

ComputerWeekly

16-22 APRIL 2013 | COMPUTERWEEKLY.COM

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGY

DELL SEC FILING
REVEALS STATE
OF PC INDUSTRY

CHARITY STEPS UP
DATA ANALYTICS
WITH CLOUD

INTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTS

EDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITY

THE MISSION
TO UNCOVER
COLOSSUS

CW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

EXAMINING THE HEALTH ACT

AS SWEEPING GOVERNMENT CHANGES COME INTO FORCE,
WHAT EFFECT WILL THEY HAVE ON NHS TECHNOLOGY?



HOME

NEWS

THE EFFECT OF THE HEALTH ACT ON NHS IT STRATEGY

DELL SEC FILING REVEALS STATE OF PC INDUSTRY

CHARITY STEPS UP DATA ANALYTICS WITH CLOUD

INTEL IT CHIEF USES CHIP INSIGHT TO SAVE \$5M COSTS

EDITOR'S COMMENT

OPINION

BUYER'S GUIDE TO CONTEXT-AWARE SECURITY

THE MISSION TO UNCOVER COLOSSUS

CW500 CLUB ON GETTING SECURITY MESSAGE CLEAR

DOWNTIME

SOFTWARE LICENSING

Businesses blow 10% of software budgets on unused products

Businesses are wasting more than 10% of their software budgets on products that are never used. An IDC study, commissioned by licence management firm Flexera, showed that over half of enterprises said 11% or more of their application spending is associated with software products that are underused.

BUSINESS APPLICATIONS

HP chief Meg Whitman defends public attack on Autonomy management

HP chief executive Meg Whitman has defended her company's attack on the former management of UK firm Autonomy, which it acquired in 2011 for \$11.7bn. Given the significant strategic misrepresentations of the value of the Cambridge-based software firm and accounting improprieties, it was necessary to explain that to investors, she told the BBC.

HACKERS & CYBER CRIME PREVENTION

South Korea accuses North Korea of launching cyber attacks

South Korea has accused North Korea of launching the cyber attacks that shut down thousands of computers at broadcasters and banks in South Korea. Attribution of cyber attacks is notoriously difficult, but South Korean investigators said some of the malware discovered on targeted computers had been used in previous attacks linked to North Korea.

RISK MANAGEMENT

UK companies cannot stop employees stealing data, study shows

Businesses are placing too much trust in their employees when it comes to safeguarding company data, a study has revealed. Three-quarters of UK employers surveyed by OnePoll for security company LogRhythm said they had no enforceable systems to prevent employees gaining unauthorised access to company data.

PRIVACY & DATA PROTECTION

Researchers discover Android Trojan built to steal text messages

Researchers have discovered an Android Trojan, called Stels, designed to steal text messages. These messages may include Mobile Transaction Authentication Numbers used for two-factor authentication, according to Dell SecureWorks Counter Threat Unit.



ACCESS THE LATEST IT NEWS VIA RSS FEED

HACKERS & CYBER CRIME PREVENTION

Fraudsters widen card-skimming operations across Europe

Criminals using card-skimming devices are targeting transport and parking ticket machines in Europe, a report has revealed. The research from the European ATM Security Team said five European countries have reported an increase in criminals attaching card-skimmers to public transport ticket machines to steal bank card data. ■

WORLDWIDE PC MARKET GROWTH RATES



Source: IDC

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

JOBS & RECRUITMENT**IT staff most in demand but skills gap remains, finds REC study**

IT and computing staff are the most in demand but a lack of skills persists. IT and computing grew from being the second most in-demand skills area, out of 10 key industry sectors in March 2012, to the first, according to the survey from the Recruitment and Employment Confederation (REC).

PC HARDWARE**HP chairman Ray Lane steps down following shareholder attack**

Ray Lane has stepped down as chairman of the board of Hewlett Packard (HP) following a meeting with angry shareholders in March. In the shareholder meeting, the strongest protest vote was directed against the two longest-serving directors, John Hammergren and Kennedy Thompson, with 46% and 45% of votes cast against their re-election respectively.

SOCIAL MEDIA TECHNOLOGY**European banks need to improve social media interaction, finds Ovum research**

Social media will become a significant channel for retail banks in Europe in three years, according to analyst Ovum. The analyst company found that, while Europe is lagging behind, Asia-Pacific and US retail banks are spearheading approaches to social media engagement, believing it to be disrupting the way in which they interact with their customers.

CLOUD COMPUTING SERVICES**Cloud applications gain ground as enterprises deliberate how to use it**

Cloud applications are gaining critical mass in enterprise IT, according to the Corporate IT Forum. Head of research, Ollie Ross, said that, for large enterprises, the challenge was now not if enterprises should use cloud, but how they should use it.

ACCESS THE LATEST
IT NEWS VIA RSS FEED**WEB DEVELOPMENT****British Library archives the web**

The British Library is about to start archiving 4.8 million UK websites and one billion web pages, following legislation that came into force last week. The British Library has piloted the archive project aimed at preserving a historical record of British web activity and will now be free to take a snapshot of the internet every year across the UK without falling in breach of copyright law.

TECHNICAL SKILLS**CIOs must reskill to succeed with in-memory computing, says Gartner**

Analyst firm Gartner has urged CIOs to ensure their teams have the right skills to exploit in-memory computing. Massimo Pezzini, a research director at Gartner, said areas include risk management, fraud detection, e-commerce, online entertainment (gaming and betting), internet banking, online trading, profitability analysis and manufacturing resource planning. ■

FCA PROBES RBS IT FAILURE

UK financial regulator, the Financial Conduct Authority (FCA), is to probe an IT failure at Royal Bank of Scotland that also affected customers at NatWest and Ulster Bank in June and July 2012.

The glitch in the CA7 batch process scheduler ended with 12 million customer accounts frozen, leaving them unable to access funds for at least a week while RBS, NatWest and the Ulster Bank manually updated all the account balances.

The IT problems lasted for several days, causing a backlog of transactions for processing.



HOME

NEWS

How Health Act will affect NHS IT

Government zeal should not overrule practical considerations such as network speeds and handling sensitive information carefully. Kathleen Hall reports

THE EFFECT OF THE HEALTH ACT ON NHS IT STRATEGY

DELL SEC FILING REVEALS STATE OF PC INDUSTRY

CHARITY STEPS UP DATA ANALYTICS WITH CLOUD

INTEL IT CHIEF USES CHIP INSIGHT TO SAVE \$5M COSTS

EDITOR'S COMMENT

OPINION

BUYER'S GUIDE TO CONTEXT-AWARE SECURITY

THE MISSION TO UNCOVER COLOSSUS

CW500 CLUB ON GETTING SECURITY MESSAGE CLEAR

DOWNTIME

HUNT WANTS PAPERLESS NHS BY 2018

NHS ANTICIPATES MOVE TO G-CLOUD FOR SECURE EMAIL SERVICES

The cornerstone of the Health and Social Care Act, which has now come into force, saw the transfer of £60bn in funding from the defunct primary care trusts to the newly-created clinical commissioning groups (CCGs).

Chaand Nagpaul, GP and member of the British Medical Association (BMA), said the NHS is in a period of considerable transition. "It is difficult to talk about an IT strategy without considering the lack of organisational stability and that the new structures are not yet bedded down," he said.

"CCGs have been advised they will be responsible for the operational delivery of GP IT but most have only just been advised of notional budgets," he said. The government has far-reaching ambitions on information in its IT strategy, but some of those aims should be subject to a rethink, say experts.

PRUDENT SPENDING

"There has been a huge push to the tele-health issue, which needs to be carefully thought through," said Nagpaul. "Government has to learn from the past and not allow ideology and zeal to drive the agenda. It needs to be slowed down and used appropriately. There is no logic in the target of three million lives as a statistic."

The move to give all GP patients access to their records by 2015 and make the NHS paperless by 2018 is not necessarily helpful in the current climate, said Nagpaul.

"Online access to patient records is being held hostage to a political timeframe. There are serious issues to be considered if it is not handled and developed in right way," he said.

For Nagpaul, there are basic issues that need addressing before wider strategy concerns are driven through. "Day-to-day we need to make sure IT is supported and progresses in real-time and make sure the infrastructure is fit for purpose," he said.

One such area is slow connection speeds, which is affecting day-to-day work. "The N3



THINKSTOCK

[NHS network] speed used in many parts of the country is 2Mbps – about a tenth of the speed of many domestic broadband providers," said Nagpaul. "This is affecting GPs and patients on a daily basis. Speeds are not fit for purpose in many parts of the country."

An over-reliance on paper, better integration between primary and secondary care and greater functionality in IT need to be tackled before broader political ambitions.

INFORMATION ASSETS

Veena Raleigh, senior fellow of policy at health charity the King's Fund, agreed that there are significant resource and practical implications behind the information strategy in the current period of change.

"The CCGs are embryonic organisations and there is a lot of anecdotal evidence many are ill-prepared for the new tasks they need to take on. Information may be low on their priorities, but they can't begin to conduct business without it," said Raleigh.

"The NHS cannot do its business without information. That is the oil that makes the

HOME

NEWS

THE EFFECT OF THE HEALTH ACT ON NHS IT STRATEGY

DELL SEC FILING REVEALS STATE OF PC INDUSTRY

CHARITY STEPS UP DATA ANALYTICS WITH CLOUD

INTEL IT CHIEF USES CHIP INSIGHT TO SAVE \$5M COSTS

EDITOR'S COMMENT

OPINION


BUYER'S GUIDE TO CONTEXT-AWARE SECURITY

THE MISSION TO UNCOVER COLOSSUS

CW500 CLUB ON GETTING SECURITY MESSAGE CLEAR

DOWNTIME

 WHAT ARE THE CHALLENGES FOR THE NHS IT STRATEGY?

 NHS SUPPLIERS MUST BE FORCED TO LIST PRICES ONLINE TO SLASH £500M OVERSPEND

machines work, but on the whole the focus is on the machines," she said.

Raleigh believes it will take a couple of years before the health service is in a position to make changes enabled through a better use of information. "Some of the new organisations won't have the necessary information skills at the moment," she said.

"CCGs will have to develop skills and information, and there is a learning curve to using information and getting the most out of it."

Under the Act, a divide has been created between local authorities and the NHS, with information on areas such as substance misuse now viewed as a social health issue and under the jurisdiction of local authorities.

Raleigh said one of the strengths of the past was the uniform approach to information standards and policies. "Now there is more diversity and patchiness," she said.

CONNECTING DATA

Phil Molyneux, former CIO at NHS Yorkshire and the Humber, and policy vice-chair at BCS Health, said the NHS has a logistical challenge on its hands, although informatics has an increasingly important role to play, particularly in passing information across organisational boundaries to support more seamless care. This inevitably requires a shift from paper-based systems to electronically-held records of patient care.

"[National director, patients and information, NHS England] Tim Kelsey, is putting emphasis on transparency and engaging the public and patients through greater transparency, giving them a voice through greater access to data on health services," Molyneux said.

Gerry McLaughlin, director of IT Contractor, has extensive experience working in public sector IT and believes decentralising IT could make it difficult to join up data.

"If the same data is on lots of databases and systems, it can be difficult to extract good information," he said. "What they need to do is work out what each data field is, its size and its name and call it that across all their systems. That way they can build get aggregated information."

CLEAR SLAs

Another key issue for CCGs is ensuring they have the right service level agreements

(SLAs) in place with the commissioning support units that will be delivering IT services to their practices, said Molyneux.

"One of my worries is that the area teams which are charged with overseeing the system, don't have the expertise to manage IT

"THE GOVERNMENT HAS TO LEARN FROM THE PAST AND NOT ALLOW IDEOLOGY AND ZEAL TO DRIVE THE AGENDA"

CHAAND NAGPAUL, GP

SLAs and to advise CCGs, and they will have therefore to rely on the four IT leads in the regional teams," he said. "The system has lost a significant amount of IT expertise and advice with the inevitable demise of the strategic health authorities. The demands on the regional IT leads will be quite challenging."

OPPORTUNITIES FOR CHANGE

Jon Lindberg, head of healthcare at IT trade association Intellect, is positive the changes could push the transformation agenda. "When the dust settles on the new organisation, we should expect more clarity," he said. "The decentralised model fits better with incrementalism, so we can see good and bad practice across the system.

"From a central NHS England and from an industry point of view, there needs to be a clear strategy. We must have stronger enforcement of standards otherwise thousands of systems will not get joined."

Time is the upmost concern in setting out a clear strategy for fulfilling the informatics ambitions. "A strategy needs to be out by the end of summer, or it won't be able to hit the targets it wants to hit," said Lindberg. "But many willing people are prepared to help and the department is more open in engaging and seeking advice than in the past." ■

This is an edited version. For the full story, please click here

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

LACK OF
KILLER APPS
CURBS PC
REFRESHGARTNER
PREDICTS THE
DEMISE OF THE
DESKTOP PC
REFRESH CYCLE

Dell buyout plan reveals a PC industry in urgent need of transformation

SEC filings suggest the days of the major PC refresh are long gone, so CIOs need to plan for change. *Cliff Saran reports*

Dell has revealed the dire state of the PC industry, poor take-up of Windows upgrades and the need for the company to invest in research and development.

The supplier's chairman, Michael Dell, is battling to win over the hearts and minds of Dell shareholders in a bid to reprivatise and reinvent the company. But US billionaire investor Carl Icahn and private equity group Blackstone are to fight Michael Dell in a bidding war over the computer company he founded.

In one of its filings with the US Securities and Exchange Commission (SEC), which was sent to staff, Dell noted that it would be hiring additional research and development, services and sales personnel to extend the depth and breadth of its capabilities and to increase the number of customers to whom such services and solutions are provided.

In a letter to employees, he stated: "Dell's strategy of becoming an integrated provider of end-to-end IT solutions is expected to require additional investments in converged infrastructure solutions, software, cloud solutions, application development and modernisation, consulting, and managed security services.

"In addition, it is likely that we will need to make additional acquisitions to complete our transformation."

DECLINING PC DEMAND

The company suffered big losses in its most recent quarter due to disappointing PC sales. Dell reported an 11% decrease in revenues in the fourth quarter of 2012, compared with the same period last year. Its desktop and mobility business declined by 20%. Much of this is due to the poor performance of the PC business.

These figures were mirrored by market analysts. IDC's Global PC Tracker for the



Michael Dell: Dell's strategy of becoming an integrated provider of end-to-end IT solutions is expected to require additional investments

fourth quarter of 2012 showed global shipments of desktop and laptop hardware slumped by 6.4% year on year.

Gartner noted that in 2010, half of device spending was on traditional desktop and notebook PCs, and 25% on smartphones. In contrast, it predicted that by 2017, half of device spending would be on smartphones, and 20% on traditional desktop and notebook PCs.

"SEPARATION OF THE CONSUMER AND ENTERPRISE BUSINESSES WOULD BE DIFFICULT AND HAVE NEGATIVE EFFECTS FOR DELL'S CUSTOMERS AND GROWTH PROSPECTS"
BRIAN GLADDEN, DELL

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGY

DELL SEC FILING
REVEALS STATE
OF PC INDUSTRY

CHARITY STEPS UP
DATA ANALYTICS
WITH CLOUD

INTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTS

EDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITY

THE MISSION
TO UNCOVER
COLOSSUS

CW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME



Dell filed several reports with the SEC at the end of March, including one which outlined why the company needs to move away from the commodity PC business.

The 274-page report highlighted the long-term challenges facing the company, including a general lengthening of the replacement cycle for PC products, uncertain adoption of the Windows 8 operating system and unexpected slowdowns in enterprise Windows 7 upgrades. It also stated that PC sales may also be affected by consumer interest in tablets and smartphones, especially given that Dell does not make a smartphone device.

DELL AS STRATEGIC SUPPLIER

Desktop hardware may not be considered strategic, but Dell needs to become a strategic supplier. To do so, the company needs substantial additional investment to continue its current strategy of developing integrated end-to-end technology solutions for its enterprise customers.

The filing explicitly mentioned extending existing capabilities, such as cloud services, suggesting the company wants to build its enterprise cloud business. It also noted that Dell cannot remain competitive in the end-user computing (EUC) business of desktop and laptop PCs, but offloading these to focus on enterprise solutions and services (ESS) would be risky.

"Separation of the company's EUC and ESS businesses would be difficult to execute and would entail significant dis-synergies, with negative effects for the company's

customers and growth prospects," said Dell chief financial officer Brian Gladden.

A NEW APPROACH

Whatever happens to Dell in the near future, CIOs need to plan for change.

"Users should design scenarios using a number of factors," said Gartner research director Adrian Connell, "including the size of their investment in the given technology area, the amount of overlap within Dell's portfolio, the level of commoditisation and margin profile of the technology area, and timeframes considered for the investment."

In the light of what has been revealed by these filings, it would seem the days of the major PC refresh are long gone. Dell is not the only PC company suffering from a decline in sales. Market leader HP's personal systems division saw significant decline in the first quarter of 2013. The company reported that personal systems revenue was down 8% year on year, commercial revenue decreased by 4%, and consumer revenue declined by 13%.

Businesses may not be fully ready to jump on the desktop virtualisation bandwagon, which will separate PC hardware from the business applications users need to run, but they are migrating from Windows XP to Windows 7 and have suitable hardware to run desktop virtualisation in the future.

The cannibalisation of PC sales by tablet devices and smartphones shows that people in business prefer these devices to corporate laptops. So it may no longer be necessary to refresh PC hardware so frequently. ■

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

CHARITIES
RECOGNISE KEY
ROLE OF
TECHNOLOGYCHARITY
CUTS COSTS WITH
XSGO NETWORK
VIRTUALISATION

Children's charity steps up customer data analytics with hybrid cloud

Action for Children chose a hybrid cloud platform to manage spikes in traffic and use analytics to customise its website to its donors, writes Brian McKenna

When Action for Children – a UK charity that helps vulnerable and neglected children – sought to improve its data analysis to gain deeper insights into its fundraising activities, it engaged open cloud provider Rackspace to provide an on- and off-premise hybrid system. The organisation chose that model because it needed to retain some dedicated hardware on site to host sensitive data.

“With Rackspace, we knew we could achieve true public, private and hybrid portability,” says Darren Robertson (pictured), a data scientist at the charity.

“With an open platform such as Rackspace, we could take a long-term approach and avoid supplier lock-in around pricing or technology restrictions. This gives us the freedom to keep innovating, moving to new technology solutions and models as they are developed,” he says.

Robertson explains the charity's data management and analytics strategy is aimed at improving targeted advertising and personalising the web experience for donors.

MANAGING AND ANALYSING DATA

Action for Children works with more than 50,000 children and young people through 600 projects across local communities. It has amassed data on customers, donors, fundraisers and potential foster parents.

One of the reasons Action for Children chose Rackspace was because of the increased analytical capability a cloud system could offer. The supplier is providing an on-demand Hadoop cluster. “I'd love to have one of those in the office,” jokes Robertson.

His five-strong team uses SearchMetrics for business intelligence. That includes the use of an application programming interface (API) which enables the team to pull data on to the Rackspace server.



Robertson: Open platform avoided supplier lock-in

The charity also turned to Rackspace because it needed to manage spikes in web traffic more effectively. When Stephen Fry tweeted support for the charity in 2012, the consequent surge in traffic proved costly. The charity had to take a physical image of the site and put it elsewhere, says Robertson.

Charities need to get a really good return on investment for their advertising. “Blanket advertising no longer works well enough. We are now using web analytics to see what, for example, is the propensity of people living within a 30-mile radius of a children's centre to give an ongoing donation, as opposed to a one-off gift. We want regular givers, since that is more economic,” he says.

“And we need to be able to personalise the web experience for each user, so we don't ask students and multinational CEOs for the same kind of donation, for example.”

Robertson says the charity's Christmas 2012 campaign saw good results from the web analytics effort and moving to an on-demand service made significant savings. ■

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

 CIO
INTERVIEW:
HERVÉ COUREIL,
GLOBAL CIO OF
SCHNEIDER
ELECTRIC

 CIO
INTERVIEW:
CAROL FAWCETT,
CIO OF DELL
SOFTWARE

How Intel's IT chief uses hardware insight to save \$5m business costs

Many enterprises' IT segments processors to run several applications, but Chris Shaw takes virtualisation to the limits of chip capability, writes Cliff Saran



Given Intel's position in the technology sector, it is perhaps unsurprising that the chip maker is not

a typical business when it comes to internal IT. But it still experiences the same challenges faced by many other large businesses.

IT director Chris Shaw is responsible for the company's IT across Europe, the Middle East and Africa. He says that, as with many enterprises, Intel's IT department is working on virtualisation and cloud computing.

Intel's cloud programme started about two years ago. Any IT organisation may have a large amount of computing power, but the challenge, says Shaw, is knowing what is available for a new application.

A few years ago, prior to the server virtualisation project, Intel had 20,000 servers with an average utilisation of only 38%.

Like many IT department heads, he faces

**"THANKS TO
HYPERTHREADING, WE
FOUND WE WERE GETTING
A 20% BOOST IN
PERFORMANCE"**

difficult conversations with business managers who want their own servers, even when cloud is available to provide processing on demand for most application needs.

"IT in Intel is very much like IT in any organisation, where some teams will fight to keep dedicated resources for their applications," says Shaw.



Shaw: "IT in Intel is very much like IT in any organisation - some teams will fight to keep dedicated resources for their applications"

The IT department provides data to demonstrate how it can save money and explain to each business manager that they can have a unique instance, full autonomy over what is installed and that the IT department will ensure performance is not compromised.

VIRTUALISATION ACROSS THE BOARD

The IT team at Intel defined ratios for physical servers to virtual machines (VMs) by monitoring use. It then negotiated with business managers to calculate an 18-month projection of anticipated growth.

One of the benefits of modern chips is that the hardware can be segmented, allowing applications to run on physical processor cores, says Shaw.

While it is possible to dedicate specific cores for VMs, it is not something he would recommend, since it is not very different to dedicating hardware to applications.

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

"We have moved from a physical server infrastructure to a set-up where almost every application is virtualised," adds Shaw.

It has taken almost three years to become fully virtualised. Intel began with small capabilities. "Web applications are low-risk and give us the ability to see how the infrastructure can scale," he says.

Intel has since advanced to virtualising enterprise systems. "We had a significant enterprise resource planning [ERP] upgrade

performance and it is cheaper than physical processor cores," says Shaw.

With hyperthreading, the operating system (OS) treats multiple processor cores as if they were distinct processors, which boosts performance.

Shaw says the performance increase has other benefits: "For example, we can accelerate video in YouTube, which means we don't need quad-core machines when a dual-core system will do."

"ANY TEAM CAN BUILD OUT HARDWARE INFRASTRUCTURE AND PROVISION VIRTUAL MACHINES (VMs), WHICH ARE CREATED FROM VM TEMPLATES"

and did software and hardware migration, which gave us economies of scale," he says.

One benefit of running enterprise systems on virtualised infrastructure is that databases can be load-balanced across VMs - which makes them more scalable - and the VM offers built-in redundancy, Shaw says.

ENHANCED PERFORMANCE

"In practice, our current implementations of database load-balancing across VMs offer superior performance compared with using the relational database management system clustering capabilities," he says.

Even applications such as simulations - which one would usually assume need dedicated hardware - are now run on Intel's

virtualised infrastructure.

"In chip design we run simulations.

We had

assumed we would not get much improvement but, thanks to hyperthreading, we found we were getting a 20% boost in

CUSTOM VIRTUALISATION MANAGEMENT

Rather than use off-the-shelf management tools for virtualisation, Intel created custom software to automate VM provisioning.

"Any team can build out hardware infrastructure and provision VMs, which are created from VM templates," he says.

Intel built a monitoring environment that looks at VM sprawl, where virtual machines are created but never removed from the infrastructure, so they continue to consume resources. Killing these unused VMs is a bit of a judgement call for the IT team, he adds.

Shaw says the virtualised infrastructure has increased server utilisation by 17%: "We increased compute cloud utilisation from 38% to 55%, which enabled the company to save \$5.6m." ■

DATA CENTRE EFFICIENCY AT INTEL

In terms of datacentre efficiency, Intel compares its current datacentre capabilities with the so-called "best achievable" model. Along with the major roll-out of virtualisation, Intel has reduced the number of datacentres from 87 to 68.

The company has reduced costs further by refreshing older compute and storage servers with fewer, but higher performing, servers. The hardware refresh uses the latest Intel Xeon processors and solid state drives, which both reduce heat and electricity usage, and increase data access performance.

The refresh has allowed the chip manufacturer to exceed its 10% target for reducing cost per compute unit.



- > MEDWAY NHS CUTS COSTS WITH VIRTUALISATION
- > INTEL AND ORACLE ON DELL POWEREDGE SERVERS
- > CW BUYER'S GUIDE: DESKTOP VIRTUALISATION

Gartner Application Architecture, Development & Integration Summit 2013

16 – 17 May 2013

Park Plaza Westminster Bridge, London, UK

gartner.com/eu/aadi



HOT TOPICS

- *Convergence of cloud, mobile, social and information*
- *Minimizing complexity and legacy thinking*
- *Mobile application strategy*
- *Innovating vs. doing more with less*
- *New application and data integration approaches*
- *Global multi-enterprise development, governance and architecture*

Find out more and register



gartner.com/eu/aadi



emea.registration@gartner.com



+44 (0)20 8879 2430

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

Business incentives, PC sales decline and Microsoft's growth

Anyone who follows this column will have seen several recurring themes we've been banging on about lately. A few recent stories reinforce some of those points:

UK GIVES BELGIUM €300M FOR THE CLOUD

Google has announced a €300m investment in its cloud datacentre in Belgium. When was the last time you read about a similar investment in the UK by one of the internet giants? Erm, never?

That's money the UK is giving away. The UK is an obvious base for developing cloud datacentres, bridging the US and Europe. Except it won't be, as there is no incentive for bringing business to the UK. Despite close links between 10 Downing Street and Google, we have failed to gain investment in the UK. Government should be embarrassed to see that money going elsewhere.

FALLING OFF A CLIFF

Gartner and IDC reported the biggest decline in PC sales they have ever seen.

Many view the digital revolution as a manageable decline. But the disruption caused by technology will not work like that. Many markets will fall off a cliff, and companies constrained by inertia will go with it. Year-on-year declines of 11% (Gartner) or 14% (IDC) in PC sales are a sign the lemmings have started to jump.

MICROSOFT IS NOT GOING AWAY

Gartner research looked at the market for user devices – PCs, smartphones and tablets. The headline was the rise of Android, which Gartner predicts will power more than double the number of Windows devices by 2017.

Much reporting has highlighted Microsoft's purported demise. But the statistics tell a different story. Gartner sees Windows device shipments growing from just over 300 million in 2012 to 600 million in 2017. That's not a bad growth rate.

It may be a different Microsoft in 2017, one that no longer dominates the consumer or corporate IT sectors – but it will still be a force. ■

Bryan Glick
Editor in chief

ComputerWeekly

Computer Weekly/ComputerWeekly.com
1st Floor, 3-4a Little Portland Street, London
W1W 7JB

GENERAL ENQUIRIES

020 7186 1400

EDITORIAL

Editor in chief: Bryan Glick

020 7186 1424

bglick@techtarg.com

Managing editor (technology): Cliff Saran

020 7186 1421

csaran@techtarg.com

Head of premium content: Bill Goodwin

020 7186 1418

wgoodwin@techtarg.com

Services editor: Karl Flinders

020 7186 1423

kflinders@techtarg.com

Security editor: Warwick Ashford

020 7186 1419

washford@techtarg.com

Networking editor: Jennifer Scott

020 7186 1404

jscott@techtarg.com

Senior reporter: Kathleen Hall

020 7186 1426

khall@techtarg.com

Special projects editor: Kayleigh Bateman

020 7186 1415

kbateman@techtarg.com

Datacentre editor: Archana Venkatraman

020 7186 1411

avenkatraman@techtarg.com

Storage editor: Antony Adshead

07779 038528

aadshead@techtarg.com

Business applications editor: Brian McKenna

020 7186 1414

bmckenna@techtarg.com

Editorial content assistant: Caroline Baldwin

020 7186 1425

cbaldwin@techtarg.com

Production editor: Claire Cormack

020 7186 1417

ccormack@techtarg.com

Senior sub-editor: Jason Foster

020 7186 1420

jfoster@techtarg.com

Sub-editor: Philip Jones

020 7186 1416

pjones@techtarg.com

DISPLAY ADVERTISING

Sales director: Brent Boswell

07584 311889

bboswell@techtarg.com

Group events manager: Jonathan Palma

020 7186 1451

jpalma@techtarg.com



HOME

NEWS

THE EFFECT OF THE HEALTH ACT ON NHS IT STRATEGY

DELL SEC FILING REVEALS STATE OF PC INDUSTRY

CHARITY STEPS UP DATA ANALYTICS WITH CLOUD

INTEL IT CHIEF USES CHIP INSIGHT TO SAVE \$5M COSTS

EDITOR'S COMMENT

OPINION

BUYER'S GUIDE TO CONTEXT-AWARE SECURITY

THE MISSION TO UNCOVER COLOSSUS

CW500 CLUB ON GETTING SECURITY MESSAGE CLEAR

DOWNTIME

How the cloud found Mitchells & Butlers

CW500 Interview: Mitchells & Butlers' Robin Young

Digital dining: Turning retail space into a connected environment

The right mix of retail, infrastructure and content presents new opportunities for a world of managed virtual trading and entertaining, says Robin Young

The technology evolution continues at pace within Mitchells & Butlers (M&B) – a journey that began in 2011 is now moving into the exciting final phase.

Having promised the Plc board an infrastructure and architecture that would move us from being hamstrung to enabled, it was critical that our IT and change team stood up to the plate and genuinely delivered.

A successful datacentre and network migration, led by director of business change and technology, Martin Taylor, and supported by our partner Fujitsu, gave M&B both credibility and the confidence to push on with the programme to rebuild our guest-facing technology. A business Wi-Fi roll-out, again solidly delivered with our partners in O2 and Fujitsu, was the final step in our foundation work. Now the real fun begins.

Mitchells & Butlers is moving on to create some exciting guest interaction by upgrading the overall experience within our businesses. We own brands including Harvester, Toby, Browns and All Bar One, and we will be providing not only an enhanced service, but moving towards the digital completion of the guest engagement cycle.

Designing, integrating and deploying point-of-sale and payment software is just the start of this final phase. We are working actively with teams at Sky and BT to push the boundaries of content, entertainment and future trade within the best retail real estate in the industry.

It is a simple concept – Mitchells & Butlers provides a physical environment where guests can enjoy high-quality food and drink and top-class service. Pair this with a virtual environment that delivers superb multi-device content, entertainment and the ability to carry out all manner of business, and the office or home becomes a much less attractive place to spend your time. Guest choices become

the driving force behind our plans as we meet a much higher proportion of their needs and demands in this rapidly moving space.

Each expert partner focuses on what they do best – this mixture of retail, infrastructure and content provides new opportunities for a world of managed virtual trading, learning and entertaining. Initial discussions have highlighted a major appetite from other possible partner organisations keen to join this new club. The key challenges will be how to baseline and structure commercial agreements so that all those involved realise the full potential of this programme.

In a country where the next generation of economic regeneration must come from combining a track record of delivering excellent services with full exploitation of innovation, this model starts to work all the key elements. The UK has some great opportunities to show the globe how to excel in the digital business world.

Contrary to the widely held, negative view that digitisation of communication, social interactions and touch points will result in future Christmas gatherings comprising a series of flat screens around a dining table on which you “meet” family and friends, I think we are only now beginning to see the real potential.

We will see fantastic physical venues providing world-class food and service combined with content over reliable infrastructure and a digital trade and entertainment zone. Get some of these right and we have a growth alternative to quantitative easing. ■

Robin Young is chief operating officer of hospitality group Mitchells & Butlers, and runs his own advisory business, CTGFT Ltd



HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGY

DELL SEC FILING
REVEALS STATE
OF PC INDUSTRY

CHARITY STEPS UP
DATA ANALYTICS
WITH CLOUD

INTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTS

EDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITY

THE MISSION
TO UNCOVER
COLOSSUS

CW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

PUTTING
SECURITY IN
CONTEXT

GARTNER:
PREPARE FOR
CONTEXT-AWARE
SECURITY



HOW TO FIND OUT WHO IS DOING WHAT TO YOUR DATA SYSTEMS

Context-aware security cannot replace point technologies, but it can tell you when an attack is imminent and what form it will take. Bob Tarzey reports

Some things only appear suspicious when seen in a broader context. An accountant may regularly access financial data when working at their organisation's headquarters in London; it may also be usual for them to access the same data on occasions when visiting regional offices in other cities. What would not make sense would be for the accountant to download data in New York when the company's physical security system shows him to be in London, already accessing other systems from there.

Spotting suspicious activity in such a way is the concept behind context-aware security. It involves reviewing a single event with other events taking place as well against historical log data and relevant information from a range of other sources. This involves real-time access to extensive volumes of data and the ability to process it in real time. Some describe context-aware security as a big data challenge, meaning that you need the ability to process and gain useful insight from large volumes of data.

There is nothing new about storing and processing log data. Suppliers of log management software have been around for years, for example LogRhythm and LogLogic (the latter acquired by Tibco in 2012). The reasons for investing in log management principally involved compliance, allowing IT staff to produce audits of who had been doing what on their organisation's IT systems by collecting and analysing data from the log files of servers, network devices, security systems and so on.

Log management suppliers have evolved their offerings over the last decade to provide a

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

broader capability to view log data against other events happening on and around their systems. This led to the term SIEM (security information event management), first used by Gartner around 2005. SIEM tools combine log data with other information, for example about users and their rights, third-party feeds (about vulnerabilities, malware, news, weather and so on), location data (using IP addresses and mobile device tracking) and new regulatory requirements. They use all of this to provide enriched reports for compliance reporting and security review.

As SIEM became a mainstream offering, many of the big IT security suppliers entered the market through acquisition, the most notable being: HP, with ArcSight (2010); IBM, with Q1 Labs (2011); McAfee, with Nitro Security (2011); and EMC-RSA, with Netwitness (2011).

LogRhythm is considered an SIEM supplier. Others include Red Lambda, Trustwave and Sensage. Splunk is often seen as an SIEM supplier, but its focus is even broader, using IT operational intelligence for providing commercial as well as security insight.

However, to go further still and provide the promise of context-aware security in real time requires SIEM tools to be souped-up, so they can conduct analysis at speed and provide real-time protection. Quocirca termed this advanced cyber-security intelligence (ASI) in a July 2012 report. Another term used by some is next-generation SIEM (NG-SIEM).

**“CONTEXT-AWARE
SECURITY IS NOT
A REPLACEMENT
FOR EXISTING
POINT SECURITY
TECHNOLOGIES
BUT SUPPLEMENTS
THEM”**

BASIC REQUIREMENTS OF CONTEXT-AWARE SECURITY

Whatever term you prefer, any supplier claiming to offer a broad, context-aware security capability should have tools that can do all of the following:

- Process and analyse large volumes of data in real time;
- Have an advanced correlation engine to process and compare information from disparate sources;
- Be able to enforce advanced rules that link disparate events and prescribe what should happen if there is an anomaly;
- Include a range of out-of-the-box rules as well as allowing customers to write their own;
- Have the intelligence and insight to act and prevent security breaches as they happen;
- Have the capability to adapt to events and improve future responses;
- Gather data from external feeds;
- Have the capacity for the long-term storage of IT intelligence data in a central repository;
- Provide an intuitive interface and dashboard for ease of use by all security staff.

NG-SIEM is not the only way to provide context-aware security. Some suppliers have added specific capability to provide context around their various security products. For example, Kaspersky Lab's System Watcher combines information drawn from its firewall, behaviour analyser and cloud-based reputation server to provide a broader overall risk assessment of suspected malware.

Other tools provide very specific context awareness. For example, Finsphere uses mobile phone numbers as an additional means of user authentication. The supplier compares this with information about the user's location to make sure a given login makes sense (similar to the example used at the start of this article). To achieve the high-speed processing necessary to deliver this in real time, Finsphere has just signed a deal with Violin Memory.

Context-aware security is not a replacement for existing point security technologies such as antivirus, firewalls and intrusion prevention systems but supplements them. It provides insight that can identify a malicious attack or undesirable user behaviour – an even greater risk that needs to be mitigated.

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

HOW CONTEXT-AWARE SECURITY SUPPLEMENTS POINT SECURITY TECHNOLOGIES

Here are some examples of where ASI may succeed where point security products fail:

■ **Detecting zero-day attacks:** Signature-based antivirus software cannot detect newly constructed malware, which is often used during targeted attacks. Correlating server access logs to identify that the same server is being used to contact many other servers and user end-points on the same private network and is sending messages home to an unusual IP address would give an early warning that something is amiss.

■ **Detecting hacking and preventing data theft:** An intrusion prevention system may prevent multiple failed attempts to access a server from a particular IP address, but may not see that data is already being copied from that server due to a single successful penetration from the same IP address. Correlating log and event files could identify that two such events are related and lead to the prevention of a data theft. Target attacks often have this sort of profile.

■ **Non-compliant movement of data:** It might be usual for an employee to access customer information; it may also be usual for them to download it to a file for reporting reasons. However, for them to copy the data to a non-compliant location – for example a cloud storage resource in a certain country – should raise an alarm. This requires rules that understand user access rights and current compliance requirements and the ability to correlate these in real time with attempts to copy data and the location of the target storage service.

■ **Absence of an event:** Scada (supervisory control and data acquisition) systems are often controlled using human-machine interfaces (HMI); this requires someone to be present, which, with physical security measures in place, should be preceded by a record of the employee involved having used an ID badge to enter the premises in question. So, if an action is logged on an HMI system at a remote location that is not preceded by a valid record of physical entry, either someone has gained unauthorised access or the HMI has been hacked remotely. An advanced correlation rule that looks for the presence of the badge reader log in a specified time prior to an HMI access request enables such a breach to be detected

■ **Anomalous system-administration activity:** If a system administrator account has been compromised, there may be an attempt to create a new account for future use. Correlating this activity with a change control system will identify that the creation of such accounts has not been authorised.

■ **Unexpected access routes:** Some databases are only normally accessed via certain applications, for example credit card data is written by an e-commerce application and only read by the accounts application; access attempts via other routes should raise an alarm if the tools are in place to correlate such events and observe that a rule about the normal access route is being broken.

For businesses, there will be no end to the struggle to get the upper hand over cyber criminals, hacktivists and indeed their own users. For governments, the situation is arguably even worse, as cyber space becomes the fifth theatre for warfare after land, sea, air and space, and terrorists see cyber space as a way to go after critical infrastructure. All have to keep upping the ante to avoid falling too far behind, or perhaps even get ahead, turning cyber security into an offensive rather than defensive act.

So much criminal activity and political activism has now been displaced from the physical world to cyber space – or at least extended to cover both – IT security teams are now on the front line when it comes to ensuring their businesses' continuity with reputations intact. To this end they must be enabled with the tools that provide broader context for the activity on the systems they manage, to protect their business from problems tomorrow that no-one can envisage today. ■

Bob Tarzey is service director at Quocirca. [Click here](#) for Quocirca's free report, Advanced Cyber Security Intelligence



- > VIDEO: HOW SECURITY LEADERS JUSTIFY COSTS
- > SECURITY AWARENESS TRAINING MADE EASY
- > LIFECYCLE OF AN ADVANCED PERSISTENT THREAT

HOME


NEWS


THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

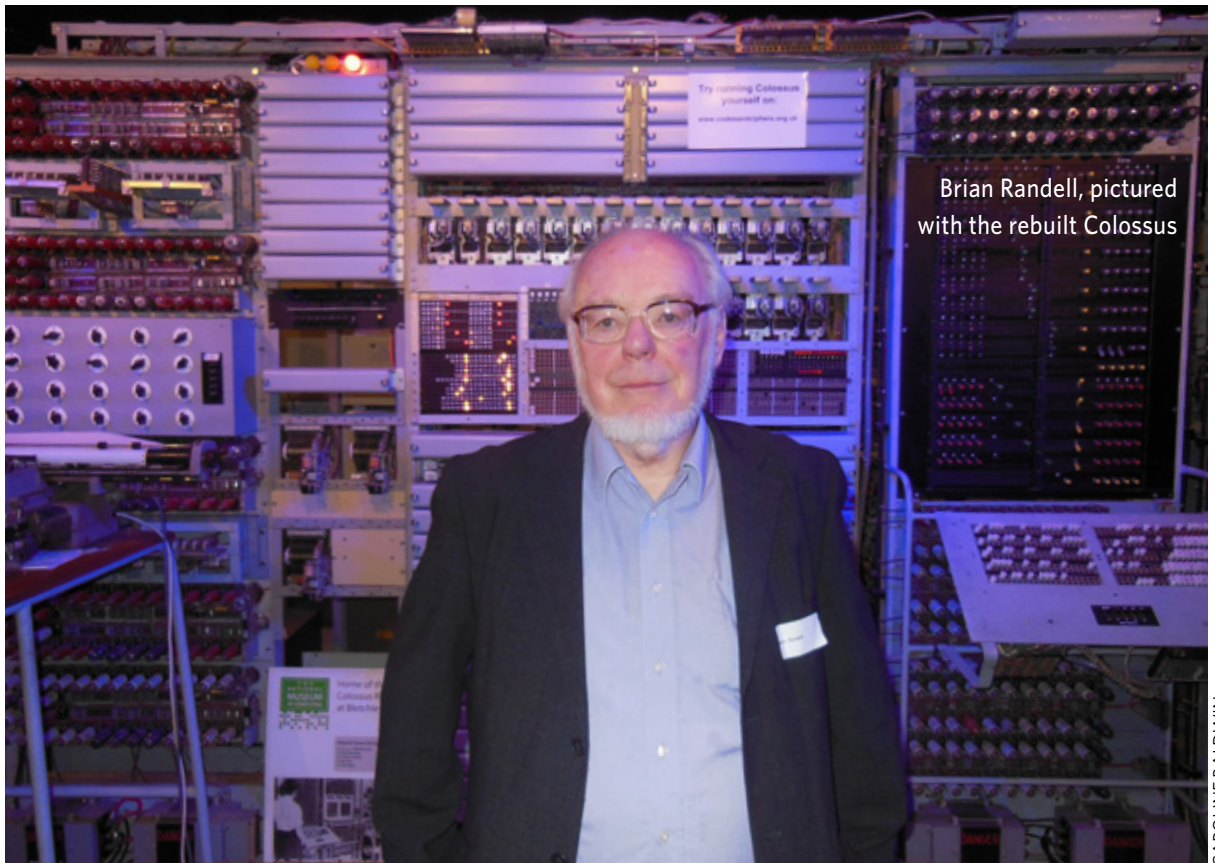
OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

 PHOTO
GALLERY:
COLOSSUS, THE
WORLD'S FIRST
ELECTRONIC
PROGRAMMABLE
COMPUTER

 WORLD'S
OLDEST DIGITAL
COMPUTER
BROUGHT BACK
TO LIFE



Brian Randell, pictured
with the rebuilt Colossus

CAROLINE BALDWIN

ONE MAN'S MISSION TO UNCOVER A WWII DECRYPTION MACHINE

Computer scientist Brian Randell relates his story of tracking down and rebuilding the world's first programmable computer. Caroline Baldwin reports

Colossus was the computer at Bletchley Park used during World War II to decipher messages sent between Hitler and his generals. The work carried out by the world's first programmable electronic computer is thought to have shortened the war by months, perhaps even years (see *panel, page 20*). However, its victorious reputation was kept secret by the UK government for many years after the end of the war.

But one curious computer scientist stumbled across a clue about the machine's existence and his persistence finally led to the computer being declassified from the Official Secrets Act to be appreciated by the world.

Brian Randell, emeritus professor at the School of Computing Science at Newcastle University, followed hints and clues about the machine over many years and his determination was instrumental to unveiling its postwar secrets and giving the credit it deserved.

While the story of the Colossus computer has been known for some time, Randell's story of how he uncovered the secret has only recently been revealed.

Kevin Murrell, trustee at The National Museum of Computing (TNMOC), attributes Colossus's rebuild in recent years to Randell's research and "sheer bloody-mindedness". But Randell said it was his "excessive curiosity" that drove the project, addressing delegates drawn from the IT industry and academia during an event honouring his achievements at TNMOC at Bletchley Park.

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

GALLERY:
THE 100TH
ANNIVERSARY OF
THE BIRTH OF
ALAN TURINGCOLOSSUS
REBUILDER
TONY SALE DIES,
AGED 80VINTAGE
COMPUTERS GO
ON SHOW AT
BLETCHLEY PARK

"I find it quite amazing, the move from seeing a photograph of the Colossus in 1975 to standing in front of the Colossus in 2013," he said.

It started when Randell set upon writing a book in the 1970s, on the origins of digital computers. "I set myself as the scope from Charles Babbage in 1837 through to the earliest computers that we would recognise as digital computers, modern in every sense other than visual. In particular, the Electronic Delay Storage Automatic Calculator (EDSAC), which was built at Cambridge and is now being rebuilt at Cambridge and at the TNMOC," he said.

Randell's curiosity was piqued by a biography of Alan Turing, written by his mother, Ethel Sara Turing. In particular, one paragraph caught his eye, describing how she knew nothing of her son's involvement in the war. Turing had "disappeared" to Bletchley Park, leaving no clue as to what he was doing. This told Randell there was something left to uncover at Bletchley.

THE START OF THE TRAIL

Randell hunted down an old *Washington Post* review of the 1967 book *The Code Breakers*, by David Kahn. The reviewer, Alfred Friendly, said Kahn had omitted important events that happened in the UK during the war. This gave Randell a new focus.

He had his first breakthrough with an obscure 1970 publication by Jack Good, a mathematician who had worked with Turing at Bletchley. *Some future social repercussions of computers (Intern. J Environmental Studies, 1, 67-69, 1970)* referred to a British cryptanalytic machine, but Randell found there was no explicit reference to the Colossus.

"This was the first – as far as I know – public revelation of the Colossus," said Randell.

However, he managed to track down Donald Michie, who had also worked at Bletchley Park during the war. Michie was prepared to name the machine.

"I put this information into a 1972 paper (*Machine intelligence: On Alan Turing and the origins of digital computers*) with permission to use quotes from people who I was sure didn't have the right to say what they said," said Randell.

**"THEY SHOWED
ME PHOTOGRAPHS
OF COLOSSUS
AND I WAS TOLD
THEY WERE TO BE
RELEASED TO THE
PUBLIC RECORD
OFFICE"**

BRIAN RANDELL

COLOSSUS – THE WORLD WAR II CODE BREAKER

Colossus was the world's first programmable electronic computer and aided in deciphering the encrypted messages sent between Hitler and his generals during World War II.

The power of Colossus significantly reduced the time it took to decipher codes, accelerating the Allies' code-breaking operation. The National Museum of Computing (TNMOC) states that over the course of the war, 10 Colossus computers, worked by 550 people, had managed to break 63 million characters of high-grade German communications.

The information taken from these decrypted messages is believed to have shortened the war by many months, according to TNMOC. However, according to Professor Sir Harry Hinsley, official historian of British Intelligence in World War II, it may have shortened the war by up to two years.

In 1992, computer engineer and programmer Tony Sale began to reconstruct a Colossus computer. With the help of his team, Sale succeeded in 2007. On completion of the rebuild, the Colossus cracked the Lorenz code used by the German armed forces in 3.5 hours. This compares with modern-day computer software, which broke the code in 46 seconds.

The rebuild of the Colossus is on display in a public gallery at TNMOC at Bletchley Park.

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME



- > GALLERY: BLETCHLEY PARK'S CODEBREAKERS REBUILT
- > COLOSSUS: THE FIRST PROGRAMMABLE COMPUTER
- > COLOSSUS STAR ATTRACTION AT MUSEUM

The paper presents evidence that, during the war, Turing was associated with a group of scientists that designed and built a series of special purpose, electronic computers – which were at least in a limited sense “program controlled” – and that the origins of several postwar, general-purpose computer projects in Britain could be traced back to these wartime computers.

“I knew the government wouldn’t have wanted it published, but it had quotes and innocence,” said Randell.

“In 1972, I wrote to Edward Heath, the prime minister, requesting Colossus be declassified, and I received a reply which implicitly suggested it existed,” he said. However, Heath replied to the effect that the Colossus programme could not be declassified, citing considerations of the national interest.

CABINET OFFICE DECLASSIFIES COLOSSUS

Randell’s book, *The Origins of Digital Computers, Selected Papers*, was published in 1973. The book included a two-page summary by Michie of Randell’s findings about Turing.

At this point, Randell felt this was as far as he could go in telling the world about Colossus and he stopped searching until 1975. A number of books were published in 1975, but Randell said the true relevance of Colossus remained a secret.

“This emboldened me to raise the issue of clearance again,” said Randell. He then approached Leonard Hooper, ex-director of GCHQ, who was at that point working in the Cabinet Office.

“I was invited to a discussion in July 1975 in the Cabinet Office with Sir Leonard,” he said. “I was ushered into a room to meet him and Dr Ralph Benjamin, GCHQ chief scientist.

“They showed me photographs of Colossus [see above] and I was told they were to be released to the Public Record Office. I was also shown a caption to the set of photographs and asked for my advice.”

This was the point when Randell first saw the machine he had been chasing for so long.

Randell was then authorised to interview the Colossus team and to publish papers, once the drafts had been cleared by the government.

He started interviewing ex-Bletchley workers. This was a challenge, as Bletchley was so fragmented and the workers were bound by tight secrecy and security. “They never discussed work in the cafeteria. Few knew what happened outside their own small group,” he said.

There were no diaries or paperwork and, it now being 30 years after the war, the interviewees found it difficult to recall all the events. “Even establishing a chronology was very difficult,” said Randell.

He taped and transcribed interviews with Tommy Flowers, Bill Chandler, Sidney Broadhurst, ‘Doc’ Coombs, Max Newman,

Donald Michie, Jack Good and David Kahn.

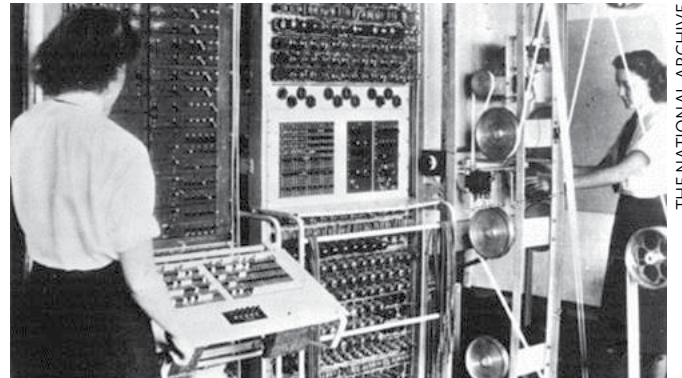
After much to-ing and fro-ing with the Cabinet Office, Randell finally got clearance for his paper on Colossus to be released in time for the 1976 Los Alamos Conference.

“I was asked not to imply that Colossus was built for code breaking,” he said. So the paper, entitled *Computing and Laboratory*, did not state the main purpose of the Colossus machine.

A year later in 1977, the BBC’s *Secret War* TV series identified Colossus as a code breaker.

Randell replied to the prime minister’s letter pleading that a report about the Colossus should be made in living memory, even if it had to be classified indefinitely.

Colossus was eventually declassified in 2003. ■



THE NATIONAL ARCHIVE

In 1975 Brian Randell attended a discussion at the Cabinet Office, where he had his first glimpse of Colossus

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGY

DELL SEC FILING
REVEALS STATE
OF PC INDUSTRY

CHARITY STEPS UP
DATA ANALYTICS
WITH CLOUD

INTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTS

EDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITY

THE MISSION
TO UNCOVER
COLOSSUS

CW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

 **CW 500
SECURITY CLUB:
MARK BROWN,
ERNST & YOUNG**

 **CW 500
SECURITY CLUB:
GARETH
LINDAHL-WISE,
BAT**

STANDARDISED PROCEDURES WILL HELP CONVINCING THE BOARD ON SECURITY

CW500 Club hears how security professionals need to move from being blockers to technology enablers to win credibility. [Bill Goodwin reports](#)



THINKSTOCK

Most businesses think their chief information security officers (CISOs) are not doing a good job at securing their organisations, according to Mark Brown, director for risk and information security at advisory firm Ernst & Young.

"Not only are they saying they don't think we are doing a good job as information security professionals, they are actually saying we are not doing a good job from the point of view of the business," he said.

Brown drew on research by Ernst & Young to challenge security professionals to start thinking less about technology and specialist security solutions and more about the business needs of their organisation.

"We need to demonstrate the moral courage to challenge our own profession, to challenge our teams and our own way of working," he told IT security professionals at Computer Weekly's CW500 Security Club.

Company boards, he said, have lost patience with security professionals who do not understand the language of business. "If we want to be listened to, we can't talk bits and bytes, we

SPEAKERS

- **Mark Brown**, Ernst & Young
- **Gareth Lindahl-Wise**, BAT
- **Alan Jenkins**, T-Systems

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

can't talk fear uncertainty and doubt, we can't talk hellfire and brimstone; we have to speak a language that will be listened to," said Brown.

To win credibility, security professionals need to move from being technology blockers to become technology enablers, he said.

"Security can make business sense. It is linked to business strategy, business process and enterprise architecture," said Brown.

Measuring the effectiveness of the enterprise security architecture and being able to demonstrate that to the board is vital, the meeting heard.

Some organisations look at risk tolerance levels, while others look at the balance between investments in IT security and savings to the business. Tracking the number of security incidents over time is another common metric.

In his previous role as CISO of SAB Miller, Brown said he was asked to present security metrics to the board.

"My predecessor had a metrics dashboard which talked about the number of virus events, the number of firewall breaches and the number of patches," he said.

Brown took the dashboard idea a stage further to present an analysis of the total cost of security incidents to the business.

"A virus costs this much downtime, that much operational profit - that is what the board wants to hear," he said. It requires an intimate knowledge of the business to understand what an hour of downtime actually means.

"Can a site operate at 70% effectiveness, or does it have to operate at 100%? You can then quantify the financial impact, through risks, and that is the key success indicator the board will actually listen to," said Brown.

Gareth Lindahl-Wise, group information security manager at British American Tobacco, said security professionals should focus on making sure the processes are right.

"It is not necessarily always a case of focusing on the outcome. It is putting faith in the idea that if you define the process correctly and you follow it, you are likely to come up with the right answer," he said. It is a mindset that does not rely on measuring the performance of patching or firewalls, according to Lindahl-Wise.

RISK MANAGEMENT

Risk management is an area where companies have a lot to learn. Too many professionals take a formulaic approach to risk, a legacy from the financial services industry, according to Brown.

"How many companies have even documented what their risk attitude is, or would even know how to start to document that risk?" he asked.

For many, the answer to risk management is simply to create a risk register. "A nice little spreadsheet. Yes, it's got a bit of red, a bit of green, a bit of amber. Have we updated it? Yeah, we changed a few colours here and there'. That is not risk management," said Brown.

Alan Jenkins, who has just left his role as CISO at T-Systems, agreed that risk management is a weak area for many IT security professionals. "Our business acumen, skills and understanding all need to get a lot better," he said.

History shows that strong risk management can make all the difference when a company is hit by a security breach. RSA, for example, had a major breach two years ago, which compromised the security of its smart tokens.

"The stated cost immediately after the breach was around \$64m to fix. I think we all

"IF WE WANT TO BE LISTENED TO, WE CAN'T TALK BITS AND BYTES, WE CAN'T TALK FEAR UNCERTAINTY AND DOUBT, WE CAN'T TALK HELLFIRE AND BRIMSTONE"

MARK BROWN, ERNST & YOUNG

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

recognise that it was a conservative number and the actual cost was a lot bigger," said Jenkins.

Yet, RSA handled the breach well, and is not only still in business, but shipped a record number of smart tokens last year.

Contrast that with Sony, which suffered a similar hacking attack. "Its market share, just over a year on, is something like two-thirds lower," he said.

PROFESSIONAL CERTIFICATION

Another area where professionals struggle is the lack of a widely-recognised professional certification for IT security specialists.

The market is overcrowded with professional associations and alternative professional qualifications.

"We need to cull the societies that want to become the professional body [for security specialists], amalgamate them and get them to come up with one certification," said Brown.

It is being tackled by e-Skills UK, the public/private sector partnership for IT training, which has won government funding to create a cyber security skills framework.

Philip Virgo, chairman of the Conservative Technology Forum, is looking for employers to take part in the framework's development.

"All the funding is around information security skills, except the reality is, if you are a user, you want a mixture of infosecurity skills, physical security and business understanding if you are going to deliver real value for money," he said.

The framework will aim to establish which security skills need to be in-house and which can be outsourced. "The good news is that e-Skills has done a good job corralling pretty much all the warring information security tribes," said Virgo. "The bad news is that they are all purists. That is why I need employers to get them into shape."

ADDING VALUE

If security professionals can demonstrate how they can add value to the business, they are unlikely to find difficulties winning funding, said Brown.

Those companies that have adopted security enterprise architecture approaches have seen their security budgets go up, he said.

"The budgets are going one way, and that is up, because you are actually demonstrating how they have added value to the company, how they protect the value within the company and how they minimise the actual risk," he said.

Most board directors sit on multiple boards, and they don't want to be seen spending less than their competitors. "In my experience, if you ask the right questions in the right way, you will get funded," Brown said.

But acquiring a business mindset can be challenging for security specialists who are steeped in technology. Brown advised information security professionals to spend time out of the IT department, to learn the workings of the business. "By doing that, you also get to know who the movers and shakers are, you learn who to contact and who can be a friend and an ally. You also learn who to avoid," he said.

Communication is also essential. Ernst & Young's survey revealed that 60% of boards only receive one or two briefings a year on security. "If they are only getting one five-minute

UK BUSINESS LEADERS' VERDICT ON IT SECURITY

- 85% state that information security is not fulfilling business needs
- 88% report an increase in external threats
- 57% report an increase in internal threats
- 61% cite a lack of budget as main hurdle
- 57% of businesses view information security resources as lacking necessary skills
- 62% do not align information security to enterprise architecture or business process
- 38% do not align to organisational risk appetite

Source: Ernst & Young

HOME

NEWS

THE EFFECT OF THE
HEALTH ACT ON
NHS IT STRATEGYDELL SEC FILING
REVEALS STATE
OF PC INDUSTRYCHARITY STEPS UP
DATA ANALYTICS
WITH CLOUDINTEL IT CHIEF USES
CHIP INSIGHT TO
SAVE \$5M COSTSEDITOR'S
COMMENT

OPINION

BUYER'S GUIDE TO
CONTEXT-AWARE
SECURITYTHE MISSION
TO UNCOVER
COLOSSUSCW500 CLUB ON
GETTING SECURITY
MESSAGE CLEAR

DOWNTIME

A NEW
APPROACH TO
INFORMATION
SECURITYSECURITY
THE FUTURE:
KEEPING UP WITH
THE BUSINESS

briefing a year, they can't be knowledgeable about the risk. We have to elevate the message in the right manner so it will be listened to," said Brown.

QUEST FOR COMMON STANDARDS

One of the biggest challenges facing CISOs is that each IT supplier approaches security in a different way. "There is no unifying standard for security architecture," said British American Tobacco's Lindahl-Wise. The more suppliers and outsourcers a company works with, the greater the complexity and challenges of getting different systems to work together.

"When you start throwing more suppliers in, you have got a slightly different feel. You multiply that challenge and complexity and confusion again and again," he said.

For Ernst & Young's Brown, the problem is analogous to having multiple firewalls on a network. "If you have one rule, it is easy to secure. If you have multiple rules, you create overlaps and gaps. It is exactly the same when you have multiple suppliers," he said.

A new security and outsourcing standard - ISO 27036 - will offer a stepping stone to simpler security. But a single standard for enterprise security architecture is unlikely.

"Industries and sectors may be able to get together and agree they can live with one standard, and that will help them and help the outsourcers," said Lindahl-Wise.

In the meantime, the best advice is to keep the enterprise security architecture simple.

"If you can keep your enterprise architecture as simple as possible, with as few moving parts as possible, it will survive a lot longer," said Brown. ■

CASE STUDY: T-SYSTEMS

T-Systems, the outsourcing arm of Deutsche Telekom, has developed a company-wide enterprise security architecture. Dubbed Enterprise Security Architecture for reliable ICT services (Eсарis), the aim is to help T-Systems reduce costs by having a single methodology for security.

"We are trying to drive standardisation. That is becoming important to reduce costs and leverage our capabilities across the group," Alan Jenkins, chief security officer at T-Systems, told the CW500 Security Club.

The company, which provides outsourcing services, believes standardisation is essential to keep down costs for customers. "These days we can see year-on-year cost reductions of around 6% as standard in our contract, so if we keep on delivering the same, that gap between our revenues and our cost base narrows," he said.

Eсарis is a complex framework with a lot of accompanying paperwork. It draws on well-known security standards, such as ISO 27001 and PCI.

And, in typically German style, there is a significant focus on standardised processes, according to Jenkins: "That is how we drive consistency, repeatability and quality, as those are key parts of what T-Systems seeks to offer the market."

T-Systems offers clients a bespoke outsourcing service, but nevertheless places a strong emphasis on standardising its approach. Eсарis offers standard building blocks, which the company can tailor to each customer.

"We aim for 70% in common across an area, 20% in common across an industry sector, and the last 10% specific to a customer," said Jenkins.

Increasingly, outsourcing customers are demanding evidence about the strength of their security, more often than not, because industry regulators are also demanding it.

"We need to make sure we have got the procedures in place, for example the granting of administration rights, so we can track who has got root access and who has not," he said.

Keeping an audit trail of systems changes is a challenge in itself. "We have one architecture, 20 concepts, 31 standards, 500 security measures and more than 12,000 pages [of documentation], and growing," said Jenkins. "We are a German company after all."

HOME

NEWS

THE EFFECT OF THE HEALTH ACT ON NHS IT STRATEGY

DELL SEC FILING REVEALS STATE OF PC INDUSTRY

CHARITY STEPS UP DATA ANALYTICS WITH CLOUD

INTEL IT CHIEF USES CHIP INSIGHT TO SAVE \$5M COSTS

EDITOR'S COMMENT

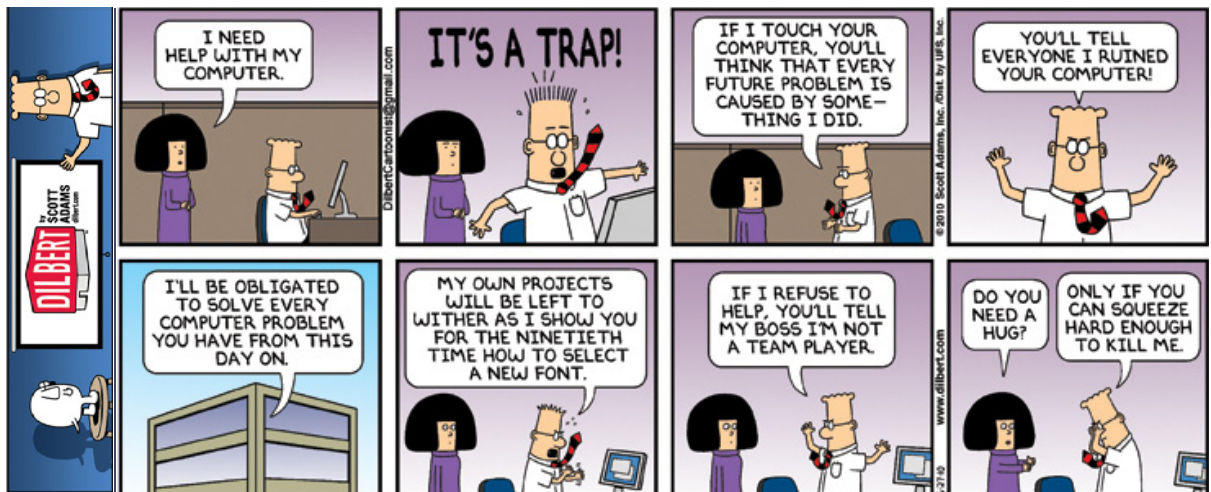
OPINION

BUYER'S GUIDE TO CONTEXT-AWARE SECURITY

THE MISSION TO UNCOVER COLOSSUS

CW500 CLUB ON GETTING SECURITY MESSAGE CLEAR

DOWNTIME



Is Wi-Fi a stairway to heaven?

The key communication device between a worshipper and their God, or so Downtime has been led to believe, is prayer or perhaps the odd ritual sacrifice.

But it seems that even organised religion wants to catch up with the times and use some technological advancements to up their game.

St John's Church in Micklegate, Derbyshire, has done a deal with The Cloud, owned by Rupert Murdoch's BSkyB (so make your own conclusion who they did the deal with) to hook the house of worship up for the modern age, by which they mean, with Wi-Fi.

The Cloud has provided the church with a slew of tablets and using the wireless connectivity can now provide the church service in full over the devices, letting those struggling to see the small fonts commonly used in The Bible or hymn books to enlarge them and follow along



with the service much more easily.

"First we saw the Pope tweeting and now this service via Wi-Fi at St John's - perhaps the church can teach others a few things about keeping up with modern technology," claimed Vince Russell, managing director of The Cloud.

Well, they may not believe in gay marriage or women as bishops, but at least the Church of England has some technological nous, hey? ■

THE JOHN-E-READER

Someone out there is hoping to get funding for a production run of a gadget that holds your e-reader when you're sitting on the loo.

The fabric sleeve attaches to the toilet paper holder by acrylic handles so you can store your tablet safely for those people who like to read on the loo and there's even a "Jumbo John-E" version available for larger tablets.

Never mind be kind to your behind, be kind to your Kindle.



READ MORE ON THE DOWNTIME BLOG