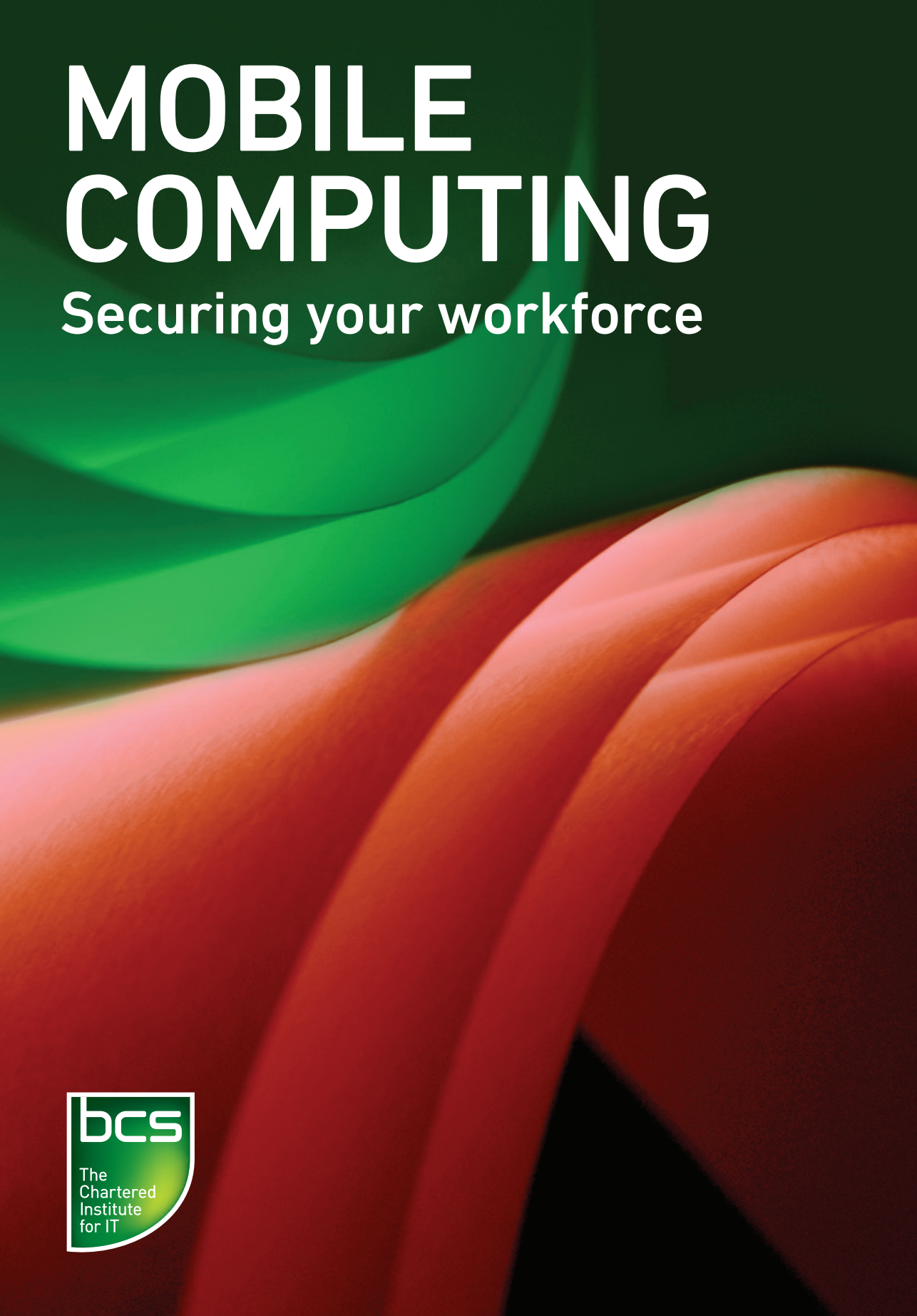
MOBILE COMPUTING

Securing your workforce



bcs
The Chartered Institute for IT

MOBILE COMPUTING
Securing your workforce



CONTENTS

	Foreword	iv
1	EQUIPPING EMPLOYEES, MAXIMISING POTENTIAL – Nathan Marke	1
2	CONSUMER DEVICES IN THE WORKPLACE: A BEST PRACTICE SECURITY APPROACH – Steve Durbin	4
3	SECURITY ON THE MOVE – Andrew Cormack	6
4	MOBILE SECURITY: MINIMISING RISK, MAXIMISING AWARENESS – Stuart Dommett	12
5	DELIVERING SECURITY ON EMPLOYEES' PERSONAL LAPTOPS – Nick Lowe	15
6	SAFETY TRAINING FOR THE WORKFORCE – Sean Glynn	18
7	CEOs IN THE DOCK – Sean Glynn	21
8	STOPPING THE MOBILE BOT THREAT – Lannon Rowan	25
9	PASSWORD SECURITY – Derek Melber and Anna E. Ryberg	28
10	ENCRYPTION IS SOMETIMES NOT ENOUGH Luther Martin	32
11	NFC: ANOTHER ONE FOR THE ACRONYM SOUP Andrea Simmons	35
12	NETWORK SECURITY WHEN GOING MOBILE – Gord Boyce	37
13	IMPROVING YOUR NETWORK AND APPLICATION ASSURANCE STRATEGY – Paul Vlissidis	40
14	MOBILE RULES FOR SECURITY OFFICERS: A 'CASE STUDY' Jane Grafton	43
	USEFUL RESOURCES	47

FOREWORD

It's been less than three decades since the first commercial handheld cellular phone hit the market. Costing some $3,995 and likened to a brick, it immediately gained a long waiting list. Price and size have come down in the intervening years and popularity has soared. The technology has moved from analogue to digital and the handsets can now do so much more than make and receive voice telephone calls.

We've seen the introduction of short message service (SMS), multi-media message service (MMS), PDA functions (address book, calendar, notes), email, browsing (WAP through to modern browsers), full internet access and applications. Each new capability has opened up additional potential exposures for users.

Modern smartphones combine elements of mobile phone, personal digital assistants (PDA) and laptop into a small, easily lost or stolen, high-value device. With e-wallets, NFC, tablets and so on, as well as storing more and more confidential information as storage capacity grows, its value – and impact when lost – increases even more.

Phones are not the only devices we're mobile with either. PDAs, laptops, tablets all add to the complexity, as does the growth in employees using their own devices and bringing them into the enterprise. Organisations need to cope, educate and secure.

Although manufacturers, operators, OS/application vendors and businesses try and control and/or secure their platforms, there are limits to what is technically possible and acceptable to users. Many people are no longer content with a device that cannot perform the functions or run the applications they see others use. Indeed, some will take exception to any level of control or security and 'jailbreak' or 'unlock' their devices so that they can run what they want on whatever network is available.

Whatever portable device you use, this ebook contains some useful advice to consider to help improve your mobile security.

Gareth Niblett
Chairman, BCS Information Security Specialist Group

1 EQUIPPING EMPLOYEES, MAXIMISING POTENTIAL

Nathan Marke, March 2011

Organisations are striving to implement supportive information and communications infrastructures to maximise employee collaboration, increase productivity and achieve efficiency savings. Equipping employees with the tools to work remotely and flexibly allows businesses to provide the best possible experience for their employees and customers whilst reducing overall IT spend, says Nathan Marke, 2e2's Chief Technology Officer.

WHAT IS A 'BETTER CONNECTED' WORKFORCE?

The IT industry has tended to use terms such as 'unified communications' or 'unified communications and collaboration' to define the ways in which the modern workforce can work together and collaborate. These abbreviations are fine, save that they tend to create a focus on technology rather than on people or process; hardly surprising given that they originate from the technical hierarchy in our IT organisations.

By using the term 'better connected workforce' we seek to draw attention to the ways in which technology may be used to provide a better working environment, one in which employees may be able to communicate via different media that are appropriate to the particular purpose (instant messaging for the quick, informal query; video conferencing for the discussion that may be enhanced by some level of personal contact; telepresence for the more immersive group interaction). In short, the better connected workforce is one that is not only equipped with the right tools, but one that is aware of how these tools can be used to make communication between individuals, groups and across organisations faster, more effective and more productive. The better connected workforce is thus able to be more costeffective and better placed to attain the benefits, not only of new technology, but of new and more flexible working patterns and structures.

'PROSUMERISATION'

This trend is accentuated by the effects of what is becoming known as consumerisation and 'prosumerisation'. These buzz words refer to the blurring of distinctions between consumer products and professional products. For example, whilst the iPhone would fit into the former camp and the BlackBerry into the latter, each is being used in the other's territory. A further example is the use of social networking products in the work environment (Twitter for marketing, Facebook for group updates etc.).

As a result employees now expect to be able to replicate the efficiency and ease of use of home apps in the workplace and to be able to move seamlessly from home to work without connecting to different systems. As business applications become ever more web-savvy and accessible via mobile browsers, we are starting to see a move in IT departments towards the allocation of per capita budgets, with employees being able to provide (and getting support for) whatever devices they choose. There is a risk that this trend creates a widening information gap between the 'haves' and 'have nots' (which is a challenge for all organisations and which mirrors a similar gap in society at large), but the momentum would seem to be unstoppable.

WHAT ARE THE BUSINESS DRIVERS?

There are a series of complementary drivers that are encouraging organisations of all sizes, both public and private, to consider how to create a better connected workforce. Firstly, there is the need for improved productivity; secondly, the push for cost effectiveness; and thirdly, the requirement to attract and retain the highest calibre staff. Common across these drivers is the requirement for staff to remain connected to business systems and be able to communicate effectively, whether in the office, at a remote site, at home or travelling. Work has become something we do, not somewhere we go. To create a better connected workforce, an organisation should implement flexible working methods, providing employees with the tools for the job and the systems they need to ensure the necessary training and support is firmly in place. These tools, which will exist in an IT infrastructure that is secure with highly available remote access, will include devices such as laptops, BlackBerries and Windows mobile devices. Additionally, there will be IP-based voice and video systems and flexible applications designed to operate in a mobile environment. The support systems will provide ongoing training, access to support services and the ability for staff to communicate with one another individually or in groups, using voice, video, email and blogs.

LOOKING FORWARD

As well as improving connectivity and flexibility, organisations are also aiming to achieve significant cost savings, either through major transformational programmes or single point solutions. These programmes increasingly demand software as a service (SaaS), hosted and cloud-based solutions that are more cost-effective than traditional in-house options and bring increased flexibility.

By investing in hosted and cloud-based solutions and equipping employees for flexible working, businesses are able to rationalise property estates, further reducing costs. Whichever combination of hosted, cloud-based or managed service is chosen, the enterprise must be able to deliver better quality service at lower cost. However, many organisations are still running costly legacy IT platforms, full of data that has become progressively less useful over time. To obtain even the most basic benefits from a collaborative, better connected workforce, these platforms need to be changed to support flexible working patterns and the applications and devices used for equipping employees. Businesses running old versions of Novell, Exchange and Notes must move to a single directory environment to provide the necessary platform.

There are many examples of businesses that have made an initial investment in IP telephony, instant messaging, presence-based systems and enterprise portals, but remain at the pilot stage – despite evidence from Gartner research suggesting that most organisations recognise they will benefit from equipping employees with the tools for flexible working. If these organisations were aware that, by diverting budget from redundant data storage and ageing infrastructure into new and innovative programmes, they could achieve an ROI of six to nine months, they might be more willing to move from pilot to full roll-out.

ENSURING SAFE END-USER ADOPTION

Any new technology must be supported by excellent staff training to ensure rapid end-user adoption – this must take place before the change so people know what to expect, during the change so that they are hand-held throughout the deployment (and their work is not affected) and after the change so they know how to access help and support. Equipping employees with the tools to work flexibly and when on the move requires security measures to be in place to reduce the risk of exposure to a minimum. Employees must be trained to appreciate the physical security risks (don't leave the laptop on the train!) and to keep locally held data to an absolute minimum. Recent heavy penalties for data breaches make this a priority, as does the need to retain customer trust. Strong authentication and policy-based control over access (enforcing the use of virtual private networks (VPNs), personal firewalls and antivirus programs) is therefore essential. Systems must be in place to ensure that remote or mobile devices are updated with the latest security and operating system patches before they access an organisation's system.

CONCLUSION

Organisations and enterprises that are investing in new collaboration architectures are showing real initiative at a time when it would be more palatable to simply reduce cost. By investing in the systems and tools to create a better connected workforce, an organisation will be able to benefit from a reduced cost base, a more efficient, effective and flexible working environment and the enhanced ability to attract and retain the best staff.

2 CONSUMER DEVICES IN THE WORKPLACE: A BEST-PRACTICE SECURITY APPROACH

Steve Durbin, October 2011

There is no doubt that, as consumers, we have fallen in love with our smartphones and tablets. As business professionals, many of us would like to bring these consumer devices into our working lives, if we haven't done so already. However, how do we safely use consumer devices as business tools, asks Steve Durbin, Global Vice President, Information Security Forum (ISF).

Many of the most popular consumer devices were not designed originally as business tools and do not offer the levels of security comparable to current desktop and laptop computers. In addition, the way we now use these devices is blurring the line between personal and business usage and behaviour, another area of concern for businesses.

Without adequate protection, consumer devices can expose organisations to a number of risks, all of which open up new routes for corporate data loss and ways for an organisation's reputation to be damaged. These include misuse of the device itself, outside exploitation of software vulnerabilities and the deployment and download of poorly tested, unreliable business apps. Symbian and Android are among the most insecure mobile operating systems (OS) and malware can find its way through via the OS or the apps downloaded onto the device and into the corporate system relatively easily.

PUTTING THE RIGHT TOOLS IN PLACE

However, by putting in place the right working practices, usage policies and management tools, organisations, regardless of size or type, can benefit from the greater flexibility, increased productivity and reduced costs that consumer devices can bring to the workplace, while minimising exposure to the potential risks.

Time is critical though, and businesses urgently need to formulate a response to this growing trend. In view of this, the ISF has worked with a number of its members – leading organisations round the world – to compile an objective, best practice focused approach to securing mobile devices.

The resulting Securing Consumer Devices report breaks down consumer device security into four manageable components: governance, users, devices and applications and data.

- **Governance:** Without control over consumer devices, organisations have little or no visibility of usage and penetration and poor knowledge of ownership, support requirements, adherence to policies or compliance. Furthermore,

- consumer mobile devices and apps are typically sourced from a wide variety of unapproved, non-corporate suppliers, with limited attention paid to service provision contracts.

  Organisations need to create a framework for ensuring correct and consistent mobile device security assurance. This involves getting an understanding of the extent of consumer device penetration and identifying the different device user groups, their requirements and the attendant risks. Organisations then need to agree a device provision mechanism, define policies around ownership, corporate access and acceptable use and identify any statutory requirements.

- **Users:** Without controls over consumer device working practices, users are free to combine work and personal tasks and data, with the risk of working in unsuitable locations and exposure to loss and theft. Users can potentially misuse or abuse the device through jailbreaking or disabling security features. They might also copy data to removable storage devices or use the device for making inappropriate calls or for downloading and sending offensive or inappropriate content.

  Organisations need to ensure employees are aware of what constitutes good working practice for mobile devices. As well as making consumer device security an integral part of awareness campaigns, organisations should create an acceptable use policy (AUP), which employees must sign. In addition, organisations should consider monitoring device usage and enforcing policy through disciplinary or financial sanctions.

- **Devices:** Without protection or management, consumer devices are exposed to a range of information security threats. These include: exploits by malware targeted at the device's operating system or apps; unauthorised connections; exploitation of software vulnerabilities by malware that exposes data or causes unexpected behaviour; compromise or irrecoverable loss of data.

  Technical solutions are needed to secure access to mobile devices and their contents. These include: enabling or installing functionality such as malware protection, firewalls and storage encryption; enforcing complex passwords; and enabling remote maintenance, upgrades and device wipes through a mobile device management (MDM) system.

- **Applications and data:** Applications on consumer mobile devices are mostly purchased or downloaded from an app store or software vendor. Often the provenance of the apps is unknown and they are unlikely to have undergone formal software development and testing or to be provided with proper documentation and upgrade regime. The apps may also lack activity reporting and logging, and typically provide poor data protection.

  Organisations need to make sure that apps used for business and the types of data they are able to access or generate are appropriate and properly tested. This might include going as far as developing apps in-house and building an organisation app store. This way, apps could be thoroughly tested and secured against malware infection or attack. Organisations could implement data classification to set limits on the type of data that can be accessed or generated by users on consumer devices.

The trend to 'consumerisation' of the workplace is fast moving and organisations cannot afford to stand still and allow mobile device adoption to run its own course.

3 SECURITY ON THE MOVE

Andrew Cormack, January 2011

Andrew Cormack is Chief Regulatory Adviser at JANET (UK) and is responsible for keeping the network and its customer universities, colleges and schools informed about the regulatory, policy and security requirements of running networks and networked services. Andrew recently took time out of his busy schedule to talk to Justin Richards of BCS about all things security and network-related in the run up to his presentation at the Real Time Club in January 2011.

What will you be talking about for your Real Time Club presentation?
I'll be starting from network security because it strikes me that that's what we've been doing for the last 15 years. We've done firewalls, we've done flow monitoring; everything is based upon being able to look at the network and saying, that's good, that's bad. I was at a conference recently where one speaker basically said that they've now given up on the user being a player in the security side of things – the user is just not involved!

If I count up all the networks my laptop has linked to recently, the free Wi-Fi one in this cafe is the ninth one this week, a hotel, three conferences, home, work, a couple of other cafes and so on. Which of those networks is supposed to be looking after my security in that model, where I'm not? And even when the network is responsible, it is quite difficult to work out what is good and what is bad, given that the client is moving around and many of the services are moving around, too.

If I'm using a cloud email provider, which country should my email traffic be going to? Is it going to be the same one tomorrow? If load changes and the cloud provider moves and they're resilient – that's what they do – the traffic patterns are going to change. It's not clear to me that the model of looking at the network and saying 'that's how we do security' is the way we should be doing things anymore. I'm therefore looking at the Real Time Club as an opportunity for talking about the things I don't know the answers to, so I'll be raising issues that interest me. I think I'll need to be provocative after two courses and some wine.

What do you think are the biggest challenges in the security field at the moment?
I think there are some big new challenges there – if we thought that networking and the web were getting rather routine, it's about to become not routine! It's becoming interesting again, and not just in technical terms. I can't see any way of avoiding putting some of the onus for security on the user, so we've got to provide them with the necessary tools, because we haven't got them at the moment.

My favourite last week was a message on my laptop that said 'the software has a problem and cannot exit'. I don't understand what I'm supposed to do with that and I'm supposed to be a technically competent person! We've got to get better at explaining security decisions to users. We still should be giving them [the user] some guidance, but I think the alternative is to end up with something that's completely constrained; there's been some debate as to whether certain commercial interests are now wanting to get rid of the open creative internet we have now.

I think there's a risk that regulatory bodies with their overwhelming desire for security will inevitably push for a less flexible internet. There's a lot of pressure now from government saying the internet must be secured (partly because of the Olympics), which will make it less flexible, so when the next application comes along (such as Skype, which just came along, didn't need permission from a network and took off to become an amazing technical, cost-saving social application, which has enabled so many more people to keep in touch cheaply) someone is going to turn round and say that's not secure, sorry you can't do it – it just won't have the freedom to take off like that again.

Do you think we'll ever have proper security on mobile devices?
I think, in general, devices aren't too bad. There's been a colossal change in Microsoft security during the 15 years that I've been studying it, for example. Back when I started off people complained because Microsoft never told them about their security problems and now people complain they're overloaded with Microsoft security updates about problems. However, I think my laptop gets less secure the moment I sit in front of it.

Do you think Wi-Fi networks need to be more secure?
Wi-Fi is just another network, and a network is just another network. The problem is, if you make it too secure you risk delaying moving the packets of information around and so, as you sit in a cafe, what you want to do won't work. This happens fairly regularly in hotels and in conference centres where fewer ports are open, hence there's a greater delay in data transfer. Some centres will use one security measure, which will then in turn prevent me from using mine.[…]

What is your definition of acceptable risk?
I know what my definition of acceptable risk is, but I'd be very nervous if someone tried to tell me what it was.

We use a lot of infrastructures in our daily lives that aren't perfectly safe – I mean there was a doubt that I'd make it today because the trains might have gone on strike, but if they had, the world wouldn't have come to an end. When it snows, transport networks will stop working, but we don't regard it as being a catastrophe for society. I haven't looked at the figures recently, but I think the road network in this country kills about eight people a day, whereas the internet is really quite safe when you compare it with those sorts of numbers and yet, as a society, we panic about internet security.

At some point I think we're going to have to work out what it is we actually want. Do we want an imposed level of risk where somebody, perhaps the government,

decides what an acceptable level of risk is – a bit like the Apple store where, unless something is approved by the equipment vendor, you can't run it? You might find that approved software will have a lot of options stripped out of it because the user can't be trusted, on that model, to use them safely. Something as basic as email allows me to send my credit card number to somebody; at what point do you put in a point of control that says 'no you can't do this Mr User, I am going to deny you that option because it's not an acceptable risk'?

We've been there before – the telephone network used to work like that, where you couldn't plug in a telephone handset unless it was BT approved. Do we follow the car model where you have to go in for an MOT on your computer every year and you have to be insured against going onto the internet without a properly secured computer? These are all models that might work, but they're not the internet as we know it.

Perhaps we should say that we users have got to start taking more responsibility for our actions and act smarter. It used to be said that people's personalities used to change when they got into a motor car, but these days they change when they use a mobile phone – how many overly loud conversations do we have to listen to on an average train journey now? But I don't know which model will work in the long term.

Surely security will always be a compromise? Outsourcing and offshoring are good examples of where organisations have to trust their vendors and partners to take security seriously.
Sure, sometimes I have to remind myself that security is all about confidentiality, integrity and availability, and a system that I need to get at and I can't is actually a security failure. It's really easy, particularly for people from technical backgrounds, to focus on the integrity and confidentiality areas of security to the point where the user can't get at their information so the user starts inventing new ways to get their job done; I think we're there in many cases.

Do you have any advice for project managers on how to avoid these problems?
I guess they should try to see the whole picture of what users are going to expect. There are a series of words that are bandied about regarding user requirements, user wishes and user expectations. I suspect it's the expectations that are the most important – you can write down the requirements and the user will still say this product doesn't work the way their intuition tells them it ought to and it's really hard working against people's intuition. So my favourite approach for getting people to do things has always been to try and match up their intuitive expectations with what you want them to do. I try to avoid saying no and say 'wouldn't it be easier to do it this way instead?'

There used to be a common scenario at universities whereby academics requested wireless access for their offices, someone said no, so the academics would go down to the high street, buy an off-the-shelf access point and plug it in. So now your network traffic is potentially accessible to anyone with a laptop, with wireless access, within a hundred meters (with a little tweaking of course)! So how have we improved security in that scenario?

I guess this is always going to be a problem with people wanting to open up communication channels with each other, for example, smart jewellery[1] where users want to pass personal information to each other without much thought for security?
I think the decision is the tricky bit – we're not good at actually formulating what our intuitive rules are. We all have rules for 'Am I in a safe place? Is this a safe action? Is this somebody I trust?', but actually writing them down, in a way they can be implemented by a machine, is very difficult – for example, the endless difficulties that Facebook has had in order to produce a set of privacy tools that matches what people want.

And it's not just Facebook – recently TalkTalk got into trouble over its network security because they were keeping a record of the websites visited by their user community.

My understanding is that there's no link back to which user visited which website – they've just got a long list of all the websites visited by their users and they're scanning those to see if there's any malware on them – an excellent security initiative by the network, but they got into trouble for privacy.

I can see how that idea got through all the checks as a wonderful enhancement to customer security and the customers then turn around and say 'Oi! You're monitoring my web browsing'. They're not, but they get beaten up for it. It's a catch 22 situation. So in relation to the project management question, I'd say beware of these types of things lurking to bite you; your users might actually be irrational and might work on feelings every now and then.

You'll always get a very vocal minority who'll complain about pretty much anything...
Yes, that's true, but the problem is you don't know what the silent majority are thinking. Are they with the complainers or are they silent because they can't be bothered, or because they haven't noticed, or because they're happy? That's always hard to ascertain.

In your proposal for the Real Time Club talk you mention incident detection tools. Could these help mobile and cloud security in the long run?
Yes, but only if you can understand what they are – what an incident looks like. Originally they were a bit like antivirus: there were patterns that helped to identify when a particular pattern represented an incident. That's fairly accurate, but by definition it could be something else too, so a new incident goes straight past it. But now we're trying to look at mechanisms that will detect patterns that are probably incidents, but then what do you do? Do you block it? In which case you might not have blocked an incident but someone playing with the next Skype. How do you make a decision on what you don't fully understand?

There's some stuff on the internet and we know exactly what it is and it's fine. There's some other stuff we know exactly what it is and it's not fine and then a whole host of stuff in the middle. What do you do with that? Do you stop it until you know it's safe, in which case you're back at the old telephone system level ('until this has been approved it can't run on my network'), or do you say, 'well, we don't know it's hostile, but we'll keep an eye on it and run some new stuff ourselves and explore it'? But then you're leaving a window of vulnerability open. Again it's

this question of who do you want regulating it and how heavy do you want the regulation to be. […]

Would you say that giving users the incentive to do it right is one of the main challenges your sector faces over the next few years?
Yes. In my job it is about trying to keep regulation steered in a direction that enables people to have the expected results, and desired results, and flag up, as early as possible, if we spot things going wrong.

With the best intentions you create a law, a policy or technology that you think will have result X and it turns out to have result Y. There's a lot of suggestions around the idea of forcing service providers to block access to stuff that we don't think is socially desirable. That works fine as long as users are in agreement that they don't want to see it either.

The moment you try to block something that users do want to see – for example, the French have recently forced ISPs to block access to offshore gambling sites – doesn't that give the users a strong incentive to get around the block? And the moment they work out how to get around it, they're going to be exposing themselves to all the stuff that was blocked, which is the stuff they didn't want to see, the stuff that was threatening their computers. The blocks may well be blocking phishing sites, dodgy ISPs (these get blocked from time-to-time quietly), so if you give people the incentive to get around the blocks and you can't get round the one without getting around the other, you will defeat them as a security tool. I'm trying to point this problem out, saying that we will be encouraging people to evade the security measures, which is not good.

What do you think have been the most important changes in the IT industry during the last three or four years?
I think the continuing development of the mobile device, from laptops through to mobile phones. The incredible functionality that we now have – always on, always with us and getting connectivity wherever we can find it. I think that's a huge social change. I don't understand many of the things that people are using socially. They're often not particularly useful for my job, they're just different, but trying to understand how much of it is ok, what the possible risks might be and then express it in a way where individuals can make their own rational choices – 'this is something I want to do, this is something I don't.'

What's your take on professionalism in the IT industry?
IT is part of the bedrock of modern life; IT isn't just for geeks any more, and it hasn't been for a long time – it's for everybody. So it's increasingly important that it doesn't just work for geeks, that it's usable for everybody in society – that's a different set of design goals. On the other hand, we also need to be helping everyone in society; I know BCS, for one, does a lot at graduate level. But it's not just graduates that use computers, it's everybody.

I heard a lovely comment recently from someone who works in the schools sector: they said 'there are no motor cars in schools, but we still teach children how to cross the road safely.' And I think we need to do that sort of thing for the internet as well,

to be honest. I think children need to be able to handle the internet by the age of 10, because they're going to be on it. […]

In your current role, what would you say is the most rewarding part of your job and what's the hardest part of it?
I'm very lucky – I have a lot of fun. I do stuff that's interesting and intellectually challenging. The most rewarding part, for me, is helping to enable people to do stuff that they couldn't previously do. For example, my work on privacy – where it was good to help people to understand that being engaged in privacy doesn't mean you can't do processing, you just have to think a bit and ask yourself, 'do I actually need this great long list of personal data to do my job?'

They should be asking, 'can I use some clever technical stuff and quite possibly get a better result?' But it comes down to how everyone wants to work – you can be far less intrusive through good use of technology. You can actually massively reduce the privacy intrusion and still deliver the licence terms that the customer requires.

Not much is hard, but a lot is challenging, particularly when dealing with the law. But you have to persist and I can now point at certain bits of the law and say that is there because of me, although they're very small subclauses, but getting them there takes an extraordinary large amount of effort.

Looking back is there anything you would have done differently, or are you fairly happy with your chosen career path?
I would have liked to have been a better people manager, but I'm starting to pick up on the fact that security people are rather hard to manage, for anybody. So perhaps it wasn't entirely my fault!

Full interview at www.bcs.org/content/conWebDoc/38622

NOTES

1. For some more information on 'smart' or electronic jewellery, have a look at 'A trip to the future' by Dr Ian Pearson.

affects everyone's pockets. The most effective strategy is to complement sensible, workable policies with centrally controlled security technology, combined with trust, education and understanding:

- Educate the whole workforce (not just those considered as mobile) to the risks posed by their activities and the devices that they use.
- Dictate the management of all mobile devices, irrespective of ownership, in a security policy.
- Specify that all staff members sign the security policy to ensure they will not download unnecessary sensitive information, nor will they disclose this information to a third party, and make sure the appropriate software is in place to enforce the policy.
- It should never be left up to the end-user to make data secure – they don't have the time or the knowledge and it certainly wouldn't be considered as 'reasonable and appropriate' (the underlying theme of mobile security regulation) if the device, and the data it contained, was lost or stolen.
- Encryption software is now available that can protect data on virtually every end-point. The ICO will require some form of evidence of data security so the ability to prove it is paramount if a £500,000 penalty is to be avoided. By using a solution that includes a central management console, every device, regardless of type or ownership, is protected and can be tracked.
- Make users of iPhones and other smartphones with full mobile internet access aware of the risks of opening attachments or clicking links to potentially malicious websites and ensure the device's firmware (operating system) and browser are updated to the latest version and patched with any security upgrades.

Companies, now more than ever, have got to protect their intellectual property and employees must play their part by respecting the information they are working with and correctly using the devices they're accessing it with, for everyone's benefit.

BCS THE CHARTERED INSTITUTE FOR IT

Our mission as BCS, The Chartered Institute for IT, is to enable the information society. Wea promote wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

Our vision is to be a world-class organisation for IT. Our 70,000 strong membership includes practitioners, businesses, academics and students in the UK and internationally. We deliver a range of professional development tools for practitioners and employees. A leading IT qualification body, we offer a range of widely recognised qualifications.

Further Information
BCS The Chartered Institute for IT,
First Floor, Block D,
North Star House, North Star Avenue,
Swindon, SN2 1FA, United Kingdom.
T +44 (0) 1793 417 424
F +44 (0) 1793 417 444
www.bcs.org/contactus



© 2011 British Informatics Society Limited

The right of the author(s) to be identified as author of this work has been asserted by him/her in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988. All rights reserved. Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted by the Copyright Designs and Patents Act 1988, no part of this publication may be reproduced, stored or transmitted in any form or by any means, except with the prior permission in writing of the publisher, or in the case of reprographic reproduction, in accordance with the terms of the licences issued by the Copyright Licensing Agency. Enquiries for permission to reproduce material outside those terms should be directed to the publisher.

All trade marks, registered names etc. acknowledged in this publication are the property of their respective owners. BCS and the BCS logo are the registered trade marks of the British Computer Society charity number 292786 (BCS).

Published by British Informatics Society Limited (BISL), a wholly owned subsidiary of BCS The Chartered Institute for IT, First Floor, Block D, North Star House, North Star Avenue, Swindon, SN2 1FA, UK.
www.bcs.org

PDF ISBN: 978-1-78017-111-1
ePUB ISBN: 978-1-78017-112-8
Kindle ISBN: 978-1-78017-113-5

British Cataloguing in Publication Data.
A CIP catalogue record for this book is available at the British Library.

Disclaimer:
The views expressed in this book are of the author(s) and do not necessarily reflect the views of BCS or BISL except where explicitly stated as such. Although every care has been taken by the authors and BISL in the preparation of the publication, no warranty is given by the authors or BISL as publisher as to the accuracy or completeness of the information contained within it and neither the authors nor BISL shall be responsible or liable for any loss or damage whatsoever arising by virtue of such information or any instructions or advice contained within this publication or by any of the aforementioned.

Typeset by Lapiz Digital Services, Chennai, India.