

Chartech

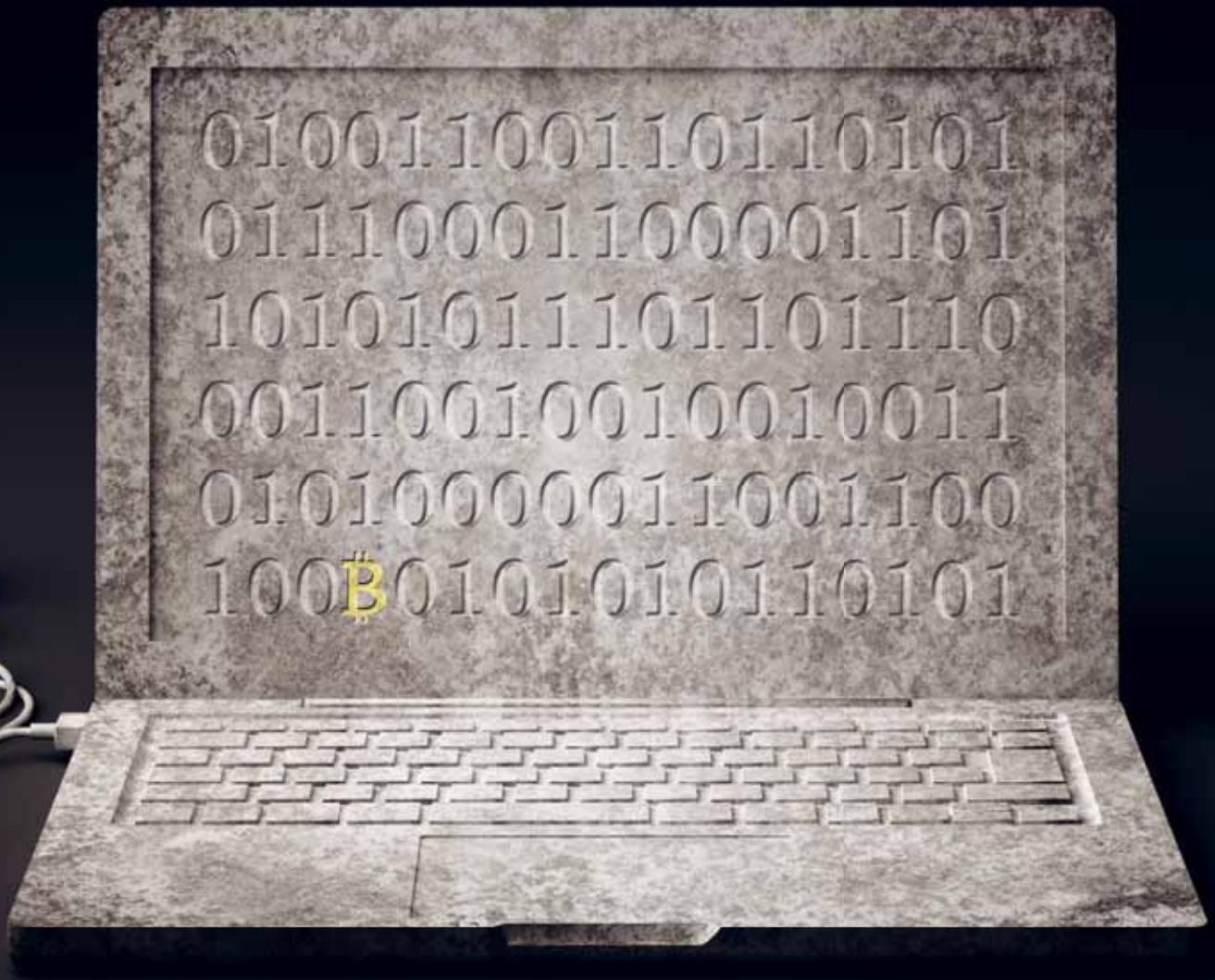


INFORMATION
TECHNOLOGY
FACULTY

ISSUE 203
MAY/JUNE 2016
ICAEW.COM/ITFAC

**EXPENSES
EVOLUTION**
TRAVEL AND
EXPENSES GET
AN UPGRADE

**DIGITAL
DIFFICULTIES**
WHAT
CHALLENGES
MIGHT MAKING
TAX DIGITAL
PRESENT?



SOLID AS A ROCK?

BLOCKCHAIN LEDGERS AND THE FUTURE OF FINANCE

Trident_ *redefined.*



THE NEW  TRIDENT

C60 TRIDENT PRO 600 – Swiss made dive watch with automatic mechanical movement, unidirectional rotating ceramic (ZrO₂) bezel and water resistance to 60 bar/600m. Available in 38mm and 43mm case sizes, five dial/bezel combinations and four strap styles.

SWISS MOVEMENT

CHR. WARD
LONDON

ENGLISH HEART

EXCLUSIVELY AVAILABLE AT christopherward.co.uk

Contents

Issue 203
May/June 2016



COVER: GETTY

11

04

Editor's letter

05

News

An overview of the IT Faculty AGM, as well as a security bulletin roundup and a summary of the Asia Roadshow

06

Events

Highlights for your calendar, including four Excel-based webinars

08

Byte size

Sandra Vogel's roundup of the latest business tech news

10

IT governance

Alan Calder looks at developing a workplace culture that helps to avoid security breaches

11

Making a mandate

Anita Monteith reflects on HMRC's plans to make tax digital

12

Never break the chain

Will blockchain technology revolutionise finance? David Lyford-Smith explains how the digital ledgers work

15

Times are a-changin'

Ros Campbell advises on how to confront timekeeping issues

16

Technical travel

Automated travel and expenses may involve some challenges, according to Lesley Meall

18

Data control

How will the new General Data Protection Regulation affect business? Dr Sam De Silva explains

20

Excel tips

Simon Hurst provides tips for eliminating errors in spreadsheets

22

A bite of the Apple

In wake of the San Bernadino tragedy, Leo Waldock considers the iPhone 'hack'

16



18



Surrender your data!



INFORMATION
TECHNOLOGY
FACULTY

The recent massive leak of data at Panamanian law firm Mossack Fonseca paints a worrying picture of the future to anyone with data to hide. Seen as the biggest data leak in history, the Mossack Fonseca



leak eclipses Wikileaks and Snowden and ushers in what *Wired* calls “a new era of megaleaks”. You may be familiar with the figures but they bear repeating. 2.6TB of data, over 11.5 million documents with some 4.8 million emails and 2.1 million pdfs. The ramifications have only just begun to be felt with more data due to be released in early May.

It is interesting to see how technology itself played a part in the leak. The unknown whistleblower (under the pseudonym John Doe) made contact with German newspaper *Süddeutsche Zeitung* in late 2014 looking to “make these crimes public”. He/she insisted on communication via encrypted channels only. The data was leaked piecemeal until all 11.5 million documents were sent. The German paper recruited the International Consortium of Investigative Journalists (ICIJ) to help analyse the data, creating a secure, curated database of leaked items available to the journalists only. OCR technology was employed to make the documents machine-readable and searchable. There were a number of months of investigative journalism before media organisations went public with the leak.

It also became quickly apparent that despite being the world’s fourth-largest offshore law firm, Mossack Fonseca’s data and website security was seen as weak and easily breachable. We have to assume there are more revelations to come.

A number of lessons arise from this leak. Initially, and as outlined in our first *Audit insights: cyber security* report, organisations have to assume they will be compromised. The report goes on to say organisations need to identify and protect their critical information assets. However, if an organisation has data to hide, motivations of criminals (or ‘leaktivists’ viewed from another direction) will drive them to get through an organisation’s defences. Second, Mossack Fonseca allowed itself to become an easier target with poor data security. Lawyers (and accountants) have to assume they have information that is valuable to someone and take steps to protect their clients’ data.

In this issue of *Chartech* we offer advice that is very pertinent in this area. On page 10 Alan Calder considers the important role staff play in remaining vigilant to security threats, and on page 22 Leo Waldock looks at the dangers to businesses of employees holding sensitive data on their mobile devices.

Richard Anning
Head of faculty

THE TEAM

George Quigley Chairman

T: +44 (0)20 7893 2522
E: george.quigley@kpmg.co.uk

Jeremy Boss

Deputy chairman
T: +44 (0)7791 293 319
E: jeremy.boss@btinternet.com

Richard Anning

Head of IT Faculty
T: +44 (0)20 7920 8635
E: richard.anning@icaew.com

Kirstin Gillon

Technical manager
T: +44 (0)20 7920 8538
E: kirstin.gillon@icaew.com

David Lyford-Smith

**Technical manager,
IT & the profession**
T: +44 (0)20 7920 8643
E: david.lyford-smith@icaew.com

Mark Taylor

**Technical manager,
technical innovation**
T: +44 (0)20 7920 8476
E: mark.taylor@icaew.com

Tracy Gray

Services manager
T: +44 (0)20 7920 8526
E: tracy.gray@icaew.com

Contact details

IT Faculty
ICAEW
Chartered Accountants’ Hall
Moorgate Place
London EC2R 6EA UK
+44 (0)20 7920 8481
itfac@icaew.com
icaew.com/itfac

Chartech is produced by
Progressive Content
71-73 Carter Lane
London
EC4V 5EQ

Advertising enquiries to:
advertising@progressivecp.com

To comment on your magazine, please
email us at publishing@icaew.com

ISSN 7748-5789

TECPLM14498

Printed in the UK by Sterling Solutions

© ICAEW 2016. All rights reserved. The views expressed in this publication are those of the contributors; ICAEW does not necessarily share their views. ICAEW and the author(s) will not be liable for any reliance you place on information in this publication. If you want to reproduce or redistribute any of the material in this publication, you should first get ICAEW’s permission in writing. No responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication can be accepted by ICAEW, the publishers or the author(s). Whilst every care is taken to ensure accuracy, ICAEW, the publishers and author(s) cannot accept liability for errors or omissions. Details correct at time of going to press.



From the faculty

IT FACULTY AGM

Roland Brook, Nina Robinson and Neil Christie were re-elected to the IT Faculty committee during the AGM on 12 May. David Ngu was elected to the committee for the first time.

David, an IT consulting manager at Protiviti, has spent the last year as an active observer on the committee. Spending time as a committee observer has worked well over the past few years, due to growing interest in

David Ngu was elected to the committee... we also welcome Sam De Silva and Tineke Booth

members standing for election.

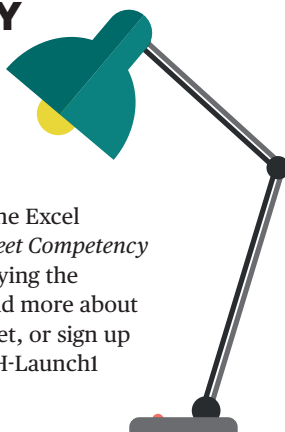
This year we also welcome Sam De Silva, partner at law firm Nabarro, and Tineke Booth, finance and operations manager at IT firm Synapse, who join the committee as observers.

We extend thanks to previous committee member Gareth Burton from Assure UK, who stood aside to make way for David on the committee.

At the AGM, faculty chairman George Quigley outlined some of the highlights from the year. These included the launch of the *Providing leadership in a digital world* publication at an event in October and its use by officeholders since. He also drew attention to the work the faculty undertook on the use of big data and analytics in audit, leading to the publication of the report *Data analytics for external auditors*.

SPREADSHEET COMPETENCY IN THE SPOTLIGHT

“Proficient in the use of Microsoft Excel” - how many times have we all seen this line, or one like it, on a CV? What does it mean and how can we trust the person’s judgement about their own skills? These questions led the Excel Community Advisory Committee to create the *Spreadsheet Competency Framework*, a simple and accessible structure for classifying the spreadsheet ability of finance professionals. You can read more about the latest framework draft at tinyurl.com/CH-Spreadsheet, or sign up to join us at the launch event on 6 July at tinyurl.com/CH-Launch1



THOUGHT LEADERSHIP IN FOCUS DURING FACULTY'S ASIA ROADSHOW

The IT Faculty's Kirstin Gillon undertook a thought leadership roadshow in South East Asia in April, during which she spoke to more than 1,200 members, students and other stakeholders in six countries.

Highlights included a presentation to a large contingent of ACA and CFAB students in Vietnam alongside ICAEW President Andrew Ratcliffe. A roundtable discussion on IT in audit at the Indonesian Supreme Audit Board was supported by ICAEW South East Asia regional director Mark Billington.

The roadshow certainly brought home the message that technology has gone up the agenda for businesses and accountants everywhere.

A report on the roadshow's findings will appear in a future edition of *Chartech*.

FACULTY SECURITY BULLETIN ROUND-UP

Cybercrime continues to be a hot topic in IT and in the news. IT Faculty staff member Mark Taylor has written a series of blog posts on cybercrime issues. These include recent trends in cyber extortion threats, the dangers of using a USB storage device found in the street and the potential danger of leaking too much personal information online.

The posts can be found within the IT Counts blog at ion.icaew.com/itcountshome, as well as at: tinyurl.com/CH-Threats; tinyurl.com/CH-USBdrives; and tinyurl.com/CH-Identity.

The Faculty has also added guidance on the GDPR and Safe Harbor legislation to the cyber resource page at icaew.com/cyber

There you'll also find an updated glossary of IT security terms under the Getting Started section.

YOUR SECURITY STORIES GET IN TOUCH

What is your experience of cyber-security issues? The faculty is keen to collect your stories of real-life examples of security flaws, breaches and lessons learned. Collecting anecdotal information on the issues faced by professionals will enable the faculty to further educate members on cyber security.

Any stories you share with the faculty will be received and treated in the strictest confidence.

To find out more or to share your story, contact Mark Taylor at mark.taylor@icaew.com

WEBINARS

RISKS IN MODELS

7 June 2016

Speaker: Alex Edwards, Savvy FM

How do you know your model is correct? How do you risk-assess a model and what questions do you need to ask a model developer to know if it's really up to scratch? Veteran modeller Alex Edwards, of Savvy FM, will give his top tips on how to check formulas, understand logic flow and question the inputs of a model.

PRESENTATION AND CHARTING IN EXCEL

12 July 2016

Speaker: Simon Hurst, The Knowledge Base

How can you get the most out of your charts and visualisations in Excel? Experienced Excel expert and trainer Simon Hurst will take you through his top advice for how to construct charts and diagrams in Excel – not only how to use the tools, but also how to select different kinds of diagrams for different situations and how to communicate clearly with pictures. Highly recommended for anyone who needs to use Excel to build dashboards or presentations.

EXCEL TIP OF THE WEEK LIVE #3

20 September 2016

Speaker: David Lyford-Smith, ICAEW IT Faculty

Back for a third round, *Excel Tip of the Week* author David will present another series of top tips for improving your workflow in Excel and cutting down on wasted time and effort. This will cover a wide variety of areas and will cater to all skill levels.

PRACTICAL EXCEL FOR ACCOUNTANTS

27 October 2016

Speaker: Glen Feechan, Glen Feechan Consulting Group

Excel Community blogger Glen Feechan looks back on his accounting-specific blog series, pulling out the most useful ideas and

tricks for the practical accountant on areas such as accounts prep, monthly management accounting charts, and more.

PROBLEM SOLVING IN EXCEL

13 December 2016

Speaker: David Lyford-Smith, ICAEW IT Faculty

Excel Tip of the Week author and IT Faculty technical manager David Lyford-Smith will attempt a problem from the ModelOff Excel competition live on air, talking through his process of how to break down the problem and how to figure out what's needed for a solution as he talks you through it. As well as some handy Excel formulas, this webinar will also cover how to think about thorny Excel problems and how to structure your workbooks to simplify the process of solving them.

Details of these webinars, including how to register, can be found at events.icaew.com. Search criteria: Information Technology/ Excel webinars.



IT FACULTY EVENT: SAVE THE DATE

MEET THE DATA SCIENTIST

21 June 2016

Speakers: Jérôme Basdevant, chief technology officer and co-founder of eRevalue; Kirstin Gillon, ICAEW IT Faculty; Rick Payne, ICAEW Finance & Management Faculty

The Harvard Business Review declared data scientist to be the sexiest job of the 21st century. But what do data scientists do and how can they work with finance professionals to improve business performance? At this event you will have the opportunity to meet with data scientists and find out about the skills that they bring in making the most of data – be it internal or external, big or small, structured or unstructured.

Book at tinyurl.com/CH-DScientist

AdvanceTrack® achieve the latest ISO9001:2015 Quality Standard

We are delighted to report that AdvanceTrack® are one of the first companies in the world to achieve the latest ISO9001:2015 Quality Management Certification. Managing Director Vipul Sheth said "The new Quality Standard was only published in late 2015. A lot of work by our senior team has enabled us to deliver the certification over 2 years ahead of schedule. It is testament to the strength of our people and processes that we now hold the two latest International Quality and Security Standards.

This demonstrates our commitment to continuous improvement of our people and processes whilst having a security management framework that allows us to manage confidential information securely."

ISO 9001

AdvanceTrack® are one of the first companies in the world to be certified for the latest Quality and Security Standards.

- ISO9001:2015 Compliant Quality Management Systems
- ISO27001:2013 Compliant Information Security Management

Shouldn't you be talking to **AdvanceTrack®** to help grow your firm?



Reasons to choose AdvanceTrack®

- ✓ Quality Service Delivery
- ✓ Secure Data Transfers
- ✓ ICAEW Member Firm
- ✓ Run by UK Chartered Accountants
- ✓ Secure and User Friendly Technology
- ✓ 24/7 Tracking
- ✓ Free up valuable time and concentrate on more profitable work
- ✓ All original client files stay securely on your premises

advancetrack®
outsourcing

University of Warwick Science Park, Sir Williams Lyons Road, Coventry, CV4 7EZ

Call: advancetrack® on +44 (0) 24 7601 6308

Email: advice@advancetrack.com @AdvanceTrack

Web: www.advancetrack.com

NEVER KNOWINGLY BETTERED

For Quality | For Security | For Service & Reliability

THINK OUTSOURCING. THINK **ADVANCETRACK®**



Byte size

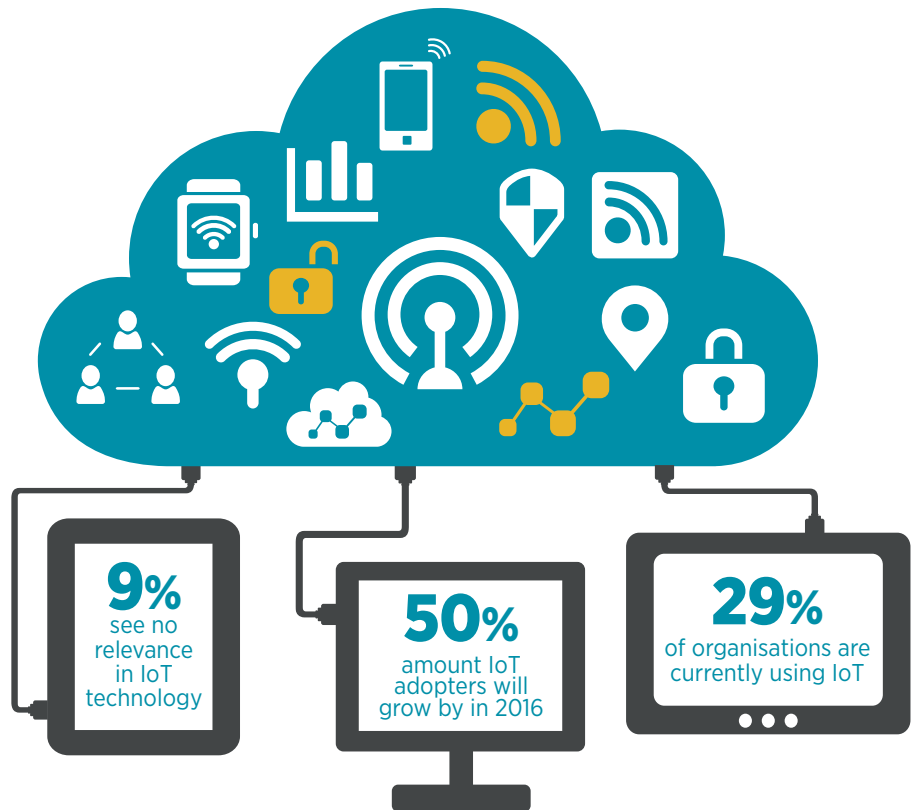


By Sandra Vogel
Freelance IT writer
sandra@svogel.com

VIRTUAL REALITY – A BILLION DOLLAR NICHE?

Virtual reality is about to hit the high street with several devices available now or due very soon. The Oculus Rift, HTC Vive and PlayStation VR are among the headsets getting coverage in the UK, and there will be more before the year is out.

But research company Forrester says that “despite all the hype, 2016 will not be the year of VR”. It is also felt that VR does not need to be on companies’ list of things to address yet. Consumer devices rely on high-end hardware to get the most out of them, while there are difficulties with marketing: it is hard to understand what VR offers without actually experiencing it, and challenging for people to understand the variation between low cost and expensive options if they can’t experience alternative products for themselves. Forrester says applications in entertainment, customer experience and psychological therapies are interesting, but that VR is very much the domain of ‘digital predators’ – a small number of forward-looking enterprises.



MAINSTREAM RECOGNITION COMING FOR THE INTERNET OF THINGS

For those feeling slightly jaded by all the talk in the technology press about the Internet of Things (IoT), there is no respite. In fact, the topic is likely to see increasing coverage, and we as customers are likely to see more real-world implementation of IoT. Analyst Gartner has said that in many industries “the IoT will move towards mainstream adoption in 2016”.

A survey of 465 IT and business professionals from 18 business sectors in North America, EMEA, Asia/Pacific and Latin America has revealed that the number of organisations adopting IoT will grow 50% in 2016, taking the overall percentage of IoT integrated organisations to 43%. The growth rate will become faster this year too. Just 29% of responding organisations said

The number of organisations adopting IoT will grow 50% in 2016, taking the total to 43%

they are currently using IoT, with 14% more planning to implement it this year and a further 21% planning to implement after 2016. Still, IoT will not be everywhere. Gartner found that 38% have no plans to implement IoT, and 9% did not see any relevance in the technologies.

The research found an interesting separation of industry types. It found 56% of businesses in what Gartner calls asset intensive ‘heavy’ industries such as utilities, oil and gas and manufacturing will have implemented IoT by the end of 2016, compared with 36% in what it calls ‘light’, or ‘weightless’ industries such as service oriented sectors.

Another interesting finding is the importance of internal operational improvements over customer facing benefits. Improved efficiencies, cost savings and better use of assets were drivers for 52% of those who have implemented IoT, with customer experience or increasing revenue a driver for 40%. Gartner expects there to be a shift towards customer facing factors in the next 12 months.

OFCOM LAUNCHES POSTCODE-BASED MOBILE BROADBAND CHECKER

Telecoms regulator Ofcom has released a new coverage checker for both mobile and fixed broadband. The service is provided with coverage, availability and speed data collected directly by Ofcom from major communications providers. This has not been readily accessible to consumers and businesses before.

To use the service visit the Mobile Broadband Checker at tinyurl.com/CH-OfcomMap and enter your postcode. Then select your network provider, call type (voice, 3G data or 4G data) and location (indoor or outdoor). A map is colour-coded according to the level of coverage you can expect and average broadband speeds are provided. Ofcom defines standard services as less than 30Mbps/s and superfast as between 30 and 300Mbps/s.

There are many potential uses of this service. Ofcom has given some examples of its uses including “businesses looking to relocate or expand to new

“Businesses looking to relocate or expand, or househunters, can use it to assess services”

premises, as well as house-hunters, can use the tool to help assess the quality of communications services in different areas, and customers wishing to upgrade their broadband package can check

whether faster services are locally available and, if so, how superfast and standard broadband speeds compare on average.”

Another use for the service is to check that the broadband service being provided is performing adequately; this can be done by comparing neighbouring properties. Individuals can use the information when contacting providers about problems.



OUR FEATHERED FRIEND: TWITTER AT 10

The first tweet was sent on 21 March 2006. Today the service claims 320 million monthly active users, with 79% of these active outside the US. Twitter has been widely reported to be experiencing a decline, but it remains



a massively popular medium. Here are the five most followed tweeters:

- Katy Perry @katyperry
85,755,390 followers
- Justin Bieber @justinbieber
78,465,202 followers
- Taylor Swift @taylorswift13
74,235,696 followers
- Barack Obama @BarackObama
72,263,553 followers
- YouTube @YouTube
61,074,821 followers

BLACKBERRY MAY HAVE MADE ITS LAST SMARTPHONE

BlackBerry was once a smartphone leader, its keyboarded handsets as much loved by city types who could do email on the move as by youngsters who could message each other for free through BlackBerry Messenger.

But times have changed. BlackBerry's most recent handset, the Android-based Priv, is an expensive competitor for top of the range phones from big brands like Samsung and Apple, and while BlackBerry did not release sales figures for the Priv in its most recent financial report, other sources say that it has less than 1% of global market share.

Meanwhile BlackBerry's own operating system languishes closer to 0.2% of global market share. The future of BlackBerry may well be as a software and services business with hardware out of the picture.



1%
of the global market belongs to BlackBerry

Security culture

Alan Calder considers the important role staff play in remaining vigilant to security threats



In the last edition of *Chartech* we looked at security breaches and evaluating the response. Now we move on to damage limitation - and that involves creating a security-minded culture in an organisation.

The insider threat to an organisation is a serious matter. According to the latest Information Security Breaches Survey (ISBS) from PwC and BIS, three quarters of large organisations and nearly one third of small organisations suffered a staff-related breach last year. Half of the worst breaches in the year were caused by “inadvertent human error”.

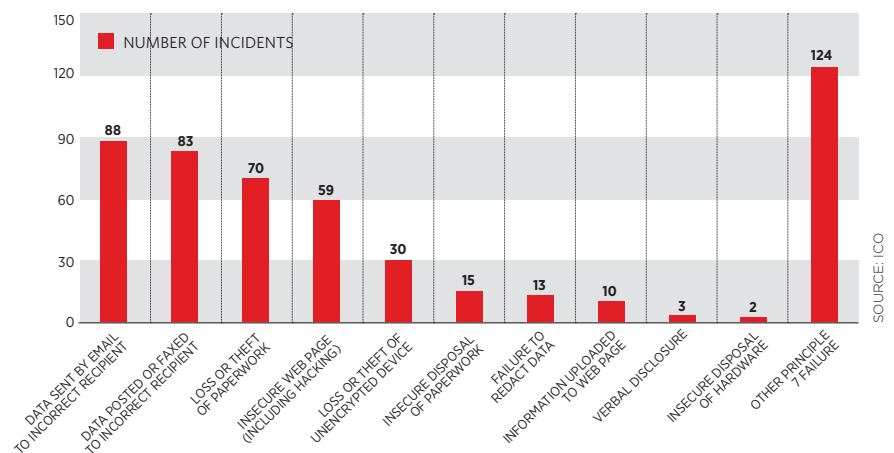
The Information Commissioner’s Office (ICO) *Data security incident trends* report from Q3 2015/2016 found that an unusually large proportion of data security incidents can be attributed to human error and/or negligence.

As a general rule, employees will always take shortcuts to be efficient and make their jobs easier, and good security can often be a casualty in this push for streamlining. If processes are too restrictive or impede working practices, staff will subvert them.

This much is simple human nature. Getting a computer to routinely behave in a certain way is easy; getting people to do so is trickier. Unfortunately, criminals recognise this and will always look to exploit people as the weakest link in the security chain. So when your own staff are one of your biggest security threats, what can you do?

Responsible organisations should know that mitigating information security risks is about far more than creating processes and procedures, installing antivirus and anti-malware programs, and then putting their feet up. When any employee can jeopardise an organisation’s security with a single

DATA SECURITY INCIDENTS BY TYPE



careless mouse-click, a more proactive approach is needed.

As PwC’s recent *Global Economic Crime Survey 2016: Adjusting the Lens on Economic Crime - Preparation brings opportunity back into focus* rightly points out: “Cybercrime is not an IT problem. If there is one lesson companies should take away from this study, it is... security controls must be embedded in organisational culture.”

Independent information systems security adviser ISACA defines corporate culture as “the pattern of behaviours, beliefs, assumptions, attitudes and norms in an organisation” - that’s to say, it’s how people actually work rather than how management wants them to work. When we talk of building an organisational security culture we mean creating a system of behaviour that ensures security best practice is instinctual to all staff - that it is, in psychological terms, a matter of unconscious competence.

Everyone in the organisation, from the board downwards, must recognise that information security is their responsibility. Everyone who has access

to data must know how to protect it. Everyone who uses the internet must understand the risks. Everyone must default to security instinctively. Good security and effective working practices must go hand in hand.

The ISBS found that 72% of companies where the security policy was poorly understood had staff-related breaches. Clearly, a comprehensive staff awareness programme - which starts at induction, is repeated on a regular basis, and is usually delivered systematically and consistently through an online e-learning solution - is essential to corporate security. But sustained top-management support and personal example are essential if the organisation is to successfully nurture and grow a genuinely cyber-secure working environment.

Since embedding culture change takes time, consider gaining an accredited security certification (eg, Cyber Essentials or ISO 27001) to help your business achieve an appropriate level and sustain it. ■

Alan Calder, CEO of IT Governance

THE MOVE TO DIGITAL AND MANDATING

Sometimes we know big tax changes are coming, sometimes we don't.

Anita Monteith explores HMRC's intentions of making tax digital

HMRC started to talk about Making Tax Easier and proposals for simpler payment at the March 2015 Budget. Later in 2015, the making tax easier element of this was rebranded as Making Tax Digital (MTD), but very little was known about what this really meant. In fact, even now, very little detail about exactly what businesses will need to do has been published. Most of our knowledge has been gleaned through a series of HMRC public workshops and presentations, many of which were attended by our members, but a picture of what the government has in mind has begun to emerge.

In December 2015, HMRC published its paper *Making Tax Digital* that set out how it intends to transform the tax system over the course of the present parliament. These proposals imply that the days of the traditional tax return are numbered.

ICAEW supports HMRC's digital transformation and considers that for the tax system to be fit for the 21st century, a 'digital first' approach has to be the right way. In practice, we are reassured that the MTD policy will not amount to quarterly tax returns as we know them now, but will involve submitting income/expenditure information in summary, 'at least' quarterly. As yet, we have no details of what these submissions might look like or contain, but they will be summaries rather than transactional.

THE CHALLENGES

We remain extremely concerned with the proposal to make quarterly digital reporting compulsory. We are yet to be convinced that this will reduce the administrative burdens of business, particularly the smallest businesses.

We also believe digital transformation needs to be done in parallel with the overall simplification of tax policy.

We are promised:

- Bureaucratic form-filling will be eradicated - taxpayers will never have to tell HMRC information that it already knows.
- The tax system will operate much more closely to 'real time', keeping everyone up to date and removing the risk of missed deadlines, unnecessary penalties, debts arising and errors in the system being carried forward from one year to the next.
- Taxpayers will have access to digital accounts, with the information HMRC needs automatically uploaded, bringing an end to the tax return.

From April 2018, small, non-VAT registered businesses will be the first UK businesses to have to comply with government's new proposals for MTD, which include making digital record keeping compulsory, and making four returns of information to HMRC each year. Digital record keeping for this purpose does not include Excel.

All VAT-registered businesses will be brought in from April 2019, and by 2020 all businesses will be required to keep records digitally and to make four returns each year.

In ICAEW's view it would be less challenging to start with the largest businesses (which will already have digital records) and work down rather than with the very smallest and work up.

We don't yet know what will need to be reported in these returns.

In our recent survey, a nationally representative sample of 500 UK businesses were asked how they keep their financial accounting records at the



moment. The results showed that just 25% currently maintain their accounts electronically using accounting software. The rest will therefore need to consider what changes they may need to make, almost certainly incurring considerable costs to comply with the new rules.

Further analysis revealed that a greater burden falls on sole trader businesses, with 82% of these one-person businesses needing to make the move to digital record keeping. Most of the burden will fall on the manufacturing and construction industries, where 41% still rely on paper-based records.

The government has promised that software will be provided free at the point of use to businesses. For some businesses, it is likely that the free packages on offer may not be sufficient to replicate the paper-based accounting that they use currently, so forcing them to buy a bespoke package. Some businesses will even have to buy their first computer. ■



Anita Monteith
technical manager,
Tax Faculty



SET IN STONE

Blockchain is considered as the system behind nefarious darknet transactions by some, but a source of innovation by others.

David Lyford-Smith chips away the confusion

Blockchains are publicly visible and editable ledgers that use complex mathematics to ensure that all parties agree on the current version of the ledger. Adapted from the technology that underpins bitcoin, blockchains can be used for many purposes, offering greater transparency and security. But there are technical challenges to overcome before the most promising implementations can become reality.

The most exciting features of blockchain technology are its resistance to tampering and its decentralised nature. Users can post transactions between each other without waiting on a middleman, and can trust transactions without needing a verifying authority. System failures can't happen as the ledger doesn't sit in one place.

However, in order to work as a major element of the financial system, the market needs to invest in research. It is not yet known how the complex work of processing new transactions in a

blockchain can be scaled up to the volumes and timescales necessary.

WHAT ARE THE FEATURES?

In accounting terms, blockchains are public ledgers. Different implementations vary just how much access users have and how public the chains are, but all blockchains share several features. They aren't hosted anywhere in particular, but instead are distributed across all of their users;

Blockchains have excellent security because it's not possible to alter old transactions. The source of any changes or new data is always indisputable

therefore they are immune to outages. Transaction costs are lower than traditional methods, because of the lack of a middleman.

Blockchains have excellent security because it's not possible to overwrite or alter old transactions. The source of any changes or new data is always indisputable.

Most companies are not interested in creating a ledger like the one that bitcoin runs on, which allows anyone to join and post transactions. They would to some degree include permissions, set up by an owner, which limit access and restrict the creation of records. Hence, the self-auditing and decentralised aspects of the blockchain are available even for private applications like interbank reconciliations.

Because the whole system of blockchains runs on automatic, inevitable software rules (as opposed to legal rules that may have consequences for breach, but aren't ironclad), some ledgers can be set up to run automatically-operating smart contracts. An example of this could be a software escrow

The most exciting features of blockchain technology are its resistance to tampering and its decentralised nature

BB1 001

01001001

BLOCKCHAIN: A HISTORY

Blockchains are a cryptographic technology – that is, they use clever mathematics to create secure systems. Unlike a traditional ledger, which is owned and managed by an institution, a blockchain is spread out in a distributed ledger – each user keeps their own copy, and whenever a new set of transactions is posted (a block), it is only accepted if it is linked via mathematical code to the previous block, creating an unending chain of transactions. The code needed for each block is based on the blocks that went before, making it impossible to post new blocks without confirming the transactions in the previous ones.

Records in a blockchain ledger are unalterable. Because there is no single central ledger, users can interact with each other directly without having to wait for a central server to approve transactions. Fees are reduced and the chance of service outages or failures is eliminated.

Blockchain is the underlying technology on which the bitcoin cryptocurrency (online currency) is based. Bitcoins exist only in an online list – the original blockchain – of who owns what. Transfers of bitcoins are

carried out by posting blocks of transactions. The bitcoin chain is programmed to automatically pay those that do the mathematical legwork of posting those transactions – called miners – a large chunk of bitcoins for their work, thereby making the operation of the network self-funding.

Bitcoin is completely without central control. Bitcoin transactions are unregulated – and impossible to censor. No one can stop someone from sending and receiving bitcoins, and so you can't freeze a bitcoin wallet in the way that a bank can freeze a bank account. There also isn't any barrier to anyone creating a bitcoin wallet that wants to, unlike regulatory checks on the creation of bank accounts.

Because of this pseudonymous and unregulated nature, bitcoin has suffered under swinging valuations and multiple brushes with scandal and illegal activity. The now-defunct Silk Road site, a 'darknet' site used for the sale of drugs and other illegal products and services, was heavily linked to the currency. But the underlying technology has much wider applications than in creating bitcoin and similar currencies.

account that would automatically release a bitcoin payment to a vendor upon completion of certain terms. There is no risk of default because the contract is automatic and binding.

IMPLICATIONS IN PRACTICE

Blockchain is gathering a lot of hype currently, with a lot of start-ups and reports concentrating on it and proponents talking about how it's the biggest innovation since the internet. Getting underneath the skin of the hype to see what is actually happening now, and what is realistically going to be done in the next few years, can take some work.

Land registry

US start-up Factom has partnered with the government of Honduras to provide a proof-of-concept execution of a land title registry system based in the blockchain. The system would be immune to alteration without record, a vital feature for countries with high rates of corruption.

Citizen identity

In Estonia, blockchain technology is used to keep track of who has accessed and changed citizens' medical records. The records themselves are not stored on the public ledger, just a list of who has been accessing and changing the records.

Bank reconciliation

Significant investment in blockchain has been made by several large financial institutions, most notably a consortium of 42 financial companies named R3. The members of R3 believe that the tremendous efforts they currently spend reconciling interbank transactions could be reduced significantly by moving to a shared ledger system.

Corporate governance

NASDAQ has begun to use a blockchain platform for trading in its private market, with plans to extend it if the pilot is successful. The platform allows middleman platforms to be cut



110 B001

GLOSSARY

Block – a chunk of transaction that is being added to a blockchain.

Blockchain – the technology behind distributed ledger systems like bitcoin. Note that, confusingly, there is a popular bitcoin client called “Blockchain”.

Chain – the series of blocks of transactions, each linked to all previous blocks via cryptographic techniques.

Cryptocurrency – an electronic currency, such as bitcoin, which uses blockchain to record transactions instead of a central bank.

Cryptography – the use of mathematics to secure information.

Distributed ledger system – any system that spreads multiple copies of a single ledger out over multiple users without a central owner. Blockchain is the most well-known example.

Miner – a computer user who donates their computer processing power to help compute the codes needed to stitch new blocks into the blockchain. Usually requires expensive specialised equipment.

Permissioned – a blockchain that has rules about who is allowed to view the data and/or post new transactions, and what kinds of transactions are allowed.

Smart contract – a special rule built into a blockchain that will automatically make one or more entries when certain terms are met.

Unpermissioned – a blockchain with minimal permissions, allowing any user to access past transactions and post records.

Wallet – a computer file noting who holds some amount of bitcoins. Wallets are pseudonymous, they don't have to clearly belong to a certain real-world person.

One key issue with blockchain is its reputation. Separating the technology from the bitcoin roil is an important first step



01001001

01BB1

out of the system, reducing the chance of fraud or default.

UK government applications

The UK government has commissioned a report on blockchains and distributed ledger systems, which discusses many possible uses of these systems by government such as tax collection, issue of passports and adding transparency to spending on overseas aid.

WHAT ARE THE PROBLEMS?

One key issue with blockchain is its reputation - its use by criminals, and certain parts of the bitcoin community's anti-government and anti-democratic politics. Separating the technology from the bitcoin roil is an important first step.

Despite being seven years old, blockchain is still relatively new. Problems with scalability are reported - the cryptographic processes necessary to chain blocks together are calculation-intensive and require specialised equipment. Also, as all ledgers contain

all transactions, the file sizes can get ever larger. It's not clear yet how to scale blockchain to the sizes needed for public sector databases or the volume needed for banking transactions. Despite holding billions of dollars, the current bitcoin chain can only handle five to six transactions per second across the entire network, often with latency of several hours.

Greater security is an opportunity with blockchain, but poor understanding by end users of how to access and operate with the format could lead to vulnerabilities. While transactions on the blockchain itself are impregnable, there is room for hackers to hijack the user's details with a so-called “man-in-the-middle” attack. ■



David Lyford-Smith,
technical manager,
IT Faculty, ICAEW

01001001

What's on the clock?

Ros Campbell looks at some best practice methods that support business and bring time-keeping issues into the light



Accountancy practices vary in the value they place on monitoring how their team's time is spent. Where time is tracked, there also appears to be wide diversity in the methods used and their value.

Questionable practice includes:

- not logging time where work goes over budget and just taking the hit;
- logging time to 'non-chargeable' client codes; and
- posting work done for one client to another whose work is under budget.

SYSTEM SET-UP

Where there are too many job codes, staff get lost in the detail and tend to post to any code that looks vaguely appropriate. I have seen accountancy practices with 60-plus codes and all this data has to be imported, manipulated and analysed in Microsoft Excel - a great time-stealer!

Review your job codes and question what is a must-have and what is a nice-to-have. Stop staff from posting to unnecessary codes and consider removing these codes altogether.

It works well when job codes are aligned to marketed service lines, for example: VAT, corporation tax or accounts.

PROCESS

The confusion of where to post time can be solved at the job planning stage, making the job codes clear to staff. Educate new staff on how to post and encourage them to update their timesheets as they go along. Where possible using their timesheet as a diary will alleviate the grind that's associated with it. For example, post dentist's appointments or external training courses in advance.

If monitoring shows that the job is going over budget, explore the reasons why. Monitor the time being spent during the job, rather than as a post mortem

Having timesheets independently checked and making staff accountable for rectifying any mistakes will build confidence in the data being generated.

MONITOR AND CONTROL

Prevent new job codes being set up in an ad hoc manner and establish a clear route to creating a new code where there is genuine need.

Avoid codes like 'General' or 'Other' - these quickly become a dumping ground. If you must use these codes, monitor them closely. Ample narrative should accompany each posting to explain why this type of code has been used.

A LEARNING OPPORTUNITY

Encourage staff to post all their time accurately - if monitoring shows that the job is going over budget, explore the reasons why. Monitor the time being spent during the job, rather than as a post mortem.

Tackle any issues as they emerge and certainly before you take on further work for the client to avoid a recurrence. Does the client need 'educating' in how they can help you to work more efficiently?

Of course, there's always a place for offering a loss leader, but this needs to be a conscious strategy.

CULTURE

Key performance indicators (KPIs) help to achieve your business goals and give clear focus at every level. However, if the culture is fixated on these results, it encourages dubious behaviour around logging time. All the following comments are genuine:

- "I posted time to another client, who is under budget, to get my bonus."
- "I posted time to a no-work code, so the profit looks OK on the client."
- "I didn't post any time. I did it in my own time, so I wouldn't get into trouble."
- "I can't be bothered to post to codes, so I just post it all to 'General'. Someone else can sort it out!"

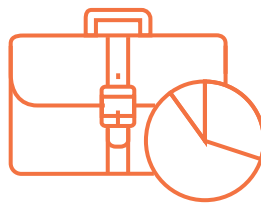
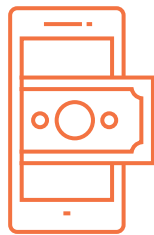
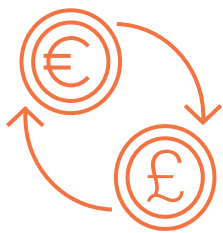
In these instances, the KPIs were not serving their true purpose and needed to be reviewed.

Practices that tackle these issues achieve greater clarity in their time-keeping, generate more accurate data and ultimately build a more profitable business. I've seen practices start reaping the rewards within two short weeks. ■

Consultant **Ros Campbell** helps practices to identify efficiency savings. She has over 20 years' experience in the accountancy profession, and as product manager for IRIS Software Group's practice management solutions. alcamassociates.co.uk

ON THE ROAD AGAIN

Lesley Meall looks at the automation of expenses management and the challenges that accountants may face



In the October 2015 edition of *Chartech*, we wrote: “Software is getting smarter while mobile devices are getting smaller and more powerful. Even the most complex, manual, and multi-faceted processes in finance and accounting can now be automated, including travel and expenses (T&E) management. It is only a matter of time (rather than a question of technology) before we can all be blessed with T&E reports that create themselves.” (see tinyurl.com/CH-Auto2).

It is not usual to begin two articles in the same way. However, in this instance it is expedient, because the previous article laid the foundations for this one. It looked at the emerging possibilities in the automation of expenses management; highlighted some of the potential benefits for accountants in business and practice; and outlined some of the technology-related factors that may inform decisions about which software, systems and services you select to provide the infrastructure this automation will require.

This article picks up where its predecessor left off and digs deeper into the automation of expenses management (and related bookkeeping and accounting processes), by sharing some of the barriers and

challenges that accountants (and some of their clients) are experiencing as they head off down the road towards this brave new world of automation.

LAYING A FOUNDATION

So, let’s begin where all organisations will need to start this journey, by pulling together the infrastructure (of software and services and PCs and mobile devices) that is needed to automate expenses management processes and the associated bookkeeping and accounting tasks. For those in practice, this can be a particularly challenging stage, because how easily and extensively you can automate all of this will (to a large extent) depend on the bookkeeping and accounting software that your clients are using.

“We always recommend Xero or FreeAgent,” says Jessica Pillow, managing director at Pillow May accountants. Pillow is a big fan of cloud-based software and the ease with which it can enable and support automation and connectivity. Pillow May uses these two applications to automate as much as possible of the expenses management and bookkeeping processes by combining them with Receipt Bank. “It works well with both of these products. That was partly why





Even the devices that are used to access expenses management automation tools can erect hurdles you were not anticipating – poor picture quality on tablets or two-factor authentication for those without a smartphone

we chose Receipt Bank over some other suppliers,” she explains.

Receipt Bank – and similar products such as Concur, Datamolino and Webexpenses – can be used to digitally capture key data from bills, invoices and receipts (and some specialist tools can do a great deal more). Invoices received by email can be forwarded to these kinds of systems, receipts can be photographed and uploaded using Android and Apple devices, then the relevant information is extracted and turned into data that can be shared in a variety of ways.

With packages that are integrated – Xero and FreeAgent are with Receipt Bank and Sage One is with Datamolino – the captured data can be automatically published to the accounting software. You can also expect it to be made available as a CSV file; so it can be downloaded and used with the endless range of bookkeeping and accounting

systems and spreadsheets that accept data in this format.

“Clients do most of the filling up of Receipt Bank and then we take it from there,” says Pillow. Most of the time this is a pain-free experience. “Receipt Bank is quite smart and you can set up a lot of rules,” she says. “If you’ve got the rules in place, you know that most of the time things are correct and it’s not too difficult to correct the occasional thing that’s wrong – such as something that has been misplaced because it wasn’t travel as usual, but something else for a change.”

A CURE FOR HICCUPS?

Hiccups in this area can be a particular issue if employees of clients do a lot of overseas travel. “Receipt Bank doesn’t always identify expenditure correctly,” says Ray Backler, from Capsa Accounting. “I can’t trust it to do tax and foreign currency calculations. Unless there is some indicator on the bill as to what the currency is, it will assume it is sterling, and it will process an item with tax on the bill as VAT when it is actually US Sales Tax.” You can easily end up having to correct this in the accounting system.

Credit and debit card transactions may also create challenges. You can set up rules in Receipt Bank (and similar systems) to pick up the last four digits of a card number from a bill and then treat the transactions accordingly. However, this process is not always as straightforward as it might be. “When you go into a restaurant you usually get the receipt for the card transaction and a separate itemised restaurant bill and this doesn’t always show the final four digits from the payment card,” explains Backler.

To minimise the potential for issues and the need for manual input and checking, employees and clients who are using

systems that digitally capture data from bills must be aware of such issues – and bear in mind that some providers will charge for the processing of two items if you scan in two items in support of a single transaction. In a recent blog for *IT Counts* (see tinyurl.com/ICAEW-Digital), Kevin Salter, a Glover Stanbury partner, shares some similar challenges with Sainsbury’s petrol receipts, which are printed with the date on the reverse.

LEARNING ORIGAMI

“A degree in origami is needed to insert the folds necessary to get date, amount, supplier etc in one photograph,” he says, noting that extra work is likely to be needed by the practitioner to prevent petrol, a KitKat and the *Daily Mail* from all ending up as motor expenses. Of course, a gap between theory and practice is to be expected. However, as Salter’s blog explains, even the devices that are used to access expenses management automation tools can erect hurdles you were not anticipating – such as poor picture quality on tablets and the security challenges of two-factor authentication for users who don’t have a smartphone.

None of these are insurmountable barriers, but they do land with a destabilising thud on the scales when you are trying to weigh up the pros and cons of expenses management automation. On the other side of those scales, however, are the benefits of systems such as Concur and Expensify, which can be used to capture data on spend, categorise it, reconcile it, export it and even automate the process of final reimbursement. “We think we’ve finally killed the expense report,” David Barrett, co-founder and CEO of Expensify, recently told *ITBusiness.ca* in the US. T&E reports that write themselves seem to be getting closer by the day. ■

PREPARE TO PROTECT

Dr Sam De Silva explores the scope of the General Data Protection Regulation and how it's likely to affect business in the long term

On 14 April 2016 the EU Parliament formally approved the General Data Protection Regulation (GDPR). The GDPR will enter into force 20 days after its publication in the *EU Official Journal* and then its provisions will be directly applicable in all member states two years after this date.

CONSISTENT FRAMEWORK

The GDPR introduces a single legal framework that applies across all EU member states. This should ensure that businesses will be subject to a more consistent set of data protection compliance obligations across different EU member states.

EXTRA-TERRITORIAL SCOPE

Non-EU businesses will be subject to the GDPR if they:

- offer goods or services to EU data subjects; or
- monitor EU data subjects' behaviour.

In practice this means that many non-EU businesses that were not required to comply with existing EU data protection legislation will be required to comply with the GDPR.

Businesses established outside the EU that are not currently subject to existing EU data protection legislation will need to consider whether any of their non-EU entities are subject to the GDPR and review the compliance obligations of those affected

entities under the GDPR. This extra territorial effect is not an entirely new concept and reflects similar developments in EU case law in relation to data protection.

ENFORCEMENT POWERS

Under the Data Protection Act 1988 (DPA), the maximum fine for breaches is £500,000. The GDPR will significantly increase this. The maximum fine would be the greater of up to €20m (£15m) or 4% of annual worldwide turnover.

We expect that businesses that previously considered non-compliance with EU data protection law as a low-risk issue will need to re-evaluate their positions in the light of the substantial new fines and the increased enforcement powers by the data protection regulators.

LEGAL GROUNDS - CONSENT

Consent, as a legal basis for processing, will be harder to obtain. Unlike the DPA, the GDPR does not distinguish between ordinary and explicit consent, instead it adopts a uniform approach and proposes that consent must be freely given, specific, informed and explicit, and demonstrated either by a statement or a clear affirmative action.

The current practice adopted by most businesses in the UK has been to rely on implied consent. The position in relation to consent in the GDPR means that businesses that rely on consent will need to carefully

review their existing practices to ensure that any consent they obtain is explicit, and indicates affirmative agreement from the data subject (for example, ticking a blank box). Mere acquiescence (failing to untick a pre-ticked box) would not constitute valid consent under the GDPR.

APPROACH TO COMPLIANCE

The GDPR adopts a risk-based approach to compliance, under which businesses would bear responsibility for assessing the degree of risk that their processing activities pose to data subjects. Such an approach is demonstrated through a number of the provisions,

eg, the new accountability principle and requirement for data controllers to maintain documentation, privacy by design, data security requirements and the appointment of a data protection officer (DPO). DPOs must be appointed for all public authorities and will be required for those organisations where the core activities of the controller or the processor involve "regular and systematic monitoring of data subjects on a large scale" or where the organisation conducts large-scale processing of "special categories of personal data".

THE ONE-STOP SHOP

Under existing law each data protection authority (the Authority) may exercise regulatory control over businesses operating in its territory. Under the GDPR, a business will be able to deal



with a single Authority as its 'lead authority'. How exactly this mechanism will work in practice is still not fully clear.

The concept of the one-stop-shop may prove problematic following recent European Court of Justice decisions that emphasised the independence of national Authorities and their competence to enforce data protection law where the data controller is 'established' in their country.

DATA PROTECTION

Businesses will be required to implement data protection by design (eg, when developing new products or services) and by default (eg, data minimisation). There is also a requirement to perform data protection impact assessments to identify privacy risks in new products.

DATA PROCESSORS

Under the DPA, the key obligation to comply with data protection legislation is with the data controller. One such obligation is for the data controller to impose contractual obligations on the data processors with regard to their use of personal information.

However, the GDPR will impose direct statutory obligations on data processors, such as implementation of appropriate technical and organisational security measures to secure personal information; the obligation to notify data controllers of data breaches; complying with the requirements of the GDPR with regard to the transfer of personal information from the EU.

DATA BREACH NOTIFICATION

The GDPR introduces a general obligation to report data breaches:

- to the competent Authority without undue delay and, where feasible, no later than 72 hours after being discovered. If this is not possible the delay must be justified to the Authority; and
- to the affected data subjects without undue delay. There are exceptions where an organisation does not need to inform affected individual data subjects in the following cases:
 - if the controller can demonstrate to the satisfaction of the Authority that it has implemented appropriate information security measures that render the data unintelligible to any person not authorised to access it (eg, the lost data are protected by encryption);
 - if the controller has taken measures to mitigate the high risk for data subjects; or
 - the notification would involve disproportionate effort on the part of the controller - in which case there should be a public communication or similar measure where the data subjects are informed.

Businesses should develop and implement a data breach response plan (designating specific roles and responsibilities, training employees and preparing template notifications) enabling them to react promptly in the event of a data breach.

BINDING CORPORATE RULES

Binding Corporate Rules (BCRs) are agreements used to lawfully transfer personal data out of the European Economic Area. The GDPR will formally recognise BCRs (unlike the DPA). They will still require Authority approval, but the approval process should become less onerous than the current system.

DATA SUBJECTS

Under the GDPR data subjects now have the following rights:

- The right of data portability: data subjects

will have the right to receive their personal information from a data controller in a machine-readable format and to have the data transmitted to another data controller, where technically feasible.

- The right to be forgotten: data subjects have the right to demand that businesses should delete or destroy their personal information on various grounds (for example, where the information is no longer needed for its original purpose).
- The right to restriction: data subjects will have the right in some cases to demand that the further processing (other than storage) of their personal information may be suspended, such as when the accuracy of the data is contested.

NEXT STEPS

Although the GDPR will not have effect until the spring of 2018, businesses should start preparing for the new regulatory framework by reviewing their current data collection practices and examining the new requirements. Consequently, businesses may need to:

- adapt the ways they collect, use and process personal information;
- build and implement the appropriate governance policies; and
- address the security aspects of the personal information collected by them. ■



Dr Sam De Silva, partner and head of commercial IT & outsourcing, Nabarro LLP, and IT Faculty technical committee member

Note: This article is not intended to constitute legal advice. Specific legal advice should be sought before taking or refraining from taking any action in relation to the matters mentioned in this article.



Finding errors and issues

Simon Hurst considers some ways to track down errors in Excel, starting with the built-in error-checking tools

START WITH DESIGN

Although we will be looking at ways of identifying errors in spreadsheets, avoiding errors involves a lot more than trying to find them once a spreadsheet is complete. Designing the spreadsheet properly in the first place will not only reduce the likelihood of errors being introduced, but will also make it much easier to identify any errors that do occur. Several of the points in ICAEW's *Twenty principles for good spreadsheet practice* are particularly relevant:

10. Separate and clearly identify inputs, workings and outputs.
11. Be consistent in structure.
12. Be consistent in the use of formulae.
14. Never embed in a formula anything that might change or need to be changed.

The separation of different elements of a spreadsheet, whether it be through the use of separate sheets or just separate rows and columns, makes it possible to check for a cell that contains a fixed value rather than a formula. If your design mixes value and formula cells, it will make it much harder to know whether the presence of a value cell is an error or not. Similarly, consistency is vital. Excel's built-in tools can identify cell contents that are inconsistent with those around them, but this is only likely to be useful where formulae are generally consistent. If all the formulae in a column or row should be identical, then it becomes possible to highlight inconsistent entries; if all the formulae are different anyway, the ability to identify inconsistencies will not help in finding errors.

Including fixed values in a formula not only prevents effective use of cell locking and sheet protection, but

is also a very common cause of spreadsheet error. If you embed something like the VAT rate in hundreds of separate cells, then ensuring each one is entered correctly in the first place is difficult enough. Making sure they are all changed correctly in the event of the rate being changed is even more of a challenge.

RANGE OF TOOLS

Given that the design of your spreadsheet makes it possible to use Excel tools to help seek out errors, there are several different features that you can use - some of them obviously related to checking for errors, but others less so:

- Built-in Error Checking;
- Formula Auditing Tools;
- Inquire Add-in;
- Go To, Special;
- Data Validation;
- Conditional Formatting; and
- Power Query /Get & Transform tools.

USEFUL BUT FLAWED

We'll start with the most obvious error checking mechanism - Excel's built-in error-checking rules. Although these can be useful (and it's certainly worth checking them when they do appear), they are far from comprehensive and have some serious limitations, so they should never be relied upon as the only check applied.

By default, Excel will mark cells that contravene its error checking rules with a green triangle in the top-left hand corner. You can choose which rules to apply, and turn the feature on or off altogether, using Excel Options, Formulas, Error Checking and Error checking rules (Figure 1).

These options can also be accessed from the alert dropdown which includes commands to correct or



Figure 1

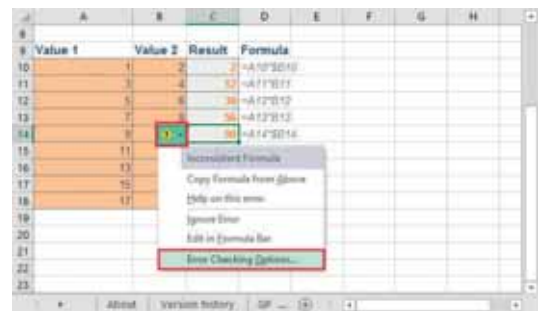


Figure 2

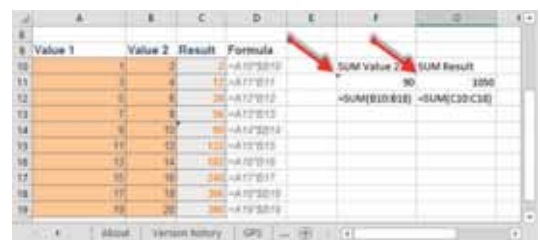


Figure 3

ignore each error (Figure 2).

Many of the error-checking rules are very helpful and highlight common errors. For example, formulas which omit cells in a region can alert you to the failure to extend a simple SUM() range to include new data entered adjacent to an existing range, or just not including all the required cells in the first place. However, do note that the rule will only be triggered if the cells in question just contain values, not if they contain formulae. In this example, the Value 2 column just contains numbers, the Result column a formula. The SUM() formula referring to column B in cell F11 is highlighted as omitting adjacent cells, but the same formula referring to column C is not (Figure 3).

I mentioned in the introduction the benefits of keeping formulae consistent, and one of the rules checks for this specifically: formulas inconsistent with other formulas in the region. However, there is a significant flaw in the way that this check is implemented. It is only triggered if the inconsistent formula is sandwiched between two consistent formulae. If it is at either end of the column or row, even if all the other formulae are the same as each other, it will not be highlighted. In the example shown in Figure 3, we can see that cells D10, D14 and D18 and D19 all include an additional \$ in front of the reference to column B. D14 is marked as inconsistent because the formulae in D13 and D15 are different and consistent, but because neither of the other three have 'consistent' formulae both above and below the formula, they are not marked as inconsistent. This would be the case even if it was only D10 or D19 that included the dollar sign.

If the block of data is turned into an Excel Table (Insert Ribbon tab, Tables group, Table or Control+T keyboard shortcut) then the top and bottom cells can be highlighted as being an Inconsistent Calculated Column Formula as in the following example (Figure 4).

As well as some potential errors being highlighted as they occur, you can also use the Formulas Ribbon tab, Formula Auditing group, Error Checking command to run through an entire worksheet, reporting each error in turn, much like a Word Spelling and Grammar check (Figure 5).

CONCLUSION

So far we have just considered one of the available error-checking tools in Excel. Next time we will look at some of the other features and techniques available. ■

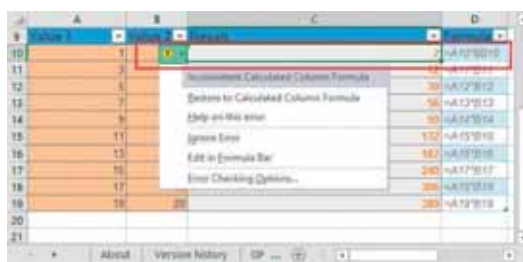


Figure 4



Figure 5

OTHER OFFICE TIPS

The Excel Community site includes articles on Excel and other office software and a forum where you can ask, and answer, questions about Excel issues: icaew.com/excel

The IT Counts site has articles of more general interest including office software and hardware, IT security, management reporting and cloud computing. It has a forum: icaew.com/itcounts

Both IT Counts and the Excel Community are available for free to all IT Faculty members as part of their subscription.

Simon's book, *Essential Excel for accountants (and others)*, is now available as a PDF: tkb.co.uk/towiee.htm (the hard copy version was formerly known as *Maximising the Impact of Accounting and Financial Spreadsheets for Finance Users*). He has included many Excel tips in the 'Lunchtime Learning' section of his website: tkb.co.uk/lunchlearn.htm

Cracking the case



In weakening security on our personal devices to help the authorities, would developers inadvertently make our businesses more vulnerable to attack? **Leo Waldock** looks at the evidence

As the Edward Snowden revelations demonstrated, the authorities aren't the least bit fussed how they get their hands on data and information. You probably aren't particularly concerned about the police or GCHQ targeting your data, but criminals and foreign agencies could be a different matter. Right now the passcode on your phone is the only barrier that stands between your data and the outside world. But is that enough anymore?

By default the lock screen on an iPhone requires a four digit passcode, meaning there are 9,999 permutations for anyone hoping to gain access to its contents. The snag is that after six incorrect attempts you have to wait one minute to make your next guess, after the seventh you wait five minutes, then 15 minutes, then one hour. Get it wrong 10 times and the phone will wipe all the data stored in its flash memory.

It is these delay and wipe features that the FBI wanted to remove in the case of Syed Farook and Tashfeen Malik. On 2 December 2015 the

married couple shot and killed 14 people in San Bernadino, California, and injured 22 others. They were themselves shot and killed by the police a short time later.

Farook, an employee of the US government, used an iPhone owned by the government. After his death the US authorities were keen to see what they might learn from the phone, presumably to try to find anyone who might have given assistance to Farook and Malik.

The FBI couldn't gain access to the data on the iPhone as it was locked with a passcode, so they asked Apple for help - and were rebuffed. Although there have been reports the FBI asked Apple to break the encryption, what they actually did was ask Apple to help them bypass the passcode.

This method would require Apple to provide a modified version of the iOS software that disables part of the passcode lock feature; the crucial factor being that this version of iOS would be digitally signed by Apple and therefore accepted by the San Bernadino iPhone.

Apple rejected the request, so the next step for the FBI was to get a court order to compel Apple to assist in unlocking the iPhone. However, during that process the FBI backed off, claiming it had gained access to the iPhone by other means - it was later suggested a fee of up to \$1.3m had been paid to an unknown hacker.

We know the San Bernadino iPhone is unusual in the sense that the state owns it, has physical possession of it and has no chance of coercing the deceased owner to hand over the passcode. Furthermore we can guess the iPhone contained no useful data. Before the attack Farook and Malik destroyed two other phones and a laptop, and it later became clear they had disabled the 'backup to the cloud' feature some weeks before. They were clearly careful about hiding their digital tracks.

Apple takes the stance that if it creates a weaker version of iOS that can be installed on one iPhone then that software can be used on any iPhone. In this scenario the San Bernadino iPhone is the thin end of the wedge, as it is possible that not only the FBI but various other entities could use the technology to extract information from other devices.

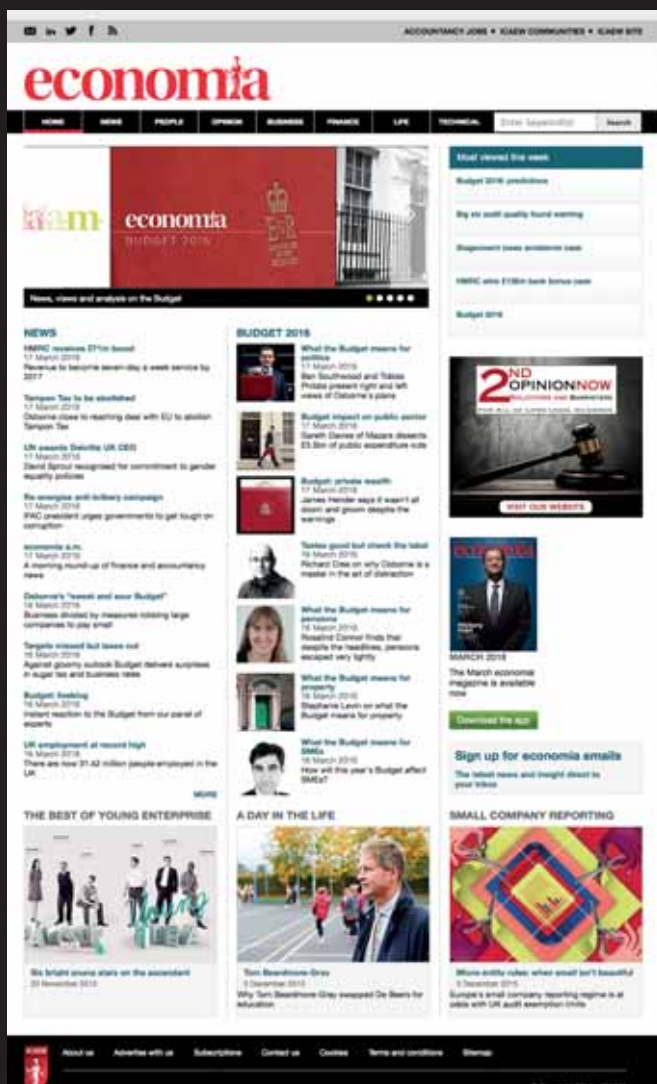
What does this mean for the rest of us? For starters we should perhaps pay closer attention to what is stored on our phones and whether it makes sense to cart our digital crown jewels with us wherever we go. If your business information is particularly sensitive, a smart move is to perform a factory reset every few months and reload just the essentials. ■

Freelance IT writer **Leo Waldock** contributes to the IT Counts blog at ion.icaew.com/itcounts



Don't miss out. Visit icaew.com/economia

news, views and analysis on the Budget, HMRC updates, the latest on the audit debate, tax and financial reporting, an online data centre, technical updates, top tips for practice management, reports on new regulation and government updates, news on mergers and acquisitions, a weekly email newsletter, *sevendays*, the *economia* blog, news and from the profession, webcasts, video interviews, jobs news and views



MOVE YOUR PRACTICE FROM IMMOBILE...



...TO "I'M MOBILE"

Manage your client accounts when and where it suits you



Your client accounts, done

Take your office with you: QuickBooks.co.uk/get-mobile