TODAY'S CIO

Summer 2014

The Security Edition

Sponsored by

bcs The Chartered Institute for IT

upland

THE TOOLS TO BUILD IT SUCCESS

CLOUD ENTERPRISE WORK MANAGEMENT SOFTWARE

PROGRAM & PORTFOLIO MANAGEMENT

POWERSTEERING® by upland

SOCIAL PROJECT MANAGEMENT

EPMLive by upland

IT FINANCIAL MANAGEMENT

comsci by upland

To Learn More:

0845 888 0999

info@uplandsoftware.com

www.uplandsoftware.com

Different IT Governance challenges require different systems. Don't settle for a "one size fits all" approach.

Welcome

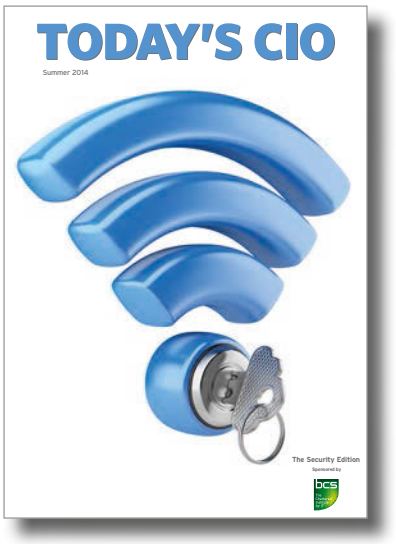
Welcome to the launch edition of *Today's CIO*. This publication recognises how central Information Technology has become in the modern organisation. Speed, responsiveness and access to immediate platforms are crucial to survival and to growth in the technological world. Therefore today, the CIO has emerged as fundamental to business success.

Whether it be routers or networks, cabling or mainframes, security or social media, the CIO has the fastest evolving company role of any C-suite executive and the rate of service and product innovation offers an almost daily challenge. Keeping up to speed with all this requires valuable information.

Today's CIO publication will focus on the main topics of Security, Big Data, Strategy, Technology and Innovation, along with a section on Spend and Budget Management. The editorial is a mixture of respected business experts providing impartial advice on modern innovations or practices as well as significant contributions from prestigious **The British Computer Society – The Chartered Institute for IT (BCS)** who have supported this publication's launch.

Today's CIO is one corner of our unique product in the market place, the C-suite, a platform to facilitate those at the C-suite level to gain access to the largest companies in the UK and Europe. Look out for our additional launch titles, *Today's CFO* and *Today's CEO*. Additional information can be found on www.theCsuite.co.uk

We hope you find *Today's CIO* an important addition to your information network.



Sponsored by

bcs The Chartered Institute for IT

theCsuite.co.uk

Sparta publishing

www.spartapublishing.co.uk
Tel: +44 (0)20 7970 5690
40 Bowling Green Lane, London EC1R 0NE

TOSHIBA
Leading Innovation

IPedge

THE EDGE
YOU'VE BEEN LOOKING FOR

The IP*edge* Advantage

Single Server Simplicity Provides Cost Savings

Multiple applications run on the IP*edge* server which delivers significent savings on equipment and maintenance costs

Unified Communications Increases Productivity

Connect, Communicate and Collaborate with presence, PC integration along with audio, video and web collaboration

IP*edge* EP
Supports up to 40 users per server

IP*edge* EC
Supports up to 200 users per server

IP*edge* EM
Supports up to 1,000 users per server

IP Telephones

www.telecoms.toshiba.co.uk

Sponsor's Feature

Foreword

Security


Over
120,000
units installed
One of
the UK's
most respected
telematics companies
Quartix
2014
HONOURS
Van Fleet World
FleetNews
READER RECOMMENDED
2013
Call us today for a quote
0870 013 6663 • enquiries@quartix.net • www.quartix.net

Big Data

Technology & Innovation

Strategy

Spend & Budget Management

Standards that
create the outstanding

Next

Are you ready for the next wave of computing?

Our ***Next Wave*** whitepaper series examines the technological trends set to impact business and the skills of the workforce

bcs.org/nextwave/tcio

BC731/LD/AD/0414

‘We want our people to fulfil their potential in Allianz. Our partnership with BCS brings us closer to our aim.’

John Knowles Director of IT and Off Shore Operations **Allianz Insurance Plc**

Are you a next wave CIO?

The era of ubiquitous computing is upon us. And with each new advance comes the need for a new, more diverse set of skills. What was once ‘next practice’ is now best practice and businesses need to stay sharp to stay ahead of the technological curve.

Consequently, the role of CIO has never been more important. However it is not a given that the IT function will remain at the centre of organisational transformation, as more and more of the IT budget starts to go directly to the users. The game has changed – so how do you ensure that you and your people remain strategically relevant?

Today’s successful digital leaders are able to understand the opportunities for their business in the next wave of computing. And they command teams with the technical ability and business acumen to harness the wave’s potential.

Lead the transformation

Technology trends such as augmented reality, 3D printing and cognitive computing are going to turn the IT industry on its head. Set the next practice standards in your team now, and you’ll transform your IT function from cost centre into catalyst for innovation and business performance.

At BCS, The Chartered Institute for IT, we provide digital leaders with the tools to align their IT resource with their strategic business goals so they can lead change within their organisation. We partner with companies of all sizes to develop people, forge culture and grow IT capability.

Developing your team

In the agile age, where ‘IT’ projects are increasingly cross-disciplinary, technical skills are no longer enough. Your IT people need to be good communicators and problem-solvers, with advanced analytical skills and commercial awareness built in. Creativity and vision are of growing importance too; how do you design and build the flows of information into cognitive systems? How can 3D printing templates enhance your product range or streamline your supply chain?

‘These are challenging times for business and individuals, so it’s more important than ever that we keep our team’s skills updated.’

Keith Lucas Divisional Director ICT
Foster Wheeler BCS Partner

In McKinsey’s 2013 global survey, IT under pressure, two thirds of CIOs agree it’s a significant challenge for their organisations to find, develop, and retain talent. McKinsey states that this challenge is ‘exacerbated by the lack of formal processes to govern IT talent and skills management.’

The Institute’s skills, training and development framework, SFIA***plus***, provides an effective best practice foundation from which to drive the development of your team.

By deploying SFIA***plus***, you can define job roles and align them to your business requirements, achieving absolute clarity around your IT skills landscape. SFIA***plus*** addresses the need for a common language and definition of skills across the profession. The framework will underpin your development, recruitment and retention processes and provide a level of transparency to your plans for growth.

‘SFIA***plus*** offered the flexibility to tailor roles to the specific needs of our employees. We now have a basis on which to build future talent management programmes.’

Gene Bernier Director of ITS Program Management Office
Kimberly-Clark BCS Partner

Organisations around the globe partner with us to exploit our unique insight and experience. We take a collaborative approach, ensuring our tailored solutions work in the relevant markets. For personal development goals, our digital leaders coaching programme offers one to one support in achieving specified outcomes.

Find out how we can help you deliver the value that your organisation needs. Visit **bcs.org/businesssolutions**

Which of these employees poses the greatest risk to your organisation?

Your existing systems will tell you about the ones in grey. idax will identify the person in red.

To arrange a demo email
webexdemo@idaxsoftware.com

idax
identity management

What the digital leader wants: 2014 and beyond

By **Brian Runciman**, BCS

WHAT DO DIGITAL LEADERS NEED TO KNOW NOW, and in the near future? There are plenty of issues of out there: enabling the mobile workforce, dealing with legacy systems, when and how to migrate to cloud services and of course the always looming security issues.

A little further ahead and businesses will be looking at augmented reality, 3-D printing and the like.

Still, the headline management issues for digital leaders have stayed consistent: business transformation and the attendant organisational change; strategy and planning; and the need for operational efficiencies.

We at BCS recently undertook a survey of CIOs and digital leaders and it showed that for 2014 that 64 per cent of respondents rate business transformation and organisational change as among their organisation's top three management issues, followed by strategy and planning at 49 per cent and operational efficiencies at 47 per cent.

As the economy slowly noses out of the double- or triple-dip recession, depending who you ask, it makes sense that organisations are now looking to their IT leaders for assistance with their transformation and organisational change, rather than asking a department that should be adding value to fight a rear-guard action to save money.

Whilst 3-D printing and augmented reality might sound like fun to explore, the thorny issue of staff resources is still close to the CIO's heart. BCS found that only one in 10 felt that their organisation had enough resources to address the management issues and IT trends that their company has prioritised.

More than half want enhanced IT skills among their existing workforce and just under half think they need additional IT staff that are suitably qualified. As might be expected, a sizable proportion (over a third) indicated they would welcome a bigger budget.

Digital leaders need to make sure there team skills are relevant not only to the business but to the time. Skills around big data, agile development, mobile security, bring-your-own-device, professional standards and adept use of social media to address corporate goals are vital in the current landscape.

Throwing money at tin?

The need for IT and business goals to be aligned is a message that is being heeded. But one concern that the more technically minded leaders have is a lack of basic computing engineering knowledge at the board level, leading to simplistic views. Some evidently think that merely buying new infrastructure will solve problems – throwing money at the tin, the hardware.

In fact that approach can often just erode profit and undermine project business cases.

One issue is the pace of change and how best utilise it. CIO's need to understand the impact of digital multi-channel trading and marketing and what to do about it.

CIO's find it tough to get beyond the now into a continuous improvement cycle and keep up to date with current and emerging technologies. One of the issues here is a knowledge gap about differences between platforms and how best to exploit them and the problems associated with the breadth of knowledge of technologies that need to be investigated.

This is a two-way street: IT really needs to understand the business to effectively translate business problems into an IT-based solution.

Legacy is still an issue – from both directions. Some professionals have out of date skills - perhaps trained in areas perceived to be dying (but still widely used) like Oracle, Microsoft – but out of their depth with open source and open standards-based modular systems. At the same time some of these skills are clearly needed when addressing legacy maintainability and obsolescence.

The near future

Is the trend toward compact smart devices and away from PCs a glimpse into an easier future? As devices such as tablets start to role out, the need for traditional IT skills will continue to drop.

Drawing together the increased awareness of IT's strategic role in the business and the move to tablet-driven workforces means that potentially there will be an even larger role for the development and design of visually compelling business intelligence applications.

There could be a need for a different kind of hybrid worker able to support legacy apps but also with the ability to author code for integration and work on new apps.

In information security areas such as operational support, data integrity, usable security for mobile users, effective identity management, cybercrime and hacking will all be issues to be addressed.

Perhaps one key question could set the agenda for digital leaders: 'How can I make a business case for change in a tough economic cycle?'

Author information

Brian Runciman MBCS is Head of Editorial and Web Services at the BCS, The Chartered Institute for IT

Network security – sticking to the core principles

Security practitioner **Alan Phillips** MBCS advises testing as the answer to network security problems

ANXIOUS IT MANAGERS ARE OFTEN uncertain that their servers are up-to-date with security and safe from successful network-based attacks. They could worry a lot less by doing what a software team does to ensure that what they have coded works properly – by testing it.

Specialist companies and government departments have expertise in performing network security audits, generally called penetration tests.

With time and experience in conducting such tests, in which the tester carries out the same actions as a hacker would (and then produces a report), a profile of the typical organization can be formed.

Findings on network security failings are surprising as it is often the basics of security that are overlooked. Here are some of the principles and specifics that crop up a lot, based on where organizations commonly fail (in no particular order):

Harden machines

Although security hardening problems are less widespread than they once were due to changes made by operating system providers, it is important that computers only run the programs that they need to. Irrelevant services left available on a machine will be tested for security vulnerabilities by hackers.

Web servers can support common gateway interface (CGI) programs to provide interactivity in web pages such as data collection and verification.

Many web servers come with 'sample' CGI programs installed by default. Sadly many CGI programmers fail to consider ways in which their programs may be misused to execute malicious commands.

These vulnerable CGI programs present a particularly attractive target as they are relatively easy to find, and they operate with the privileges and power of the web server software itself. Exploitation

of CGI programs can lead to credit card information theft, web page defacement and much more.

Removal of sample programs is therefore another way to help to security harden a machine.

Maintain firewalls properly

Hardware and software firewalls create a protective barrier between networks (such as a company internal network and the internet).

They prevent access by unauthorized users. Poorly configured firewalls are common among small businesses and this often leads to security breaches.

Merely possessing a firewall does not mean that it is properly installed, configured and up-to-date but when used properly these bastions can be extremely effective control points for network traffic.

Use access authentication controls

Access authentication software checks the identity of users who attempt to enter the computer network.

The goal is that access is granted only to parts of the network or server that have been nominated, thus ensuring that users only have access to the files and data to which they are permitted.

When improperly configured, some services that allow file sharing over networks may also expose system files or in some circumstances give full file system access to anyone connected to the network.

Many system administrators use such services to make their file systems readable and writeable in an effort to improve the convenience of data access.

Establish strong network passwords

Users will be prompted to input confidential network passwords when they attempt to access network resources. In an ideal world employees should create passwords that are not easily guessed.

Requiring employees to change their passwords frequently is also important. Some systems come with 'demo' or 'guest' accounts with no passwords (yes, it's very common) or with widely-known default passwords.

Use encryption

Network encryption prevents those who do not hold an encryption key from accessing data stored on a network. All data sent between two or more parties on the network is encoded, meaning that only the intended parties have access to such data.

Often internal penetration testing assignments reveal clear text communications that can be eavesdropped and unencrypted sensitive data which is easily viewable. Where it is required encryption can be a valuable tool for enhancing security.

Patch machines

Making sure operating systems and applications are patched with the latest service packs and hotfixes is such an important undertaking.

It is stating the obvious but it should not be forgotten that keeping systems patched will close vulnerabilities that can be exploited by hackers.

Systems administrators are often busy with user requests and it can be easy for them to become complacent about the mundane task of keeping operating system, software and anti-virus up-to-date.

Conclusion

An interesting question is: Who monitors the systems administrators to ensure that they are keeping the organization safe?

Usually the answer is 'nobody', showing the importance of impartial, third party penetration testing, which often shows that some basic principles have been overlooked.

Many of today's system administrators are able to perform such testing on their own networks (in addition to the independent tests) after receiving appropriate training in this area.

Securing the virtual enterprise

Leon Ward, Field Product Manager, Sourcefire reports

CIOS CONSISTENTLY RANK virtualization and cloud computing among their top strategic IT initiatives. In fact, earlier this year a study by IDC found that virtualisation is the number one priority for CIOs in 2012 with cloud computing second. However, security is still seen as a big issue when it comes to virtualisation and using the cloud.

Another study, by Vanson Bourne, concluded that large enterprises in the UK are leading the way when it comes to adopting server virtualisation, compared to its European counterparts.

It found that the UK topped the leader board with 95 per cent of organisations having either partly of fully virtualised their servers - eight per cent higher than the average. Germany was next in line with 90 per cent, followed by the US at 87 per cent, but only 78 per cent of large enterprises in France had begun using the technology.

CIOs have begun to realise the benefits of virtualisation from data centre deployments – reduced

operating costs, energy savings and increased flexibility. But as they look to expand their virtualisation strategies to the desktop to drive further value, security concerns compound – and these concerns are the main inhibitor to the adoption of these technologies.

Blind spots, virtual machine (VM) sprawl, lack of separation of duties, new advanced threats and the dynamic nature of virtual deployments all contribute to their security concerns. In order to reap the substantial benefits virtualisation promises, CIOs must be able to move forward with confidence.

So what's keeping security professionals from being able to secure the enterprise against threats to their virtual environments, just as they protect their physical assets? The challenge is a lack of visibility into and control over virtualised infrastructure to defend it effectively.

In essence, they haven't established Information Superiority over attackers. This becomes particularly challenging as organisations expand their virtualised systems from the data centre to the desktop.

To achieve information superiority in their virtual environments, security professionals must be able to enforce security policies across both physical and virtual environments. They also must be able to establish visibility and control to detect and stop threats targeting virtual infrastructure and the impact of these threats to applications and users.

When considering technologies to help secure the virtual environment, security professionals should look for the following attributes:

- **Comprehensive -** connecting physical and virtual security elements together. Corporate security and risk management policies as well as compliance mandates demand consistent protection across physical and virtual environments.

> Information superiority lets CIOs pursue their virtualisation strategies to maximise business flexibility, agility and cost savings

The ability to monitor, manage and report on security activities across the entire infrastructure from a central console is a critical step in enabling Information Superiority for the virtual enterprise.

- **Integrated –** combining network and application awareness with big data analytics. Threats today are increasingly sophisticated and no aspect of the environment is safe. Integrating total network visibility – including hosts and other devices, applications, services and users– with big data analytics for increased security intelligence helps eliminate the blind spots in security controls that only monitor physical systems for malicious activity.
- **Intelligent –** delivering the right information needed to structure defenses. In today's resource-constrained IT security departments working smarter, not harder, has become a mantra. The ability for technologies to automatically assess new threats to determine which are relevant and business-impacting helps to focus response efforts and adapt defences to quickly address changing conditions.
- Continuous – responding completely and systematically across deployed security infrastructure.
  The hyper-dynamic nature of virtualised environments exacerbates the need for continuous protection. Real-time visibility from the data centre to the desktop, automating network security functions and management, and the ability to continuously detect and stop the latest attacks and control the inevitable outbreak are just a few examples of the capabilities needed to help maintain effective protection on an ongoing basis.

Without information superiority, implementing effective IT security is much more difficult because of all there is to know about rapidly changing modern physical and virtual network environments.

Information superiority lets CIOs pursue their virtualisation strategies to maximise business flexibility, agility and cost savings without losing visibility and control over data integrity, security and business continuity.

Technologies that support a holistic approach to IT security, providing the same level of visibility and control from the data centre to the desktop and across physical and virtual systems, enable organisations to achieve Information Superiority and realise the full benefits of virtualisation.

To encrypt, or not to encrypt: that is the question...

Charlotte Walker-Osborn, technology partner, and **Aonghus Martin**, technology solicitor, from Eversheds LLP, discuss the English legal position in relation to encryption

MORE THAN 8,500 LAPTOPS ARE LEFT IN UK AIRPORTS and over 10,000 are left in London taxis every year. Human error and the increasing adoption of portable technology inevitably means these figures are unlikely to decrease. The Information Commissioner's Office (ICO) is starting to get tough, giving clear messages that data controllers (in this context employers) must encrypt certain personal data.

It had previously been a question for consideration as to whether, under the 7th Principle of the Data Protection Act 1998, which requires data controllers to take 'appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data' meant that encryption technology should be used.

There was little guidance expressly addressing this point. However, there have been a number of high profile companies who have received enforcement notices which specifically detail a failure to encrypt as being a breach of the DPA and DP principles.

Data protection law is therefore, largely by way of enforcement notices and guidance (issued on security and encryption both in 2007 and 2008), beginning to impose certain specific obligations and recommendations on companies, in relation to encryption.

Although these are not definitively stated, it seems pretty clear that where personal data (data which can identify a living individual which can include name, HR records etc.) is placed on mobile devices, encryption must now be used.

Otherwise, there is currently no strict legal obligation to encrypt personal data, although it may be helpful in some cases to do so voluntarily, for example where such data has to be emailed to a higher risk country or is particularly sensitive or potentially valuable or damaging. There is no specific legislation imposing obligations to encrypt confidential information not containing personal data in the UK.

However, you should consider using encryption in relation to relevant technology to protect important business information. This is likely to include certain HR information (which also gets squarely caught by the DPA), plus board information, certain financial information such as pricing, confidential information on customers and other important confidential information.

So, outside of mobile devices, you should be making judgements around the types of data that should be encrypted as well as keeping an eye on ICO and other security guidelines on this area.

With newly granted powers given to the Information Commissioner now is a good time to undertake a review of the security applied to personal data being processed within your organisation and how this is treated in your contracts, for example with service providers, including your encryption obligations.

This will assist in guarding against a security breach and the resultant adverse publicity, reputational damage and loss of customer confidence which flows from such incidents.

In addition, buoyed by a plethora of recent data loss incidents and new powers recently introduced, such as the ability to levy fines for serious breaches, it is clear that the Information Commissioner will be looking to flex his new found muscles.

How to choose an encryption solution

Encryption is something all companies should use. **Frank Schlottke** from Applied Security looks at different approaches to data encryption and discusses the pros and cons that must be examined to ensure a best fit solution

WITH STORIES OF DATA GOING MISSING ALMOST DAILY, it's difficult to understand why more of it is not encrypted. After all, the most effective countermeasure against the theft or loss of critical or sensitive data is to encrypt it. If it gets into the wrong hands, it remains worthless unless the keys can be compromised to decipher the information.

One of the problems may be that there is a multitude of software solutions on the market that claim to offer the answer and it is difficult to select the one that will best fit your needs. And get it wrong and your data could be lost forever.

Different methods for different requirements

Before choosing any encryption solution, it is essential to clarify exactly what the encryption is needed for to specify and classify the data that needs to be protected. If the aim is to secure correspondence with the outside world and data on the move for example, the ideal solution may be a virtual private network (VPN) or email encryption.

While it is easy to think that encryption is encryption is encryption, there are big differences in the solutions available on the market; and of course the most suitable method will depend on your requirements.

One of the biggest concerns about encryption is that it presents a barrier to day-to-day workflow and is complex to use and manage. So, a critical factor for enterprise systems is the ability to encrypt data automatically and seamlessly, without user interaction.

Hard drive encryption

Probably the most common solution is hard drive encryption, which is mainly used on notebooks and other portable devices. These encryption solutions encrypt the entire hard drive or at least one partition of it sector by sector.

Only by entering the correct password, which in many cases needs to be provided before booting

(called pre-boot authentication or PBA), can the computer be started and data accessed as usual.

Even removing the hard drive or booting from CD won't work unless the correct password is known. Hard drive encryption solutions help in cases where a computer is stolen or lost. And since the entire hard drive is encrypted, users don't have to think about where to store data to ensure it is protected.

Unfortunately it does also have disadvantages that make it unsuitable for every encryption application. The biggest and perhaps the most crucial disadvantage is that hard drive encryption only has two states: all data locked or all data readable.

As soon as the user is logged on using the correct password, all data can be accessed – and this includes other users connecting to the computer via the network. This renders hard drive encryption solutions totally unsuitable for protecting running workstations or servers on a company network. And notebooks are not always operated offline so may provide a back door to sensitive data.

A hard drive encryption solution does not allow for the definition of different work spaces with distributed access rights to encrypted data for individuals, workgroups or departments, for example. It is also important to note that a hard drive encryption solution encrypts non-sensitive data and as every program start requires some decryption, this causes unnecessary system load and delays.

Container encryption

An encrypted container is a virtual drive that automatically encrypts all of the data stored in it. Only the owner of the proper key is able to open the container and decrypt the data.

For the authorised user, the virtual drive looks just like a partitioned drive. Technically speaking, a container is just a file encrypted for one individual user, so that data remains locked away and protected from anyone else; even when accessing the physical drive via the network.

One disadvantage of a container encryption solution is that users have to be careful when storing their sensitive information because it is only protected within the container. A more crucial disadvantage is that containers generally do not allow shared access for workgroups and provide no central administration, making them suitable mainly for single PCs.

File and folder encryption

As the name implies, solutions of this kind encrypt files in pre-defined folders. These solutions make use of the existing folder structure on file servers or local hard drives, so that the network administration does not have to be interfered with. Also, standard processes such as automated backups are not affected. The only difference is that the files written to backup are encrypted.

File and folder encryption solutions available on the market provide similar features like multiple user and workgroup support or central administration. Their differences lie mainly in manageability.

Potential buyers must be sure to check whether the many features promised on product data sheets actually match their requirements or whether they are just gimmicks that merely complicate administration without providing any real benefit. Less is often more.

File and folder encryption is the only one among the encryption solutions discussed here that provides protection for the network as well as for local hard drives. However, like container encryption, the user must be careful to store data in the correct place.

Security doesn't have to be complicated

Many providers of encryption solutions push their products on the basis of crypto algorithms, complex password rules and highly granular configuration options.

In the end, this can lead to a product that can't be used without costly training and consulting services. Also, some of the more complicated solutions have high requirements regarding the system environment required to operate the software or need an existing fully rolled-out Public Key Infrastructure, for example.

These issues must be clarified prior to the purchase. And other key aspects influencing the choice of a solution should be:

- Impact on the existing workflow of users;
- Options for central administration;
- Support for workgroups;
- Easy and clearly laid-out configuration;
- Separation of power between system administrator and security officer;
- Emergency recovery in case of a key loss.

When making a decision on which product best meets your requirements, it is important not to be taken in and influenced by technical gimmicks. What really matters is the product's suitability for daily use.

It is not just a commodity or cost factor but also a very important aspect of security. And nothing is more insecure than a security solution that is poorly configured and makes companies think they are covered, while in fact it is not delivering that vital protection.

With 24/7 coverage, Deloitte's Cyber Intelligence Centre monitors and responds to the cyber threats which are most relevant to your business, your customers and your stakeholders. We go beyond technical feeds. We frame the threats around your organisation and priorities, enabling you to swiftly and effectively mitigate risk and strengthen your cyber resilience.

Find out more at
www.cyberintelligencecentre.com

Deloitte.

The cyber threat landscape has evolved dramatically in recent years; channels of attack are changing, techniques are evolving, and large scale attacks are becoming more prevalent.

Last year, we saw huge losses of data from US retail company Target Corp[i] and E-Bay[ii] while the Heartbleed bug stirred global panic. Such high profile incidents often prompt knee-jerk reactions from organisations to implement costly cyber security solutions.

CIOs now have access to tools, techniques and advice to enable them to help transform their organisation's culture. The introduction the Cyber Essentials Scheme[iii], developments in EU Cyber Security Law, and industry sector cyber exercises will provide the framework necessary to address the increasing scale of security risk while imposing a set of rules around information and cyber security capabilities.

Cyber Risk Awareness

The Cyber Governance Health Check Tracker, conducted in 2013,[iv] provides insight into the attitudes of FTSE 350 Boards toward cyber risk and can provide CIOs with valuable insights into their executives' views. The report concluded that despite 56% of companies including cyber in their strategic risk registers, 40% of admitted that their board does not receive regular cyber threat intelligence updates and 59% stated that their board had only a basic understanding of what their information and data assets were.

CIOs need to raise internal awareness of the security threats specific to their organisations. Securing this information is crucial to protect organisations, as it is a core asset to business continuity and revenue generation. Considering cyber risk at the CIO level can aid overall risk reduction as top-level 'buy in' undoubtedly leads to the necessary investment needed to keep up with the ever changing security landscape.

Governance, regulations and security testing

The UK Government recognises that some organisations may struggle to become secure and have designed the Cyber Essentials Scheme to assist in this process. The Scheme launched on June 5th, 2014 and outlines basic controls for cyber protection.

Businesses will be able to request a certification of their level of security based on several tiers of independent assessments. The scheme builds on the '10 Steps to Cyber Security'[v] launched in 2012 by the Department for Business Innovation and Skills, which stated that 'basic information risk management can prevent up to 80% of the cyber-attacks seen today'.

To mature their cyber risk approach CIOs must gradually shift from being reliant on lessons learnt from high profile cyber risk incidents, to complying with new industry standards and regulations.

The Network and Information Security (NIS) Directive,[vi] is a recent positive example of collaborative regulation. Given the inter-connectivity of EU information systems, cyber threats cannot easily be contained to one country. The directive is designed to ensure that cyber security standards are prioritised across high-risk sectors (Energy; Health; Transport; Finance; Information society enablers, and Public Administration). It is believed that implementing the directive can reduce the costs of security incidents and prevent crimes facilitated by stolen or misused information. In the UK, sectors identified by the directive already spend an estimated £1.98 billion[vii] per year on security.

Financial regulators are already taking a hands-on approach to cyber security and risk management as they try to protect the stability of the markets. They issued detailed self-assessment questionnaires and appear to be moving towards requiring active cyber stress tests to confirm financial institutions' ability to detect, protect from, and respond to attempted cyber attacks. With the recent introduction of the UK Cyber Emergency Response Team (CERT) and proposed changes to EU regulation spanning several sectors, this type of approach is likely to be adopted more broadly by other industries and their regulators and CIOs should ready their organisation for these changes.

Act now, don't pay later

As a priority, CIOs should ensure their current cyber defences, risk strategies and general awareness is reviewed at boardroom level and implemented across the enterprise. They should also create an industry benchmark to evaluate their standing against their competitors, to understand the cyber threats relevant to their organisation and to prioritise their defences.

Given the huge risk cyber threats pose to organisations' ability to conduct business, reputation and customers, it is extremely important to affirm the governance for cyber risk. CIOs should rise to the occasion and take the lead in building their organisation's responses to the continued increase in cyber threats. Taking the necessary steps to protect information and data assets now rather than when governance structures become mandatory will put organisations in a better position to face cyber criminals.

Invest now; don't pay the price later.

James Nunn-Price, Partner
Luke O'Brien, Analyst

www.cyberintelligencecentre.com

i Hovav and Gray (2014) "The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis", Communications of the Association for Information Systems, Volume 34: Article 50ii
ii Harrison and Barinka (2014) "EBay Asks Users to Change Passwords After Cyber-Attack", Bloomberg, http://www.bloomberg.com/news/2014-05-21/ebay-asks-users-to-change-their-passwords-after-cyber-attack.html
iii HM Government (2014) "Cyber Essentials Scheme", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/301383/BIS-14-696_Cyber_Essentials_Requirements_scheme_basic_technical_protection_from_cyber_attacksV2.pdf
iv HM Government (2013) "FTSE 350 Cyber Governance Health Check, Tracker Report", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268643/bis-13-1293-ftse-350-cyber-governance-health-check-tracker-report.pdf
v HM Government (2012) "10 Steps to Cyber Security, Executive Companion", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf
vi HM Government (2013) "Network and Information Security Directive", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/244978/bis-13-1206-network-and-information-sec\urity-directive-impact-assessment.pdf
vii https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/244978/bis-13-1206-network-and-information-security-directive-impact-assessment.pdf

Deloitte.

Legal compliance within ICT asset disposal

By **Steve Mellings**, Asset Disposal and Information Security Alliance (ADISA)

Whilst technologists focus on cyber as being the front line in data protection and information security, the much maligned process of asset disposal continues to spit assets out of the enterprise with precisely the same data on it that was protected so carefully when in life. As an area of potential vulnerability asset disposal remains a glaring omission on many of the CIO's agendas, after all, it is easy isn't it?

Over the past six years Professor Andrew Blyth at The University of South Wales (formally Glamorgan) has taken part in a global study of data that is still resident on hard drives purchased from auction sites. This study has shown an improvement over time, but in 2013 there were still around 40% of hard drives containing data from the sample. This demonstrates that whilst ICT disposal seems simple, it is still an area of continual underperformance within the information security profession.

Of course, the question will be raised; why should we care? For many the current financial threat of a fine of up to £500,000 imposed by the Information Commissioner's Office, whilst significant, won't cause them sleepless night. Even the potential for brand erosion many not cause too many concerns, after all, the headlines regarding data loss/ breach are daily leading to decreased reader interest.

This position will soon be challenged as the legislators are busy at work creating a compelling data protection theatre in which only the brave or foolish will take their responsibilities lightly. Within this theatre, data sanitisation during the disposal process will be the final undertaking required on each asset to conclude corporate compliance responsibility. Without control over this final stage, all of the expenditure on in-life security could be let down by the most innocent of processes; asset disposal.

THIS EDITORIAL REVIEWS THE PROPOSED HEADLINES in the changing Data Protection Act and helps outline sensible steps which businesses should follow when disposing of ICT assets in order to comply with their own data protection requirements.

If we were to position Windows 98 as a current operating system I think even the most tech-ignorant of users would know that this is a dinosaur within the OS world, and yet, UK data protection law is still governed by The Data Protection Act 1998. Since this law was passed the Internet, social media, mobile working, cloud computing and a general attitude of decreasing our privacy and increasing our availability, has swept through not only the business world, but our very culture. In the face of this the law, which is meant to help protect the privacy of the individual, has clearly been left behind and after acknowledging this, the EU commission are currently re-writing the legislation from the ground up.

At this point in time, April 2014, there are thousands of amendments still to be discussed and some crucial elements to be agreed. However, there are some key elements which have been consistent throughout the development and so would appear to be retaining their place within this legislation, which will be passed into EU law later this year and enshrined into UK law by 2016.

Increased penalties

The current maximum fine of £500,000 is being eclipsed by the proposed fines of up to €100million or between two and five percent of global turnover for data breach. These figures are still to be confirmed and clearly each incident will be judged on its own unique circumstances, but there is no doubt however, that the regulators are now able to bring into play a much bigger financial incentive/stick than previously.

Mandatory breach notification

Currently, outside of the telecommunication sector, it is not mandatory to notify the data regulator of any actual breach. In a company governed by shareholders where brand is key I may feel significantly less inclined to disclose a breach to the ICO, unless the number of records was so significant or it was sure to make the press. However, this is changing, within the new act there is provision for obligatory breach notification to occur. The mechanics of this remain unclear and the crucial question of "what constitutes a breach" is also unclear, but this is further evidence of the hardening of the position of the regulators.

Legal liability for data processors

Companies who are classed as data processors (such as those who collect ICT assets for data sanitisation) at present have no legal liability should they fail to do what they say they are doing. In other words, currently the data controller owns all of the risk. Within the new regulation the data processor *will have legal liability* alongside the controller. Largely to address cloud computing, this subtle but important change will see those companies who offer data processing services step out of the shadows and into the firing line. Therefore in order to have your partners share in the liability a formal professional relationship will be required.

Changing attitudes to technology

There are a whole host of ICT initiatives that could impact significantly on ICT disposal. Bring your own device (BYOD) and cloud bring with them a whole range of in-life security issues, but also include the issue of data sanitisation at end of life or in mid-life disposal. Suddenly some of the business benefits of these solutions appear all the more costly in terms of increased risk. Data replication, solid state storage on tablets and uncontrolled downstream processing media will lead to non-compliance unless managed appropriately.

Data Protection Officer

For businesses of a certain size – records relating to 250 or 400 data subjects has been quoted as the entry point – they will be required to have a designated role; Data Protection Officer. This role will have express responsibility for the company's overall data protection activities and at the time of going to press, the job specification will have elements mandated by law including a guaranteed time in position making this perhaps the safest, but least desired role in many organisations!

So with the strengthening of legislation what can businesses do to help them show compliance with the law when disposing of ICT assets?

For many companies compliance with the law, with industry regulations or even with their internal policies can sometimes be an opt-in and opt-out approach. The pressure of business ensures that focus is given to those areas where operations directly impact the business itself. However, it is clear that with the somewhat onerous changes to the Data Protection Act, this law is acquiring far sharper teeth, which is lifting data protection to the top of many corporate agendas and ignorance or trust will no longer be a viable or defendable position.

For those who have data protection, information security, or even brand protection within their remit, all areas where their own company could be compromised needs to be reviewed, a risk assessment undertaken and remedial action enacted. We can see that where data stored on technology is concerned then the process of ICT asset disposal MUST be included, as this is clearly the final part of the overall battlefield of information security/data protection.

In order to comply with existing legislation and to future proof against changing legislation, the following (in my opinion) would be deemed as "Appropriate Technical and Organisations Measures" which are the key requirements under the current Seventh Principle of the UK Data Protection Act 1998.

A company should have:

- A policy, which controls the release all of these media types within all business activities.
- An approved means of media sanitisation, encompassing all media types.
- Internal procedures which ensures consistent approach to this activity across all product sets, departments and locations and which shows adherence to the overarching policy.

- Full asset management throughout the process and verification at each point.
- Third party contracts clearly defining the operator as the data processor and controlling any downstream processing including a strong e-waste strategy.
- Detailed and measurable specification for service delivery.
- Evidence of professional competence of the supply chain.
- Management and reporting on the process with incident reviews, to take place as matter of course.

Of course, the pressure on business IT teams is enormous. These teams are expected to deal with a wider range of technologies than ever before, in environments which are often out of their control and so it is easy to see why asset disposal often finds itself relegated to the bottom of the to-do list. To help take some of pressure away, data controllers can manage their risk by using a certified company safe in the knowledge that independent auditing is being carried out to confirm competence.

So when you are reviewing your data protection strategy if your team doesn't include prescriptive and detailed control over data sanitisation within ICT disposal then ask yourself, why do we bother locking the data centre door at night? What harm could possibly happen?

Further information

Founded in 2010 by John Sutton (Former policy developer at CESG) and Steve Mellings (Author of National Computer Centre's guidelines on ICT disposal and lead contributor to the UK ICO's guidance notes on ICT Disposal), ADISA are the custodians of the ADISA IT Asset Disposal Certification Scheme. Already firmly embedded in the UK market, this programme has gained international recognition with certified members in 9 European countries. With companies in North America, South Africa, India, UAE, and Asia Pacific all working towards certification, businesses should look for ADISA certified IT asset disposal companies wherever they may be in the world.

What's keeping you awake at night?

Certification to key information security standards will help CIOs sleep more soundly, **BSI** explains

CIOS COULD BE FORGIVEN FOR FEELING ANXIOUS AND bewildered. Barely a day goes by without the publication of another report on the increasing scale and complexity of information security (IS) risks, or the emergence of yet another fiendish cyber threat. Not to mention the need to comply with an ever-rising tide of regulation in this area.

Is the 'noise' around IS simply scaremongering? Or is it all too late, with the Internet no longer fit for purpose, and 'cybergeddon' all but inevitable? The truth almost certainly lies somewhere in between. The threats are very real, but it is also possible to 'calm down and carry on' – to make sense of IS risks and to put in place robust measures to manage and mitigate them. There are tools to help, including respected international management standards in IS and business continuity, that many companies are already using to great effect.

Threats loom large

One of the gloomiest IS analyses comes from the World Economic Forum's (WEF) *Global Risks 2014* report, which describes the potential for various global technological risks to combine, causing 'digital disintegration' due to the world's reliance on the Internet despite its vulnerabilities. The report highlights the risks of increasing hyperconnectivity, focusing on the potential damage caused by threats that go 'viral', both in a social media and malware pandemic sense. "The underlying dynamic of the online world has always been that it is easier to attack than defend," it says. "The world may be only one disruptive technology away from attackers gaining a runaway advantage, meaning the Internet would cease to be a trusted medium for communication or commerce."

If the WEF report sounds alarmist, there is only limited solace to be found elsewhere. According to the Information Security Breaches Survey 2014, commissioned by the Department for Business, Innovation and Skills (BIS) and carried out by PwC, the number of IS breaches affecting UK businesses has actually decreased slightly over the last year – but the scale and cost of individual breaches has almost doubled. The survey reveals that 81% of large organisations suffered a security breach in the last year, down from 86% in 2013. But the cost of breaches has shot up for the third consecutive year, with serious breaches typically costing between £600,000 and £1.15m.

Andrew Miller, cyber security director at PwC, observes that the number of breaches remains high, and they are becoming more sophisticated and their impact more damaging. "Given the dynamic nature of the risk, boards need to be reviewing threats and vulnerabilities on a regular basis," says Miller. He adds that while investment in IS has increased in the last year, businesses must make sure that the way they are spending their money in the control of cyber threats is effective. "Organisations also need to develop the skills and capability to understand how the risk could affect them and what strategic response is required."

GCHQ has piled on the agony, with its director, Sir Iain Lobban, recently revealing that cyber attacks described in the media are just a snapshot of what is going on. "On average, 33,000 malicious emails a month are blocked at the gateway to the Government Secure Intranet," he said. "They contain sophisticated malware, often sent by highly capable cyber criminals or by state-sponsored groups. And a far greater number of e-mails, comprising less sophisticated malicious e-mails and spam, is blocked each month."

It is not just an issue for the defence and security sectors. GCHQ is aware of theft of intellectual property on a massive scale, compromises of commercial data and disruption of key networks. The cyber threat applies to all, regardless of size or location. "Basic information risk management can stop up to 80% of the cyber attacks seen today, but experience suggests that few organisations get it right," says Sir Iain.

Help is at hand

The better news is that help and advice in countering IS threats is now widely available. GCHQ, for example, has identified 10 key steps organisations should consider to protect their most important information, data and IP. Controls range from establishing the right governance framework at board level, through technical measures on secure configuration, network security, malware prevention and mobile working, to 'people' issues such as user privileges, education and awareness.

For small firms, the current 'Cyber Street' campaign from the Home Office not only highlights the risks to watch out for, but also provides guidance on what to do in the event of a cyber attack. The government has also launched Cyber Essentials, a scheme enabling organisations to implement simple recommendations in order to apply for the Cyber Essentials Standard, showing potential customers that they have achieved a basic level of cyber security.

The international information security management system (ISMS) standard ISO/IEC 27001 is already well established. In fact, ISO/IEC 27001 is among a number of respected standards – including ISO 22301 in business continuity management – that have long helped businesses manage and protect valuable information assets, giving confidence to stakeholders.

Dr Mike Nash information security specialist and BSI committee member says ISO/IEC 27001 is the only certifiable

international standard to define the requirements for an ISMS. "It adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS," says Nash. "It can be used with ISO 22301 to establish 'information continuity' and greater organisational resilience if the confidentiality, integrity or availability of your information is compromised."

Nash adds, "Both standards are applicable to businesses of any size or sector and essentially they're technology agnostic. Good information governance should stretch from the boardroom to the switchboard."

Lisa Dargan, business development director at Ultima Risk Management, a consultancy and training organisation specialising in business resilience, agrees. "My concern is that people will buy technology solutions thinking they're a 'silver bullet'. Technology has a role to play, but it won't fix the problem on its own," she says. "It's just as important to educate your people."

Dargan continues, "ISO/IEC 27001 is a fantastic framework because it looks at IS in the broadest sense, starting with the question, 'what information are you trying to protect and why?' and recognising that a large part of the security solution lies in employee training and awareness." She says the standard addresses key issues, such as what to do if your data has been breached, and who is authorised to communicate what information, to whom and when.

BIS's Information Security Breaches Survey 2014 reinforces the point. It found 70% of companies that have a poor understanding of security policy experienced staff related breaches, compared with only 41% in companies where security is well understood.

Be prepared

But the experts agree that cyber risks will, at times, become reality. As in the physical world, even with the doors locked and alarms fitted, break-ins will still occur. "Sooner or later you will have a breach," stresses Alan Cook, director of management consultancy Agenci Information Security. "Businesses don't realise it can come from anywhere – from their 'soup' of systems, from their processes, and especially from their people. If everyone adopted ISO/IEC 27001 there'd be a fantastic improvement in IS across the UK. Then you can build on it depending on what business you're in – with ISO 22301 say, or STAR Certification if you're a cloud service provider."

The coming months will see a raft of international regulations ratchet up the stakes, potentially including the ratification of new harmonised Data Protection Regulation across the EU, introducing some of the world's most comprehensive and heavily enforced data breach notification regimes. Under the proposed measures, businesses must report data breaches as soon as possible, or face draconian penalties of up to 2% of their turnover, imposed by 'one stop shop' regulators within the EU. In addition, organisations with more than 250 employees will be required to appoint a data compliance manager.

"Most businesses have no idea what's coming," says Cook. "But if they adopt ISO/IEC 27001 it will help them to plan ahead, manage IS risks and comply with the new regulations."

Capgemini: Standard practice

Capgemini is a global leader in consulting, technology, outsourcing and local professional services, operating in over 40 countries and 100 languages. It uses ISO/IEC 27001 to increase its resilience, reassure clients and gain a competitive edge.

The group has adopted a comprehensive approach to IS, introducing a range of measures to address the confidentiality, integrity and availability of information it holds. Key security drivers include potential attacks by computer system hackers, but also new 'threats' such as increased government regulation and tougher requirements from the PIN card industry. "If we fail to comply we risk heavy fines and severe damage to our reputation. Security has also become a major concern for clients. Without robust systems in place, we could lose business," says Bill Millar, global chief information security officer within the firm's UK Infrastructure Services division.

"That's why we went down the standards route," continues Millar. "We wanted to prove best practice to ourselves, but we also wanted to demonstrate it to both commercial and government clients who are insisting on it."

Capgemini's Dutch and Indian operations were the first to adopt the information security standard ISO/IEC 27001 and "they were clearly getting benefit from it," says Millar. For example, in putting together bids and tenders, "We were producing reams of paper on each occasion, spending huge amounts of time and money proving our infosec credentials, whereas our overseas colleagues simply provided their ISO/IEC 27001 certificate number."

Millar created a business case and won the approval of his board. "It wasn't difficult. In fact, the board asked 'why aren't we doing this already?'" he says. BSI, the business standards company, was identified as the preferred external auditor. "BSI advised us to reduce our scope and approach the task in 'bite-sized chunks', which made it much more manageable."

First, the company's risk approach was clarified; then it started to communicate with staff and gain buy-in from account leads; next, it brought its security documentation up to date, adding new areas such as mobile security; and finally it began a cycle of security audits, systematically covering the areas initially scoped.

Just 10 months from the start of the project, Capgemini's UK outsourcing business achieved its goal of having an information security management system certified to ISO/IEC 27001. It has since gone on to recertify itself, and will do so again in 2014, this time to ISO/IEC 27001's updated 2013 edition. Future goals include recertifying ISO/IEC 27001 in many other parts of the group.

Millar lists a host of benefits, but above all, he says, "It's not just about looking after data; it's about looking after people and physical security too – it's not just for techies."

A LEFT LAPTOP MEANS LOST DATA. PROTECT YOUR BUSINESS.

Is your customer and sensitive business information safe?

Not protecting sensitive customer and business information can lead to both embarrassing and serious consequences. Kaspersky gives you the tools to simply and easily protect your data. So whatever happens, you can be confident that your customers' information and your business reputation – are safe and secure.

of employees use
PERSONAL SMARTPHONES
FOR BUSINESS TASKS

44%

of employees use smartphones
TO WORK IN COFFEE SHOPS
OR OTHER PUBLIC PLACES

47%

of employees use smartphones
USE SMARTPHONES
WHILST TRAVELLING

Source: Forrsights Workforce Employee Survey, Q4 2012, Forrester Research, Inc

Based on our award winning anti-malware technology, Kaspersky Lab products combine industry leading security and network management tools such as encryption, mobile device management and application control; all through one console, on one platform and at one cost, putting you truly in control.

wickhill.com/kaspersky

Protect your customers. Protect your business.

KASPERSKY lab

WICK HILL

Telephone: 01483 227600
email: info@wickhill.com

WICK HILL

Industry's integral role in educating cyber security talent

By **John Colley**, CISSP,
Managing Director EMEA, (ISC)²

IDEALLY, PEOPLE DEVELOP THE RIGHT INSTINCTS FOR their craft at an early stage in their career. They have the opportunity to pick up the basics during their formal education and build upon them as they gain experience through their work. When it comes to computing, such an ideal can be very difficult to achieve. The pace of change within computing technology is so great that the world of work and the formal education new university graduates are armed with are often leagues apart. Information security is a subject area where this is particularly true with few computing science courses imbedding basic knowledge within their programs.

Earlier this year, the UK government outlined ambitious plans to address this skills gap in recognition of the need for cyber talent as part of its national security strategy. There are some very welcome ideas outlined in their plans including encouraging greater collaboration between industry and the education providers that supply it with new talent. They are making a comprehensive call to action for universities to improve cyber security education and they recognize that such a call is not enough on its own. Industry must play an integral role in this development to ensure the "employment outcomes" that prospective students, who pay significant tuition fees for their course of study, say they are looking for. It's a call industry must answer, for the sake of the bottom line.

The business case goes well beyond the litany of losses and hits to reputational damage and share price that has been the stuff of news headlines for over a decade now. The threats that continue to increase, in number and impact, are driving investment in security and demand for people with skills to deliver it. But as the demand rises, so too does the cost. Since 2004, our research indicates employers have been facing an inflationary spiral in their search for security talent. Even at the height of the economic recession demand for security skills remained robust as companies moved to cost-cutting cloud and mobile device–enabled systems. Only 4 % of our members participating in a 2011 survey to quantify the impact of the recession on their careers reported that they were not employed, and many of these were by choice. The lion's share, 70%, of those with hiring responsibilities were looking to add one or more people with security skills to the team, with 85-90 per cent struggling to find the

"right" people, and taking up to six months to fill positions. Employers then and now demand experience making it very difficult for newcomers to find their way into the field.

Our more recent studies show how this struggle is beginning to bite. The 6th Global Workforce Study Report released last year suggested that the skills gap was becoming acute. Threats are driven by the rapid introduction of new technologies that don't have security "baked in" the product development process, at a time when organised attacks are on the increase. Against this background open information security positions are going unfilled; 56% of those responding to the survey felt their organizations currently have too few information security workers to manage the current load. This understaffing is felt greatest on the existing security workforce — 71% reported feeling strained without enough staff in place and 52% reporting that the shortage is having a direct impact on data breaches – more are happening! Nearly half admitted that the IT security staff shortage is impacting their customers.

Clearly, if security remains a low priority for the educators that produce the computing graduates that are to be the future of the IT industry, we can only expect this situation to worsen. Many suggest that employers need to recognise that they can no longer continue to buy in experience and must invest in training the much needed new talent. I would suggest that we could have a greater impact by supporting the academic community's ability to meet this need. Information security is a relatively new discipline, which makes it difficult for employers to recognise potential in raw talent or understand how much of a training investment is required. In more mature professions such as engineering universities are providing that filter, attracting students with the aptitudes and interest in the discipline, then helping them identify whether the right instincts are present as they make their way through a three or four year programme. Employers can view graduates with a good degree of confidence in the competencies being sought. This is the scenario that we must develop for information security. To achieve it educators are going to need support both in recognising the need as they battle to prioritise changing demands from across the IT spectrum, and in fulfilling it.

For our part, (ISC)² as a professional body that has worked 25 years to foster recognition for the existing profession, we are now opening up our knowledge base, to publish undergraduate and graduate resources, in a Global Academic Program. The objective is share the front-line experience learned, documented and maintained in consultation with our 100,000 certified professional members around the world. This will inform curricula, and support knowledge development within academic staff. Further, many of our over 15,000 members in EMEA are keen to make themselves available to visit universities, host career talks, and guest lecture, while local (ISC)² Chapters of which there are now 33 and growing across the region, welcome student members to support their development and mentor the transition into work.

We are also working to support groups such as the Council of Professors and Heads of Computing (CPHC), an association representing computing in UK Higher Education. Their vice-chair Carsten Maple estimates that a single module, approximately 5% of the total credits in a degree, is dedicated to information security in a three-year Computer Science degree, and agrees that this isn't enough to give computing students the best opportunity to succeed. He also notes that many universities are keen to work with industry to understand what companies are looking for.

When it comes to security, in addition to developing talent, imbedding security knowledge within computing science is also a way of addressing industry's security problem at source. Four years ago, I wrote in CIO about IT's accountabilities in security: identifying that the biggest concern at the time was software. Because it is now connected, security plays a critical role in the requirements analysis, design, management and even decommissioning of software. Today software still remains a top security concern. It's telling to see the little progress that has been made on the OWASP top 10 security concerns for software over the 10 years that it has been published. Security has not yet become the development priority that it needs to be and this has to stem from how the subject is taught and/or learned. With fundamentals imbedded within the core education security can take its place among the development requirements, policy decisions, procurement requirements etc, that are identified for all systems development, not just software.

If industry is to get IT systems that are fit for purpose, we must invest in both the talent we need and in academia's ability to develop it. The Government is creating new incentives within universities to work with business, and there are various ways to get involved. This can include freeing up specialists' time for guest lectures to engaging with organised initiatives or professional bodies such as (ISC)², or reaching out directly to a local institution. While such activity should be considered a long-term investment, the rewards are often immediate as companies become exposed to raw talent in the process. This ideal is well within reach.

Further information

John Colley, CISSP, is Managing Director for EMEA at (ISC)². (ISC)² is the largest membership body of information security professionals, and the administrator of the CISSP®, with nearly 100,000 certified members worldwide. Accredited academic institutions now have access to new resources and support with the launch of the (ISC)² Global Academic Programme. Classroom materials and services for universities can be tailored for both undergraduate and post-graduate programmes. (ISC)² is making its educational resources, which are updated regularly by its members and industry luminaries, available to academia to help meet the global demand for more skilled cybersecurity professionals. The (ISC)² common body of knowledge (CBK®) incorporates disciplines within information security, software security, forensics and healthcare. To learn more: www.isc2.org/global-academic-program

It's time to fight back against the spammers

By **GFI Software**

EMAIL IS A CONSTANT. EMAIL IS everywhere. Email is something few of us could live without. Billions of messages are sent each month, and countless hundreds are received every week, often every day by your end users. And each of these missives could be a vector of attack, a container of malware, or a way to destroy your company's very business.

It would be easy to stop attacks if there was just one way hackers use email to bring your shop to its knees. Unfortunately, email is vulnerable in myriad ways and hackers have nearly unlimited ways to attack. And it gets worse literally every second.

Why is email so vulnerable?

Email can be an insanely easy way for attackers to get into your network, and once they're in, they truly have the keys to the kingdom. Not only can they gain higher level access to the network, especially if they launch an elevation of privilege attack, they now can see all the targeted user's email content, and at the same time can impersonate that user by taking over their identity.

And email is far too vulnerable. Not only are passwords commonly weak, but users are easy prey for social engineering, and controlling a user's address book is a bot's delight.

Don't believe it? How many times have you got bogus emails from friends or colleagues because their address books were hacked? And because they are from people you trust, how easy is it for a security novice to fall for these ploys and, say, click on an infected link?

Meanwhile this entire threat is organised, international, criminal, and ever growing in sophistication.

What harm can hackers do via email?

We sometimes think of certain email attacks as an annoyance. So what if Auntie Betty's Gmail got taken over by a bot and we got a bogus message? Even if you sidestepped the danger of Auntie Betty's bogus email, not everyone did. And those who fell for it probably harmed other users, including those in your own corporate or personal address book.

The evil beauty of these attacks is the user sometimes only knows they were compromised once they get email back from their contacts asking about suspicious mail. And if the email is taken over just to spread spam, the victim only knows if their performance slows to a distinct crawl.

And these attacks may be the least of your worries. There is far more to fear, and battle. Traditional style email viruses are still a massive problem.

This threat was really brought to the fore with a little nasty virus named Melissa back in 1999. Far from sweet,

Melissa used email to bring systems to their knees simply by overloading them. The virus spread by tricking users into opening an attachment hoping to get free pornography by offering up a list of supposed passwords. The attack was finally beaten back after much harm was done, but that didn't mean the virus was done for the good. To the contrary, Melissa proved to hackers what was possible, and those creeps took the Melissa code and propagated new versions.

This is one of the biggest drivers for hack attacks. The bad guys share code, and these days even a programming dunce can relaunch an existing attack with just a few tweaks. These clowns are known as script kiddies, and with a slight bit of knowledge and a penchant for social dysfunction can indeed wreak havoc.

With Melissa, the hacker gloves were off, and email was suddenly prime game.

Attacks broaden and worsen

Hackers love easy pickings and they more so love a target that is ubiquitous. This is why Microsoft® software has long been the biggest target, and email fits the same exact profile of near-total commonality. And the typical email user is regularly confronted by phishing, malicious links, elevation of privilege exploits, and address book attacks.

The rise of email makes it a bigger problem: today users have corporate email, but they likely also have multiple web mail accounts, multiplying the attack vector.

The very use case of email makes it vulnerable. For most all of us, email is the app we still spend the most time with. It is hard to keep up with the volume of legit mail, never mind the spam. So when malicious mail masquerades as legitimate, even seasoned users can fall victim.

Email is the perfect conduit for worms, a form of malware that multiplies and spreads largely through email distribution. And with script kiddies, these worms never die: they are simply tweaked and turned into more dangerous entities.

Take Win32/Brontk, which has been around for years. This is a classic worm with proliferates through mass mailing. In typical fashion, this worm mails itself off with an innocent-looking email attachment, and finds addresses by hijacking end user address books. To make things worse, worms like Win32/Brontk can shut off your defenses such as anti-virus software and even use the hijacked email to launch denial of service (DoS) attacks.

One new clever, near diabolical attack is a variant of the Nigerian scams. In one example, Mrs. Bridggie William from Kenya writes that her husband died after a "Cardiac Arteries Operation," leaving behind over $10 million As Bridggie herself is dying of cancer, she wants the recipient to provide a safe place for all this money. Instead of an email address to respond to, Bridggie was kind enough to include an Outlook meeting invitation. Acknowledging such invites can open you up to serious attacks.

Of course, these meeting requests must be deleted immediately, and not just moved to your junk folder. And just as you ought not to respond to spam, do not decline the invite as this is akin to a response.

Having multiple accounts that employees use at work multiplies the threat. It is best to restrict user to the corporate email system while they are on the corporate network that hopefully is equipped with defense-in-depth protection tools. Unprotected accounts are a major source of data leakage, worms, and other malware.

On the other hand, if users do a lot of web surfing and sharing, it may make sense for you to help support these web email clients. They can use these accounts for non-business purposes, but still need to make sure they are protected since they can ultimately impact the company.

Spam still a problem, maybe more than ever

Spam is often seen as a pure annoyance. Our inboxes are daily flooded with junk, and we are exposed to often offensive messages.

But spam is a main conduit for hack attacks, be it malware or phishing. And spam is more dangerous than ever. The bad guys are not just trying to lure you to buy bogus wares, but want your information, your address book, and to use your connection to elevate their privileges and attack your company's network.

Even worse, with newer attacks, you don't need to open an attachment to be compromised, nor do you need to click a link.

The 2013 Microsoft Security Intelligence Report laid this out with precision. "More than 75 percent of the email messages sent over the Internet are unwanted. Not only does all this unwanted email tax recipients' inboxes and the resources of email providers, but it also creates an environment in which emailed malware attacks and phishing attempts can proliferate. Email providers, social networks, and other online communities have made blocking spam, phishing, and other email threats a top priority," the report said.

There is far more to it than that. Spam wastes productive time as your workers pore over their inboxes and sift through the garbage. And spam is not going away. While not exploding as in years past, spam isn't exactly disappearing either. At the same time, it is getting more dangerous and laden with malware and phishing attacks every day.

It's time to fight back

Your company's network, applications and data are the lifeblood of your business. Compromised a little and you are seriously damaged. Compromised a lot, and you may be down for the count. Protection is of the essence, and this protection must be deep and rich.

Further information

GFI Software develops quality IT solutions for small to mid-sized businesses with generally up to 1,000 users. GFI is a channel-focused company with thousands of partners throughout the world. The company has received numerous awards and industry accolades, and is a longtime Microsoft® Gold ISV Partner.

MITIGATING THE RISK OF DATA LOSS DURING ICT DISPOSAL

Fully Audited International IT Asset Disposal Standard.

Launched into the UK in 2010 and formally recognised by DIPCOG in 2013, the ADISA Certification programme now has certified companies throughout Europe and in the United States. With companies being certified in Australia, China, Singapore and Dubai during 2014, the ADISA Standard offers end users confidence that their IT Asset Disposal Company operates to the very highest of standards.

The audit process is rigorous to ensure certified members meet the Standard consistently. This process includes full independent audits against each element of the Standard and twice yearly unannounced forensic audits.

Don't worry about your assets when they reach end of life, use an ADISA certified company and have confidence that your assets, data and reputation are being managed by a professional partner.

Find a partner for your ICT Disposal requirements at

WWW.ADISA.ORG.UK

To learn more about ADISA go to **www.adisa.org.uk**
e-mail **info@adisa.org.uk** or call us on **0845 557 7726**

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Beating bribery – the battle begins in the boardroom

By Suzanne Fribbins, BSI Risk Specialist

Bribery is a major issue for businesses, putting them at risk of criminal prosecution, unbudgeted costs and reputational damage. According to recent research bribery and corruption in the UK is rising with 5% of UK respondents reporting paying a bribe in the last year.

Bribes can take many forms, from cash exchanged in "brown envelopes", to facilitation payments, inflated commissions, excessive hospitality or holidays disguised as business trips.

Amid rising international concerns and more effective reporting of bribery and corruption, the UK responded with the introduction of the UK Bribery Act 2010. Strengthening previous legislation, it has made it easier to prosecute offenders and introduced a new area of corporate liability.

The Act introduces a Section 7 offence of an organization failing to prevent those associated with it committing bribery. An individual breaching the legislation may face up to 10 years imprisonment; fines are unlimited for both individuals and companies. The only defence against a Section 7 offence is if the organization can prove it had "adequate procedures" in place to prevent bribery.

Businesses across the spectrum need a working anti-bribery management system, such as BS 10500, to hardwire the mitigation of bribery risk into their processes and culture. The effective implementation of policies, procedures and controls will help ensure an organization's compliance with the law and provide a tight anti-bribery compliance regime. Measures include assessing bribery risks; assigning responsibilities; embedding the procedures organization-wide, through employee training and communication; whistleblowing, disciplinary and investigation procedures; and monitoring and auditing for compliance.

If a bribery event takes place thereafter, either by an individual or a person associated with the company, BS 10500 will provide evidence of adequate procedures; a process to investigate and address the incident; and preventative measures to minimize repetition.

For more information, visit:
www.bsigroup.com/anti-bribery

bsi.

Securing mobile estates and workers

By **James Taylor**, product development manager, Wick Hill Group, specialists in secure IP infrastructure solutions

THE FIRST THING TO CONSIDER WHEN LOOKING AT mobile security is 'What is the mobile estate?' The mobile estate is any device or storage which is outside our corporate fortress (either physical or logical). Mobile devices, or more importantly the data on them, raise security issues that necessitate additional security measures.

In recent years, the myriad of mobile devices, as well as cloud storage, needing protection has exploded beyond the traditional laptop to include tablets, smart phones, iCloud, SkyDrive, etc. All of this makes the CIO's job exponentially more difficult.

Who are the mobile users? In the traditional workplace, they were the field personnel and board members. But with disaster recovery considerations, as well as work-from-home policies, they could be the entire workforce.

From a training perspective, we should be including everyone in managing their mobile devices. We need to encourage staff to respect corporate property as if it was their own, and to take personal responsibility for the safe use and storage of equipment. Moreover, we must allow employees a safe reporting procedure if anything is lost, because the faster the IT department is made aware of any loss, the quicker it can react.

Once we understand who is using portable devices, we can consider the data risk. We need to ask where the data is held and what our exposure is, in the case of loss. Management of data is a critical step. When data is held centrally and securely, and is accessed via a Virtual Desktop Infrastructure (VDI), this will always provide a stronger security profile than allowing data to be stored at the edge on mobile devices.

However, in order to recognise the risk, we must have first defined our sensitive corporate documents, by protectively marking our data. Protectively marking data can be kept to three simple levels:

- **Sensitive**
  Employee records, intellectual property, etc.
- **Confidential**
  For business matters, profit and loss statements
- **Not Classified**
  An RRP price book or the canteen menu are examples of documentation that should not be embarrassing if seen by anyone outside the organisation.

Security at the gateway

Mobile devices which are used for company business have to be fit for business purpose and, importantly, they must be capable of either running corporate software or providing a thin client back to HQ. You might also consider limiting the choice of operating system on such devices. The benefits include more manageable vulnerability patching, as well as mobile device management (MDM) software suites which are compatible with industry standards.

Now we can get smart with our security provisioning. If the remote end point is there to provide a remote desktop session, our security can be centred on strongly authenticating the user at the point of entry - the gateway.

Two factor authentication is absolutely essential today for mobile workers. With a VDI session, one assumes the data is securely and centrally held back at HQ. With VDI, there's the added bonus that we don't need the most powerful computer in the world for the mobile worker, because the computer is just providing the screen and keyboard for the remote worker. All the grunt work is being done by the server farm.

Unfortunately, not many of us have adopted a VDI environment. We run around with a fat client, not a thin client, and use the standard operating system that came

with the appliance. With a fat client, all the inherent security problems with mobility are exacerbated.

Because we don't centrally store data, there are a lot of things we need to do in order to ensure security. We need to encrypt drives, control the ports, load anti-virus programs, possibly adopt an MDM solution, and so on.

Working as the CIO, we really need to question whether we require a full client for remote enablement. By running on skinny operating systems, and being configured to only access back to HQ, we gain portability, without all the overheads of managing a fat client.

Smartphones, BYOD or CYOD devices, tablets, etc. complicate our mobile estate further. There's no doubt that the high degree of portability, instant access to e-mail, and so on, that we get with such devices, has really improved efficiency for the remote worker.

However, from an infrastructure, security and support point of view, this situation definitely creates the need for much more vigilance, organisation and stronger security policies.

Whilst corporate e-mail is one concern, the ease with which documentation can be attached "for your review" means we have the potential for multiple, unsecured documents across many platforms. It's more secure to link document back to the central location, than to blindly send to multiple recipients.

Having identified our remote worker, fully trained them, marked our documentation and given them the right mobile devices, we now need to think about our remote access gateway.

Should we enforce end-point security checks and give an appropriate access, dependent on the risk? If you have someone accessing the corporate network from an internet café in an untrusted foreign land, then it's sensible to grant minimal access permission. For someone who is strongly authenticating, on a fully patched corporate device, over an IPSec client, from a trusted geo-location, the risk profile is much lower and we can allow greater access.

Most UTM firewall technologies can easily handle company security needs at the gateway, including mobile SSL traffic. With this scenario, there's the added bonus that any additional security features which we bolt onto the firewall, such as anti-virus, can also be applied to our remote workers' sessions.

The great benefit of running a UTM firewall is that the IT Security team only has to deal with one interface. The protective marking methodology we used to prevent sensitive documents leaking out over email, can also now be applied to our mobile workers' remote sessions.

With regards to personal cloud storage, I propose it is simply not allowed, because it can't be controlled by corporate policy. We can prevent this happening, by leveraging the capability of the firewall, from within the corporate local area network.

Wireless and MDM

Now we come to the question of wireless. With wireless mobile devices being issued to more staff, as well as multiple appliances to single users (I have three), the requirement to secure, monitor and control these devices, as well as reviewing the wireless infrastructure, is much greater. We need to keep wireless connectivity secure and we need to keep up to date with the current changes in wireless technology.

A key driver for the future of wireless is the newly ratified 802.11ac standard. Starting initially at 1Gbps, with future potential up to 7Gbps, this new standard is going to transform the use of wireless in the office and will move many environments from wired to wireless. As many users already have 802.11ac routers at home, there will be a strong demand for the same experience at work. Securing and managing expectations early will be a key element in minimising the security risks that this will create

One way of addressing these issues is to adopt a mobile device management (MDM) solution to secure and manage mobile devices, and that should be able to encompass devices with different operating systems and from different manufacturers. We need to know whether mobile devices belong to the employee or the company and whether sensitive company data is held on those devices.

The sort of features which are going to be necessary from an MDM system include anti-malware for the devices, the ability to remote block or wipe data, and GPS-find. One very desirable function is the encryption and secure containerisation of company critical data and applications, keeping them separate from employee personal data.

Some systems will allow you to manage all 'end points' within your network from one central management console, whether that be a mobile phone, tablet, laptop, workstation, file server or virtual server/desktop. With this option, you can rest assured that you have done everything you can to enforce compliance to your company-wide data security policy.

Conclusion

With strong guidelines, approved devices and reinforced training for mobile workers, companies can take advantage of mobility and become more flexible and more productive. However, mobility has to go hand in hand with proper planning and appropriate security measures, such as MDM systems. If you get it wrong, you have to be prepared for the consequences.

Further information

Kasperksy Security for Mobile is a leading MDM solution that integrates essential mobile endpoint security technologies and efficient mobile device management capabilities, to make it easier to protect mobile devices against viruses, spyware, Trojans, worms, bots and a wide range of other threats.

As soon as a mobile device appears on the network, it becomes visible, so you can deliver security software to it and configure data access restrictions. Security for each device can be configured and controlled from one easy-to-use management console so you can enable mobile access to contacts, calendars, the corporate email system and other business systems.

Twin Design / Shutterstock.com

What do your apps know about you?

By **Harry Sverdlove**, CTO of Bit9

EACH DAY, CONSUMERS DOWNLOAD millions of applications to their smartphones, tablets and other mobile devices. Unbeknownst to them, along with games, news, utilities and other things, they also often download software that could put their privacy at risk.

That problem is compounded when people use their personal mobile devices at work to connect to their employers' network, the same network that carries sensitive company data.

We have analysed a statistically meaningful sample of more than 400,000 Android apps available from Google Play. We chose Android because it is the most widely used smartphone OS and Google Play is the default marketplace for downloading Android apps. We also conducted a survey of select IT decision makers who are responsible for the mobile device usage policy of more than 400,000 employees.

We looked at the permissions, categories, publishers, ratings and popularity to rate the overall trustworthiness of each mobile app. While perhaps not surprising, the results should be a wakeup call to IT professionals about the challenges of today's BYOD culture.

Unlike traditional desktop and server software, the risks in mobile devices come not just from malicious programs; they also involve privacy and control of confidential or sensitive data.

We found that the majority of Android apps (72 per cent) use at least one permission that gives the app access to private data or control over the smartphone's functionality. But it's not just what permissions an app requests that matter, it's whether those permissions make sense for the nature of the application.

For example, it is less suspicious for a social media app to have access to email contacts than it is for a wallpaper app to do the same.

We took into account information about the publisher, the number of high-risk permissions requested, and the category of the application, and grouped our results into three buckets: green (trustworthy), yellow (low trust, but not malicious) and red (no trust and suspicious). We found that 25 per cent, or more than 100,000 apps, fell into the red category.

We're not saying that 100,000 apps on Google Play are 'malicious'. In fact, very few apps are actually evil, and Google does a pretty good job of catching and removing them from Google Play. But these 'red' apps do perform questionable tasks and have access to private information, which represent a risk to enterprises that allow BYOD.

Why do companies deploy security technologies? To stop bad guys from

getting into their network and stealing intellectual property. When a company owns (or controls) all of the computers that manage its data, it can react to changing threats because the company can control what runs on those systems.

Imagine if a company allowed employees to bring their own personal laptops and desktops into work and use them for business with few, if any, restrictions on what other programs those personal systems might be running. It would be a security nightmare.Conceptually, this is not too different from having a BYOD smartphone policy, as 71 per cent of the companies we surveyed do.

Mobile devices are used to access corporate email, documents, contacts and more. And who knows what else they're running? Less than a quarter of the IT decision makers we surveyed have visibility into what else is on these mobile miniature computers.

When a smartphone is used for business, the line between personal data and corporate IP gets blurry in a hurry. Personal and business contacts intertwine and email accounts merge. A social media app that an employee uses to interact with friends might now have access to email addresses and information about company executives or customers.

A game app with advertising banners might now have access to the internal internet addresses or at least the keywords used for business browsing activity.

In fact, most free apps that embed advertising to support their development do not understand or control what information those third-party advertisers may collect (the advertising component automatically inherits the permissions of the app itself).

The risk for IT security departments is not just in losing primary control over data stored on (or transmitted from) a smartphone. Mobile data such as contacts and emails can easily be used to launch more sophisticated spear-phishing or other targeted attacks directly against traditional desktop and laptop systems.

So to put the research in context, we are not saying the sky is falling. We are not saying 25 per cent of all apps are malicious. What we are saying is a large percentage of mobile apps are accessing more information on their devices than people realise, and when those devices are holding both corporate and personal data, this is a problem for individuals and their employers.

What can consumers do to protect themselves and their employers from these risks? Pay better attention to the permissions requested by the mobile apps they download. Don't just automatically check 'Yes' to every permission request from an app.

Be wary if, for example, a wallpaper app asks to use your GPS data. Mobile consumers don't have to become paranoid that every app is a potential threat, but we need to be aware of that possibility and act thoughtfully and responsibly.

Ignoring IT security – is it a risky strategy?

The upsurge in recent large-scale data breaches should be the impetus needed for boardrooms to finally take IT security seriously. So, will yours? **Håkan Saxmo** explains

EDWARD SNOWDEN'S REVELATIONS LAST JUNE SENT shockwaves around the globe. As well as exposing the NSA's widespread surveillance culture, he catapulted data protection into the public eye. As if that wasn't enough, the ensuing months have seen a barrage of high-profile hacks cement the risks of lax IT controls – Target, eBay, and Office are just some of the heads hanging in shame. What these incidents demonstrate is IT security can't be kicked under the carpet as sophisticated cyber defences are vital to prevent breaches becoming the new norm.

Notoriously, IT security has been a 'grubby' word in the boardroom – with the C-suite considering it an overhead, instead of a mission-critical business priority. As a result, rank-and-file workers are left responsible for data protection. However, best practice states security must be 'top-down and holistic' to be effective.

It's obvious that a cultural change has to happen. Data breaches – whether in the form of opportunistic attacks or coordinated military campaigns – are increasingly able to affect a business' bottom line.

Target pays the cost for lax security practices

Unfortunately for Target, it offers the perfect illustration of just how catastrophic the consequences of lax security controls can be. Following its attack (announced during its busiest trading period), the retailer has seen a 46 per cent year-on-year revenue drop, reputational damage, constant bad press, and an expensive C-suite reshuffle – with both CIO Beth Jacob and CEO Gregg Steinhafel forced out. Putting this into figures - revenue was just $520 million, down from $961 million a year previously. Profits fell 34 per cent – from $2.999 billion to $1.971 billion, and that's despite better-than-expected sales in the first half of the quarter!

Beyond income, Gartner analyst – Avivah Litan, estimates that, in order to reimburse the banks having to send out millions of replacement debit and credit cards, pay fines for non-compliance with PCI DSS, cover legal fees and credit monitoring, Target is looking at a bill of around $420 million. And if it rolls out chip and PIN, that's a further $100 million.

Looking more broadly, Ponemon Institute's latest Cost of a Data Breach report suggests that the average cost of a security incident has increased 15 per cent between 2013 and 2014. In US dollars, it passed $3.5 billion, or $145 per lost or stolen record. US businesses paid a higher price for lax IT security than the global average, incurring a bill of around $201 per record.

Scale of data breaches increasing

While the cost is rising, the scale of the problem is increasing too. For example, Target is understood to have lost around 110 million records in its December hack. Mandiant's report

on Unit 61398, the Chinese group alleged to have hacked more than 140 US companies in a 2013, states that in one instance it was able to syphon a total of 6.5 terabytes of data from a single company over a ten-month time frame.

A final pertinent point from the Ponemon Institute study is that many respondents – who were rank-and-file IT workers, not senior executives – thought their departments were desperately underfunded. The average respondent expected an annual IT security budget of $7 million – half of the $14 million they actually thought was necessary for effective defences.

Combating network credential abuse

Mega breaches typically occur because hackers are able to get their hands on other users' network credentials. Though the specifics of the Target incident are sketchy, the retailer has confirmed that intruders stole a vendor's username and password in order to install point-of-sale malware. Similarly, Unit 61398 is alleged to have used spear phishing to acquire network credentials at targeted companies.

With this in mind, here's a question for the C-suite: how much havoc could a hacker wreak with the average employee's username and password? Will the damage be contained, or is there excessive potential for disruption on account of workers having wider network access than they actually need to do their jobs?

The Snowden leaks are a perfect example of this. As a contractor, he was able to singlehandedly compile a cache of the NSA's most sensitive data – simply because his credentials allowed him to. You could write this off as a HR mistake and say the NSA hired the wrong person, but you'd be ignoring the bigger picture - can employees always be counted on not to abuse usernames and passwords, and to protect them from loss or theft?

Instead, Snowden should have been prevented from accessing such a huge volume of classified information in the first place, or to put limits on that access. From an outsider's perspective, it looks like his level of NSA clearance opened up everything – there doesn't seem to have been any barriers between separate projects and offices. The ideal scenario would have seen Snowden's access restricted to only what he was working on directly.

The problem of administrator abuse

Wide-open administrator access represents a major affront to the principles of effective IT security. It's always possible a company could put a Snowden-type figure in a position of genuine power and risk a crippling insider attack. This should act as another impetus for the C-suite to bring IT security into the boardroom - it's no good putting an administrator in control of cyber defences when he or she could be a rogue operator.

Of course, that alone won't stop disgruntled or criminally-motivated individuals abusing the access privileges they retain. Similarly segmentation won't be much comfort to a company that suffers the loss or theft of network credentials that do provide permission to sensitive data. Instead, a few other steps could be taken to minimise the risks:

- Two factor authentication and more granular access parameters, so a login attempt from an otherwise authenticated user can be short-circuited if it comes from a suspect location or operating system.
- The four-eye principle could be introduced ensuring employees are always monitored when working in a way that requires high-level access.
- Where this is impossible, the threat of administrator abuse can be addressed with other safeguards such as encryption. If high-risk files are encrypted, and if key generation and management occur outside the domain of the administrator, then he or she has no way to compromise the data inside, even with carte blanche network access.
- Even if that proves impracticable, there are other routes to consider. A decent logging and reporting system, for instance, could be configured to send an alert straight to the CIO should an administrator show signs of accessing sensitive data. This might even have the side effect of instilling some accountability in employees whose attitudes toward IT security would otherwise be lax.

As business networks become more complex, so do the risks

Ultimately, the C-suite needs to be aware that it's not the current climate alone that should act as an impetus to take cyber security more seriously. Even as international tension escalates over allegations of cyber espionage and as data breaches become more catastrophic, business networks are growing in complexity. This is evident in trends like bring your own device and the cloud, both of which are putting pressure on IT departments to roll out holistic usage policies – often with limited success.

Until senior executives wake up to how these issues create new attack surfaces for their data, many organisations will continue running the risk of breaches by pushing the responsibility for security down to rank-and-file workers.

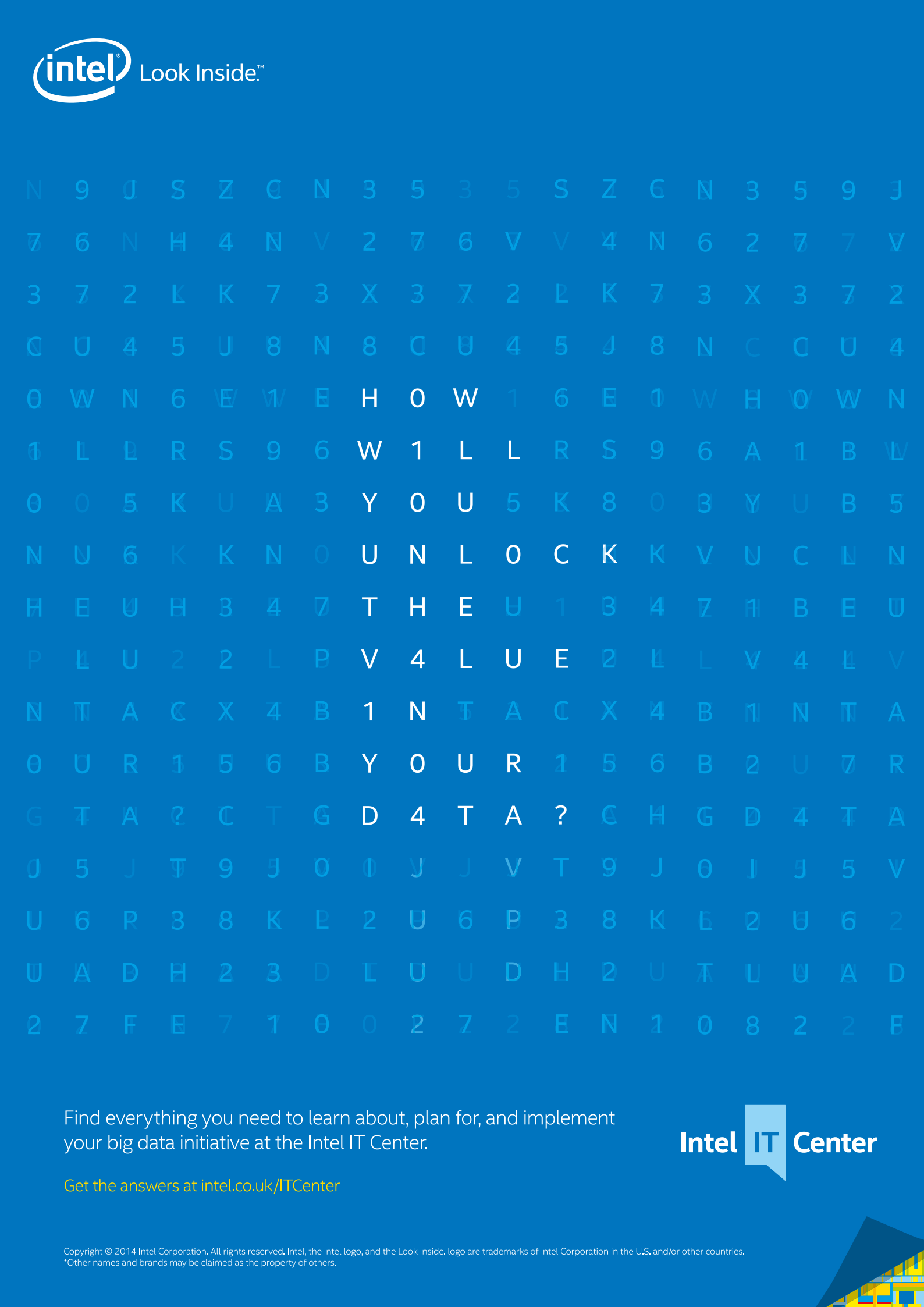
Further information

About Cryptzone

Håkan Saxmo is the CTO at Cryptzone, a global IT security vendor focused on cybersecurity. The company's solutions deliver innovative approaches to Encryption, Identity and Access Management solutions. The vision and strategy of Cryptzone is to deliver trusted IT security solutions that disrupt traditional security models, as they no longer work in a world of cloud-based applications, ubiquitous devices, and distributed workers.

Headquartered in the United States with Research and Development located in Sweden, the company has a global presence through an extensive partner network.

For more information visit: www.cryptzone.com.



Find everything you need to learn about, plan for, and implement your big data initiative at the Intel IT Center.

Get the answers at intel.co.uk/ITCenter

Intel IT Center

Big data vision

Adam Davison MBCS CITP asks whether big data means big governance

FOR THE AVERAGE UNDERGRADUATE student in the 1980s, attempting to research a topic was a time consuming and often frustrating experience.

Some original research and data collection might be possible, but to a great extent, research consisted of visit to a library to trawl through text books and periodicals.

Today the situation is very different. Huge volumes of data from which useful information can be derived are readily available – both in structured and unstructured formats – and that volume is growing exponentially. The researcher has many options. They can still generate their own data, but they can also obtain original data from other sources or draw on the analysis of others.

Most powerfully of all, they can combine these approaches allowing great potential to examine correlations and the differences. In addition to all this, researchers have powerful tools and technologies to analyse this data and present the results.

In the world of work the situation is similar, with huge potential for organisations to make truly informed management decisions. The day of the 'seat of the pants' management is generally believed to be on the way out, with future success for most organisations driven by two factors: what data you have or can obtain and how you use it. However, in all this excitement, there is an aspect that is easy to overlook: governance.

What structures and processes

> What is clear is that big data presents numerous challenges to the organisation, which can only be addressed by robust governance

should organisations put in place to ensure that they can realise all these possibilities? Equally importantly, how can the minefield of potential traps waiting to ensnare the unwary be avoided? Can organisations continue to address this area in the way they always have, or, in this new world of big data, is a whole new approach to governance needed?

What is clear is that big data presents numerous challenges to the organisation, which can only be addressed by robust governance. Most of these aren't entirely new, but the increasing emphasis on data and data modelling as the main driver of organisational decisions and competitive advantage means that getting the governance right is likely to become far more important than has been the case in the past.

Questions, questions

To start with there is the question of the overall organisational vision for big data and who has the responsibility of setting this? What projects will be carried out with what priority? Also one has to consider practicalities – how will the management of organisational data be optimised?

Next we come to the critical question of quality. Garbage in, garbage out is an old adage and IT departments have been running data cleansing initiatives since time immemorial. But in the world of big data, is this enough? What about the role of the wider organisation, the people who really get the benefit from having good quality data?

There is also the issue that a lot of the anticipated value of big data comes not just from using the data you own, but from combining your data with external data sets. But how do you guarantee the quality of these externally derived data sets and who takes responsibility for the consequences of decisions made based on poor quality, externally derived data?

Although garbage in more or less guarantees garbage out, the opposite is not necessarily true. There are two elements involved in turning a data asset into something useful to the organisation; good quality data and good quality models to analyse that data. As was clearly demonstrated in the banking crisis, however, predictive models rarely give perfect results.

How therefore can organisations ensure that the that the results of modelling are properly tested against historic data and then re-tested and analysed against real results so the models and the data sets required to feed the models can be refined and improved?

Above all, how can organisations ensure that the results of analysis are treated with an appropriate degree of scepticism when used as a basis for decision–making?

Confirmation bias

Also, when considering how such models are used, the psychological phenomenon of confirmation bias needs to be considered; the human tendency to look for or favour the results that are expected or desired. Inevitably analysis of data will sometimes give results that are counterintuitive or just not what was looked for, leading to the age old temptation to dismiss the results or massage the figures. What policies and processes are needed to ensure that this doesn't happen?

Another important governance issue is around how to protect the valuable data. The information security threat is constantly evolving and as big data becomes the critical driving force for many organisations, the risk of having their data asset compromised or corrupted becomes acute. Great clarity on who is responsible for managing this issue and how it is managed will be critical.

So, when starting to consider all these issues, the most fundamental question is; where should responsibility for these issues lie? Generally speaking, four options tend to present themselves:

- The CIO as the person responsible for managing the data asset;
- The person or people who get the benefit from the data asset;
- With a neutral third party;
- A mixture of the above.

As things stand, in many organisations, the CIO is the default answer. After all, the 'I' in CIO stands for information, so surely this should be a core responsibility? This approach does have some justification.

CIOs are often the only people who have an overall understanding of what data, in total, the organisation owns and what it is used for. Also, the CIO tends to have practical responsibility for many of the issues listed above such as IT security (not quite the same as information security, however) and data cleansing (not quite the same as data quality).

However, the CIO typically has responsibility for managing the data. Is it therefore appropriate that he/she should also own the governance framework under which this data is managed? Furthermore, CIOs tend to have a wide range of responsibilities, so their ability to give sufficient focus to data/information governance could be limited. Finally, CIOs may not be ideally positioned when it comes to influencing behaviours across the organisation as a whole.

Responsibility with the user?

For many, having overall responsibility for data governance resting with the users, the people who gain benefit from the data, is an appealing concept. They are, after all, the people who have most to lose if good governance isn't applied. Again, however, there are downsides to this.

Only in the relatively small organisation will it be practical for the user side to be represented by a single individual. More frequently, one runs the risk of ending up with a sort of governance by committee, with a range of stakeholders each with their own viewpoints. In this scenario, the chance of a consistent and appropriate governance model being created and such a model being successfully applied are very limited.

Faced with these issues, some organisations have chosen to take a third way and create the post of chief data officer (CDO): someone who has overall responsibility for organisational data but who sits outside of either (usually) IT or the end–user communities.

This approach is in many ways attractive. It means that overall governance responsibility rests with someone who is able to focus themselves entirely on the issues related to data (not the case with either the CIO or the user community) and who can take an entirely neutral viewpoint when setting rules on how such data is managed, and used.

However, issues again emerge. The CDO concept can be undermined by the question of organisational authority to ensure that the decisions that they make are binding, particularly as CEOs, already under pressure from multiple directions for increased senior level representation, will naturally be reluctant to create yet another C–level role.

Finally there is the hybrid approach, for example sharing governance responsibility between the CIO and the users or putting a CDO in place to report to the CIO or a senior user fi gure such as a COO. It is certainly true that all significant stakeholder groups will need to be involved at some level in ensuring good governance around data. However, this again brings in the issues around governance by committee and unclear overall responsibilities.

Any of the above models could work, but ultimately, which of them will work is most likely to be highly influenced by the nature of the organisation. In an organisation with a very strong cooperative culture, the hybrid approach might be the one to choose.

Last but not least, giving this important responsibility to an individual with the right experience and personality can be seen as being at least as important as their job title. Give the job to the right person and the chances are it will get done, give the job to the wrong person and the chances are it won't. What remains true in all cases, however, is that this issue will become more and more important and addressing it successfully is going to be of vital importance for all organisations.

The rise of hybrid cloud

As the cloud dust begins to settle, it has become clear that extending an organisation's internal environment through seamless integration to an off-premise infrastructure is often more desirable than a full-scale move to the cloud. Welcome, hybrid cloud.
By **Peter Grant**, CTO at Xtravirt

IN RECENT YEARS "CLOUD" HAS BECOME SYNONYMOUS with a new age of modern computing. It claims to transform traditional IT into a new world of on-demand computing, leaving behind the days of building server cabinets and worrying about data centre power, maintenance, and unplanned outages. Cloud promises to be an enabler, allowing IT to focus on improving agility and responsiveness to business demands whilst providing flexible and scalable IT services.

The above description is somewhat of an IT nirvana and, throughout the introduction of previous technological advances, the industry has learnt that the truth is somewhere between the status quo and the aforementioned description. Today's IT is evolving at an enormous rate of change and, with technologies available to solve many of today's IT challenges, the problem is knowing which solutions to choose. Cloud is certainly no different; it's often referred to as if it's a *product* when it should be more accurately thought of as a *model*. It's the model of renting vs. owning, and means considering numerous benefits and disadvantages that cloud may bring to your organisation. The concept of cloud services comes in many forms, from utilising Internet-presented applications as in "Software-as-a-Service", down to renting hosted server operating systems in an "Infrastructure-as-a-Service" model.

The adoption of cloud solutions has been slower than many predicted due to a healthy level of caution, particularly around security and compliance implications. Over the last couple of years, as the technologies have matured and the cloud dust begins to settle, the term "hybrid cloud" is becoming more prevalent. The terminology isn't critical but what *is* important is the growing recognition within the industry that there isn't necessarily a desire to move to a full cloud offering, and that the most appropriate use of cloud technologies is to augment the existing internal environment rather than a wholesale *move* to the cloud.

Business enablement through IT is all about the applications. The fact that organisations spend so much capital on data centres – building and patching servers, power and cooling, and platform maintenance – is simply part and parcel of running application services. Cloud computing has the opportunity to be disruptive and to benefit organisations by allowing them to focus on application delivery, whilst letting cloud providers focus on providing the underlying platforms. And so cloud computing allows organisations to *focus on what really matters*, that is delivering a strategic advantage to the business via the use of technology, rather than focusing on actually keeping the lights on.

Some organisations embark on cloud initiatives by taking a product-based viewpoint, whereas, in our experience, IT decision makers should first take a holistic view of their IT challenges to prevent them from embarking down the wrong

path where they risk not realising the full opportunities of cloud solutions. One opportunity, which is seldom mentioned, is the *potential* to simplify the IT estate.

Modern IT solutions often encompass so many elements that the final result is a melting pot of technologies, capabilities and limitations that can be difficult to manage. What were once innovative visions often end up being replaced with concerns of just keeping the lights on.

By removing the overhead of the hosting platform, organisations should, in theory, be able to reduce complexity in their environment. However, the hidden danger with any new solution is exactly the opposite. On the surface, cloud may provide the ability to offload this complexity, but before adopting cloud organisations should ensure all aspects of the proposed solution are considered, as follows:

- Requirements to upskill the IT staff on the cloud platform, and complexity within the platform itself
- Modification of existing applications and services to run on a third party platform
- Organisational challenges in integrating the cloud billing model or chargeback adoption
- Complex service desk workflows now spanning internal IT staff and external service desks
- Integration of cloud management toolsets, and so on…

A move to cloud adoption must evaluate these aspects to ensure that whilst one set of challenges are being eliminated, others aren't being created elsewhere. The importance of seamless integration and the reduction of complexity should be carefully considered, yet are often overlooked in favour of the easy-to-understand, tangible costs.

Some prominent providers now market their offerings as a "hybrid cloud" service with a large emphasis on seamless integration between internal and external systems. This approach is aligned to the industry trend which recognises that integration and augmentation of IT services is an easier pill to swallow than a large-scale migration. This holistic view of cloud adoption illustrates the importance of not simply doing a "per unit" price comparison when deciding on the right cloud solutions or providers.

A recent survey showed that the majority of organisations are investigating, conducting trials or implementing cloud solutions. Organisations *are* moving towards the cloud and many already have some form of cloud service, official or otherwise. Many organisations have users utilising consumer services such as Dropbox, making the boundary between home computing and corporate computing difficult to defend. People, by nature, often choose the path of least resistance and it's up to IT to either provide them with the services they demand, or stand back and watch the "cloud-by-credit-card" services enter through the back door.

To prevent the uncontrolled adoption of cloud services, organisations should consider their approach. IT strategies are often driven by desires to implement technology stacks without first having performed the due diligence to understand why this may or may not be suitable.

A cloud IT strategy should encompass a 4-step approach to increase the chances of success:

1. **Analyse the environment**
   Conduct a detailed audit using toolsets designed for the job. What an organisation *believes* they have is often different from the reality. Once a detailed audit has been conducted there will be a better idea of what really needs to be achieved moving forward. There will also be a better understanding of the challenges and their root causes, some of which may or may not be resolved by a cloud solution.
2. **Select the appropriate technology stack**
   Following a detailed analysis of the environment, it's time to choose the right solution stack. Often this doesn't equate to selecting the "best" technology stack, but instead means choosing the "most integrated" stack.
3. **Consolidate and rationalise before cloud adoption**
   Customers shouldn't migrate IT systems to the cloud and expect their problems relating to a complex, sprawling system to disappear. It is important to get the house in order first.
4. **Implement cloud based on clear deliverables**
   Large and complex IT transformations can span months or even years, and it's easy to end up chasing new technology updates and ever-changing demands of the business throughout the implementation. Whilst some change in scope is often inevitable, it's important to ensure that the urge to have the latest solution and updates doesn't overtake a completed project. Going for the 80/20 approach can, and in many cases will, deliver a *good and well-implemented* solution, rather than the gold solution that is poorly implemented and never fully completed.

Whatever form they may take, cloud solutions present organisations with tremendous opportunities for modernisation and innovation, but they must be careful to understand the challenges they're trying to resolve and strive to adopt the services whilst reducing complexity.

Author information

Peter Grant is CTO at Xtravirt, a leading, industry-recognised consulting organisation, solely focused on virtualisation as the enabler for all modern IT solutions. Having worked in a variety of infrastructure roles for global technology, banking and government organisations, Peter is considered a leading subject matter expert on IT best practices.

Xtravirt delivers data centre, workspace and cloud transformational solutions to clients across public and private sectors. Its consulting organisation is recognised globally for astute management, sound methodology and a proven track record, which provide unsurpassed value to Xtravirt's customers.
xtravirt.com

Hybrid storage:
the new powerhouse for the data centre

By **Emily Ford**, Imation

WE ARE NOW AT THE THRESHOLD OF A TRANSFORMATIVE stage in the evolution of data storage. Performance has always been a central factor in a storage infrastructure's overall success, but three key drivers have made it an even higher priority. Virtualisation has driven application consolidation in a wide variety of organisations. It has also created what is referred to as the "I/O blender," in which a single server supporting a large number of virtual servers, each running their own applications, drives more IOPS at the storage system and in turn increases the need for speed. Second, the need to extract business value out of Big Data has driven a requirement for low latency data analytics and exponential data retention growth. And third, technology advancements have lowered the overall price of performance to a level now affordable for everyone.

Despite these drivers, industry analyst and consultant Tony Asaro of The INI Group has said that only 5-10 percent of an organisation's data truly requires high performance. As a result, the challenge is to determine which data requires that high performance. As an environment's most frequently accessed data changes over time, manually managing this flow and adjusting performance levels across a storage infrastructure can become a data management nightmare. An IT administrator's goal should be to remove the requirement to manage performance bottlenecks, analytics and ongoing optimisation. Just as important, they need to meet these critical application performance needs while controlling and minimising both capital and operating expenses. As Asaro said, "Providing performance transparently and cost effectively is the next major transformative milestone in the evolution of storage."

Hybrid storage has emerged as today's most powerful tool for handling the overwhelming data growth and extreme performance requirements that organisations face. Hybrid storage is defined as a storage system that combines solid state disks (SSD) and hard disk drives (HDD) in a single system. HDDs provide high capacity storage at a reasonable cost per terabyte, while SSDs enable low latency and high IOPS performance. Hybrid storage solutions provide the flexibility to address performance requirements where needed without making tradeoffs, whereas conventional storage can't keep up with the increasing performance requirements.

These benefits have made hybrid storage systems the new powerhouse for the data centre. Hybrid storage system sales comprised $7B of the market in 2013, and are expected to double to $14B by the year 2017 with a compounded annual growth rate of 21 percent. This growth would mean that hybrid storage would comprise nearly half of the total external storage system market (Source: IDC Worldwide External Storage System 2013-2017 forecast).

There are several key considerations for organisations to keep in mind when evaluating hybrid storage systems.

- Not all hybrid storage systems are created equally. Some storage vendors retrofit conventional storage with solid state drives, while others design new systems optimised for solid state technology. But it takes more than SSD to make a real hybrid. It takes unique software functionality and the ability to dynamically manage data between SSD and HDD, using caching or tiering.
- Hybrid caching techniques provide performance efficiency. The data path for caching is short and safeguarded, and hybrid caching allows you to scale your storage write and read caching beyond that of high-speed DRAM using SSD flash capacities. In the case of read caching, hybrid caching uses predictive algorithms to proactively copy large chunks of data from HDD to SSD ahead of the read requests for fast data access. When the application looks for data and the data is stored in the cache, you get a cache hit and accelerated read operations. All data continues to be stored in underlying protected HDD or SSD storage with copies of the most active data in the cache. On the other hand, the data path for tiering is longer and more complicated. Data dynamically moves between SSD and HDD storage automatically, using algorithms that predict the need for the moves. The SSD tier holds the only copy of the data in a system and uses a RAID-like data protection scheme. The overhead this creates impacts performance and capacity, because it

requires the overprovisioning of both SSDs and HDDs and adds complexity and risk to the environment.

- Optimise write caching. To create a hybrid storage system that can support a wide range of workloads, it's important to start by ensuring the system can sustain the high performance write workload for mission-critical databases, VDI and similar applications. The central factor in doing this is the system's ability to de-stage data from the write cache to the slower spinning HDD efficiently so that the system does not overflow its cache capacity. An effective and balanced approach to achieve this is to aggregate cache writes and to de-stage them sequentially to HDD storage. This approach ensures the highest possible write performance while ensuring your data is protected.
- Caching customisation translates to performance where you need it the most. The way that hybrid storage systems leverage DRAM and SSD for write caching and read caching gives you better performance and longer flash life. But hybrid's most important feature is customisable read caches that let you decide how to maximise the use of premium-priced SSDs. Consider this virtual machine (VM) example: a hypervisor processing multiple VM I/O streams will drive heavy random workloads on HDD storage, resulting in longer latency and reduced VM responsiveness. But a customised read cache in front of the HDD volume eliminates this performance bottleneck, increasing performance on this storage volume. Hybrid storage will even allow for 100 percent cache by configuring the SSD to the same size as the HDD volume, resulting in blazing-fast performance for this specific application. That kind of flexibility could be a real boon for your databases.
- Back-end storage infrastructure matters. Performance gets most of the attention in storage because it enables applications to respond lightning-fast – or when it's designed improperly, it can cripple an organisation's applications. But don't forget about the guts of your storage system – the agile, efficient and reliable back-end storage infrastructure that deals with your flood of data. The best hybrid solutions offer a lot in terms of guts: density and space savings, non-disruptive capacity scalability, power and cooling savings and offload task processing capabilities…all at a low cost of ownership that any cost-constrained data centre will prize.

In addition to the performance and latency benefits that hybrid storage brings, organisations also should be sure their storage infrastructures have all the capabilities needed to manage their most valuable data. As Asaro recently wrote in a paper describing hybrid storage, "SAN, NAS, data protection, replication, ease of management, highly virtualised storage, capacity scalability and feature-rich storage combined with performance will define this next stage."

One important capability to watch for is scalability. Today's exponential data growth has forced many organisations to handle large volumes of unstructured and structured data. However, they don't want the high cost of overprovisioning for the expected growth. Organisational needs change quickly in today's dynamic business environment, so they need highly scalable and efficient data storage that can adapt appropriately.

Today's IT demands require storage infrastructures with various features and functionality to ensure proper data protection and management. Business continuity and data protection services that are easy to use and manage are essential. Thin provisioning, compression and online expansion have emerged as features that can drive infrastructure efficiency in the face of ever-changing storage needs. Additionally, replication, snapshots and active data integrity checks help ensure valuable business data is protected.

Storage infrastructures also need to deliver both file and block storage services without increasing storage administrative overhead. Gone are the days of storage silos that result in administrative complexity and underutilisation of storage. The amount of unstructured data (files, images, videos, audios, etc.) being created today far exceeds that of structured data. But transactional, structured data driven by database applications is often the core of a company's business. Both data types have great importance in terms of value and impact on IT infrastructure, so it's prudent to look for a storage system that supports both block and file-based storage within a single software stack and a single-pane-of-glass management interface.

Hybrid storage systems have emerged as a popular solution, and the right one can deliver all of these benefits in a transparent and cost-effective manner. It will be fascinating to see how their capabilities translate into organisational benefits – and just how quickly they are adopted by organizations everywhere.

Author information

Emily Ford is senior product marketing manager at Imation. For more information on Imation's Nexsan storage system family, or the emerging category of hybrid storage, visit www.imation.com.

KILOBYTES

MEGABYTES

GIGABYTES

TERABYTES

PETABYTES

VOLTA

As the business world adopts ever more sophisticated forms of technology, the need to process large amounts of data increases on an almost daily basis.

WHERE ARE YOU STORING YOUR DATA?

Volta Data Centres understand the need for every connected business to store and process data in an ever-more efficient and cost-effective manner.

Volta's 91,000 sq ft Central London data centre is a purpose built 9.6MW facility, offering the optimum solution for data storage.

BOOK FOR A TOUR TODAY:

sales@voltadatacentres.com

VOLTA DATA CENTRES

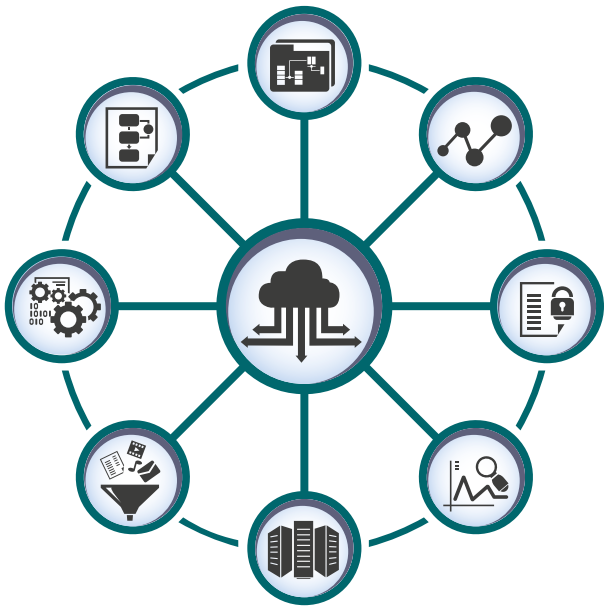
36–43 Great Sutton Street,
London, EC1V 0AB

T +44(0)20 7036 8077
W www.voltadatacentres.com
E sales@voltadatacentres.com

@voltadatacentre
search Volta Data Centres

VOLTA
Smart, Secure, Resilient

Big data, big questions, big answers



Data is a new factor of production; used well, it can boost productivity, profits and customer service. What does 'big data' mean for business? **Intel** experts share their views

'WHAT IS BIG DATA? A MEME AND a marketing term, for sure, but also shorthand for advancing trends in technology that open the door to a new approach to understanding the world and making decisions,' says the *New York Times*'s Steve Lohr.

Big data is more than just 'data'. It combines technology, people, methodologies and management; it stands for a cluster of innovations that combine to offer a new competitive edge.

- **Gartner predicts** that the 10-15 percent of organisations who take full advantage of big data in the next few years will outperform their competitors by 20 percent across major financial metrics.
- **The McKinsey Global Institute** estimates that a retailer using big data to the full has the potential to increase its operating margin by more than 60 percent.
- In 2011, **UPS cut 85 million miles** out of drivers' routes, using telematics sensors in its trucks, thereby saving more than 8.4 gallons of fuel.

While making use of big data clearly requires investment, training, experiments and possibly an entire redesign of your management structure, one thing is for sure: it's worth it.

Towards Analytics 3.0

The most recent incarnation of big data, 'Analytics 3.0' as the Harvard Business Review (HBR) has termed it, means 'investing in analytics to support customer-facing products, services and features.'

Big data now means going beyond internal efficiencies and customer service, using data to actually inform the front-line of your operations. Most companies, however, are nowhere near that stage yet, so let's take a step back and break down big data a little more.

The 'big' part of big data refers to the three main properties of data now being collected: Volume, Velocity and Variety. These three V's, **originally coined by Gartner**, sum up the opportunity and problem of big data. Data is getting bigger in all three axes, thanks to the internet of things, social media, the proliferation of mobile internet and the digitisation of business processes.

This offers great opportunities for real-time insight into all sorts of behaviours and activities, but learning to bring this big data into your business and make effective use of it means addressing more than just technology (not that technology is a small challenge). You need:

- Technology and architecture for collecting, storing, cleaning, collating, interrogating and visualising structured and unstructured data across the business
- Human business expertise to understand what particular business problems big data can answer and the technical expertise to know what questions to ask of data to get meaningful predictions and optimisations
- An integration of IT into the business so that insights can drive decisions and a company culture that prioritises what you know over what you think

How to find the starting line

The easiest way to approach big data is to figure out where your business stands along the evolution of analytics; that will tell you how far you are from 'Analytics 3.0' – using big data for customer-facing products, services and features – and what the route to get there looks like.

Analytics 1.0 is familiar territory, having been around since the mid-1950s; tools began to emerge that could produce, capture and discern patterns in data faster, and in greater quantities than unassisted human minds could. The first mainframes were used to manage airline bookings, insurance policies and similar internal business process. This was a great leap forward no doubt, but analytics 1.0 'addressed only what had happened in the past; they offered no explanations or predictions,' explains the HBR.

Analytics 2.0 was the dawn of big data; it began

to include data generated outside the company's transactional systems and required tools that could process and make use of unstructured data. In addition, it made use of machine learning methods and predictive analytics to start asking why something had happened and how future events or trends could be predicted.

Unfortunately, many firms are struggling even to take advantage of the first two stages, let alone reaping the front-line rewards of Analytics 3.0.

Get the technology right

'The biggest reason that investments in big data fail to pay off…is that most companies don't do a good job with the information they already have,' argue **Jeanne W. Ross, Cynthia M. Beath and Anne Quaadgras**.

For big data to be of genuine value, it has to be clean and reliable so that useful comparisons and predictions can be made. This means having a single version of the truth across the organisation, which in turn requires a shift in attitude, both in terms of IT architecture and management practice and culture.

'The old formats haven't gone away, but new processes are needed to move data and analysis across staging, evaluation, exploration, and production applications,' **says the HBR**.

The biggest and usually the first challenge involves breaking down barriers between silos of information in different areas of the business and creating a single, shared infrastructure to allow everyone to access a single, de-duplicated set of data.

You then need infrastructure and software that can handle the quantities and varying types of data that you are collecting and that can make them accessible and able to integrate.

Luckily, as systems become more sophisticated and automated, the value that can be extracted from big data will inevitably increase. After all, less time spent prepping data means more time interrogating it.

Get the right people

You can have all the technical wizardry in the world, but big data is worthless without data scientists who know how to ask the right questions of data and managers who will listen to data over hunches and instinct. Finding people with the right skills is therefore a significant challenge.

'By 2018, the United States alone could face a shortage of 140,000 to 190,000 people with deep analytical skills as well as 1.5 million managers and analysts with the know-how to use the analysis of big data to make effective decisions,' says the **McKinsey Global Institute**.

The best way to circumvent this shortage is to build the skills you need with the talent you already have in house. It's harder to learn business knowledge that makes data into valuable information than it is to learn the IT technical skills.

Collaborate

Even with a brains trust of data scientists and an evolved IT infrastructure, everyone still has to be able to work together to realise the value of big data. IT has to become integrated into the business, and departments have to allow IT some authority in guiding their direction. The solution? Partner with business units to identify where hidden potential is.

Without a connection between the collection and application of data, there is no incentive to ensure data is accurate, timely and relevant. And without a good working relationship between the business and IT, any insights derived simply won't be respected or implemented to best value.

Pick your battles

'Managers need to become comfortable with data-driven experimentation,' **Thomas H. Davenport** argues. This doesn't mean, however, that their business acumen is no longer relevant: managers will need to prioritise business problems by potential value and they 'will have to establish guidelines for when early warnings [provided by big data] should cue decisions and action.'

It's also the role of managers to empower their employees with data; 'it's about betting your business success on the ability of good people to use good data to make good decisions,' says Ross, Beath and Quaadgras.

Learn to walk with your little data before you run with the big

Here are some tips that can help those just entering the arena get it better first time:

- Start small. Build your skills and engage with the business. This will take time so start with short specific initiatives that have fixed targets, eg six months, a team of five, $10 million incremental value, and then build on that reputation. And know that it's okay to walk away from a project if you realise there's no real opportunity there.
- Big data is a means to an end. Big data shouldn't be some special, siloed project buried away in the basement. It's a tool for powering other line-of business problem-solving projects. Don't lose sight of the big picture.
- Start with what you have. Use data you already collect internally and build up the skills necessary for big data initiatives by solving business problems with this data before you start expanding into third party sources like social media and public government data.

Why you need an "Open Hybrid Cloud"

By **Alessandro Perilli,** GM Open Hybrid Cloud, Red Hat

BEFORE GETTING INTO THE DETAIL OF why you need an open hybrid cloud, let's take a look at the building blocks. An open hybrid cloud consists of five core pillars: the first pillar is the capability to empower IT organisations with the right tools to address the demand of the line of business in the cloud era. The second pillar is the capability to embrace and support the IT diversity in an enterprise environment, irrespective of the selected IT strategy for cloud computing. The third pillar is the capability to adapt to your IT maturity level, providing more sophisticated cloud capabilities only when the IT organisation is ready to deploy them. The fourth pillar is the capability to extend easily, supporting a broad set of hardware and enterprise management tools, thanks to a modular architecture and a rich ecosystem of partners. The fifth and final pillar is a strong foundation on open source technologies, which provide the innovation necessary to transform your IT.

Today our technology-driven lives are supported and augmented by cloud services such as messaging, content and collaboration systems, file storage and productivity tools. We consume cloud services wherever we're located be that in the home or on the road. And we consume them on daily basis, because they "just work".

Corporate users are first and foremost individuals. When individuals consume public cloud services outside the corporate boundaries and they just work, that experience leads to a completely new class of expectations. As individuals at home, corporate users experience cloud-based IT that just works and they expect the same frictionless, instantaneous, cost-effective interaction with corporate IT. Why should corporate IT be less efficient than personal IT?

Public cloud infrastructures are designed from scratch to be frictionless, agile and cost-effective. These are the pillars of their core business and anything that gets in the way, like compliance to security regulation, is sacrificed or taken care of at a later maturity stage. Corporate IT, however, is built on layers of legacy software and hardware systems, stacked up through decades, designed in a different eras, after different technology paradigms. In addition to the technical challenges there are security policies and regulations to consider. And then political and cultural issues that influence the IT strategy in ways

that become obvious only years after decisions are made.

Corporate IT struggles to compete with public cloud service providers and has a long way to go before it will just work, but line of business managers cannot wait. Why stick with a less efficient service when there are a plethora of better alternatives around? So the line of business simply spends its budget outside the corporate environment. The risk, ultimately, is that corporate IT becomes less and less relevant and corporate data gets more and more at risk.

Why a hybrid cloud?

The IT organisation realises that increasing IT agility is the only way to address the demand of the line of business. Public cloud computing is great in specific scenarios but the industry is not mature enough yet to address all the needs an enterprise has to host mission critical applications.

Every group within the IT organisation thinks about how to speed up the application lifecycle from a different angle and each one could have confidence in a different technology. Prototyping, testing, and provisioning in production line of business applications can be done through traditional virtualisation, Infrastructure as a Service (IaaS) cloud computing, or Platform as a Service (PaaS) cloud computing.

The application development team may feel closer to the PaaS approach while the infrastructure and operation team could have a preference for traditional virtualisation or IaaS. There is not the "right"itool. Most likely, the IT organisation will have to leverage some or all of the above in combination selecting the most efficient tool for each situation, hence the hybrid cloud. We don't use a hammer for all our home improvement and repairs jobs, do we?

Each of the aforementioned technologies has advantages and disadvantages, in all likelihood the IT organisation will host different components of the same line of business application on different platforms. For example, as the organisation starts its cloud computing journey, the web frontend will be served by a scale-out IaaS or PaaS cloud platform, while the backend database and the middleware will likely remain hosted on the virtualisation platform which supports better scale up architectures. Over time, scale up middleware will be replaced by scale out middleware and transitioned from the virtualisation platform to the IaaS platform, some application components will be moved to PaaS, while others will be hosted on a public cloud platform.

Of course, offering multiple cloud platforms is not enough. Without a unifying management layer, IT organisations would end up building multiple management silos, recreating the same policies and automation steps for each platform. That unifying cloud management platform is what keeps the different portions of the same application together, no matter if they are hosted on a scale up or scale out platform, on a maintaining consistency from provisioning to retirement.

Ultimately, being "hybrid" really means embracing and supporting IT diversity while maintaining consistency. A hybrid cloud should support the organisations' IT strategy, no matter if it evolves towards an IaaS or a PaaS approach, or if it just focuses on premises deployment rather than consuming a mix of private and public cloud services.

Why an open cloud?

Public cloud took off because it just works, and it just works because cloud providers innovated and continue to innovate the whole IT stack, from the infrastructure to the application. And they could innovate because of the possibilities offered by open source technologies.

Open source is not just about code transparency. More than anything, open source is about open collaboration. In mid-2014 the most brilliant minds in our era get together and work together to solve world-class problems that didn't even exist a decade ago, and their platform of choice to innovate is open source.

Because of its open collaboration model, open source moved from being a mere replacement for proprietary technologies to being the platform of choice for innovation. Think about web scale companies like Facebook, Google, LinkedIn, Netflix, Yahoo, and hundreds more. In those IT environments, serving hundreds of millions of concurrent users, billions in some cases, the choice between open source and proprietary software is not even discussed. The former is the default option, the latter requires building a business case.

Compared to the aforementioned companies, however, traditional enterprise organisations cannot consume raw innovation built on open source technologies. Large corporations need things like multi-year support lifecycle, certified integration with third party vendors, training programmes, intellectual property indemnification, security incident responsiveness, and more.

Enterprises need the innovation coming out of open source software and its open collaboration model to remain competitive in their industry and against public cloud providers. At the same time, those enterprises need a reliable business partner to help that innovation fit their infrastructure and culture.

Further information

The Red Hat Open Hybrid Cloud

If you think that Red Hat is just Linux, think again. Red Hat worked hard to expand its portfolio beyond Red Hat Enterprise Linux and JBoss, and being able to offer an open hybrid cloud. Today we can count on three cloud engines (i.e., a traditional virtualisation management platform – RHEVM, an IaaS platform – RHELOSP, and a PaaS platform – OSE), a unifying cloud management platform (i.e., CloudForms), and a set of underlying resource abstraction technologies (i.e., for compute resources – RHEV, for storage resources – RHSS and ICE).

On top of this rich portfolio, coming together in a solution we call Open Hybrid Cloud, Red Hat has its decade long credibility as the most trusted provider of open source technologies for the enterprise. We believe these ingredients are what we need to help our customers address the demand of their line of businesses and innovate their IT.

xtravirt

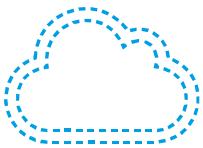
Ahead in the cloud

For fluctuating workloads, a fully integrated test and development area, or a disaster recovery solution, the VMware® vCloud® Hybrid Service™ seamlessly extends your internal environment to a unified off-premise infrastructure.

Xtravirt offers a range of professional services to ensure optimised adoption of the vCloud Hybrid Service.

We demonstrate how to achieve:

- Scalability
- Cost efficiency
- Full compatibility
- Increased resilience
- Accelerated time to value



CloudConcept

CloudConnect

Contact the experts

information@xtravirt.com xtravirt.com +44 (0)800 4880 038

Are the CIO and line of business executives after the same thing?

Cloud Computing is a catalyst for digital transformation – and required today because business is changing faster than ever before, Sven Denecken reports

DIGITAL TRANSFORMATION REQUIRES IT and other business areas to rethink their technology approach – change and adopt or face the consequences. Over half of the Fortune 500 are no longer there, just since 2000. That's change.

To be successful, the CIO and the other line of business executives have to take business challenges head on.

Consider this statement – the IT department is a line of business as well. But in my job, based on dozens and dozens of discussions weekly with co-innovation customers, one thing is clear: the tension between CIO and LoB leader – CMO, EVP of Sales, CHRO, CPO, etc., is getting worse, not better in many companies.

Why? Based on past experience – line of business managers hesitate to bring in their IT colleagues when making technology investments or decisions out of fear of being blocked. And they're turning to the cloud because they don't need IT to implement or maintain. This reality is keeping many CIO's awake at night. Because once something becomes part of the infrastructure, the real work begins.

Most people in business agree that innovation is a game-changer. There's a new sense of urgency. We can see an accelerating pace of change and innovation requested by many realities – and fuelled by many technological advances in the recent years. Cloud is at the heart of this change.

Does IT matter?

Nicholas G. Carr, a 2011 Pulitzer Prize finalist who writes about technology and culture, poses an critical question: does IT matter? The CIO's in today's organizations are under fire. By 2016, according to IDC, LoB executives direct 80% of new IT investments; in 2013 they were already behind 58% of them.

In today's fast-paced business world, companies need to be able to predict the future with confidence, assess the right response, and have the agility to quickly adapt their business processes to capitalise on changing market dynamics and to stay ahead of the competition.

Imagine the significant pressure this puts on CIO's to reinvent their departments. Many companies talk about the need for the **CIO** to be the **C**hief **I**nnovation **O**fficer. LOB's are demanding: faster innovation, faster time-to-value, all mobile, vastly improved ease-of-use AND a general **simplification of consumption.**

The Inherent Disconnect Today
What does the CIO want?

It is all about efficiency: doing the right things and doing them securely

- Approach a need with research and problem identification
- Analyse your options
- Come up with a plan that covers technology, logistics, schedule, costs
- Implement the plan avoiding changes as much as possible

Requirement: a constant focus on balancing between **run** the company and **change** the company.

What does a Line of Business leader want?

It is all about effectiveness: doing the right things and doing them quickly, so you can adapt on the fly as new competitors emerge and new realities present themselves

- Plans are general guidelines, as long as we are on track we're fine
- Planning is more brainstorming than research, driven by a "we can do it" priority (do you want to say something about 57% of purchase decisions are made before the vendor is contacted?)
- When problems occur, we adjust the plan flexibly
- The implementation is focused on quick usage and fast adoption

Requirement: A consistent balance between **faster** outcomes and needed **innovation**.

Innovate - use cloud, but focus on business outcome

These recent infographics on innovation and connectivity published by Oxford Economics provides some good insights and guidance. A high percentage of business surveyed reported embracing the cloud to develop new products, enter new markets, establish new business models to engage with customers, employees and partners; and strategically transform their IT departments into profit canters.

Cloud computing is having a massive influence on every service and product, and ultimately the end user in a big way. What the cloud enables B2B and B2C companies to do is really put customer and the end user at the centre of their business. Cloud customers have full flexibility to consume what they need when they need it and on a simplified, unified and real-time platform

Even more interesting, 69% of respondents credit the cloud for reshaping IT into a more strategic partner. The top concern is still security – a starting point for an educated discussion with IT.

Cloud computing has the potential to further reduce and commoditise the traditional footprint of IT organisations, freeing up resources to focus on value-adding activities. An historic opportunity for IT – but requires a change in mindset and different, non-traditional skills.

Thanks to cloud computing the distance between the engineer and the end user of the product is now dramatically reduced. The result is unmatched speed of innovation, simplicity and reduced time to value. The cloud has enabled businesses, whether they are using public, private or hybrid cloud, with the simplification of processes and time of value that trumps any other technology

What we're looking at is a lessening of commodity-oriented roles. These new roles must focus on delivering technology-driven added value.

An internal cloud-broker is needed to ensure that various deployment scenarios can be addressed because most businesses are not ready to for an enterprise-wide rip-and-replace approach.

CIO's can lead to prepare the companies for the digital transformation

As we can see in the recent whitepaper from E&Y, the modern CIO can lead this transformation. Even more, it is a major opportunity to fulfil their career aspirations. Clearly proactive CIO's within IT-intensive sectors are better suited to transform their business.

So we think if innovation is approached in the right way, and the digital transformation agenda touches us all – the collaboration between IT and the other leaders will improve. And that benefits the business.

After decades of IT decisions following the path of "Run the Company in the best possible way" we now face a decade of "Run the User in the best possible way". The consumerisation of IT.

Further information

Let us know what you think and follow us via twitter @SDenecken

About Sven Denecken
Sven Denecken is Global Vice President of Strategy for Cloud Solutions at SAP. He collaborates closely with varied market constituents to supports the strategy of cloud and its alignment with the SAP field organization and ecosystem.

About SAP
SAP (NYSE: SAP) is committed to being the cloud leader, powered by SAP HANA. We offer the industry's most comprehensive portfolio of Cloud solutions for business, all built for mobile and leveraging the industry expertise from more than 258,500 SAP customers in 191 countries across 25 industries. 36 million people use SAP Cloud today. Learn how SAP Cloud can provide the innovation and agility your business needs to run like never before - www.sap.com/cloud.

NEXSAN™
by imation

SCALABLE HYBRID STORAGE

- ENORMOUS CAPACITY
- INCREDIBLE SPEED
- HIGHLY RELIABLE
- CONTINUOUSLY AVAILABLE

LIMITED TIME SPECIAL OFFER ON NST5100

GET ON THE FASTIER™ TRACK

Nexsan products are purpose-built for the needs of small-to-mid-sized business. Imation's NST flexible hybrid storage appliance with proprietary FASTier™ caching speeds up applications and keeps virtual machines running, consuming up to 85% less power when idle.

IT'S A DIFFERENT KIND OF STORAGE EXPERIENCE.

Learn more about Nexsan at:

www.imation.eu/nexsan

Death of the Comms Rooms?

Matthew Dent examines the challenges of managing increasing amounts of data

NEW TECHNOLOGIES HAVE ALLOWED US TO STAY MORE connected, disseminating large amounts of information on a 24-hour basis and inferring real-time knowledge from large data pools in a way that wasn't previously possible. There are a lot of buzzwords around these processes including "big data" and "cloud". But what do each of processes mean for the once-humble comms room whose job it is to back up all this technology and ensure information really is seamlessly accessible on a constant basis?

There's a big, wide world out there

Big Data can be daunting in terms of simply untangling the different types of data out there, extracting insight out of the so-called "noise". Companies interested in reaping the advantages of Big Data are having to familiarise themselves with advancements in new data management systems and the options available for storing and, more importantly, quickly and accurately retrieving relevant data sets.

An obvious common thread in this challenge is the sheer volume of data that new technology either uses or produces. References to terabytes of data are being replaced with petabytes and even exabytes (1 million terabytes). To give you an idea sense of scale, Google processes more than 1 petabyte (1PB) of data every hour.

As the world adopts ever more sophisticated forms of technology, an unprecedented drive is being created for firms to store and process data in an ever-more efficient and cost-effective manner.

Can cloud save us?

The components and operations applications, accessories, services and architectures of exponentially increasing amounts of data need to be housed somewhere. Whether private, public or hybrid, the use of cloud technology has sometimes been hailed as the answer to managing large amounts of data as it gives the flexibility of processing spikes during traffic overflow in peak times. The development of 'cloud balancing' systems means that the communication between two clouds can be controlled, allowing for the selection of best locations (whether a primary or secondary data centre, or an on-premise location) from which to serve an application.

Whether or not cloud is adopted as a method of managing petabytes of data, the question remains as to whether the comms room can keep up with the flexibility of technologies currently on offer.

Can the comms room cut it?

Every connected business nowadays is considering how to better handle its data today, how to prepare for the anticipated exponential increase, and how to ensure that it meets its 'disaster recovery' requirements and regulatory obligations.

Firms face a choice. Either to store data on-premise in their 'comms room', outsource to a data centre / collocation facility, or a combination of both. It all depends on the business model of the firm, the ambition of anticipated growth and the scale of required data handling. Whatever the site, firms are seeking resilient, reliable and flexible storage. Not only do firms need a back-up 'DR' plan, but the sites themselves must be fully resilient and backed up. Confidence is critical.

Essential infrastructure

The nerve centre of modern business, data centres are deemed to be an essential part of industry infrastructure, housing the servers, storage and networks. This is partly due to the scale of the demand as industries become ever more electronic, partly due to the efficiencies on offer. As every CIO and CFO will testify, resources need to be managed diligently today needing careful consideration and cost control.

Our discussions with London businesses weighing up

comms rooms versus data centre options focus on a number of requirements ranging from internal resource and expertise, to cost management, resilience of power and connectivity and also location. Each firm will put different store on their storage and management needs, but broadly speaking they all outline the following requirements:

- **Technology & Expertise:** The amount of in-house technology – including power and cooling – combined with the on-going human expertise and resources to provide 24 x 7 physical infrastructure management and support can represent a considerable cost. Moreover, these costs and resources might better be deployed elsewhere and contribute instead to the core revenue-generating function of the firm. Firms running their own comms rooms must be confident that their technicians are well informed about the latest changes in data centre technologies, which are becoming increasingly efficient and are quickly deployed in a purpose built hosting environment.
- **Resilient power:** IT infrastructure and data management place a huge demand on facilities in terms of power and cooling and the costs to deliver a resilient infrastructure can be prohibitive. Access to a resilient and diverse power supply is critical to minimise any potential downtime. By design, data centres inherently offer an uninterruptable power supply. To give a sense of what this means, our tier 3 Central London facility in Great Sutton Street offers diverse 33kV power supply from not one, but two independent substations of the national grid. A large proportion of London would have to suffer an outage before we would need to invoke our back-up generators.
- **Diverse connectivity:** Domestic and international links are important when accessing global markets and firms are looking for diverse carrier feeds to ensure fast and effective connections. Connecting these feeds into in-house facilities can be a challenge, whereas, by nature, data centres have multiple carriers with diverse links already in place. The ability to cross-connect with other carriers is also key. When a business connects into a data centre it is also becoming part of a whole ecosystem including the carriers who link this ecosystem to the rest of the world – also clients of the same data centre. This allows for the potential of greatly expanding a company's global footprint with not only increased local connections but also greater global connectivity for the business, without enormous overheads. Experience has taught us that on the whole, suppliers are quicker to deploy and support the connections to data centres than individual sites – we put that down to the benefits of scale.
- **Flexibility & Scalability:** It is interesting to note that many firms are employing heads of data and data strategists. Heads of Technology are considering how to handle the scale and inevitable growth of data and we talk to many firms about the constraints they are facing and can anticipate. Can their comms room handle the data requirements today? Do they have the space and facilities to handle future expansion both in terms of rack space, power, cooling and internal and external connectivity? Scaling up at the right pace can be a gamble. Empty facilities waiting to be filled cost money. Overfilled spaces run the risk of being adversely impacted by operating in sub-optimum conditions.
- **Security & Location:** It is interesting to note that firms are also looking at data in different ways. What types of data should be kept on-site? What can be housed in an outsourced data centre? Regulatory and security obligations can underpin these discussions and we have seen a lot of interest from firms attracted by the convenience of our central London location, our security procedures and protocols, as well as the choice of connectivity and resilient power. Location can also be a factor when companies would like to feel more in control when accessing their systems. Whilst Smart Hands technical support service should be a prerequisite of every modern data centre, there are times when engineers prefer to be able to get quick access in person. Data centres located in proximity to your offices could be a potential attribute.

Time will tell

As firms are considering their data management, storage, handling and potentially cloud strategies, they are considering how to support and serve the growth at the right pace and in a way which will immunise them against having to over-invest in order to stay on top of technological developments. Whether this is a full cloud or in-housed approach, or perhaps a hybrid approach with data centre support, 2014 will be filled with debate about how today's firms will need to innovate and adopt technology, including their approach to data management.

Author information

Matthew Dent, CEO, Volta Data Centres

Matthew Dent was appointed CEO of Volta Data Centres in the summer of 2012, when Volta took over the former Reuters facility on Great Sutton Street to redevelop it into a brand new, state-of-the-art data centre. The facility was formally opened by Deputy Mayor Kit Malthouse in September 2013, by which time Volta's data centre had undergone a complete refit which included a significant power supply upgrade, now being fed at 33kV from two separate substations of the national grid.

Matthew is a finance and property investment professional with over 16 years' experience in acquisitions, fund structuring and management, strategic asset management, corporate financing and restructuring. A Chartered Surveyor, Matthew previously worked for Chelsfield plc. Whilst at Chelsfield, he was appointed to the main board of Global Switch to implement corporate restructuring and business turnaround across its 3 million square foot data centre portfolio, located in London, Paris, Amsterdam, Frankfurt and Madrid.

Utilising profiling technology to drive the business case for data quality

There is a lot of commentary in the market today around the perception that data quality has finally moved up the corporate agenda to become a board level priority, Experian Data Quality reports

BUSINESSES NOW ACKNOWLEDGE THAT GOOD QUALITY data fuels a successful organisation, be it improving operational efficiencies, delivering a high quality customer experience or securing a profitable business. Growth rates in the data quality technology industry certainly seem to ratify that fact with investment being made globally

However, the reality is the business case for data quality is not always driven by altruistic plans, such as improved operational efficiency, customer service or increased revenue. Often data quality issues get noticed as a result of reactive problems, such as a fine from a regulator, or poor customer experience leading to negative press. Usually these issues occur too late in the day, where time constraints may result in a purely short term, corrective approach to data quality. The resulting strategy may focus on fixing issues after they have occurred, leaving little room for more proactive approaches that look at prevention.

If an organisation pursues a reactive data quality strategy and there is a culture of apathy that surrounds tackling the challenge of unlocking the value of corporate data, it can often be difficult to get improvement initiatives off the ground. Any data quality initiative designed in a silo runs the risk of delivering a poor return on investment as the value is contained to one department and lack of consideration to an organisation's broader data processes represents a potential concern in terms of diminishing returns.

To move away from a reactive approach to data quality – that can be a drain on resource and money - strong and effective business case is required. The business case for data quality should look beyond the present or limit itself to data silos. It should also try and extract maximum value from any solution, so that issues are prevented in the long term, and business resources are used to their maximum potential.

Most data quality issues are experienced by someone in the field, such as business users who have seen first-hand evidence of how poor quality data can impact business operations or performance. As part of your business case for data quality, you will want to build a clear picture of the scale, impact and cause of these issues, beyond verbal evidence

One of the most important technology tools you can leverage in this situation is that of data quality profiling. Software of this nature is used to understand the breadth and depth of data quality issues, often discovering challenges you were not aware of and then drilling down into what could be the root cause.

This technology can uncover the necessary evidence from data that would not be visible to the naked eye which can help you understand the link between data issues.

Discovering the scale

Data profiling can help you understand how extensive and pervasive an issue really is, taking you beyond verbal and circumstantial evidence of a problem, and into actual analytical evidence. Data profiling discovers issues that you were not aware of. You can use the technology to look for the same issue beyond the data you know, and expect to have problems in areas you were not aware of.

Profiling technology can help identify that potential

data quality issues are not just limited to one department or data entity, but present in other areas of the business, uncovering the true scale of the problem. This helps gain a broader business interest in fixing the data quality problem, and starts looking at solutions that present a larger return on investment, such as technology that can prevent the problem, with an increased chance of securing budget due to multiple interested parties.

Quantifying the impact

The next stage is to understand what these poor quality records are worth to the business. Traditional methods of quantifying data quality present the issue as a percentage of the total number of records. So an issue that amounts to only one percent of the total records may not be seen as a serious problem.

Using techniques for measuring data quality may also lead to a more reactive approach, fixing problems unless they snowball into a much bigger percentage before acknowledging a solution is required. It is likely that one percent of records with the data quality issue could represent a much larger chunk of your revenue generating business, for example, and may impact customers who have been loyal and expect superior customer experience.

By applying key business performance metrics as a measure when calculating data quality, you can sway the percentages to what they truly mean to the business. Evidence can be drawn out that a small percentage of records with a quality issue may be worth looking into if they impact the business in a significant way.

Without priority, data quality improvement can be blindly executed, where time and effort is spent to try and fix any and every problem. Linking quality to business metrics can reveal which data is more worthy of budget and resource when it comes to retrospectively fixing problems with quality.

Using data profiling software you can drill down into the detail of the poor quality records and segment out the data that is linked to the most impactful business metrics. Money and time saved using this approach, and can be invested towards preventative data quality

Finding the root cause

Data profiling software can also help in understanding why issues have been occurring in the first place. This is important when trying to find solutions that prevent the problem from recurring and may also point at root causes such as poorly implemented technology, people's apathetic attitudes to data quality or failing processes. For example, using data profiling software you can drill into the other factors such as the systems that produced the data, the users or teams who entered the data incorrectly, or other factors specific to your business such as product, customer lifecycle, region, etc.

Data profiling technology not only provides the evidence of poor quality data, but also gives you food for thought when it comes to investigating why issues occur. Using the findings from data profiling software, further investigation can be carried out into people, process and technology to truly eliminate the problem at source.

> Data profiling technology not only provides the evidence of poor quality data, but also gives you food for thought when it comes to investigating why issues occur

In Summary

Profiling technology can be a key enabler to your business case for data quality improvement. Businesses wishing to leverage profiling technology should considering the following key factors:

1. Uncover the evidence of reported data quality issues by profiling data, preferably all data and not just a sample.
2. Discover the scale of the issues across multiple data silos.
3. Understand the relationship between poor quality data and business metrics.
4. Identify the channels that are driving inaccuracy.

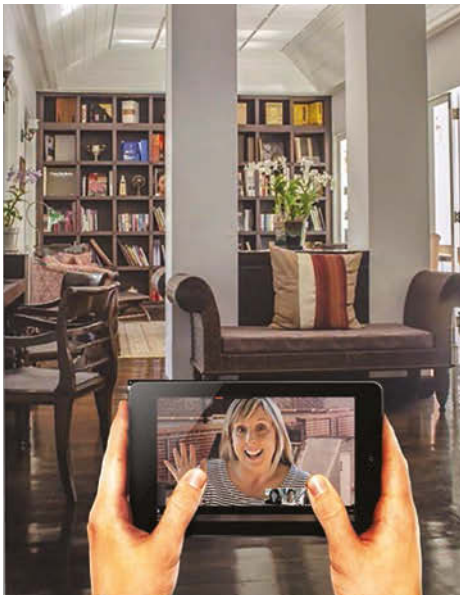
Further information

This new Experian Data Quality advisory note delves into the role profiling technology plays in uncovering the bigger picture and building the business case for a more effective data quality initiative.

This note provides food for thought and can help organisations make that all important move, away from a reactive approach to data quality. Reactively dealing with data quality issues can be a drain on resource and money thus a strong and effective business case is required.

Experience true collaboration from Google...

...and transform the way you work – **forever.**



To understand how Google and Devoteam can transform your business processes and empower collaboration throughout your enterprise, please contact

David Bartoli on
07507 572777 or at
david.bartoli@devoteam.com

Today, web and device innovation keep us all connected. But many hurdles to true collaboration remain for remote workers.

Google's revolutionary **Chromebox for Meetings** is the long-awaited solution. It unlocks working-in-parallel with real-time collaboration like you've never seen before.

From now on, executives, colleagues, suppliers and customers can all experience the power of working together, face-to-face, on the same content, without the high cost of in-room systems or time wasted on travel.

Why not take part in an interactive business case development scenario where Google and **Devoteam** will show you the power of connecting all of your teams, all of the time in a truly collaborative way, using Google technology?

Once you've experienced high velocity collaboration from Google you'll be ready to lead change in your organisation.

Going Google is easier than you think with over five million companies currently experiencing the benefits of Google Enterprise.

Chromebox for Meetings
the *new* gold standard for collaboration pioneered by Google

Google APPS AUTHORIZED ENTERPRISE RESELLER

DEVOTEAM
Consulting • Solutions • Expertise

Apps: development, deployment, security and more

Brian Runciman MBCS looks at the current app market and implications for the enterprise, developers, security pros and more

THE NUMBERS ARE HUGE: 1,000,000 apps on the Apple store was passed in late 2013, with over 60 billion individual apps downloaded.

There are 1.1 million Android apps available, along with 160,000 or so Windows Phone apps. Mobile apps are everywhere: making consumers' lives easier, offering new career paths to developers, offering new ways for enterprises to interact with customers and suppliers and bringing complexity to the IT landscape for security experts. The impact off the app is huge so – how to deal with it?

The thriving app industry is one that has a huge impact on the enterprise, even if at first glance it looks like a mainly consumer phenomenon.

As apps are so simple to use they have invaded our lives exceptionally quickly. They are approaching the intuitive software the industry has long promised and so will continue to impact the enterprise world whether those involved with corporate governance, IT and mobile support like it or not.

The experience that people have with apps – their intuitiveness, clean design and responsiveness – affects how they want to interact with IT systems in the workplace.

For developers there are huge opportunities. Traditionally powerful vendors of enterprise software like SAP and Oracle don't dominate in the mobile app market. Small agile organisations with a good idea can make a big impact. And this, as Edward Hadley points out in a blog post for app platform supplier Mendix.com, means 'the notion of the single, monolithic system is losing favour in the enterprise.

> CIOs and IT directors need to consider the impact of apps on their enterprise application strategies and end user expectations

'While a lot of those systems will continue to be used for managing core processes behind the scenes, business users today are bringing this app mentality into the enterprise with multiple, lightweight apps that address specific needs – most of which can't be addressed with packaged applications.'

All this means that CIOs and IT directors need to consider the impact of apps on their enterprise application strategies and end user expectations; developers have a lot of careers options, marketers have new ways to get to their markets and any number of industries will undergo interesting and disruptive change.

Defining apps

The definition of 'app' is not as straightforward as it first appears. Oxforddictionaries.com calls an app 'a self-contained program or piece of software designed to fulfill a particular purpose; an application, especially as downloaded by a user to a mobile device.'

So an app is simply a piece of software that does something other than run the machine it's on – something of use to a user beyond the system software or the operating system itself. But as the latter half of the definition indicates the meaning has morphed to something more specific in the consumer world. Although any IT person knows that 'apps' are more than just shiny small programs on a mobile device, common usage has made that almost a default meaning.

The phrase 'killer app', which we can define as an exceptionally useful piece of software that was unique to a platform, harks back to a more traditional definition.

In 2011 when Apple brought a case against Amazon over the use of the phrase 'App Store' it wasn't just the use of the word 'store' that was the problem. Apple knew how consumers in general defined 'app.'

Apps of course can run on the internet via a browser, on your desktop or laptop computer or on a phone or other electronic device. Web apps are typically written with HTML, JavaScript or other web-native technologies. Mobile apps, which come in a huge variety, are authored in C, C++, Javascript, HTML5 and more.

The functionality of mobile apps increases with mobile device capabilities – now including software with map functionality, using wifi to improve geolocation services; utilising orientation via the gyroscope; near-field chips; different touch combinations; linking in with cloud storage and more.

Enterprise App Stores: turning IT into rock stars – without the celebrity hangover

By **Flexera Software**

YOU KNOW THE MOOD IN THE corporate world is 'optimistic' when enterprises shift their focus from 'down to the bone' cost cutting measures to enhancing operational efficiency and innovative projects. 46 per cent of CIOs report increases in IT budgets in the last year to fund projects that improve the effectiveness of their operations, a recent survey by Harvey Nash highlights. This is indeed good news.

Technology-led as we are today, innovation in the enterprise is to a large extent being driven by software applications – look at the consumerisation of IT, virtualization and cloud trends. To better connect employees to the world of business applications, organisations are setting up enterprise app stores, giving employees iTune-style access in the corporate environment.

While both employees and organisations benefit from enterprise app stores, there are risks and rewards for the organisation. IT wants to look like a rock star – delivering technology that employees love and use every day. But at the same time, IT doesn't want the hangover effect – the major headaches that ensue when the enterprise app store rollout is not thought through and executed properly.

What can IT do to ensure its celebrity status without the painful fallout?

Reducing license compliance risk from Enterprise App Stores

First is the issue of software compliance – the requirement that an organisation restrict usage of an application to the terms and conditions in the software contract. Greater employee access to applications via an app store means potentially broader use, and therefore greater risk of inadvertently falling out of licence compliance.

Software license noncompliance creates great risk and cost exposure for organisations. Most software vendors have the right, built into

their contracts, to audit their customers' use of their software and if non-compliance is found, vendors will issue an invoice (true-up) for licenses the organisation is using but has not paid for. Often times, in addition to the true-up bills, penalties can also be incurred. Because true-ups are unbudgeted, paying these fees can create a rock star-sized hangover by draining funding for other IT projects.

A survey prepared jointly with IDC looking at software licence management, shows that already businesses are paying unbudgeted software licence true-up (balancing) fees in excess of £1 million. This figure could potentially be even higher with applications available 'on tap' through app stores. That's a major headache.

On the other hand, if enterprise app store initiatives are executed properly, they can deliver their desired benefits while actually reducing licence fees and costs.

Fundamental to organisations' success delivering consumer-friendly enterprise app stores will be their ability to streamline the front-end and back-end IT infrastructure. IT must integrate the app store with back-end software licence optimisation and Application Readiness (i.e. compatibility testing, remediation, packaging, deployment readiness) processes, across the lifecycle of every single application. This will ensure that employees have timely access to a well-stocked repository of applications from any device, anytime, anywhere – while pre-empting unexpected risks and costs of unforeseen software usage.

The number of licences a company has rights to, and the specific manner in which those licences are entitled to be used – i.e. its licence position – plays a key role in managing an enterprise App Store. If an enterprise issues licences it doesn't have, or those licences are issued in violation of specific entitlements in the licence agreement – the enterprise can expose itself to penalties.

The enterprise App Store should provide safeguards preventing access to and download of applications that are unavailable due to licensing and entitlement restrictions. With built-in App Store capability to alter the approval process based on ever-changing usage of applications, licensing requirements and entitlement rights; enterprises can adapt quickly to licence availability limitations and prevent non-compliant use that would subject them to software licence audit risk.

Organisations that have integrated their enterprise app store with their software licence optimisation systems are much better armed with the tools necessary to make real time decisions around licensing. It also allows faster business decisions and more sophisticated cost controls. And it provides the end user access to applications without increasing audit exposure risks due to non-compliant use.

An app store integrated with back-end software license optimisation processes and technology also provides for much more efficient license reclamation or reharvesting – the process of reclaiming applications that aren't being used by certain employees, so that they can be redistributed to those that actually need them. This enables the organisation to save costs while avoiding having to purchase new software licenses when perfectly good unused licenses are waiting to be reharvested.

Manual processes for determining software use and reharvesting unused licenses are cumbersome and time consuming – and therefore will fail in most organisations. Implementing automated systems to determine reharvesting candidates and reclaim unused licenses is the only practical solution for most organisations. An enterprise app store should offer functionality to automate the reharvesting process.

With these fundamental systems in place, the enterprise App Store will deliver the feel of consumer App Stores that end users are comfortable with – and the organisation will simultaneously ensure central accountability and control.

One NHS Trust is a good example of an organisation that has accomplished this. The Trust's vision was to empower users to request, obtain and consume applications without needing IT services, and make those applications available to users on their device-of-choice.

To improve patient care, the organisation has built a system whereby clinicians can access the applications they need, when they need and on a device (iPad, smartphone or any other) of their choosing, increasing their efficiency. Today, a clinician can get an app within 15 minutes – previously it used to be days. As a result of end-to-end automated processes, the Trust also has complete visibility into, and control of IT assets, helping reduce ongoing software costs and while optimising existing licences for software purchased.

Partnering with employees in reducing software costs

With users demanding the freedom to choose their applications with an enterprise app store, ideally they can be empowered to partake of the responsibility for licence compliance and waste reduction too. Businesses now have the ability to design their enterprise app stores in a way that gives employees visibility into the usage and cost of software licences installed on their devices – so that they understand the true cost of the applications they're using, and don't inadvertently hold on to applications they don't need or use applications outside of the compliance guidelines.

For instance, alerts can be sent to users notifying them of policy infringements such as when an application hasn't been used for a specified period of time (say six months), or if there is no record of a licence associated with software found on an employee's device. Similarly, to encourage employees to optimise their software licence usage, software policy scores can be granted indicating how closely applications installed on their devices comply with corporate policy.

Enterprise app stores can be a vehicle to make IT look like rock stars – getting applications to employees in an environment as intuitive and friendly as the consumer-based app stores they're already used to. But unless IT take the necessary steps to tie together the back end with critical processes to ensure accountability and control – that rock-star status might also come with a celebrity-sized hangover as well. Best to avoid the hangover altogether and do the planning today to ensure a smooth and effective rollout.

Many Devices.
One Solution.

Absolute® Software

TRACK. MANAGE. SECURE.

Absolute Software provides endpoint management and security for all of your desktop, laptop, tablet and smartphone devices – regardless of user or location.

Optimise productivity, reduce operating costs, prove compliance, and remotely secure all of your devices and the corporate data they contain.

absolute.com

UC: making your professional communications more personal

By **Daniel Fuller-Smith,** Sales Manager of Toshiba Unified Communications Division

TODAY'S WORLD IS INCREASINGLY social. The rise of social media platforms, technologies such as 4G and app markets, and devices including the smartphone and tablet have placed us in a constantly connected environment. We can interact with our friends, families and even our favourite celebrities and brands whenever and however we want to. The smartphone in particular is central to our day-to-day lives – we can access email, contact one another through apps such as WhatsApp and Skype, and of course make calls and send texts wherever we are.

It has never been so easy to stay in touch with such a vast array of platforms at our fingertips. For example, if one friend prefers WhatsApp yet others are more active on Facebook, it's simply a case of a couple of taps on a smartphone screen. Yet when we think of how seamless such conversations are in our personal lives, it begs the question why, when it comes to professional communications, businesses are not acting at the same level?

This is where Unified Communications (UC) comes in – a system to integrate the range of business communications platforms staff use each day to ensure maximum productivity. UC offers customer service advantages across all channels, from deskphone to instant messenger and video, so it is about time that CIOs started to think about how they can introduce it to their company and create a more seamless way for their staff to communicate regardless of their location, or the device or platform they are on.

Enhanced productivity

The most significant gains that UC brings are in the realm of productivity. Every company wants, and probably needs, to be more productive – UC adds functionality that enhances efficiency regardless of business size or sector. Even seemingly small perks demonstrate this value – for example click-to-dial allows users to call a colleague or customer through their PC rather than by having to manually punch a number into their deskphone or mobile, due to the integration between their contact book and PC. Similarly, when making or receiving a call, data connected to

the number can be automatically displayed on screen so that the employee has all of the information needed to offer the highest level of service, from who is calling to details of the last interaction and location data. The School Information Management System (SIMS) is a prominent real-life example of how this works, as it enables school offices to manage and vet calls based on the information stored within the system. For example, if a parent calls for information about their child, the staff can immediately see if they are allowed to share this information with the person who is calling.

In many respects, UC can act as an equaliser, levelling the playing field for those smaller businesses that do not have the manpower or budget to offer dedicated customer service teams. As mentioned earlier, we, as consumers, are mobile, always on, and ever-connected, which means that we expect a more dedicated, real-time service from the companies we deal with.

Take, for example, an independent estate agent. Integrating a UC platform enables its staff to receive and respond to enquiries from clients even when out of the office. In an industry where being mobile is central to the role, providing customers with these numerous touchpoints is of paramount importance. With UC, employees can be waiting to show one customer a potential house and still responding to incoming enquiries from others at the same time. By integrating the deskphone with smartphone and email, calls can be automatically transferred, with voicemail messages being sent via email or text straight to the device of the employee. The downtime that takes place during viewings and travelling can thus be transformed into productive periods that also boost customer satisfaction. Ultimately a business that responds to its customers within minutes will win the clients off one that takes hours – such is the level of expectation today.

More than anything, it is through making this 'dead time' effective that businesses will really see the impact of UC. Mobility is a continuing trend within the UK workforce, so the ability to contact colleagues, customers, partners and other stakeholders regardless of location is more important than ever before. With an integrated UC system, working from the train or even from home is as simple and productive as being in the office itself.

The mobile office – integrating UC with hardware

An example of a small business reaping the benefits of UC in this way is charity Go ON UK. This organisation is dedicated to making the UK the world's most digitally skilled nation, by educating individuals and organisations on the benefits of the digital age. Its small workforce is almost entirely mobile as it focuses on driving the campaign throughout the country, so using UC services alongside devices built for mobility has been essential in the charity's growth and the success of its projects.

The built-in 3G slot in a mobile business laptop enabled a consistent internet connection for GO ON UK's staff regardless of location, allowing them to remain productive while on long train journeys and away from WiFi access. This gave the team access to Outlook for ongoing communication, but also Skype and Sky Drive to ensure they were able to communicate with their teams while away from the office. Tying UC into these devices also equates to enhanced security for businesses. Built-in mobile device management (MDM) solutions ensure that devices remain safe and data is protected in the case of theft or loss.

Value

ROI is a major stumbling block for UC adoption in the UK – businesses aren't prepared to invest without receiving immediate returns. According to Frost and Sullivan, 80 per cent of companies are looking for a return on UC investment within two years, while 25 per cent expect it within just six months. In tough economic times, this was somewhat understandable, but those businesses that took the risk have realised that, while ROI in six months isn't realistic, UC's long-term value makes it more than worth the cost.

UC is a reliable, long-term investment, with installations lasting from seven to ten years – businesses need to understand this before writing it off as unaffordable and unnecessary. Rather than expecting immediate ROI, companies can ensure they will get value for money just by researching the vendor, reseller and product roadmap. UC is scalable, so it can grow with the company if a business buys into a reputable vendor and reseller, while the ability to build in applications as and when needed is just another way in which UC enhances productivity and adds value.

With developments such as Federation, which enables an even greater level of cross-platform integration, as well as the rise of video conferencing, the time is ripe for UK businesses to adopt and benefit from UC. Technological innovation has only led to heighten the value that UC can bring to organisations, so companies of all sizes and across all sectors need to embrace it sooner rather than later or they risk being usurped by rivals. Of course, there is responsibility on the part of vendors and resellers to educate customers on what UC brings in terms of productivity, value and ease of use, but there is also an onus on those businesses and CIOs to keep ahead of such IT trends and implement a UC system that is suited to their organisation, and can keep them at the forefront of business innovation.

Further information

As one of the world's top ten providers of telephony and business communications solutions, Toshiba offers a comprehensive portfolio of communication systems and applications – each designed to support businesses as they build and maintain customer relationships, drive productivity and maximise profitability.

With a 130-year pedigree in telecoms, Toshiba's Unified Communications product range spans every aspect of business communications – from handsets and basic telephony systems through to remote working solutions, advanced IP-based unified communications servers and contact centre systems.

Be Free.

BE WIRELESS!

PortHole III is the new in desk, wireless charging module from CMD Ltd - connecting directly to the mains power supply to provide wireless charging in any commercial and public spaces.

Features

- Compatible with all wireless enabled and wireless ready devices
- Sound and light system that lets you know when charging begins
- Automatically turns off when charging is complete
- Stylish design available in a choice of three colours
- Easy fit system designed to fit any surface installed with an 80mm grommet hole

with wave™ technology..

t 01709 829511
e marketing@cmd-ltd.com
w www.cmd-ltd.com
/cmdltd
@cmdltd
company/cmd-ltd

cmd

Redefining device management

By **Stephen Midgley**, VP of Global Marketing, Absolute Software

IF WE TAKE A LOOK AT THE MOBILE DEVICE management (MDM) landscape, it's hard to believe that only ten years ago built-in Wi-Fi was just an option on laptops. And while mobile connectivity and simply the invention of laptops irreversibly changed the endpoint management landscape, at this stage companies were able to maintain control of data and devices through simple but strict restrictions via the likes of client management software, VPNs and restricted admin rights. Similarly, BlackBerry offered the same fenced-in, one-size fits all approach for managing smartphones.

The iPhone entered the market in 2007 to great fanfare. While it would eventually be a significant cog in the mobile working machine, it was actually the launch of the iPad in early 2010 that significantly moved the goal posts in terms of managing a network of devices. The iPad immediately became a favourite of senior management who had no qualms about jumping the queue in IT to get their latest toy supported. This led to the Apple MDM API and a trickle-down effect that quickly became a deluge of bring-your-own-device (BYOD) users.

Suddenly, the strict policies that protected the more basic and static devices of yesteryear were now neither relevant nor possible. Instead, what existed was a whole fleet of devices that were no longer owned by the company, and to add to the confusion, the act of limiting the type of device an employee could use and where they could take it quickly became perceived as old fashioned and draconian.

This scene was the origin of the struggle to define best practice for MDM and client management. Most CIOs will testify that this struggle has increased exponentially as devices and data become more common, mobile, complex and valuable. Indeed, this has spawned a number of models for mobile working – BYOD, CYOD, COPE – all of which are nuanced enough to account for varying employee preferences, but at the same time, they all bring their own set of MDM challenges.

A new MDM landscape

So where does that leave us now? With all these MDM models creating a moveable feast, how do IT decision makers create best practice to protect a business's data on personal and corporately owned devices?

Firstly, it's important not to focus solely on devices – let Apple, Samsung, and Microsoft do that. Instead, CIOs should build policies around how these devices will be managed and there are three main drivers to the new management landscape:

1. **The typical user relies on more than one device and for the foreseeable future; one of these devices will be a computer.**
   This means that MDM cannot replace traditional client management technology. Instead it must complement and coordinate with it. Ideally it will be an integrated part of the same infrastructure. This perspective is supported by leading industry analysts who agree (in a rare moment of consensus) that separate management frameworks for different form factors is unsustainable in the long run. Ultimately, the practices and tools for client and mobile device management must converge.
2. **As the price of the hardware has come down, the value (and portability) of corporate data has gone up.**
   This has introduced entirely new risks or emphasised existing hazards. After all, companies that allow Outlook Web Access from employee-owned computers are facing no greater risk when they provision email to employee-owned smartphones. But the risks are real and they've become one of the biggest considerations when it comes to device management.
3. **It's not only about the device… it's about the user getting what they need when they need it.**
   As ownership has shifted to the end user, it's become increasingly clear that it doesn't really matter if they are using a laptop, tablet or smartphone. They just want to have their stuff. Users want to be productive on the devices they've chosen, regardless of operating

system or form factor. And if you don't help them, they will help themselves. This is a problem when you have strict policies because the more troublesome the restrictions, the more likely the user will be to circumvent them – not maliciously, but simply in order to get the apps and data they need to be productive.

Add this up and it points to a new management paradigm that is user-centric, not user-restrictive…an approach that focuses less on the device and more on security for corporate data and apps. It's not about BYOD, CYOD, COPE, or any other acronym. In the end, it doesn't really matter who owns the device – instead IT should focus on who is using it and how. A policy-driven, user-centric framework will adapt easily to this approach.

Implementing MDM

The best approach to MDM can only be determined by your specific requirements for security, regulatory compliance, and the business. Fortunately, many highly secure options are available that can be tailored to account for all these factors. Persistent endpoint security provides the ability to track and secure all the devices in a deployment. Laptops, tablets, and smartphones can be remotely managed and secured to ensure — and most importantly prove — that endpoint IT compliance processes are properly implemented and enforced.

You have to get it right

There is a broader picture beyond the need to cater for employee device habits. Data on devices is valuable because in the wrong hands it can cause myriad problems. A competitor could use profit and loss information to gain an advantage. One employee could gain access to another employee's personal information, such as salary, review notes or confidential information from their private lives. Data could be leaked, leading to regulation or compliance breaches. This is just the tip of the iceberg – it's probably not hard to imagine certain types of data within your organisation that would cause harm on a number of levels if it fell maliciously or accidentally into the wrong hands.

There are moves to protect against this on a macro level. In March the European Parliament approved the draft Data Protection Regulation. This regulation will replace the Data Protection Directive – legislation written in 1995 that has become dated in its attempts to deal with social media and the cloud. The document will 'create greater harmonisation across member states' by giving more power to the users of online services, increasing regulatory enforcement and focusing on transparency in the way data is used and shared. It also proposes stronger safeguards for EU citizens' data that gets transferred abroad. However, there will be the expectation that business will adopt more proactive governance structures to manage privacy risk, and it considerably increases the fines that can be imposed on companies that break the rules.

And the fact is huge penalties for losing data exist. The ICO can fine companies up to £500,000 for breaches of the Data Protection Act. Indeed in March, data protection law specialist Kathryn Wynn of Pinsent Masons claimed the UK government should consider raising the level of fines that the ICO can impose, as it would reinforce the importance of data security. Regulators are also now proposing fines up to five per cent of global corporate turnover.

The bottom line

We're shifting to a new understanding of endpoint management; a policy-driven, user-centric framework that accounts for data, apps and security across multiple operating systems, form factors, and owners. It's not about the device, it's not about the acronym for working with the device – ultimately it's about being able to manage and control the data flowing in and out of the device. This is what CIOs should focus on, and even though it will continue to be fashionable to invent new device management models, it's important to see through this by focusing on the data. Once past this, it becomes simple to implement un-restrictive policies by using software to account for data, and at the same time tallying with employee device expectations.

It's vital businesses strike a balance with MDM. Allow employees to use the devices they want to work in the way they want, but ensure policies are in place that can track and manage the data stored within and accessible from these devices.

Further information

Absolute Software is the industry standard for persistent endpoint security and management solutions for computers, laptops, tablets, and smartphones. As IT security and management requirements have converged, we've responded by providing our customers with a consolidated experience, allowing them to manage and secure all of their endpoints regardless of user, location, or form factor. This singular view of the IT landscape is extended to include IT processes and infrastructure with our IT service management offering.

3 essential skills for Today's CIO

In order to fulfil their promise as leaders in a digital world, CIOs should ensure they have the financial and change management processes to work effectively with the C-Suite. **Jonathan Walls**, Principal Consultant at Upland Software, explains

THESE ARE TREMENDOUSLY INTERESTING TIMES to be a Chief Information Officer. To quote Marc Andreesen back in 2011, "Software is eating the world". Every business process is being digitised in whole or in part. They are accessible online and on the go.

At the same time, well-covered trends are upsetting the IT boat. From the invasion of the enterprise by consumer devices to the flanking of technology departments by cloud vendors, there are a growing number of routes by which your fellow executives can procure their digital capabilities.

The CIO role is not going to disappear due to pervasive technology, any more than the CFO role is about to disappear because everyone manages a budget. Nonetheless, the success of the cloud in particular presents a great opportunity for CIOs to raise their profile and relevance (or watch it fade).

Business divisions can often start a new initiative with a cloud solution. They no longer have to procure hardware or hire an army of sysadmins. Rather than assess and satisfy technology requirements, the goal is now to ensure a successful outcome for those initiatives.

Your peers in the C-Suite remain unsure about what opportunities technology affords them. They still rely on their CIO for advice and support – if they feel their CIO is the right person to turn to.

This raises a question: What are the skills a CIO needs to play a leading role in their enterprise? Here is my top three:

- Building trust through transparency
- Building credibility through delivery
- Shifting from negotiations to collaboration

Building trust through transparency

It is trite but true to say that a leader needs to be trusted. Of particular concern is that financial misunderstandings cause tension in the strongest of business relationships. The worst kept secret in IT departments is their financial processes are often based on manually maintained, error-prone spreadsheets. That holds true for budgets in the hundreds of millions – even billions - of pounds of annual expenditure.

Consumers of IT services struggle to relate the services they use to how much they pay. Usually there is a simple reason for this: even the CIO does not know how much it actually costs to run a given IT service. That makes them impossible to price correctly, and impossible to invoice via a production process.

Managers will recognise the consequences: tense conversations, attempts at side negotiations, meetings with multiple conflicting spreadsheets. The central problem: more time is spent on trying to understand the past than make plans for the future. Supposedly retired apps live a zombie life. Low priority applications are left running on expensive hardware. Application rationalisation initiatives fail or don't even start, because the time isn't available for the hard work of rationalising the associated business processes.

No matter how strong the personal relationships you build, the best way to build real trust between departments is an IT Financial Management (ITFM) process that publishes service costs transparently. Think "WYSISWP", or "What You See Is What You Pay". **With an IT Sub Ledger and a Bill of IT that breaks down IT costs by service line, managers can see what they are paying for**, how much of it they used, and the price per unit consumed.

Transparency is best delivered via the intranet: published figures that can be accessed online like any other business application.

Building credibility through delivery

Credibility is a close relation of trust. IT still carries a reputation for delivering late and over budget. As with financial matters, concerns about future IT failures can also lead to management overhead. It can also lead to bad decisions, such as going around IT and ending up with redundant applications.

Service cost transparency manages the 70 – 80% of IT spend that goes to Running The Business, while project expenditure typically accounts for the remaining 20 – 30% for Changing or Transforming the Business.

30% of the annual budget is significant in its own right. Innovation has a high profile: in business models, in product design, and in operational processes. Your success tomorrow is likely to come from today's new cloud services and application rollouts. **Adopting a Project and Portfolio Management process significantly improves their odds of success.**

The most popular source of innovation information for today's "Digital Executive" is online. Those seeking a strong, credible reputation for delivering innovation will benefit from an online system for capturing ideas and reporting on the performance of projects and programmes.

In the ongoing cycle of balancing supply and demand, I find it useful to think in terms of 6 A's:

- **Acquire**
  Proactively engage with other departments to capture ideas and demand
- **Align**
  Assess, filter and prioritise proposals and work into investment portfolios
- **Allocate**
  Agree budgets and assign people to projects and tasks
- **Act**
  Execute work using project management, agile development, and collaboration tools
- **Assure**
  Track financials, project status and benefits realised
- **Attract**
  Promote the value delivered and goals achieved to your customers

The CIO should recognise the importance of their personal engagement in the Acquire and Attract stages: never underestimate the value of reaching out to a colleague on the phone to discuss their ideas and outcomes. Sitting down with a coffee and a print out can make all the difference.

This is not purely for the benefit of your colleagues. Many CIOs, particularly those new to the role or the company, struggle to understand what their staff are working on. **By instilling the discipline of managing IT as set of investment portfolios, you have valuable information regarding future performance**: staffing and skills shortages, projects with budgets at risk, and new work in the pipeline that isn't aligned to an agreed goal. Simply identifying overlapping activities can reveal significant savings.

Shifting from negotiation to collaboration

The third critical skill is the one that is perhaps receiving the most attention: the ability of the CIO to earn "a seat at the table". They not only represent their department during budget negotiations and IT reviews, but influence the thought processes and investment decisions of their colleagues.

Cost transparency is consistently the best starting point. Different CEOs will look for different things from their team. Some things don't change, though: they like an executive with a firm grasp of the numbers which describe their world.

It's good to have a reputation for getting projects done, or even done on time and on budget. T**oday's CIOs should also be "digital pathfinders", helping guide other executives through the intricacies of building out a digital strategy.**

Good decision making demands a balanced approach: both long-term and short-term, combining bottom-up with top-down. The CIO needs to be able to simultaneously present her budget in broad strokes, and to give precise details of particular services. One minute she might be making the case for shifting the sourcing strategy from 3rd party hosted applications to an internal private cloud. The next, giving a pounds-and-pennies explanation for why the field staff have been given a particular model of mobile phone.

To have such a breadth of information to hand, the only answer is to implement a holistic approach to reporting. **Integrating processes such as ITFM and PPM enables the Office of the CIO to perform closed loop budgeting and rolling forecasts, combining the finance, technology and business perspectives.**

The digital executive

Our perennial goal is to run IT like a business – and business is always changing. Speak to anyone in sales or marketing, and they will tell you about the increasing sophistication of the customer. Executives now expect to be able to perform their own research online. Proactive visibility is necessary to get their attention and hold their trust.

Today's leading CIOs do not just run a tight ship, investing in the best business initiatives. They are proactive, collaborative leaders that help shape the business strategy itself.

Author information

Jonathan Walls is the Principal Consultant, EMEA Region, for Upland Software. Over a 15 year career, consulting for solutions like HP PPM and Apptio, he recognises technology leaders' biggest challenge lies in understanding true cost drivers and effectively managing change and transformation programmes.
Linkedin: www.linkedin.com/in/jonathanwalls

Upland Software helps organisations do the right work, the right way. They are the leading provider of cloud-based enterprise work management applications, enabling organisations to focus resources on strategic priorities, and empowering those resources to execute flawlessly. Their product family includes Comsci (ITFM), PowerSteering and EPM Live (PPM), along with other complementary tools.
Website: www.uplandsoftware.com/

Oasis™ Indirect Evaporative Cooler is key to advanced cost efficiency for Data Inn Lithuania

Data Logistics Center's Data Inn in Vilnius, has installed Munters' award winning Oasis™ Indirect Evaporative Coolers (IEC) to deliver super energy efficient cooling with a PUE of 1.3, for its high quality, secure data services.

The new Data Inn facility is generating and storing large amounts of data for commercial banks, telecom operators and service companies, and is on track to become one of the largest and most advanced Tier III data centres in the Baltic States certified by the Uptime Institute.

The 3,200 m² energy efficient Data Inn facility will at full load cool 2.5 MW, with the capacity to operate more than 10,000 servers, all working in a 18-27°C climate, as recommended by ASHRAE.

The modular design allows capital investment to be phased as data centre facilities grow, with the systems reducing not only energy running costs but also capital costs on mechanical refrigeration, switchgear, generator sets etc., by 25%.

Data Inn Product Development Manager Edvinas Bakanas, says

"The Lithuanian electric energy sector, data communication operators and biggest Lithuanian banks, need their data to be safe and accessible without any interruptions, whilst employing cost effective and eco-friendly solutions."

"Munters cooling solutions enable us to achieve a PUE of 1.3 or less, which will make us very cost-effective and competitive in the market. Every 0.01 reduction in our PUE represents an energy saving of approximately 210,000 kWh in our data centre"

- **Data Centre air fully separated from outside air**
- **65% lower energy than common free cooling solutions**
- **25% reduction in refrigeration,**
- **Low PUE**

www.munters.com/datainn
airtreatment@munters.com
+44 1480 410223

Munters
Your Perfect Climate

IT Service Excellence from Devoteam offers you an opportunity to showcase your IT to the business and drive innovation.

Our 2,000 consultants have the technical & business experience to help you transform IT

How can you exploit this opportunity?

For over 20 years Devoteam's Peter Hoygaard and his team of specialists have been helping UK organisations realise tangible IT Service Excellence.

Take advantage of our advisory and consultancy services. Call us on 020 3574 4572, quoting **'CIO-Jun14'**, for a free assessment of your IT service transformation strategy.

Alternatively, contact Peter at **peter.hoygaard@devoteam.com**

DEVOTEAM
Consulting • Solutions • Expertise

Are cables a thing of the past? Is induction the new buzzword!

By **CMD Limited**

UNLESS YOU ARE PARTICULARLY organised and good with cable management, you probably have a few dusty power cord tangles around your workplace. You may have even had to follow one particular cord through the seemingly impossible snarl to the outlet, hoping that the plug you pull will be the right one. This is one of the downfalls of electricity. While it can make people's lives easier and in this fast paced technology driven world we can't live without it, it can add a lot of clutter in the process.

In the workplace, it is the responsibility of the business owner to provide a safe working environment, so that the employees can carry out tasks safely in the vicinity. Employees must be trained to use the equipment correctly to prevent any unnecessary risks. But why is electrical safety considered so important? Electricity is dangerous as you in the trade well know. Electricity always seeks the shortest path to the ground, usually through a conductor; so because the human body is around 70% water, this makes it a suitable route for electricity to take. Thus if a bare, live wire is touched by a human, electricity will pass through that body to the ground causing electrocution as you will know only too well. Electrocution as you know can be mild, depending on the voltage of the object; however a small amount of electricity if passed straight through the heart, even as little as 100-200 milliamps, can kill a human.

So with this in mind, scientists have been seeking the holy grail for many years now trying to develop methods of wireless power transmission that could cut the clutter or lead to clean sources of electricity. While the idea may sound futuristic, it isn't particularly new. You only have to consider the Serbian American inventor and electrical engineer Nicola Tesla who proposed theories of wireless power transmission

in the late 1800s and early 1900s. Tesla gained experience in telephony and electrical engineering before emigrating to the United States in 1884 to work for Thomas Edison in New York City. Tesla went on to pursue his ideas of wireless lighting and electricity distribution in his high-voltage, high-frequency power experiments in New York and Colorado Springs and made early (1893) pronouncements on the possibility of wireless communication with his devices. One of his more spectacular displays involved remotely powering lights in the ground at his Colorado Springs experiment station.

Tesla's work was impressive, but it didn't immediately lead to widespread, practical methods for wireless power transmission. Since then, researchers have developed several techniques for moving electricity over long distances without wires. Some exist only as theories or prototypes, but others are already in use. If you have an electric toothbrush, for example, you probably take advantage of one method every day. The wireless transmission of energy is common in much of the world. Radio waves are energy, and people use them to send and receive cell phone, TV, radio and WiFi signals every day. The radio waves spread in all directions until they reach antennae that are tuned to the right frequency. A similar method for transferring electrical power would be both inefficient and dangerous.

For example, a toothbrush's daily exposure to water makes a traditional plug-in charger potentially dangerous. Ordinary electrical connections could also allow water to seep into the toothbrush, damaging its components. Because of this, most toothbrushes recharge through inductive coupling.

Wireless charging solutions for the office, home and public spaces will soon be an everyday essential as we all become increasingly dependent on mobile devices. Even though it is early days with this technology, inductive charging is being built into an increasing number of Smartphones and tablets, (such as the Google Nexus 5 and 7) and we all have a part to play in helping to build the infrastructure to enable us to make use of this technology and continue its development. Did you know that we will also soon be able to charge our devices in cars: the technical committee of automobile manufactures, CE4A, has endorsed Qi (what is Qi I hear you ask? Qi is the wireless power consortium) as the worldwide charging standard for passenger cars. From 2014, Mercedes-Benz will be introducing Qi wireless charging technology into their vehicle range.

So what is the Wireless Power Consortium? Well the Wireless Power Consortium believe that wireless charging is a better way of charging, much more convenient than plugging in a wire with connector. They want to see wireless charging adopted in all battery operated products. They believe that wireless chargers must be compatible. Consumers don't value chargers that work with one phone and not with another phone so they want to establish a global standard for wireless charging that makes all wireless chargers compatible with all phones and other battery operated products.

However before we all rush out and get ourselves a new wireless charger you do have to be mindful that your device, whatever this might be, needs a certified wireless receiver built in or some kind of wireless charging compatible

technology – many mobile phone manufacturers now do this as standard very much like the universal power charger you get but you can literally buy the receive outright for as little as £5 and add to your device. You can then just place your device with receiver on a wireless charging product, a "handshake" happens between the charging spot and the receiver device, identifying the device and then beginning wireless energy transfer to the device. It is an intelligent system and will only send power to devices it has identified. Some new Smartphones and tablets already have wireless charging compatible technology built in as standard. We hope this technology will continue to be built into more devices in future; but for now, accessory cases can be used as mentioned earlier.

Further information

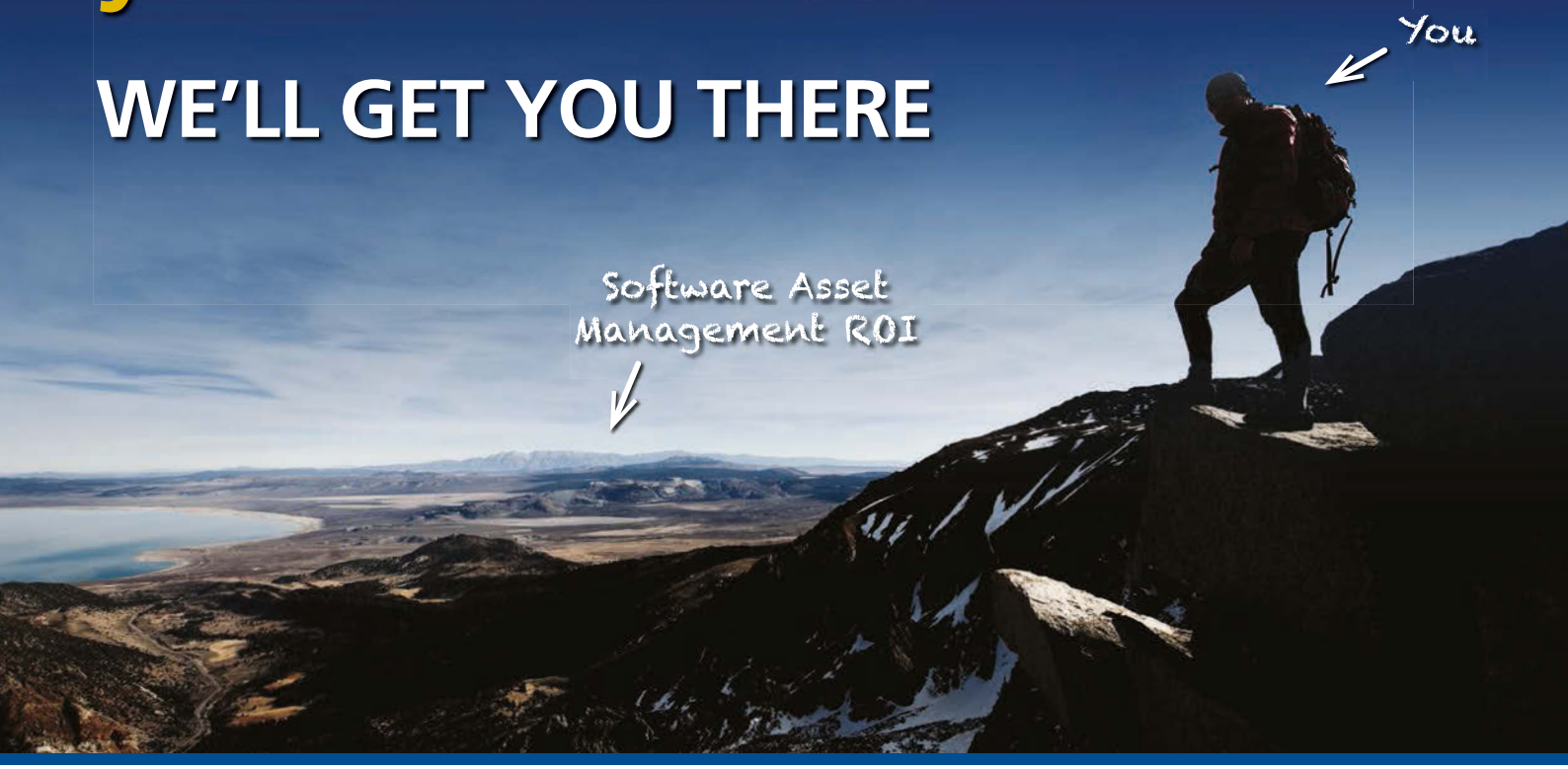
Companies like CMD have launched products like their PortHole III with Wave Technology that brings wireless charging to the forefront and CMS Ergonomics with their aircharge. Both products can be used at home or in the office, the aircharge comes with a 2m USB cable which is connected to a hub (which can be purchased separately) whereas CMD's PortHole III has an integral power supply, both delivering the DC 5V you need, both products can be retrofitted into an 80mm grommet hole which can simply be dropped in to enable easy charging.

Make the most of this new Technology
Although wireless charging is an emerging technology whereby a magnetic field in the charger transfers power to a receiver without using any cables. We know that as we become increasingly more dependent on mobile devices, powering them is always going to be an essential need.

Want to know more about these products that can help make that difference, why not talk to CMD who are British Electrical manufacturers, celebrating 30 years in the business this year. CMD also have a new catalogue out for 2014, or order yours on http://campaigns.cmd-ltd.com/2014/brochure_request/request.asp, call 01709 385469 or visit http://www.cmd-ltd.com or email marketing@cmd-ltd.com for more details.

STILL not seeing any value from your SAM solution?

WE'LL GET YOU THERE



FLEXERA SOFTWARE®

FlexNet Manager® Suite for Enterprises

Many organizations are struggling to get real value from their Software Asset Management (SAM) program.

Often there are issues with getting accurate inventory data across a wide range of platforms, including Windows®, Linux® and UNIX®, as well as virtual environments. Some organizations apply lots of manual effort to perform software identification using all that raw inventory data—just to determine what's installed on all of their computers. And many organizations have a hard time keeping track of and applying their license entitlements, even if they've already invested in a "license management" tool. That's because many tools on the market don't provide the automation necessary, at each step in the process, to achieve real business value.

If you've bought a license management solution but you are still not seeing much of a return on your investment, contact Flexera Software today. We've helped hundreds of companies realize significant savings on software using our market leading Software License Optimization solution—FlexNet Manager Suite for Enterprises.

For more information go to:
www.flexerasoftware.com/slo

FLEXERA® SOFTWARE

Indirect Evaporative Cooling provides energy efficient data centre heat rejection

By **Jon Pettitt**, Munters

THE IT INDUSTRY IS RESPONSIBLE FOR 3% OF THE world's electricity production (345Mw per year, 183m tons CO2) and the millions of instructions per second (MIPS) transmitted via today's servers create heat energy that requires removal to prevent overheating of data centre equipment.

Today's engineers are switching to Indirect Evaporative Cooling (IEC) to achieve a balance of reliability and energy efficient rejection of data centre heat.

The rising price of energy – coupled with a rising understanding amongst management of the social responsibilities that companies have in reducing their energy consumption footprint – means that data centre owners, their clients and managers have been revisiting power consumptions issues in a big way over the last few years.

In parallel with this, the data centre industry has developed a measure of how effectively a data centre uses its energy. Known as the PUE (Power Usage Effectiveness) this measure quantifies how much energy is used. PUE is defined as the ratio of total amount of energy used by a computer data centre facility to the energy delivered to the computing equipment.

According to data centre association the Uptime Institute, a typical data centre has an average PUE of 2.5 – this means that, for every 2.5 watts in at the utility meter, only one watt is delivered to the IT load.

Indirect Evaporative Coolers are applicable to data centres in almost any locale giving minimal need for air filtration and enhanced data centre supply temperatures resulting in partial Power Usage Efficiency (pPUE) of less than 1.06.

Particularly impressive are the levels of control of these innovative systems provide. Supply and outdoor airflow do not mix so preventing contamination, and there is no added moisture/humidity to the data hall supply, so preventing server corrosion. Reclaimed /grey water can be also used, which is ideal for rain water harvesting, Indirect evaporative coolers can provide 100% required cooling in some regions all year eliminating mechanical refrigeration and allowable supply air temperature to server inlet increases, so IEC efficiency increases further.

Figure 1 shows a typical schematic of an indirect evaporate heat exchanger.

With Polymer-Tube Indirect Evaporative Coolers, outdoor fresh air is drawn across the exterior of elliptical tubes, which are wetted by a recirculation water pump. The elliptical shape of the heat exchanger tubes maximizes the allowable surface area for heat rejection and is sufficiently elastic such that its subtle expansion and contractions from normal operation aid the shedding of residual solids that are a by-product of evaporation.

With fresh air flowing over the wet exterior tube surfaces,

Figure 1

evaporative heat transfer efficiently cools the data centre hot aisle air flowing through the inside of the tubes.

Because the data hall air is recirculated and cooled with an IEC system, no outdoor air is introduced into the data centre by the heat rejection units, so filters may be eliminated from some or all of the heat rejection air-handling units (AHUs). This result's in reduced filter, maintenance, and fan power costs compared to filters on all heat rejection units.

Unlike water-side and wet-bulb economizer systems, IEC systems operate dry during cooler ambient conditions, resulting in lower annual water consumption and elimination freeze concerns. IEC systems are able to achieve 100% heat rejection operating dry when outdoor air temperature is below 10°C based on a hot aisle temperature of 36°C, cooling to 24°C.

Indirect evaporative cooling requires about one-third of the water flow rate of conventional water-side economizer systems, resulting in annual pump power savings.

To facilitate Indirect Evaporative Cooling design and predict annual cost of operation, including water consumption, many suppliers have to look at the power to transport the fresh air that rejects the heat from the system; pump power (when evaporative cooling is used); and power for supplemental refrigeration when required. In addition to the electrical power, water consumption including evaporation and sump flush cycles are taken into account.

Large multi-national collocation and enterprise companies are already seeing the benefits of choosing Indirect Evaporative Cooling as their main source of cooling eg. DigiPlex's new data centre facility in Oslo will use indirect evaporative cooling 10MW of IT to achieve an ultralow partial PUE of 1.06 making this the largest IEC user in europe. DC02 in Belgium, another reference site, are using the IEC systems and are reaping the rewards of a low PUE of 1.11, more than half the average 2.5, making this an energy efficient option.

In the latest review from Cundall (data centre design consultants) for sustainable data centre cooling solutions, IEC scored top marks. The independent review details the differing operating modes of various IEC solutions and more crucially the advantages and disadvantages that IEC has over other common free cooling solutions.

With this game changing energy efficiency, many companies are optimising their data centre operations utilising reliable innovative IEC solutions.

So how does Indirect Evaporative Cooling work?

Typically IEC systems operate in three modes.

Mode 1: Cold and cool days – "Dry mode"
The heat exchanger operates dry and acts like an air-to-air heat exchanger, cooling the data centre without the use of any water.

Mode 2: Warmer days – "Evaporative mode"
The heat exchanger is cooled by outside air evaporating water on the exterior of the heat exchanger tubes. As the air streams are completely separated, humidity is not introduced into the data centre.

Mode 3: Very warm and humid days – "DX mode"
In some climate zones and for only a few hours a year, small mechanical cooling systems ("trim DX") is used for supplementing the indirect evaporative cooling process.

Testing

To assist owners and operators decide on the best IEC selection, there are a number of IEC test facilities to choose from. Data centre managers are be shown what they need to do to create secure energy efficient data centre cooling and how they can optimize power consumption with the use of IEC cooling technology. The test facilities verify the IEC performance in extreme temperature and humidity climates and show how very low partial PUE's of less than 1.06 can be achieved in various situations before deploying a particular solution to site.

Recommendations for a Factory Acceptance Test

The Factory Acceptance Test (FAT) is a project milestone designed to demonstrate to data centre owner and operators that their selected cooling system design and manufacturing meets their requirements.

First, these test centres receive a list of required points from the customer, they then calculate with the return air temperature the required airflow (reference m3/h). The test facility has to maintain in the test data hall these conditions (summer/winter). The main target is to prove the operational conditions:

- At low T° (<10°) without water
- At high T° (around 35°) with water

Often test facilities follow ASHRAE data hall conditions defined for most of the points in the world.

To test cooling performance, the test centre stabilises the external conditions and starts the necessary test equipment.

Post-test

A report is submitted where all discrepancies and non-conformities of the system should be compiled into a non-conformities list and at the end of the FAT these non-conformities are discussed and agreed.

In summary, the Indirect Evaporative Cooling solution offers proven technology with energy saving benefits and a cool stable environment making this the first choice solution for Data Centre Cooling.

Further information

With this game changing energy efficiency many company's which are optimising their data centre operations are utilising this reliable innovative IEC solution. To hear customer cases and movies on how the IEC technology can be applied to your site visit www.munters.com/datacentres or email airtreatment@munters.com or Tel: +44 1480 410223

MATS®
Bringing business process to life

Making Molehills out of Mountains

Less development. Less software. Less delay.
Less cost. Less risk.

MATS® is the next generation cloud BPM platform.

Find out how MATS can help you accelerate process improvement in the “Age of the customer”.

Read the whitepaper at www.matssoft.com/cio

+44 (0)1234 581003 • www.matssoft.com • info@matssoft.com

The consumerisation of IT and knowing your legal risks

Charles Sweeney outlines some of the risks involved with the growth of BYOD

THE CONSUMERISATION OF IT IS prevalent where ever you go. Be it a big enterprise or a small start up, employees jump from smartphone, to tablet PC, to laptop without so much as a second glance. The days when you were tied to a PC that resided on your desk seem like a whole lifetime ago. And in many ways it was.

The rise of Bring Your Own Device (BYOD) has also revolutionised the face of IT in terms of how it is delivered and consumed. But BYOD is about more than employees being able to use a device of their choice to connect with the corporate network. By enabling a more flexible model of working, companies can benefit from substantial cost savings and productivity gains. It is well documented that such business advantages don't come without causing some real headaches for IT, especially from a security perspective. However, increasingly CIOs feel they have a good handle on the security risks that taking data outside of the 'four walls' of a business introduce and can take steps to address these. What they are less sure of, and therefore becoming more concerned about, is their legal exposure and how to identify and mitigate the possible legal risks.

In the last few years, CIOs just haven't been asked to do more with less; they've also the need for their role and knowledge base to expand. As a consequence, being compliant is no longer the remit of the legal team alone, CIOs are expected to be well versed in the potential ramifications of the technologies that they implement and work with the business to ensure that their backs, and the organsiation's reputation, are covered in the event of an incident.

The Data Protection Act

The key legal risks that derive from a BYOD policy are focused around the Data Protection Act (DPA) 1998. Compliance with the Act necessitates keeping personal data relating to individuals (e.g. customers or employees) held by the company secure and furthermore taking suitable measures to prevent "unauthorised or unlawful processing of personal data" and "accidental loss or damage to personal data." To comply with this requirement companies have to take appropriate measures to ensure that unlawful processing of data does not occur.

BYOD introduces a certain loss of control. Data is no longer protected by the four walls of corporate HQ. Instead it is constantly on the move, making complying with the Act easier said than done, especially as the main threat to non-compliance with the DPA is data breach or loss. Typically this tends to be viewed as being most likely to happen if an employee leaves a USB stick, tablet PC, Smartphone or their laptop in the back of a cab or on a train.

But when data is being proliferated

across multiple devices, there is more than one way in which it can be compromised. For example, when an employee leaves a company they may well walk out the door with their email still enabled on their smartphone giving them access to confidential information that could be used for commercial gain. Or a conscientious employee might log on using an unsecured Wi-Fi network in order to send an email whilst in transit. Savvy to the fact that unwittingly humans are the weakest link in any security policy, hackers consider data being sent across these networks as prime hunting ground, greatly increasing the risk that data can be intercepted by people other than the user and the intended recipient.

Or perhaps a department has implemented a free storage cloud. One that is great for holding vast quantities of data, but because it hasn't been provisioned through IT no one has really thought about how to secure the information. Everyone has a password – that's enough right? Recent high profile breeches prove just how easy hackers find it to steal passwords and sell them on the black market.

My point is that the loss of data, by whatever means, poses a significant threat to companies ability to comply with the Data Protection Act. There has been much debate about who is responsible for the security of an employee device being used in the workplace, but don't be sidetracked by such discussions. Unauthorised or unlawful access to data held on a device is, as the data controller, the responsibility of the company. The Information Commissioner's Office makes it very clear that when it comes to BYOD, organisations need to ascertain what type of data is being held, where data may be stored, how it is transferred, the potential for data leakage and the device's security capabilities to name but a few points for consideration.

HR risks

Whilst the DPA is big legal responsibility, equally businesses need to be aware of the possible HR risks that BYOD brings with it. The Internet is not just a fantastic business resource, it also hosts a wealth of inappropriate content such as pornographic material or websites that incite hatred based on characteristics such as race, sexual orientation or religion. It is also very easy for such content to be distributed through the workplace.

In a managed device environment, the vast majority of companies have taken steps to ensure that employees cannot access this type of material whilst at work. This is primarily to avoid claims of harassment, discrimination or unfair dismissal by employees not involved in the accessing or distributing of such content. But now they also need to secure their BYOD workspace as well.

This is especially true as the next generation start entering the workplace. Having grown up with social media as simply a 'fact of life' they are unaware of how content they consider to be everyday might cause offence to others. Yet if they are inviting people to look at content in the work environment and a member of staff finds it offensive, it is still the company - rather than the individual – that is legally at risk.

Under the Equality Act 2010, harassment is defined as "unwanted conduct related to a relevant protected characteristic, which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that individual." Sharing inappropriate content could lead to an employee bringing action based on the employer's failure to maintain a safe working environment that is free from harassment or even that such conduct amounts to discrimination. This may be the case even if the content was not specifically aimed at or even distributed to a particular employee.

Tackling the risks

This can all seem a bit daunting, but there are some basic steps that you can take to help protect yourself and your company:

- Do an audit in order to ascertain what devices you have in your organisation and how they are being used.
- Once you have undertaken this audit, the next step is to understand where the weak points are and how to protect against them. This could involve encryption of corporate data, encrypting data when stored on a device, monitoring the use of devices as well as implementing a filtering solution to ensure inappropriate content can't be viewed and shared using BYOD devices.
- Engagement with end users is key. They might view securing their laptop or smartphone as onerous and unnecessary, but even something as basic as having a PIN in place can offer a basic level of protection.

Educate end users in order to get them on board and adhering to usage policies. If you bombard them with lots of things to do, they'll forget. Instead make it fun, interesting and relevant.

Please note that this article is for indicative purposes only and looks to discuss the issues of BYOD; it does not constitute legal advice.

Author information

Charles Sweeney, Chief Executive Officer, Bloxx
Charles has worked with a number of successful high-growth companies across a variety of sectors including medical devices, animal health and software development. He has been CEO of web security specialists Bloxx since 2012.

Bloxx content filtering and security solutions enable IT staff in all sectors to control and manage Internet use more effectively and efficiently. From corporations to small businesses, healthcare to government, there's a Bloxx content filtering and security product to match. Bloxx has recently been awarded an international patent for their real-time content analysis and categorisation engine Tru-View Technology (TVT).

Three priorities for CIOs in the "Age of the Customer"

Customer Experience Improvement is becoming a top priority for CIOs, because today's customers have unprecedented power. So what can your business do to thrive in the "Age of the Customer"? Richard McCann investigates

TODAY'S CUSTOMERS HAVE UNPRECEDENTED power. Access to information, services and products has never been easier. And if they don't like the service or product they're getting, with a search and a click they can switch allegiance to a new supplier.

Switching is a growing phenomenon. According to a recent survey by Accenture, 66% of global consumers have switched providers (of one or more service or product) in the last year, because of poor customer service.

Add to this the prevalence of social media, and it's easy to see why customer retention is creating heartburn for many businesses.

Crime and Punishment

Social media makes customers powerful advocates if they like what a business does – but formidable enemies if they are unhappy with the service they receive. People are still talking about the day when a United Airlines traveler saw his guitar damaged by luggage handlers, and found his protest ignored by customer service staff. Before social media his complaint would have counted for nothing.

The mistake United Airlines made was to ignore an opportunity to secure a customer as an advocate, by improving his experience. UA saw him as an insignificant lone-voice; but he was certainly not a lone voice for long. His YouTube video went viral and he was soon joined by eleven million supporters, attacking UA's poor customer service. UA's failure to understand "customer power" cost its shareholders a reported $180 million.

However, getting better at putting out "PR fires" isn't the answer. Instead companies need to get better and more agile at improving customer-facing processes. Customer Experience improvement is now top priority for CEOs as their competitive weapon of choice!

Process standardisation and improving efficiency were significant drivers of business transformation during the past twenty years. But squeezing ever more efficiency from what has already been improved becomes increasingly difficult. In this "Age of the Customer" continuous improvement is not what's needed; instead businesses must innovate.

Supporting such innovation must be a top priority for CIOs. According to Forrester, the global research and advisory firm, there's a seismic shift underway between two different categories of IT investment. Traditional back office "systems of record" (such as ERP – enterprise resource planning) and a new category they call "systems of engagement" (processes and technology focussed on winning, serving and retaining customers). Expenditure on systems of record is in decline, partly due to lower infrastructure costs and Cloud computing. Expenditure on systems of engagement is on the rise, and is actually forecast to overtake other IT spend by 2018.

Accelerating change

Accelerating customer experience improvement is a high priority for most businesses; and it's possible to make rapid progress, as illustrated by Cambridge Building Society. Three tactics that the Society employed, with award winning results, deserve particular focus:

- Reducing chaser phone calls
- Transparency of customer service KPIs
- Accelerating change with the help of Cloud Computing

(1) Reduce chaser phone calls

Whether you have a few customer service staff or multiple contact centres employing thousands of customer service agents, improving customer communications and self-service can have a dramatic effect not just on customer experience, but on your efficiency and cost-effectiveness as well. Do you know what proportion of inbound phone calls are chaser calls? For example: "I called earlier, I'm trying to find out when my order will be delivered?" "You're processing my insurance claim, what's the status?" "What's the status of my TV repair, I've heard nothing for a week?"

Chaser calls are a major cause of customer dissatisfaction. Particularly as in many cases to get through to someone to ask the question will involve navigating call menus, waiting in interminable queues, and then eventually having to answer umpteen security questions. No wonder tempers fray!

> "Accelerating customer experience improvement is a high priority for most businesses"

According to Forrester survey, 71% of consumers say that valuing their time is the most important thing a company can do to provide good service.

Chaser calls are not just a sign of lousy service; they're a drain on morale and productivity. They occupy customer service staff who should instead be serving and delighting other customers.

As illustrated by The Cambridge, such calls can be minimised by proactive messages, controlled by a business process management (BPM) platform.

(2) Reduce Performance Black Holes

The use of a BPM platform, doesn't just streamline a process; it also makes the process completely measurable. The Society can now see how long a case resides at each approval stage. Management have complete oversight of the approval pipeline, enabling them to balance workload across the processing team. Process monitoring dashboards and alerts help the society meet service level agreements and identify performance bottlenecks, including further process improvement opportunities or staff training needs.

The old adage "you cannot improve what you cannot measure" reaffirms the validity of applying business process management tools and methods to customer service.

(3) Reduce project duration and complexity with the help of Cloud

The quest to become more agile at improving customer-facing processes is likely to put Cloud Computing at the centre of your process improvement strategy. The majority of CRM software implementations are delivered via the Cloud, so that will not come as a surprise. But if we consider what it takes to enable agility, the benefits of Cloud or Software-as-a-Service (SaaS) become even more distinct.

Firstly, provision of Cloud software is very fast. You don't need to install software or servers, so projects can get off the ground in a day or two instead of months.

Secondly, agility requires that companies should enable and encourage innovation. SaaS makes that possible in a way that traditional, perpetual software licensing cannot. Some SaaS vendors provide "Pay-as-you-go" licensing; which provides a commercial backdrop that fosters experimentation. Whereas old school thinking was "return on investment", the advent of SaaS offers the potential of "return before investment". Business people can now afford to experiment with technology-enabled customer experience improvement initiatives, in a 'test-and-learn' manner.

Improving Customer Experience at The Cambridge Building Society

Reducing chaser calls dramatically improves customer satisfaction, service levels and cost efficiency. Such improvements can be achieved surprisingly quickly. The Cambridge Building Society reduced in-bound chaser phone calls by 50% within a few weeks of implementing a case management system. This project took just three months to deliver, considerably faster than traditional IT projects. Selecting a Cloud application meant they could get started straight away without the delay of installing infrastructure and software. Using a business process management platform meant that they were able to design a new process very rapidly and configure the required solution rather than being dependent on extensive programming.

The system is incredibly simple. Customers or intermediaries receive automated alerts (by text or Email) the instant their mortgage application passes one of several approval stages. By keeping customers informed of such progress, the Society has seen a dramatic reduction of in-bound chaser calls, because every customer is now up-to-date with the status of their application.

The difference this has made to customer service at the Cambridge has been dramatic, as customer service agents now spend less time reacting to needless inquiries, and more time processing applications. The result? Increased business volume, without increasing headcount, while at the same time improving customer satisfaction. Within a year of implementing these changes, The Cambridge won the prestigious award; Moneyfacts - Best Mortgage Service Provider, 2013. Learn more about The Cambridge's process improvement project here http://www.matssoft.com/customerscambridge-building-society/

Last word

Lastly, consider this. Such experimentation can actually reduce risks that are normally associated with software projects. It's widely known that more than 60% of large software projects either fail or are "challenged". Whereas smaller software projects that are business-led are ten times less likely to fail.

Many businesses are keen to empower operational departments to improve systems and processes more quickly. Perhaps the segregation of systems of engagement and systems of record can help in this regard? As shown by The Cambridge, improvements led by the operations department can be made rapidly. The BPM platform that they deployed augmented rather than replaced their back office platform. So the improvements they delivered so rapidly for the front office, were achieved without disruption to their overall IT architecture.

Author information

Richard McCann MBA, PhD is an author, broadcaster and journalist.
Contact Richard at info@fridays-group.co.uk

Nothing Protects Like Tru View

Patent Protected Web Content Security

With over 100 websites created every minute it's important your web security stays ahead of the game. Recently awarded an international patent, Tru View is our unique, real-time content analysis engine.

Make sure you're protected with tomorrow's technology today.

For an online demo, visit
www.bloxx.com

BLOXX™
NO NONSENSE.

Turning on energy savings in the workplace

Taking steps to reduce your office's energy consumption needn't be the uphill struggle you think it is, **Energenie** explains

THERE ARE MANY REASONS WHY cutting this expenditure should be towards the top of your priority list. First and foremost, it is one of the largest controllable overheads and the potential to save money is huge.

Even though it seems the country is starting to emerge from the financial crisis and ensuing recession - albeit slowly – it is likely to be a long time before the economy is in a state that can be regarded as healthy. In light of this, any money-saving endeavours should be eagerly embraced.

A typical office's energy bill could be as much as 65 per cent higher than that of an equivalent workplace that has undertaken efficiency measures.

Making strategic energy-saving decisions can also help to bolster your company's corporate reputation, which could reap dividends in the future. By improving working conditions, this could also have the knock-on effect that your employees' productivity increases.

Furthermore, taking an active decision to cut back in this way means you are part of the wider initiative to lower the world's carbon footprint. While this is a massive task, it is made much simpler if everybody plays their part.

However, maybe you are of the opinion that, as much as you would like to be part of this, is it just another item on your ever-growing to-do list that you could do without? Here are some ways in which you can effectively cut your expenditure.

Small steps, big savings

Simply changing the way in which you use the appliances and items in your office is a good place to start.

Leaving a computer and monitor on 24 hours a day could cost as much as £45 every year. It is not just the financial implications that are worth bearing in mind - leaving it on overnight would create enough carbon dioxide to fill a double-decker bus.

Office equipment that has been left on standby during bank holidays and weekends could set back a small or medium-sized business as much as £6,000 every year. Appliances like this are the fastest-growing use of energy in the corporate world, constituting 15 per cent of total consumption in the workplace. In addition, this is expected to double by 2020, so this is a key area in which you could be making savings.

Leaving the photocopier on standby overnight can waste enough energy to make as many as 30 cups of tea. Incidentally, it is likely your office kitchen will often be busy with staff making hot drinks and preparing their lunch.

As the milk is taken out of the fridge countless times throughout the day, have you thought how much energy is being wasted as the door remains open? Leaving it open for as little as 30 minutes a day wastes enough energy annually to power a lighthouse for approximately four days. Encourage personnel to shut the chiller while it is not in use and, if possible, make hot drinks in bigger batches so it is being opened less frequently.

Stop the office becoming heated

It is thought heating costs amount to as much as 40 per cent of energy costs in a standard office, meaning there is huge scope for savings to be made.

Firstly, consult your staff over the office temperature. It is important your employees know they are being listened to and that their opinion is important. A democratic approach to this situation can help to resolve problems and dissuade workers from secretly tampering with the thermostat.

Try to ensure your workplace is shielded from draughts and direct sunlight. Not only is this a free way to provide a more agreeable temperature, but it will also make working conditions more pleasant – thereby increasing office productivity.

Lowering the overall office temperature by just one degree C could cut fuel consumption by eight per cent and save enough energy to print in excess of 40 million sheets of paper.

Pay attention to the seasons when it comes to setting the overall heat level. Ensure your system's operating times are changed depending on when ventilation, cooling and heating are needed. Make sure you do not fall foul of basic mistakes, such as having the heating on when the building is empty.

Even something as simple as having the boiler regularly serviced could cut ten per cent from your annual expenditure – gas-fired boilers once a year, oil ones every six months.

Make the most of natural ventilation when it seems a little hot and get a draft going by opening vents, doors or windows. However, ensure you consider what security implications this may have.

It is a myth that costs can be slashed by leaving the air conditioning on overnight – it will simply result in higher energy consumption. An office only needs a very small amount of overnight energy to be at a suitable temperature the following day.

Furthermore, capitalise on the lower external temperatures at night to ensure your office is adequately cooled – a practice known as night cooling.

Flicking the switch on savings

Office lights left on overnight use enough power every year to heat a home for nearly five months.

The recent drive towards energy-efficient light bulbs has been well documented, but with so many out there, which are the best ones to choose?

For the best value for money, start using light emitting diodes (LEDs). While they can be more expensive initially, some of them have a lifespan of as much as 30,000 hours. Not only are they more energy efficient, but they also don't need replacing quite so frequently.

Furthermore, you can save as much as 85 per cent if you make the switch to LED bulbs.

One common complaint about energy-efficient bulbs is they take a long time to power up. While this may be true of some types, LED lights reach full brightness instantly.

A report by Lux Magazine showed how the NHS is already saving £1.2 million annually due an initiative that involved turning off lights and closing doors. However, it is thought this drive could save the taxpayer £35 million every year if all staff were fully behind the scheme.

Consider putting stickers or posters in strategic places around your workplace to remind personnel to switch lights off when they are not being used.

Bigger steps

Are you regularly checking whether or not you are getting the best deal when it comes to how much you pay? Energy suppliers have featured in the news quite frequently as of late and, while it may seem burdensome to browse comparison sites and go through the hassle of switching suppliers, it is worth the effort for the potential savings.

When you need to replace computers and equipment, think whether or not your staff really need high-spec computers with fast processors that consume a lot of power? Just because they are appealing does not mean they are necessary.

Take time to investigate the most energy-efficient computers that you can purchase. Flatscreen monitors – also known as LCD – could be a potential option as they not only reduce energy, but also take up less space.

One thing to note is the government's Electricity Demand Reduction (EDR) pilot, which will be launched in June this year.

It is meant to incentivise businesses implementing energy-saving measures - such as more efficient motors, air conditioning and lighting - by providing financial backing.

There will be in excess of £20 million in funding for the scheme and companies will be able to bid for a share in this pot.

How to engage your staff

A report by the Carbon Trust revealed that, while the overwhelming majority (92 per cent) of employees were concerned about saving energy at home, fewer than half (47 per cent) considered it a key issue to help their boss to do the same in the workplace.

Creating a green team could be one way to combat this and engage staff. Like a social committee that organises the Christmas party and general social activities,

a green team could be an effective way of raising awareness in your office as your workforce value the fact they have been entrusted with some responsibility and start to take ownership of the initiative.

Select employees who seem to be the most passionate and are already keen to promote sustainability in the office. Ensure there are members of senior management in the team so employees know it is something that has backing from the top of the hierarchy.

Not only will it strengthen friendships within the office – as these people will spend more time together – but you will also garner a variety of different ideas and be able to select the best ones that will work for your company.

Similarly, see if you can turn this green initiative into a competition, as this can really help to get an idea off the ground. If you make it clear what the objective – and winning prize – is, you could see a greater number of staff getting behind the drive.

Whether it is which department can use the least paper in a month or which sub-team can cut energy usage by a certain date, a light-hearted competition could build morale and inject a touch of excitement into this eco-friendly boost.

Further information

Energenie sells products that enable consumers to save money, be safer in their homes and help the planet, thereby making their lives that little bit easier.

Examples of the merchandise on offer include remote control sockets, which make it easy to turn off your plugs off at night, and rechargeable smartphone chargers, meaning you won't have to worry about your device running out of battery anymore.

A large selection of LED lights are also sold to lower your carbon footprint.

All products are CE marked and comply with safety and other regulatory requirements.

theCsuite.co.uk

Sparta publishing

www.spartapublishing.co.uk
Tel: +44 (0)20 7970 5690
40 Bowling Green Lane, London EC1R ONE

THE INTERNET OF THINGS – MORE THAN JUST SMART FRIDGES?

LIKE ANY BIG TECHNOLOGY TREND, THE INTERNET OF THINGS COMES WITH CONSIDERABLE BAGGAGE AROUND SECURITY. IT IS A PRETTY BIG CHALLENGE TO ESTABLISH TRUST AND CONTROL IN A WIDE AND ENORMOUS RANGE OF 'THINGS' PARTICULARLY WHEN THEY ARE WIDELY DISTRIBUTED TO HIGHLY UNTRUSTED LOCATIONS OR WHEN THEY HANDLE SENSITIVE DATA OR PERFORM SENSITIVE TASKS

The murmurs of excitement around the hotly anticipated Internet of Things (IoT) are hard to ignore. OK, it's a ridiculously vague term, rather like describing a gorgeous meal as a plate of stuff, or a gripping book as pages of words, but the IoT does look set to hit the big time, rapidly becoming an increasingly integral part of our lives and infiltrating everyday objects. Google is already making pioneering moves in this space, purchasing connected device company Nest Labs in January. But with billions of devices set to become connected to the internet and intended to do something intelligent, the IoT holds the potential for far more interesting things than controlling our fridges, thermostats and smartphones.

At the outset of this year Gartner identified the IoT as one of the top 10 Strategic Technology trends for 2014, but many believe that it is in fact the big technology concept that will dominate the sector for years to come - and it's not just about home automation. The revolution will impact much of the critical infrastructure we all rely on – utilities, transportation, smart cars, smart buildings, smart cities – smart everything.

These intelligent, connected devices will eventually become our eyes, ears and finger tips, operating in places we would never want to visit, environments we couldn't survive, and with levels of performance we could never achieve.

Familiar challenges – but taken to a new level

Of course, the positive potential of the IoT has been matched with an equal amount of concern over its security - not to mention the significant legal implications these devices carry with regards to data privacy. The scale, complexity and geographic spread of IoT networks, coupled with the amount of data that makes them tick, make them highly vulnerable. The types of data flowing through the IoT network come in many forms, spanning personal data such as behaviour and location, to command and control data driving our critical national infrastructure. A main reason for these concerns is that the devices themselves are often in vulnerable locations, may have very little physical protection, and the networks through which they communicate can't always be trusted. This makes them a prime target for malicious hackers and cyber criminals. It's not just about the devices themselves, it's also the back-end systems, the points of aggregation where data from millions of devices is collected and analysed - where decisions get taken and instructions issued. Compromise at the centre could drive breaches the scale of which we've never seen before.

Building trust across these huge scale, distributed systems must be a main priority for companies seeking to implement a successful IoT adoption strategy.

Trust and control

Fortunately one of the key technologies which will establish trust and control in the IoT has been around for years – Public Key Infrastructures (PKIs). PKI is a tried and tested method that has been used for years to secure communications across the internet, and is the backbone of security in the global payments networks, playing a central role in the protection of users, networks, data and business systems. Sectors such as gaming, online banking and e-commerce rely on PKIs to establish the identity of users, devices and applications.

They work by using digital credentials based on encryption to ascertain that devices and individuals are who they say they are. Through encrypting data and using digital credentials to identify web services, devices and users, PKIs can enforce access to sensitive systems and protect data from unwanted intruders. Tied to a pair of cryptographic keys, these digital credentials can form the basis of trust, with the keys only able to be used by the device or user to which they belong.

Like any technology relying on encryption, proper key management is absolutely paramount. Failure to properly look after the secret cryptographic keys compromises the security of the entire PKI and leaves the entire systems vulnerable to attackers. Managing and securing these secret keys becomes one of the foundations of the entire security model.

Over time the Internet of Things will stop being mostly talk but something that is ubiquitous (just as cloud computing and e-commerce are now). It will be of critical importance that the identities and data of devices, individuals and organisations are properly protected through encryption. Failure to do so will have serious implications on privacy, business integrity and even the safety of individuals themselves. PKI as a technology and an industry has had its ups and downs, with the 'year of PKI' never quite materializing. However, instead of a big bang, PKI has quietly become a fundament component of the systems we rely on today ranging from the internet, to credit cards to smarts phones and the cloud. Analysts are already branding this next era of PKI with the IoT triggering the rise of 'PKI 3.0' – we'll have to wait and see what that actually turns to mean.

Looking just five years down the line, we could find ourselves living in a futuristic world where many of the day-to-day responsibilities in our critical systems are entirely handed over to machines. It's clear that the IoT is an exciting advancement in our technological evolution, but the question of trust and security has never been more paramount. We need to ensure that we build in the appropriate safety measures to these networks now, to avoid catastrophe.

Richard Moulds, VP Strategy, Thales e-Security
www.thales-esecurity.com

THALES

Introducing Virtual Token® MFA security from Sestus

making user authentication **practical** and **affordable**

the challenge

Hackers want your passwords, either directly or through social engineering. Traditional methods of securing against such attacks have proven to be expensive and inconvenient to users.

the Sestus Virtual Token® MFA solution

Sestus solves the current challenge by offering a proven and patented solution that turns the user's computing device, PC, tablet or smartphone into an additional factor of authentication, alongside the password. No additional hardware or software is needed. The Sestus Virtual Token® will only work from the registered device, so that a stolen password will prove insufficient for unauthorised access.

total cost of ownership

The simplicity of the Sestus Virtual Token® MFA solution results in a Total Cost of Ownership lower than any other MFA solution in the market today. The solution is available in both on-premise and cloud editions, to meet all your needs.

Sestus Virtual Token® MFA

Practical user authentication

- √ No client hardware to be deployed
- √ No client software to be deployed
- √ Works independently of user's OS or browser
- √ Easy to integrate into applications
- √ Acceptable by end users
- √ Low help desk involvement
- √ Complies with international regulatory requirements for multi-factor authentication
- √ Field proven over many years across a range of industries.

Looking to upgrade or change your authentication system?

Call Sestus today for a demo and your chance to save 10% on the license cost. Quote Key Code 071402

Sestus International Limited 367 Caledonian Road London, N7 9DQ **Telephone:** +44 208 133 3062 www.sestus.com