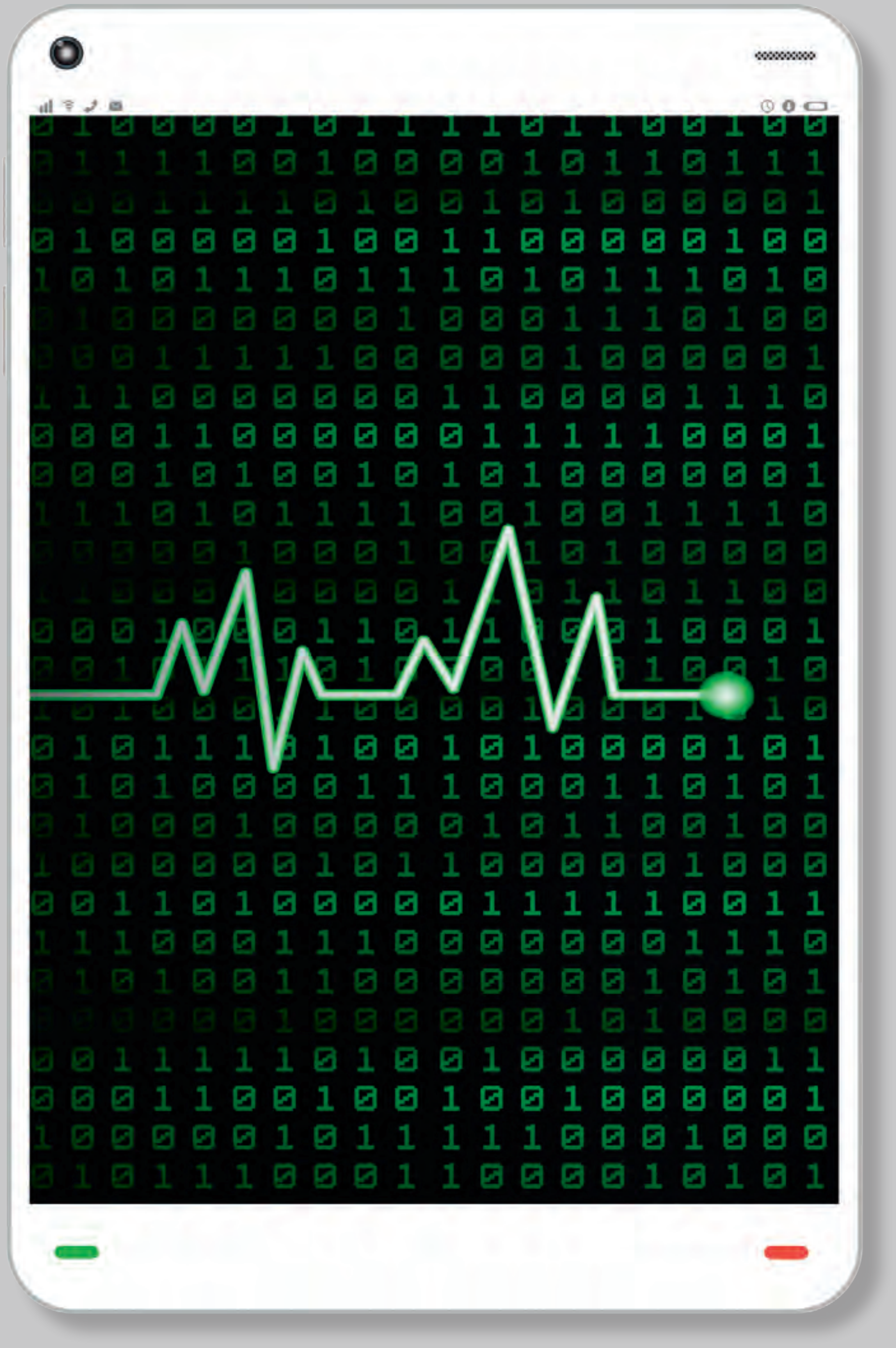
govtech review

PLUGGING THE **I.T. BRAIN DRAIN**

I.T. CHALLENGES FOR MERGING COUNCILS

INNOVATION NEEDS **REGULATORY CHANGE**



ON LIFE SUPPORT

AUSTRALIA'S HEALTHCARE I.T. NEEDS A SHOT IN THE ARM

Q1 2017
PP100021607

GTR
GOVERNMENT TECHNOLOGY REVIEW

informing technology decision-makers

Contents

Q1 2017

gov tech review

PLUGGING THE I.T. BRAIN DRAIN

I.T. CHALLENGES FOR MERGING COUNCILS

INNOVATION NEEDS REGULATORY CHANGE

ON LIFE SUPPORT

AUSTRALIA'S HEALTHCARE I.T. NEEDS A SHOT IN THE ARM

GTR informing technology decision-makers

Cover photo courtesy © stock.adobe.com/au/siiixth

Insider

Nothing to fear from disruption

Welcome to the new combined GovTech Review and BizTech Review magazine from the Technology Decisions media group... now reaching a larger audience of private and public sector technology decision-makers right across Australasia.

The uniting of two of Australia's leading technology magazines is a reminder that we live in an age of change. Our private and professional lives are being turned upside down by new technologies and the possibilities they present. For instance, spare a thought for those Sydney councils that have been forced to merge recently, and for the potential for disruption and dislocation this will bring them, particularly in terms of their IT systems. Fusing entire enterprises' technology solutions is no easy task, and is something that can take a lot of time. But one newly merged council, Cumberland, is off and running already, as our article in this issue ('Synergy of systems') describes. The council is well underway with its transformation plans, which include replacing up to 150 legacy applications with one enterprise suite.

Of course, those in the business world might say that this is nothing new — corporate mergers happen all the time, and those involved have to just muck in and make the best of it. And perhaps in this day and age, making the best of it might in some ways be easier than it used to be. The rollout of new enterprise technologies, using the benefits of cloud, mobility and virtualisation, can make the whole process far more rapid than it used to be. But this raises the question — what can be done in your organisation to improve processes through proactive disruption that helps you keep up with the times? And what could be the consequences of failing to do so?

This is a question faced by Australia's healthcare industry, and in particular the various government agencies, departments and partner organisations involved in the sector. With recent breaches and malware attacks at Melbourne Health and the Red Cross Blood Agency still fresh in everyone's minds, and with such sensitive personal data at stake, it's no wonder that — according to technology consultancy West Monroe Partners — just 48% of respondents to a survey said they fully trust their healthcare provider with their personal data. Put this together with episodes such as #Censusfail, and it's clear that the IT world — public and private — has a lot of work to do to restore and maintain consumer trust... something that will be essential when arguing the case for more digital innovation to replace tried and true systems.

Jonathan Nally, Editor
editor@govtechreview.com.au

wfmedia
connecting industry

A.B.N. 22 152 305 336
www.wfmedia.com.au
Head Office: Cnr Fox Valley Road & Kiogle Street
(Locked Bag 1289), Wahroonga 2076 Australia
Ph +61 2 9487 2700 Fax +61 2 9489 1265

EDITOR
Jonathan Nally
jnally@wfmedia.com.au

FEATURES EDITOR
David Braue
dbraue@wfmedia.com.au

PUBLISHING DIRECTOR/MD
Geoff Hird

ART DIRECTOR/PRODUCTION MANAGER
Julie Wright

ART/PRODUCTION
Linda Klobusiak, Tanya Barac, Colleen Sam

CIRCULATION MANAGER
Sue Lavery
circulation@wfmedia.com.au

COPY CONTROL
Mitchie Mullins
copy@wfmedia.com.au

ADVERTISING SALES
Liz Wilson Ph 0403 528 558
lwilson@wfmedia.com.au

Gemma Burr Ph 0413 220 178
gburr@wfmedia.com.au

If you have any queries regarding our privacy policy please email privacy@wfmedia.com.au

All material published in this magazine is published in good faith and every care is taken to accurately relay information provided to us. Readers are advised by the publishers to ensure that all necessary safety devices and precautions are installed and safe working procedures adopted before the use of any equipment found or purchased through the information we provide. Further, all performance criteria was provided by the representative company concerned and any dispute should be referred to them. Information indicating that products are made in Australia or New Zealand is supplied by the source company. Westwick-Farrow Pty Ltd does not quantify the amount of local content or the accuracy of the statement made by the source.

Printed and bound by SOS Print+Media Group
GovTech Review PP 100021607 • ISSN 1838-4307
BizTech Review PP 100009359 • ISSN 1446-2230

To enable its **Digital Transformation**, Volvo relies on Veeam to ensure Availability of all data and applications. **24 . 7. 365**
Veeam makes Volvo Available. 24.7.365
AVAILABILITY for the Always-On Enterprise™
VEEAM

LIFE SUPPORT

David Braue

WITH CONSUMER TRUST SHAKEN, AUSTRALIA'S CONVALESCING HEALTHCARE IT ECOSYSTEM NEEDS A SHOT IN THE ARM.

"From my work with health bodies in Australia, we are seeing thousands of attempted ransomware attacks per day." — Keith Holtham, Check Point Software Technologies

A series of high-profile data breaches during 2016 exposed IT problems in Australian healthcare agencies, which joined peers around the world in being ravaged by human error and targeted by data-hungry hackers. As if that wasn't enough, the Australian Taxation Office's core data infrastructure collapse offered a stark reminder to all large government organisations that data security in this day and age is about more than just stopping hackers.

That would have been an empty reminder for the IT teams at Melbourne Health, where a malware attack paralysed pathology services at the Royal Melbourne Hospital (RMH) last January. Or the Red Cross Blood Service (RCBS), whose IT service provider Precedent made 1.28 million healthcare records, containing the sensitive medical information of over 550,000 blood donors, available online. An investigation by the Australian Privacy Commissioner is underway and the findings are unlikely to be complimentary.

The RCBS breach was Australia's largest to date, but it pales in comparison to recent compromises at US health insurers such as Anthem, which lost 78.8 million patient records in an attack given a risk-severity rating of 10 out of 10 by the Breach Level Index, or the Korea Pharmaceutical Information Center (43m records), Excellus BlueCross BlueShield (10.5m) and an unnamed US healthcare insurer that suffered an identity-theft attack that saw 9.3m records compromised.

Australia's lack of breach-notification laws — already well enshrined in other countries and due to be legislated here soon — means that we just don't know how many breaches are happening behind closed doors. But "from my work with health bodies in Australia, we are seeing thousands of attempted ransomware attacks per day", said Keith Holtham, ANZ emerging technologies lead with security firm Check Point Software Technologies.

Close linkages between healthcare institutions and university research organisations have created a matrix of vulnerabilities that is "a fairly unique environment in Australia", Holtham said, with so-called 'shadow IT' particularly problematic. "We have traditionally seen monolithic systems where people have had records and data repositories, and they're not necessarily under the control of IT or IT security."

The haphazard nature of healthcare IT security has helped compromise the public's trust in an entire industry. Recent research by technology consultancy West Monroe Partners (WMP) found that just 48% of respondents to a survey said they completely trust their healthcare provider with their personal information.

This, despite findings that patients are enthusiastic adopters of healthcare portals and mobile apps — used by 86% and 91% of consumers respectively. Such findings suggest a significant disparity between consumers' desire for digital health care, and providers' ability to deliver those services.

"Government CIOs need a sense of urgency and a willingness to take calculated risks to survive," Gartner analyst Rick Howard noted, "particularly as they are laden with more responsibilities than their private-sector counterparts."

>>

While some government programs will thrive based on participation from citizens — Gartner believes half of all citizens will voluntarily share personal data to drive smart-city programs by 2019 — healthcare programs will only be successful if citizen-related data can be guaranteed safe. Building those guarantees will be crucial to the recently announced National Digital Health Strategy (NDHS), which was opened to public consultation in November by the fledgling Australian Digital Health Agency (ADHA).

The ADHA's creation is the latest stage in a stop-and-go e-health transition that was for years managed by the National E-Health Transition Authority (NeHTA), whose My Health Record has arguably been a modest success — some 4 million Australians currently use the system. But broader adoption will require healthcare CIOs to reassert their legitimacy and capabilities in a climate where healthcare and other personal data are being actively targeted for harvesting by bots on a 24x7 basis.

ALL TOGETHER NOW

As if the threats weren't bad enough, Australian healthcare organisations are being plagued by bad habits and deficiencies in areas such as skills and committed resources. They also face stricter-than-usual limitations around the adoption of Internet of Things (IoT) technologies — which are being snatched up in other parts of government, but must be adequately secured to guarantee they won't lead to potential compromises of sensitive healthcare data.

That's proving harder to guarantee than one might expect. Their curiosity piqued, hackers spent much of 2016 probing all manner of IoT devices and specialised medical equipment, and found a range of vulnerabilities that could have life-threatening consequences.

> *"There is a general feeling that most attacks against health care are against US healthcare entities. But Australian health care is also a very lucrative target for cybercriminals." — Richard Staynings, Cisco Systems*

Despite healthcare organisations' indisputable reliance on technologies of all types, the threat of equipment hacks has created a level of risk that, surveys suggest, Australian organisations are poorly equipped to manage. Some 85% of respondents to Capgemini Australia's recent 2016 World Quality Report, for example, said IoT applications were important to their organisations — but 68% admitted they weren't ready to deal with the additional workload the IoT presents.

Cloud computing — which has been enthusiastically embraced by many levels of government — is also lagging in health care, where requirements for data security and control have forced CIOs to kerb their enthusiasm.

While 28.4% of Australian organisations in the Capgemini study were running applications in the public cloud — leading the world — they were well behind global averages when it comes to use of DevOps, the emerging discipline focused on keeping operational procedures in lockstep with development practices.

Such deficiencies will increase drag on Australian healthcare organisations' ability to innovate, even as their less encumbered peers pivot towards a future built around new technologies. Navigating these unique circumstances will require healthcare CIOs to carefully straddle the gap between citizen expectations and their own capabilities. But that won't be easy, warned Richard Staynings, principal and cybersecurity healthcare leader with Cisco Systems.

"Australia has really dragged its feet around breach notification" legislation, said Staynings. "As a result there has been lower prioritisation of healthcare and a general lack of understanding of the magnitude of the risk with which providers are being faced."

"There is very little in the way of security operations capabilities and visibility tools," he added, "and there is quite little from a regulatory compliance perspective that is forcing people to look into that, or to provide repercussions when data is not secured.

Staynings also noted, "[There is] a general feeling that most attacks against health care are against US healthcare entities. But Australian health care is also a very lucrative target for cybercriminals."

Reports tracking the sale of stolen healthcare data support that contention. Intel Security's recent McAfee Labs Health Warning report, for one, found medical records selling for anywhere from a fraction of a cent to US$2.42 (AU$3.32) per record — well below the cost of financial data, largely due to factors related to economies of scale.

"Medical data adds value to the [financial services] transaction," the report noted. "Stolen medical data ... already has a higher per-record value than in markets of non-financial account data."

COST VERSUS BENEFIT

Even as cybercriminal market forces progressively monetise the data held within Australian healthcare organisations, those same organisations are facing some far more pedestrian issues.

Ever-present budget limitations, for one, have forced healthcare organisations to drag out the value of their IT assets for much longer than would normally be recommended. Witness the Windows XP systems breached in last year's RMH malware attack, which had not had official support from Microsoft for nearly two years at that point.

Such systems are sitting ducks for hackers. The thought that they are being relied on to protect extremely sensitive healthcare information is rightly a cause for concern. Even environments that are supposedly well protected — such as the ATO's core infrastructure, which scrambled to recover from the loss of nearly 1 petabyte of data after a catastrophic failure of its HP Enterprise storage — remain susceptible to major problems that have nothing to do with security breaches.

Yet with budgets tight and cloud alternatives still representing too high a risk for many healthcare environments, healthcare CIOs have few real options.

Some are considering ways to revisit their on-premises infrastructure, which allows them to retain citizens' healthcare within internal databases while using technology like virtual desktop infrastructure (VDI) to reduce exposure to client-side issues such as outdated and vulnerable desktops.

"The more people digitise their businesses, the more they worry about patient data getting into the wrong space," explained Pat Devlin, ANZ regional director with infrastructure provider Simplivity, which recently expanded its OmniStack platform with explicit VDI support for healthcare institutions running the widely used EPIC Systems Hyperspace patient management system.

Explicit support for that platform allows the VDI environment to be tuned for the rapid responsiveness that's critical for everyday performance in healthcare environments, while "allowing infrastructure teams to be able to lock down their endpoints a little tighter", said Devlin, noting that the platform will soon be certified to Common Criteria and FIPS defence-level security standards. "There are some environments that just cannot tolerate high levels of latency, and VDI delivers very consistent VDI performance regardless of scale."

Such upgrades require a major change in healthcare IT philosophy, however, since they necessarily involve a major overhaul of operating infrastructure. And while the technology is established, mustering the willpower and resources to implement it is another issue altogether.

Senior leaders "are in a sticky situation because they don't have the

>>

> *"Government CIOs need a sense of urgency and a willingness to take calculated risks to survive." — Rick Howard, Gartner*

money or the mandate to fix what needs fixing", said Staynings. "Security is competing for scarce resources around increased digitalisation and improved patient-outcome initiatives. They're in a bit of a catch-22."

The results of this situation are hardly conducive to digital revolution. Forecasts of key IT trends in 2017 all revolve around cloud technologies, IoT, virtual assistants and the like. But none of these technologies can be properly exploited within healthcare environments without some serious infrastructure overhauls. The net result is likely to be that many healthcare providers will stand still and watch the technology state-of-the-art recede into the distance.

If budget limitations are one complicating factor for healthcare IT, management support is another. Gartner, for one, recently warned that many executives are using inappropriate benchmarking practices to gauge their security spend against other industry players.

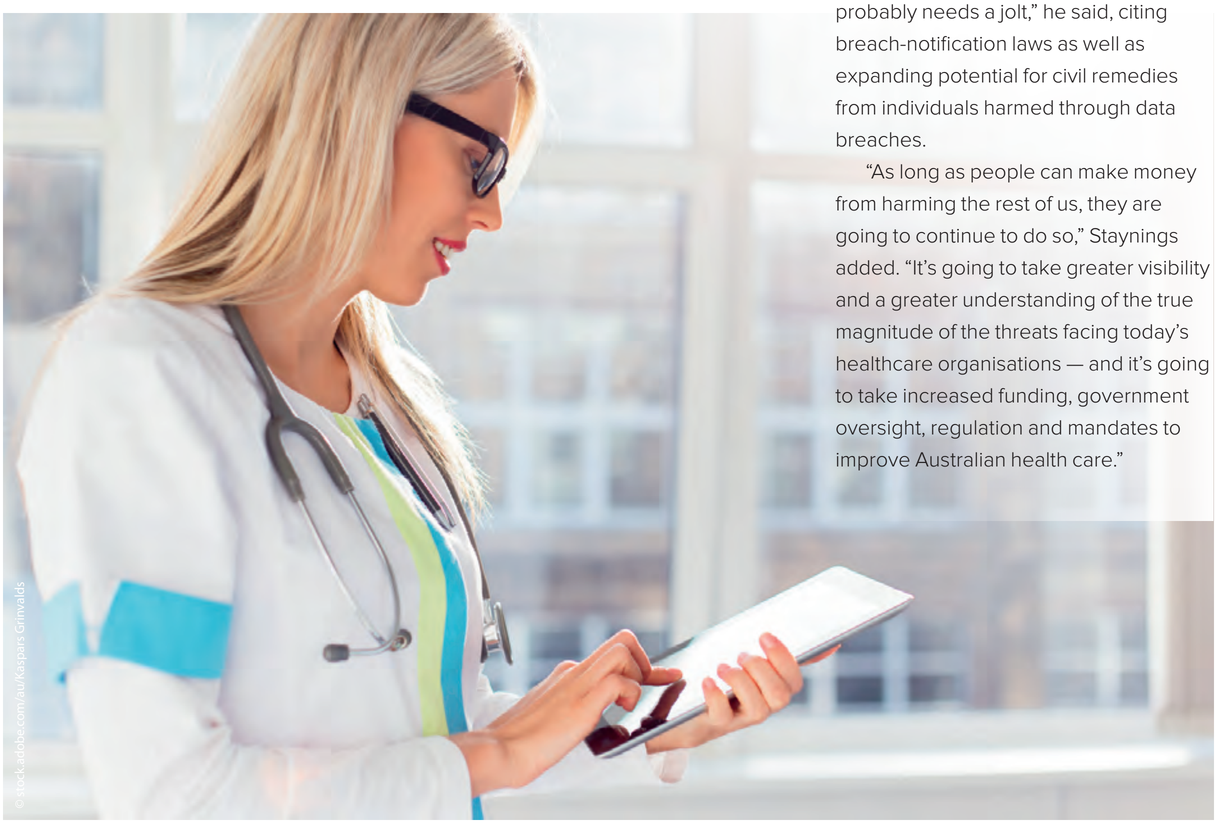
This approach — particularly when used to manage costs in budget-sensitive government agencies — may seem appropriate for managers schooled in unit-based expense tracking; witness the catastrophic failure of management that led to the Queensland Health Payroll System Commission of Inquiry fiasco. When similarly absolutist metrics are applied to cybersecurity risk, these methods can obscure natural organisational idiosyncrasies and gloss over some very real risk indicators.

"General comparisons to generic industry averages don't tell you much about your state of security," Gartner research director Rob McMillan warned. "You could be spending at the same level as your peer group, but you could be spending on the wrong things and be extremely vulnerable. Alternatively, you may be spending appropriately but have a different risk appetite from your peers."

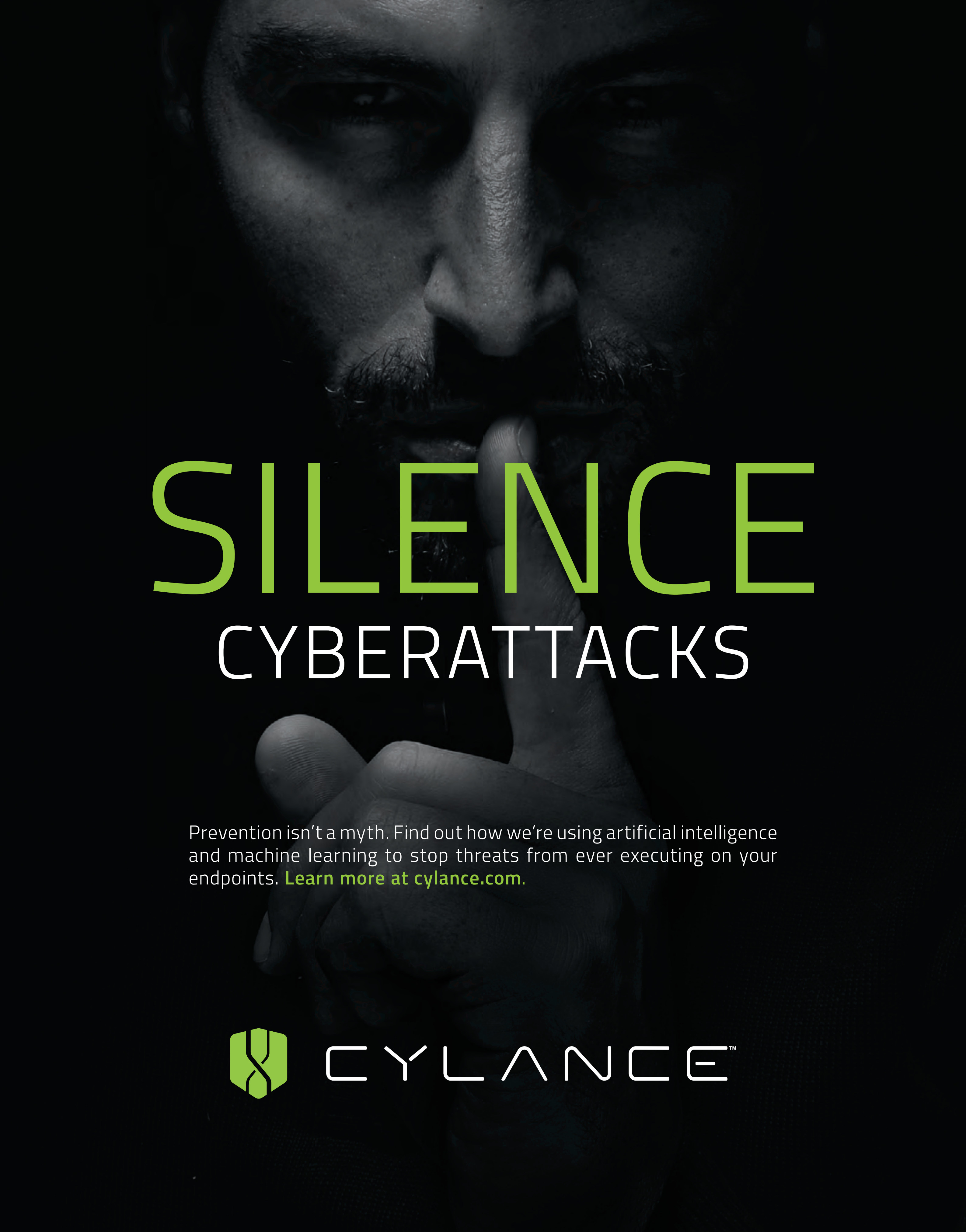
Even as healthcare providers continue to climb the learning curve around data security and infrastructure reliability, the people seeking to steal their data will continue redoubling their efforts to do so. This, Staynings warned, is likely to keep tightening the screws on healthcare CIOs through 2017 and beyond — forcing them to step away from traditional operationally focused models of IT to develop, and execute on, broader strategy and governance frameworks.

"The Australian healthcare market probably needs a jolt," he said, citing breach-notification laws as well as expanding potential for civil remedies from individuals harmed through data breaches.

"As long as people can make money from harming the rest of us, they are going to continue to do so," Staynings added. "It's going to take greater visibility and a greater understanding of the true magnitude of the threats facing today's healthcare organisations — and it's going to take increased funding, government oversight, regulation and mandates to improve Australian health care."



© stock.adobe.com/au/Kaspars Grinvalds


SILENCE
CYBERATTACKS

PLUGGING THE **BRAIN DRAIN**

THE AUSTRALIAN PUBLIC SECTOR SHOULD USE WORKFORCE PLANNING TOOLS TO TACKLE THE TALENT 'BRAIN DRAIN'.

Joe Abusamra, Vice President, Product Marketing, Acendre

It's well known that a career in public service offers security, challenge, a sense of purpose, enviable work-life balance and other entitlements. Increasingly, though, the Australian public sector is losing talent to private enterprise at almost double the return rate (a factor of 1.8, according to a LinkedIn report).

This is why it is important that government agencies adopt tools and strategies associated with workforce planning to provide an emerging, highly integrated, enterprise-wide approach to personnel oversight.

Cloud-based workforce planning solutions lend total visibility into all areas of the workforce, exposing skills gaps and performance discrepancies. Going beyond a mere assessment of whether there are enough qualified personnel in a particular department, it determines the precise competencies within a department's different areas, ensuring all bases are covered. For example, software engineers and analysts both work in R&D, but they don't do the same thing. They are, however, both needed to advance an agency's missions. Many roles are interdependent, so the identification of talent shortfalls always be with respect and consideration for the entire department.

With more than a quarter (28%) of public sector professionals looking for new employment opportunities at any one time, organisations must be proactive in recruiting talent. But new talent will not serve an organisation in the future if they're not equipped with the skills accurately identified as being in need. Organisations today are recognising that they simply cannot look to 'fill in the blanks' and recruit strictly based upon 'hard skills' or position-specific experience. They must also take 'soft skills' into account. For example, a talent engineer who's unable to communicate problems or work collaboratively may be a hire that causes more issues than it solves.

Through workforce planning, public sector employers can determine the minimum ratio of hard and soft skill qualities needed for every conceivable function. This 'tagging' function will also help to identify employees with abundant soft skills for future leadership roles.

People come and go from organisations for a variety of reasons, but retirement is inevitable and therefore should be both anticipated and planned for. Armed with a forecast into anticipated retirements, talent managers can anticipate, track and match talent to roles being vacated. Planning in advance, and identifying internal and external talent who can quickly step into these roles, will enable organisations to efficiently fill vacancies before a shortfall materialises.

Unfortunately employees leave jobs for many reasons besides retirement, and often disengagement or better opportunities elsewhere are forces that push talent away from public sector roles. Therefore, it is critical for organisations to take full advantage of workforce planning solutions that measure employee engagement throughout the organisation and across a range of metrics.

By evaluating which departments have the most engaged employees and which have the least, organisations will be able to incorporate best practices from the 'haves' to elevate satisfaction levels among the 'have nots', and retain their expertise for years to come.

SYNERGY OF SYSTEMS

Images courtesy Technology One.

Jonathan Nally

THE MERGER OF SEVERAL SYDNEY COUNCILS IS SEEN AS A GOLDEN OPPORTUNITY TO REBOOT AND RATIONALISE THE NEW MUNICIPALITY’S ENTIRE SOFTWARE SUITE.

The forced merger of councils in Sydney has been in the headlines for years, and with those mergers now taking place the rubber is really hitting the road. But when it comes to the impact on the IT operations of one merged council, it is hoped that that road will be a brand new, six-lane freeway rather than an old, clogged suburban street.

Cumberland Council in Sydney's west was formed from the merger of Auburn and Holroyd Councils, with some of Granville Council's wards thrown in as well. This fusion is necessitating the consolidation and union of many disparate activities and processes. And in 2017, perhaps none is more important than the IT systems.

"It's a huge opportunity," Cumberland Council Executive Manager of Operations Peter Fitzgerald said. "Very rarely are you given a chance to build a council from the ground up. This is a once-in-a-lifetime opportunity for everyone involved in Cumberland Council, or any other merger for that matter. We're in a really unique position where we are literally on the ground floor of something that's going to be around for a very long time."

In a way, an IT renewal was underway well before the merger took place. The former Auburn Council had made the decision to adopt Technology One's enterprise software platform in December 2013, with the rollout commencing in early 2014. "We went live with our financial accounting software first off. We then implemented the enterprise asset management system," said Fitzgerald.

"We were considered quite a leading council in relation to the software, so we were put on an early-adopters program, which was called the Ci Anywhere Early Adopters Program," added Fitzgerald. "That's for councils that are quite advanced in the rollout, and it gives you access to a whole heap of innovation and software upgrades that Technology One have just rolled out now."

Part of that rollout will be removing the reliance on some of the more outdated systems that council had in its possession. "We had a bit of a look just post the merger and amalgamation... at how many applications had. Council had between 100 and 150 standalone applications across the new Cumberland Council, and so we have to merge all those applications into one process," said Fitzgerald.

"Technology One will naturally assist us in doing that. It's really exciting times for us, and especially the Cumberland community."

The merged council began the cut-across of the financial enterprise software late last year. "The enterprise asset management should be completed within 12–18 months, and we then need to make a decision overall about out data location and our data security, ie, do we keep it in a localised server or do we store it in the cloud? We're currently making that decision now," said Fitzgerald.

POWER FOR THE PEOPLE

One of the biggest challenges facing any enterprise undergoing the kind of change seen with Cumberland Council is change management... bringing people along on the journey.

"People get a little bit concerned with change... they get uneasy with change," said Fitzgerald. "But when you look at the bigger picture and you look at what this actually could achieve, you have the opportunity, 1) as an individual, but 2) to be part of the team that can actually build a completely new organisation. And that is just massive."

Fitzgerald cites as an example the situation when the former Auburn Council supplied Toshiba tablets to its outdoor staff in December 2014. "We gave some of those tablets to our younger staff, who were used to operating iPhones and iPads, and within 3 months the tablet was almost rendered useless because the guys wanted it to do 100-odd different things beyond what it could do," he said.

"And that's ultimately because the space is moving so quickly — everyday there's a new app... some functionality being incorporated into the Apples or Androids that our staff want," he added. "So council now has the task of keeping up with all that innovation. It's like a bit of a Pandora's Box — once you start you never stop.

"The existing council has very skilful staff that can accommodate the transition, but there are naturally going to be some technical areas where we're going to need Technology One's help," said Fitzgerald. "Technology One will provide that support when it's required."

Fitzgerald said one of the main focuses of the effort is to try to simplify processes. "As simple as providing a leave form, or applying for training, or having a DA form come across the counter — that can all be done on a digital platform now, and that's what we're really, really keen on having. We're really keen on pushing that type of innovation," he said.

"It's been quite a hard process to begin with, but what we're finding now is that the further we go down the track, we're finding more things we have to move onto a single platform and a single enterprise approach," said Fitzgerald. "You're never going to get it perfect — you're never going to get the whole process perfect, but if you're committed to the challenge of doing it, the long-term benefits will be there for years to come."

SEEING THE BENEFITS

"There are going to be some natural cost savings, but you've got to treat what we're doing as a form of disruption as well. With any disruption you're going to see a lot of efficiency gains," said Fitzgerald. "But naturally working in a local government you

>>

have the responsibility to protect the workers' rights, which will always be accommodated for.

"But like in any space [where] you're going to see efficiency gains, you're going to see productivity gains and you're going to see natural cost savings as a result of it. That's part of the whole merging-of-councils process, is that there are those cost savings there, and we're starting to see some.

"But we want to push innovation, and with any innovation you're going to have disruption, and with any disruption you're going to have cost savings."

According to Fitzgerald, there's a core group of councils leading the way in this kind of modernisation, particularly in NSW. "Councils in Queensland went through it quite some time ago, and councils have adopted this kind of technology previously in other states," he said.

As an early example of the benefits improved systems bring, Fitzgerald cites the time it takes to deploy a works order request to a council truck — which for other councils ranges from hours to days or even weeks. "We've tested it and we can get it down to 5 minutes," said Fitzgerald. "We have the infrastructure and the capability now for a resident to ring up [to report a problem], and we can deploy a works order to the truck in as little as 5 minutes.

"Where we want to differ in the future, is we want to look at GPS-enabled devices as well, so that we can then have an allocation-based system based on geography," said Fitzgerald. "When someone rings up and orders a package [over the internet] these days, you can watch that package get transferred across the entire world and you can keep track of where it is up to and when it's going to get delivered. It should be no different for the public community.

"In the future, if someone wants to ring up and report a pothole or a trip hazard on the footpath, they should be able to see exactly when that footpath is going to be repaired," he said. "They should also be able to see where our resources are in the field, and it should be completely transparent and trustworthy from that perspective.

"These are some of the things we're trying to do now, and that's what's really exciting about the whole thing," Fitzgerald added. "And that's where Technology One falls in line for us — we want to have that transparency and that trust with the community.

"There is a drive to constantly improve on service delivery," he said. "Any government organisation [has] to be seen to be advancing the community's interests at all times. And that's what we want to do here at Cumberland."

> *"Council had between 100 and 150 standalone applications across the new Cumberland Council, and so we have to merge all those applications into one process." — Peter Fitzgerald, Cumberland Council*

Images courtesy Technology One.

Cumberland Council Executive Manager of Operations Peter Fitzgerald

DATA CENTRE DECISIONS

Jonathan Nally

WHILE GOVERNMENTS SHARE MANY OF THE SAME SORT OF DATA CENTRE CONCERNS WITH THE PRIVATE SECTOR, THERE ARE SOME PUBLIC SECTOR CHALLENGES THAT NEED ADDRESSING.

Choosing the right data centre (DC) strategy can be one of the biggest IT decisions a government department or agency will make. Public, private or hybrid; spinning disk or flash; software defined or not — these and other selections (such as addressing security concerns) must be gotten right from the beginning, or endless years of headaches will follow. Fortunately, there are solid guidelines to follow and commercially available solutions that address pretty much every concern a department or agency might have.

To get an insight into the pros and cons of some of the particular nuances of public sector data centre operations, we spoke with one of Australia's foremost experts on the topic, Matthew Kates, country manager at Zerto Australia and New Zealand.

GTR: WHAT DATA CENTRE REQUIREMENTS DO (OR SHOULD) GOVERNMENTS SET THAT ARE DIFFERENT TO THOSE OF PRIVATE SECTOR CUSTOMERS?

MK: The first and most important requirement for public sector data centres is the security clearance levels to which many government organisations must adhere. Government agencies and departments should always place security as the primary consideration, but it's also vital to incorporate resiliency and uptime as important requirements. Government systems are not just internal; they can often be public facing or systems that supply critical information and services to citizens and businesses.

With new digital government services there is an expectation and demand for 24x7 availability so there is little tolerance for downtime. Everything from health records to automated payments can be affected by downtime, and the results can have far-reaching consequences in terms of costs. But we are also seeing greater risk to the reputation of government or their suppliers. So ensuring resiliency in the data centre can be an even greater need for government than their private centre counterparts.

GTR: HOW DO YOU THINK AUSTRALIAN GOVERNMENTS ARE DOING WITH RESPECT TO IMPLEMENTING THEIR DATA CENTRE STRATEGIES?

MK: Government faces ongoing challenges when implementing data centre strategies that the private sector simply doesn't need to consider. There are some elements of government systems that appear to be lagging behind the private sector, particularly in the more heavily regulated financial services industry.

The federal government has driven a consolidated approach to data centres over recent years following the Gershon review in 2008, and more recently we are seeing similar initiatives at the state level. While there is significant value in

© stock.adobe.com/au/Cybrain

a decentralised decision structure and allowing each department and division to manage its own data, it does make it difficult to develop a broad national data centre strategy.

While public sector agencies are not necessarily bound by the same regulations as the private sector, they do have Australian National Audit Office (ANAO) best practice guidelines and the Australian Signals Directorate (ASD) Information Security Manual (ISM)... including the recently expanded Essential Eight recommendations, such as the requirement to have daily off-site backups of important information.

Current technology solutions offer dramatically reduced data loss from the 24 hours that could be lost with a daily backup regime. Systems and data can now be brought back in minutes within seconds of an outage or downtime occurring.

GTR: WHAT ARE THE PROS AND CONS OF EDGE COMPUTING FOR GOVERNMENTS?

MK: Edge computing can offer many benefits, such as making users and teams agile, mobile and flexible. It does, however, increase exposure to security risks like hacking, particularly for those who operate in roles that have access to sensitive data.

GTR: WHAT SHOULD GOVERNMENTS DO TO ENSURE THEIR DC SOLUTION IS STILL ABLE TO DELIVER 5 YEARS FROM NOW?

MK: Commercial scalability is important to consider when looking towards the future of your data centre solution provider. As the department or agency progresses, grows and changes, the services you provide will require the infrastructure and capability of a growing data centre. Looking toward the next few years, it would be prudent for governments to seek data centre solution providers that can provide hybrid cloud capability, allowing for agility, elasticity and scale. This should be true from both an infrastructure and commercial, or cost and billing perspective.

GTR: IS SOFTWARE-DEFINED 'EVERYTHING' THE KEY TO IMPLEMENTING A FLEXIBLE STRATEGY?

MK: Software is key to implementing a strategy that provides scale and elasticity. Moving intelligence to software gives you a level of flexibility that isn't possible when it is held only on isolated physical assets. Yet government should not ignore hardware completely, as there are always advances in hardware technology. Software-defined replication and migration enables a mix of underlying hardware platforms to seamlessly allow applications to run and easily refresh the underlying hardware.

GTR: SPINNING DISK OR FLASH MEMORY — WHICH IS THE BEST SOLUTION?

MK: It is less important to engage in the spinning disk and flash debate and more important to look at application performance needs and cost constraints. The performance required to drive vital apps will drive component choice.

Depending on the performance requirements of the software and underlying data, it may make sense in some instances to sweat older storage assets in an environment for the storage of infrequently used data. Some cases will still see a return on investment when taking into account the ongoing maintenance costs and the ability of the hardware provider to provide ongoing hardware support. This is where software that can manage applications and data across disparate hardware platforms can add considerable value.

GTR: IS OPEN SOURCE NETWORKING AND SOFTWARE THE WAY TO GO FOR GOVERNMENT DCS, OR ARE THEY TOO RISKY?

MK: The very nature of government means there will always be areas of government IT that can never utilise open source due to sensitivity and security requirements. Many areas of government can benefit from open source networking and software, but security requirements mean that this should always be viewed on a case-by-case basis.

GTR: FINALLY, WHAT ARE YOUR TOP TIPS FOR IMPLEMENTING A SUCCESSFUL DATA CENTRE MIGRATION STRATEGY?

MK: There are three key tips in implementing a successful data centre migration for government: protect, automate and test. Finding consistent ways to protect workloads before, during and after migration will decrease risk and increase flow. Testing is important throughout the process, so make sure you can test before you move data and test again to ensure it has arrived in the right state. Automating the migration regardless of infrastructure will make it more successful, reducing risk, time and costs.

ENABLING EFFICIENT COMMUNITIES WITH ENTERPRISE CLOUD

In today's landscape, IT plays a critical role in enabling councils to manage their responsibilities. Manual processes are being replaced by digital applications, giving employees access to resources in the office, at home and in the field.

But despite this, many councils continue to struggle at the hands of legacy IT infrastructures that are not adaptable enough to deliver today's applications reliably. An enterprise cloud platform provides a simple solution to this problem. An enterprise cloud platform combines the best of web-scale engineering and consumer-grade design to natively converge compute, storage, virtualisation and unstructured data management into a single, resilient, software-defined solution that is easy to manage.

The rich machine intelligence, predictable performance, cloud-like infrastructure consumption, robust security and seamless application mobility it brings enables councils to adapt and respond to changing demands and better serve the community.

© sheelamohanachandran/Dollar Photo Club

This means they can virtualise server applications and traditional desktops to efficiently use infrastructure, provide consistent and reliable user experiences on a range of devices and simplify management for IT administrators because the technology runs almost invisibly.

Many councils in Australia and New Zealand have made the move to the Nutanix enterprise cloud platform.

"Nutanix stood out as the clear solution for a number of challenges we were facing, mainly due to its management simplicity, scalability and excellent visibility of server and storage workloads and trends," Mildura Rural City Council Senior Technical Officer Greg Maiorana said.

Mildura is the largest council in Victoria, covering more than 22,000 square kilometres. This presents challenges in delivering IT services to council officers in the more remote areas.

"Nutanix runs everything — it manages our data centre, more than 100 applications, 30 remote sites connected by wide area network (WAN) and a mix of local and Citrix-powered VDI for more than 450 users," said Maiorana. "Historically, even the simplest of upgrades might have taken three months to complete from order to implementation. Nutanix gives us the visibility to monitor trends and growth areas to ensure we are in a position to provide important upgrades instantly.

According to Maiorana, Nutanix has given the council public cloud-like performance but with on-premises presence.

"The platform has reduced the amount of storage space in our data centre by more than 80% and has given us more capacity," he said. "Since the initial installation, we've already expanded our Nutanix environment with an additional host. The flexibility to expand as we need is far more efficient and cost-effective, and Nutanix's compatibility across all major software services gives us control over how we want to grow."

It's a similar story in the Shire of Dardanup in Western Australia.

"Nutanix provides us with a secure on-premises enterprise cloud environment through which we deliver our key workloads and applications, including local government-specific financial management, exchange server, GIS services and SQL along with library and recreation centre management servers, among others," Shire IT Manager Stephen Eaton said.

"It has also enabled us to run our SharePoint farm that various departments use to access all business-critical records and documents without the performance issues we were seeing with our previous infrastructure," he added.

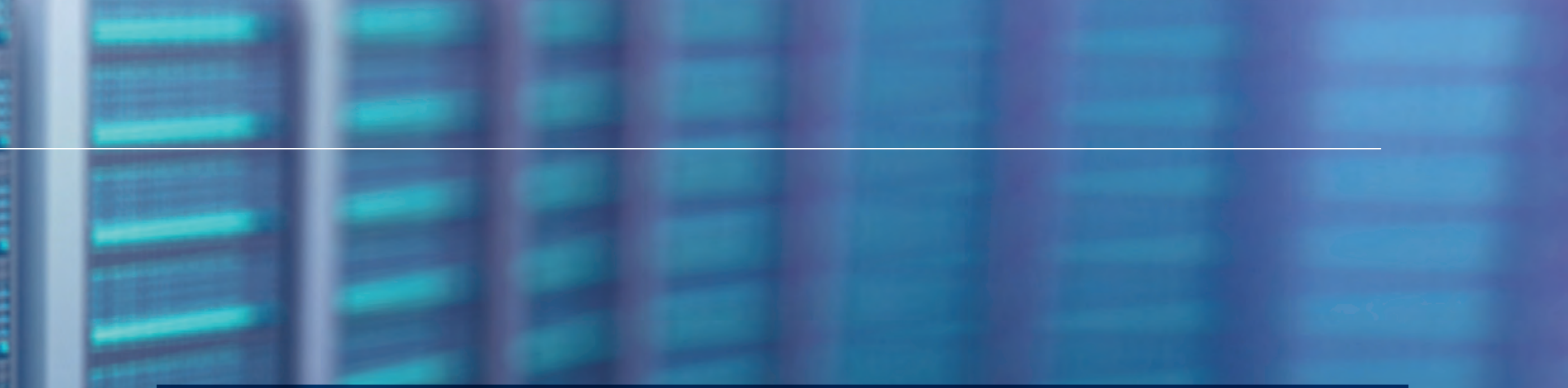
Dardanup is in a regional country area where connectivity is expensive and can be unreliable, and this was a big factor when choosing where to locate the council's data centre and services. "In the past, we've had scenarios where we've been without internet for up to a week, so public cloud is not an option for us," Eaton said, adding that because it's a hyperconverged platform, "Nutanix has allowed us to centralise our data centre, saving two-thirds of the rack space in the process and significantly reducing maintenance times and costs."

Nutanix
www.nutanix.com

2017 SET TO BE THE YEAR OF THE DATA CENTRE

Nathan Steiner, Head of Systems Engineering ANZ at Veeam Software

AS WE START THE NEW YEAR, IT'S CLEAR THAT 2016 WAS A WATERSHED IN HIGHLIGHTING THE IMPORTANCE OF AVAILABILITY AROUND THE GLOBE, BUT IT IS ONLY GAINING MOMENTUM AS CUSTOMERS AND PARTNERS DEMAND AVAILABILITY. OVER THE LAST 12 MONTHS, MASSIVE DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS BROUGHT MANY GOVERNMENT SERVICES TO THEIR KNEES, WHILE ALSO INTERRUPTING BUSINESS OPERATIONS AND HARMING REPUTATIONS FOR SOME OF THE WORLD'S BIGGEST ORGANISATIONS.



There's little doubt that 2017 will be the year data centres will take the main stage and come to dominate IT as government departments and businesses alike look to harness information to provide tailored services to their diverse stakeholder groups. Availability will be a requirement and not merely a 'nice to have' for any department looking to succeed and meet customer demand in the coming year. No longer will stakeholders tolerate downtime; the time has come for every organisation to be available 24/7.

Through the next year, Veeam will continue to help IT teams deliver on the public's expectation to have access to accurate information and critical services on-demand. There has never been more focus on digital delivery of services for government and the seamless delivery of services. Veeam has been solely focused on availability since its inception and is now well positioned to address the four key trends modern organisations and departments face today:

- Blurring lines between public, private and hybrid clouds: A few years ago, the thought of extending data-centre infrastructure to a hyper-public cloud may have seemed a futile endeavour of connectivity, security and a mix of unknown surprises. However, now the market is ready to accept the adoption of hybrid cloud architectures from both the infrastructure and application side. It's already happening and much greater mainstream adoption is on the horizon as agencies look to enhance operational agility and reliability, while ensuring that data and applications are available at any time, from anywhere.
- The explosion of the software-defined infrastructure: It's no secret that the software-defined data centre has been a huge trend in recent years — thanks in part to the popularity of virtualisation. Running applications in a virtualised environment brings many advantages for companies to help build efficiencies, provide reliability and a flexible IT infrastructure to ease management and free time and resources. Through 2017, expect to see more demands on vendors to provide software and services to meet the expectations of the next generation of innovators.
- Stay one step ahead of hackers: Threats from hacking, as well as the proliferation of botnets, and malware (specifically ransomware) will keep IT managers up at night throughout 2017. We've seen enormous burdens placed on organisations looking to maintain availability during 2016, with large attacks on DNS services causing major services to be unreachable during critical times. As more government departments look to provide digital services, the hackers will be nipping at their heels. More than ever before, organisations will need to place additional emphasis on end-to-end data security, backup and recovery to ensure their services remain reliable.
- More data, more possibilities: The data centre of today, and definitely of tomorrow, will increasingly hold more data — both historical and mission-critical. Whether it be an influx of inputs from the Internet of Things, more complex systems or growing amounts of existing data sets, the conclusion is obvious: the data deluge will continue. On the positive side, this will bring benefits to departments looking to leverage advanced analytics to hone their existing operations and provide new services to customers. As the calendar ticks over to 2017, organisations will be able to gain more insight from the data they have collected; helping shape decisions and inform strategy. However, these analytic capabilities will only bear fruit if data is both available and robust. For those relying on advanced analytics to drive operations, any downtime not only halts the ability to transact with customers and suppliers, but also stymies informed decision-making. IT departments will need to direct their attention to maintaining availability of mission-critical systems that underpin their analytics.

Specific predictions are always challenging, but the technology landscape today provides endless possibilities for organisations to provide great services based on the data centre and the information a data centre both houses and delivers. The expectation is that data is available whenever and wherever it is required. Gone are the days where downtime is considered a 'normal' part of day-to-day operations.

In 2017, the data centre will take centrestage and will serve as a critical piece of infrastructure to both store information and provide services to customers, employees and partners alike. Having a plan to ensure availability will be vital to maintaining operations to meet — and exceed — expectations. Success will depend on it.

© stock.adobe.com/au/Abstract Technology

CeBIT AUSTRALIA

OFFICIAL PARTNER

NSW MAKING IT HAPPEN

The largest business technology event in Asia Pacific

23-25 May 2017
ICC Sydney, Darling Harbour

SAVE $100 off any conference pass simply by quoting the promo code **WWF17** at the checkout

Featured international keynotes:

EUGENE KASPERSKY
Chairman & CEO
Kaspersky Lab

RANDI ZUCKERBERG
Founder & CEO
Zuckerberg Media

DENNIS ANDRUCYK
Deputy Associate Administrator, Space Technology Mission Directorate
NASA

GREG WILLIAMS
Executive Editor
WIRED Magazine

Immerse yourself in 8 strategic conference programs with insights from over 250 leading executives

Big Data & Analytics	Cloud	Cyber Security	Enterprise Mobility	eGovernment	FinTech	Digital Health	StartUp

PLUS a guaranteed seat during any of our Strategic Panel sessions

- CEO Panel
- Women in Tech
- CIO Panel
- Innovators Panel
- Next Gen & STEM
- SME Business Growth

Register at cebit.com.au/register

Deutsche Messe

#CeBITAus
www.cebit.com.au

CHANGE THE REGULATORY ENVIRONMENT TO ENABLE INNOVATION

DIGITAL INNOVATION NEEDS MORE THAN TECHNICAL ADVANCES — IT ALSO NEEDS ORGANISATIONAL AND REGULATORY CHANGE.

Al Blake, Principal Analyst,
Ovum's Australian Government practice

Public servants are continually encouraged to do everything faster in the name of innovation. Unfortunately, saying something doesn't necessarily make it so, and that is especially true when there is a disconnect between the desire for 'agility' and the organisational environment in which it must be delivered.

Often the CIO has endeavoured to deliver 'agile' outcomes, while grappling with organisational environments that need months to procure software or recruit new staff. Frustration is compounded when legislative or regulatory compliance concerns are thrown into the mix. Fortunately, the tide seems to have turned, with recognition that the rules and regulations under which agencies do business are at least as important, and maybe more so, than the database engine they use.

Late last year, the newly rebranded Digital Transformation Agency announced its agenda to implement simplified digital government services at the national level. Apart from the rationalisation of its efforts to a smaller number of projects, the most interesting aspect is recognition of the impact of the wider regulatory environment on the ability to deliver "changes to existing policy and legislation that blocks change will underpin the success of the transformation".

This is a crucial and, as yet, neglected aspect of the innovation agenda, as in many instances discussion of new approaches is pre-emptively shutdown by invoking a (real or perceived) legislative impediment. When discussion reaches "the legislation won't allow us", investigation halts — rather than considering whether a) the interpretation is correct and b) whether the legislation should be changed. Placing potential legislative change front and centre sends a welcome message about the new approach.

Practical expression of the new attitude can be seen in changes to the myGov authentication service, where the user experience to date has often been frustrating and disappointing. Using long, random numeric IDs and complex password reset procedures may provide adherence to an ultrahigh-grade security requirement — but at the expense of usability.

To address this myGov will move to using email addresses and mobiles for authentication — after all, if it's good enough for online banking, surely it should be acceptable for tax and welfare transactions?

A similar understanding of the importance of taking a rational approach to the legislative environment has been identified across the Tasman, where a cross-agency working group on collaboration in the NZ government called out a tendency to use 'security' or 'privacy' issues — real or imagined — to prevent unwanted change. Furthermore, it cautioned senior executives and project managers to sanity check claims that something can't be done "because of privacy".

The increased understanding that innovation will not come about through purely technical implementation but that it is fundamentally dependent on external, non-technical, environmental factors is a welcome sign of increased maturity. It will help CIOs to assist agencies in holistic digital transformation — rather than being simply viewed as a problem for IT to 'fix'.

It's time for next generation PTT

Kevin Noonan, Lead Analyst, Government, Ovum

© stock.adobe.com/au/ChiccoDodiFC

Telstra LANES® offers a robust, ready-made solution to public safety's need for a national mission-critical data service.

Two-way radio has been a core part of emergency services operations since its first use in the world by Australia's Victorian Police Force in 1923. Over time, Land Mobile Radio (LMR) has been a transformational technology for the sector. It has not only helped drive numerous productivity improvements, but it has also been pivotal in saving lives.

However, LMR is not without its shortcomings. It is physically constrained by bandwidth and by the restrictive assignment of radio channels. In times of emergency, individual radio channels can become overcrowded, and when this happens important messages can be lost.

Today, LMR is just one technology in an increasing array of digital capabilities. Officers in the field now need data… and lots of it. It is common for first responders to use mobile phones, tablets, cameras and IoT devices for a variety of advanced services such as mapping, video streaming, data analytics, personal health management and office automation.

Recently released global industry standards have significantly bolstered the value proposition for advanced push-to-talk (PTT) technologies. These standards lay a common framework and agreed performance requirements to meet the stringent requirements of mission critical systems.

The standards have targeted Mission Critical Push-To-Talk (MCPTT) as a specific use case. (Other standards 3GPP is developing include targeting Mission Critical Video and Mission Critical Data.) There is also another project (Mission Critical Core) to recognise the common standards that need to exist across a converged data, video and PTT market.

With the majority of MCPTT standards now well defined, it is time for an industry response, using these standards to create common and strategic solutions.

Achieving mobile broadband

In 2015, the Australian Productivity Commission was tasked with undertaking a 'first principles' analysis of the best way to obtain a mobile broadband capability to meet the long term needs of public safety agencies.

The Commission considered three delivery options — dedicated, commercial and hybrid — in detail, and found "a commercial approach is the most cost-effective way of delivering a [public safety mobile broadband] capability".

The Commission went on to find that "a dedicated network is nearly three times more expensive than a commercial option. The cost difference between a hybrid and commercial option is lower and narrows as the size of the dedicated network component decreases."

Since the time the Commission delivered its report, one particular risk factor has increased in importance. There is a growing opportunity risk that arises through inaction and delay. Public safety mobile broadband (PSMB) is one critical piece of the infrastructure necessary for delivering the next generation of hardware and software services for the sector. Without an operational PSMB solution, it will be extremely difficult if not impossible, to guarantee the performance and quality of service requirements set in the MCPTT international standard.

The need for LTE

In times of emergency, network performance is crucial. Network congestion at public events, such as New Year's Eve celebrations, creates big headaches for network planners. Such congestion has essentially become a question of economics. Each provider needs to make a business decision about how much spare capacity it should build into its architecture to cater for peak loads in known locations.

However, most providers would understandably struggle to deal with unexpected peaks of unknown magnitude in unknown locations. This is exactly what happens in times of disaster.

If emergency workers are sharing the same mobile network as the general public, all their carefully procured advanced capabilities slowly grind to a stop if there are no Quality of Service mechanisms in place to provide emergency workers with a prioritised service. Consider the problems during 9/11 in New York, the London bombings, New Zealand's earthquake, or Australia's summer bushfires and floods. In these cases, it is impossible to predict the location and severity of the disaster. It is not commercially viable for telecommunications operators to purchase and configure sufficient mobile spectrum to cope with an event that may happen in that location once every hundred years.

But an example of a technology that can provide the core network infrastructure necessary for the development of mission critical broadband is Telstra's LANES® solution.

After a long period of testing, Telstra has launched a commercial release of Telstra LANES®, which can address PSMB requirements as outlined in the Productivity Commission's report. Moreover, the Telstra LTE network has the added flexibility to deliver a commercial option or a hybrid option, depending on a customer's particular needs.

Telstra has already trialled Telstra LANES® in conjunction with public safety organisations in a range of situations, such as the G20 Leaders' Summit in Brisbane (2014) and an AFL grand final with 100,000 people (2015).

The Telstra LANES® approach is conceptually similar to the move toward cloud-based as-a-service solutions that are becoming increasingly popular in other parts of the IT industry. Indeed, many governments are now mandating a 'cloud first' policy as a lever for driving change.

The advantages of adopting Telstra LANES® include:

- A significantly smaller investment is required due to the reuse of existing infrastructure;
- Avoiding the allocation of excess spectrum for public safety services, which would be underutilised for most of the year;
- A coverage footprint equal to today's commercial LTE networks is available immediately;
- Public safety will benefit from technology upgrades deployed for the commercial network, such as Video over LTE, 5G, IoT support and additional spectrum bands.

Future directions

Since there will be clear benefits for public safety agencies from delivering next generation PTT, it is now time to chart a path forward. Over the past year, there has been a perfect convergence of development in core infrastructure: international standards for MCPTT are largely well defined, Telstra LANES® has been launched, a new generation of ruggedised LTE devices have come onto the market.

It is encouraging to see that key industry players are already coming together to focus on operationalising these solutions. In March 2016, Telstra, Motorola and Ericsson announced a collaboration to develop next generation PTT facilities for the public safety market. The partner companies will work to progress the PTT technology through concept testing in Australia, and will collaborate in standards forums globally.

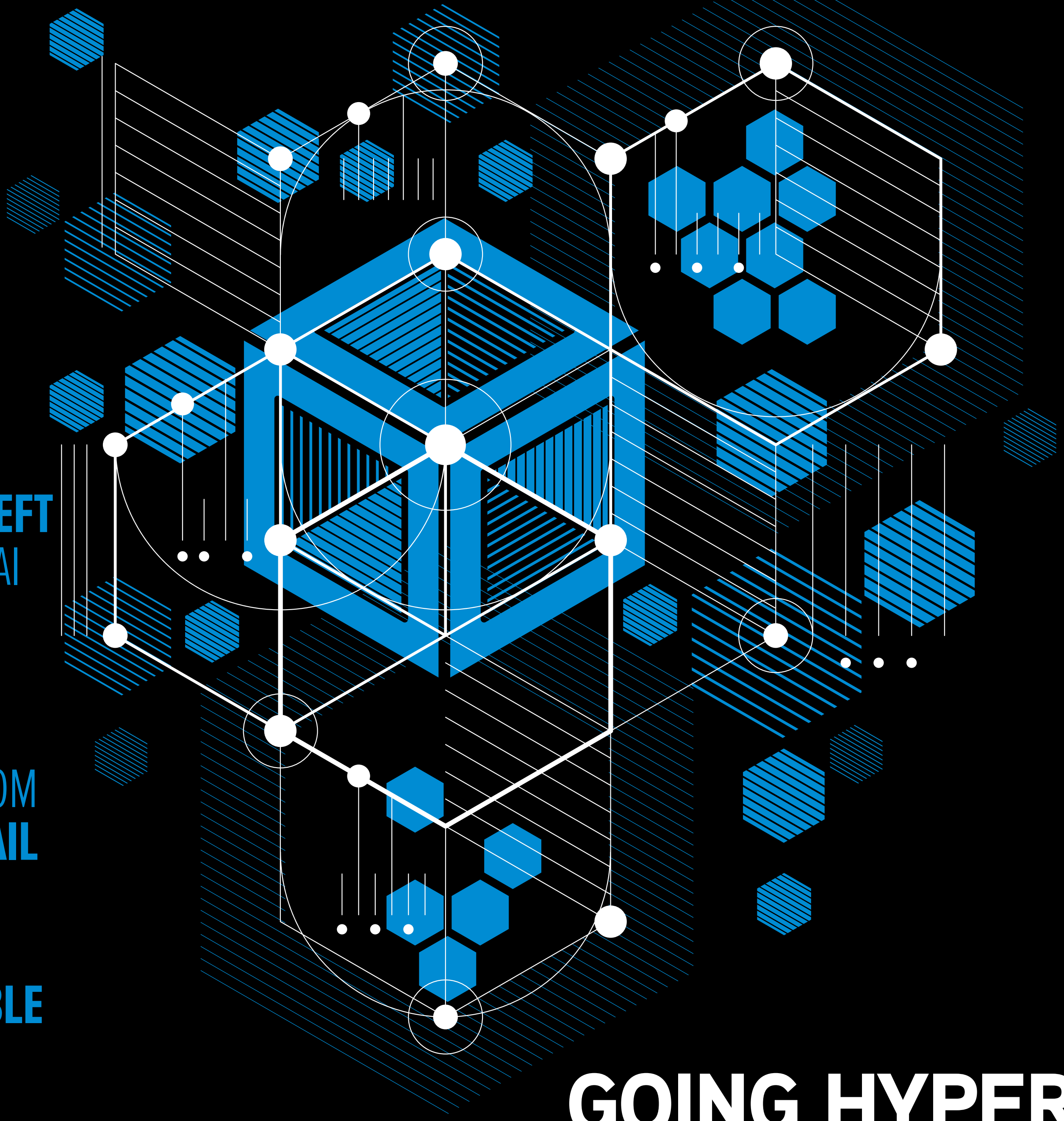
Join Alex Stefan (Public Safety Industry Executive, Telstra) and Kevin Noonan (Global Lead Analyst for Government, Ovum) for an online discussion on "Transitioning to Public Safety Mobile Broadband" to be held 11am, Thursday 11 May 2017.

Register now at the "Virtual Event" tab in the link below.
www.telstra.com.au/business-enterprise

In conclusion, the days of big budgets, big assets, slow procurement and silos of public sector infrastructure are long gone. Legacy equipment such as LMR will continue to play an important role, but it is time consider a much broader transition strategy to converged mission critical voice, data and video.

The challenge for public safety agencies is to find better ways to engage with industry partners to facilitate a planned and orderly transition to these next-generation solutions.

biz tech review



DON'T BE LEFT BEHIND BY AI AND BOTS

LESSONS LEARNED FROM **#CENSUSFAIL**

TIME TO **GET RESPONSIBLE** WITH DATA

GOING HYPER

WILL HCI SAVE YOUR BUSINESS?

Q1 2017
PP100009359

technology Decisions

informing technology decision-makers

2015
2016

We are proud to welcome you to this new hybrid magazine from the Technology Decisions media group. By combining two of Australia's premier tech magazine brands, WF Media, our authors and advertisers are able to reach a broader audience of private and public sector technology decision-makers across Australasia.

Our lead BizTech Review story in this issue deals with hyperconvergence. It's one of those buzzwords that's been around for the past few years, and which seems to be gaining more currency. But while some swear by its perceived benefits, others are not so sure that it's right for every use case. Our author, Andrew Collins, has sought out what the experts have to say about it... so that you can make up your own mind.

Don't forget that CeBIT Sydney is rapidly approaching (23–25 May). As always, it promises to be an outstanding event packed full of world-class speakers and fascinating vendor exhibits. We'll be there, and we hope you will be too — please drop by our stand and say hello.

Jonathan Nally, Editor
jonathan@technologydecisions.com.au

Q1 2017

INSIDE

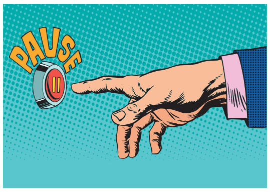
cover image © stock.adobe.com/au/Sylverarts

FEATURES

Many commentators spruik the benefits of adopting hyperconverged infrastructure, but not everyone is convinced it's the right choice for every company.

Instead of accepting 'mandatory evolution', companies can choose a path that frees up funds and expertise.

Australia's health sector is sitting on a data goldmine, the full exploitation of which could lead to better health outcomes and reduced costs.



The Census failure has reduced the public's confidence in a once-trusted fundamental government service.

HOW TO GO HYPER AND NOT REGRET IT

Andrew Collins

© stock.adobe.com/au/arabel0305

MANY COMMENTATORS SPRUIK THE BENEFITS OF ADOPTING HYPERCONVERGED INFRASTRUCTURE, BUT NOT EVERYONE IS CONVINCED IT'S THE RIGHT CHOICE FOR EVERY COMPANY.

Infrastructure is continuing its trend towards integration, a pattern that has seen traditional siloed infrastructure deployments — in which organisations buy, deploy and manage server and storage infrastructure in separate stacks — give way somewhat to converged infrastructure, in which customers buy pre-integrated bundles of servers, storage and networking. Hyperconverged infrastructure (HCI), one recent incarnation of this increasingly integrated endeavour, appears to be gaining popularity across the globe.

It's worth noting at the outset that there are a variety of competing accounts of exactly what HCI entails — how the term should be defined — and many of those differences are driven by different vendors trying to convince potential customers that their specific flavour of HCI is the best option. So in quantifying the precise nature of HCI it's perhaps best to defer instead to the analyst firms, which provide their definitions after casting their gaze across a wide and varied market. In Gartner's report 'The Positive Disruption of Hyperconvergence Adoption in the Midmarket', analyst Mike Cisek uses the term 'Hyperconverged integrated systems' (HCIS), which is defined as: "Tightly coupled compute, network and storage hardware that dispenses with the need for a regular storage area network (SAN)". In HCI systems, according to this definition, storage management functions and compute provisioning are delivered through a management software layer and/or hardware.

IDC defines hyperconverged systems as "pre-integrated, vendor-certified systems containing server hardware, disk storage systems, networking equipment and basic element/systems management software". In IDC's eyes, a key difference between HCI and other types of converged or integrated systems is that HCI systems can provide all their compute and storage functions through the same server-based resources.

Global sales figures certainly seem to suggest that HCI is taking hold. IDC's latest Worldwide Quarterly Converged Systems Tracker report, which provides statistics on revenues in the converged systems market, indicated that HCI sales appear to be increasing, while other related technologies — integrated infrastructure, certified reference systems and integrated platforms — are experiencing a drop in sales. According to that report, hyperconverged systems sales more than doubled from Q3 2015 to Q3 2016, leaping 104.3% from US$279.3m to US$570.5m. Sales in the other three converged categories covered by the report fell between those two time points.

But while these sales figures might indicate that HCI is gaining global market share, it's not necessarily the case that it is dominating infrastructure conversations in Australian companies. Peter Hall, an advisor at research and advisory firm IBRS, said that his organisation sees more of its clients looking to move to cloud-based services, rather than HCI, to replace or expand their computing power. "One reason is so that they don't have to worry about acquiring, managing,

>>

maintaining and upgrading their own infrastructure, and of course a desire to have the right amount of capacity available at all times," he said.

Hall also said that local organisations considering integrated infrastructure aren't focusing specifically on HCI. These organisations may also be looking at converged infrastructure (CI) solutions, he said, "or CI software only solutions which can give them more flexibility with the hardware components. It will still be a case of purchasing the right sort of systems to be fit for purpose, and at an appropriate investment level."

ALL THINGS CONSIDERED

There are several issues that organisations should consider when buying or implementing HCI. According to IBRS's Hall, the first issue involves looking at the market and deciding what sort of solution will best suit the organisation.

"HCI may not even be the answer. HCI vendors typically supply appliances that package up all the vendor's components: servers, storage, networking, virtualisation and the vendor's software in the one box. The goal is of course rapid and simple deployment," he said. "Alternatively, some vendors are offering a software only approach to CI, which can provide a cheaper and perhaps more flexible option, but probably with more effort required in the deployment versus a fully integrated HCI."

Organisations considering HCI solutions should also cast their eyes to the future, and ask questions about upgrades and flexibility. "How do the specific offerings get upgraded? How rigid is the architecture and how flexible is it, especially if a new innovation comes out that might be important to the organisation," Hall said. He suggested a hypothetical case where an organisation deploys an HCI solution, and later down the track a new hypervisor is released that the organisation wishes to use — but the vendor doesn't support that hypervisor, and may not support it for some time. "Issues like this may drive an organisation to consider a CI software only approach, or a traditional CI offering."

> *"One reason [companies adopt HCI] is so that they don't have to worry about acquiring, managing, maintaining and upgrading their own infrastructure." — Peter Hall, IBRS*

Along similar lines, the Gartner report 'Beware the 'Myth-Conceptions' Surrounding Hyperconverged Integrated Systems', penned by Gartner analysts George J Weiss, Julia Palmer and Andrew Butler, nominates several questions that infrastructure leaders need to consider in relation to HCI solutions: "What are the form factors, configurations and management control points, and are they delivered as interchangeable components? Are the components disaggregated so that they can be upgraded on individual technology life cycles and integrated for maximum performance and efficiency — for example, solid-state drives (SSDs) versus hard-disk drives (HDDs), non-volatile RAM

(NVRAM) and Peripheral Component Interconnect Express (PCIe) cards?"

If an organisation does go with HCI, Hall said they should consider how much flash storage will be needed. Given that flash costs more than traditional storage, they should ask whether an HCI offering comes in all-flash, or if it allows hybrid configurations. Additionally, "When investigating the various offerings from the vendors, consideration should be given to issues like hypervisor support (what are the options), flexibility of the hardware components, management and security capabilities, and scalability limitations. These will vary amongst the vendors."

IDC Australia Vice President, APeJ Cloud & Services Group Chris Morris nominated three issues an organisation should consider when looking at HCI: 1) whether an HCI offering's architecture is compatible with or suitable for the planned workload, 2) whether the required level of support is available from the vendor and its ecosystem, and 3) how suitable the ecosystem of applications providers and SIs is for the organisation's industry. "The business managers buy the applications that need the platforms, and they will want relevant applications and experience," he said.

© stock.adobe.com/au/everythingpossible

VENDOR CHOICE

The market for HCI solutions now includes older traditional infrastructure vendors that are offering HCI solutions, as well as specialist HCI vendors that only came into existence sometime in the last 10 years or so. As such, an organisation deliberating over HCI solutions may itself be torn between an older (and potentially more reliable) traditional vendor and a relative new (and potentially more risky) vendor.

"There is always an element of risk with small or new vendors for hardware or software. And given that the HCI market has become very competitive and demanding of R&D investment it is likely that some will fail or, if they have unique capabilities or market presence, be acquired," said IDC's Morris. "However, the selection depends on the risk assessment by the buyer — it could be that the necessary product life is short or that the target workload can be easily ported to another platform. If the risk assessment shows that then the use of a smaller vendor's solution could be OK."

Hall said that an assessment of a vendor would also include examination of the depth of their local personnel; their level of experience, spare parts and logistics; and how rapidly they are growing locally. He added that organisations should consider these issues based on where they are in Australia. As an example, Hall asked: "What is a vendor's ability in Perth versus Sydney?"

SKILLS

Traditional siloed infrastructure — with separate stacks of compute and storage — is in many organisations managed by separate server and storage administrators. One of the supposed drawcards of HCI is that these infrastructure elements can be managed through a single, unified management console. As a consequence, if an organisation does go ahead and replace its traditional, siloed infrastructure with HCI, it theoretically may no longer need those specialised administrators.

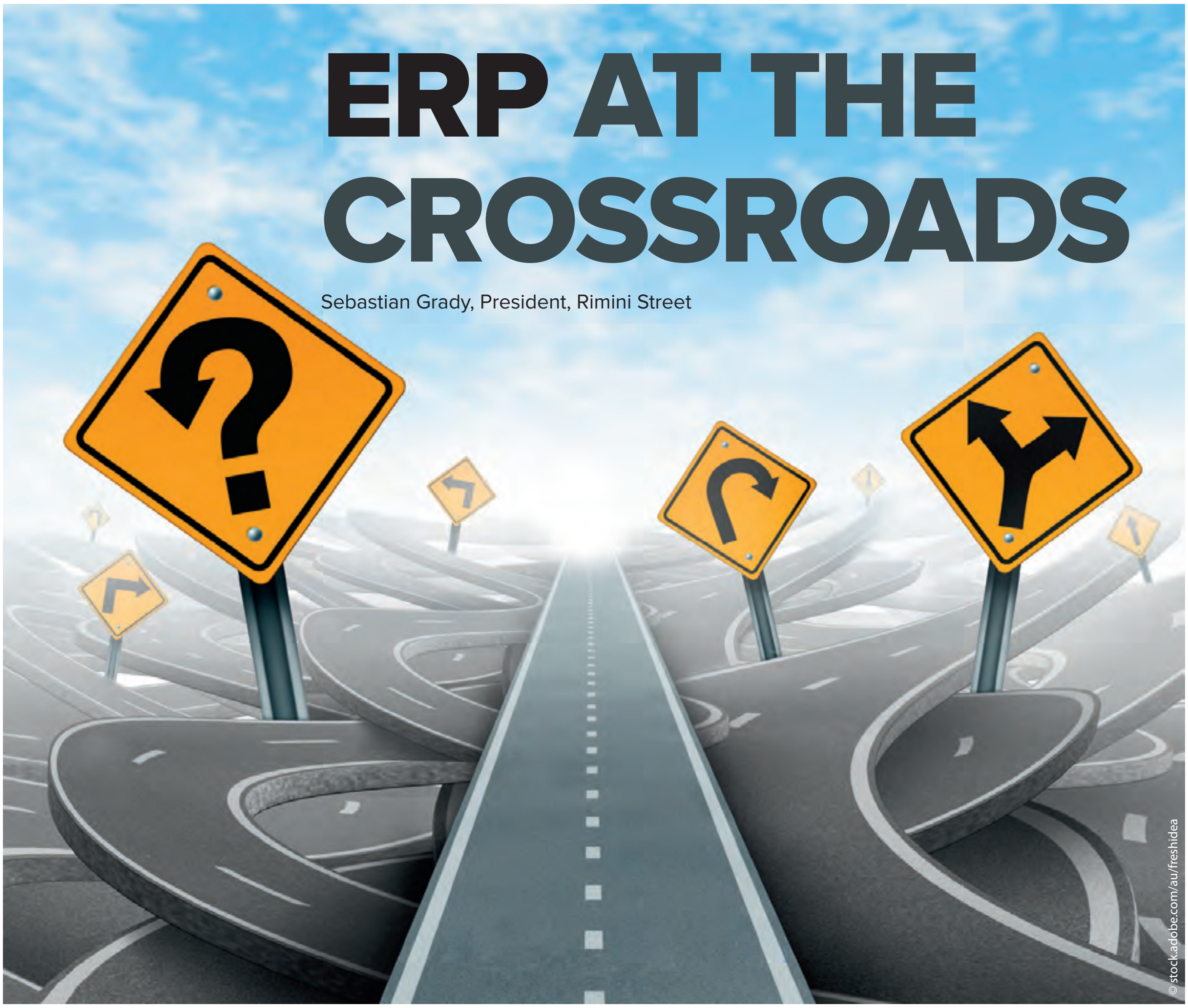
Hall noted, "It is true that one of the promises of HCI systems is that they are supposed to be easier to manage through a single environment, and that includes the servers, storage and network". However, he added, "It may take years for an organisation to completely replace one style of computing with another, so IT staff will continue to be required, and will most likely evolve to manage these new HCI environments. You may have been a server specialist in the past, and now you learn to be an HCI specialist."

And when it comes to planning and sizing systems, "skills are still going to be required to understand how to determine the server capacity required, as well as the storage, and the plans for backup and mirroring of the storage", Hall said.

Morris said that some organisations do indeed find themselves with unnecessary server and storage admins following a move to HCI. "But organisations are retraining staff to deal with software-defined environments and new systems management platforms. They're a different set of specialised skills that is additional to what they already have — the need for the old skills won't go away quickly as it will be some years before the old systems are replaced with HCI."

ERP AT THE CROSSROADS

Sebastian Grady, President, Rimini Street



© stock.adobe.com/au/freshidea

INSTEAD OF BLINDLY ACCEPTING VENDOR-DICTATED ‘MANDATORY EVOLUTION’, COMPANIES CAN CHOOSE A NEW PATH THAT FREES UP FUNDS AND EXPERTISE AND FOCUSES ON OVERALL VALUE.

When I talk to CIOs from some of the world’s leading brands that run enterprise resource planning (ERP) software, they tell me they are at a crossroads with their software strategy. The fundamental choice they must make comes down to this: Should they follow the vendors’ upgrade path or is it time to consider other options?

It’s not a simple question because the challenges these CIOs face today are unprecedented. Their companies have been burned in the past by the rush to ‘stay current’, but they know they need to invest in digital transformations and analytics to improve the customer experience and run smarter in order to compete.

At the same time, 89% of their IT budgets are gobbled up by ongoing operations.

HOW DID WE GET HERE?

In the 1990s and early 2000s, when most ERP customers started their journeys, they bought into continuously upgrading their ERP software. No matter which release they started with, they often spent millions of dollars to get their ERP systems implemented.

Along the way, giant software vendors listened to their customers and created real enhancements that delivered real value.

>>

HYPAFOX

WARREN & BROWN TECHNOLOGIES

THE PERFECT BALANCE BETWEEN DENSITY & USABILITY

HYPAFOX | MTP®/MPO SOLUTION:

- Patch Panels
- Cassettes
- Adaptors
- Patch Cords
- Trunk Cables
- Array Cables

Contact us today for a tailored-made solution.

WWW.WBTNETWORKS.COM.AU

But over time as the software became more mature, the real enhancements that delivered real value slowed to a crawl, and for many customers support quality faltered.

To add insult to injury, some ERP vendors raised maintenance fees and many customers revolted.

During this time period, a vast majority of ERP users created customisations and integrations to give themselves a competitive edge. And according to actual case data, 65% of customer issues are related to customised code, not the base vanilla software.

The giant software vendors don't support custom code, and some CIOs say that the very existence of custom code just gives their ERP provider an excuse to avoid delivering support.

Software doesn't wear out, so what makes it break? Once the vast majority of bugs are discovered in the new release of software — in let's say, 2 or 3 years after its general availability — what causes it to break? Two things: 1) You change the code, or 2) You change the data.

The software then sees conditions it has never seen before and can therefore react negatively.

TOWARDS A NEW STRATEGY

The good news is that ERP customers have excellent options. The first and most basic strategy that we're seeing is a wait-and-see approach with regard to new software the vendors are developing.

For these customers, we believe they should consider a third-party support and maintenance strategy to free up as much as 90% of their overall annual support and ongoing maintenance costs.

Still, there is an even better reason, and that's to be able to implement an innovation agility strategy as a result of the move to independent support. With ERP maintenance and support cost savings realised, CIOs can redirect these funds into initiatives that really make a difference to their business.

Smart CIOs recognise the benefits of maintaining a stable ERP system but, instead of standing still, focus their attention and energy on adding innovation around the edges of their ERP core.

There is simply no complete ERP cloud solution available that can fully replace the robust ERP systems that have matured over 30+ years. By adopting a hybrid IT strategy, for example — as many analysts, including Gartner and Forrester, advise — CIOs are able to maximise the value they've already built into their core systems of record and re-invest the considerable savings into digital systems of engagement that help their businesses grow and compete.

With additional funds, organisations can make investments in best-of-breed technologies such as mobile, social and big data.

© iStockphoto.com/Clint Spencer

Smart CIOs recognise the benefits of maintaining a stable ERP system but, instead of standing still, focus their attention on adding innovation around the edges.

OPEN ROAD AHEAD

The CIOs I talk to are really starting to like this strategy of keeping their core ERP and innovating around the edges. Plus, it's an easy strategy to communicate that makes immediate sense. Consequently, CEOs and line-of-business managers are getting behind it, too.

An organisation's core goal is to maximise customer value while minimising waste. Instead of optimising a department or particular technology stack the old way, the IT department gets to take part in optimising the movement of products and services through entire value streams that flow horizontally across technologies, assets and departments to customers.

Instead of blindly following a path of vendor-dictated 'mandatory evolution', companies can choose a new path that frees up funds, frees up expertise and focuses on overall value that has the power to deliver tangible business benefits.

From what I'm seeing and hearing out and about in the industry, more companies have arrived at similar crossroads and are turning towards strategies that maintain their core ERP while encouraging targeted investments in truly new applications.

This sort of thinking really changes what a business can accomplish and in what time frame. It's the kind of innovation agility that energises me because — for the first time in a long time — it helps put organisations on a truly smarter path.

RETHINKING CLIENT COMMUNICATION

© stock.adobe.com/au/nd3000

When KPMG's Sydney team relocated to new offices at the top of the International Tower in Barangaroo last year, the firm capitalised on a significant opportunity to upgrade client services and boost employee satisfaction and productivity at the same time.

This has included launching new digital services, opening shared innovation spaces where clients and consultants come together to tackle complex business challenges, and the provision of open plan offices, organised by industry solutions and client teams where employees of all levels sit next to one another.

Speaking about the role of technology in this new era of the company, KPMG National Managing Partner, Markets and Growth James Hunter outlined how new applications and platforms are helping employees, and the organisation, achieve more.

"Technology is the fundamental enabler for the way KPMG operates," he said. "Cloud and digital services have fuelled our move to the digital world, and provided a seamless and efficient way of working that empowers every employee to deliver on our client strategy — solve complex challenges, steer change, disrupt sectors and grow through collaboration and innovation."

A core component of KPMG's digital transformation is the firm's use of Microsoft Dynamics 365, which is improving communication and collaboration among the company's 5500 employees in Australia.

"We are growing rapidly [and] providing a diverse range of services to over 15,000 companies in Australia," said Hunter.

"With rapidly changing customer demands, including most senior executives seeking integrated solutions, bringing across KPMG capabilities to deliver outcomes faster than ever before, we need to operate more effectively and seamlessly.

"Microsoft Dynamics 365 enables KPMG meet these challenges, and provide a much stronger client experience every time we interact," he added.

"The enhanced capabilities around internal collaboration and 360-degree client views are features we've been looking to develop for over five years, and moving from our old system to the Microsoft platform has helped deliver them."

In provisioning its services, KPMG will commonly hold relationships with a number of stakeholders in each of its clients — from a handful in growing and family businesses up to 100+ among larger organisations.

This creates challenges in efficiently keeping track and sharing most recent updates — including lead and opportunity management, and event management — limiting KPMG's ability to offer its full range of services to tackle the challenges at hand.

The need to address this challenge was made more pressing as KPMG encouraged employees to be more agile in their working day.

Using Microsoft Dynamics 365, KPMG now has a single view of each client contact, with a record of the latest interactions, updates and opportunities available on any device at any time.

Employees are increasingly finding themselves empowered to deliver an improved standard of service due to the level of insight they now have.

"We needed a vehicle through which we could better understand client issues across different people within the same organisation," Hunter said.

"Microsoft Dynamics 365 brings these insights into one single platform, enabling us to offer a better value proposition for clients.

"There is no longer a need to recap discussions between team members, with updates now taking place rapidly and seamlessly — sometimes on the way to and from meetings via the mobile application.

"Client experiences have improved significantly as a result, and relationships and the way they are managed have risen to another level."

KPMG selected Microsoft Dynamics 365 following a tender process, where the firm noted three features that made the technology the most suitable.

Beginning with usability, KPMG needed a tool which was easy to use, and which would integrate seamlessly with its existing Microsoft stack.

Microsoft Dynamics delivered on this with the solution integrating effortlessly into Outlook, as well as being offered through a mobile application, ensuring updates and interactions could be easily and efficiently logged in near real time.

Secondly, the firm wanted a comprehensive CRM platform that required minimal customisation to allow future updates to be incorporated rapidly as they became available through Microsoft's trusted and intelligent cloud services.

The third requirement was for a CRM platform that could be deployed quickly and easily.

"Integration, ease of access and strict security protocols around entire business records were crucial factors in our selection of Microsoft technology," said Hunter.

"The solutions deployed allow us to fulfil a real desire to offer every part of KPMG to each of our clients through a simple and secure platform," he added.

"Being a large organisation with thousands of users this can sometimes be complex, but this is not the case with Microsoft Dynamics.

"We have had a fantastic response to the rollout — [just] last month we had each of our 450 leaders using it on their mobile devices."

Delivered ahead of time and on budget, KPMG's Microsoft Dynamics deployment is driving a cultural change at the firm and shaping new innovations being made available to clients.

MONITORING 4.0

Andrew Timms, Sales Director, APAC, Paessler AG

MONITORING THE BILLIONS OF CONNECTED 'THINGS' WILL BE CRITICAL IN THE IoT AGE.

Image courtesy Paessler AG.

We've all seen the numbers — experts predict that by 2020, the IoT will reach 26 billion units and hundreds of billions of dollars in revenue. While it's safe to say the IoT will be transformative for businesses, all of the possibilities opened up by these new connected devices will also bring new challenges to overcome. For the network administrator of the future, the rising complexity brought on by more than 200 billion connected 'things' creates a whole new set of challenges. Forget about BYOD and start thinking about BYOT — Bring Your Own Thing — where the 'thing' could be anything from a coffee machine, to wearables, to cars.

Monitoring these devices will be critical in order to guarantee a constant flow of reliable data. For instance, wearable technology in healthcare. Devices can monitor a patient's pulse or heart rate and, if there's a sudden drop, an ambulance could automatically be dispatched to find the patient via GPS. But if the software crashes, the device gets disconnected or is simply turned off, the patient might die.

All of these connected devices need sensors, networks, back-end infrastructure and analytics software to make them useful. So the question is, who monitors the monitor?

One of the biggest challenges will be integrating a heterogeneous group of devices into an extant network structure, particularly in industries where there is a huge scope of possible 'things'. Data that gets picked up has to be added to the central IT system in order to enable further processing, useful display and a basis for action. Monitoring things isn't so different from monitoring network devices — what matters is getting relevant data that can be analysed and put to a purpose.

When network monitoring was first introduced, the technology was mostly used to monitor physical IT devices like routers or switches (Monitoring 1.0). Then, as virtualisation became more prevalent, new concepts and functionalities had to be found in order to gather and process new kinds of relevant data (Monitoring 2.0). The next logical step was to run applications in the cloud. To give users of SaaS solutions and other cloud applications continuous access to their productive environment, the connection to the cloud has to be closely monitored (Monitoring 3.0).

The IoT launches a new era in network monitoring — Monitoring 4.0. This is because with every new thing connected to the network, the amount of data that can and should be monitored is continually growing.

Due to the heterogeneous nature of the 'things' and applications, many of which we probably can't even conceive of today, it will be difficult to have an out-of-the-box solution that covers every possible scenario. What is interesting is that we're already seeing IT pros ride this evolution and adapt to the developments. By utilising customisable sensors, IT admins are currently monitoring everything from office buildings to swimming pools.

Although we might stand at the beginning of this revolution, it's important to start planning for the future now. Sensible integration with the existing IT infrastructure should not be taken lightly. The goal is to create intelligent networks that can control each other autonomously along the entire value chain.

© kasto/Dollar Photo Club

DIAGNOSIS DATA

HOW ANALYTICS CAN IMPROVE MEDICAL DIAGNOSES AND REDUCE FRAUD

Adrian Smolski, Solutions Architect ANZ, MapR Technologies

AUSTRALIA'S HEALTH SECTOR IS SITTING ON A DATA GOLDMINE, THE FULL EXPLOITATION OF WHICH COULD LEAD TO BETTER HEALTH OUTCOMES AND REDUCED COSTS.

The Australian healthcare sector is undergoing continuous automation and digitisation, with many new initiatives aiming to make it easier for patients to use medical services and manage their health, while reducing costs.

In the past few months alone, Cairns Hospital became the largest regional hospital in Australia to go paperless through its Digital Hospital initiative, while eHealth NSW rolled out a major digital transformation project across its electronic media records in NSW hospitals. While these are very promising developments, the sector is still going through tough times, trying to find answers to rising costs that are driving patients to cancel their private health insurance.

Digital analytics technologies can help healthcare organisations stay on top of these and other challenges. Let's pick just two — the delivery of better medical diagnoses, and fraud management.

TAPPING INTO BIG DATA

In recent years, medical institutions, government entities and hospitals have collected massive quantities of data that are yet to be effectively utilised to benefit the industry and its customers. Australia's health sector is sitting on a data goldmine, which could be the key to solving critical issues that are costing our economy and our citizens' health.

And still, many healthcare professionals and organisations have yet to invest in sophisticated data analytics solutions to help uncover opportunities hidden in unstructured data (80% of healthcare information) that comes from a wide range of sources — professional and personal medical devices (eg, health apps and wearables), doctors' notes, lab results, correspondence between professionals and institutions, hospital and clinical data, and financial data.

IMPROVE DIAGNOSES

Medical diagnoses are now expected to be fast and precise, with healthcare practitioners and facilities looking to provide more proactive and simplified care for their patients. In today's digital age, in-hospital patients' vital signs are continuously monitored and every individual is empowered to monitor their own health at anytime and anywhere through wearables, apps and smart devices.

These sources of data represent opportunities to fine-tune diagnostics, either by preventing a condition or by better addressing it. All the data collected by medical monitors, whether they are in-hospital or worn by the patient in their everyday life, needs to be analysed, cross-referenced and effectively leveraged to affect results. Combining real-time event data with machine learning algorithms can provide physicians with insights to enable lifesaving decisions and effective interventions.

For example, Flinders University recently developed an analytics program that is able to simplify dysphagia diagnoses, speeding up results and eliminating the need for X-rays. Another example — predictive modelling of data derived from electronic health records (EHRs) is being used for early diagnosis, for example for reducing mortality rates linked with congestive heart failure and sepsis.

REDUCING FRAUD

Another significant benefit that effective data analytics can bring is the clear, accurate financial insight that can lead to fraud reduction and prevention.

In 2016, Medicare lost $1.6 million through fraud by doctors and others, and private health insurers have been shown to be still very much challenged by the fraud issue. Finding ways to prevent and monitor fraud would benefit the entire industry, as well as patients.

Dig data and analytics tools could be a game changer here, as the technologies available today can prevent, identify and neutralise fraud based on the analysis of unstructured data sets.

For example, based on patient records, billing details and history, healthcare organisations can use analytics to detect anomalies such as a hospital's over-utilisation of services within short time periods, receipt of services from different hospitals in different locations simultaneously or identical prescriptions for the same patient filled in multiple locations. Based on historical data and specific patterns, analytics tools can also predict future risks and help prevent fraud before it happens.

In the United States, for example, the Centers for Medicare and Medicaid Services prevented more than $210.7 million in healthcare fraud in one year using predictive analytics. United Healthcare also transitioned to a predictive modelling environment based on a Hadoop big data platform, identifying inaccurate claims in a systematic and repeated fashion which generated a 2200% return on its big data and advanced technology investments.

As EHRs continue to grow and evolve, combining records with data analysis across multiple data sources will enable better diagnoses and services for patients, while reducing costs and providing better patient experiences.

Getting security right
becomes more important than ever in 2017 for the connected enterprise

Companies need security across people, things, processes and information, with safeguards at the intersection of the internet and internal networks.

Data security has always been paramount for global enterprises, because the consequences of a breach are just too devastating to take a 'wait and see' approach. The Ponemon Institute's 2016 study on The Average Consolidated Total Cost of a Data Breach put the number at US$4 million, or US$158 per lost or stolen record. That's not including the lingering damage to a company's reputation and customer confidence.

But as critical as security has always been, we at Equinix don't think there's ever been a time when it will be more important for companies to have sound digital security strategies in place than in 2017.

The enterprise today operates in an environment where digital assets are becoming more internetworked and distributed. The continued proliferation of the cloud and interrelated technologies, like the Internet of Things (IoT), guarantees that trend will continue. As businesses become more digital, global and interconnected than ever before in 2017, their security challenges will be greater than ever before.

Companies will need to solve for security across people, things, processes and information. They'll need effective safeguards at the intersection of the internet and their internal networks. They'll need to own the security of their applications and data within a hybrid or multi-cloud environment and maintain company and government compliance regulations. If they can't figure it out, they won't be successful, and may not even survive. According to the National Security Alliance in the US, as many as 60% of hacked small and medium-sized businesses go out of business after six months.

Solving the security challenge is a daunting prospect, but the enterprise isn't without resources. Here are some projections about what's ahead, and how companies will handle it all.

- Security will become distributed as new approaches to safeguarding data and transactions emerge, such as blockchain for digital ledger transactions. Blockchain records and verifies all transactions across a public network of distributed participants in a chain that is open and visible to all. This makes transactions faster and less costly, while lowering the risk of fraud.
- Increased interconnection will enable customers to move from individual point security solutions to more flexible solutions, such as Security-as-a-Service, a cloud-based service that can be provided anywhere within an enterprise's network. Cloud-based security offers speed of implementation, ease of maintenance, and economies of scale that increase the scope and effectiveness of security programs at lower cost. Cloud-based security services are also offered for specialised attacks such as distributed denial of service.
- As hybrid cloud adoption accelerates, the enterprise will realise that cloud providers only take responsibility for securing the cloud infrastructure, and they must own the security of their applications and data within the multi-cloud environment.

At Equinix, our global data center and interconnection platform, Platform Equinix, enables enterprises to ensure their security is meeting the evolving requirements of digital businesses by enabling private, direct and secure interconnection that bypasses the public internet. Every one of our interconnection solutions and services can be deployed as a component of an Interconnection Oriented Architecture (IOA) strategy on Platform Equinix, which our customers are using to bring themselves as close as possible to their people, data, cloud and locations, improving security for themselves and their end users.

Learn more about securing your data and leveraging an IOA strategy to develop secure IT infrastructures at Equinix.com.au/ioa

Equinix
www.equinix.com

WHAT 'SOFTWARE DEFINED' MEANS FOR HARDWARE

© stock.adobe.com/au/djvstock

Matthew Kates, ANZ Country Manager, Zerto

HARDWARE CHOICE IS BECOMING LESS IMPORTANT AS SOFTWARE-DEFINED SOLUTIONS GIVE IT DEPARTMENTS THE POWER TO MANAGE SERVICE LEVELS RATHER THAN MACHINES.

When it comes to running IT departments, the type and brand of hardware that CIOs and IT managers choose to use is becoming less important. Cloud computing has been a catalyst for this. When a workload is moved to the cloud, considerations and planning become about service levels, not the hardware. But the decline of hardware as a strategic part of the IT decision-making process is not just about cloud… it has also extended into the on-premise data centre.

We have moved to a point where every part of the IT stack can be software defined. There is now less concern about compatibility between vendors, as IT departments manage service levels rather than hardware. As an example, flash disk will often still perform faster than spinning disk, but for IT departments that are managed through software, the type of disk doesn't matter.

It is more important to look at application performance needs and cost constraints. The performance that is required to drive vital apps will then drive component choice.

Depending on the performance requirements of the software and underlying data, it may make sense in some instances to sweat older storage assets for the storage of infrequently used data. Some cases will still see a return on investment when taking into account the ongoing maintenance costs and the ability of the hardware provider to provide ongoing support.

DATA CENTRES

A software-defined data centre removes dependence on a single hardware vendor and allows interoperability between hardware from multiple vendors as well as reducing the risk of trying new technologies from new vendors. The net effect is that the large hardware vendors are having to reinvent themselves; they are embracing the software-defined approach and, in doing so, becoming open to working with other vendors.

Software is key to implementing a flexible data centre strategy that provides scale and elasticity. If organisations are tied to isolated physical assets, they are inherently locked in to the capability of those. This means businesses will not have the ability to adjust as they grow and change, and can make it more difficult to move to the cloud further down the line.

While hardware is becoming less important, organisations must not ignore hardware entirely. There are always advances in technology. Software-defined replication and migration does allow for a mix of underlying hardware platforms to seamlessly allow applications to run, and to allow for ease of refreshing the underlying hardware.

The approach for architecting software and hardware is changing, too. Customers want to know about workload protection and workload mobility, something that is becoming increasingly important.

A hardware, hypervisor and platform-agnostic approach resonates because the application and workload is becoming the primary concern. Software that abstracts the underlying infrastructure enables CIOs and IT managers to focus on application service levels and at the same time reduce focus on simply keeping IT running. The net effect is that hardware decisions will continue to become less strategic.

©stock.adobe.com/au/ studiostoks

#CENSUSFAIL SHOWS NEED FOR PS CULTURE CHANGE

Kevin Noonan, Lead Analyst, Government, Ovum

THE CENSUS FAILURE HAS REDUCED THE PUBLIC'S CONFIDENCE IN A ONCE-TRUSTED FUNDAMENTAL GOVERNMENT SERVICE.

The implications of the Census denial of service attack go far beyond a single security incident. This is no longer just about a technical problem to be solved. In the light of the recommendations from two government enquires, there are much bigger issues about governance and leadership, as well as some long-term questions about entrenched public service culture.

As Bureau of Statistics senior executives ponder the recommendation for them to attend a cyber boot camp in the coming year, it is time to move the spotlight from technology, contracts and blame attribution. There is now a clear need to look at the impact of digital transformation not only in the way government services are delivered, but also in terms of the implications for the underlying ground rules of public sector leadership.

IMPORTANT IMPLICATIONS

On Census night, many Australians settled down after dinner to fill out their online Census form, only to be locked out due to a series of distributed denial of service (DDoS) attacks.

No data was lost, no government IT infrastructure was compromised, and the Census was eventually completed. From a technical purist perspective, there was no actual security breach, and the system was successfully shut down before there could be any chance of damage.

However, the damage in public credibility had already been done. The Census gained its own hashtag #CensusFail, and commentary in social media quickly took over from official government messaging. It was no longer a situation of government informing the public, but the public informing government via a wide-ranging social media discussion. The ABS had already lost control of the agenda, but doggedly kept going with the original public information campaign. As the technical recovery progressed, the widening gap between the unchanging information campaign and public commentary became all too apparent.

The loss of public support is a significant challenge for any government agency. The government sector differs in some very important ways from the private sector. Typically, government does not have competitors in the market, and citizens are frequently compelled by law to deal with particular government agencies. However, in any democratic government, the role of the public service is to serve the public. In a 21st-century digital world, community feedback is very quick and very direct.

NEED FOR CHANGE

In the aftermath of the DDoS attack, the federal government commissioned its Cyber Security Special Advisor, Alastair MacGibbon, to undertake a comprehensive review of the events. The Senate also decided to undertake its own separate review. Both studies took a broader view of the events.

The MacGibbon report was particularly clear in its findings about the need for broader cultural change to address the reality of digital government. The report's executive summary commenced: "The Australian Government's new paradigm for online engagement and services is not coming. It is already here... Cyber security is about availability of services and confidence in government in a digital age. And the public's confidence in the ability of government to deliver took a serious blow, more so than any previous IT failure... But crucially important is the need to understand how the Census got to the point where the cyber security arrangements brought into question the trust and confidence in a fundamental government service. The public's lack of confidence will linger."

NUMBERS TELL THE STORY

In the end, the Census did achieve an impressive online response rate of 96.5%, with 58% of households participating online. However, the damage is played out more importantly through measures of public sentiment. In the past, the ongoing success of the Census has been due to its reputation as a reliable and valued tool, both for business and for the community. This time, government surveys found the Census had taken a significant blow in the eyes of the public. A massive 42% of the public said that to some extent the Census had been a failure, and 33% agreed to some extent that the data collected by the Census was unreliable.

Looking forward, the big challenge will be to deal proactively with the realities of digital government. The digital genie cannot be put back into the bottle.

IT'S TIME TO **BE RESPONSIBLE** WITH DATA

ORGANISATIONS NEED TO EMBRACE THE EMERGING DOCTRINE OF 'CORPORATE DIGITAL RESPONSIBILITY'.

Joshua Kennedy-White, Asia Pacific Managing Director, Accenture Security

Organisations with access to personal data are continuously faced with a range of difficult questions concerning the ownership of that data, including: Do appropriate restrictions exist for those governing how the data is used? Who enforces such restrictions? Where do you draw the line between what is public and what is private?

As organisations continue along the path to becoming digitally responsible, there are five principles they should embrace.

Stewardship. Organisations must use the data they collect in a responsible and secure manner. Companies such as Apple and Amazon are leading the way by refusing to share detailed personal data with third parties. Meanwhile, platforms such as Google and Facebook face increasing pressure to be more transparent about how they share anonymised data to third parties, the extent to which they personalise advertising based on personal data and the indefinite storage of personal information on server logs.

Transparency. Organisations need to develop strategies to manage growing customer expectations for greater digital transparency. For example, Spanish telecommunications giant Telefonica is beginning to offer customers opt-in choices for sharing personal data in exchange for new services. The company also incentivises active data sharers with rewards.

Empowerment. Organisations can use data in their control to offer individuals greater digital empowerment, supporting them to make better decisions about their health, education and finances. Here in Australia, the Commonwealth Bank uses data and predictive analytics captured via an interactive platform to help customers make better-informed personal finance decisions. Although there may be short-term costs (for example, fewer overdraft charges going to banks), with this approach, the bank experiences the benefits of long-term customer loyalty and enhanced reputation.

Equity. As customers become more aware of the value of their data, organisations will need to offer greater digital equity. This means viewing data collection as a two-way transaction. Launched in 2014, New York-based social network Tsū earns its revenue through on-site advertising. The firm distinguishes itself by sharing 90% of its advertising revenue with its users via a sliding scale that rewards them according to how active they are on the site.

Inclusion. Organisations should seize the opportunity to practise greater digital inclusion, multiplying the impact of their digital assets for social good. For instance, in 2014, Johnson & Johnson allowed Yale University to access all of its clinical trial data to help advance science and medicine — positioning itself favourably with consumers and medical professionals alike. In the same year, Twitter launched data grants to share tweet data with selected researchers in order to address issues ranging from urban flooding to foodborne illness.

The gap between principles and practice remains significant. Today, any responsible digital strategy will have to be implemented at the core of the business as a key lever towards providing enhanced differentiation and new sources of growth.

KASPERSKY lab

ZUCKERBERG MEDIA

NASA

WIRED

EYEING THE VALUE IN 2017'S TECHNOLOGY WAVE

ARTIFICIAL INTELLIGENCE AND ROBOTS ARE THE BUSINESS AREAS LEADERS SHOULD BE FOCUSING ON THIS YEAR.

Manish Bahl heads Cognizant's Centre for the Future of Work in the Asia Pacific

An economy based on platforms, algorithms and bots is emerging, yet many business leaders are still currently underestimating the challenges and opportunities these will bring. Those businesses are sitting on untapped cost savings and new revenue sources.

Optimising an organisation's middle- and back-office operations can be a hidden goldmine for cost savings. Companies such as TriZetto are using software robots to decrease healthcare payer costs by as much as 90% for some middle-office business processes. Others such as Blue Prism are applying bots to handle risk, fraud, claims processing and loan management in banking to save millions.

Denying these savings is essentially a self-imposed tax. Automation of processes within business reduces costs, and smart leaders are using that newly freed digital dividend as investment fuel for innovation.

If businesses were to invest in only one new technology in 2017, they'd be wise to earmark artificial intelligence (AI) for this cost. The majority of business leaders see AI combined with analytics as the leading driver of business change in the next two to five years.

Businesses can apply AI to change the way work is done and how customers engage with a business throughout the entire value chain of an organisation, process by process. AI technology is redefining entire job functions — from call centre processes to manufacturing and logistics functions. In the long term, AI should create more meaningful work and more value.

Analytical, communication and learning skills, as well as the ability to relate to other people, are still all vital for business success and will never be replaced by robots.

Investing in AI technologies will actually empower workers, helping them to enhance specific skills and focus on tasks that are more interesting and ultimately add more value to the business. Freed from administrative tasks, staff can be redeployed to value creation activities rather than service functionality.

Organisations that are behind the technological curve face a 'laggard penalty' — the difference in both cost and revenue performance due to technological disability. Laggard penalties exist across all industries. In financial services, for instance, digital laggards, on average today, have a total economic impact of about 3.1% of all costs and revenue.

How can organisations turn this around? A first step is to benchmark against others in the same industry, and then get a rough idea of whether or not technology can drive profit in terms of both saving on costs and delivering new revenue opportunities. This analysis will help create the much-needed financial justification for taking the bold steps needed towards becoming digital.

Business leaders in APAC expect an average of 116% return on their digital investments by 2018. These strategic investments can help organisations win new markets, innovate and improve efficiencies, while also helping to initiate critical internal change.

COMMS CONNECT 2017

Events for critical communications users and industry

Important dates for your diary ...

Sydney
7-8 June 2017
Sydney Showground

Melbourne
21-23 November 2017
Melbourne Convention and Exhibition Centre

Comms Connect WELLINGTON

11-12 April — Te Papa Museum

In association with the *Radio Frequency Users Association of New Zealand* (RFUANZ), Comms Connect Wellington, a two-day conference and exhibition, returns to Te Papa Museum on 11-12 April, 2017.

A series of case studies, technical presentations and workshops are supported by an extensive exhibition of local and international suppliers and manufacturers. Day one sees networking drinks on the exhibition floor followed by the very popular annual RFUANZ Gala dinner and awards night.

By registering to attend this year's conference and exhibition in Wellington, you'll hear what the experts have to say, advance your understanding of critical communications and the land mobile unique industry event — do not miss this once-a-year opportunity!

Registration Open — visit www.comms-connect.co.nz to register or for more information.

Lanyard Sponsor

Cambium Networks

Platinum Sponsor

tait communications

Gold Sponsor

STI Survey Technologies

Delegate Lounge Sponsor

Aviat NETWORKS

Supporting associations and media organisations

TCCA DMR DMR APPLICATIONS TETRA APPLICATIONS dPMR digital LTE APPLICATIONS RadioResource INTERNATIONAL IWCE

Media Partner

comms critical

Association Partner

RFUANZ Radio Frequency Users Association of New Zealand

In conjunction with the RFUANZ Gala Dinner and Awards Night
11April – Te Papa Museum, Wellington

Book your tickets with your conference package or visit www.rfuanz.org.nz

For further information regarding speaking or sponsorship at Comms Connect events in 2017 please

CALL OR EMAIL PAUL DAVIS +61 2 9487 2700 | pdavis@wfmedia.com.au
NARELLE GRANGER +61 2 9487 2700 | ngranger@wfmedia.com.au

comms-connect.com.au **comms-connect.co.nz** follow us on