date has been borne by banks and citizens, who have had to set up new accounts and passwords.

Theme two: sharing data with secondary parties, including informed consent

It was agreed by participants that the boundaries of data stewardship needed to be made totally clear when data was shared. It was important that the collection of excessive data in the first instance needed to be stopped. Also the context in which the original data was collected was vital information for downstream users. Inappropriate dissemination and aggregation are major problems.

When the original collector of data shares it with a second party, the collector must ensure that it is for a legitimate purpose and necessary, agreed participants. The collector should also tailor the data to the secondary use. By minimising data shared, there is potentially less to lose and less to keep up to date.

It was suggested that the BCS set of principles needed to be more precise in using the term 'duty of care', in the context of the original data collector. It can mean very different things to different professions, for example, to lawyers and other groups with ethical considerations.

When passing on data for secondary use, it becomes very important to include extra information about it – to explain the context of its collection, and have a way of recording if data is factual, subjective or anecdotal. Metadata (data about data) can be used to record such details.

Also, the recipient of data for secondary uses ought to have a continuing obligation to stewardship – this is not mentioned in the BCS set of principles. As it's extremely difficult to implement and track corrections once data is passed down the chain, it was suggested that secondary users could access the data via web services (rather than actually receiving data), which would give the original holder more control over its ongoing accuracy.

An example of the complexities of stewardship in the health sector was given. Although GPs support electronic patient records, they are concerned as to how they can be their guardians when they are held on a hospital server or central patient record. It also makes it harder to inform patients of how their data is likely to be used for secondary purposes.

The proposed principle of obtaining 'informed consent' to use data for a purpose other than for which it was collected is, however, not straightforward and raised a number of concerns. It was pointed out that citizens do not always have a choice about what data the government holds on them (for example, the police holding criminals' fingerprints) and it could be misleading to suggest consent could be given in such cases. Also, what about people who are too ill to give consent? And should you tell the person the implications of not agreeing to data sharing, for example in terms of healthcare? Is it acceptable to expect the person on the street to understand what is required? Achieving truly informed consent is therefore very difficult.

It was agreed that citizens must be able to revoke consent if trust runs out or something goes awry, but very few mechanisms currently allow this. And again, there needs to be some form of redress for inappropriate data sharing.

Technically, revoking of consent, when data is shared, is very difficult as few of the systems on which the data is held distinguish between data for which consent to share has been given and those for which it has not.

Theme three: engendering public trust in the government

Citizens are prepared for organisations to hold their data if they get something in return for it. Laws on data protection, however, are not enough to reassure citizens, according to one participant; to win the public's confidence, organisations need to bring the statute to life via their deeds. One suggestion was that government departments, could, for a start, say on their websites what data they hold about people and for what purpose.

It was agreed that the privacy impact assessments, recently introduced by the information commissioner, should be made mandatory in the public sector and be published. Another idea was to have different procedures for different risk categories of personal data along the lines suggested in the BCS position statement – some information is more sensitive than others, and some people will be more affected by its disclosure than others.

The BCS set of principles could, it was suggested, include an obligation for proposed new systems to undertake a risk assessment related to personal data privacy. This would then cover the main new systems due to come on stream, for example those of Connecting for Health and ID cards. Another set of principles is not really what is needed, thought one participant; many participants felt government departments need to be given practical advice and training on implementing good data practices, and BCS could play a role in this.

The way ahead

The momentum created by recent high-profile data breaches can be used to try to lead change, making now a good time to tackle it. The BCS approach to improving data governance was widely welcomed by participants at the seminar. The BCS proposed set of principles were judged to be broadly acceptable, although participants suggested refining some of the wording, and adding some extra points. Once finalised, the principles should then be promoted to the highest level of government as an extension to the Data Protection Act principles. Action is also needed to help the public sector understand how to put the principles into practice, set up effective data protection systems, and promulgate examples of good practice. The key next steps involve 'operationalising' the principles in complex large-scale data sharing environments.

Compliance is not security

As we all learned back in school, it's quite possible to do the bare minimum and still get a pass grade. But simply studying for a test doesn't equal a good education, and passing an audit that attests your business is in compliance with the Payment Card Industry Data Security Standard (PCI DSS) doesn't mean your data is secure either. All that it means is that you've done the bare minimum, and that's simply not good enough.

Being in full compliance with PCI will result in a decent level of data security, and for some merchants that will be an improvement. But PCI was never intended to be an end point, it's a foundation that merchants are meant to build on. Unfortunately, the good intentions of PCI are lulling some businesses into a false sense of security, and the need to achieve compliance can siphon off time and budget that would be better spent deploying real data protection.

If your security consists of just doing the bare minimum that simply isn't good enough. Gordon Rapkin, CEO of, Protegrity goes back to school and explains why compliance isn't security.

Take, for example, the recent case of the US grocery chain that was certified PCI DSS compliant and yet was still wide open to an attack that exposed 4.2 million credit and debit card numbers. Apparently, malware installed on servers at more than 270 of the company's stores captured card data as it was transmitted from point of sale to payment card processors. The data was then forwarded to offshore servers. Had that data been encrypted it's safe to assume that the subsequent 1,800+ reported fraud cases wouldn't have occurred, but PCI doesn't specifically require data to be encrypted at point of capture so we have a PCI compliant merchant with a huge security hole that was just waiting to be exploited. If you were a

savvy criminal, wouldn't you be looking just past those well-publicised PCI points of compliance for holes to exploit - such as data travelling unencrypted from cash registers?

Security simply cannot be achieved by ticking off steps on a checklist. Real security is holistic, encompassing technology, people, processes and policies. It is hardwired into everything a company does, and is part of that company's culture. And while it may seem like a real challenge at first to institute a comprehensive data security plan, ultimately a unified approach will be far more effective, increasing security and saving both time and money.

Beyond compliance – implementing a holistic approach

Before you devise or revise a comprehensive security plan it is critical to have a clear view of the big picture. Data flows through a company, into and out of numerous applications and systems. Think of your network as a municipal transit system - the system is not just about the station platforms. The tracks, trains, switches and passengers are equally critical components. Many companies approach security as if they are trying to protect the station platforms, and by focusing on this single detail they lose sight of the importance of securing the flow of information.

A critical first step in any data-driven security project is to conduct a thorough audit of the entire system and identify where sensitive data is processed, transmitted and stored. Not an easy task, but an essential one: you can't protect data if you don't know where it is. Audits typically reveal sensitive personal data tucked away in places that you'd never expect to find it, unprotected in applications and databases across the network.

Unfortunately, PCI doesn't explicitly require merchants to audit the flow of payment card data through their systems, but once you know where the data goes, you can develop a plan to protect it.

The plan should address such issues as data retention and disposal, user access, encryption and auditing. As you devise this strategy you must take into consideration that business need will often trump security requirement. An effective security plan must also take all of the stakeholders' needs into account or it will fail. People will always find a way to thwart security measures that they don't understand or that impact negatively on their productivity.

Thus it is best to develop the plan and its ensuing policies in tandem with representatives from departments throughout the company. Many of your employees are stakeholders in security and should feel as if they are a valued participant in protecting company data, not miscreant children. People's concerns about data security interfering with business processes and productivity must be respected and taken into account when developing security policies and processes.

Collaboration across the enterprise is critical to holistic security. It's obvious that effective security has to be everyone's problem, and the processes that support real security need to be embraced by all. But simply devising policies isn't enough. Given the differing feelings that may be present about data security, policies and procedures should be enforced by technology controls such as role-based access, data encryption and auditing tools. These ensure that everyone is following the rules and protects data from misuse and/or exposure even if the rules are broken.

One of the most positive steps an enterprise can make is to institute ongoing security awareness training for employees. Ensure that all employees understand:

- how to identify confidential information;
- the bottom-line business importance of protecting data and systems;
- how to choose and use passwords,
- what is acceptable use of system resources, email and the company's security policies and procedures.

Security training should not be generic but should instead be targeted to an employee's role in the company with refresher courses bi-annually, or more frequently, depending on the person's role in the company and their access to sensitive data.

Processes and policies also need to evolve. Consider instituting a monthly meeting with senior managers to talk about upcoming data security and regulatory concerns. Look at what's starting to happen, what tools people are using, what threats are out there and consider what policies the company may need to enact to deal with these issues. However, except in emergencies, adjustments should be made to policies on a quarterly basis rather than bombarding people with constant changes.

Finally...

One size will never fit all in security so assess the data flow and risk environment within your company and devise a comprehensive plan to manage information security that dovetails with your business needs. A data protection-driven holistic plan is the only way to truly secure data - it allows you to think strategically, act deliberately and get the absolute best return on your data security investment.

Digital cocktail party

Andrea Simmons reviews the influence social networking technologies are having on privacy management in the naughties.

Face party, MySpace, Facebook, Bebo, Second Life – they all seem to have been in the news continually over the past few months, for one reason or another, most recently as a result of concerns over privacy, but that's for another time. Notwithstanding their clearly huge popularity, the key cause for concern appears to have been the late realisation of the open nature of the web and thus how much personal information has inadvertently been left exposed to any passing stranger with an eye to the value of the 1s and 0s.

A recent report from credit agency, Experian stated that identity fraud has leapt by 66 per cent over the past year.

Too many individuals are experiencing what is wrongly termed identity theft (your identity itself cannot actually be stolen but information relating to you can indeed be used to create another identity).

You can check out but you can never leave

Attending a seminar session on social networking at InfoSec 2008 in April this year, the soundtrack to the event was the Eagles' eighties classic Hotel California and the apt juxtaposition of the key line: 'you can check out but you can never leave'.

Web 2.0 sites, according to Facebook, are social utilities not social networks. This is an interesting and subtle distinction, implying that Facebook could be looked at as an identity management tool.

However, if that was the intention, as ever with a useful technological system, the users have done more than could have been anticipated with them and so we are experiencing this Hotel California situation where people have engaged positively, provided lots of information up front and then been surprised, when they wanted to walk away, that it was harder than first imagined.

However, there are obviously those journalists who will imply that by not being involved in all this social networking, we are missing out and potentially damaging our careers. Can this be true?

It seems that you need to pick and choose carefully where to place your information and with whom to interact. In business circles we have, amongst others, ecademy **www.ecademy.com** and LinkedIn **www.linkedin.com** as networks to belong to. It appears that there is some sort of class system attached to them so that it is not clear whether you have actually registered with the right one for the industry you are seeking to be part of and whether it will say the right things about you by virtue of your liaison.

The International Association of Privacy Professionals (IAPP) recently ran a 'tell us in 100 words or less' competition, to come up with the best description of what a privacy professional is - and the result was the following:

So whilst a privacy professional in their day job should be able to achieve this, there seems to be the capability to drop the 'real time shields' when it comes to conducting one's own private life outside of the working environment. And yet we are now in an age of 'blended' edges - where your employer is more than likely to do a check on some of the social networking sites to see whether you have an avatar or online presence and, if so, a judgement is made as to how you are conducting yourself and thus, whether, by your actions, you are the kind of person that they, as an employer, want to join their organisation. Oxford University trawled Facebook for evidence of students behaving inappropriately - 'trashing' each other.

Obviously social networking sites provide a great insight into people and their out of office habits - but this certainly reduces the difference between work and play and continues to further blend our existences - is that what we really want?

IBM has a Code of Conduct (**http://tinyurl.com/4y9xsq**) that extends into virtual worlds. It warns employees to back away from inappropriate people, behaviour or transactions. Participation must be approved by a manager, and the avatar's appearance should be 'appropriate'. An employee's digital persona should not be abandoned to another person who changes its behaviour. It appears that a privacy setting in the online world is not the same as that expected by us in the real world.

It appears that a privacy setting in the online world is not the same as that expected by us in the real world

Apparently, for example, Facebook has more privacy settings than MySpace. But presumably you would need some level of technical or legal expertise to have clarity about the ramifications of the set up.

Companies have been wooing people using Second Life. A recruitment fair was held where avatars were greeted by virtual recruiters, including KPMG and Yell.com. Given how easily you can make stuff up online, if the real world were previously worried out bogus CVs how will the wheat from the chaff process take place between the virtual and the avatar?

An NHS organisation has set up its own Facebook site inviting users to chat with patients and staff. The South West Yorkshire Mental Health Trust offers people the opportunity to discuss the stigma suffered by those with mental health. Everyone is talking about it. YouGov did a survey recently in which, unsurprisingly, the results showed that employees are being distracted by the use of social networking sites - to the tune of some three hours a week - which adds up to six days a year, outstripping online banking, shopping or music downloads.

So the revolution is definitely on. We are in the process of the Gartner hype cycle. From initially feeling that the sites should be considered to be frivolous, there are obviously those who can see that, if used and managed in the right way, the technology can actually improve business collaboration. This was recently hinted at when an article expressed the concern that the model for Web 2.0 at the moment hasn't really borne financial fruit. Squarely in the trough of disillusionment then. People remain happy to communicate with each other but this is a social thing, not a commercial thing - hence the term social networking - beyond the social utility as first intended.

And what did we do before it? We are a highly evolved species already, when it comes to communication – is this just another element of that? Presumably so. But given that there are companies and organisations who struggle with individuals not wishing to have their photographs shown on the corporate intranet, there is a long journey still to be had.

Common sense tells us that either way it is important to make sure that people know what is expected of them in terms of using privacy settings, and what information is and isn't appropriate for sharing. The social networking site you are using are a third party and you need to be happy that you would trust that third party with your personal information. As privacy professionals, we should have our 'real time shields' up further than most – and be more aware of data processor / data controller, data transfer issues – none of which 'push the buttons' of most normal people but all of which are fundamental to a best practice approach with regard to privacy and identity management.

Remain consistent

Bruce Schneier's Counterpane newsletter from July 2007 had a privacy flavour to it and the following struck a chord:

'Given recent news stories on UK government intentions with regard to potentially intrusive systems and data sharing, this statement should ring true for all those who are considering systems development for future data manipulation.'

It's up to us as privacy professionals to ensure that we remain consistent with our messages - and always seek to ensure they are understood - without appearing to stop everyone's fun. This is not an easy task, but we owe it to ourselves and to those who are not as aware of the issues as we should be, to make sure that the key messages are listened to and understood and that appropriate controls are put in place wherever they are needed.

Security on the move

Having access to your data when you're out of the office is a must for many people, but it also needs to be secure at all times.

Getting to grips with information security is like trying to decide whether you are on the inside or outside plane of a moebius band. No matter which way you look at it, no matter which way you turn, something eludes you. The jelly wobbles and the blancmange collapses at just the moment you think that you have it finished and therein lies the problem with information security: it is never finished. Information technology expands just like the universe, with dizzying speed. The Hubble red shift has nothing on what has happened with IT since the 1950s. At first momentum was slow. Very little movement in the mainframe environment for a couple of decades and then the rapid expansion of storage technologies, networking and end-user computing. Then with even dizzier speed, the reduction in size of components bringing mobile networking, personal digital assistants and radio frequency identification. Implants which are currently in their infancy, will become common place, especially if governments get their way. New technology raises new security challenges and by default new control problems to be solved.

As devices became physically smaller physical security became more difficult to enforce. As an example ten thousand mobile devices are simply lost on the London transport system each year. Add to this the number stolen in robberies, or left behind at the security screening areas in airports and you have a large potential exposure. So we close this exposure by adding logical security ranging from simple PINs through to biometric scans, such as fingerprint recognition.

PIN problems

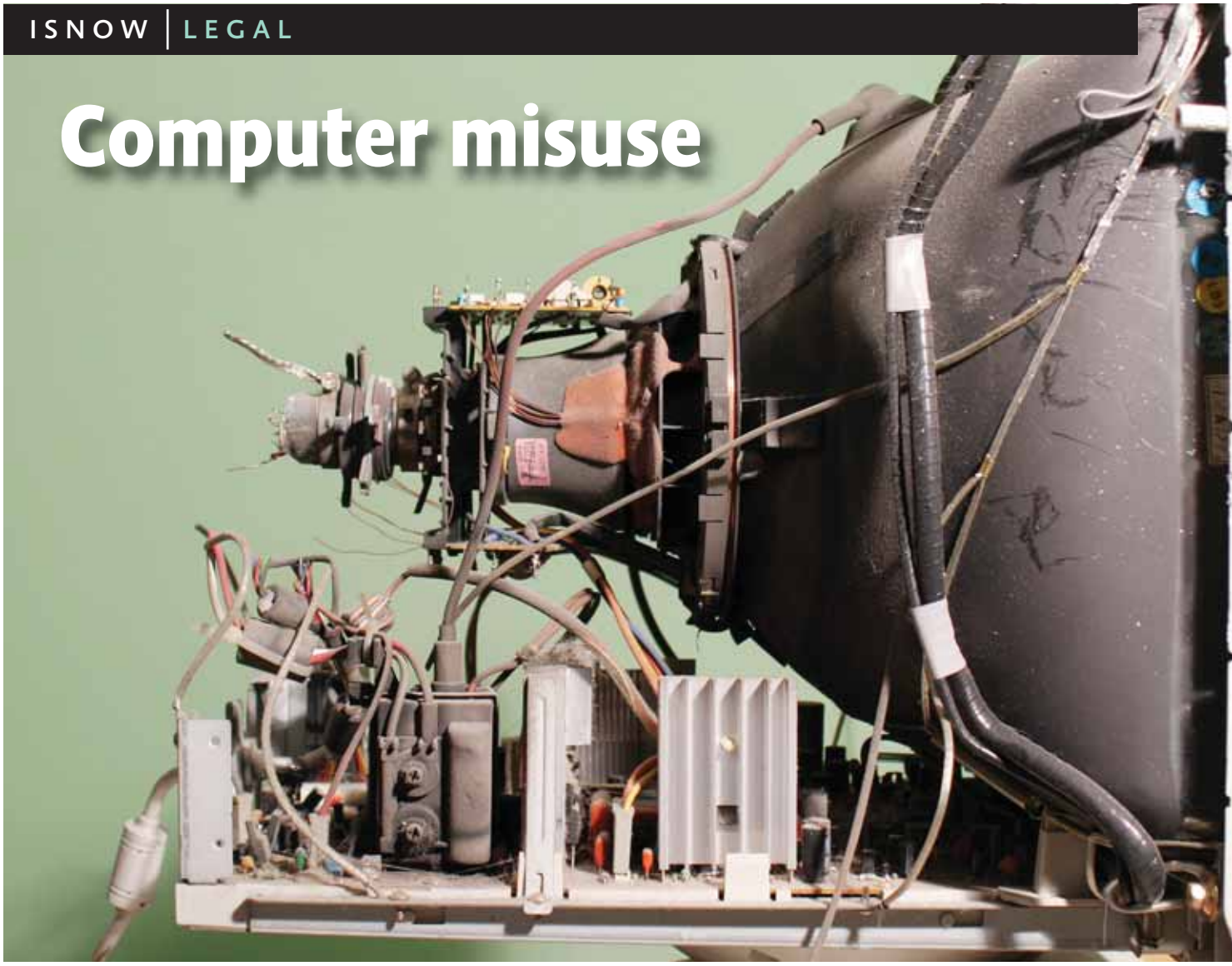
Considering that most mobile telephones provide internet access to office systems the simple PIN is woefully inadequate. If the telephone is stolen whilst it is online, then the thief has access to the associated office systems. Many users do not even use a PIN and have the telephone/PDA configured to automatically log on once the device is switched on. BlackBerry users never seem to switch them off anyway. We then consider multi-factor authentication, but as we already know from cash machines, the criminals then simply apply the threat of injury to obtain the access credentials. With PDAs there is some merit in using proximity alarms. If the PDA moves out of range of the proximity monitor it could be programmed to automatically shut down. This would cover the risk of loss as well as theft. Likewise if you wish to protect data from unauthorised access, then splitting a key data between (say) three separate locations will complicate the problem for the hacker as s(he) now has to break into three systems to obtain anything useful.

The careful application of the confidentiality, integrity, availability and compliance (CIAC) framework using risk assessment and management techniques enables even complex technologies to be broken down into their key aspects. How can we keep things secret and accurate? How can we make sure that they get to the people who should have them when they need them? How can we remain legal?

I was recently dealing with a government department which wanted to release a new internet based tool to enable certain parts of the community to gain access to personal data stored on a government database. Using risk analysis techniques I was able to quickly establish that the developers had done an excellent job in preventing unauthorised access to the data. However, what about unauthorised disclosure by an authorised user? There was nothing the IT people could do to prevent that scenario. It could conceivably be detected after the event if the sensitive data entered the public domain, but by then the damage would be done. A typical outcome of applying risk analysis techniques to data leakage. In this case we have a relatively low likelihood, but very high consequence (reputation, breach of trust and conceivably non-compliance with legislation). The politicians have two clear choices: terminate the risk by not deploying the tool, or tolerate the risk and be damned if it crystallises. Tough call, but that's what they get paid for. I get paid for pointing out the risks and the available choices. Mine is the easier of the two jobs.

John is editor of BCS IRMA's award winning journal and managing director of LHS Business Control.
www.lhscontrol.com

Computer misuse



Anti-hacking legislation and making sure that e-tailers are doing what they are supposed to.

Many of you who have been following the strengthening of anti-hacking laws under the Computer Misuse Act, as part of the Police and Justice Act 2006, will have expected those changes to come into force by now. Eversheds spoke to the Home Office to check on progress. We were informed that the deadline for commencement orders for the Police and Justice Act for March was missed as they were waiting for another piece of legislation to go through first. The next commencement orders will be in July as the Police and Justice Act commencements are passed on a quarterly basis. The Computer Misuse Act amendments are still due to be actioned and we, therefore, anticipate that July may bring further news.

Office of Fair Trading web sweep

The Office of Fair Trading (OFT), in partnership with the Local Authority Trading Standards Services, has carried out a web sweep of around 600 of the UK's top retail websites to ensure they comply with key e-tailing laws.
The Press Release can be viewed online at: **www.oft.gov.uk/news/press/2008/34-08** (with a link to the results of the analysis).

It is worth reading through the findings to note common mistakes that are being made and the compliance checklist that was used. Particular attention was paid to checking compliance with the distance selling regulations (DSRs) and e-commerce regulations (ECRs). The DSRs deal with business-to-consumer sales made in a non-face-to-face context, such as internet sales and set out a number of rights, which must be given to the consumer whilst the ECRs require e-tailers to provide shoppers with certain information. The web sweep also looked at compliance with other legislation – including the unfair terms in consumer contracts regulations, the consumer protection act, the price marking order and the sale of goods act.

If you are e-tailing, now is a good time to revisit your website terms and check you are not making common mistakes, especially as more sweeps are likely in the future.

Charlotte Walker-Osborn,
Senior Associate Solicitor,
Technology Group, Eversheds LLP.

15 ways to lose your database

There have been many articles written that examine the risks posed of data being exposed and the potential damage caused. In addition, external threats have long been recognised with billions of pounds spent strengthening defences to mitigate against them yet there is little acknowledgment of the very real threat from within. The statement 'don't leave your valuables on show' is a simple principle so why is it often ignored by Corporate UK?

It is proven to be easier to bribe someone on the inside (or even implant them there) to gain access to sensitive data. Leaving this risk aside, how often has someone left your organisation taking company stationary with them? Do you know what else has been taken? Could they have sneaked out with sensitive material? What about a copy of the entire corporate database? Would you even know if they had?

Here are some of the most common techniques individuals will employ to copy sensitive data:

Legitimate access yet inappropriate use

Let's be realistic, employees need to have access to corporate data in the normal course of their duties. Increasingly today, this need is 24 hours a day - seven days a week and is not restricted to within the corporate walls or to company owned devices. It is this need that is opening up one of the biggest and growing weak points for Corporate UK as data is seeping out via unprotected end-points, a significant number of which the company is unaware exist, or they are simply outside the company's domain, such as private USB sticks or iPods.

Arguably an organisation's most vital asset is its databases, often containing financial information, customer and employee data and intellectual property. Peter Mitteregger, European vice president, CREDANT Technologies tries not to lose his.

To illustrate, an employee in sales may need to legitimately access customer records whilst on or off site and during a normal day may do so up to 100 times, another employee in R&D may need access to the secret formula for a product that's in development, whereas another employee in the marketing department may need to access the marketing plans for this new product's launch and email them to the various agencies tasked with delivering the plan.

However, there is no viable reason for all of these different employees and departments to be able to access all of this information, in the same way, and do the same things with it. In many instances, the company may be legally obligated to limit access to information on a need-to-know basis.

Access must be restricted to just the records that are needed to perform the task, with control over which bits of each record can be viewed, combined with limiting what can be done with the record.

If there is no obvious explanation why an employee should need to be able to access confidential and sensitive data, whilst off site, then they shouldn't be able to. It would be prudent to employ a solution that can detect devices trying to connect to the enterprise and sync up with corporate data. Additionally, if there is no reason why they should need to make an electronic copy of these records – be it to a corporate or personal endpoint, such as a CD, a USB/memory stick, an iPod or even a BlackBerry, then they should not be able to do so. If there is a valid reason why they need to make a copy then it should be force encrypted with a

solution that does not impede the system, regardless of the device it is stored to, to ensure the integrity of the data is protected once away from the safe corporate environment.

By the same token, if an employee does not need to print a copy of the data then they should not be able to do so and even if they do, this should be regulated as I'm positive that there can be no genuine reason for complete records to be printed. Perhaps an alarm bell should be sounded if someone does print the entire database and a means deployed to ensure that it is not removed from the premises.

Another way to identify if an employee is abusing their access rights is if their usual behaviour alters and they suddenly start accessing a greater number of records then usual for longer, or even shorter, periods of time. This could indicate that they are writing the records down in some format to bypass any security restrictions in place.

In the case of a disgruntled employee, determined to cause mischief, records could be altered, or even worse deleted, thereby damaging the reliability of the data.

Another danger is if an employee wishes to steal a copy of a database and may attach it to an email and send it out legitimately through the corporate gateway. A savvier employee, worried at leaving a trail, may try to bypass this by uploading the file to an external system, such as yahoo, hotmail or a hosted document storage and management solution.

There have been a few instances of people seeking employment to steal data to order or even for an employee persuaded to divulge corporate secrets for financial gain.

Opportunistic access is still a real risk

There are some risks that aren't hi-tech and, therefore, harder to detect and even harder to protect against. For example, the business case for a printed hard copy of sensitive records needs to be strong as an opportunistic may access this and make a photocopy of it, completely undetected.

Another increasingly recognised threat is the mobile employee, justifiably working while travelling; either on the train, in a service station or another location, with someone looking over their shoulder and making a note of material displayed on the screen.

One further, really obvious, risk is writing down and/or sharing passwords. This is a truly naïve practice, with no justification, yet it is still widely abused today.

Illegitimate access so of course they're up to no good

The easiest, yet inexcusable, way for data to be violated is by an ex-employee whose access rights have not been timely revoked accessing the network remotely, perhaps initially just to see if they can, and then tempted into taking liberties with this oversight.

Another potentially soft target is a portable endpoint; such as, but not limited to, a laptop, BlackBerry or USB/memory stick, that is misplaced or stolen. Should the device be unprotected then any data stored on it is exposed. Additionally, in the case of a laptop or BlackBerry, it may prove to provide a back door to the corporate network.

So what's corporate UK to do?

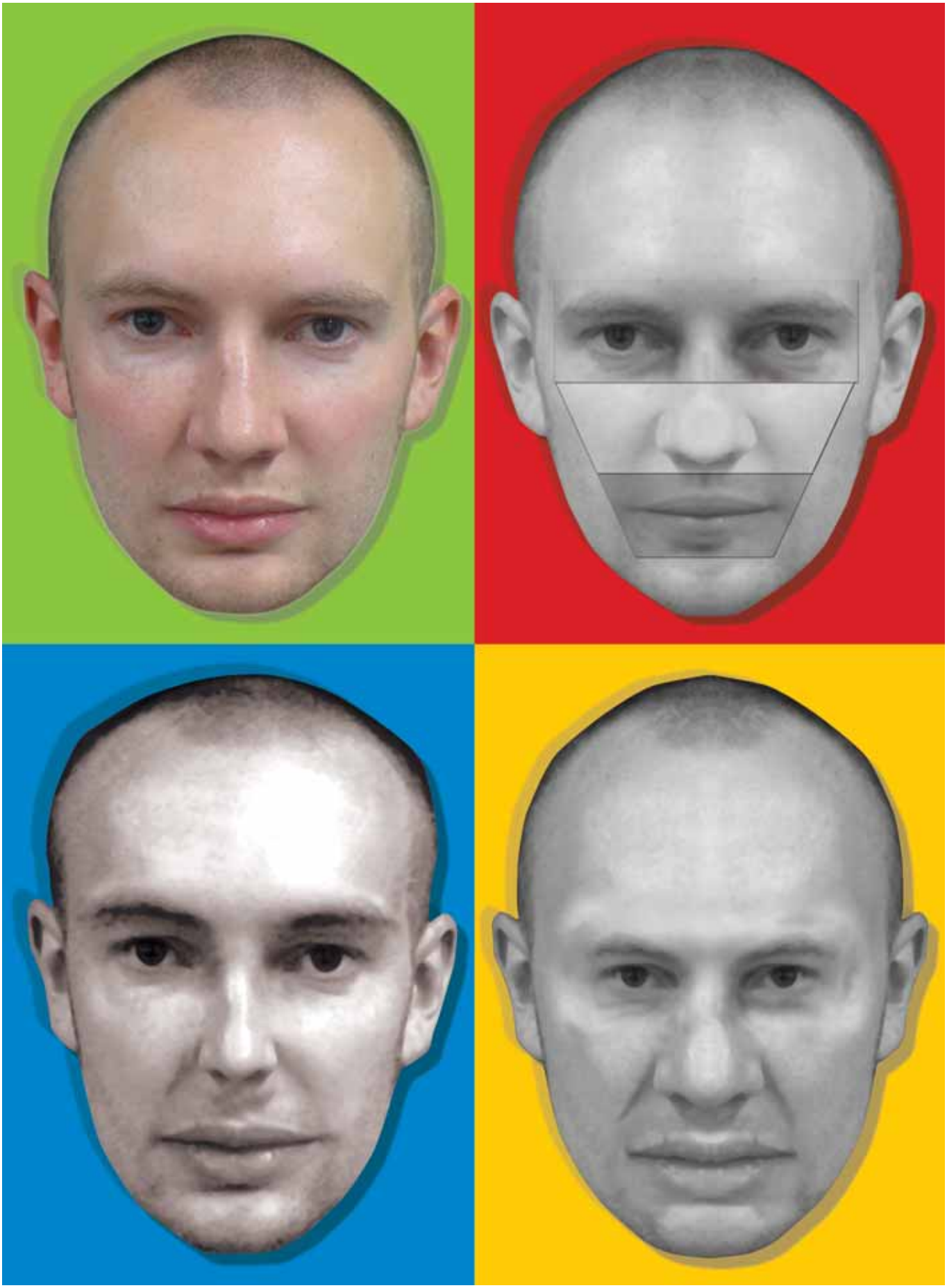
It may seem like a nightmare with so many trusted employees out to steal your most vital asset yet there are ways to mitigate against these risks:

- Restrict access to only those employees who need it and limit what they can see, and what they can do, with the records;
- Appropriately monitor employees' behaviour, ideally setting control mechanisms to flag any significant deviations from the norm;
- Employ a solution that can detect devices trying to connect to the enterprise and sync up with corporate data and force encrypt information when it is removed, legitimately or illegitimately, from the safe environment of the corporate network;
- Do not make unnecessary hardcopies of records or leave them unsecured;
- Educate the mobile workforce to the risks posed by their activities and the devices that they use;
- When an employee leaves, ensure all access rights are revoked immediately;
- Never leave a written record of passwords;
- Perform background checks on new employees, including contractors and any periodic workers. It may be prudent for these checks to be conducted at regular intervals to ensure that nothing has changed as is the case for those working with children via the criminal records bureau;
- Never leave data security up to the end user. It is imperative that this is controlled and managed centrally, which can also reduce TCO as machines don't need to be locked down or brought in to the office to update them;
- Corporate governance requires you now to have security and to be able to prove it. Use a solution that includes a central management console – that way every machine is protected and can be tracked.

Quick overview of 15 ways to lose your database :

- Employees able to access a database regardless of their need to do so, with sight of complete records including information that they do not necessarily need to see;
- Unrestricted downloading of the data base to removable media;
- Employees able to print individual records, or even the full database, in hard copy format;
- Employees able to access records, in undefined quantities or for unlimited periods of time, providing the opportunity to make a written copy;
- Records, or even the entire database, altered or deleted;
- The full database, or individual files, emailed as an attachment;
- The full database, or individual files, uploaded to an external storage facility/website or a hosted document storage and management solution;
- Secure employment for the purpose of having unrestricted access to confidential data with criminal intent;
- Existing employees being coerced into removing data for financial gain;
- Ex-employees who have not had their access rights revoked;
- Photocopy hard copies;
- Over the shoulder screen theft from mobile workforce;
- Writing down, or even sharing, pass words;
- Loss of external or portable media (memory sticks, CDs, laptops, etc) that contain unencrypted information, often during travel;
- Misplaced, or stolen, devices (laptops, BlackBerrys, etc) used as a back door to the corporate network.

For more information contact:
www.credant.com



Facebook, trolls, temples and death threats

Online, if you're not careful or plain unlucky, anyone can pretend to be whoever they want to. Graham Cluely, senior technology consultant at Sophos, takes a personal look at managing identities online.

I wouldn't exactly describe myself as a naïve ingénue when it comes to the risks that people can face on websites like Facebook.

Indeed, last year I, and some colleagues, showed just how easy it was to steal identities on social networking websites after we created a fake profile of a small plastic frog called Freddi Staur (an anagram of ID Fraudster) and invited strangers to become Freddi's friend. Scores of people accepted the invitation, many revealing their full names, addresses, dates of birth, phone numbers and even - in one example - their mother's maiden name in the process.

It was,therefore, a surprise to me in April when I discovered that someone had, without my knowledge, stolen my very own identity on Facebook - at least in one fashion.

Inflammatory comments

What happened was this. Some pumpkin-brain on Facebook thought it would be a good idea to create some controversial groups on the social-networking website and feed the flames by posting inflammatory language. So far, so normal. But what this chap also did was decide to steal an online photograph of me and use it as his profile picture.

Inevitably, someone on Facebook recognised my picture, put two and two together, made five, and announced that I must be the person posting the nonsense onto the website. Furthermore, encouragements were posted to bombard both my own work email address and other email addresses at Sophos with 'information about what Cluley has been up to'.

All this was occurring as I was having a rather splendid holiday - with very poor internet connectivity - in Siem Reap, Cambodia.

Things got progressively nastier, as photos of me and my wife were posted to Facebook (complete with rather unflattering comments about the bushiness of my eyebrows and speculation as to where I buy my shirts). One guy, who claimed to be with the armed services, said that he had found out where my wife lived (probably not that tricky as my surname is somewhat unusual) and was considering shooting her. Another emailed me saying he intended to burn down my house.

As my wife and I were adventuring Indiana Jones-style, amongst the temples of Angkor Wat at the time, you can understand why we might have felt a little alarmed as to what we would find upon our return to the UK. The poor internet connectivity also made it tricky to contact the outside world, but I did file reports to Facebook asking them to delete the offending material.

> **It was only when a journalist published a story about my experience that Facebook removed all the slurs against me**

Call the police

Facebook's response was, I'm sad to say, mixed. Maybe I've upset them in the past with my Frog-related antics, but I would have expected them to have taken stronger action when presented with evidence of death threats on their network. Instead, Facebook advised me to contact the police and only eventually removed the photographs when I logged them as a breach of Sophos's copyright.

What is perhaps most disturbing is that not only were hotheaded internet users making death threats against me and my wife, because they believed I was responsible for the troll-like postings on Facebook, there was also at least one group on Facebook which was created claiming I was a paedophile, and saying that web users could visit my site at grahamisakiddyfiddler.c**t.uk. Another group listed me as one of the 'Top 20 c**ts on Facebook.'

I'm used to being disliked for expressing my opinions on computer security - I've even had virus writers lampoon me in their malware before - but to be on the receiving end of death threats against my wife and accusations of being a child abuser takes things to a whole new level of seriousness.

It was only when a journalist published a story about my experience that Facebook finally removed all the slurs against me and my family and closed down the discussion groups that were, frankly, out of control.

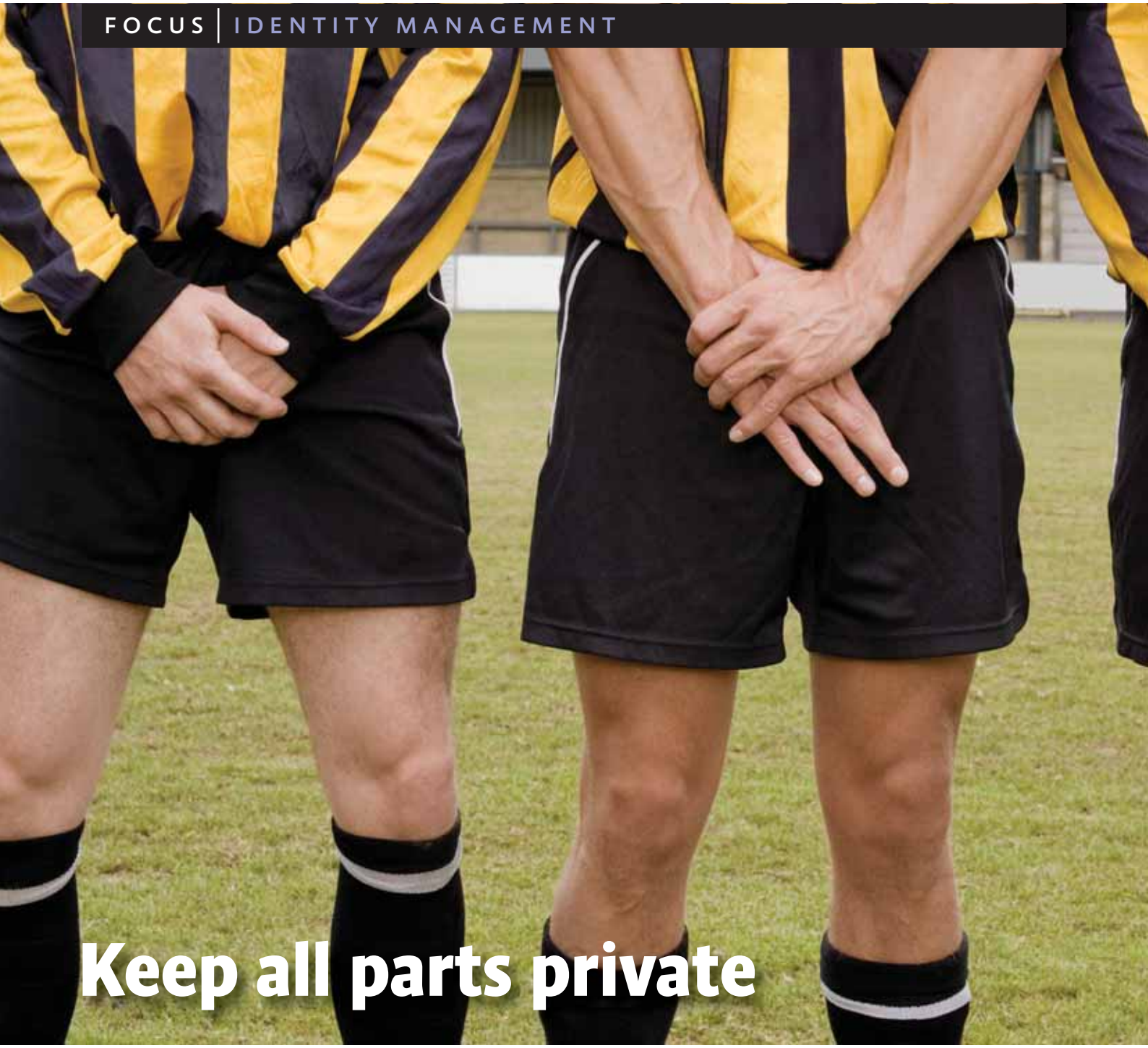
To my mind, Facebook should have reacted faster in my case. But I was fortunate enough to have connections in the media to make my position clear. Imagine if I had been a more vulnerable member of society, or had not been alerted to what was being said about me?

And what is Facebook doing to stop this kind of abuse happening in the first place? A quick search on their website finds literally thousands of groups with extremely inflammatory titles and highly vulgar language.

News of the World

Readers with long memories may remember in 2000 that The News of the World newspaper published a 'name-and-shame' list of alleged paedophiles, which resulted in a paediatrician having her house vandalised, and innocent families asking to be rehoused as mobs descended onto the streets. It seems to me that as more people get on the internet and believe everything that they read, the chances of mobs attacking innocent people rises all the time.

The News of the World was far from the most highbrow newspaper in the UK in the first place, but its decision to publish the names of alleged sex offenders brought it into even more disrepute.



Keep all parts private

Privacy is a hot topic – one that the business world ignores at its peril. A stronger legal and regulatory environment, high profile privacy failures and increasing public concerns build the case for business and organisations to take privacy seriously to avoid incurring hefty fines or breaching trust.

Yet privacy is still not sufficiently addressed at boardroom level and arguments may be needed to ensure that it gets on the agenda of IT executives. There are, however, many high profile cases where failures in information systems have crossed the line of the public's expectations of privacy. In December 2007, the Information Commissioner's Office found the Department of Health in breach of the Data Protection Act, following an alert that sensitive personal details were accessible to anyone accessing the website of the Medical Training Application Service.

Privacy is something that every business should take very seriously. Nigel Jones, director of the Cyber Security Knowledge Transfer Network explains why we should all cover up.

Social networking

In addition, popular social networking site Facebook had to back down over the introduction of its 'Beacon' feature in 2007, which automatically notified the 'friends' of any user making a web purchase. The site's reputation was arguably damaged over the issue of its customers' privacy.

On a personal level, privacy is an issue we are too relaxed about. People are willing to take the chance of giving away personal data because of the perceived benefits and the knowledge that, for

example, they can get their money back from the credit card company or vendor.

So what can be done to avoid such problems relating to privacy? My work with the Cyber Security Knowledge Transfer Network (KTN), which recently produced a privacy engineering White Paper, has started to set the case for designing privacy within IT projects.

We strongly advise that privacy issues cannot be 'bolted on' at the end. IT organisations must commit to protecting its customers' privacy up front. Such commitment must imbue the culture of an organisation and must shape the project before design starts.

Privacy requirements must be fed in at four stages of software design - initiation, planning, execution and closure.

At project initiation high level privacy objectives need to be set. At the end of the project initiation stage, the designer should have a general idea of what the project will entail and what assets will be involved, introduced or addressed by the project. For example, the project owner will need to be aware of applicable privacy laws and regulations, such as the EU Data Protection Directive or the US Safe Harbour agreement. Technology envisaged for use by the project should be subject to a high level review to ensure that appropriate privacy controls can be implemented. As a result of this, the project manager will be aware of, and be able to factor in, the appropriate privacy requirements at the next lifecycle stage. The project planning stage in the lifecycle enables the owner to develop detailed requirements for the project. The privacy requirements at this stage will need to be just as definitive. They will enable the enterprise to take account of applicable laws and regulations. Further privacy requirements, relating to information assets, will be made clear. Technology that will be introduced as a result of the project will also be defined. The privacy requirements for the technology will be appropriately and accurately described. Mechanisms, such as encryption, will be proposed to protect, for example, consumer and client data on storage media. Additional privacy requirements will be made if necessary, for example, to ensure that identifiable data is not made available when viewed by personnel who do not have a 'need to know'.

During the project execution phase, any problems relating to the privacy solutions proposed for the project should be identified, and decisions made on alternative solutions to ensure that the required level of privacy is still maintained. The project should document any privacy related issues and exposures. The project owner should be made aware of these prior to the project 'going live' in the production environment, and should sign-off any privacy related issues that have been raised by the project.

Privacy requirements need to be consistently and continually addressed after project closure, in the production environment. This should be achieved with audits and change control procedures. Internal audits should be conducted at regular intervals to ensure that there aren't any breaches of the agreed privacy implementations and policies.

Privacy must also be addressed at system decommissioning - whether this involves secure deletion of data from computer media before disposal, or destruction of paper records before vacating buildings, for example.

The KTN recommends that organisations take more responsibility for ensuring data privacy.

Issues associated with privacy breaches are not those which can be addressed by users, they must be addressed by those planning, designing and implementing new IT systems.

Organisations must stop delegating responsibility for privacy issues to junior members of staff, it's a board-level issue.

The development of information systems and associated products must build privacy into every stage of the product development process. It is not sufficient to see privacy as a bolt-on to good design, integrated as a last-ditch effort to protect personal data.

Board-level issue

Organisations must stop delegating responsibility for privacy issues to junior members of staff. Privacy is a board-level issue and should be the duty of a senior decision maker with the power to make important changes at the highest levels.

The Cyber Security KTN believes that much further work is needed to develop privacy concepts. We will be holding an event in November that will look at privacy case studies. We have also commissioned a working group on the related topic of user-centric electronic ID, jointly with the Information Commissioner's Office and Technology Strategy Board. In the meantime, we welcome members of the IT industry to join the Privacy Engineering Special Interest Group of the Cyber Security KTN to help take privacy issues forward.

Excellence in Data Security and Compliance conference

High-profile data security blunders have an unsettling similarity to the proverbial bus scenario: a calm horizon for ages, then several come along at once. In this vein, just as the government was reeling from HMRC and the DVLA's data security indiscretions, as well as last week's débacle (in which secret documents containing assessments of Iraq's security forces and Al-Qaeda's vulnerabilities were left on a train), we learn that it has happened once again after a second set of secret government documents was left on another train. The documents included briefing notes for a meeting organised by the Financial Action Trust Force, an inter-governmental body which was created to combat financial crime and the funding of terrorism. An issue not only of data security, then, but of national security.

Following the spate of security blunders featuring not only governmental departments, but also well-known high street brands, it's more important than ever to know how to accurately assess, identify and manage risk to protect your company and client data. It is now equally more important than ever before to identify risk and understand and comply with DPA regulations, ISO and PCI-DSS standards, to not only protect your company and clients' personal and financial details but also avoid heavy fines.

The issues surrounding this area are many. As a security professional, what are the risks involved in outsourcing your security functions as opposed to keeping them in-house? How can you effectively communicate the imperative of data security to your staff at all levels to prevent leakage? How can you stay fully compliant with PCI, ISO 27001 and Sarbanes Oxley and transmit this compliance to your clients so as to ensure their renewed trust? And of course, there remains the perennial issue of financial viability and how to ensure board buy-in for new applications and processes around data security.

And where data breaches happen, where do these leaks occur? Well, forget hackers, the biggest issue this year, around security breaches, has been to do with poor internal security policies as opposed to the risks from external attacks, meaning that as a business, it is far more a case of the enemy within.

So how to take steps to overcome this enemy within and make sure your organisation's data is hermetically-sealed? From SocGen to SOCA, make sure your company is not the next one to hit the headlines for a breach in data security by attending SC Magazine's Excellence In Data Security And Compliance conference. Taking place on 16 September in London, this 3-stream event offers you the chance to absorb best-practice as well as learn from poor practice to ensure that you remain visibly and successfully compliant and secure. Book before 24 July & Save up to £100 @ **www.scconference.com** or call +44 (0) 20 8267 4011 for further details.

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

UCL

M.Sc. in Information Security

UCL s MSc in Information Security is an advanced programme for computer science, mathematics and electronic engineering graduates. The programme is organised around Computer Security, Cryptography and Digital Intellectual Property.

Programme Outline

- Cryptography
- Network security
- Computer security
- Digital Rights Management
- Operating systems
- People and security
- Systems requirements engineering
- Communications and networks
- Software engineering
- Human computer interaction

The programme is directed and supervised by Professor Ingemar Cox and Professor Yvo Desmedt .

Location

Students can enrol at either UCL s main Bloomsbury Campus or UCL s Adastral Park Campus in Martlesham, Suffolk. Most classes are taught from Adastral Park with live videoconferencing to Bloomsbury.

Contact Information

Brian Riley (0)1473 663 710

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


UNIVERSITY OF
OXFORD
part-time study
network security
trusted computing
systems design
security processes
people and security
msc in software and systems security
www.softeng.ox.ac.uk/security