DATA
WHERE IS IT?
HOW SECURE IS IT?
WHO CAN ACCESS IT?
Manage the Full Lifecycle of Your Software Assets with Flexera Software Solutions

 Enterprises face many obstacles in their efforts to use software assets effectively and gain maximum value from them. Thousands of applications may be spread across multiple business units and geographic locations. Those applications change constantly as IT rolls out upgrades, patches and new applications. Moreover, licensing terms, conditions and use rights differ from one application and from one vendor to another.

Flexera Software solutions help companies manage application usage – from request to deployment to licence compliance and spend optimisation - throughout the software lifecycle.

AdminStudio® Suite powers an enterprise’s Application Readiness process, streamlining and accelerating migration to Windows 7 and 8, virtualization of desktop and server applications, mobile application management and day-to-day application packaging operations. It removes a major barrier to cloud adoption by automating the assessment, conversion and publishing of multiple virtual formats to both physical and cloud environments.

App Portal makes the enterprise online app store a reality. With App Portal, users benefit from on-demand software provisioning that delivers all the advantages of self-service while giving IT complete control of request, approval and fulfillment.

FlexNet Manager® Suite for Enterprises is a comprehensive, proven, next generation software asset management, licence compliance and licence optimisation solution. The Suite provides entitlement based licence management and optimisation to enable organisations to reduce ongoing software licensing costs and maintain continuous licence compliance.

To learn more visit www.flexerasoftware.com

DATA

08 DATA RETENTION WRANGLING
10 DATA COLLECTION DANGERS
14 RISK ASSESSMENT
16 DUDE, WHERE’S MY DATA?
18 CLOUD REGULATION

LEARNING AND DEVELOPMENT

42 DEVELOPING AND MENTORING
44 TECH MEETS TRADITION

HEALTH

46 INTRODUCTION TO BCS HEALTH
47 EMAIL ARCHIVING AND HEALTH

SECURITY

24 SCoE UPDATE
26 SECURE DEVELOPMENT
28 PAYING THE PRICE
30 PERSISTENT THREATS
32 MAINTAIN INTEGRITY
34 HOW SECURE IS SECURE?
36 SOMEONE IS WATCHING YOU
38 SECURING TRANSACTIONS
40 SECURITY BALANCING ACT

LEARNING AND DEVELOPMENT

42 DEVELOPING AND MENTORING
44 TECH MEETS TRADITION

HEALTH

46 INTRODUCTION TO BCS HEALTH
47 EMAIL ARCHIVING AND HEALTH

SECURITY

24 SCoE UPDATE
26 SECURE DEVELOPMENT
28 PAYING THE PRICE
30 PERSISTENT THREATS
32 MAINTAIN INTEGRITY
34 HOW SECURE IS SECURE?
36 SOMEONE IS WATCHING YOU
38 SECURING TRANSACTIONS
40 SECURITY BALANCING ACT

The current year and two previous

years’ subscription prices from Oxford

University Press can be obtained from

Periodicals Service Company, 11 Main

Street, Germantown, NY 12526, USA.

E psc@periodicals.com

T +1 518 537 4700, F +1 518 537 5899

For further information, please contact:

Journals Customer Service Department,

Oxford University Press, Great Clarendon

Street, Oxford OX2 6DP, UK.

E jnlscustserv@oup.com

T (and answerphone) +44 (0)1865 353 907

F +44 (0)1865 353 485

The opinions expressed herein are not necessarily those of BCS or the organisations employing the authors.


COPYING: Permission to copy for educational purposes is allowed free of charge or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage; BCS copyright notice and this notice is given; and notice is given that copying is by permission of BCS.

To copy otherwise, or to republish, requires specific permission from the publications manager at the address below and may require a fee.

Printed by Rotolito Lombarda, S.p.A


BCS The Chartered Institute for IT

First Floor, Block D, North Star House,

North Star Avenue, Swindon, SN2 1FA, UK.

T +44 (0)1793 417 424

F +44 (0)1793 417 444

www.bcs.org/contact


Liz Bacon

BCS President

Paul Fletcher

CEO

Feedback

email: editor@bcs.org

For payment details and terms and conditions, please see:

www.oxfordjournals.org/our_journals/combul/access_purchases/business/start.htm
BAREFOOT COMPUTING PROJECT

With almost 3,000 teachers from over 800 different schools in England having received training via the Barefoot Computing Project since its launch last summer, BCS, The Chartered Institute for IT is pleased to announce that the scheme is to be extended.

BT has agreed to support the project from March until the end of this school year. The scheme was due to end in March, but given its popularity to date, BT is pleased to announce it will be working with BCS and Computing At School (CAS) to ensure that it continues to run through the summer term.

The Barefoot training workshops are run by volunteer professionals from the IT/computing and education sectors. These events introduce the new computing curriculum to teachers and explain the support available to them through Barefoot and other related projects.

The programme of events will help equip teachers with the skills and knowledge needed to incorporate the computer science elements of the new computing curriculum into their lessons. By providing high-quality cross-curricular computer science resources for primary school teachers, supported by explanations of the key computing concepts, we are providing support for teachers who may have little previous knowledge of computer science. A list of teachers are already introducing many of these concepts in to their classrooms without realising it and we want them to see that it’s not as complicated as they may think.

For more information about the scheme contact: paul@barefootcas.org.uk (BCS, The Chartered Institute for IT).

WELCOME REVIEW

BCS, The Chartered Institute for IT, welcomes the review of the accreditation of computer science courses in UK universities announced by the Department of Business, Innovation and Skills.

Paul Fletcher, Group CEO of BCS, The Chartered Institute for IT, said: ‘It’s very important that university accreditation should undergo regular reviews to ensure that courses offer students the best opportunities. We are pleased that computer science is the first course to be reviewed as this reflects the importance of this discipline today and in the future.

As an accreditation body, we welcome this focus; however, we want to ensure that the review considers all factors. Employability is critical as one of several measures that need to be taken into account; the ability for universities to drive social mobility by helping students from under privileged backgrounds is also important.

We will be working with Tech Partnership, employers and universities to discuss these issues and how we can help ensure students have access to an education that provides them with the skills for a career both at the end of their course and a professional career over the long-term.

For computer science courses specifically, this means that we champion the teaching of the principles that underpin computer science rather than specific technologies. By being part of this we will be able to adopt the best practice standards that are recognised across the globe.

He added: ‘The scheme will also help individuals map out their career paths and identify how they fit with the industry standard Skills Framework for the Information Age (SFIA). By doing this, they will be able to identify what they want to achieve in their own careers and how they can achieve it.’

http://teamtalk.bcs.org.uk
Tell us a bit about your background.
I’ve spent the last ten years at RM Education where I was Group Managing Director, Education Technology. My time there was about getting tech into schools and universities in the UK and solving the problems that arise where education and technology meet. Before that I spent some time in consultancy, which followed on from seven years in the aerospace industry. Those are the first three chapters of my working life – I view BCS as the fourth.

What attracted you to BCS?
It felt like a natural progression for me, the right time to move on to keep things fresh. There is a big crossover with RM, with both the education and technology focus, and I genuinely think I have something to offer. I also liked the opportunity to work in a not-for-profit organisation, a sector I had not been in before. The laudable purpose of the Institute was relevant in my decision-making so, although like everyone I need to make a living, I like the idea of an organisation whose purpose and aims I share.

What does BCS do well at the moment?
We have an unrivalled market position and a mandate created through legacy and the charter. ‘We have an unrivalled market position and a mandate created through legacy and the charter.’

to various Institute meetings I have found that the amount of effort people put in is humbling – I’ve been really impressed that our BCS people are so interested in giving back to their profession that they give their time for free.

What should the organisation be doing more of, or better, than what you’ve seen so far?
We pursue too many projects and so far? when you look at what we do and its alignment with our organisation’s purpose, the connection is sometimes tenuous. This means we are spread a bit thinly and that, in turn, reduces our impact. Likewise, we need a stronger voice on the big technology issues that are impacting society. We need to have an opinion, and that could even be controversial if needs be. For example, the tension between the safety of the UK in the context of the terrorism threat and people’s understandable concerns about privacy – this is something on which we should facilitate debate.

Is the breadth of the royal charter a problem?
I don’t think so, it is in old English but the fundamental principles still hold true.

What is the executive team’s vision for near future?
When I came in I first wanted to work with the team to deliver services for the members this year and hit current targets. Last year’s small financial surplus was good, after all we need the commercial activities to be successful to allow us to invest. And that investment is not only in systems for members and products, but so we can fulfil our mandate to society. Some of our intellectual property is now getting a little old – so that needs work as well.

And the longer term?
It is time to refresh the BCS’s vision and strategy. The executive team, alongside the boards and council, have been working on this and we have a revised purpose and new strategic pillars to inform the vision. We will be saying more about that in the near future.

‘We need to have an opinion and that could even be controversial if needs be.’

The more of relevance we have to say, the more we can feedback into useful products, and the more we network the better what we have to say is. It goes round in an ever-improving loop. There is plenty for us to talk about. People are concerned about IT; it’s so prevalent in society.

People want to keep their kids safe, they are concerned about privacy, the legal and regulatory areas have a lot of challenges ahead, some are worried about unchecked AI research.

And this goes way beyond technology to societal impact, ethics and our way of life in general.

What upcoming tech excites you most?
Technology that continues to drive efficiency. For example the internet of things can distract you with its consumer applications, but actually it can make a real and more basic difference in industrial applications. Also, the way our children learn is fundamentally changing – AI, if used properly, can be used to assist in this.

Will traditional classrooms die?
I like the Ted Talks. For a daily read I turn to Tech Market View. Then I cherry-pick anything related to tech and education, apprenticeships, digital skills and so on.

Personal philosophy?
It’s about authenticity – you need to understand who you are, your strengths and weaknesses – and be yourself. Tell people what you think.

QUICK QUESTIONS

What tech couldn’t you live without?
My iPhone and iPad.

What gadget would you want if you could have anything?
I hate traffic – I’d pay money to have reroutes traffic and keeps it flowing.

Mac or PC?
PC, but, as above, Apple devices. iOS for mobile and a Windows desktop.

Killer app?
For me it’s about connectivity, email, Facetime, texting. As I travel a lot I want to stay connected.

Netflix or Amazon Prime?
Both. Terrestrial TV is dying. No-one wants to sit through adverts, they just want good programmes when they want them. At the moment I am watching Prison Break.

Favourite blog?
I like the Ted Talks. For a daily read I turn to Tech Market View. Then I cherry-pick anything related to tech and education, apprenticeships, digital skills and so on.

What do you think the BCS’s current vision is?
It is time to refresh the BCS’s vision and strategy.

And the longer term?
It is time to refresh the BCS’s vision and strategy.

Would you like to see more of that?
Yes, I would like to see more of that.

What do you think the BCS’s current vision is?
It is time to refresh the BCS’s vision and strategy.

And the longer term?
It is time to refresh the BCS’s vision and strategy.

Would you like to see more of that?
Yes, I would like to see more of that.
RETENTION WRANGLES

Charlotte Walker-Osborn, Partner and Head of Eversheds’ Tech, Media and Telecoms Sector, talks about a couple of hot topics relating to security in tech and media.

A new Counter-Terrorism and Security Bill (the bill) was introduced to the House of Commons on 26 November 2014 that will, among other things, allow the government to require communications providers to retain data necessary to attribute an IP address to an individual.

What? Earlier in 2014, the European Union’s Data Retention Directive was found to be invalid. The government passed a new Data Retention and Investigatory Powers Act 2014 (DRIPA) in order to replace the Data Retention regulations 2009 (2009 Regulations), which had implemented the EU Directive and was at risk of being found invalid. DRIPA contained various amendments to the Regulation of Investigatory Powers Act 2000 and set out a new regime for the retention of communications data.

Among other things, DRIPA amended the definition of telecommunications service to cover services that consist of, or include, facilitating the creation, management or storage of communications, catching over-the-top players, internet mail providers and social media businesses who may not have been required to retain communications data under the 2009 Regulations.

The bill makes certain amendments to the provisions of DRIPA including the definition of ‘communications data’. Providers may now be required to retain internet data that relates to internet access services or internet communications services and may be used to identify or assist in identifying which IP address or other identifier belongs to the sender or recipient of a communication (whether or not a person). The effect is that providers that are potentially required to retain communications data may now need to attribute IP addresses to individuals or devices or retain information to assist law enforcement authorities to identify the users of certain telecommunications services.

So what? In some ways, the new requirements do not go much further than the existing requirements of DRIPA. For example, internet access providers could already be required to retain IP address details.

However, providers may be under a higher obligation to retain such data and, unlike in the 2009 Regulations, there is no defence for a provider in the event that another organisation is already retaining the relevant data.

The requirement for data to be collected and retained to attribute IP addresses and other internet identifiers to recipients and senders may well be controversial given that providers need to comply with the data protection laws and regulations with respect to the communications data that they retain. Much will depend on how draconian the government will be in issuing data retention notices under the amended DRIPA.

While DRIPA, and previous bills proposed by the government on the subject of data retention (including the Communications Data Bill from 2012), have been the subject of great debate, the new focus of the new bill has been on the wide-ranging powers that the government has requested including the power to place universities under a statutory duty to prevent people from being drawn into terrorism. Line by line examination of the bill took place during the final day of committee stage on 28 January 2015. Amendments discussed covered clauses 21, 22, 24, 25, 28, 30, 32, 34, 36 and 42 of the bill. At time of writing, the report stage – further line-by-line examination of the bill – was scheduled for 2 February 2015. Whatever form the bill finally takes, there is little doubt that the government will continue to push its agenda for greater powers in relation to communications data.

Recent studies on cloud computing suggest that security concerns are still hampering the adoption of cloud computing. BT, Fujitsu and Netspoke recently commissioned studies which, predictably, revealed that confidence in the security of the cloud is at an all-time low. Despite the predictable results, these studies will provide cloud computing services providers with insightful prospective customer feedback.

In September, BT published the results of a study it commissioned that explored the attitudes to, and use of, cloud-based services of IT decision makers from enterprise organisations in 11 countries. BT reported that three quarters of those surveyed (74%) cited security as their main concern about using cloud-based services. Despite security being a major concern, surprisingly, 50% of those surveyed admitted to adopting mass market, consumer cloud services, rather than those designed specifically for the enterprise.

Fujitsu’s study reported similar findings. The study, ‘Two Years On: The Financial Services Landscape: Is your organisation super-powered?1, follows up on a 2012 study. 176 IT decision makers were surveyed at a range of financial sector firms. The study found that, two years on from the last survey, less than a quarter of financial sector firms have implemented cloud computing and of those who either use cloud or plan are planning to do so in the future, nearly half (42%) said that they believe that it opens up too many security threats.

The Netspoke commissioned study, Cloud Multiplier Effect in European Countries, reported similar findings to those of the BT and Fujitsu studies. Just over half of the respondents did not agree that their organisation’s cloud service use enabled security technologies to protect and secure sensitive and confidential information and 72 per cent said these cloud service providers are not in full compliance with privacy and data protection regulations and laws.

As expected, and in line with concerns over security, the studies suggest that it tends to be non-sensitive data and non-business critical processes and data that are being hosted in the cloud.

For example, Netspoke found that, on average, only 23 per cent of a business’s critical applications are in the cloud and only 10 per cent of sensitive or confidential data is stored in the cloud. Whilst Fujitsu found that around three quarters of those using cloud do so for internal operations.

So what? For those parties who supply cloud solutions, the results of the surveys provide insightful prospective customer feedback which can be used to tackle certain barriers to the adoption of cloud computing, including security.

For those procuring or considering procuring cloud, it will be interesting to see how suppliers deal with the continuing concerns around security and data. This is an area I will be taking an in-depth look at in a future briefing this year.

To help enterprises better understand the cloud, the International Organisation of Standardisation (ISO) has recently released two international standards on cloud computing. ISO/IEC 17788 and ISO/IEC 17789. ISO/IEC 17788, Cloud computing – Overview2 and vocabulary, provides definitions of common cloud computing terms, including those for cloud service categories such as software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS). It also specifies the terminology for cloud deployment models such as public and private cloud. ISO/IEC 17789, Cloud computing – Reference architecture3, contains diagrams and descriptions of how the various aspects of cloud computing relate to one another.

Whilst many reading this article will find the standards potentially quite basic for them, these standards will be significant in helping a number of organisations’ understanding of the cloud and are expected to pave the way for more technical standards dealing with issues such as security.

www.bcs.org/security

References

Andy Smith from the BCS Security Community of Expertise examines the security risks of data aggregation and mining. The BCS Security Community of Expertise and more specifically the Identity Assurance Working Group have been looking at various subjects related to online security.

One of the issues that is becoming much more serious is the ability for organisations, including sales and marketing departments, advertising companies and serious organised crime, to use data aggregation and data mining to their advantage and to target individuals.

Aggregation is the collecting together of individual items of data or databases to form large sets of data, for example, bring together social media accounts, internet searches, shopping preferences and email for millions of people.

Data mining is taking a large data set and using tools to search for particular words or phrases, then narrowing the search with combined search terms to find individual records of interest. For example, searching the vehicle database for a car registration number for a car in long-term parking at Heathrow and using the name results to search for travel details, electors and school databases for other people living at the address.

Targeted online marketing can be aggressive and unwanted. We are all victims of spam, ad-ware and other unwelcome methods of trying to separate us from our money. However, most online marketing is actually good and welcome. Targeted marketing can be very useful, but to achieve this, the advertising organisations need to track and hold a significant amount of information about a person.

Some of this can be personal such as age and where you live. When they are tracking spending profiles and the types of products people buy this can become very sensitive. Basically they are gathering (aggregating) huge amounts of information and then mining this for marketing purposes.

However, there are laws to protect the public from aggressive marketing, invasion of privacy and to ensure data protection. This is especially true in Europe, including the UK. These laws cover the type of data that is held and ensure it is properly protected, and to a certain extent, not misused. But this only applies to reputable companies and those in jurisdictions covered by such laws.

Applying the same capability to organised crime and you have a wholly different and much more serious problem. Between the law-abiding professional organisations that provide useful advertising services on the internet and organised crime there is a spectrum of organisations ranging from slightly aggressive targeted marketing to malicious code authors that install ad-ware on your machine to replace official adverts with nefarious ones.

This is one major area of data mining and the one most people think of, but it is not the only one. Organised crime, terrorist organisations, investigative journalists and private investigators all use data sources on the internet and data mining tools to find and target people.

It is amazing what is now achievable from knowing small snippets of information and using these as keys in different databases, which give further bits of information, which in turn can be used as search keys in other databases.

Given large aggregated data sets and the right search terms, it’s possible to find a lot of information about people including information that could otherwise be confidential, for example, that someone is having an affair.

In democratic societies with good governance and oversight, it is not unreasonable for law enforcement to use large government databases to track and find criminals. Knowing a car was used in a crime, finding the owner and tracking the driver at the time is something expected in the UK. However, in oppressive regimes this can now be used for suppressing human rights, such as finding a posting on a news group that goes against the regime and using the IP address to find the service provider, then the credit card details to find the poster, even though they thought their posting was anonymous.

It’s easy to find people, even if you have a pay-as-you-go tablet, it really depends on whether it is worth the time and effort, which in most cases it is not.

Take, for example, a hacker managing to get into a loyalty scheme databases. It would be easy to mine the data and identify alcoholics, newly pregnant women etc. This is why certain large supermarket chains put huge amounts of effort into protecting their databases. The security controls do not just stop unauthorised access, they stop authorised staff doing unauthorised things. The security controls on some of these databases are better than those on military databases.

The trouble is that not all organisations do such a good job of protecting their data. Worse still, individuals are very bad at protecting their own information. One aspect of preventing data mining is helping the naïve protect themselves online, for example, parents protecting their children, as the children do not understand the implications of giving out sensitive personal information.

So what can organisations do? The first thing is to recognise where information is being aggregated. This can apply to one database or dataset, but it is also important to look at that dataset in the context of related datasets. By itself, a database of customer details in a CRM system may not seem that sensitive, but when related to other databases it may be possible to extrapolate additional information such as someone with an addiction.

Having decided that a dataset aggregates to something more sensitive than the sum of the individual entries, additional controls need to be added to address the aggregation. Information may be classed as personal if its one entry or one million. But losing a copy of one entry should have a much lower impact than losing a copy of a million entries, especially if it includes credit card information or
other sensitive data. Even if from a basic business impact perspective, having to send a letter to one customer to say their credit card has been compromised may cost £1; letters to a million customers on the other hand...

The key controls are already there, but they should be enhanced for aggregated data. Access control should ensure only authorised people have access to the data, but do staff need access to all the data to do their job or just some of it? If they only need regional data, or access to single entries at a time, then the authorisation should be configured to enforce this policy. More importantly the accounting should be of sufficient quality that it can be used as evidence in a court, should legal enforcement be required.

Accounting is very important in dissuading people of stepping over their remit. Just because someone can do something, it does not mean they should. The ability to look at all records in a database does not mean a member of staff should start looking at details about their neighbours or famous people.

There may be some records in a database that you want to add a flag to. Well known people are obvious examples, but also company directors may be deemed sensitive and could be flagged. By this I mean using a host-based intrusion detection system or other method to alert security if someone looks at a particular record. They would have a list of those authorised to do so and would pay a visit to anyone who was browsing.

If databases have search functions there are also controls that can be put in place to reduce or prevent data mining. Putting a specific type of proxy in front of the database that prevents more than a set number of searches or only allows a small number of records to be returned at a time can help. If people only need to see single records to do their job, why would you permit multiple records to be returned?

It could also prevent wildcard searches on the database or limit the search keys. Banks do this very well. When a person contacts the bank via a call centre, the advisor will look up the record for the person based on, for example, postcode and surname. They will then be prompted for information that only the caller would know. Without this the record cannot be seen.

The other control is to prevent bulk extraction. A database may only be searched for single records as part of a normal business process. Again a firewall in front of the database could prevent file transfer or extracts of the database being taken. Specific controls that prevent extraction of data and data mining is the best method for ensuring malicious code, hackers and staff cannot take copies of the dataset or perform searches on inappropriate search terms including wildcards.

The last aspect is people who do not realise they are sharing their lives, not just with friends and family but also with anyone that has a good search engine, from marketers to organised crime. This is especially true when some social media sites change their terms and conditions and open up privacy settings.

I no longer have accounts on certain social media sites, as they now own all photographs posted on xxx. They also twice removed the privacy settings so that my information was exposed until I added the privacy controls again. Millions of people still do not realise that their information is public. Even simple things like putting too much detail in a CV uploaded to job sites can be a bad thing. It does not take much for a criminal to open an account as a potential employer and browse CVs, which can include full names, address, contact details and so on. It is vital that people think about what information they are putting on the internet and why. A short CV with an email address and note that a full version is available on request is all that is needed on job sites. Searching for medical websites and certain information should be done with caution, including ensuring the browser is set to do not track. I would suggest using a different web browser type for sensitive sites, one that does not share cookies or cache with your main browser. If you look after the computers for children and family members that may be adults, but new to the internet, it best to ensure that their computer has a full internet security package, which includes parental controls. Configure this for them to prevent personal information being exposed and prevent access to blacklisted websites. Though this will not solve every issue it will certainly help.

As storage gets cheaper, processing power increases exponentially and the internet becomes more pervasive in everyone’s lives, the data mining issue will just get worse. Criminals are going to follow the money online. They are going to target people for identity theft, blackmail and worse. Private investigators and investigative journalists are going to use those massive data sources to their benefit and marketing will become even more accurate and targeted.

However, this does not have to be as bad as it sounds; fear, uncertainty and doubt can be just as bad, as they prevent people making full use of the advantages offered by the internet. If you protect your personal data, as you would in the real world, and minimise where your personal data is exposed and stored on third party databases, you can enjoy the internet with minimal risk.

www.bcs.org/security
The difficult part is the risk management of the issues surrounding the collecting, storage and use of data. The underlying risks are the usual CIA ones, plus compliance, which is often forgotten, but may be the biggest risk of all as we shall see later. Taken together these are a huge risk management challenge, especially when it comes to providing assurance that the end product of our investment, the information, can be relied on. BCS has a specialist group that deals with this challenge; the Information Risk Management and Assurance (IRMA) group is one of the oldest within BCS and this year celebrates its 50th anniversary. It has gone through three name changes along the way (Auditing by Computer, Computer Audit and now IRMA), which illustrates its need to adjust its name to suit the changing nature of the risk due to changes in technology. It is interesting to note that 50 years ago, in the very early days of computing, some far sighted people realised the need to develop a control framework to provide assurance that the information being created by the technology could be relied on. Data collection and subsequent processing stages need to be controlled in a way which provides for confidentiality, integrity, availability and compliance at each stage of the journey from raw data to management information. When I reflect on what is involved in that journey I am amazed that we get anything approaching reliable output, and yet by and large we do. This is because over the years we have identified the key risks and put in appropriate controls to manage them to an acceptable level.

This is not the same as no risk and the acceptable level will vary from industry sector to sector, from company to company and even from system to system, but we now have a pretty good understanding as to what that level of acceptability should be for any given situation. The only reason that we have all that hardware, software and networks is to capture the raw data, store it and then process it to produce information for (hopeful) sensible decision making. The necessary control framework is formidable. We must provide for confidentiality, integrity, availability and compliance within the worldwide regulatory framework.

Although this is a daunting concept you can start by thinking of it as a pyramid with hardware at the bottom and information at the top, then the successive layers between the two are: base software (i.e. operating system), middle software (i.e. database management), application software (i.e. payroll) and data. This last level is stored and manipulated by the lower levels to produce information. The network which provides the interconnectivity to distribute this information can be imagined as running up the spine of the pyramid. This means that for information to be reliable and available when required we must manage every underlying asset and process. The underlying risks are the usual CIA ones, plus compliance, which is often tolerable if we apply the confidentiality, integrity and availability (CIA) framework. The only reason that we have all that hardware, software and networks is to capture the raw data, store it and then process it to produce information for decision making. The necessary control framework is formidable. We must provide for confidentiality, integrity, availability and compliance within the worldwide regulatory framework.

Although this is a daunting concept you can start by thinking of it as a pyramid with hardware at the bottom and information at the top, then the successive layers between the two are: base software (i.e. operating system), middle software (i.e. database management), application software (i.e. payroll) and data. This last level is stored and manipulated by the lower levels to produce information. The network which provides the interconnectivity to distribute this information can be imagined as running up the spine of the pyramid. This means that for information to be reliable and available when required we must manage every underlying asset and process. The underlying risks are the usual CIA ones, plus compliance, which is often tolerable if we apply the confidentiality, integrity and availability (CIA) framework. The only reason that we have all that hardware, software and networks is to capture the raw data, store it and then process it to produce information for decision making. The necessary control framework is formidable. We must provide for confidentiality, integrity, availability and compliance within the worldwide regulatory framework.

Although this is a daunting concept you can start by thinking of it as a pyramid with hardware at the bottom and information at the top, then the successive layers between the two are: base software (i.e. operating system), middle software (i.e. database management), application software (i.e. payroll) and data. This last level is stored and manipulated by the lower levels to produce information. The network which provides the interconnectivity to distribute this information can be imagined as running up the spine of the pyramid. This means that for information to be reliable and available when required we must manage every underlying asset and process. The underlying risks are the usual CIA ones, plus compliance, which is often tolerable if we apply the confidentiality, integrity and availability (CIA) framework. The only reason that we have all that hardware, software and networks is to capture the raw data, store it and then process it to produce information for decision making. The necessary control framework is formidable. We must provide for confidentiality, integrity, availability and compliance within the worldwide regulatory framework.

Although this is a daunting concept you can start by thinking of it as a pyramid with hardware at the bottom and information at the top, then the successive layers between the two are: base software (i.e. operating system), middle software (i.e. database management), application software (i.e. payroll) and data. This last level is stored and manipulated by the lower levels to produce information. The network which provides the interconnectivity to distribute this information can be imagined as running up the spine of the pyramid. This means that for information to be reliable and available when required we must manage every underlying asset and process. The underlying risks are the usual CIA ones, plus compliance, which is often tolerable if we apply the confidentiality, integrity and availability (CIA) framework. The only reason that we have all that hardware, software and networks is to capture the raw data, store it and then process it to produce information for decision making. The necessary control framework is formidable. We must provide for confidentiality, integrity, availability and compliance within the worldwide regulatory framework.

Although this is a daunting concept you can start by thinking of it as a pyramid with hardware at the bottom and information at the top, then the successive layers between the two are: base software (i.e. operating system), middle software (i.e. database management), application software (i.e. payroll) and data. This last level is stored and manipulated by the lower levels to produce information. The network which provides the interconnectivity to distribute this information can be imagined as running up the spine of the pyramid. This means that for information to be reliable and available when required we must manage every underlying asset and process. The underlying risks are the usual CIA ones, plus compliance, which is often tolerable if we apply the confidentiality, integrity and availability (CIA) framework. The only reason that we have all that hardware, software and networks is to capture the raw data, store it and then process it to produce information for decision making. The necessary control framework is formidable. We must provide for confidentiality, integrity, availability and compliance within the worldwide regulatory framework.

Although this is a daunting concept you can start by thinking of it as a pyramid with hardware at the bottom and information at the top, then the successive layers between the two are: base software (i.e. operating system), middle software (i.e. database management), application software (i.e. payroll) and data. This last level is stored and manipulated by the lower levels to produce information. The network which provides the interconnectivity to distribute this information can be imagined as running up the spine of the pyramid. This means that for information to be reliable and available when required we must manage every underlying asset and process. The underlying risks are the usual CIA ones, plus compliance, which is often tolerable if we apply the confidentiality, integrity and availability (CIA) framework. The only reason that we have all that hardware, software and networks is to capture the raw data, store it and then process it to produce information for decision making. The necessary control framework is formidable. We must provide for confidentiality, integrity, availability and compliance within the worldwide regulatory framework.

Although this is a daunting concept you can start by thinking of it as a pyramid with hardware at the bottom and information at the top, then the successive layers between the two are: base software (i.e. operating system), middle software (i.e. database management), application software (i.e. payroll) and data. This last level is stored and manipulated by the lower levels to produce information. The network which provides the interconnectivity to distribute this information can be imagined as running up the spine of the pyramid. This means that for information to be reliable and available when required we must manage every underlying asset and process. The underlying risks are the usual CIA ones, plus compliance, which is often tolerable if we apply the confidentiality, integrity and availability (CIA) framework. The only reason that we have all that hardware, software and networks is to capture the raw data, store it and then process it to produce information for decision making. The necessary control framework is formidable. We must provide for confidentiality, integrity, availability and compliance within the worldwide regulatory framework.

Although this is a daunting concept you can start by thinking of it as a pyramid with hardware at the bottom and information at the top, then the successive layers between the two are: base software (i.e. operating system), middle software (i.e. database management), application software (i.e. payroll) and data. This last level is stored and manipulated by the lower levels to produce information. The network which provides the interconnectivity to distribute this information can be imagined as running up the spine of the pyramid. This means that for information to be reliable and available when required we must manage every underlying asset and process. The underlying risks are the usual CIA ones, plus compliance, which is often tolerable if we apply the confidentiality, integrity and availability (CIA) framework. The only reason that we have all that hardware, software and networks is to capture the raw data, store it and then process it to produce information for decision making. The necessary control framework is formidable. We must provide for confidentiality, integrity, availability and compliance within the worldwide regulatory framework.

Although this is a daunting concept you can start by thinking of it as a pyramid with hardware at the bottom and information at the top, then the successive layers between the two are: base software (i.e. operating system), middle software (i.e. database management), application software (i.e. payroll) and data. This last level is stored and manipulated by the lower levels to produce information. The network which provides the interconnectivity to distribute this information can be imagined as running up the spine of the pyramid. This means that for information to be reliable and available when required we must manage every underlying asset and process. The underlying risks are the usual CIA ones, plus compliance, which is often tolerable if we apply the confidentiality, integrity and availability (CIA) framework. The only reason that we have all that hardware, software and networks is to capture the raw data, store it and then process it to produce information for decision making. The necessary control framework is formidable. We must provide for confidentiality, integrity, availability and compliance within the worldwide regulatory framework.

Although this is a daunting concept you can start by thinking of it as a pyramid with hardware at the bottom and information at the top, then the successive layers between the two are: base software (i.e. operating system), middle software (i.e. database management), application software (i.e. payroll) and data. This last level is stored and manipulated by the lower levels to produce information. The network which provides the interconnectivity to distribute this information can be imagined as running up the spine of the pyramid. This means that for information to be reliable and available when required we must manage every underlying asset and process. The underlying risks are the usual CIA ones, plus compliance, which is often tolerable if we apply the confidentiality, integrity and availability (CIA) framework. The only reason that we have all that hardware, software and networks is to capture the raw data, store it and then process it to produce information for decision making. The necessary control framework is formidable. We must provide for confidentiality, integrity, availability and compliance within the worldwide regulatory framework.
Data is everywhere. Some of this data is information we voluntarily give away through social media or other online tools, but data is also being generated as a by-product of us simply going about our day to day lives. This raises ethical questions, says John Quayle MBCS, a member of the BCS Ethics Specialist Group.

Every day we are adding to our digital footprint and, given the ubiquity of the devices we all use out of necessity rather than choice, there is very little we can do, as individuals, to change this.

Our industry has barely scratched the surface of big data so it is therefore unsurprising that a new generation of products has emerged specifically to gather data they’re giving away and the potential consequences of doing so?

To give a few examples: people are happy to provide data about their shopping habits via store loyalty cards in return for special offers; smart cards track their owner’s travel habits in return for the convenience of being able to tap in and out of the transport system; files and emails are hosted on somebody else’s servers so that they can be accessed from anywhere that has an internet connection; photographs are posted on social media sites so that people can share experiences with their friends.

Generally this seems to work. Quid pro quo. You take my data, you provide me with a service in return. Everybody wins. But do people really understand how much data they’re giving away and the potential consequences of doing so?

In this article location data will be used as an example to show some of the ethical issues relating to mass data collection, before concluding with some realistic proposals about what can be done about these issues.

Unintended consequences

Let’s take Twitter as an example. People use Twitter as an example. People often tweet about whatever is on their mind using 140 characters or less. Tweets sit there for all the world to see. It’s all good fun. However, it is also a goldmine of information for those that are interested. And a lot of people are interested - especially if a user tweets a lot and has elected to add their location data to their tweets.

The presence of Twitter has spawned a number of publicly available Twitter aggregators such as Stramaededia, Twitonomy and the aptly named Creepy. With the time and inclination, it’s possible to extrapolate all sorts of information from an unsuspecting user’s tweets. From trivial snippets such as a user’s favourite band or preferred coffee shop, to more private things such as an individual’s route to work and where they live. All of this information derived from data that users have leaked one tweet at a time!

This is a key point. Even though the Twitter user may never have expressly said, ‘I live here’, it is, nevertheless, possible to put the pieces of the jigsaw together to see the bigger picture.

(Should be pointed out that Twitter has merely been used as an example here and there is no question of there being any malpractice on its part.)

Hidden data

Mobile phones are able to track their owner’s location with remarkable accuracy. The apps installed on mobile devices have access to this data with the user’s permission. It is likely that there are a large number of users unaware that their data is being transferred to third parties without it being obvious to them that this is happening.

Having already seen what can be done with the limited location data we know about, it’s only a small logical step to see what might be possible if all location data was aggregated in some way.

Ethical questions

The examples above start to raise some ethical questions.

Are the terms and conditions to which users sign up need to be simplified. Key facts documents similar to those in the financial industry would go a long way to helping end-users decide if they want to sign up to a service or indeed how they might want to use a service.

Many users don’t even read the T&Cs because they are so long and complex; literarily longer than a Shakespeare play in some cases. A key facts document is far more likely to be read and understood than a verbose legal document.

Secondly, people should know about all the data that is held about them. Data controllers should, therefore, be obliged to send an annual statement of data to each and every individual for whom they store personalised data. On the face of it, this might seem controversial, creating a vast overhead for companies but, in practice, this should be a relatively simple task for any company that is competent to handle the data. Google, Facebook and Twitter all offer the option for users to download all the data that is held about them. Organisations that cannot comply with this request would either have to anonymise data or delete the data they hold.

Finally, there should be an assumption that individuals own their own data and should have the right to have their data deleted within certain parameters. It wouldn’t make sense, for example, to allow individuals to delete missed payments from their credit history, but the individual does have the right to make sure their credit history is correct.

Data can be used for purposes contrary to the spirit in which it was provided. Furthermore, personalised data is also being collected about individuals who may not even be aware it’s being collected in the first place. The IT industry has duty of care to ensure that data is handled competently. This would ensure that individuals are protected but also give end-users confidence that their data will not be misused.

The methods by which the industry protects its end-users is a matter of debate, but options include making terms and conditions easier to understand, providing greater transparency of the data that is held on individuals and the adoption of the general assumption that the end-user owns any data from which they can be identified.

www.bcs.org

References


The EU’s regulatory planning for cloud computing and data protection is an expanding domain worthy of everyone’s attention. Whether you are pro-EU regulation, or anti, the European Commission is addressing vital solutions to key issues so says Stephen Meachem, a barrister and solicitor with the Law Tribe and a member of the BCS Law Specialist Group.

Currently the market norm is complex contracts or service level agreements that are insufficiently specific and balanced and which contain extensive disclaimers. The use of take-it-or-leave-it standard contracts might be cost-saving for the cloud provider, but is often undesirable for the user, including the final consumer. Standardised contractual terms would reduce the transaction cost of legal advice. Contractual litigation should be regarded as a sign of regulatory failure. Robust and transparent standard contractual terms must be the way forward. Usefully, therefore, the EU is working towards model contract terms and a code of conduct for cloud providers. See also ISO/IEC 27018 mentioned below.

Data protection in the cloud

The cloud is blurring the boundaries of the enterprise and creating security issues. People need to know where their data is and who has the right to see it. Issues arise in the cloud when cloud services are used to process personally identifiable information (PII).

It is hard to imagine an organisation that does not hold a certain amount of PII (related to employees for instance). However, in the cloud, whilst the data processing is outsourced and under cloud provider control, the legal obligations regarding PII protection remain with the client of the cloud services; under the Data Protection Directive 1995, as implemented in the UK by the Data Protection Act 1998.

The EU has developed an auditable voluntary standard known as ISO/IEC 27018. An auditor can verify whether a cloud provider meets the requirements of the standard and, if the level of compliance is adequate, it can issue a compliance certificate. This certificate can be used both as a marketing tool for the cloud provider and as a warranty that the cloud provider meets its obligations regarding PII.
processing. To complete the regulatory system the compliance certificate can then be registered in the contract signed between the client and the cloud service provider. This is an admirable solution in my view.

The Data Protection Directive 1995 is relevant to the cloud and big data as it contains a purpose limitation principle that provides that personal information must only be processed for specified, explicit and legitimate purposes, and that it must not be further processed in a way incompatible with those purposes. Derogations are only permitted where this is necessary to safeguard one or a list of public policy objectives, including, for example, public and national security, defence and the prevention of crime.

The UK’s Information Commissioner’s Guide to Data Protection links the compatibility of two or more purposes to the question of whether or not any further processing can be considered fair. Using or disclosing personal information in a way that is outside that which the individual concerned would reasonably expect, or which would have an unjustified adverse effect on them, would be considered unfair and thus incompatible with the original purpose.

Accordingly when assessing the compatibility of new purposes, data controllers must take into account, inter alia, the nature of the data, the legal grounds on which it was originally collected, and whether the data subject was in a weak bargaining position or whether it was mandatory for the data subject to provide the data in the first place.

However, Section 35 of the Data Protection Act 1995 permits disclosures ‘under any UK enactment’, even if those disclosures would otherwise violate the purpose limitation principle. The practical effect of this provision in its current form is that UK data controllers have no right (or obligation) to refuse a request for the disclosure of personal data to public bodies on the basis of their data protection obligations as long as that disclosure is mandated by any statutory or common law obligation. It could, of course, be argued that such a lawful request from a UK government agency would itself be in breach of its obligations under the Data Protection Directive; which would be a potentially costly and lengthy litigation matter.

Article 6(4) of the proposed General Data Protection Regulation will dilute the purpose limitation principle somewhat in that it will provide a statutory basis in EU law for data processing activities for purposes that would otherwise prima facie have been judged as incompatible with the original purpose where inter alia ‘processing is necessary for compliance with a legal obligation to which the controller is subject’ (Article 6(1)(c)) or ‘processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data’ (Article 6(1)(f)).

Safeguards in respect of 6(1)(c) appear at Article 6(3): the ‘legal obligation’ must meet an objective of public interest or be ‘necessary to protect the rights and freedoms of others’ and ‘respect the essence of the right to the protection of personal data’ and be proportionate to the aim pursued. Moreover, it must be consonant with the Charter of Fundamental Rights of the European Union. Stronger safeguards may be required. Data processors may disagree.

Arguably to restore and maximise trust in the cloud more transparency is needed on government access to data, for example, for reasons of law enforcement and national security, including commitments on what constitutes legitimate government access to data and transparency about what access requests have been made.

Summary of the proposed EU General Data Protection Regulation:

• A right to be forgotten. When a data subject no longer wants data to be processed and there are no legitimate grounds for retaining it, the data will be deleted. The rules are about empowering individuals, not about erasing past events or restricting the freedom of the press.

• Data subjects will have easier access to their own data.

• A right to transfer personal data from one service provider to another.

• When a data subject’s consent is required, they must be asked explicitly.

• More transparency about how your data is handled, with easy-to-understand information, especially for children.

• Businesses and organisations will need to inform data subjects about data breaches that could adversely affect you without undue delay, within 24 hours. They will also have to notify the relevant data protection authority.

• Improved administrative and judicial remedies in cases of violation of data protection rights.

• Increased responsibility and accountability for those processing personal data, through requirements for data protection risk assessments, organisational data protection officers and the principles of ‘privacy by design’ and ‘privacy by default’ to be enacted in the General Data Protection Regulation are certainly food for thought and a source of potential instructions for software engineers.

• The above principles and the principles of ‘privacy by design’ and ‘privacy by default’ in the proposed General Data Protection Regulation are certainly food for thought and a source of potential instructions for software engineers.

Love or hate it, being in Europe can’t be all bad for business! Can it?

www.bcs.org/law

This treaty is the closest instrument to a universal declaration of data rights in existence. A key amendment is the explicit formulation of the principle of proportionality, which is to be respected at any stage of data processing.

New duties of data controllers and processors include a duty of active transparency and an obligation to establish internal mechanisms to demonstrate compliance, to carry out risk analyses, and to design processing in such a way as to minimise risks for data subjects.

The above principles and the principles of ‘privacy by design’ and ‘privacy by default’ to be enacted in the General Data Protection Regulation are certainly food for thought and a source of potential instructions for software engineers.

Love or hate it, being in Europe can’t be all bad for business! Can it?

www.bcs.org/law

Further information

Sources of further information


The European Commission


-
We are all susceptible to being hacked and our private records compromised. The trick to defending yourself or your organisation is to learn from the experiences of others and understand who might wish to target you. Avoiding the mistakes of others is a low-cost method of improving your security posture.

The big attacks of 2014 was against Sony, which was comprehensively taken over by hackers. Other than the debate as to who perpetrated the hack, it was apparent that Sony has not learned from previous compromises, that it and others had suffered, as it continued to operate with lax security controls. Observers might wonder how a large organisation, more than able to afford capable professionals, administering appropriate security policies and procedures, and underpinned by technology could allow many terabytes of data to be exfiltrated without anyone or anything noticing something was awry. The practice of keeping a directory of static passwords for corporate accounts shows how even a large business struggles to find a way to balance security with usability.

Attacks leveraging zero-day vulnerabilities can crack open even the strongest layers of defence, so you still need to also be checking on the inside. All of us rely on software and many of us rely on it being robust and secure. It is impossible for functional software to have no bugs or vulnerabilities, but many can be squashed during the software development lifecycle, with code analysis / testing. Secure software development can make our digital environment safer.

When it comes to dealing with hacks such as the one Sony suffered, Gareth Niblett, Chairman of the BCS Information Security Specialist Group says we should all learn from others mistakes.

FURTHER INFORMATION

Information Security Specialist Group (ISSG):
www.bcs-issg.org.uk

Information Risk Management and Assurance Specialist Group:
www.bcs.org/groups/irma

BCS Security Community of Expertise (SCEt):
www.bcs.org/securitycommunity/muniny

INFORMATION SECURITY
EXPERT GUIDANCE

Andy Smith MSc FBCS CITP provides an update on the BCS Security Community of Expertise.

The BCS Security Community of Expertise (SCoE) (www.bcs.org/scoe) and its various subgroups have been very active over the last few months.

There have been a number of changes on the committee with some long standing members retiring and new members being voted on to the committee. We now have a liaison with ISOC2 and better representation on the ISO standards panels as a result.

The Identity Assurance Working Group (IAWG) has also been very active and representatives will be at UK IGF this year and will submit proposals for talks at EuroDIG and UN-IGF www.intgovforum.org/cms. A summary paper of the activity from last year will be placed on the website shortly www.bcs.org/scoe.

The focus of the SCoE remains on providing advice and guidance for the BCS membership and ensuring BCS is a voice of content not the security and ownership of devices (note this also applies to the cloud);

• Cyber security aspects of internet of things. This will mainly be done via the IoT WG focusing on the awareness and impact of IoT on the public in cars, smart TVs, smart metres, smart lights etc;

• Education: security sense/home advice/risk assessment – linked to security top tips and Get Safe Online, which BCS contributes to, including developing a basic security sense guide for individuals and SMES;

• Presence online – how do you protect yourself online legally, morally, personal and social – plus such things as malicious code and privacy that still need to be addressed properly.

The SCoE came up with a number of areas is look at during 2015. A few of these will be selected based on what we feel will provide the most benefit to the membership.

The short-listed topics are:

• Hold a top tips Q&A at Infosec 2015 as part of our workshop on professionalising the security industry and education;

• BYOD security aspects focused on: stop looking at the devices, look at the data – the security and ownership of content not the security and ownership of devices (note this also applies to the cloud);

• Cyber security aspects of internet of things. This will mainly be done via the IoT WG focusing on the awareness and impact of IoT on the public in cars, smart TVs, smart metres, smart lights etc;

• Education: security sense/home advice/risk assessment – linked to security top tips and Get Safe Online, which BCS contributes to, including developing a basic security sense guide for individuals and SMES;

• Presence online – how do you protect yourself online legally, morally, personal and social – plus such things as malicious code and privacy that still need to be addressed properly.

From this list a few topics will be chosen and as much as possible achieved over the next year.

There are a large range of subjects that are now proving interesting and critical to daily life, from internet of things and NFC to Bluetooth and ‘my life in my hand’ where people have their whole lives: calenders, contacts, email, social media, basically everything, on their smartphone. So many of these technologies are becoming ubiquitous and combined in previously unimaginable ways. Now your smartphone can control your TV, sound system, cooker, lights, etc., which means that unless its properly secured, so can other people.

With the internet now being a standard inclusion on most TVs including video conferencing and web browsing right from your sofa, life is so much easier. But how many people read the user agreement? The ones that gives the manufacturer the right to monitor your web usage, turn on your camera and microphone remotely and listen in. Yes there are some that include this. It is subjects like this that show how people should be protected from cool features that have hidden security issues.

BYODs now becoming a much more important subject for organisations, with staff using tablets for taking meeting notes and managing their calendar to some diverting their work email to their personal device and others working out they can access that wonderful cloud email service the company just started using from their phone. This is a topic we are looking at further and may become a key theme for 2015.

I think 2015 will be an interesting year with many lively debates on privacy and anonymity and ongoing security issues surrounding merging technologies.

The SCoE will endeavour to represent the BCS membership across a wide variety of forums. There are regular talks and meetings at the BCS office, especially useful if you live in London, but security events do take place on a regional basis too. Check out your local branch for more details: www.bcs.org/branches.

www.bcs.org/security

ITNOW March 2015
SECURE DEVELOPMENT

Steve Daniels FBCS CITP, Strategic Business Advisor for Cyber Security in CGI UK, looks at the best practices for secure cyber development now being adopted.

Today’s reality is that an insecure system will be breached. Secure systems engineering has often not been sufficiently prioritised, over being faster to market and adopting new technology.

The many publicly quoted data breaches demonstrate that this approach is not good for business. Failing to keep customer and organisation data private, available and correct now comes at an escalating cost.

This can include significant remedial costs and lost revenue (e.g. Sony ‘The Interview’)

huge fines (e.g. TJ Maxx’s) lost customers, getting swallowed up (e.g. HBGary)

This can include significant remedial costs and lost revenue (e.g. Sony ‘The Interview’), huge fines (e.g. TJ Maxx’s) lost customers, getting swallowed up (e.g. HBGary) or going out of business (e.g. Nortel). Recent evidence shows that recovery costs can be 2.5 times larger than mitigating the issue in the development process.

Applying structured risk management within the development approach is the best way to address this challenge.

Why is it seemingly so hard?

Securing systems is not trivial. With millions of lines of code on a complex mesh of servers, running multiple protocols across a network, with the applications on top, it is often considered an insurmountable challenge.

Such architectures can quickly become riddled with security vulnerabilities. Numerous security industry reports show a substantial number of vulnerabilities reported annually. One study cited that 53 per cent of the systems scanned contained exploitable vulnerabilities. A study of applications showed 86 per cent of their websites contained at least one serious flaw.

Software development lifecycles are being increasingly compressed to deliver results sooner. Monthly ‘waterfall’ phases are now weekly ‘updates’ and ‘daily stand-ups’ within rapid development (AGILE) processes. These challenges are not new. Many organisations have established secure development lifecycles to fundamentally reduce system vulnerabilities. These have resulted in accessible techniques and guidance, with corresponding improvements in secure systems.

Microsoft’s STRIDE is one such model for structured analysis of threat or attack patterns.

The central role of risk assessment

A comprehensive risk assessment of a systems development provides a common language for ‘potential problem management’, usable throughout the lifecycle. Numerous scenarios have proven to be helpful in communicating the threats and risks to the proposed system, to architects and developers. But, additionally, these scenarios provide an excellent mechanism through which to ensure that:

1. the right amount, level and frequency of management engagement can be obtained.

2. architects and designers understand why they are implementing security controls rather than seeing them as annoyances which delay implementation.

3. security investment in the project overall, and effort to be invested in each of the security activities themselves, is ‘right-sized’ and appropriately ‘weighted’.

4. in an agile environment, security is more suited to the ‘sprints’ process.

5. proposals to trade-off controls for functionality and delivery can be addressed objectively.

Plotting the secure development journey

Risk assessments are successful when a consensus results. Communication and collaboration between the business users, developers, security experts and other stakeholders are essential. Too many business managers today consider that development is for developers. But, even if it takes some effort to get initial engagement to build the risk assessment, many benefits then accrue.

My experience is that this can actually bring the business and IT closer together.

In an agile development some processes are well suited to integrating security, such as the iterative code development phase. But the architecture analysis can seem at odds with the iterative nature of agile.

In fact, design reviews and code clean-ups can easily be added to the backlog to become part of scheduled sprints. The risk model is then very effective both at ensuring that this happens and that progressive sprints focus on completing the relevant parts, in priority order and sufficient detail.

Sufficient testing

Then comes the vitally important step of real-world security testing, often wrongly seen as the final development step.

With all the system modules integrated, the testing seeks to confirm that the system performs and security controls operate as expected. This will include testing of:

1. the original security requirements;

2. common security issues with the adopted technologies;

3. specific application features;

4. specially developed security controls.

This can again be best structured by reference back to the risk model. This will resolve such questions as: should the testing be done by an independent testing house, perhaps undertaking a CREST or CHECK review? Does the really merit standard testing? How much specialist and user engagement should there be to probe such issues as performance of the interface? What testing tools would be appropriate? What testing of capacity would be justified?

Achieving and demonstrating assurance

When a total cost of operation view is taken of the development, the real last stage is providing a sustainable assurance regime. The risk model again plays a major role in defining how user acceptance will be obtained from the business, and who from.

Associated activities can also be shaped by risk to include what user acceptance training should be undertaken and what the audit regime’s scope, frequency and depth of review needs to be.

Another critically important aspect of development, which can be shaped by the risk model, is how to handle waivers or non-compliances, i.e. those issues that remain unfixed. By identifying relative priorities, the risk model will enable this to become a business-based decision.

The start point will then be whether there can even be afforded. But if they can, what is the relative priority to fix them? In what timescale and how soon must the issue’s continued existence be subject to re-appraisal and by who?

Last, but not least, no good system goes live without appropriate performance reporting i.e. critical success factors supported by metrics. The risk model is ideal for defining what these need to be.

By using risk assessment to calibrate the development activities, they will remain proportionate and relevant to the real risks to which the live system will be exposed.

Whilst a more secure system will have been delivered, many other material benefits will emerge that mandate the adoption of this approach. These will encompass: lower development costs, lower running costs, more up-time, more throughput, higher end-user trust and, as a consequence, more end-customers.

Secure systems development is therefore achievable and entirely worthwhile.

REFERENCES

1. Sony’s costs for The Interview

Breach: Bloomberg, January 2015; http://tinyurl.com/oy7dpxg

2. TM, Visa reach $49.9M settlement for data breach; USA Today, November 2007; http://tinyurl.com/nxcc4n4

3. Anonymous speaks: the inside story of the HBGary hack: Ars Technica, February 2011; http://tinyurl.com/7bvy6mp


7. 2013 A Great Year Inbreach Report, Volume 18; http://tinyurl.com/cc7856t


When it comes to cyber security, why do large companies do it so poorly, asks Rob Pritchard.

In 2014, when these breaches occurred, large companies will usually have a security team working alongside those responsible for IT management. The admissions of compromise of some credit card details were stolen by point-of-sale malware, Home Depot suffered a similar breach. JP Morgan came later in the year, with the admission of the compromise of some 80 million customers’ details by a Russian criminal gang, with media allusion of 80 million customers’ details by a Russian criminal gang.

When it comes to cyber security, why do large companies do it so poorly, asks Rob Pritchard. How can you assess your exposure to a threat if you do not know the extent of your perimeter and what software you have running on what operating system? It is simply not possible, and budget and remit for cyber security projects rarely extends to remediating these issues.

Effective cyber security stems from a well-managed infrastructure, with a security team working alongside those responsible for IT management. Furthermore, we will not see a decline in security incidents. More data will be lost, accounts breached and organisations suffer huge losses, lawsuits and damage to reputations. Equally, spending on cyber security will continue to climb. There will be more conferences, government initiatives and conferences recognising that their IT is a critical asset by different companies, in geographically diverse parts of the world.

Paying the price

Significant compromises do not occur overnight. It takes time to gain, and maintain, persistent and deep access to a large network. The failures in security we see today are the consequences of a long-term failure to invest in what is business-critical infrastructure.

Compounding the concern is that the vast majority of these attacks are not actually particularly sophisticated. Clever in elements of their implementation perhaps, but using known vulnerabilities and off-the-shelf tools. Properly patched and maintained organisations, with dedicated security teams and security software in place should not be failing victim to hackers of this level of capability.

It seems remarkable then that, when cyber security is so high-profile, such breaches can still occur with such depressing frequency. What is going wrong? In the defence of big organisations, ensuring consistent security standards across a large, often multinational estate, which may have grown through acquisition, and with different cultural approaches in each region, is non-trivial.

However, the root of the problem is deeper and more systemic. For too long IT has been treated as something that should be subject to cost cutting, often very effectively. The failures in security we see today are the consequences of a long-term failure to invest in what is business-critical infrastructure.

Properly patched and maintained organisations, with dedicated security teams and security software in place should not be failing victim to hackers of this level of capability. Indeed, in nearly all of these examples the unfortunate organisations had been spending money on cyber security initiatives. Target had deployed a security monitoring product which alerted them to the problem, but no action was taken. Significant compromises do not occur overnight. It takes time to gain, and maintain, persistent and deep access to a large network.

An initial breach is made, often through a phishing email compromising the machine of a single user, and slowly expanded, with the attackers stealing credentials, accessing more computers on the network and ensuring they have persistent access. They have to do all this without triggering any monitoring systems. Compounding the concern is that the vast majority of these attacks are not actually particularly sophisticated. Clever in elements of their implementation perhaps, but using known vulnerabilities and off-the-shelf tools.

Properly patched and maintained organisations, with dedicated security teams and security software in place should not be failing victim to hackers of this level of capability. Indeed, in nearly all of these examples the unfortunate organisations had been spending money on cyber security initiatives. Target had deployed a security monitoring product which alerted them to the problem, but no action was taken. Significant compromises do not occur overnight. It takes time to gain, and maintain, persistent and deep access to a large network.

An initial breach is made, often through a phishing email compromising the machine of a single user, and slowly expanded, with the attackers stealing credentials, accessing more computers on the network and ensuring they have persistent access. They have to do all this without triggering any monitoring systems. Compounding the concern is that the vast majority of these attacks are not actually particularly sophisticated. Clever in elements of their implementation perhaps, but using known vulnerabilities and off-the-shelf tools.

Properly patched and maintained organisations, with dedicated security teams and security software in place should not be failing victim to hackers of this level of capability. Indeed, in nearly all of these examples the unfortunate organisations had been spending money on cyber security initiatives. Target had deployed a security monitoring product which alerted them to the problem, but no action was taken. Significant compromises do not occur overnight. It takes time to gain, and maintain, persistent and deep access to a large network.
**PERSISTENT THREATS**

Valory Batchelor and Neil Warburton from IBM take a look at the recent attack on Sony and ask what we can learn from it.

2014 saw a number of very high-profile attacks on major companies and continued the trend for more frequent and bigger breaches. It was rounded off by an attack on Sony Pictures Entertainment in the USA, which had a far-reaching impact and still making news in early January.

A group called Guardians of Peace (GOP) claimed responsibility. Estimates of the data stolen vary between 1 and 100 Terabytes, including employee sensitive personal information and personal emails between senior executives. Unreleased personal information and personal emails for long periods (e.g., Inside Man, 2006). With insufficient details on how Sony was attacked, we have to refer to a well-known historical APT attack to illustrate common attack patterns and make recommendations.

Target was attacked in 2013. Its systems were first breached by attackers using credentials stolen from an employee of a third-party company (phase one). From there the attackers penetrated as far as the point-of-sale systems where they installed malware (phases two and three). They also breached data servers, installed more malware and used all of this to steal credit card data (phases four and five).

The in-house security systems actually detected the activity early on, and raised alerts, but these were missed or ignored. How did this happen?

Too much information

An IBM survey found that a major challenge facing many organisations is a plethora of security tools – one respondent reported 85 tools from 45 vendors. We all know what it is like to be overwhelmed by a constant stream of information coming at us. How do you prioritise which alerts should be investigated? Especially if they are on multiple screens from multiple systems. How can you improve your chances of not being the next APT victim?

Steps to mitigate risk

First, you need a clear view of your organisational security posture. Not all data is created equal, and budgets are limited. Define where the most important data is and take all necessary steps to protect it. What data has most value for the company? Where is it held? What is the best way to protect it? What risks can you bear?

Second, understand trends in security tool technology. Tools that use behaviour-based technologies to detect unusual activity have several advantages over traditional signature-based solutions that detect exploits:

- Many attacks share common behaviours, so one behavioural pattern can cover many specific attacks.
- Zero-day exploits (no signature available) can be detected by their activity.
- You do not need thousands of up-to-date signature files, this means less reliance on updates from a vendor and quicker identification of an attack.

Third, you need to be able to interpret the output from the security tools and respond to protect your business according to the severity of the risk and potential business damage. This means visualising the activity in the infrastructure and determining quickly what matters most.

This is where the application of analytics to security, security intelligence, can help. While many people have heard of security information and event management (SIEM) systems, security intelligence is more than just a SIEM. An integrated approach to security intelligence directs and augments the skills of security professionals and allows them to use their experience and judgement to best effect. Security intelligence takes input from multiple security tools and other sources of infrastructure information such as event logs and network flows, and correlates this against knowledge such as: infrastructure and network layout; historical behaviour; known bad agents; known vulnerabilities in the infrastructure; importance of specific assets and routes to exploit those assets. From this it should provide a ‘single pane of glass’ into the organisation showing where the greatest threats and risks are at any given point in time. It takes advantage of the outputs from good tools and the work done to define your security posture. Although there will be set-up costs, these will be offset by much greater productivity and accuracy in dealing with incidents.

Security intelligence will also increasingly become available via managed service providers or cloud-based deployments. Finally, it will help you mitigate simple human error or poor processes. Security intelligence can be the smoke detector in your organisation: check the status regularly, change the battery (i.e., review policies as your organisation evolves) and pay attention when it goes off!

www.bcs.org/security

**References**

http://en.wikipedia.org/wiki/Advanced_persistent_threat
http://www.politics.co.uk/story/2014/12/6th-anniversary-sony-hack
http://www.politics.co.uk/story/2014/12/6th-anniversary-sony-hack-theory-113866.html
http://www.bbc.co.uk/news/technology-36432791
http://www.cbsnews.com/8301-3954_162-20074045
http://www.politics.co.uk/story/2014/12/6th-anniversary-sony-hack

**THREATS**

The term advanced persistent threat (APT) is used to describe modern cyberattack techniques. Advanced refers to the sophistication of the attack and the fact that one or more elements are often as yet unrecognised by security products. Persistent refers to the fact that they take place over a long time (often months) and usually involve some kind of remote monitoring by the hackers. The following explains the five broad phases of an APT:

1. Break-in: reconnaissance, spear phishing and remote exploits to gain access;
2. Latch-on: malware and backdoors installed to establish a foothold;
3. Expand: lateral movement to increase access and maintain a presence;
4. Gather: acquisition and aggregation of confidential data;

APT attacks involve a good deal of planning and often multiple attack vectors. Once in, they spread to wherever they find a weakness, constantly growing their knowledge of the infrastructure and where its weaknesses are until they find what they can exploit or steal. Data is then often extracted over a long period of time.

The development of cyberattacks over time has an analogy in bank heist movies.

Once, we liked our bank robbery movies to show daring smash-and-grabs, where a gang was in and out as fast as possible. If they were in the bank more than a few minutes, it was going wrong.

Now, we like movies about sophisticated bank robberies that are carried out over months, often with inside help and sometimes with the robbers inside the bank for long periods (e.g., Inside Man, 2006).}

Valory Batchelor and Neil Warburton from IBM take a look at the recent attack on Sony and ask what we can learn from it.
When it comes to security planning, John Mitchell says you can hope for the best, but you must also plan for the worst.

The correct information at the time and place of need is what every manager desires. To do this we need to add the requirement that the information complies with the statutory and regulatory framework. Every security manager quotes confidentiality, integrity and availability (CIA), but the compliance aspect is equally important. Indeed it may be argued that it is more so, because what is the point of having good CIA if you can go to prison for a breach of the law?

As an example, one could design a secure image collection, storage and retrieval system that meets all necessary CIA criteria, but if the images are of a paedophilic nature, then the CIA aspects are trumped by the compliance criterion.

Likewise, one could have really excellent CIA for government secrets only for these to be put into the public domain USA networks and online gambling is an offence in the USA.

Even ignoring the compliance aspects we may face major problems with data integrity due to the way the data is initially collected. Data entry, or garbage in-garbage out (GIGO) as it is better defined, needs far more attention than it currently receives.

Simply eyeballing an entry and then pressing the enter key can lead to a nearly two per cent error rate.

Even when coupled with instant validation of the entry the error rate is rarely reduced to zero. If the data quality rules allow a range, then anything within the range will be accepted regardless of its integrity.

Even where only an absolute entry is allowed, such as gender, the resulting entry of M or F may still be incorrect, as we found from comparing gender with operation type in a patients’ records system, where we found several males associated with hysterectomies!

We know that we are not going to get the right data integrity at the collection stage, it simply depends on how much additional care we are willing to put into those data items that really matter. We may decide that we can live with incorrect post codes, but not with incorrect account numbers.

The risk analysis should determine what is acceptable and then we should design the controls to provide for that level of acceptability. Control design is both an art and a science and really should be done at the system design stage. Ideally we should generate a table of data quality rules for each data item.

For example, configuration data may impact on the entire system, whereas standing data will only impact on the transactions to which it is applied. Derived data usually uses some standing and transaction data manipulated by some logic. So there is even more opportunity for the resulting information to be wrong.

We once found a bug in a Unix compiler that resulted in a numeric one divided by a numeric one not equalling a numeric one, which made a real mess of the information being produced.

Even if the compliance and integrity aspects are okay we still need to consider the availability and confidentiality aspects. The data may produce accurate information, but if that information is not available at time of need then it is totally useless, as NATS found when it had to close a significant part of UK air space due to their air traffic control system failing.

With real-time information systems the failure to deliver at time and place of need is immediately known to the customer, whereas an integrity problem may go unnoticed for years.

Which brings me to the confidentiality aspect of CIA. We spend vast amounts of money in trying to ensure that only authorised people have access to our data, but as I have argued previously, once you grant privileges, then your entire control framework is based on the trust you have in that individual and trust is not a control, but as I have argued previously, once you grant privileges, then your entire control framework is based on the trust you have in that individual and trust is not a control, it is a hope. I was taught to hope for the best, but plan for the worst. I am sure that Sony corporation wish that they had spent more time on the latter.

www.bcs.org/security

Data entry, or garbage in-garbage out (GIGO)
as it is better defined, needs far more attention than it currently receives.
HOW SECURE IS SECURE?

Gareth Baxendale FBCS CITP Head of Technology, Clinical Research, Network National Institute for Health Research, looks at the ways to secure critical infrastructure.

Despite popular belief, hackers do not tend to don balaclavas, before they begin their silent attack on your infrastructures. However, we do seem to associate this bank robber-esque image with the activity of hacking and IT security. In today’s world, security is a way of life for all of us, only you have to go to the airport and you will be reminded of how serious it can get.

For technologists the securing of data is no doubt ‘business as usual’, but as we evolve more complex methods to present our services and allow users to interact with them, the greater the risk becomes.

How secure is secure?

Securing your infrastructure can take considerable effort, and getting the correct level of security in place, at the right level, is key. It is easy to over-engineer a solution that may impact the entire user experience. On the other hand, a poorly designed solution will require greater effort at the other end in maintaining and monitoring, and may even result in sleepless nights.

When designing an approach, the infrastructure, application and data layer must be viewed as a whole, or you may secure one layer but leave another open to attack. Some questions to consider: do you want to use a DMZ (demilitarized zone) and open ports on your internal firewall for every service required? Or do you want to simply key everything on the internal side so as not to turn your firewall into Swiss cheese?

Then there is the CMZ (classified militarized zone) which, by choice, contains your sensitive data and is monitored to an extreme degree to ensure it is protected at all costs.

When presenting data do you use a staging database in a different subnet to limit the chance of a direct connection to your back-end data layer? Will you consider emerging proactive database monitoring tools such as FortiDB? Of course, your approach will depend on the services you are exposing and every vendor will have a different set of options for you to choose from.

Good practice

The annual security review and pen test, while still important, is now giving way to more live security reporting and analysis to provide you with assurance that your data is safe. Many security vendors now offer proactive monitoring of your external services to ensure that known exploits have not accidentally been opened up by trigger-happy firewall administrators.

Some simple good practice can make a real difference, such as ensuring you have multi-vendor firewalls separating your networks. This may seem like an expensive luxury at first, but it means that any would-be attacker has two highly complex firewall technologies to overcome instead of just one. It also means that in the rare case a vendor’s firewall has a known weakness it is unlikely that the second vendor will have the same exploit, reducing the chances of an attacker’s success.

Ensuring your systems are patched to current levels is also an essential activity in the battle against the hacker. But let’s not just limit this to technology itself; ‘change control’, as a process, is an important defensive weapon against human error that might otherwise cost you dearly. Knowing what needs to be changed, gaining approval, planning who will do the work and when, along with ensuring a full impact assessment is carried out, will save you a lot of pain later on.

In most cases the attack vector will be your database. This is where an attacker can collect personal details about your customers, harvest passwords and login details, collect credit card data, or, even worse, medical history and other sensitive data. While these data assets may be ‘hashed and salted’ using complex encryption techniques, the reality faced is that many organisations suffer immense reputational damage having to admit publicly that the data was stolen in the first place, even if there is no chance the data could be unencrypted.

Attacks from within, by members of staff, are also now common place. Take for example a very high profile insurance company who suffered embarrassment when two members of staff acquired data on customers’ recent insurance claims and sold it to claims management companies. Also, don’t assume that a hacker will always attack from the perimeter of your network. He may simply plant it behind the desk.

The tiger hunts

Take the following as an example, if a hacker knows where your office is located it’s a breeze. Google will show them the front door. If they lay an attempt to access your premises as the air-conditioning or printer repair man. Of course they are not on the list of expected visitors, so off reception go to find out the score from facilities management leaving the reception desk unattended. Our hacker printer repair man pulls out his Wi-Fi router and loops it to the back of the reception PC and hides it behind the desk.

The receptionist returns and informs our hacker printer repair man that no repairs are scheduled.

It must be a mix up at HQ he says and politely leaves. He now heads for his car and connects over Wi-Fi to the router he has just planted. He now has access to your LAN and the attack begins. This activity is often done by ‘ethical hackers’ who are paid by companies to find weaknesses in their security processes and is known as a ‘Tiger Attack’. It could, however, be a real event if your data is valuable enough to an organised crime syndicate or someone who wants to damage your company’s reputation.

Sadly, the weakest link in data security is almost always the human. Socially engineered attacks are the first weapon in the arsenal of the hacker. With it they can pose as your local service desk team and email unsuspecting staff of an ‘urgent security breach’ that requires them to change their password immediately. Your staff are super trained in security and the like. Each site though typically uses a different selection of security options and this poses an easy way for a hacker to collate a security profile on us. It only takes one site to reveal some data on us for a hacker to use that data to access another site.

Basic security questions like ‘What’s the name of my dog?’ can easily be harvested from your Facebook account where you’ve shared cute pictures of your little mutt. The oft used mother’s maiden name is also at risk with your family history being on show on Facebook. Hackers can even use

However, since we always use different passwords for all our internet accounts there is absolutely no chance that our hacker might use the same harvested details to access our personal eBay, PayPal or other financially related site, right?

Know thy enemy

We all hope that our online accounts are secure and that we have dutifully set up all the mandatory PINs, secret words, picture security and the like. Each site though typically uses a different selection of security options and this poses an easy way for a hacker to collate a security profile on us. It only takes one site to reveal some data on us for a hacker to use that data to access another site.

Basic security questions like ‘What’s the name of my dog?’ can easily be harvested from your Facebook account where you’ve shared cute pictures of your little mutt. The oft used mother’s maiden name is also at risk with your family history being on show on Facebook. Hackers can even use

this information to ring up support lines and pose as you to get account passwords reset so be careful about your choice of security questions. Where possible always use two-factor authentication where a random PIN is generated to a device you have such as your smartphone. Oddy eBay doesn’t offer this feature, probably one of the sites we use the most!

In the battle to protect your data the best advice is to think like a hacker. A hacker will target the weakest link, so the question for you is what’s your weakest link? This applies to your company’s data assets and your own personal data.

Don’t be caught out by focusing exclusively on the complex end of security. The real risk lies in the simple and often overlooked day-to-day functions of your organisation. And don’t forget to review your own personal security profile so it is not the next victim of those pesky hackers.

www.bcs.org/security

ITNOW March 2015

INFORMATION SECURITY
The attack on Sony Pictures was one of the most widely reported in 2014, however, in my experience many organisations choose to keep mum about them. One incident I looked at in 2013 involved a serious security incident at a relatively small subsidiary of a major corporation. The company chose not to disclose it for fear of it leading to the subsidiary winding up, or that it could adversely affect the reputation of the parent company.

Many companies adopt the same approach. The number of attempted security breaches is probably impossible to assess, but is almost certainly more extensive than most people think or most surveys suggest.

Atos, the worldwide IT partner for the Olympic Committee, detected over 255 million security alerts on its security information and event management (SIEM) system during the London Olympics, of which 4.5 million, constituted significant events and over 5,000 resulted in incidents that required further assessment.

No security incidents impacted live competition, but it can clearly be seen that the scale of the assaults on organisations can be staggering.

Small businesses who do not court controversy or international attention may feel that the firewalls, security patches and password systems they have in place constitute the extent of the controls they need to have, but the leading information security management standard, ISO27001, identifies no less than 114 areas where controls are likely to be required. And the need for adequate controls is critical even for a small undertaking.

I run a number of websites and it is revealing to analyse the traffic I receive. Take one website, SwissWinterSports.co.uk, a site aimed at informing English-speaking skiers and snowboarders about winter sports in Switzerland. It gets a modest amount of traffic, with several hundred legitimate visitors a day.

However, the leading sources of hits during one typical week in December were respectively an ISP in Israel, a suspicious unknown IP address, a known comment spammer, a Russian spam harvester and a Ukrainian spam harvester. Throughout the list of visitors and in the error logs was evidence of highly suspicious activity.

Two of the most common sources of 404 ‘document not found’ errors were to the administrative log pages associated with Wordpress and Joomla, neither of which I host at this site, so presumably these are attempted security breaches. The 404 errors included a number from known bugs and legitimate sources, such as hits on icon files that don’t exist, but most were not.

As you might expect for a website of this nature, the countries associated with the most traffic are the UK, USA and Switzerland, but lurking in the top ten are China, the Russian Federation and Ukraine, Brazil, India, Israel and Romania also often feature in the top 20 of countries visiting the site, countries not renowned for their love of skiing.

This unwanted traffic may not breach security (although one day it might), but it is a source of unwanted consumption of bandwidth and processor performance. The cloud has become a large diversified organisation. If anything, it is the smallest enterprise. If anything, it is the smallest operation that is more at existential risk from poorly managed information than large diversified organisations.

Associated with the architecture are clear policies and these should not only cover networked assets but embedded systems and stand-alone systems, indeed anything that has a microprocessor; remember Stuxnet?

Even a well-designed security architecture does not offer full protection if security operations are not effective. As the breaches at Sony demonstrate, a truly determined hacker may be able to overcome virtually any security measures.
With today’s smartphones, transferring money at a branch or ATM is quickly becoming a thing of the past. But how can you be sure that your money and personal information are secure when banking on your smartphone asks Alex Grant, Managing Director, Fraud Prevention, Barclays.

According to a recent study, over £4 billion worth of transactions were processed in a single month using smartphones in 2014. It’s undeniable. Using banking apps on smartphones to check balances or manage your money is becoming a way of life.

The growing reliance on these kinds of transactions has put security at the forefront for banks and customers alike. The new BSI Kitemark for Secure Digital Transactions assures security for a wide range of online transactions including entertainment and gaming.

Today’s website and software developers have to consider a wide range of threat vectors. Moreover, they have to ensure functionality over numerous disparate browsers and operating systems. This is particularly crucial with financial transactions, where the threat of password compromise or malicious URLs needs to be managed. Currently, criminals target websites and smartphone applications that manage financial transactions because the rewards are quick and plentiful, and because they’re able to exploit complexities within the systems that lead to vulnerabilities.

Despite the many secure software development methodologies already available, the pressure on developers to be more agile and deliver to market often leads to shortcuts and the acceptance of unnecessary risks.

Collaboration

BSI created the Kitemark as a sign of quality in the early 1900s, and it’s become a familiar symbol of quality, safety and trust in marketing and consumer materials over the years.

Barclays commissioned a survey to determine whether the presence of the BSI Kitemark would provide banking customers with a similar level of comfort – encouraging them to register for their free banking products. The survey concluded that wary customers were more likely to register for and use a product associated with the Kitemark.

Testing

A key part of any Secure Digital Transactions Kitemark would be the testing of the systems to be certified to ensure that they were secure to a measurable standard.

The common vulnerability scoring system (CVSS) was chosen as the most consistent and reliable method to measure the risk of vulnerabilities across software, infrastructure and services.

The Open Web Application Security Project (OWASP), Application Security Verification Standard (ASVS) was chosen as the standard to define the level of depth and rigour that testing would be conducted.

The functional testing of the product in its production environment rather than development releases was critical to understanding how susceptible the banking products were to external malicious attack and in setting a benchmark of what good looks like.

Penetration testing company Gotham Digital Science (GDS) performed the security testing to the level defined for the Kitemark and delivered a functional penetration test report that identified some vulnerabilities, but importantly none were above the critical CVSS value of 7.0, which would be considered a major vulnerability.

The management and resolution of lower risk vulnerabilities used a standard model that was an existing component of the ISO/IEC 27001 Information Security Management System operated by Barclays. A continuous surveillance visit by BSI ISMS auditors resulted in several actions that needed to be addressed to achieve the Kitemark criteria.

The BSI Kitemark certification ensures that a product or service meets the required British, European, international standard for quality, safety, performance and trust. Like ISO/IEC 27001, it is a voluntary certification, but is provided by BSI – which maintains impartiality and independence and is recognized for its rigorous standards for apps and online transactions. This includes a process of ongoing assessments to maintain high levels of security.

www.bsi.org

Reference
1. FS Tech. www.fstech.co.uk/fst/Barclays_Smartphone_App_Payments.php

SUBMISSIONS NOW OPEN

Journal of Cybersecurity is a new open access journal committed to providing quality original research and scholarship in the inherently interdisciplinary cyber domain.

Submissions are now open and published content will be available from Spring 2015.

cybersecurity.oxfordjournals.org
Security is a requirement on the business and the IT department have delegated to departmental level. However, the deliberate attacks have come from a few high value information incidents are the result of mistakes or deliberate acts. Where does the threat come from? The potential risk in the information security field is hard to quantify. From an actuarial point of view, rare major losses are harder to estimate than more frequent lower level losses. The biggest single risk to the business of not providing effective security is enormous, possibly ruinous. In general the business decisions relating to information security spending should be made on the basis of what level of risk is acceptable, and what is the most efficient way of achieving the necessary risk mitigation. IT security is a necessary burden for most organisations. Customers, partners, staff, suppliers and other stakeholders expect an organisation to be secure and it is, therefore, hard to sell security as a value-added commodity. However, the cost to the business of not providing effective security is enormous, possibly ruinous. Despite this, security professionals are always under pressure to cut costs. The cost of a security breach is often borne by a party other than the one that was responsible for the lapse. For example, individuals bear the consequences of leakage of their personal data, and are only partly compensated by the organisation that leaked them. The cost of a security breach is often borne by a party other than the one that was responsible for the lapse. For example, individuals bear the consequences of leakage of their personal data, and are only partly compensated by the organisation that leaked them. Security is subordinate to the business. In general the business decisions relating to information security spending should be made on the basis of what level of risk is acceptable, and what is the most efficient way of achieving the necessary risk mitigation. IT security is a necessary burden for most organisations. Customers, partners, staff, suppliers and other stakeholders expect an organisation to be secure and it is, therefore, hard to sell security as a value-added commodity. However, the cost to the business of not providing effective security is enormous, possibly ruinous. Despite this, security professionals are always under pressure to cut costs. The cost of a security breach is often borne by a party other than the one that was responsible for the lapse. For example, individuals bear the consequences of leakage of their personal data, and are only partly compensated by the organisation that leaked them. Security must therefore be viewed as a component within the risk management infrastructure of the organisation. The level of security should be determined by the needs of the business and in relation to the provision of all forms of risk mitigation. Various frameworks such as the ISO27001 family of standards, COBIT and its extended form RiskIT help to steer these deliberations, but judgements remain subjective. On a positive note, the growing importance of online transactions, the increase of regulatory compliance (including initiatives such as those of the payment card industry), and increasing awareness of cyber risks have increased the awareness of business leaders of the need for security.

You can’t secure what you can’t manage. Securing IT systems is an integral part of managing IT systems. The first requirement to secure something is to have an accurate record of what you have, how it is being used, and how it is being protected. Security information needs to be viewed from a holistic perspective in order to identify residual levels of risk resulting from policies and practices in each area of the corporate operations. Where does the threat come from? There is a wide gulf between headline-grabbing stories such as the Sony Studios hack and a typical cyber-attack. Most incidents are the result of mistakes or random malware attacks. However, the deliberate attacks have the most serious consequences. Deliberate attacks are planned, determined and often long-term. Such attacks may come from displaced employees and former employees, competitors, criminal gangs usually intent on fraud or theft, or governments. The criminal gangs are the main danger for most businesses. Attacks can involve a multi-stage process that starts with a social engineering approach aimed at stealing key passwords and user credentials for use in subsequent stages of the attack. In some cases spyware is downloaded into the organisation. However, ultimately attackers are driven by their own need for profit. This can come from a few high value information assets, a multitude of relatively mundane information assets, or from inflicting damage on an opponent.

Security management is a developing area for product support. The higher levels of security management have to dovetail into business process frameworks and risk management. The intermediate layers include monitoring and managing the configuration of IT infrastructure, and the security information and event management (SIEM) field. While most compliance regulations are expressed in business terms (with the notable exception of the payment card industry data security standard), the delivery of these requirements necessitates numerous security controls. This means that the reports available from security management products are crucial to satisfying compliance requirements. However, they do need to be re-presented in a format required by each set of regulations. When it comes to deploying security products it is helpful to get products that are well integrated with each other, even if this means selecting on a basis of fit-for-purpose, rather than best of breed. Many organisations are seeking to rationalise their suppliers to help achieve this, as well as to get better contractual terms.
DEVELOPMENT AND MENTORING

Jill Dann FBCS CITP, Director at Consultation Ltd, takes us on a whistle stop tour of BCSWomen Specialist Group’s methods and tools.

It is an individual’s responsibility to take on their own professional development and mentoring. The BCSWomen Specialist Group seeks to support women returning to STEM careers as well as to inspire women to have the best possible career utilising their potential.

That doesn’t absolve any employer from their responsibility to support employee development, however; development needs to support an individual in ways that make sense to them; one which extends beyond their workplace or current role.

Some women may not have resources from an employer or be on a career break or have other responsibilities holding back their ability to focus on their careers, for example, parental care, childcare responsibilities. Women are encouraged to join BCS and BCSWomen to gain access to the Personal Development Plan tools, the Career Mentoring Network (currently in pilot phase) and the group’s initiatives, such as the events run this past summer on the 3 and 23 June 2014, to train mentors in some of the necessary skills. The materials are available, both a slideshow and exercise workbook; Scotland and Wales have run their own branch events using them.

Your goals, your outcomes

Any development activity is only valuable in its effect on the individual, which is why we focus on outcomes. Reflection on what was gained from an activity is essential, as it can help focus on the valuable outcomes and aid future planning. Reflection on personal direction and development undertaken can then lead to goals and a clearer idea of what is actually helping.

A broad view of what works

What are relevant development activities? Basically, anything that helps you progress in a measurable way. If you are looking for activities with specific outcomes to meet development goals, then it is important to think broadly about sources of help and to recognise the triggers for changing behaviours. BCSWomen hold events around the country and can make materials available wherever you are based. Anything from an eBook, seminar, discussion and online material, to a conversation can contribute to your development. Structured activities like BCS courses and certifications can be very useful and, in some careers, necessary. A blended approach is a good idea focused on a goal to employment, role change or progression.

Reports and articles, through to joining a group committee, working group or contributing to a policy statement can lead to relevant outcomes against goals. Going for Chartered status can help to move your career forward. Simply meeting up with other professionals can expand your horizons, all the way through to more structured mentoring towards a particular purpose.

Guidance and resources

www.bcs.org/cpd contains a range of guidance notes that can help you set out on a development journey and has suggestions on resources and events that might be useful to you.

Getting systematic

Setting goals and recording your activities provides a basic structure for your development. With this in mind BCS has the Personal Development Plan (PDP), an online tool to help you record and plan goals and activities and is highly customisable to your needs. It’s available to all at www.pdp.bcs.org, but with some functions restricted to members. It embodies our philosophy of development, and it can be configured to suit your way of working. Members can also report against goals for sharing with others.

Mentoring

A mentor can, for example, help a mentee to acquire technical expertise, to gain knowledge and skills, understand appropriate behaviour in social situations and to understand the workings of an organisation and its expectations of their role.

No blueprint exists for the ideal mentoring relationship, but what is common to all cases of mentoring is that the mentee comes to view things in a different way with expanded horizons. The mentor engenders change in the mentee, helping that person towards a new vision of attainment.

Mentoring can be useful through any part of your development journey, helping you look at your career direction, planning goals, or as an activity against a goal. Mentoring others can, in turn, be very rewarding and a useful development activity in itself, as well as supporting the wider development of the profession.

This is a great way of getting support in your development and is a key element of BCS’s professional culture. Being a mentor is open to anyone who has something to offer and is not restricted solely to those with long experience.

The BCSWomen Specialist Group can provide the materials for interested members to run events to educate mentors and mentees. BCS plans to launch its Career Mentoring Network, which will enable members to make connections with mentors and mentees as well as through specific programmes (e.g. BCS Women, BCS Entrepreneurs).

www.bcs.org/bcswomen
What is the role of the Company? The Company is immensely active and despite its youthful status it punches far above its weight among the other livery companies. Some of the more tangible ways in which the Company achieves its Royal Charter aims include:

Charity The Company has been successful in supporting several charitable initiatives including partnering with Littleites – an organisation that provides assistive technology to severely handicapped children. The Company also founded IT4Communities, which links IT professionals seeking to give their time and talent to non-profit organisations.

Industry The Company is described in City circles as ‘a working company’, meaning it is made up of members who are still active in the occupation represented by the company. The Company also has links with BCS at both the organisation and membership level, and those links form the basis for several joint initiatives, such as an Oxford Union style debate in 2013.

The Company also has links with the trade association techUK, and many employers of IT professionals.

Fellowship The Company hosts a monthly informal get together at Bangers Wine Bar in the City of London, it also hosts four annual business lunches with notable speakers drawn from industry. There are a further three formal events; The Master’s installation service and dinner, The New Freemen’s Dinner and The Partners’ Dinner – a white tie banquet held at The Mansion House, which is the apex of the social calendar.

Civic duty The senior members of the Company, known as liverymen, have the right to participate in the annual election of the two sheriffs of the City of London, and with the City’s Aldermen they elect The Right Honourable The Lord Mayor of London - the world’s oldest extant democratically elected office.

Armed forces and cadets The Company has a long-standing relationship with The Royal Signals, the IT combat support arm of the British Army. The Company awards prizes for excellence among the soldiers and officers of the Royal Signals and provides career advice and mentorship for those transitioning from the military to civilian occupations.

The Company also has affiliations with two cadet forces units in the Greater London area. The cadets often provide a carpet guard at formal company events.

Church Whilst the livery companies welcome those of any faith or none, each Company is affiliated with a church in the City. The Priory Church of Saint Bartholomew the Great is the place where the Company comes together to worship for a number of annual events.

Relationship with BCS The Company and BCS have complimentary roles that enable both to collaborate where relevant, but focus on different societal issues. BCS focuses on developing the IT profession for the benefit of UK Plc, and for the IT professional. The Company focuses on charitable giveback and providing an environment for fellowship. The Company counts among its members many Members or Fellows of BCS and several past presidents.

Who joins the Company? The membership comprises business leaders, IT entrepreneurs, freelance IT professionals, academics, IT practitioners in businesses of all sizes and those working in allied professions such as law, financial services and the information content industry. With nearly 800 members, the Company is among the largest of the livery companies.

The Company has a diverse membership, already having provided three female Masters, and there are members from a wide range of social and ethnic backgrounds. What binds them all together is a desire to give back to the profession, and to meet in fellowship.

The Company also operates a very successful journeyman school, a mentorship programme for graduates in the early years of their occupation. Many of these journeymen (the term imports both genders) go on to become Freeman of the Company.

How does the Company link with tradition? The Company participates in many city-wide traditions such as the annual Lord Mayor’s Show and the United Guilds Service at St Paul’s. The Company also embraces the customs and ceremonies associated with all livery companies at formal dining events. Members have the opportunity to become Freemen of the City of London and even to stand for elected office in the City. Four members of the Company have served in the office of Lord Mayor of London.

What are the benefits of membership? The Company is one of those organisations where members get out what they put in, and consequently each member experience will differ. Some of the highlights of membership include:

- meeting with some of the most influential people in the IT profession in a neutral setting;
- participating in the traditions, customs and ceremonies of the City of London;
- becoming a Freeman of the City of London (yes, they can and do take sheep across London Bridge);
- the opportunity to make an immense difference in the lives of less fortunate people through charitable activities;
- participating in some truly memorable and historic social, civic and professional events;
- mentoring entrepreneurs, small business, students and soldiers to help them develop and grow their IT career.

A common misconception is that livery companies are a branch or offshoot of Freemasonry. Whilst there is no direct connection between the livery companies and Freemasonry, it is probable that Freemasonry grew out of the City of London livery companies in the late 17th Century. You don’t have to be a Freemason to join a livery company.

What if I don’t live in or near London? Livery companies are creatures of the City, and as such their life is centred on the City of London. However, the Company has members all over the UK and there are regional groups outside of London. There is a wealth of sporting and social events that happen outside of the City and many ways for members to get involved without regularly coming into London.

How would I go about joining? The Company is always keen to welcome new members, male or female, young or old, short or tall! The best place to start is to contact the Company at IT Hall and ask for the application form. If you don’t know anyone in the Company, then the staff at IT Hall will put you in touch with someone who shares a similar background or perhaps lives near to you.

www.wcit.org.uk
INTRODUCTION TO BCS HEALTH

Gareth Baxendale FBCS, Head of Technology, National Institute for Health Research, Clinical Research Network, University of Leeds, introduces himself and BCS’s health informatics group, BCS Health.

We all like a warm welcome, so please accept a convivial welcome from the volunteers and BCS staff that make BCS Health what it is today.

Now we’re all friends please let me share with you a little about who we are…

What is BCS Health

Well, perhaps I should start with the role I play on behalf of BCS Health. I have recently been privileged to take on the role of Vice Chair Communications and Publications, so it will come as no surprise that I am somewhat keen on socialising and educating (pretty much with anyone who will listen) on the amazing work and effort that goes on at BCS Health.

We work as volunteers bringing our professional experience to the table to help with health IT challenges and support the interests of both patients and health professionals.

We work as volunteers bringing our professional experience to help with health IT challenges and support the interests of both patients and health professionals.

BCS Health has many branches of activity that you may not be aware of, in fact many of the activities you are welcome to join and participate in. BCS Health’s focus is really about modern healthcare and both the technology and patient data that support it.

On the subject of data, BCS Health feeds into an independent group called the Professional Records Standards Body, which was set up to represent patient and care professional organisations on the type and structure of data that should be included in care records.

BCS Health also works to influence policy and is represented on the BCS Policy & Public Affairs Board who consider policy affecting the IT profession and wider society. BCS Health also works with government and responds to relevant activity that you may not be aware of; in fact many of the activities you are welcome to join and participate in. BCS Health’s focus is really about modern healthcare and both the technology and patient data that support it.

On the subject of data, BCS Health feeds into an independent group called the Professional Records Standards Body, which was set up to represent patient and care professional organisations on the type and structure of data that should be included in care records.

BCS Health also works to influence policy and is represented on the BCS Policy & Public Affairs Board who consider policy affecting the IT profession and wider society. BCS Health also works with government and responds to relevant activity that you may not be aware of; in fact many of the activities you are welcome to join and participate in. BCS Health’s focus is really about modern healthcare and both the technology and patient data that support it.

On the subject of data, BCS Health feeds into an independent group called the Professional Records Standards Body, which was set up to represent patient and care professional organisations on the type and structure of data that should be included in care records.

How to get involved in BCS Health

As a member of BCS you can simply join our merry band by selecting ‘BCS Health’ from the list of specialist groups in your secure membership area. Upon selecting the option you will not only enjoy a warm fuzzy feeling, but also start to receive updates and invitations to specialist events sent out by BCS Health.

You can also join a regional BCS Health Group including BCS Health Wales, Scotland, Northern, London & South & Eastern England, Ireland, and Northern Ireland and other supporting groups such as BCS Primary Health Care, BCS Assist and BCS Nursing. All play a part in shaping and influencing key issues faced by patients and professionals across the health IT spectrum.

www.bcs.org/health

BCS Health also works to influence policy and is represented on the BCS Policy & Public Affairs Board who consider policy affecting the IT profession and wider society. BCS Health also works with government and responds to relevant activity that you may not be aware of; in fact many of the activities you are welcome to join and participate in. BCS Health’s focus is really about modern healthcare and both the technology and patient data that support it.

On the subject of data, BCS Health feeds into an independent group called the Professional Records Standards Body, which was set up to represent patient and care professional organisations on the type and structure of data that should be included in care records.

How to get involved in BCS Health

As a member of BCS you can simply join our merry band by selecting ‘BCS Health’ from the list of specialist groups in your secure membership area. Upon selecting the option you will not only enjoy a warm fuzzy feeling, but also start to receive updates and invitations to specialist events sent out by BCS Health.

You can also join a regional BCS Health Group including BCS Health Wales, Scotland, Northern, London & South & Eastern England, Ireland, and Northern Ireland and other supporting groups such as BCS Primary Health Care, BCS Assist and BCS Nursing. All play a part in shaping and influencing key issues faced by patients and professionals across the health IT spectrum.

www.bcs.org/health

Within the UK healthcare sector, NHSmail is rapidly being adopted by NHS trusts. As the only dedicated mail system to have received government OFFICIAL SENSITIVE accreditation and be fully approved by the Department of Health for the purpose of sharing patient identifiable and other sensitive information.

As a result, the vast majority of NHS organisations are using it in some form, with usage growing due to the refresh initiative driven by HSOIC, as well as the approval of the ISB 1594 Secure Email standard in March 2014. NHS trusts and organisations are being encouraged to either move to NHSmail or bring existing email systems in line with the new standards.

NHSmail is currently being used by over 500,000 GPs, healthcare workers and other staff within the NHS. It brings a number of benefits to users, especially the ability to efficiently store, access, share and archive sensitive information. NHSmail or bring existing email systems in line with the new standards.

NHSmail is currently being used by over 500,000 GPs, healthcare workers and other staff within the NHS. It brings a number of benefits to users, especially the ability to efficiently store, access, share and archive sensitive information.
manifestos
making the UK THE IT PLACE TO BE

According to Nesta UK (formerly NESTA, National Endowment for Science, Technology and the Arts) political manifestos have actually been quite successful in incorporating new trends – for example the rise of automation and the creation of the internet. However, they also caution that ‘they rarely set out clear policies for taking advantage of new trends, or for mitigating their risks.’

Noting that government is also poor at predicting the shocks that such trends can cause and taking into account the increasing speed of change in the digital landscape, getting the approach to national digital strategy right requires expert input.

landscape, getting the approach to national policies for taking advantage of new trends, or for mitigating their risks.’

UK startups and innovation

1. UK startups and innovation

The Coalition for a Digital Economy (Coadec) report that the ‘UK’s internet economy makes over 8 per cent of GDP and predict that this will grow to 12 per cent by 2016. Also noting that the UK was the fastest growing economy in G20, it draws attention to the role of micro-entrepreneurs in creating innovative services. This means that innovation often has its roots in the startup ecosystem, making it key to continued UK growth.

One problem Coadec draws attention to is that of funding, noting that whilst seed funding can be easier to get, taking ideas, products and innovations forward, which needs more funding, is increasingly tough.

Like many of the eight main themes there is cross-over with other areas. In this and the earlier discussion on job creation the link is made explicit by e-Skills, in quoting the 2007 Kauffman Foundation study, which says that most job creation comes from entrepreneurship.

The link is made explicit by e-Skills, in quoting the 2007 Kauffman Foundation study, which says that most job creation comes from entrepreneurship.

Coadec wants to create an ‘environment to encourage permission-less innovation where possible’. e-Skills adds a practical aspect to this with their view that every country in Europe needs a ‘jobs through e-entrepreneurship’ campaign. TechUK sees even further, asking that we make the UK a ‘global hub for talent with a smart migration policy’ to attract wealth creators to the UK economy who can use and disseminate the skills needed to make innovative ideas fly.

What is BCS’s take on this? Simply that we should aspire to make the UK a melting pot for innovation.

The UK should be the destination for innovation in IT, and the organisations that can make this happen go beyond the exciting start-ups at digital roundabout to the bodies that take the lead in the profession, government, policy bodies and more.

Indeed, the BCS Entrepreneurs Specialist Group aims to engage with entrepreneurial communities to grow the digital ecosystem for the benefit of members and society, provide a real-time forum for existing and would-be entrepreneurs to network with an expert group of innovation stakeholders from government, established and emerging technology enterprises and digital support clusters.

Tech in government services

A phrase that comes up several times in the government services space is ‘government as a platform.’ Whilst it may be tempting to see this as buzzword creation, both Coadec and the Policy Exchange put substance to the bones, with the idea that government should release APIs for government services, allowing others to innovate on top of them.

TechUK also discusses the use of commoditised and utility solutions to standardise functions and the sharing of data. If there is a need for bespoke services, which TechUK concedes there may be, it adds the useful corollary that these be implemented in ways to promote further growth – for example allowing SMEs to reuse the intellectual property (IP) they may have originally developed for government contracts.

More specific suggestions come from the Policy Exchange, which thinks that the civil service competency framework should be updated to include IT skills and TechUK suggests the next government should appoint a chief privacy officer to oversee and maintain public services.

As BCS notes, services are increasingly digital by default – and that is a good thing. The Institute necessarily has this default position – indeed BCS already does a lot of good work in tandem with government, including influencing at the policy level. More specifically in recent years the Institute has had a pivotal role in introducing a proper computer science curriculum for schools – and continues to support users with ECDL.

Digital skills

The need for support and ongoing support for digital skills comes out loud and clear in nearly every manifesto available. As eSkills comments, one of the problems is ‘Warhol-esque: Today when you graduate you are set for, say, 15 minutes.’ But it also adds in the problem of the narrow field of view because national IT policies tend to focus on developing basic IT skills. One of the problems is the digital inclusion gap. It would be tempting to think that we are completely over digital skills when only 83 per cent of the population is online (Policy Exchange compares this to the 98 per cent plus penetration in Norway and Iceland). The new computer science curriculum, which, as noted above, BCS was instrumental in bringing into being, is mentioned in several manifestos. Coadec notes that the suggested £3.5m to support teachers in their teaching of the new curriculum amounts to only £175 per school – unfavourably comparing that to the £15,000 per school that Jersey has provided – albeit with fewer schools.

Policy Exchange is even more parsiomous with its £13m pot for a competitive grant to fund third parties to deliver teacher training for the new curriculum.

On the same issue the UK Digital Skills Taskforce says a minimum of £20m over the next Parliament is needed to assist teachers.

One suggestion to combat this issue comes from Coadec, which suggests incentives for startups to help train teachers. Where an entrepreneur would find the time may be another question - a job too far?

Conversely, the National Institute of Adult Continuing Education (NIACE) says that investment in skills is ‘too heavily focused on young adults at expense of over 24s.’ And with the issue of extended working lives coming nearer then life-long learning becomes even more necessary.

As e-Skills notes the ‘full potential of e-government will only be seen when the European population is connected to the internet and e-skilled.’ For the population at large e-Skills suggests a European standard for e-competency, calling for EU-wide indicators of digital competencies and media literacy. This follows an EU report showing that only 25 per cent of people self-report a high level of digital competency.

Managers and others in the digital skills space – and not just in education and large business organisations, but also SMEs and the civil service. This is not just an education piece – there is a disconnect with actually policy.

Lessons can and should be learnt from recent history. In the UK the education system has failed to educate those coming into it, with a historic failure to educate at the school level in computer science disciplines and, whilst there is progress now, it could be said to be 20 years too late. Technology is already at the core of all businesses. The House of Lords is currently undertaking a review of digital skills, and skills have been added as an important part of this inquiry. BCS sees this as a good starting point in the vital upskilling process that needs to happen. However there are caveats to this discussion. BCS notes that there is a strong sense of déjà vu about some of these initiatives. Similar discussions took place in Peter Mandelson’s Knowledge Economy drive in the 1990s. Now these things must be actioned.

One route that needs pursuing is ensuring that there is a tax regime that stimulates growth, especially as the EU already looks to the UK as a good exemplar in this area.

And what about IT professionalism and digital skills in the civil service itself? Reportedly, no government departments are pushing for continuous professional development initiatives, yet it is understood, can promote and views as vital for the
development of the industry. To help the public to take advantage of digital services it was suggested by BCS that there could be incentives and help made available so the public can all use them. There also needs to be confidence in the system, as there are still fraud issues and perceptions of cyber-danger that put users off. People will be reluctant to access online services if there are no assurances.

BCS notes a strong sense of déjà vu. Similar discussions took place in Peter Mandelson’s knowledge economy drive in the 1990s.

End-to-end services should be securely coded. The example of GDS, which has developed products and services that people want to use, was mentioned. But, in the end, BCS wants people to use digital services because they are the easiest way rather than because of incentives.

Identity assurance and security

For members of the public this is a big issue. The Policy Exchange put forward the concept of an independent data ethics committee. Its idea is that this would include not only representatives from government, business, the charity sector and legal groups, but from citizens’ groups as well. It sees the creation of a Code for Responsible Analytics to guide the government in the responsible use of data. If this included collection and re-use issues, that would be a good approach.

European and global integration

An European Commission report from 2014, Does digital tech create or kill jobs?, suggests that there is a strong sense of déjà vu. Previous discussions on opening data use, said that the UK needs to continue to succeed in superfast broadband and raise the level of ambition for digital infrastructure. Especially taking into consideration where the next areas of growth for IT are likely to be. According to figures from the techUK report, these are (with value estimates):

- IoT $7.3bn by 2017;
- wearables $70bn 2024;
- $6-40 fold increase by 2018;
- robotics $24bn 2018;

As techUK notes these tech trends are disruptive and global. Three interesting views come up here: Coade suggests that ‘most investment in digital infrastructure should be funded by the private sector’. But we may well ask where that leaves less well-populated areas, which are more expensive to get to. The Policy Exchange gives a specific example of opening data use, saying that ‘Ordnance Survey should cease to be a government monopoly and be removed from the Shareholder Executive to make their maps and data free to use’.

Policy Exchange: HMRC has 80 times as much data as the British Library

There is a danger of over-regulation, which could stifle business and restrict freedoms – especially as UK PLC’s success is increasingly based on services provided over the internet. The BCS view is that generally the UK approach is ahead in aspiration and delivery. However there are issues around identity assurance. There is a presumption that a citizen is in control of their own data – very much in keeping with web-creator Sir Tim Berners-Lee’s recent comments on the subject, which BCS agrees with.

It goes on to say that DP legislation should focus on use rather than the collection of data, quoting the stunning figure that HMRC has 80 times as much data as the British Library.

Policy Exchange recommends that the government conduct annual reviews to ensure that legislation and the regulatory and legal systems on intellectual property keep pace with technical change. Is this laudable goal realistic or even workable?

The work force

The work force suggests that the skills gap is larger in UK tech workforce. Coadec usefully asks how the European Commission report from 2014 on EU data protection and privacy regulation do not take into account such issues 'the value of user ratings, social media and personal data and reputation. It calls it a retrograde step with unintended consequences, perhaps an example of being badly affected by well-meaning provisions’ mentioned by Coadec. It maintains that there should be a presumption that a citizen is in control of user ratings, social media and personal data and reputation. It calls it a retrograde step with unintended consequences, perhaps an example of being badly affected by well-meaning provisions’ mentioned by Coadec.

EU views: Europe and regulation

Does digital tech create or kill jobs?

The UK has had an uneasy relation with the EU. Beyond the toing and froing of political posturing, the Institute aims to take the global view into account too. The internet is global and therefore should be talked about in a global context - and not all EU views are shared globally.

In a joint submission from the techUK committee, its idea is that this would allow of data use to benefit UK business are huge – and get bigger when it moves from heavy industry. Progress in the allowing of data use to benefit UK is less forward-thinking. For example, there is less well-populated areas, which are more expensive to get to. The Policy Exchange gives a specific example of opening data use, saying that ‘Ordnance Survey should cease to be a government monopoly and be removed from the Shareholder Executive to make their maps and data free to use’.

Policy Exchange: ‘Ordnance Survey should make their maps and data free to use.’

This means that the interface needs to be functional and simple to use. As mentioned before, Estonia is an interesting case – a place where everyone is online. Could that be the aim for the UK? This raises questions on the extent of the role of government and where it should cross-over with the private sector on, for example, the rollout of high-speed broadband to the whole population, regardless of the geographic difficulty in doing so.

The government also has a huge role in protecting citizens’ data. As technologies, app-driven experiences and online traffic volumes have increased, has the idea of consent been made more no viable? The BLS skills agenda should include educating parliamentarians – they are making decisions based on briefings that may not give a full enough picture. The BCS campaign strand on professionalism includes the idea of accountability – and whilst we would not expect parliamentarians to be held to the standards of a fully-fledged IT professional, education at this level is paramount. The pace of change outstrips legislation easily. We are facing a future of work that will include driverless vehicles, computerised health diagnoses (see Watson), streams of data coming from personal databases and autonomous machines on the IoT - possibly anonymised, possibly de-anonymisable.

BCS views: The impact on the individual

Individual citizens need to know where they stand, have a clear view of their rights and expectations and a way of keeping abreast of workplace change. Notable IT systems failures in the past have made people wary, with the feeling that adequate security controls are not yet in place. We have not yet reached the point where citizens make decisions based on trust of government.
When Henry Tucker went to CES2014 one of the things he was most impressed by were Audi’s computer controlled cars. You could park them simply by pressing a button on your smartphone. They could also take the controls in slow moving traffic, but because of legislation they couldn’t do more than that.

At CES2015, Audi was once again in attendance with what looked like the same cars and the same technology. This time though at least one of the cars drove itself from California to Las Vegas for CES. This is the sort of leap forward I was expecting. After all, the previous year’s car had control hardware and software the size of a laptop whereas the previous year had a whole boot full! The thing is the technology exists to make self-driving cars safe. The Audi has six radars, three cameras, and two light detection and ranging (LiDAR) units. The computers that allow the car to analyse the road, choose the optimal path and stick to it fit neatly in the boot. What is holding the industry back is legislation. The common argument, when people are presented with computer controlled cars is, ‘what if the software crashes?’ To which I would say: is that any different from your car breaking down? When you look under the bonnet of modern cars there are two things you can access yourself, unless you happen to be a mechanic, and they are the oil and the water for the windscreen washer. With a computer-controlled car it’s exactly the same. The other thing people sometimes say is, ‘what if it goes out of control?’ Now this is clearly from the realms of a Michael Crichton thriller where the cars go wrong and start acting malevolently. Again this isn’t going to happen. Software and hardware already exists to remotely disable cars – car rental firms use it to disable stolen vehicles. Software and hardware only go out of control because of human intervention, not through their own will.

I think that computers will be better drivers than humans; they won’t take risks, they’ll stick to speed limits and will be more efficient. One thing you do need in order to have these self-driving cars though are accurate maps. Paper maps and sat navs are never 100 per cent accurate. With this in mind we had a chat with Nokia about its mapping project called Here.

It is sending cars out around the world to map roads in amazing detail so that cars, such as the Audi and every other one, can drive safely on the roads worldwide is road works and the associated traffic jams that they often cause. The constant stop-start nature of these jams is something that Bosch is looking to address with its Traffic Jam Assist technology that it is introducing in the first part of 2015 to give drivers a ‘hands free experience’ in jams up to around 45mph.

QNX, a subsidiary of Blackberry, showed off a system of driver assistance that uses sensors, cameras, navigation engines, cloud-based services, speech interfaces, and acoustics software to create experiences that simplify driving tasks, warns of possible collisions and enhances driver awareness. At the 2014 show I spoke to BMW and they told me about their system for in-car apps and it now seems that Ford has got in on the act too. The company showed off its systems where you can access your phone’s apps using the app link tool, including services such as streaming music app Spotify. One thing that annoys probably every driver on the roads worldwide is road noise, and the associated traffic jams that they often cause. The constant stop-start nature of those jams is something that Bosch is looking to address with its Traffic Jam Assist technology that it is introducing in the first part of 2015 to give drivers a ‘hands free experience’ in jams up to around 45mph.

Even companies such as nVidia, which is usually associated with computer graphics development, have got in on the act. In fact at CES2015 the main features of its stand were two cars. It showed off its new nVidia Drive PX that features a Tegra X1 processor that is designed to power a car’s digital cockpit experience such as the sat nav and entertainment functionality. It also showed off its nVidia Drive PX in-car computer that allows for app development for semi and fully autonomous driving. One such application is nVidia’s own Deep Learning that, according to nVidia, allows your computer to learn from its surroundings and, to quote nVidia, ‘become intelligent’. It also features surround vision, 360 degree cameras, that can be used for autonomous parking.

Driving around in our cars is, statistically, one of the most dangerous things we can do. Technology such as this will, I think, start to make the road a lot safer for all of us.
THE ACCESSIBILITY BUNFIGHT

AIS is now part of the UK Disability Strategy and is a developing model for other sectors. Documents in alternative formats and face-to-face support are in scope. However, despite obvious overlaps, the web was ruled out. I immediately called for development of a parallel standard for ‘the orderly conduct of bunfights’.

Stuck in the very problem I’m trying to solve, I am a deaf and blind health informatics academic. Reading, writing, presenting, facilitating are all impossible for me without technology.

The right tools in the right hands help everyone, said Stephen Hawking at the 2012 Technology For Good Awards.

Yet I have found very few, truly accessible academic tests. My assistive technology – a screen-reader that converts onscreen text into synthetic speech or braille – works with few of the guides and tools avalable in education and collectively known as EduApps.

I cannot send a legible text message on an iPhone without a bluetooth keyboard.


Evidence of considerable need

Accessibility should be mainsteam by now. Small screen, multi-environment mobile phones are widespread, while literacy challenges are a known, national problem (the Office for National Statistics [ONS] quoted 56 per cent of the Northern Irish adult population as examples, before updating that page [accessibility policy] in 2013).

This - from the consultation document preceding the NHS Information Strategy – suggests possibilities for mutual understanding between the IT mainstream and disabled people through shared (assistive) technologies.

‘Voice recognition software is used to great effect in a number of clinical settings. Significant improvements are expected in devices to allow touch and even gesture input of information into computers.’

Support for professional personas, like me, is unclear. A Freedom Of Information Request in 2010 showed that Access To Work (the Government agency supporting disabled people in work) does not record job roles or technology provided.

Across university students, ca. 10 per cent have disabilities (in 2011/12 78,905 out of a total of 870,910). The Higher Education Statistics Agency provide free data on students by disability categories, but not their academic disciplines.

The chart below shows the spread of impairments reported to HESA in 2011/12, the latest year for which figures are available. ‘Learning difficulty’ probably means dyslexia and is the highest group by far. Those with sight or hearing loss seem very under-represented. Data on staff were not available. It should be noted that these are self reported impairments. Many people choose not to reveal any impairments they may have, so the true numbers will be higher.

Data on the general population come from the ONS. Its ecommerce monitoring development programme includes mobile and internet use from its existing Never Ever online survey.

Between 6 and 7 million people have never been online. A further 9 million people are online but in need of help. Most of the people in these categories are older or disabled people.

Assumptions about who needs what might be made based on another ONS process, from version 1 in 1999. WCAG updated to version 2 in 2010.

WCAG2 is expanding (mapped to and appropriately adjusted) to cover documents and software, through general ICT, and to interactive web pages, via the rich internet applications (RIA) programme.

Between 6 and 7 million people have never been online. A further 9 million people are online but in need of help.

A special working group - on cognition and learning disabilities - has recently formed to encompass many traditionally excluded by the predominance of text. Their scoping document identifies many groups, including dyslexia, and many missing technologies.

WAi is built into the British standard (BS8878). It is developing through several specialist teams, an interest group and an education and outreach task force. Nevertheless, I still feel more needs to be done to make the WAi approach easy to understand and implement, especially by those like me dependent on assistive technologies.

Join the bunfight

I focus on health. It keeps doors open in all other sectors of society.

We know the scale and we have the data to estimate needs. The accessibility standards, though not fully developed, are essentially in place.

The AIS Chair, who launched the bunfight, also said ‘I’ll buy the champagne if we pass full stage approval.’

Now is the time to make the party happen. Support NHS England through the BCS Digital Accessibility Specialist Group and all its connections.

The champagne is on order, and I’ve promised to provide the buns!

www.bcs.org/groups/dasg

The Society of IT Managers ‘better connected’ programme found only 25 per cent of council web and mobile sites met even basic accessibility standards. Abilitynet have found similar in eNation reports.

The One Voice Coalition for Accessible Technologies.

Accessibility Alliance advising government.

EAT has now merged with the former e-access forum to become the Digital Accessibility Alliance advising government.

One Voice also won this pledge at the Lib Dem’s 2014 main conference: Review anti-discrimination law, accessibility policy and all its connections.

ITNOW has promised to provide the buns!

Join the bunfight

I focus on health. It keeps doors open in all other sectors of society.

We know the scale and we have the data to estimate needs. The accessibility standards, though not fully developed, are essentially in place.

The AIS Chair, who launched the bunfight, also said ‘I’ll buy the champagne if we pass full stage approval.’

Now is the time to make the party happen. Support NHS England through the BCS Digital Accessibility Specialist Group and all its connections.

The champagne is on order, and I’ve promised to provide the buns!

www.bcs.org/groups/dasg
STATE OF PLAY REPORT

BUSINESS INTELLIGENCE


The 2015 IT spending forecast from computerworld.com listed five areas where respondents expected increased spending, and third position went to analytics and business intelligence.

Harnessing big data through enterprise analytics, data mining and BI had 38 per cent of IT executive respondents to the survey expecting to spend.

They quote Gartner analyst Richard Gordon on the new data coming into the enterprise: ‘There’s a wave of data coming from customers and social media. And as the internet of things rolls out, there will be even more information on customers. Businesses are scrambling to figure out how they can extract value from that information.’

According to Andrew Brust, Research Director of Gigaom Research, in each of the last few years there has been an overarching theme in the data arena. He says that 2012 was the year big data became really hot; 2013 was the year it grew more accessible, through SQL-on-Hadoop; and 2014 was the year it became far more versatile, with the addition of ‘YARN and Spark. 2015 will be the year Hadoop matures.’

Whilst that may mean that there are no huge breakthroughs, Brust notes that the maturing of BI technologies will see a move to more standardisation, more adoption and therefore a more successful integration of BI into the enterprise.

He predicts that Hadoop will become more usable, more adoptable by the enterprise and more developer friendly. More on Hadoop, NoSQL, and relational databases are in the Gigaom report ‘Outlook: Big data and analytics in 2015’.

The mention of analytics in that title is key – there has been a lot more coverage during 2014 on the role of analytics. BI solutions are more readily embraced the more obvious their benefit is, so easy-to-use analytics are key to a successful BI platform.

Big data continues to be a much-bandied phrase, especially as it relates to predictive analytics, but of course many industries have been using data and analytics for decades – the new tools just make it much easier. One article in the BCS report shows the potential benefits of predictive analytics for the healthcare industry. IT Professional magazine examines what is truly new in terms of predictive analytics, and what it means for the IT industry.

Pat Saporito from the SAP Global Center of Excellence for Analytics, says that BI centres of excellence can play a key role in managing corporate growth and in enhancing the ‘analytic IQ’ of business managers and owners. He shows that centres of excellence can define and rationalise a BI strategy, and ensure that the analytics get put into action.

Amongst other areas discussed, the BCS report highlights pieces that look at the need for supply chain organisations to use effective business intelligence tools to stay competitive; the role of real-time data warehousing as a powerful technique to achieve operational business intelligence; and the increasing use of BI outside commercial organisations.

For example, public sector offices in the US are now expected to perform like private industries in collecting and providing pertinent information, according to one piece in the report. Even though the use of BI in the public sector is still in its infancy, the case study from the DeKalb Country Government located in Georgia, which has implemented business intelligence tools for its data management including social services, billing and public safety, makes for an interesting read.

In other areas, there are three case studies looking at the use of business intelligence tools by accounting firms in the USA. And in terms of practical applications, the BCS report covers an article on how one Fortune 500 company built itself a real-world Microsoft BI dashboard; a piece on how BI can support marketing strategies, based on a case study approach; and an article on how to take control of your BI with the tools offered by SharePoint 2013 and Microsoft SQL Server 2012.

Strategy

Best practices for business intelligence

This short article presents a list of 11 best practices for business intelligence, which the writer has adopted from a number of online resources. They include: the need for solutions to produce findings that are immediately actionable and trustworthy; and having constant input from business leaders to keep IT on the right track. The key point, according to experts, is to form an ongoing partnership between business, so the resulting BI solutions are embraced as easy-to-use and strategically relevant.

By Dennis McCafferty
Source: CIO Insight, October 2014

Selecting the BI platform for your organisational requirements

This article discusses ways of finding the right business intelligence (BI) platform for business enterprises and government agencies. The writer describes the factors which typically define the different types of BI tool users. He also explains the different integration characteristics and the level of importance on which evaluation of a BI platform should be based.

By John Mateicki, DeKalb County

Government (Georgia), and president of the Independent Oracle Users Group
Source: Database Trends & Applications, June/July 2014

Analytics

Getting started with predictive analytics

This article discusses the emergence of business intelligence, and particularly predictive analytics, in the healthcare industry. The writer describes what predictive analytics is and its potential for the healthcare industry, and then goes into various cases of how it is being used by marketers and medical professionals in the USA. One hospital, for example, targeted people considering a mammogram with a campaign about its mammography equipment, greatly increasing take-up. The article includes a section on best practices for putting together a predictive analytics strategy.

By Lauren Dretl and Julie Davis
Source: Marketing Health Services, autumn 2014

Big data and predictive analytics: what’s new?

There’s a lot of noise about big data, especially about its role in the new and exciting field of ‘predictive analytics’, but many industries have been using data and analytics for decades. This article examines what is truly new in terms of predictive analytics, and what it means for the IT industry.

By Seth Earley, Earley & Associates
Source: IT Professional, January 2014

SAP, Oracle Lead Sluggish BI and Analytics Software Market

This article discusses research by Gartner that showed the global business intelligence (BI) and analytics software market rose to US$14.4 billion in 2013, with annual growth slowing to 8 percent. Macro-economic factors were the most important reason behind slower growth, but it was also due to BI budgets remaining flat and confusion on how to use analytics. At a segment level, businesses were moving from reporting-centric to analysis-centric tools. SAP had the largest share of the worldwide market with Oracle in second place.

By Nathan Eddy
Source: eWeek, May 2014

Business process analytics using a big data approach

Business users can continuously improve their processes by using advanced analytics methods and emerging technologies, such as business intelligence systems, business activity monitoring, predictive analytics, and behavioural analytics, and in enhancing the analytic IQ of business managers and owners. The writer says that today BI COEs define and operationalise a BI strategy, and ensure that the analytics get put into action. She lists the practices to consider including in a BI COE, such as ensuring data is trustworthy, and providing easy access to reports and analytics.

By Pat Saporito, SAP Global Center of Excellence for Analytics
Source: Best’s Review, October 2014

An overview of information tools and technologies for competitive intelligence building

The paper looks at competitive intelligence (CI), which is a subset of BI, and concentrates collecting and analysing information about the behaviours of the various markets’ actors in order to make decisions based on market trends. This type of information is mainly of a semi-structured or unstructured nature, in contrast to the well-structured information used in BI. The research study is mainly exploratory and descriptive in nature, with the objective of providing an overview of CI issues and investigating the various information tools and technologies for CI building. It also highlights the most important differences between BI and CI. By Celina M Olszak, University of Economics Katowice, Poland
Source: Issues in Informing Science & Information Technology, 2014
WHAT DIGITAL LEADERS WANT AND NEED

Everyone wants a larger budget, but when only 8 per cent of participants feel that their organisation has enough resources and more than 79 per cent indicate that they need enhanced IT skills among their existing workforce or additional IT staff, the digital leader has plenty on their plate for 2015.

For the fourth year BCS, The Chartered Institute for IT has run a survey looking at the needs of the digital leader. And as the development of IT systems, the more the business views and key problems stay much the same.

For example, fifty five per cent of participants rate business transformation and organisational change as among their organisation’s top three management issues for the next 12 months. This is followed by strategy and planning (50%) and operational efficiencies (48%).

Businesses are clearly seized of the need for IT to effect change in their business dealings and internal organisation. As would be expected, SMEs and corporates have slightly differing needs: Among SMEs the issue most likely to be in the top three over the next 12 months is strategy and planning (59%).

For companies with over 250 employees, business transformation and organisational change (61% versus 40%) and operational efficiencies (53% versus 36%) are more likely to be high priorities than for SMEs.

Some issues were mentioned in the ‘free text’ part of the survey that will undoubtedly become more common concerns in the medium-term, such as, regulatory response (which perhaps only comes onto the radar when legislation is more immediately looming); and platform rationalisation.

Specifics: top IT topics

As to specific issues that need to be addressed, it’s no surprise to see the greatest number of respondents (60%) rate information security as among their organisation’s top three IT topics for the next 12 months. This was followed closely by areas that have moved well out of the ‘jargon’ phase and into business critical applications: cloud computing (55%) and mobile computing (53%).

These are the same three issues that were identified in last year’s survey. However, the order has changed with information security and cloud computing going up one place and mobile computing dropping two places.

Analysis by number of employees shows that information security is the top answer for both SMEs and large companies (over 250 employees).

Mobile computing is more likely to be a high priority for larger companies compared with SMEs (56% versus 45%); whereas social media is more likely to be a high priority for SMEs compared with larger organisations (24% versus 9%) – perhaps a reflection of the shift in marketing approaches.

The next concerns for the large organisation were big data (36%) and agile (22%).

Some of the issues much-discussed in the media are not yet really on the business radar in a large way, perhaps indicating their niche market status at present. These were the internet of things, with only 11 per cent representation, and 3D printing with a paltry one per cent. Other topics mentioned were agile and operational alignment; robust IT for SMEs; hosted telephony; general IT reliability issues; the government digital agenda; human-centred computing; network bandwidth growth and new platforms.

Having said that, the survey suggests that recruitment and retention is a higher priority for more companies compared with 2014 (up from 14% to 20%).

CEO’s in large enterprises are idiots - they no (sic) nothing about the processes the IT department uses for risk acceptance and design.

‘Larger organisations are more likely than SMEs to need additional suitably qualified IT staff (58% versus 43%). Other concerns that cropped up, although in much smaller numbers, were effective corporate and IT governance; business change expertise; and, to quote a comment, better CEOs and other execs who understand digital tech and its impact on organisations’

There is a need for, ‘quality managers who understand much more than simple economics.’

Biggest IT skills gaps: people

people issues surrounding IT skills are broad ranging. Let’s start with a refreshingly honest assessment of those at the top: ‘CEO’s in large enterprises are idiots – they no (sic) nothing about the processes the IT department uses for risk acceptance and design – and are more interested in shiny things or things that make them look good. They need to think about what they are doing and stop poncing about pretending to know what they are doing when it is clear that they have never worked in IT for real, ever.’

Some comments on this problem were more circumspect helpful! I – summed up well with the need for ‘understanding of
the business and bridging the gap with the organisation’s vision and ‘understanding of the business objectives driving IT choices.’

The gap in knowledge is more than just in management for some. One person said businesses need to do a better job of looking at where they are going – and now meaning that the world has moved on. IT departments themselves are in danger of becoming the biggest blocker on effective organisational modernisation.

One comment mentioned the need for, ‘quality managers who understand much more than simple economics – people who are the key resource to be managed and encouraged, not beaten into submission.’

Other places where soft and hard skills may overlap, and mentioned specifically by commenters as problem areas included simple experience: commercial knowledge and experience; the need for more and better project managers; implementing agile methods; and fostering a competitive workforce market. People issues seem to be in the category of problem areas – by definition a small recruitment pool. More forward-looking were some of the technical concerns that may impact the business. Mentioned specifically were concerns over the complexity of virtual environments, agile systems maintenance and migration to a post-Java script web.

One organisation’s loss is another’s gain in this scenario, with problem areas included such as: professional development of solutions provided by the private sector.

Some commented on the implications of outsourcing, asking for, in one case, ‘In-house staff [project coordinators] to be better captioned, getting delivery of service providers included from the private sector.’

This respondent notes that skills are lost to outsourcing and with them an ability to respond to new technologies.

Specific types of organisation face particular sets of issues. A public sector digital leader lamented: As a public sector organisation it is difficult to recruit suitably qualified staff due to the limitations on salary (nationally agreed salary scales). Even training our own staff will not fully address all issues. This is further complicated by the organisation seeing efficiencies of technology adoption without the necessary investment in the backend staff to make those efficiencies a reality.

SMES faced something a little different, one person noting ‘silos of knowledge – not specifically because information sharing is poor, but because the organisation is small and we have specialists in individual areas.’ Some larger organisations face related situations, with some commenting on the breadth of skills now needed in IT people, making them look for those who can play multiple roles in a team and have knowledge of different technologies to support business partners.

Here’s a laudable, if tough, goal. ‘We need future proofing abilities – the organisation is running to stand still at the moment.’

One commenter gave an interesting solution to some of these issues: ‘Our operation operates on a lean staffing model, with skills augmented from external service providers.

The model envisages the system landscape and architecture to be designed in-house and bringing in external suppliers to provide the requisite infrastructure and applications. This organisation still has needs though: ‘Having a good system architect and IT security expertise, with the key gaps that the organisation faces.

We spend too much time “keeping the lights on” and not enough time innovating.’

Supplier (service) management is a close second.

Biggest IT skills gaps: hybrid

As implied by the last section sometimes the skills gaps are not in the organisation itself but in their suppliers. Several commenters pointed to the issues surrounding assessing skills within their outsourced partners. One respondent complained that, ‘IT capability is being delivered by an outsourcer agent who puts in sub-standard agents without the skill sets necessary. This causes major delays and welcome panic.’

Another ‘people issue’ is around an increasingly aware consumer base. A public sector digital leader said that they need people with ‘outdated awareness in service design, to ensure we’re as digitally savvy as our citizens.

Then there are the problems in actually finding those with skills in emerging trends – by definition a small recruitment pool. This creates a tension when trying to be innovative, with one digital leader saying that the organisation suffers from ‘too much time spent ’keeping the lights on’ and not enough time spent innovating.

The next three to five years

Looking three to five years’ ahead, the same three main issues are expected to be at the top of the list of priorities. However, the order is slightly different, with strategy and planning coming out top (44%), followed by operational efficiencies (44%), and business and information and organisational change (42%).

When asked which IT topics will be the top three priorities in three to five years’ time, information security is again the top answer with 54 per cent. This is followed by big data (42%), cloud computing (40%) and mobile computing (39%). The information security concern is the top answer for both SMEs and large companies.

There are a number of issues which are expected to become a higher priority in this time frame – the two showing the highest percentage increase (compared with plans for the next 12 months) are succession planning (up from 9% to 17%) and data protection legislation in 2017; compared with the priorities for the next 12 months the IT topic showing the biggest rise is internet of things (up from 11% to 28%).

Some issues were perceptual, for example (all commenters’ views):

• The build-up of technical debt by making wrong product selections;
• The illusions of remote access; that everything is an app that appears to have no cost;
• The speed of competitor change, to avoid the risk of products becoming outdated;
• The possible effects of the revised data protection legislation in 2017;
• The corrosive effect of hype and nonsense in IT;
• Slow change in large organisations, ticking boxes around superficial initiatives to cope with the financial and recruitment issues.

People issues seem to be in the category of ‘we get them eventually’ with the IT skills shortage, performance management and recruitment and retention issues all scoring higher in this future-looking question than in immediate priorities.

More forward-looking were some of the technical concerns that may impact the business. Mentioned specifically were concerns over the complexity of virtual environments, agile systems maintenance and migration to a Post-Java script web.

Sleepless nights?

The final question BCS posed in this survey was: When considering upcoming changes and trends in the IT industry, what is it that is most likely to keep you awake at night? All, the answers were a mix of the expected, and some thoughtful ideas on the longer term.

As ever, security is at the top, and came in a variety of guises: information risk and security; availability; security and stability in cloud computing and security breaches. There’s a lot of mentions of topic-specific security issues around, for example, the internet of things; smart solutions; the compliance agenda, and general reputational risk. Zero-day exploits and the ever-changing nature of security threats, were also mentioned.

Some issues were perceptual, for example (all commenters’ views):

• Unannounced changes to suppliers/ customers systems;
• Provision of high-speed broadband to customers for free;
• Cost of software licensing - Microsoft vs open source.

Some have identified bigger issues. One commenter laments ‘the complete lack of human beings involved in recruitment – applicant tracking systems have reduced the quality of the recruitment process to almost useless.’

And there are even-prior-present dichotomies, for example the combination of the need for computer security and privacy protection against the public expectation of easy and quick access. If this tension leads to shortcuts, that will cause problems. One commenter warns about the government’s desire to integrate and adopt collaborative data sharing without full investigation into the consequences in terms of resources and IT security.

Alarms are also raised at the risks associated with cloud computing and the US government’s stance on data stored on infrastructure belonging to US companies - with the associated data protection nightmare.

One commenter warns of a ‘collapse of trust in online systems because of over-complexity and lack of attention to resilience and security.’

Positive notes to end on

So, there’s plenty for the digital leader to do, consider, worry about, look forward to… and clearly many of them, whilst concerned about the risks, take an admirably positive view, one that takes people rather than just cold technology into account.

One commenter’s chief concern? Being ‘people-centric: developing systems that people want to use. Another points to the importance of the shift of capability from traditional IT roles to a more distributed user-oriented model, whilst maintaining control and governance over the enterprise architecture.

Here are some final answers to ‘When considering upcoming changes and trends in the IT industry, what is it that is most likely to keep you awake at night?’

• ‘Nothing – that’s why I have a CI!’
• ‘Not a lot – that is what claret for! I’m confident that we are up to the challenge.’

The full research is available to BCS members in the Members’ Secure Area at bcs.org
FROM THE BLOGS

GAMIFICATION AND PROJECTS

The term ‘project gamification’ caught Project Eye’s attention. As some of the Project Eye team have had brushes with delivering project management training, the idea of using computer games to simulate project scenarios sounded great.

Given the sophistication of computer gaming platforms, there could be some interesting developments. It started out with so much promise.

Project Eye looked at a report on project gamification published by its old friends at APM, which directed it to the insights of Dan Pink on the nature of motivation. If you have got 18 minutes to spare, his TED presentation is really worthwhile.

He presents a body of scientific research that shows that financial incentives can improve work performance on mechanistic tasks. However, for more creative and problem-solving tasks (which Project Eye guesses includes most software project activities) an intrinsic interest in the challenge of the task is more likely to generate superior performance. In these cases, financial incentives can actually get in the way.

Some have promoted gamification as a way of increasing intrinsic motivation. Gamification refers to the use of computer games thinking and mechanisms in non-computer games environments. The key elements that have been taken from computer games are:

• points – you get points for getting things right and achieving things;
• rewards – you get some kind of reward if you get lots of points (apparently this might even be financial rewards!);
• badges – you can also get some kind of recognition for your successes;
• leader boards – you are publicly ranked competitively with your co-workers.

One Project Eye acquaintance of mature years commented that this reminded him exactly of what his teachers at his north Kent grammar school did decades ago.

The idea of games is that they should have an element of fun, but in today’s cut-throat, competitive, work environment gamification just sounds awful. Is this just Project Eye? Project Eye has just been reminded it should stress that this is a personal view and should not be taken as reflecting any policy formulated or position taken by BCS. The Chartered Institute for IT as a learned institution.

Much of the research that Dan Pink described has been around for decades. The classic ways of increasing the intrinsic interest of work have been job expansion – increasing the range of tasks carried out by an individual, such as getting software developers to carry out some business analysis roles – and job enrichment, letting a worker carry out some tasks previously carried out by managers, such as when maintenance programmers are allowed to talk directly with end users. This seems to be a much more promising approach in the world of IT projects than silly point scoring.

Still the whole point of Project Eye is to stimulate heated debate. Can project gamification really be as irrelevant to IT projects as Project Eye perceives? Put us right below – but we can’t promise you any points, rewards or badges for your contributions.

For the links mentioned in this post to comment and to get regular PM updates visit: www.bcs.org/blogs/projecteye

EVERYONE BENEFITS FROM DIGITAL SKILLS

Last year marked the 25th anniversary of the WWW. During this time digital technology has transformed every aspect of public, private and working life.

Skills For A Digital World

Digital education starts early in schools, with children expected to be digitally literate by the time they leave. After this time, and for people who are not considered digital natives or not interested in computers, the onus is very much on the individual to develop skills.

In the Government Digital Inclusion Strategy, 21 per cent of the UK population is quoted as lacking basic digital skills.

This could be down to a lack of access, skills, motivation or trust, but to put this into perspective, it means around 11 million people are not benefitting from the digital world.

There are numerous initiatives by the government and other organisations, such as Barclays, Digital Eagles and the Tech Partnership, that offer help to encourage more people online. At BCS, we provide IT user qualifications to schools, universities, training centres, local authorities and employers which aim to support digital skills development from the classroom to the workplace.

Digital skills could enable people to benefit from things such as:
• savings by shopping online;
• flexibility of paying bills online;
• keeping in touch with family and friends;
• searching for special deals or employment;
• finding or accessing local services;
• staying up to date with news.

For these 11 million people though, does the digital concern outweigh the benefits? Let us know what you think and how these fears might be better addressed.

To be part of the debate and get further updates on digital skills visit: www.bcs.org/digitalskillsblog

LATEST CONTENTS

Interacting with Computers - The Interdisciplinary Journal of Human-Computer Interaction

Volume 27, issue 1, January 2015 special issue: Methods for Studying Technology in the Home, contains the following papers:

• Mixed methods for HCI research in the home
• Disruption as a research method for studying technology use in homes
• At home with users: a comparative view of living labs
• Researching young children’s everyday uses of technology in the family home
• Seeing the first-person perspective in dementia
• Tailored scenarios

For the links mentioned in this post to comment and to get regular PM updates visit: www.bcs.org/blogs/projecteye

The winning papers for The Computer Journal Wilkes Award for 2014 have been announced.

Exceptionally, this year the prize has been awarded to two joint winners. These articles are now available free online, the extracts appear below.

A movable architecture for robust spatial computing

David H. Ackley, Daniel C. Cannon and Lance R. Williams, Computer Science, University of New Mexico, Albuquerque, USA

For open-ended computational growth, we argue that: (1) instead of hardwiring and hiding component spatial relationships, computer architecture should soften and expose them; and (2) instead of relegating reliability to hardware, robustness must climb the computational stack toward the end users.

We suggest that eventually all truly large-scale computers will be robust spatial computers - even if intended neither for spatial tasks nor for rich environments. This paper is an extended introduction for the spatial computing community to the movable feast machine (MFM), a computing model in the spirit of an object-oriented asynchronous cellular automata.

We motivate the approach and then investigate a model touching on robustness mechanisms such as redundancy, compartmentalisation and homeostasis. We provide simulation data from prototype movable elements such as self-healing wire for data transport and movable ‘membrane’ rings for spatial segregation, and illustrate how some larger computations like sorting or evaluating a lambda expression can be reconstructed for robustness and movability within a spatial computing architecture.

On selecting the nonce length in distance-bounding protocols

Aikaterini Mitrokotsa (1,2), Pedro Peris-Lopez (3), Christos Dimitrakakis(1) and Serge Vauthey (1) from (1) EPFL, Lausanne, Switzerland; (2) University of Applied Sciences of Western Switzerland (HES-SO), Geneva, Switzerland; (3) Carlos III University of Madrid, Madrid, Spain.

Distance-bounding protocols form a family of challenge - response protocols which have been introduced to thwart relay attacks. They enable a verifier to authenticate and to establish an upper bound on the physical distance to an untrusted prover.

We provide a detailed security analysis of a family of such protocols. More precisely, we show that the secret key shared between the verifier and the prover can be leaked after a number of nonce repetitions. The leakage probability, while exponentially decreasing with the nonce length, is only weakly dependent on the key length.

Our main contribution is a high probability bound on the number of sessions required for the attacker to discover the secret, and an experimental analysis of the attack under noisy conditions. Both of these show that the attack’s success probability mainly depends on the length of the used nonces rather than the length of the shared secret key. The theoretical bound could be used by practitioners to appropriately select their security parameters.

While longer nonces can guard against this type of attack, we provide a possible countermeasure which successfully combats these attacks even when short nonces are used.

To view these papers visit: www.oxfordjournals.org/our_journals/computer_journal/wilkes_award.html

FREE WILKES AWARD PAPERS
The following papers are from The Computer Journal, issue 58, 2015. The overviews are largely based on the abstracts. They are provided by Editor-in-Chief, Professor Fionn Murtagh.

**Identifying Compiler Options to Minimize Energy Consumption for Embedded Platforms**

This article is available on open access. The authors are with the Department of Computer Science, University of Bristol and Emerson, Lymington.

This paper presents an analysis of the energy consumption of an extensive number of the optimisations a modern compiler can perform.

Using GCC as a test case, a set of 10 carefully selected benchmarks are evaluated for five different embedded platforms. Hardware power measurements on each platform are taken to ensure all architectural effects on the energy consumption are captured.

It is shown that fractional factorial design can find more optimal combinations than relying on built-in compiler settings. The relationship between run-time and energy consumption is explored and the difference in energy consumption are captured.

**Performance Modelling and Simulation of Three-Tier Applications in Cloud and Multi-Cloud Environments**

The authors are with the Department of Computer Science and Information Systems, Cloud Computing and Distributed Systems (CLOUDS) Laboratory, The University of Melbourne, Australia.

A significant number of cloud applications follow the 3-tier architectural pattern. Many of them serve customers worldwide and must meet non-functional requirements such as reliability, responsiveness and Quality of Experience (QoE). Thus the flexibility and scalability offered by clouds make them a suitable deployment environment.

Recent developments have shown that using multiple clouds can further increase an application's reliability and user experience to a level that has not been achievable before. However, research in scheduling and provisioning 3-tier applications in cloud and across clouds is still in its infancy. In this article, therefore, an analytical performance model of 3-tier applications in cloud and multi-cloud environments is proposed. It takes into account the performance of the persistent storage and the heterogeneity of cloud data centres in terms of virtual machine performance.

Furthermore, it allows for modelling of heterogeneous workloads directed to different data centres. The CloudSim simulator is used, and extended, in this work.

**Reusing Garbage Data for Efficient Workflow Computation**

The authors are with IBM Center for Advanced Studies (Atlantic), University of New Brunswick, Canada; Faculty of Mathematics & Computer Science, University of Lethbridge, Canada; and School of Computer Engineering, Nanyang Technological University, Singapore.

High-performance computing systems, including clusters, grids and the most recent clouds, have emerged as attractive platforms to tackle various applications. One significant type of application in HPC systems is workflow computation, which has been applied in various scientific and engineering domains. Workflow computation frequently produces intermediate result files, which become garbage after being used and are usually cleaned up without making any contribution to future computation.

In this paper, it is argued that such garbage data could be useful for future computation and should not be immediately cleaned up. This is because workflow computation usually contains multiple instances that may share some common data products produced in the past. This sharing scheme provides opportunities to reuse the historical data to speed-up subsequent computation and simplify re-computation due to faulty or crashed runs.

To this end, a garbage data manager (GDM) is proposed, for the workflow computation in HPC systems. The GDM organises and manages the garbage data for batch schedulers to enhance the performance of subsequent computation.

The Computer Journal

The Computer Journal has published advances in the field of computer science for over 55 years. Members can get heavily discounted subscription rates.

www.bcs.org/cjournal/subscribe
No photos please
Is it sad that while I was at CES 2015 recent BCS campaigns keep coming into my mind? asks Brian Runciman MBCS.
Let’s start with the Women in IT campaign we did last year. The problems women face in society in general are inevitably linked in with any industry-specific situation such as ours. So when Henry, BCS Editor-in-Chief, and I were looking at an (impressive) display of 80 inch 4k TVs, we were not surprised to see close-ups of roses lightly covered with water droplets, so far so generic.
But then the ladies started appearing. Initially beautiful faces, where you could clearly see the makeup in skin pores, perhaps this is making a subversive point, we thought.
Then, and this is not a joke (on any level), two lightly clad ladies appeared, pillow fighting. If it wasn’t so awful it would be funny, summing up in a nutshell some of the implications, ethics and political correctness of the situation and my head explodes (not literally).
Anyway, this is why BCS works so hard on the ethical side of things.

The magnificent seven
The first session at CES had lots of numbers of varying interest and the obligatory (?) Yul Brynner reference. Steve Koenig, Director, Industry Analysis at CEA split the global consumer technology market into two main areas: mature, including the US, Asia Pacific and Europe; and developing - the rest.
The thrust of this session was the popularity of our ever-more loved/invasive devices and CEA’s predictions for 2015 usage. Unsurprisingly smartphones are still the main driver, described by Koenig as the leader (Yul) of the Magnificent seven: digital cameras, desktop PCs, tablets, laptops, video game consoles and LCD TVs. Not sure which one is Charles Bronson, as he seemed to prefer a different sort of hardware...
One interesting question was posed in passing: will hardware battles soon be a thing of past as cloud delivery takes hold?

The three screens
The three screen motif refers to smartphones, tablets and TVs. The first two will have a 46 per cent share of the tech market this year. Indeed they’ve been rapidly ballooning (as was I in Vegas) for a while now. Will that continue? Yul Bryner will move around 1.5 billion units this year, a 19 per cent growth rate - slowing down but huge. New low cost handsets coming in 2015 will see 75 per cent of that, mostly in developing markets. More than a third of that in China alone.
The likes of OnePlus, coolpad and xiaomi are pressurising Apple and Samsung in China. But these companies have global aspirations too.

Tablet (Steve McQueen) unit sales are predicted to hit 337 million this year, again a slight taper in growth. Like smartphones a lot of lower cost models are coming in, Koenig referred to this as ‘maturisation and modification’: a number of players, a number of form factors, screen sizes making tablets, phablets, phone and laptop forms mutate.
TV (surely Robert Vaughan) used to be called the small screen, but that doesn’t work now does it? The TV market has returned to growth: 2 per cent for 2015. The average screen size for 2015 will be a not inconsiderable 43 inches. 60 inch plus LCDs are getting larger shares too. (Apparently 60 is the new 50!)
4k ultra HD will see a 150 percent unit increase for 2015 to 23,3 million, with China dominating demand. Existing 1080p will be good for consumers because they’ll get...cheaper, cheapish, cheap (relatively)!
Connected TV will grow, quitele surprising! 60 percent of TVs will be connected devices in the US, for example, during 2015. What of the curved screen? At present the numbers are tiny: barely 1 per cent of the market. The trends at CES 2015 were largely as expected: smart watches, health and fitness tech (mostly wearables), new automotive tech and the internet of things.

Urrghh....
Some of the marketing terms at CES made me a bit queasy. Would any self-respecting dad or mum refer to themselves as a ‘data-driven parent’? And while we are looking at this particularly egregious example, if parents need to be ‘empowered to stay connected to their newborn’, they are not ready for parenthood!
Public Seminars and In-House Training

- Enterprise Architecture
- TOGAF™ 9 Certification
- Zachman Certification
- Architecture Skills
- Corporate IT Strategy
- Enterprise Investment
- Implementing Change
- Business Architecture
- Business Processes
- Business Rules
- Requirements Process
- Business Analysis
- Data Modelling
- Information Strategy
- BI, Big Data & Analytics
- Data Quality

Conferences

- TDWI BI Summit, 7-9 September 2015, London
- Enterprise Data & Business Intelligence Conference Europe 2015, 2-5 November 2015, London