GTR

GOVERNMENT TECHNOLOGY REVIEW

DEALING WITH THE INEVITABLE **DATA BREACHES**

GOVERNMENT'S **SECURITY SCORECARD**

DELIVERING E-LEARNING FOR LOCAL COUNCILS

DIGITAL REVOLUTION

THE TECHNOLOGIES TRANSFORMING OUR EMERGENCY SERVICES

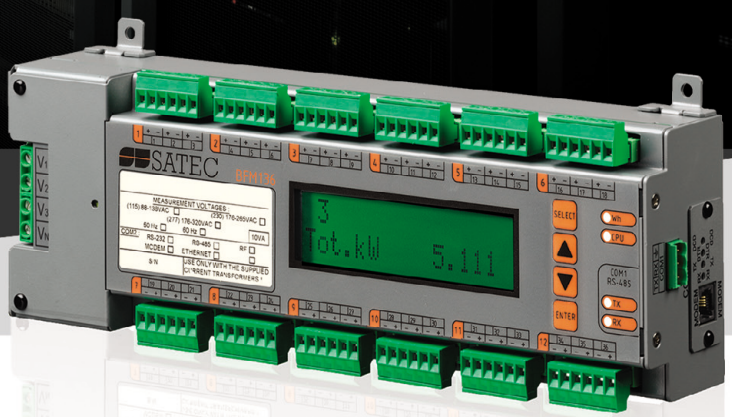
OCTOBER 2016 • ISSUE 33
PP100021607

CLOSING IN ON THE DARK WEB • DELIVERING ON PROJECT SUCCESS

THERE IS A DIFFERENCE

SUB-METERING FOR DATA CENTRES

- ACCREDITED
- PROVIDING UP TO 90% SPACE SAVING
- INNOVATIVE DESIGN
- COST EFFECTIVE INSTALLATION
- ONE DEVICE, UP TO 36 CIRCUITS
- FREE LICENCE PAS SOFTWARE
- EXPORT TO MS EXCEL OR ACCESS DATABASE



Smart Metering

- NMI/Pattern Approved
- Electricity Billing
- Interval Data
- Demand Load Control
- Time Of Use (TOU)
- Real Time Clock
- Ethernet Communications (TCP/IP)
- Accuracy Class 0.5S

Energy Efficiency

- NABERS
- Green Star
- BCA J8
- BEEC

T +61 2 4774 2959
sales@satec-global.com.au
www.satec-global.com.au

SATEC
Powerful Solutions

Contents

10
Beyond the communications gap
Social media, the Internet of Things and big data gain traction within citizen-minded emergency services agencies.

18
Changing customs brings project success
Stunted by outsourcing, the UK's Revenue and Customs service used cultural transformation to reinvent its application infrastructure.

22
The inevitable breach
Traditional methods don't work anymore, so it's time for a 'secure breach' approach.

24
Roundtable: Security scorecard
How good are governments at keeping our data safe?

30
Early adopters
The process of digital transformation is fostering innovation and cultural change.

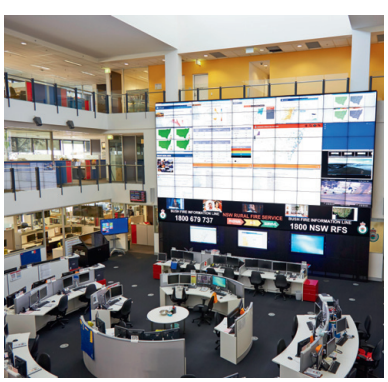
october 2016

36
Closing in on hackers
Increasingly powerful analytics engines are helping law enforcement agencies find cybercriminals hiding on the 'dark web'.

40
The IoT's role in health and aged care
Mobility devices, the IoT and app development are helping providers improve healthcare outcomes while also boosting their own balance sheets.

42
Configuring the cloud
Understanding the essential characteristics of cloud-based solutions and security requirements is critical for making informed decisions.

46
On the open market
New South Wales' GovDC Marketplace is setting an example for similar efforts in other states.



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

Insider

New ways of doing business

It seems axiomatic, but in this day and age, all public sector enterprises are seeking new ways of doing business with their customers and clients, both internal and external.

Nowhere is that more evident than in the emergency services sector, where new digital capabilities are enhancing organisations' abilities to gather and disseminate information, streamline workflows and emergency responses, and analyse important data both in real time and retrospectively. This issue's cover story describes several ways in which new technologies are enabling Australian emergency services agencies to improve efficiencies while saving lives.

But there are other ways in which governments are putting new paradigms to work. The New South Wales Government's GovDC Marketplace is a perfect example. The service-based marketplace is designed to make it easier and quicker for government agencies to commission cloud services. And it's fair to say that, so far, it has been a tremendous success, with potential far beyond what its architects originally envisioned.

That could just as easily be said of the transformation taking place within the UK Government's Her Majesty's Revenue and Customs department, which has learned that starting small and empowering its staff is the key to ensuring the success of digital reform projects. Finding that the traditional outsourcing approach wasn't working, the HMRC team realised that adopting the UK Government Digital Service guidelines — 'understand users' needs', 'build a service that can be iterative', 'create a service that's simple and intuitive enough that users succeed the first time through' — would be one of the keys to success.

The other major field in which new ideas are needed is information security and the prevention of data breaches. While it's tempting to think that everything would be okay if only we all followed basic security rules, the reality is that the crooks are continually finding ways to exploit weaknesses in security systems and in the vulnerabilities of the humans who design and use those systems.

It's a problem that all public sector organisations must face head on. Governments hold some of the most sensitive and private information about citizens, so it is vital that that information be protected. In this issue, we look at ways in which governments are, or should be, safeguarding our precious data. To that end, for our roundtable, we sought the views of respected industry security professionals, each of whom shares their insights into what governments are doing right, what they're doing wrong and what they can do better in the near future.

Jonathan Nally, Editor
gtr@wfmedia.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
Tanya Barac, Odette Boulton, 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

Printed and bound by SOS Print+Media Group
PP 100021607 • ISSN 1838-4307

SECRETS ... WE ALL HAVE THEM

Protecting your personal, business proprietary and customer's information is vital. Don't risk it being exploited.

Providing the only direct national secure destruction service with local teams in each state, Shred-X is the highest certified and government accredited secure destruction provider in Australia. By partnering with Shred-X, you are assured of a complete chain of custody and an environmentally sustainable solution.

It's not only best practice it's the law.

Shred-X provide:

- **Digital media & hard drive destruction**
- **Paper-based document shredding**
- **Office cleanouts and archive destruction**
- **Product and uniform destruction**
- **e-Waste recycling and IT end of life asset management**
- **Paper recycling and Printers solutions**

Contact SHRED-X today on 1300 SHRED-X (747339) for an obligation free privacy assessment.
e. info@shred-x.com.au
w. shred-x.com.au

BESTPRACTICE CERTIFICATION ISO9001 QUALITY MANAGEMENT SYSTEM
BESTPRACTICE CERTIFICATION ISO14001 ENVIRONMENT MANAGEMENT SYSTEM
BESTPRACTICE CERTIFICATION AS4801 OH&S MANAGEMENT SYSTEM
BESTPRACTICE CERTIFICATION ISO27001 INFORMATION SECURITY MANAGEMENT SYSTEM
NATIONAL ASSOCIATION FOR INFORMATION DESTRUCTION AAA CERTIFIED

SHRED-X SECURE DESTRUCTION
"OUR BUSINESS IS MAKING SURE NO-ONE KNOWS YOUR BUSINESS"®

OUR BUSINESS IS MAKING SURE NO-ONE KNOWS YOUR BUSINESS ®

Headlines

Data.gov.au getting major overhaul

The government is preparing to build the next generation of the data.gov.au open data portal, which will introduce new functionality to improve usability and data publishing.

The Department of Prime Minister and Cabinet's Public Data Branch is working with the CSIRO's Data61 to overhaul the platform.

Under the project the Public Data Branch's Data Infrastructure and Government Engagement (DIGE) team and Data61 specialists will seek to transform data.gov.au into a world-leading example of open public data infrastructure.

A prototype of the new system demonstrating improved search functionality across multiple data repositories will launch late this year.

Further prototypes will be developed in 2017 focused on improved data publishing and data quality, better spatial publishing, and integration between the portal and the National Map geospatial database.

To support the prototyping process, PDF files harvested from Geoscience Australia repositories, including maps and publications, are being made available on the data.gov.au portal. There are now just over 23,000 discoverable datasets available through the site.

DIGE meanwhile plans to conduct a training program to help users understand and publish data to the portal.

The current Data.gov.au site went live in 2013. It was built on open source data platform software CKAN.

As part of the government's National Innovation and Science Agenda, Data61 was instructed to "use data analytics to connect disparate government datasets for public release and publically release them on open data platforms".

WA launches interactive spatial planning map

The Western Australian Government has launched a new online interactive map designed to let government agencies and the public access spatial planning data for any parcel of land in the state.

PlanWA has been developed by the Planning Institute of Australia and launched by Planning Minister Donna Faragher.

Image courtesy of yaruman5 (via Flickr) under CC BY-SA 2.0

Property owners, businesses and local government stakeholders will be able to access relevant planning schemes and policies, including information on zoning and residential density codes, for any parcel of land.

Users can also use the platform to tailor maps for their own use and connect to aerial imagery to further improve the planning process.

Data is collected from the Western Australian Whole of Government Open Data Policy and Shared Location Information Platform.

Faragher said around 100 local WA governments do not have an online mapping system for planning purposes, and PlanWA will be able to compensate for this absence.

"Those local government authorities which don't have a mapping system on their websites will now be able to access this online resource to assist with planning for their local areas and provide more information to their communities," she said.

"Having information such as zoning and residential density codes can help [users] make more informed decisions, particularly in relation to any future development that may or may not be able to occur in an area."

Headlines

US appoints first federal CISO


Image courtesy of Karen Neoh (via Flickr) under CC BY 2.0

The Obama administration has appointed the USA's first federal chief information security officer (CISO) as part of its Cybersecurity National Action Plan.

Gregory Touhill, a retired brigadier general in the US Air Force, has been selected for the position. In his new role, Touhill will drive cybersecurity policy, planning and implementation across the government.

Touhill is currently deputy assistant secretary for cybersecurity and communications at the Department of Homeland Security's Office of Cybersecurity and Communications.

In a blog post, US CIO Tony Scott said the US CISO will lead the team that has been at the forefront of driving cyber policy and practices across federal agencies.

"Strong cybersecurity depends on robust policies, secure networks and systems and, importantly, a cadre of highly skilled cybersecurity talent," he said.

"The CISO will play a central role in helping to ensure the right set of policies, strategies and practices are adopted across agencies and keeping the federal government at the leading edge of 21st century cybersecurity."

Touhill will be assisted by the newly appointed acting deputy CISO, Grant Schneider. Schneider is currently director for cybersecurity policy for the White House's National Security Council staff.

Scott said the deputy CISO role was created after studies of successful organisational models across government determined that partnering a career role with an appointed senior official is both the norm and beneficial.

Global policymakers sign ITU smart city declaration

Policymakers from around the world have pledged to take the actions required to transition to smart sustainable cities at the International Telecommunication Union's 6th annual Green Standards Week.


© stock.adobe.com/au/jorisvo

More than 650 participants, including ministers, mayors, businesses and academics, have agreed to the Montevideo Declaration in Uruguay, which aims to address the sustainability challenges arising from an increasingly urbanised population.

The UN estimates that 70% of the world's population will be living in cities by 2050, which will present major challenges in terms of supplying basic requirements including food, water and energy efficiency while ensuring economic, social and environmental sustainability.

The declaration promotes the use of international technical standards and KPIs to achieve sustainable development in urban areas and meet these challenges.

It encourages the use of open data platforms and a central knowledge base, as well as developing practices for e-waste management and improving ICT accessibility.

The Montevideo declaration also promotes smart sustainable cities and technologies as key elements of the UN's new urban agenda, which will be adopted at the global Habitat III summit next month.

In a separate but related development, nearly 400 entrepreneurs, experts and policymakers have pledged a commitment to ICT education and training to help companies achieve the sustainable development goals through digital transformation initiatives.

At the ITU's Global ICT Capacity Building Symposium in Naiobi, participants discussed expected future priorities for capacity building and new skill requirements in today's fast-changing ICT environment.

MOBILITY
MADE FOR GOVERNMENT

NETCONNECT

With NetConnect - Work is an Activity, Not a Place.

NetConnect allows you to **carry your office in your pocket** & perform all your office activities from anywhere, just as if you were sitting at your desk. NetConnect requires **zero data migration**, running alongside your existing IT infrastructure. Users can **become mobile in a matter of hours,** with no change to your internal security policy.

Gartner predicts by 2017, half of all employers will require employees

to supply their own device for work.

Enterprise Grade Security - Out of the Box.

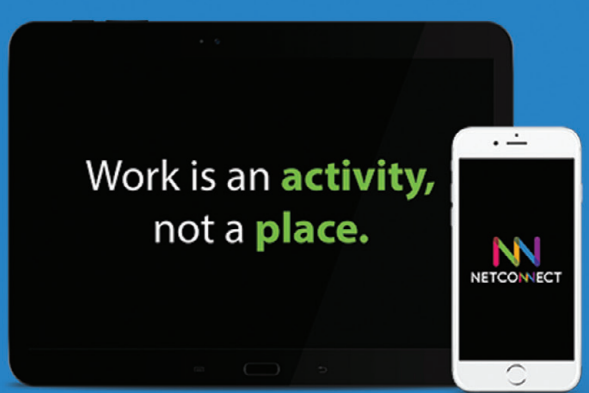
NetConnect comes standard with multi-layered security offering industry leading data encryption & never stores data on a user's device. Employees can use their personal devices with no security risk to your infrastructure. All this ensures that **NetConnect is trusted by governments,** as well as law enforcement & healthcare agencies globally.

See For Yourself

Download our free mobile apps for Android & iOS or jump on to **netconnectdemo.com** through any web browser.

Download on the App Store

GET IT ON Google Play



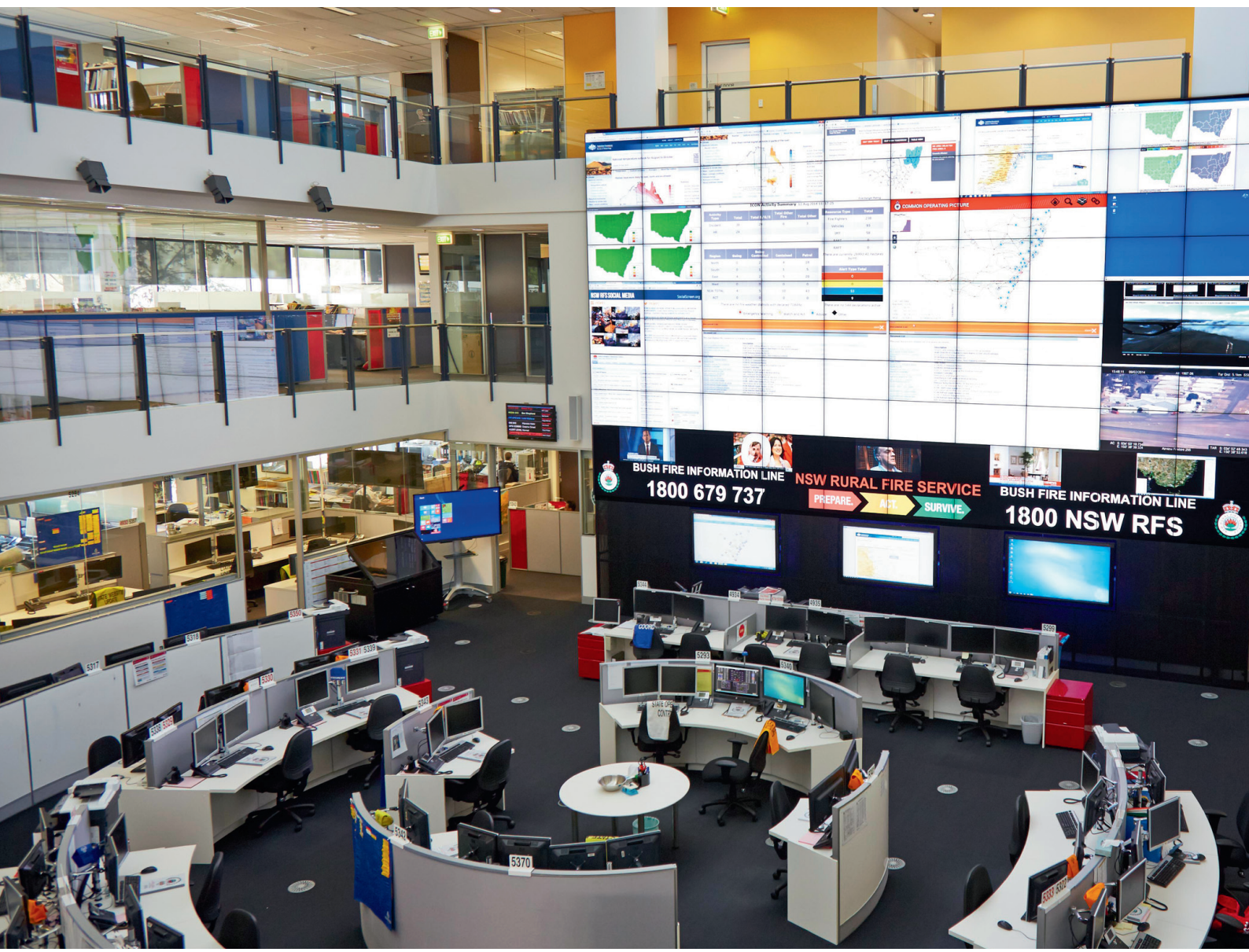
sales@northbridgesecure.com

www.netconnect.co

Powered By
NorthbridgeSecure

BEYOND THE COMMUNICATIONS GAP

David Braue



The NSW Rural Fire Service's operations room. Courtesy NSW RFS.

SOCIAL MEDIA, THE INTERNET OF THINGS AND BIG DATA GAIN TRACTION WITHIN CITIZEN-MINDED EMERGENCY SERVICES AGENCIES.

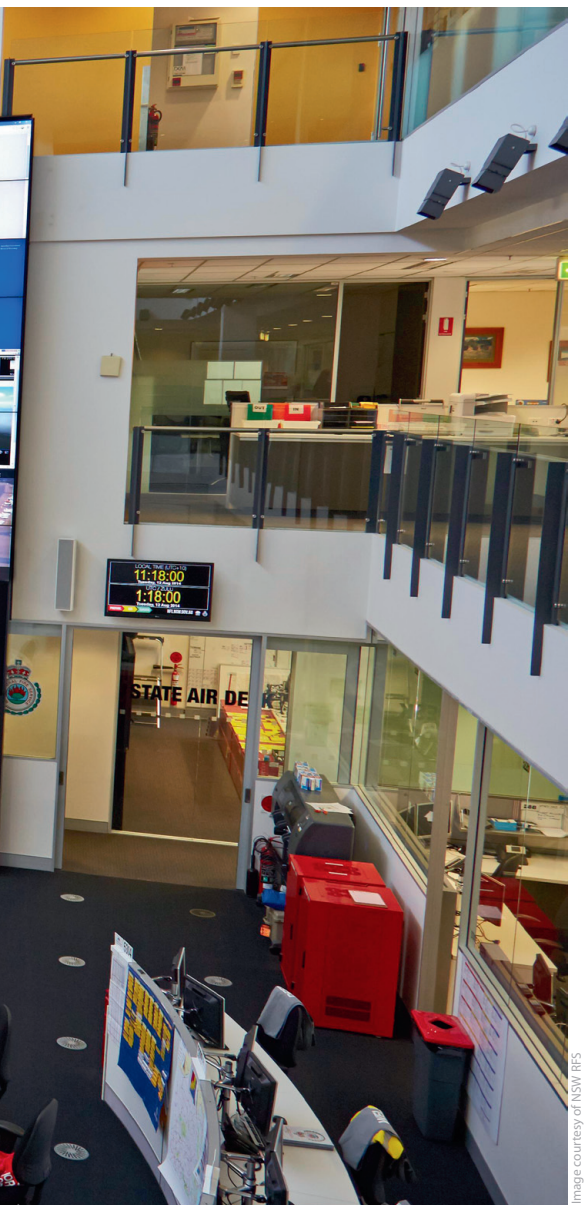


Image courtesy of NSW RFS

In a country where natural disasters are frequent and distance makes communication an ongoing challenge, new technologies have been a mixed bag for emergency services agencies (ESAs) struggling to modernise legacy technology and processes. With core mobility projects now well established, emerging devices and communications channels are driving a quiet revolution in ESA service delivery that promises to finally deliver information-led emergency services.

Potentially improved outcomes are taking shape thanks to a recent flood of miniaturisation, which has fuelled demand for new technologies such as unmanned drones, body-worn video (BWV) cameras, videoconferencing and all manner of wireless environmental and situational sensors. These devices increasingly coordinate their activities through far-reaching Internet of Things (IoT) networks — connected initially by 3G and 4G mobile networks, and eventually using extremely low-powered, long-distance networks based on emerging technologies like LPWAN, Sigfox and Flexnet.

IoT technologies, paired with a flood of new information through social media channels and a host of analytics tools to make sense of it all, are set to help ESAs get on the front foot in a battle for information dominance that will help them police more effectively, fight fires more safely and save more lives than ever before.

A NEW WORLD OF BENEFITS

ESAs that are struggling to cost-justify the necessary investment in time and training for such tools should think of their benefits in terms other than just better communication, said NEC Australia Solutions Director Andy Hurt.

"You start to look at what's necessary for those kinds of algorithms that get used to analyse very complex environments, and there aren't just outcomes in being able to make law enforcement agencies work more efficiently," he explained. "It actually adds a new dimension, which we've found to be a major indicator: employee safety outcomes."

Video-equipped unmanned drones, for example, can be flown into a fire zone ahead of firefighters to pick out risks, drop emergency supplies, identify trapped individuals or even to hover and provide wireless internet access to support ESA staff on the ground. Onboard sensors can provide invaluable information about temperature, wind speed, humidity, the presence of dangerous chemicals and other factors that can affect the safety of rescue efforts.

There is also great hope from new applications for biometrics — an area where NEC has been particularly active in recent wins with agencies such as CrimTrac and the South Australia Police. Biometrics can improve safety by enabling automated identification such as allowing police to automatically process inmates with less physical intervention — NEC's Watch House project with the NT Police won this year's Infrastructure and Platforms Innovation of the Year iAward.

"Our facial recognition technology platform is now rapidly identifying people brought into custody and making a significant contribution to how we conduct investigations and combat crime," said NT Police sergeant Chris Brand upon accepting the award, who estimates the system has already eliminated 1800 hours of police administration work. "Importantly, it's also improving overall safety and freeing officers to spend more time in-field."

Biometric techniques are also being applied for in-field assistance, such as scanning a situation for noises from wounded people or evaluating a suspect's emotional state through physical movements or speech patterns. "It goes beyond use cases of just recognising an individual," Hurt said.

>>

"It can be recognising patterns of behaviour that allow ESAs to anticipate and pre-empt certain activities. We're finding the conversation with governments is becoming a lot more broad and the use cases are becoming much different."

COMMUNICATIONS

Responsiveness goes both ways. One straightforward but critical use case for ESAs emerged in the wake of the Black Saturday bushfires, where inquiries slammed the lack of an early warning system that could automatically broadcast updates and potentially life-saving information to all mobiles in an area.

Subsequent years have seen several standalone efforts merged into the Early Warning Network (EWN), a centralised alerting service whose Situation Room product "fills the gap between public alerting and national alerting systems," director for government, enterprise and emergency management, Michael Hallowes — a former career police officer and Victorian Emergency Services Commissioner who previously served as national director of the national Emergency Alert Program — told *GTR*.

Situation Room allows the creation of asset and event layers that are used to track areas of interest and to direct relevant alerts to people who are currently located in those areas. Its goal is to deliver what Hallowes calls 'decision superiority' — "getting decision-makers the intelligence that they need, on the device of their choice, over the network of their choice".

The innovation around the platform — which is designed to ensure messages can be transmitted to relevant people via their existing mobile phones without requiring them to monitor Facebook and a range of different mobile apps — has attracted interest from governments in Japan, the UAE, Canada, UK, Belgium and elsewhere, Hallowes said.

"People need factual information very quickly, that is relevant to their situation," he continued. "The community is as important as the operational response. If we can inform people that they need to get out before it happens, and we don't need to send in emergency services workers to get them out, we can focus on fighting fires and not on rescuing people."

SOCIAL MEDIA SOLUTIONS

Social media is another key frontier for ESAs, offering real-time insight into situational changes that is often impossible for responders to get in other ways. Social media services are both rich enough and widely used enough that any significant event with public implications — whether it be traffic accident, bushfire, chemical spill, injured person or persons, flooding, livestock on the road, or any of a hundred other emergencies — will create a textual, photographic and even video footprint that can be fed into ESAs' decision-making streams if properly curated.

There's the rub, warns Caroline Milligan, associate director of emergency management with emergency-response consultancy Crest Advisory. "Rapid adoption of social media became a pain point for agencies in public safety environments because they could only manage it and couldn't control it," Milligan explained.

"Communities are no longer happy to be waiting for your information; they are sensors and potential eyewitnesses, and using social technologies they can push out real-time intelligence. We saw early on that this was going to be vital potential intelligence — and there are so many ways that you can use these sensors that people meeting communities face to face should be doing due diligence to do their work ahead of time."

That work includes finding out who are local influencers and what information they are gathering and sharing, and building lists of their social media presence so their information feeds are quickly available when they are needed.

Doing early groundwork to improve collection of social media information also paves the way for faster conversion of raw situational information into response-relevant data, thanks to large-scale analysis techniques that rely on social media monitoring and big data analysis.

"You can't process the sort of data that is coming in in volumes, unless you're using analytics capabilities," EWN's Hallowes said. "Embracing these in the spirit of collaboration in the industry is key to accelerating success. But you can't roll these out without a communications and education plan."

That plan must, Milligan is quick to point out, be a two-way street — >>

Hallowes calls it 'decision superiority' – "getting decision-makers the intelligence that they need, on the device of their choice, over the network of their choice".


DO MORE
FOR YOUR BUSINESS WITH I.T. SECURITY SOFTWARE FROM ESET
Whether you're a start-up or a global operation, ESET's IT security products are fast, easy to use, and deliver market-leading digital threat detection. We deliver the protection that allows you to DO MORE with your business. Find out more at WWW.ESET.COM/AU
eset
ENJOY SAFER TECHNOLOGY™

engaging social media leaders as part of the ongoing emergency response. This is often easier said than done, she said, noting that "it is staggering to me how many agencies are simply using open-source tools and technologies like social media to push information out and don't have the infrastructure to bring this intelligence to decision-makers. But in an emergency, knowledge is power."

PAINTING THE BIGGER PICTURE

Areas of focus for any ESA include implementing effective listening strategies, considering what monitoring and geosensing technologies they are using, and refining reporting frameworks to get cohesive developments in both traditional intelligence and open-source information. Such skills may not be in ready supply within many ESAs but successfully harnessing contemporary technologies will require building or acquiring those skills.

These requirements continue to evolve based on the evolving social media landscape, and to be effective in the long term ESAs will need to continue reaching out to citizens using the channels that are most meaningful for them. This is a new imperative that will test the flexibility of agencies that have to date been largely focused on enabling their own responders with new technologies, such as in-car police terminals and rugged in-ambulance laptops.

Such projects may deliver immediate benefits for field staff but they're just the beginning of the information-led emergency services revolution, said Steven Crutchfield, managing director of Motorola Solutions Australia.

"While [a mobility rollout] is strong with the productivity and efficiency angle, it is really laying that foundational building block of what can be done with a device in the hands of a public safety authority when connected to the broadband world," Crutchfield said, noting that the ability to predict future activities increases as the volume of collected information increases.

"By stepping back and taking a look at this as users in the field, we're moving towards that prediction and prevention effort that is really the Nirvana for a lot of our PSAs, Crutchfield said, noting the value of this information in fuelling a faster prototype-deployment-evaluation cycle that will put new technologies into the hands of field staff faster than ever.

"We're seeing early wins where just looking at legacy information contained within ESAs' systems can help them predict even 30% of the next day's events," he added. To demonstrate the improvements that are possible, Motorola is running a hackathon with Australian PSAs later this year to see what kind of challenges can be solved through new applications of available technologies.

NEC's Hurt sees the current excitement around innovation as feeding a larger agenda around smart cities, which will unite sensor and information infrastructures with broader citizen-centric initiatives that will improve the relevance and responsiveness of public safety authorities.

"We're seeing some tremendous initiatives in some of these agencies," he said, "with very intelligent people being given latitude to explore new use cases. We can start to put together proofs of concept and bring things to life with a proper use case. This is where it's going to start to get exciting."

DataTraveler 2000

Alphanumeric Keypad Secure USB Drive

Ideal When Security is Key.
DataTraveler 2000 is accompanied with an alphanumeric keypad for direct encryption on the drive. Lock and unlock using a word or number combination without other systems or software, leave no trace of your PIN with others.

Read up to 135MB/s
Write up to 40MB/s

Encrypted Protection

- Encryption done on the drive, leave no trace on other system
- 256-bit AES hardware-based encryption in XTS mode
- Locks down and reformats after ten consecutive failed attempts
- Auto-lock feature upon drive removal

Fast Speeds

- Newest USB3.1 Gen1 interface
- Speeds up to 135/40MB/s read and write

Guaranteed Durability

- IP57 certified water and dust resistant ability
- Durable aluminum sleeve cover

Maximum Compatibility

- Windows
- Chrome OS
- Linux
- MacOS
- Android

kingston.com

Next Generation Mobile Intelligence: What does mobility really mean for public safety agencies?

Steve Crutchfield, Managing Director, Australia and New Zealand, Motorola Solutions

Public safety agencies globally are investing in technologies to enable them to access essential information in a more mobile way — a concept often referred to as mobility.

Public safety agencies globally are investing in technologies to enable them to access essential information in a more mobile way — a concept often referred to as mobility.

Being able to access critical information while on the move is an important way of helping public safety agencies manage their daily workflows, while helping increase productivity and safety.

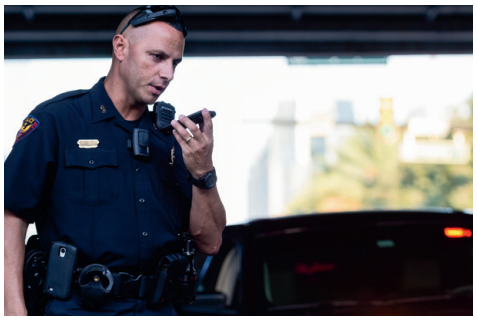
As technologies shift to broadband-based solutions, public safety agencies are looking for more effective ways to share intelligence between first responders working either in the field or in vehicles with their colleagues in the command centre.

In response to this need, Motorola Solutions has developed its vision for smart public safety, Next Generation Mobile Intelligence (NGMI), which is designed to help public safety agencies reach their goals of greater safety and operational efficiency. This can be achieved by placing the right information into the hands of first responders using a choice of devices, the best available networks and purpose-built, public safety grade applications.

We have identified the combination of four key principles which help define how public safety agencies can achieve their goals of better performance through smart technology, and these principles are central to NGMI. They are mobility, connections, intelligence and partnerships. Let's look at the first principle of mobility in more detail.

In the context of public safety, mobility solutions enable agencies to integrate a choice of devices and applications to deliver information in a format that suits technology users in accordance with their roles.

Rugged LEX L10 LTE Handheld



A choice of devices

A vital element of mobility is having the ability to perform a role using a choice of devices. The challenge for public safety agencies is to ensure their teams' ability to communicate and coordinate responses is not compromised by the use of a mixed fleet of devices, networks and applications.

The range of devices available will naturally be more limited due to greater requirements for durability, security, reliability and accessibility to specific systems.

Nevertheless, working in public safety, as with any other work environment, involves completing a range of tasks which could mean using a selection of communications devices. This may include a combination of mission-critical devices, such as the rugged LEX L10 handheld, or consumer-grade devices like a smart phone or tablet. Some responders may need waterproof devices for their role. Others need rugged devices for harsher environments or a larger screen to manage data input tasks.

Having the right device is essential. This frees responders from work they might otherwise need to do back at the station by placing the right device at their fingertips, bringing convenience and efficiency in managing their daily workflows.

Right information to the right person

Once the choice of device/s is determined, the right information must then be delivered to the right person in a format that is easy for them to consume. This enables improved collaboration, enhanced decision-making, more efficient use of resources and better outcomes for both agencies and the community.

So what does mobility look like in a practical sense?

Imagine a siege situation where an offender has taken a small group of people hostage in a public building, such as a library. With the right mobility principles in place, officers can collaborate on the best approach to the incident. Utilising a public safety grade mapping and whiteboard application can enable all responders to access a single, common operating picture of what is transpiring at all times.

Meanwhile, operators at the command and control centre can scan footage relayed back via the officer's body-worn camera. The control centre can also monitor social media feeds for vital information.

The outcome is the ability to filter and analyse multiple information sources to identify 'actionable intelligence', meaning information that can be acted upon.

Summary

Mobility is a key principle in placing information into the hand of first responders.

With access to superior intelligence delivered to the right people in the right format and on the right device, responders can make better decisions and deliver better outcomes, helping to keep the community safe.

MOTOROLA SOLUTIONS

Visit www.motorolasolutions.com.au

PROJECT SUCCESS

STUNTED BY OUTSOURCING, THE UK'S REVENUE AND CUSTOMS SERVICE USED CULTURAL TRANSFORMATION TO REINVENT ITS APPLICATION INFRASTRUCTURE.

The size and complexity of government organisations has led to mixed results for digital transformation efforts, but the experiences of teams in one UK government project have shown that sometimes the greatest successes come from starting small and empowering staff to keep control of their projects.

Following the lead of the transformation-minded UK Government Digital Service (GDS), UK revenue authority Her Majesty's Revenue and Customs (HMRC) embarked on a major transformation several years ago as it worked to build a scalable new applications architecture that would support its business into the future.

Over the course of three years, the project would expand from what Alun Coppack, partner with HMRC implementation partner Equal Experts called "humble beginnings — just a few people in a room" to span 50 software delivery teams across multiple locations across the UK.

Those teams, which each manage a few of the 250 componentised 'microservices' that make up HMRC's new application infrastructure, collectively number more than 8000 people who manage systems handling nearly 2 billion transactional page views annually.

Getting to that point, however, took time and effort — largely because

the historical legacy of government outsourcing had destroyed any hope of creating flexible, innovation-minded teams.

"With outsourcing, the government completely removed any innovation and introduced the inability to make change," Equal Experts partner Duncan Crawford told attendees at this year's Agile Australia conference.

"There was this really restricted environment where there was no product ownership, step change was not possible and we wouldn't have been able to deliver early and show value."

Trying to brute-force this culture was a road to nowhere, so the change-minded team decided to start small — identifying "something small that has high impact", as Crawford put it, "and creating a small team filled with subject matter experts... Isolate that small team, create a clear deliverable, and ask the team to work within core principles" that emphasise agile, iterative functioning over monolithic habits.

Government was not completely without its inspiration, however: to their surprise, the team found strong and valuable guidance in the GDS's Digital Service Standard — a set of 18 guidelines for transformational government service delivery (subsequently appropriated by Australia's Digital Transformation Office) that Coppack said aligned better with the principles of agile development than he ever would have expected.

"If you'd heard that the government had defined 18 rules for good software delivery you might be a bit sceptical," said Coppack.

"But it advises things like 'understand users' needs', 'build a service that can be iterative', 'create a service that's simple and intuitive enough that users succeed the first time through', and 'test the service from beginning to end with the person that commissioned it'," he added.

"By the time I got to the end I thought that if I worked for an organisation that embodied these principles, this would be a great thing."

The iterative development of HMRC's new digital platform progressively expanded as teams, empowered to think differently for the first time in a long time, began mapping out ideas about service delivery and building the microservices to deliver them. Those microservices interact online, working together to create the living, breathing whole that is continuously revisited, expanded and improved.

The key to maintaining flexibility with a growing team is to ensure that the architecture retains its unitary design, with microservices given simple names that describe the one — and only one — behaviour of the microservice performs.

"By the time I got to the end I thought that if I worked for an organisation that embodied these principles, this would be a great thing." – Alun Coppack, Equal Experts

"Naming is really important in software services," Coppack explained. "If you can't give that one name to a service, it's not a microservice. If you're making it do two, three or four behaviours, you end up with multiple teams working on that thing.

"But we did one set of services, and as we grew the services and features it was easy to apply another team to own those things," he said. "The concept mapped beautifully for the relationship, and ownership, and growth of the organisation."

The success of the HMRC's massive technological and cultural shift reflects the potential benefits that can be had when transformation is embraced fully and given leave to grow progressively within even the most regressive environment.

Small, early wins speak volumes for the success of the project and that success quickly begets more success, which in turn provides even more impetus for cultural change.

Getting that change in motion can be harder than even the staunchest advocates of transformation realise early on — and despite years of progress, there is still much work to be done before organisations are ready to enjoy the benefits of transformation.

A recent Unisys survey of 175 IT and business executives highlighted the challenges organisations still face around digital transformation. While 72% of the surveyed senior executives said they see a digital business model as critical for success, just 24% of respondents believe they are making any progress in developing scalable IT for their digital business.

Worse still, only 15% believe their organisations are actually nimble enough to operate as a full digital business.

As the Equal Experts and HMRC teams found, pushing reality closer to expectations is a long and complex process. And in the end, Coppack said, success comes from designing an effective team structure and maintaining it throughout the transformation.

"Teams that are able to work in the way that suits them best, and with the least amount of dependencies, are in our experience the ones that are highest performing," he explained.

"Transferring ownership for the product to some external governance body just doesn't work; the teams themselves, and the people working in the teams, are the ones best placed to manage these things.

"By promoting and championing autonomy within your organisation and designing for loose coupling, you can enable teams to take ownership of their products. The greatest indicator of our success is that we now have other government departments using our platform to deliver their services."

DELIVERING E-LEARNING TRAINING TO NSW'S LOCAL COUNCILS

A PARTNERSHIP BETWEEN LGP AND ARCBLUE IS DELIVERING TAILORED PROCUREMENT AND CONTRACT MANAGEMENT SOLUTIONS TO LOCAL GOVERNMENT.

Mark Osborne, Acting Operations Manager, Local Government Procurement, lgp.org.au

Five years ago, the local government sector in New South Wales would have baulked at the thought of using web-based technology to deliver training and education programs to their councils. Now, it is not a wish, but a demand that local government training and support is provided through a wider range of channels. Councils expect Local Government Procurement (LGP) to be able to deliver flexible training services, from traditional face-to-face and e-learning through to fully integrated, blended programs.

As a prescribed entity for local government, LGP is uniquely placed to provide services to councils across the state. LGP supports all local councils, regional groups and joint organisations — from Bourke in the north-west to Wentworth on the Murray River. Our offerings of aggregated procurement, consulting services for procurement, networking and training have been well received by councils over the last 10 years, but it is critical that we continue to adapt to changing needs.

While councils have responded well to our face-to-face training over the years, the sheer numbers of staff involved in procurement and contract management — and the distances between towns — mean that councils and regional groups are increasingly requiring e-learning services to complement traditional training methods.

To that end, LGP has developed partnerships with key organisations that share our vision and passion for the sector. One of our key partners is ArcBlue Consulting, an expert procurement and contract management consultancy and training firm that works with many sectors, enhancing procurement and contract management practice and performance. Partnering with ArcBlue was a natural fit to provide an expanded range of services and solutions to councils.

The new training needs analysis, e-learning and face-to-face training content that has been specifically tailored for local governments, taking into consideration their evolving learning objectives and the unique challenges faced by NSW councils. The package has been designed to make the participant and administrator experience as streamlined and user-friendly as possible.

The solution is configurable, scalable and delivers appropriate training to all levels of council staff as individuals, groups, whole-of-council or even regional programs. The modules have been designed to cover the needs of council procurement and contract management roles and general purchasers, and span a range of introductory and advanced topics. LGP and ArcBlue have used reliable open source technology to deliver the ProcureLearn platform, eliminating expensive third-party software fees and ensuring the solution is cost effective.

Designing and implementing this comprehensive tailored solution has not been without its challenges, but the collaborative approach between LGP and ArcBlue and the involvement of councils throughout has led to successful outcomes.

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™

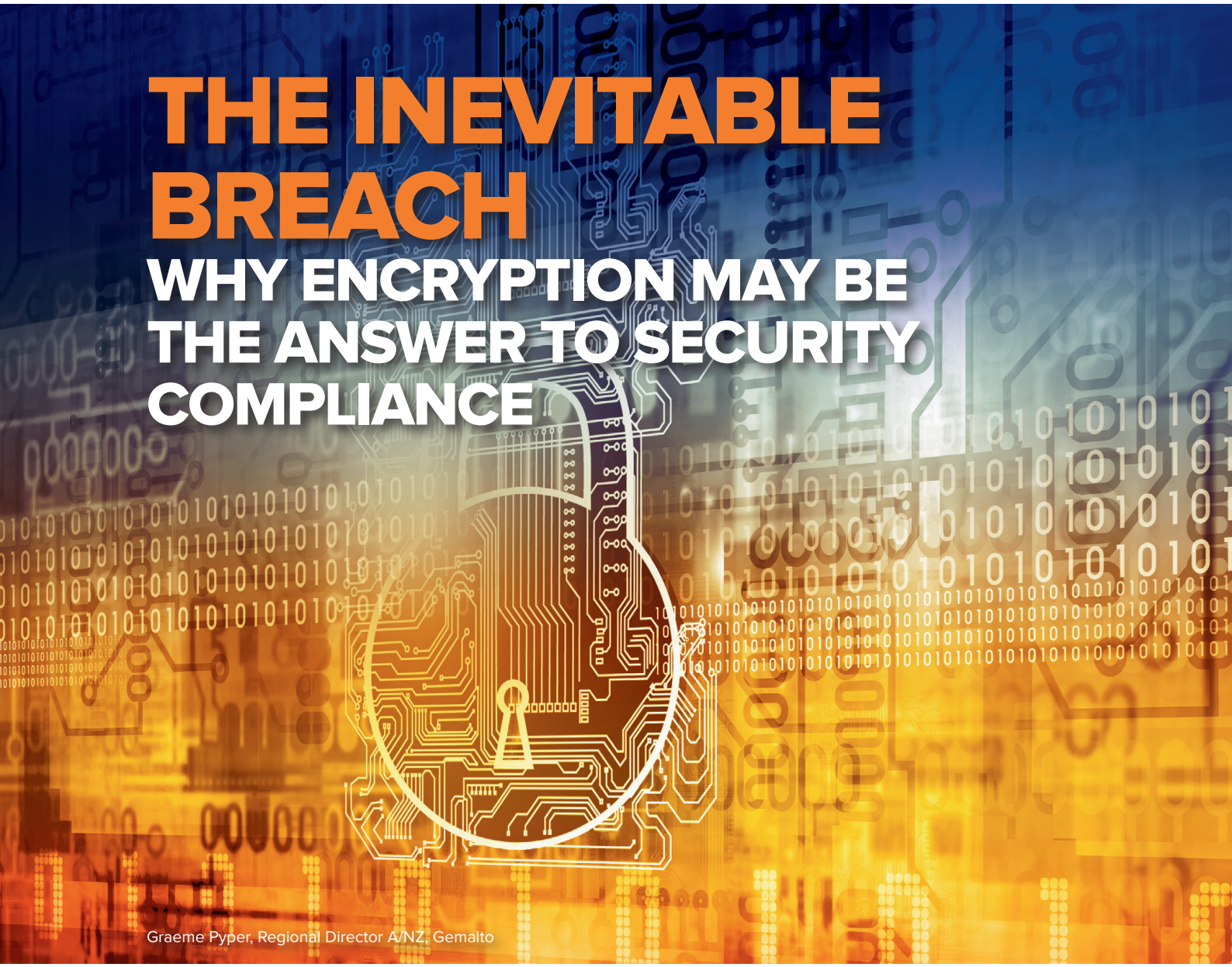
VEEAM

For more information, contact Veeam ANZ: T **1800 055 929** (AU) | T **0800 452 588** (NZ)

Veeam.Sales.ANZ@veeam.com | www.veeam.com

THE INEVITABLE BREACH

WHY ENCRYPTION MAY BE THE ANSWER TO SECURITY COMPLIANCE



Graeme Pyper, Regional Director A/NZ, Gemalto

TRADITIONAL DATA SECURITY METHODS DON'T WORK ANYMORE, SO IT'S TIME TO MOVE TOWARDS A 'SECURE BREACH' APPROACH.

The federal government's plan to implement mandatory data breach notifications speaks to the inherent value of personal information and the rights of individuals to be alerted when the control of that information has been taken from them — from home addresses and phone and banking numbers, to images and videos, shopping behaviours and even health card and passport numbers.

The recent momentum for the Bill, currently making its way through parliament, has been driven by relentless news of security breaches and loss of personal information.

If we've learned anything from recent events, it's that we have a growing data security crisis and Australia is a primary target. As we watch hackers hone in on data critical to our lives and our businesses, we need to develop a

mindset that accepts attackers will find a way in — but that our critical data is protected so it doesn't make its way out.

National regulations — in the form of mandatory breach notifications — support encryption strategy by holding accountable those that fail to protect the most sensitive information through robust encryption solutions.

Under the draft Bill, organisations will be required to alert people affected by a compromise of their personal data if there were a risk of serious harm posed by the release of the information. Companies currently report breaches to the Privacy Commissioner on a voluntary basis.

The Bill offers an opportunity for government to provide clear guidance, so long as the legislation applies to all and signals to both government agencies and commercial organisations that they cannot afford to take an isolated view of information security mapped to budget allocations.

All stakeholders must be confident they can trust the digital infrastructure and that their transactions and information are ultimately safe — even in the event of a successful cyber attack. This confidence requires a combination of government and business initiatives, with government setting the regulatory framework for everyone — including government agencies.

AVOID THE SPOTLIGHT

But why is regulation being introduced? What does it mean for decision-makers across all levels of government and suppliers to government? What do you need to know?

The new regulation will have major implications on the way in which data is collected, stored, accessed and secured. Most importantly, it will require an entirely new mindset when it comes to securing data, what is considered a serious breach and the steps an organisation must take in response to one. These steps cannot be actioned overnight and require careful planning by IT departments, security teams and those in charge of mitigating business risk across public and private sector organisations.

"Being a better steward of customer data is not just good public relations, it is good business sense, too."

The word data often appears insignificant but when you define data as personal information it's not difficult to understand why some details should be guarded more closely. Those with lax security will be put in the spotlight with the requirement to notify both authorities and affected individuals when a data breach occurs. And being breached is not a question of 'if' but 'when'.

Current legislation does not yet give clarity to what is considered sensitive information and what constitutes a 'notifiable data breach'. But you can bet if you hold identifiable information on individuals you will be held liable — and the penalties for a data breach could involve not only monetary loss and legal proceedings but also irreparable reputation damage.

The Bill offers an opportunity for decision-makers to act now in order to be compliant when legislation passes, to implement robust security measures and signal that government agencies and suppliers to government won't risk the loss of citizens' sensitive information by taking a relaxed approach to information security.

RESPONSIBILITY AND ENGAGEMENT

So where can you start? Let's face it — traditional data security methods don't work anymore, so it's time to move away from breach prevention and towards a 'secure breach' approach.

Here are four recommendations for IT and security professionals:

1. Out with the old, in with the new. Today's security strategies are dominated by a singular focus on breach prevention that includes firewalls, antivirus, threat detection and monitoring. But if history has taught us anything, it is that walls are eventually breached and made obsolete. The next and last layers of defence need to focus on both the data and the individuals that access the data, by surrounding them with end-to-end encryption, authentication and access controls that provide the additional measures necessary to protect citizen data.

2. Protect citizen data as if it were your own. If you want to help your department or agency earn and retain trust, you have to view the protection of sensitive customer data not just as a regulatory mandate but as a responsibility essential to your success. Being a better steward of customer data is not just good public relations, it is good business sense, too.

3. Transparency is the road to trust. Put security front and centre and tell stakeholders about the security measures your department or agency has put in place to protect its data. The industry is much more open about what they are doing to protect customer data following the most recent breaches. If you're doing something better than the rest of the industry, like encrypting data end to end, then you might be seen as a trusted innovator.

4. Security is a two-way street. Just as you tell customers what you are doing to protect them, tell them what they need to do in order to protect themselves. If a customer experiences identity theft or a data breach while doing business with your department or agency, your reputation suffers. A better-educated consumer is a safer consumer of your services.

IT and security teams need to adopt a data-centric view of digital threats and start with better identity and access control techniques such as multifactor authentication and the use of encryption and key management to secure sensitive data. That way, if the data is stolen it is useless to the thieves.

SECURITY SCORECARD

DIGITAL DEFENCES IN THE AGE OF DISRUPTION

Jonathan Nally

HOW GOOD ARE OUR GOVERNMENTS AT KEEPING CITIZENS' DATA SAFE AND SECURE? WE POLLED SEVEN INDUSTRY EXPERTS TO FIND OUT.

Every day we read about another major security hack somewhere in the world that results in identity theft, industrial espionage, national security consequences, immense personal embarrassment and so on. Australia is not immune to these system attacks, and they're not restricted to private companies — government systems are attacked all day, every day. Think of the Bureau of Meteorology attack, which reportedly originated in China. And the Census night debacle, blamed at least partly on a DDoS attack.

It's a problem that's only getting worse. So with all levels of government holding vast amounts of sensitive data on members of the public, as well as the activities of businesses and government themselves, it's more vital than ever that governments institute solid security practices and robust technical solutions to protect themselves, and us, from malevolent actors.

So how are our governments doing on this front, and what can they do better? To get a feel for the kinds of security challenges facing governments and how well they're dealing with them, we polled a group of security industry experts to obtain their views — a sort of government security scorecard, if you will. Those experts are: Michael Steer, District Manager for Federal and NSW State Government for NetApp Australia; Gerard Nunez, ICT Government Specialist at ESET Australia; Andy Solterbeck, Regional Director for Cylance; John Ellis, Chief Strategist, Cyber Security (APJ) for Akamai; Guy Eilon, Senior Director and General Manager ANZ, at Forcepoint; Michael Wilkinson, Director of Security and Intelligence for Asia Pacific at Nuix; and Simon Green, Vice President, ANZ, Palo Alto Networks. We're sure you'll

agree they have some interesting insights to share.

HOW IS THE AVAILABILITY OF CLOUD-BASED SECURITY TOOLS AND SERVICES ASSISTING GOVERNMENT BODIES?

SOLTERBECK: Australia has been extremely fast to adopt cloud-based applications, but the adoption of cloud-based security tools has been less expeditious. Cloud services are supposed to allow agencies to be more efficient and responsive in delivering services to the community, and at a significantly lower cost, and there has been a concerted push towards a 'cloud first' approach. But security has to be at the forefront to ensure adequate protection of data and minimisation of breaches occurring. We do recognise there is a group of customer-specific environments for which public cloud is an inappropriate approach; therefore, flexibility in deployment approaches is key.

STEER: Recent research into data management strategies amongst Australian government organisations showed that only 1 in 2 had a data management strategy in place, yet the primary issue they needed to address to ensure effective data management outcomes was to create a robust and compliant environment. Security is an extremely critical component, yet skills shortages, the fast pace of change in attacks and vulnerabilities, and the rise in state-sponsored activity mean that agencies may not necessarily have the resources immediately on hand to ensure a strong, secure environment. Also, unless there is a clear ability to scale and immediately patch or deploy new solutions, exposure remains anyway. Cloud tools help mitigate against these issues. Throw in a far greater awareness of attacks and vulnerabilities drawn from across a much wider range of customers and geographies, and cloud-based tools can be quicker to implement, more effective and easily shared across multiple agencies.

NUNEZ: The federal government could be seen to be taking a two-pronged and slightly cautious approach to cloud-based security tools and services. Reading the federal government's Cyber Security document of 2016, you sense that there is a willingness to embrace technology and look at cloud computing as a new and exciting frontier on one hand, but then there is a sense of caution and paranoia as well relating to cloud-based security tools. This is still highly evident with some government departments and organisations not entertaining the thought of any of their networks being hosted anywhere but on-site.

ELLIS: There is certainly an increasing awareness amongst agencies of the need to leverage cloud-based tools and services from a security standpoint. At present, the Australian Signals Directorate (ASD) has actually set in place a Certified Cloud Services List that makes it necessary for government agencies to only deploy cloud services that are InfoSec Registered Assessors Program (IRAP) assessed and accredited. What this means is that, in theory, no agency is allowed to purchase any cloud technology unless it is listed as a certified cloud service. As such, most agencies are still trying to plot a pathway to the various gateway providers to assess how they can best utilise these cloud services.

WILKINSON: While a handful of agencies are embracing cloud-based security, due to the level of bureaucracy or red tape, most government bodies take time to implement changes, especially major infrastructure changes such as moving internal operations to the cloud. However, cloud-based security services are a quick win for smaller departments that do not have full-time security staff.

John Ellis, Chief Strategist, Cyber Security (APJ), Akamai

"If we were to compare Australia to regional counterparts, we have certainly done a very good job at defining the policy settings."

HOW DOES INFORMATION SECURITY FIT IN WITH GOVERNMENTS' OVERALL RISK APPROACHES?

GREEN: Government agencies are constant targets, and they are taking a number of steps to protect themselves. A proactive and agile approach to cybersecurity is critical. By integrating network security controls, and sharing threat intelligence, agencies can improve threat prevention and reduce response time. Also, understanding internal cyber ranks and processes, demanding accountability, and testing and evaluating to ensure teams are working together to address cybersecurity are key ways to address concerns. Agencies must gain visibility into what applications are running on their networks, who is using them and why. Using a zero-trust approach even with slower-than-desired patch cycles in large government networks helps >>

Guy Eilon, Senior Director and General Manager ANZ, Forcepoint

"There is not a one-size-fits-all approach to cybersecurity, and each department needs to be assessed on a case-by-case basis."

prevent sophisticated attackers trying any opportunity to get in and move laterally.

NUNEZ: There has always been a focus on risk mitigation within government. Information security commands the highest priority for an organisation's risk strategy. Attempting to identify uncertainty of future events and outcomes is at the core of any federal government risk strategy, whether information security risk or other identified areas of risk. The government has a systematic approach to minimising this potential risk, and it appears to be open to new initiatives and solutions for the reduction of information security risk.

WILKINSON: A reasonable level of security awareness now exists throughout the majority of government departments. At the federal level, this is pushed by the ASD and its 'Strategies to Mitigate Targeted Cyber Intrusions'. However, it appears the motivation for improving security is still being pushed by IT staff and the CIO rather than being included as part of an overall risk management plan.

ELLIS: Historically, the ways in which systems are designed tend to focus on the 'need to know', but today information systems are very much structured around a 'need to share'. The dichotomy between the two approaches is where the challenge lies at the moment, as a lot of the security models traditionally used by the government will no longer be as effective today. Therefore, it is vital for government agencies to address the finer details — they need to look at new security models and architectural frameworks by which information can be shared in a secure fashion, so as to narrow the gap in the risk profiles and scale more efficiently.

SOLTERBECK: Unfortunately, based on any objective view of the threat landscape, the current information processes and tools are not capable of creating the right balance. We believe that there needs to be a fundamental rethink of the current compliance-based approach. The adversaries are moving faster than our current tactics are capable of responding. New more agile process and procurement methods are required.

IS IT BETTER FOR AGENCIES TO BUILD THEIR OWN IT SECURITY CAPABILITIES, OR CAN OUTSOURCED OPTIONS MEET GOVERNMENT REQUIREMENTS?

GREEN: Demand for managed security services is on the rise as many governments struggle with an increasingly complex threat landscape, a shortage of skilled staff and the need to rapidly adapt to changing business conditions, while still keeping security costs under control. Agencies that are struggling to build their own capabilities should consider outsourcing IT security to managed security providers. Outsourced partners can simplify management, provide the flexibility to tailor solutions, give agencies more granular control over the IT stack and reduce the total cost of ownership.

STEER: Many organisations struggle to either hire or internally develop the requisite skills levels to keep abreast of the continually evolving environment. As compliance and regulatory environments also change, the security environment becomes even more complex to manage. Add in the issue of security threats now operating in an automated manner and many organisations cannot keep pace on their own with advances in attacks. We're certainly not advocating a total handover of security to a third party as ultimately accountability for adherence and compliance remains

Simon Green, Vice President, ANZ, Palo Alto Networks

"Many governments struggle with an increasingly complex threat landscape, a shortage of skilled staff and the need to rapidly adapt."

the government's responsibility. However, outsourced managed security solutions in conjunction with a robust internal security program can combine to create a flexible, compliant, partnership-driven approach that can be highly effective.

EILON: There is not a one-size-fits-all approach to cybersecurity, and each department needs to be assessed on a case-by-case basis. What we do know is that today's threat landscape sees increased use of kill chains and attacks that utilise multiple vectors in a blended attack. For those who outsource, this means the importance is no longer just about having 'security in-depth' by having multiple vendors, but instead having a single vendor who can provide intelligent and contextual security to stop threats across the entire kill chain. The benefit of outsourcing is the ability to quickly scale security programs.

Michael Steer, District Manager, Federal and NSW State Government, NetApp Australia

"We're not advocating a total handover of security to a third party as ultimately accountability for adherence and compliance remains government's responsibility."

However, it's critical for government partners that need to understand compliance obligations as they impact the delivery of services.

HOW WELL ARE INFORMATION SECURITY CONCERNS BEING ADDRESSED WITHIN THE OVERALL INFORMATION STRATEGIES OF GOVERNMENT DEPARTMENTS AND AGENCIES?

WILKINSON: This is a very broad question. Larger departments and agencies tend to be aware of the need for security and to have dedicated security staff, or at least have IT staff with a reasonable level of security competency. Having said that we are seeing compromises of government organisations; for example, the Bureau of Meteorology in December 2015 and Western Australian Parliament in February 2016. The fact departments are being compromised clearly indicates that their security is inadequate.

SOLTERBECK: The prioritisation of strong cybersecurity practices and understanding of the threat environment is probably not equal across all government departments. We have spoken with a number of federal government departments, and there has been a lack of consistency and comprehension of the strategies needed to better respond to threats, as well as the necessity of building a strong security culture — and not just within their security teams.

NUNEZ: The Australian Government takes information security very seriously. Developed through the Attorney General's Department is the Protective Security Policy. The policy is comprehensive and is designed to assist agency heads and senior executives to identify their responsibilities in relation to major security risks to their people, information and assets; provide assurance to the government and the public that official resources and information provided

Andy Solterbeck, Regional Director, Cylance

"Australia has been fast to adopt cloud-based applications, but the adoption of cloud-based security tools has been less expeditious."

to their entities are safeguarded; and to incorporate protective security in their culture. There are 36 mandatory requirements as part of the framework of the policy. The ASD's information security manual has been developed to complement the Protective Security Policy framework.

ELLIS: Earlier this year, the Australian government established some really strong policy settings through the introduction of the national Cyber Security Strategy. However, every agency has a different degree of maturity, so there will always be challenges with how strategies are implemented due to resources, budgets and conflicting priorities, amongst other factors. So the biggest question is not the 'what', but the 'how'. At a policy level, the federal government has certainly set up the right framework, and if we >>

were to compare Australia to regional counterparts, we have certainly done a very good job at defining the policy settings for the government and industry.

HOW DOES THE MATURITY OF THESE PROCESSES COMPARE BETWEEN FEDERAL, STATE AND LOCAL JURISDICTIONS?

NUNEZ: The federal government's approach could be seen as a more comprehensive strategy. As the goal posts continue to shift, the federal government is looking to be up to date and continually vigilant. Yet, as seen recently with the issues arising from the Census, it is evident that members of the public have very valid concerns about the security of their own personal information.

SOLTERBECK: The disparity between the jurisdictions is very evident, especially with local and state governments where they typically lack the specialised security resources and skills to be able to protect their assets and constituents as rigorously. Local governments are prime attack targets as they have a wealth of private citizen data, which can be used for identity-related crimes — and they are typically viewed as an easier target due to less stringent preventive mechanisms and breach identifiers.

Gerard Nunez, ICT Government Specialist, ESET

"As seen recently with the issues arising from the Census, it is evident that members of the public have very valid concerns about the security."

HOW MUCH GUIDANCE ARE BODIES SUCH AS THE AUSTRALIAN SIGNALS DIRECTORATE AND DIGITAL TRANSFORMATION OFFICE PROVIDING?

STEER: There has been a tremendous amount of support provided by bodies such as the ASD to help organisations continue to build and strengthen their security capabilities. The ASD has been integral in creating references; providing deep and relevant advice, awareness, education and evaluation; as well as working alongside agencies to help create stronger defensive and aggressive cybersecurity capabilities. There's been a marked increase in support and engagement, as well as increased focus on sharing more relevant security information amongst all agencies as the security threat environment evolves.

ELLIS: ASD is world class when it comes to offering technical guidance to government and civilian agencies. This is evident by the numerous publications that ASD provides, specifically the *Information Security Manual* and the *Strategies to Mitigate Cyber Intrusions*. The problem isn't with the ASD, which, along with the Prime Minister and Cabinet and the Australian Cyber Security Centre (which PMC and ASD are part of), has done a great job in defining the 'what' in what needs to be done. The issue is with the 'how', and this is centred on a shortage of skills, funding and prioritisation of investment.

EILON: In 2010, ASD developed a list of 35 strategies to assist Australian government entities achieve the desired level of control over their systems and mitigate the risk of cyber intrusions. ASD has advised that if fully implemented, the top four mitigation strategies would prevent at least 85% of the targeted cyber intrusions to an agency's ICT systems.

However, while the ASD provides useful guidance on potential controls and strategies to prevent the malicious entities from entering the network, there are some pretty significant risks that these controls fail to address. Primarily, and unfortunately, third-party agencies agree that the types of risks that cause the greatest cost to agencies today come from inside the network, and not from outside. Therefore, strategies need to be developed to prevent data breaches not just from intrusions but from internal extractions too.

Michael Wilkinson, Director of Security and Intelligence, Asia Pacific, Nuix

"Cloud-based security services are a quick win for smaller departments that do not have full-time security staff."

NEVER PAY

up for your data.

Ask us how to
recover
from **seconds**
before an
attack.

Zerto

www.zerto.com

EARLY ADOPTERS

David Braue

EARLY GOVERNMENT CLOUD ADOPTERS ARE FINDING THAT THE PROCESS OF DIGITAL TRANSFORMATION IS FOSTERING INNOVATION AND CULTURAL CHANGE.

Public-sector cloud adopters are chalking up early wins but anecdotal reports from Australia's government-cloud front line suggest there is truth in warnings that many change-minded CEOs are still rushing into cloud with the right intentions but the wrong expectations.

Despite considerable momentum behind digital transformation within government, the mismatch between expectations and enthusiasm remains a common issue, Gartner Research Director Michael Warrilow recently opined. "Some are making dangerous assumptions that [cloud] will always save them money, which it's not necessarily going to do. What they will get is more agility and a different mix of capex and opex, which the business likes. I am having this conversation every week with companies in Australia and New Zealand," he wrote.

ServiceNow ANZ solution consulting director Michael de Landre is having similar conversations. "One of the things we're continually seeing is that we've got to start each time with a conversation on clarity around what the issues really are," he said during a panel session at the AC Events Connected Government Summit in Melbourne earlier this year.

"There is some mythology and lack of clarity around what the rules and guidelines are. We've often been able to get through some of the concerns people might have by getting through to the way things really are."

Many organisations are finding expectations being shaped more gradually as they ramp up their cloud efforts and increasingly engage both business and technology leaders. Such has been the case at Victoria's Department of Health & Human Services, where Alex Thomas, principal report developer within the application development area, said innovation during the agency's cloud journey has come not from top-down mandates but by empowering staff to think differently about infrastructure and how cloud can improve it.

"Just because a cloud service is out of the question now, doesn't mean I shouldn't store my data in a way that allows me to have that choice later on." — Alex Thomas, DHHS

"We are finding that innovation happens at the periphery," said Thomas. "The disciplines of experimentation and participatory design are very key elements, and we basically then ingest and promote the things that we're working on."

Engaging employees in the transformation effort not only draws out the talent and combined intellect of the organisation, but is helping to drive cultural reinvention at some government bodies. This has proven to be a big boon for Consumer Affairs Victoria where, general manager of corporate services Chris Balfour said, collaboration is "something that is very firmly ingrained in our business case".

"What we do is maximising public value," he explained, "and there are a lot of things we touched upon in the organisation. It helps build your cost-benefits model, and it's a very positive way to integrate that into the business and to have people working with that. People feel they're getting better value from their jobs and that there is more purposefulness in what they're doing."

The use of Agile methodologies has helped drive greater buy-in from employees that have driven "a genuine redesign of the processes", Balfour continued.

"We've been trying to get there through the Agile methodology," he said. "Project teams are building the user stories together. We've got different heads in the room suggesting different approaches and thinking through it. It has really been quite inventive."

This type of collaboration has often been harder to foster in organisations that haven't progressed towards digitisation efforts, but Keith Don, director of strategy and consulting at HSD, believes being digital and cloud based often makes all the difference.

"Having digital as part of the conversation allows you to answer a lot of customer expectations," he explained, "as well as looking at ways our existing systems can do that. This allows there to be a platform where both digital and IT teams can start to talk to each other, and to work out a solution that both can agree on to move forward."

Organisations struggling to find their transformation momentum often get the ball rolling with "little projects that make sense to both sides and allow you to break the ice", Don added. "You realise that these new guys on the block are pretty much like >>

us, and doing the same thing we've been doing all along."

Social media has proven to be a catalyst for reinvention at the NSW Government's OneGov centralised-services organisation. There, technology head Rahul Dutta believes that as well as focusing on "the little things that are simple", a key driver for change has been to find ways to engage staff with social media and other digital channels.

"The idea," he said, "is to advance the digital experience into a day-to-day platform that we use as something different or special, that you have to make a jump to."

BUILDING THE BUSINESS CASE

Steady progress towards cloud adoption has driven a perceptible shift in the way that vendors and government bodies are engaging when discussing new cloud-based initiatives.

"There's no doubt that we've seen a shift in language and conversation while talking with government organisations," said ServiceNow's De Landre. "We used to talk about which bits we should move into the cloud in terms of infrastructure and assets. But the conversations we often have today are about which business processes are causing pain, which are inefficient across multiple different departments and multiple different processes."

Evolving results-focused approaches to cloud transformation have driven a reduction in large, infrastructure-based projects and a surge in short projects, he added. "We used to talk about projects that might be 12 to 18 months before we realised benefits, but it's very common for us to be talking with customers and seeing true benefits realised within 12 weeks.

"By taking a SaaS approach, you are able to skip that whole conversation about which platform I'm putting it on and how I am acquiring it."

Even in organisations where there is internal enthusiasm for cloud and digital business, the transition is "genuinely not easy", warned Balfour, who said Consumer Affairs "has taken twice as long getting to the starting blocks" as it expected.

One frequent obstacle has been the forming of business cases in a way that they appeal to executives with differing agendas, while other projects have struggled not because the need for change was questioned but because there were so many ideas about how to accomplish it.

"It's a matter of finding some common approaches and common solutions that start to work," he explained, "then putting in a chunk at a time. That chunk approach has worked for us and we can focus on which chunks need the most help — and trying to make the most effective change."

Backlogs can be tricky to manage, Balfour said, particularly as Agile projects take off and the number of chunks increases. "It can make everyone nervous," he said, "trying to work through that and having executives say we'll only deliver 80% of what they want — and that delivering the other 20% is a matter of trying to work through priorities.

"Once they have comfort that the 80% will deliver the benefits you're promising, you can actually start to tangibly show them the benefits. That's pretty helpful."

For his part, Thomas warned against over-optimistic estimations of the cost savings to be achieved from the shift to the cloud. "You do suddenly hit release of consideration around hardware, but you still have to have quite a lot around administration," he said.

"In most of the cloud economic models we've done, we've found that we already run quite lean and that there is not that much savings in some of the administration spaces. But we are just getting ahead and doing it."

Some discussions about business cases had been stymied by governance concerns about the location of hosted data, with many cloud services out of the question because they stored data offshore. But policies change, said Thomas, adding that the inflection point provided by the cloud transition is also a good time to make sure data can be moved as appropriate down the track.

"It's about how do I build things that give me the opportunity to do things later on," he explained. "Just because a cloud service is out of the question now, doesn't mean I shouldn't store my data in a way that allows me to have that choice later on. As long as what you do right now gives you the option later on, that's what becomes really important and really powerful."

HARNESS THE POWER OF BROADBAND TO WORK SAFER, SMARTER AND FASTER

Within the LEX L10's rugged hardware lies a secure, dedicated software platform and user interface that supports capabilities above and beyond consumer-grade smartphones.

- **Extra loud**, dual 1-watt speakers for best-in-class audio quality.
- **Ergonomic design** for one-handed operation, non-slip grip, textured PTT button & 4.7-inch touch screen.
- **IP67 rating** to withstand dust, rain and water immersion of 1 metre for 30 minutes.
- **Gorilla Glass 3** resistant to scratches, drops and pressure.
- **Highly secure** FIPS 140-2 hardware encryption and security enhanced Android OS.

When equipped with specialised applications, the LEX L10 becomes a powerful tool enabling faster decision-making, improved efficiency and easy collaboration and information sharing.

LEX L10

RUGGED LTE HANDHELD

NOW AVAILABLE FOR ORDER

To learn more, visit **motorolasolutions.com.au**

DELIVERING NEXT GENERATION MOBILE INTELLIGENCE

MOTOROLA SOLUTIONS

Kingston DataTraveler 2000 encrypted drive

The Kingston DataTraveler 2000 encrypted drive is designed to be secure. It features an alphanumeric keypad that locks the drive with a word or number combination, for easy-to-use PIN protection. Its auto-lock feature is activated when the drive is removed from a device and it deletes the encryption key after 10 failed intrusion attempts.

The product has hardware-based, full-disk AES 256-bit data encryption in XTS mode. Encryption is performed on the drive, not on the host computer, and no trace of the PIN is left on the system.

The product is OS independent and can be used on any device with a USB 2.0 or USB 3.1 Gen 1 (USB 3.0) port. It is compatible with Windows, Mac OS, Linux, Chrome OS, Android, thin clients and embedded systems. In addition, the drive requires no software or drivers. It is FIPS 197 certified, to meet a frequently requested corporate IT requirement. Its durable design protects the drive from everyday elements such as water and dust.

Kingston Technology Far East

www.kingston.com

Black Box wireless presentation system

The Black Box AVX-HDMI-WI-HD features a high-definition wireless presentation system, enabling users to give a wireless presentation from their PC, Mac, smartphone or tablet.

It has both HDMI and VGA connectors and can be used with a wide variety of projectors and displays. Depending on the application, it can be connected to a wired Ethernet LAN. Users can also connect to the wireless 802.11b/g/n network.

The system functions as both a wireless receiver and an 802.11b/g/n access point. It enables as many as 32 laptop users to log in and display their computer screen video and audio from up to 300 feet away in full 1080p HD resolution. The system's application software captures the images and sends them through 2.4 GHz radio waves to the receiver for output.

Other features include changing presenters with one click; fast and easy file sharing via Word, PowerPoint or other files; a plug-and-show set-up; conference control functionality; WEP/WPA/WPA2-PSK network and content security; four-to-one split-screen for multiple users; web-based control interface; remote desktop function; and two USB ports.

Black Box Network Services Australia

www.blackbox.com/en-au

CLOSING IN ON HACKERS

David Braue

© stock.adobe.com/au/Lasha Kilasonia

INCREASINGLY POWERFUL ANALYTICS ENGINES ARE HELPING LAW ENFORCEMENT AGENCIES FIND CYBERCRIMINALS HIDING ON THE 'DARK WEB'.

Bill Searcy still remembers the days when catching an online criminal was pretty straightforward — follow the audit log to get the IP address, then trace that back through the culprit's IP address to get their identity. Dispatch a police officer, and prosecute the offender for wire fraud or other related activities.

"That was back in the days when things were simple," recalled Searcy, who recently left a career in US law enforcement — including a role as former assistant director of the US Federal Bureau of Investigation (FBI) — to continue the fight in the private sector. "You'd have one break-in, one agent and no problem. It didn't take a lot of analytics or a lot of detail."

These days, the situation is very different — cybercriminals lurk on the periphery of the internet, hatching plans and exchanging tools on the dark web, known as a harbour for seedy criminals of the cyber and the more conventional type.

Searcy knows it well — he was part of the team that brought down Silk Road founder Ross Ulbricht in 2013 after an extensive investigation that, Searcy said, was characterised by its massive complexity and the huge volume of information the investigators were collecting and analysing.

That information — more than 1 terabyte per day of traffic logs as well activities and details of suspects and clients of the Silk Road marketplace that Searcy calls "the Amazon.com of drugs" — created a massive investigational

burden that highlighted the crucial importance of big data organisation and analytics engines to help pick out patterns of behaviour and previously unseen relationships.

"The goal was not only to identify the individual who was hosting Silk Road, although he was the big fish," explained Searcy, who is still helping catch criminals in his new role as vice president for Global Justice, Law Enforcement, and Border Security Solutions at Unisys. "We wanted all the other little fishes as well and sent out a lot of requests for collecting data to other agencies."

"If you are collecting terabytes of data every day," he added, "you're not going to task an individual with going through each piece of information individually; that's not happening. What you have to have is outstanding analytics with the capability to do link analysis, data reduction and all of those things."

"It's very difficult to stay completely dark and to go completely off the grid. You're always giving yourselves away somewhere; it's just a matter of us finding it." — Bill Searcy, Unisys

GREATER AWARENESS

Long accustomed to developing specialised systems to manage information collected during law-enforcement investigations, makers of specialised software — for example, Unisys's U-LEAF (Law Enforcement Application Framework) tool as well as Wynyard Group's Advanced Crime Analytics and Advanced Cyber Threat Analytics — are finding a new raison d'être by melding their proven organisational capabilities with the information-crunching capabilities of big data tools.

Those tools have helped reduce what Searcy calls the "time to awareness" — the gap between when an investigator finds something out and when it becomes broadly known to investigators.

"Just as DNA and fingerprints are important in the physical world, analytics are equally important when you're working in the cyber world," he said. "An agent might know about a particular item but until that information is brought back to our data system and placed in that system in such a way that it can be indexed, searched properly and categorised, then the FBI doesn't know about it."

The greater use of analytics is one of numerous capabilities formally adopted within guidelines for the protection of government information — encapsulated in Appendix III of the so-called OMB Circular No. A-130 — which in July were updated by the US government for the first time since 2000.

Finalised after a public consultation process that included thousands of inputs over more than a year, the new A-130 Circular — which offers important guidance around enterprise security that is as applicable in Australia as it is to the US government bodies for which it was intended — highlight the importance of real-time knowledge of the environment, proactive risk management and shared responsibility for the security and privacy of information.

The new guidelines are built around "the shift away from checklist exercises and toward the ongoing monitoring, assessment, and evaluation of Federal information resources", the circular's authors note.

Searcy agrees, noting that this type of proactive role has become the de facto expectation from government agencies both in protecting their information and in actively investigating data breaches.

BETTER TOOLS

Many government organisations well appreciate the need for better security but are let down again and again by poor internal controls — such as giving outside parties privileged access to their internal systems — and poor monitoring and visibility of breaches.

Here, too, analytics is proving useful by helping individual agencies keep on top of the ongoing tsunami of security-related information they must deal with every day. "People can be their own enemies," Searcy said, referencing the massive 2013 hack of US retailer Target. "Some things you just can't protect against — but there are some things you can do to protect yourself that, quite frankly, if you don't do them, they're unforgivable. And people will lose jobs."

Ever-improving capabilities, and some highly effective hacking tools — as discovered in the recent release of hacking tools stolen from the US National Security Agency (NSA) — reflect a law-enforcement fraternity that has come a long way from the early days when cybercriminals were often caught red-handed through simple IP matching.

Despite the early success of cybercriminals who leveraged the dark web to avoid detection by law enforcement, growing awareness of their tactics is helping investigators more readily accumulate massive troves of data that are, when properly massaged, often turning up nuggets of information that offer key evidence in increasingly complex, global online investigations.

"To solve these cases, every one of them always relies on good analytics," said Searcy. "It's very difficult to stay completely dark and to go completely off the grid. You're always giving yourselves away somewhere; it's just a matter of us finding it. And that's where the analytics comes in."

ZETTA 1:
Infusing New Life into Content Governance with PublishPoint

As Microsoft gears up to release its new range of products, great opportunities stand wide open for technology companies. However, the challenge to fully realize the potential of Microsoft's products can test the resources and efficiency of even the most experienced Microsoft solution providers. This is where ZETTA 1, a Microsoft Gold Partner and having numerous years of experience in the collaboration and content field on the SharePoint platform, shines. Using its extensive knowledge and understanding of the products, the company has helped customers to create powerful content strategies. The company's product PublishPoint bridges the gaps in content governance by providing visibility of the whole publishing lifecycle via a user friendly dashboard.

"With functionalities such as scheduling items, items for review and site analytics, PublishPoint gives clients peace of mind, knowing that their content is governed well," emphasizes Stuart Fergus, Managing Director. With PublishPoint, customers gain the ability to distribute content authoring amongst teams, giving them a dashboard view of what they are working on and where it is at in the process of publishing. PublishPoint's 'Work in Progress' view quickly identifies the work that is currently being done via the dashboard. It allows Check-in items, Check-out items, Pending Approvals, Rejected items and Publishing History to be easily edited directly from the dashboard. These features not only help improve the content, but also ensure that certain pages or pieces of information don't remain live when they should have been removed. Stuart explains, "Any large organization or company can identify with the pain of having large amounts of information that constantly needs monitoring, regulating, updating, approving, removing and ultimately 'governed'." By enabling clients to use content management tools in new ways, the ZETTA 1 team has unlocked capabilities of the SharePoint platform, in order to ensure quality content governance.

ZETTA 1 has a large focus on the education sector and has provided numerous solutions to clients in the domain. The company has piloted projects such as "Websites for Schools" for over 1100 schools using SharePoint and is currently developing a solution for the schools' intranets using Office 365 as the platform. The plan is to develop the intranets as a schools' administration tool, and then provide both teachers and student dashboards. Stuart explains, "Using O365 we believe that we can utilize the power of the AZURE architecture to introduce machine learning into the students' dashboard to surface learning objects and resources to the student, based on their needs. It is truly an exciting time to be a Microsoft partner in the education sector."

Going forward, ZETTA 1 will continue to develop PublishPoint and is actively developing the product for the O365 platform, which will be ready by mid-2017. ZETTA 1 is also developing a provisioning tool for O365 called "SiteBuilder" to enable the rollout of Intranets for Schools. "SiteBuilder" is the beginning of the vision of having dashboards for teachers and students by applying the power of machine learning. The company is confident to provide new functionality and support to customers with its products. Stuart concludes, "We hope other government agencies and corporate organizations using SharePoint will value the visibility, peace of mind and confidence that PublishPoint brings — therefore understanding and valuing the role content governance brings to protecting their business."

ZETTA1
www.zetta1.com

ZETTA 1 Make it happen!
PublishPoint®

Enabling Wireless Everywhere

WirelessTech commits to provide latest and innovative wireless products, networking technologies and tailored services in pursuit of supporting Australian System Integrators.

- Licensed and Unlicensed Wireless Point-to-Point
- Licensed and Unlicensed Wireless Point-to-Multipoint
- Wireless Mesh Technology
- Wireless Hotspot and Outdoor Wi-Fi
- Multi-WAN Load Balance Routers with VPN Bandwidth Bonding
- Multi-Cellular Mobile Routers
- IP Cameras, NVR, Video Encoders & Decoders
- Enterprise Switches, IP SAN & NAS Storage
- Antennas, POEs, Lightning Surge Protectors
- Customised Network and RF Cable Assemblies
- Touch Monitors

Public Safety

Service Provider

Industrial/Mining

Transportation

WirelessTech

sales@wirelesstech.com.au
www.wirelesstech.com.au
+61 2 8741 5080

THE IoT'S ROLE IN HEALTH AND AGED CARE

Fadi Geha, CEO, Simble

MOBILITY DEVICES, THE IoT AND APP DEVELOPMENT ARE HELPING PROVIDERS IMPROVE HEALTHCARE OUTCOMES WHILE ALSO BOOSTING THEIR OWN BALANCE SHEETS.

What do 30 to 60% declines in the share prices of Australia's publicly listed aged-care providers indicate about changes sweeping through the sector? They show that these companies have not kept pace with the changes and reforms that are rapidly disrupting the industry.

While those reforms are designed to ensure Australia has the best possible system for its ageing population, pressure is mounting on providers to differentiate themselves. Providers must ensure that they not only retain their current clients but also attract new clients while reducing costs to protect their operating budgets and profit margins. Mobility has a significant role to play in this transformation.

Over the last 10 years there has been a steady uptake of mobile device usage through the introduction of smartphones,

tablets and wearables. Along with this has come a high level of maturity in the applications that reside on these devices, plus there has been the advent of the Internet of Things (IoT). The IoT has long been talked about, but it is now at a very mature level, enabling providers to implement both 'active monitoring' and 'passive monitoring' solutions, ensuring greater transparency around their carers and increasing service levels for clients.

ACTIVE MONITORING WITH CARER APPS

While there is a myriad of software companies that provide client management systems, these systems do not generally translate well onto mobile devices as they try to replicate the whole system. A smarter approach is to engage a software solutions provider that specialises in mobility and uses a platform with a robust and intelligent middleware layer to perform rapid development of multiple mobile applications that handle only what is required.

One such app would be used by the carer. In most cases the carer only needs to know their scheduled client visits for the day, what tasks they need to perform for the client and also the shortest route between clients.

From a provider viewpoint, the ability to not only push this information out in real time, but also have the information that is entered by the carer sent back in real time, gives assurance that the carer has performed their tasks at the time they were scheduled. Carers are then only remunerated for their time on-site as well as travel time for the shortest routes.

Estimates put savings at around $3000 per carer per year. More importantly, through the use of smart middleware that can provide alerts and alarms, the client experiences a better quality of service while the carer can also be monitored with KPIs.

PASSIVE MONITORING

While RFID tags have been around for more than 20 years and are very effective for performing tasks such as asset tracking, other applications of the technology have emerged. These include beacons and smart hubs that use reading technologies such as Bluetooth, BLE and ZigBee, which have been used to enable smart home technology.

In the aged-care and home-care sectors, this technology has evolved to enable providers to install a small smart hub in the client's home and monitor — in an unobtrusive manner — details such as continuous heart rate, location, activity levels, temperature, appliance utilisation, medication dispensed, as well as timing of entries and exits via door sensors.

This information is then transmitted in real time back to a middleware layer which, using either manually configured actions or artificial intelligence, can then send alerts or alarms to the provider, carer or loved one.

Through the use of artificial intelligence, historical data, dwell, power and motion sensors, the activity of a client can be monitored. If they sit down in their favourite chair and turn on the television at 2 pm every afternoon to watch their favourite show and this consistently happens for a defined period of time, an alert can be triggered from the middleware to notify the appropriate people to ensure that the client is alright in the event that the normal activity does not occur.

Another example of this is in dementia management of clients, either in the home or in assisted care. Through the use of machine-washable RFID tags attached to the client's clothing and beacon technology, virtual gating or geofencing can be implemented to ensure that the client does not wander outside a specific geographic perimeter — and that if they do, carers or staff are alerted immediately.

The key to passive monitoring is that it needs to be unobtrusive within the home or village so that while the client receives the best care possible from the provider, he or she does not feel that 'Big Brother' is watching. When looking to implement this technology, a solution should be sought that can be installed with minimum fuss and can also be uninstalled and re-used with no damage to the home. Estimates show that by implementing passive monitoring, the provider can save around $5000 to $10,000 per client per year, depending on the level of care required.

WHAT TO LOOK FOR IN AN IOT PROVIDER

When exploring IoT technology it is important to ensure that a solution provider has a solid track record in designing and developing mobile solutions that interface to a secure middleware platform that provides not just data retention, but analytics, machine learning (AI) and easy-to-use dashboards for viewing clients' data in real time.

Estimates show that by implementing passive monitoring, the provider can save around $5000 to $10,000 per client per year.

In addition to this, it is important to ensure that the provider has either pre-built connectors to your client management system, your CRM and your accounting package, or has the necessary skills in-house to custom develop a connector that meets your specific need(s).

Finally, a technology provider should be able to rapidly build role-specific mobile applications that can be changed as required to ensure that they are cost effective, and which make your internal change management requirements, including uptake, as easy as possible.

www.simble.io

CONFIGURING THE CLOUD

Luke Mackinnon, CTO, Vocus Communications

UNDERSTANDING THE ESSENTIAL CHARACTERISTICS OF CLOUD-BASED SOLUTIONS AND SECURITY REQUIREMENTS IS CRITICAL FOR MAKING INFORMED DECISIONS.

Global data is expected to grow by nearly 50 times within the next decade, and organisations are under immense pressure to futureproof themselves against big data with innovative network configurations and storage solutions, particularly as the Internet of Things (IoT) exposes even more information to users anywhere they are.

In a time where government agencies are mandated to increase productivity and reduce overheads, cloud-based infrastructure potentially delivers the most reliable, scalable and secure solution to respond to the big data challenge.

The cloud represents one of the most significant shifts that computing has gone through. As we discover a new cloud-based world, traditional IT

terms such as servers, data centres, operating systems, middleware and clustering will cease to be important on the client side.

And, while the importance of network configuration is vital for any enterprise, government agencies have a vested interest in safeguarding large volumes of sensitive data with efficient cloud solutions. If the foundation of the network is strong, the cloud solution will function at an optimum level; if not, the network will be compromised and cloud strategies will potentially fail.

Agencies should consider the following questions to ensure they have the right configuration before heading to the cloud.

WHAT'S THE NEED?

Identify the purpose for migrating to the cloud — it may be derived from an increased level of sensitive data that requires strict protection or does the existing network need to be upgraded to process large volumes of data during a major event such as the Census?

Next, think about which cloud-based structure suits your need: public, private or hybrid.

- Public cloud is open to be managed and utilised by any user. Virtualisation is the foundation of the flexibility that public cloud offers; it delivers true efficiency in scale and cost.
- A private cloud service is solely utilised by an individual organisation and is protected by additional cybersecurity measures such as firewalls and dedicated infrastructure that is not shared with other cloud customers. With private cloud solutions, the organisation can more effectively grant access to the data contained with the network and manage who has access.
- A hybrid cloud solution utilises a combination of both private and public solutions where the more sensitive applications can be contained in the private cloud, and other forms of non-sensitive data can be open to the public.

WHAT LEVEL OF SECURITY IS REQUIRED?

Security is an important, possibly the most important, consideration for government agencies looking toward a cloud solution. When considering a move to cloud computing, agencies must clearly assess potential security risks at the provider, network and physical access levels.

"Some argue the responsibility for data protection falls with the provider, but we argue the responsibility rests with the customer, the carrier and the cloud provider."

Some argue the responsibility for data protection falls with the provider, but we argue the responsibility rests with the customer, the carrier and the cloud provider. When one fails, all fail.

By protecting data assets and information within the network, agencies can build the barriers against cyber attacks or sensitive information being leaked.

As technology becomes more advanced and more available, the more vulnerable systems become. This means additional security procedures are required to be put in place to protect the integrity of the agency. While the risks will never be removed by moving to the cloud, agencies doing their homework will minimise the potential issues and be better off in the long term.

Cloud solutions with the most effective security infrastructure will recognise issues as they arise and provide safeguards, ideally automated to quickly address those issues.

HOW FLEXIBLE SHOULD THE NETWORK BE?

Moving to the cloud doesn't remove the need to have strong, efficient and secure data networks. Agencies need to be able to quickly and securely connect to their cloud infrastructure, ideally through dedicated network links which don't traverse public internet.

Network scalability is an important consideration. The great benefit of cloud infrastructure is the ability to scale up rapidly as demand dictates.

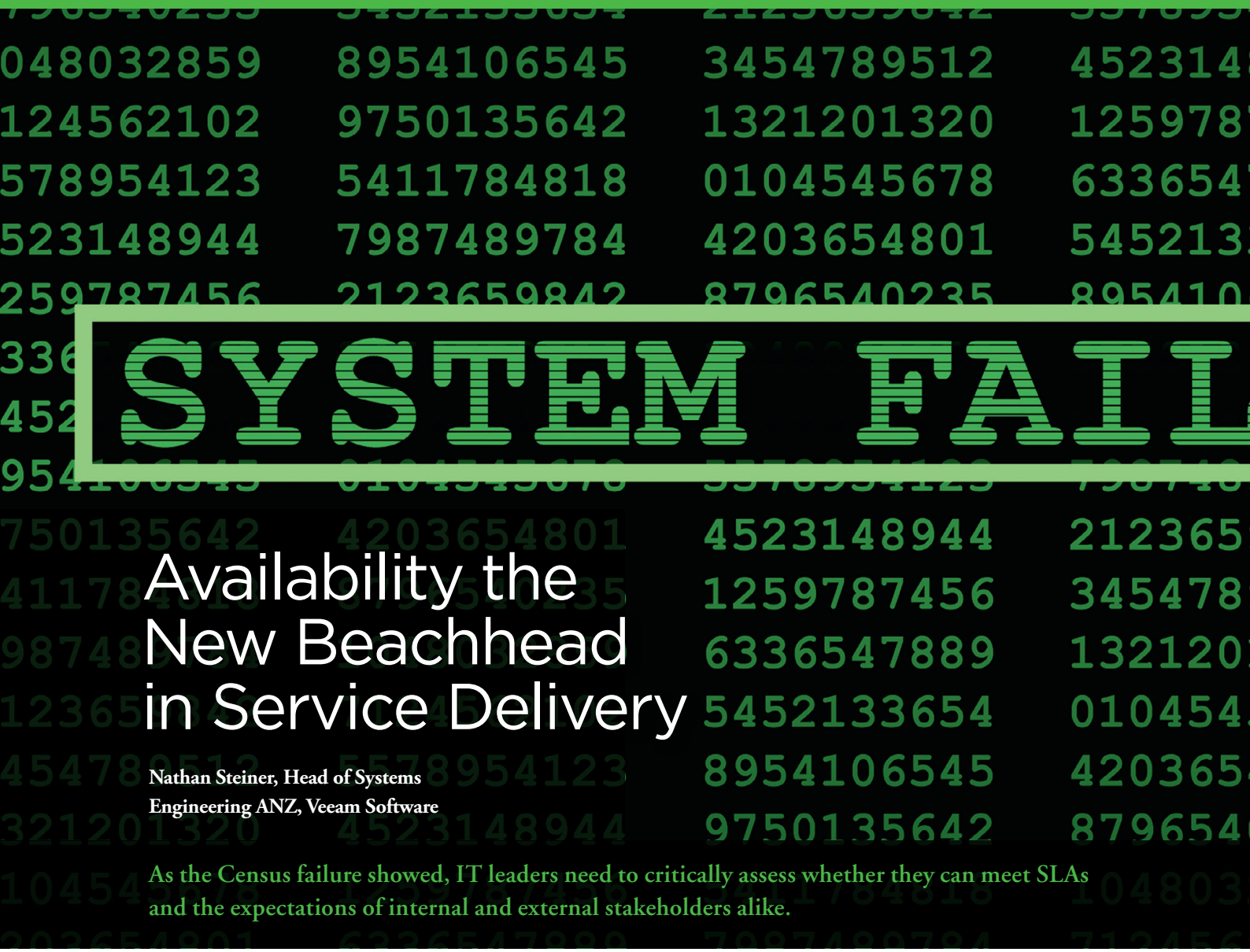
If a network cannot withstand the level of data travelling through, this can lead to network congestion and could result in damaging downtime.

Scalability enables flexibility for environmental fluctuations, which can assist in accommodating for those times of high traffic and low traffic, whether it is legitimate traffic or attack traffic. Ensuring the scalability of the network is a necessity when deciding a cloud strategy.

CONCLUSION

Cloud computing is changing the way IT departments buy IT. Today, with the right partner, cloud is fast becoming more accessible, easier to adopt and more useful 'out of the box'. Government agencies have a range of paths to the cloud, including infrastructure, platforms and applications that are available from a range of cloud providers.

However, understanding the essential characteristics of cloud-based solutions and security requirements is critical for making informed decisions on the appropriate platform to meet their data needs.



Availability the New Beachhead in Service Delivery

Nathan Steiner, Head of Systems Engineering ANZ, Veeam Software

As the Census failure showed, IT leaders need to critically assess whether they can meet SLAs and the expectations of internal and external stakeholders alike.

The 2016 Census may prove to have been a watershed moment in how Australian government departments come to view the availability of public-facing digital services. Within a short period of time on that night in August, those trying to complete the census online were frustrated by error messages. It took only moments for social media to come alive with the hashtag #censusfail as participants vented their frustrations publicly and in real-time.

The failure pose many questions for the Australian Bureau of Statistics as well as its partners tasked with maintaining availability of the census website.

While lots of analysis and finger-pointing has already taken place in the aftermath of the chaos, the situation has also thrust into the spotlight the issue of robust service availability planning and recovery in case of a downtime event.

Trust underpins all online transactions. Technologies such as SSL help maintain confidence that data won't be stolen while accessing applications via a browser or mobile app, and there's an expectation that when a user enters a .gov.au URL into a browser that services will be available securely and promptly. Members of the public trust that when they visit a website or other government-run digital service, it will be available and will 'just work'.

When a system goes down or becomes otherwise unavailable — be it a critical internal system or public-facing infrastructure — there's a risk of a negative reputational impact. In a business context, this can translate into lost sales as customers turn to competitors. In the case of not-for-profit organisations or government departments, the impact of downtime is similarly reputational

© Stock.Adobe.com/au/Mila Gligorić

and economic. Research conducted by IDC suggests that the median cost for an organisation experiencing application downtime exceeds US$100,000 per hour. However, for some large, complex organisations that rely solely on providing services online, the cost can be substantially higher. And that's not taking into account the reputational damage — or in the case of government departments, the cost of official enquiries and implementation of recommendations if required.

When — not if — a downtime event takes place, it's critical that businesses, not-for-profit organisations and government departments are able to restore services quickly and maintain data integrity. As more and more services move into the digital space, application availability is becoming the raison d'être for modern IT departments, within both the public and private sectors.

IDC has conducted interviews with senior IT leaders in more than 1,200 organisations deploying Veeam's availability solutions across the globe. According to the research, IT departments are choosing to prioritise technology investments that help ensure systems avoid downtime and maximise availability.

Availability can make or break IT careers

Cost is a factor when evaluating availability solutions, but it is less important than ensuring delivery of services and minimising disruption to operations. Senior IT leaders may have some flexibility in their budgets to deliver against organisational objectives, but absolutely must meet availability targets in order to be successful.

Indeed, it's not uncommon for modern IT departments to be measured on recovery point and time objectives (RTPO), giving them less than four hours to restore services in case of downtime. These service level agreements (SLAs) will become more critical in coming years, such is the importance organisations place on application availability.

As IT systems become more complex and more organisations continue to move towards virtualised environments, it's critical that IT systems are designed from the ground up to align virtual infrastructure with data protection and recovery solutions to meet RTPO requirements and ensure that potential downtime is minimised. It's no secret that virtualisation, while not yet at saturation point, is all but ubiquitous. According to IDC's research, nearly 70% of x86 systems ran in a virtualised environment in 2014 (with that figure expected to slowly climb to exceed 71% by 2018). A commonly held belief is that organisations adopt x86 virtualisation primarily for cost reduction, but IDC's data shows that speed of recovery was at the top of the list of benefits of shifting to a virtualised environment.

The IDC study analysed data collected directly from Veeam's customer base and looked into the relationship between VMware ESXi hypervisor deployments and Veeam's suite of availability solutions. It found that the main drivers of adoption of virtualisation were to simplify operations, help meet availability SLAs and the opportunity to align and integrate infrastructure with data protection capabilities.

Perhaps more importantly, the survey pointed to reduced recovery time when relying on Veeam's availability solutions in conjunction with VMware's hypervisor. In fact, recovery time was more than halved compared to environments that just rely on VMware for data protection and recovery, helping exceed organisational RTO (recovery time objective) requirements.

Benefits of Veeam's availability solutions are even more pronounced when it comes to RPO (recovery point objective) measurement, with businesses being able to point to a ten-fold improvement when using Veeam instead of relying on VMware alone. This symbiotic relationship between software suites helps exceed SLAs across the board and ensures that trust can be maintained between application users and the organisation making services available.

As organisations ratchet up the pressure on IT departments to ensure application availability — both for critical systems and public-facing infrastructure — IT leaders need to critically assess whether they can meet SLAs and expectations of internal and external stakeholders alike. Simplifying IT infrastructure and focusing on availability needs to be a key priority for any modern organisation. After all, your reputation might just depend on it.

VEEAM
IT JUST WORKS!™

Veeam Pty Ltd
www.veeam.com

ON THE OPEN MARKET

NEW SOUTH WALES' GovDC MARKETPLACE IS SETTING AN EXAMPLE FOR SIMILAR EFFORTS IN OTHER STATES.

David Braue

The creation of a service-based marketplace to support the New South Wales Government's GovDC strategy reflects the maturation of its customer-centric vision and sets an example for similar efforts in other states. That's the view of one technology executive in the wake of a significant contract that will enable state agencies to commission cloud services faster and more easily than ever before.

Approved vendors are already marketing services through the GovDC Marketplace, a self-described 'ICT supermarket' that was launched in July on the back of a key supply contract awarded to ServiceNow and UXC Keystone by the NSW Department of Finance, Services, and Innovation (DFSI).

The portal both standardises and streamlines the sourcing of approved services by state agencies as they progressively embrace cloud services — a key structural transformation that is driving similar state efforts at transformation that has already delivered considerable benefits for proactive early adopters.

A user-centric design — also reflected in Service NSW's recent adoption of Google's Android Pay digital-payments system — was critical to bringing the marketplace vision to fruition with a broad enough range of services to support myriad NSW state agencies, ServiceNow ANZ Managing Director David Oakley told *GTR*.

"The whole system of user engagement and experience has

been quite key to getting adoption going," he explained.

"The nature of the project is as a brokering environment, but the emphasis on the project has been around a design experience. It's allowing different agencies to come together in a marketplace, and through government and partner support we have made the system of engagement and user experience very compelling."

That compelling experience would drive the evolution of the GovDC initiative into a "digital community where we have on-premises environments connected to clouds globally for the government," said Derek Paterson, director of the NSW GovDC and Marketplace Services within DFSI.

Agencies, he said, "will be able to utilise services from anywhere, any time. The Marketplace project gives government the opportunity to buy on-premises and off-premises cloud services that encourage better efficiencies and better use of government spending."

Current GovDC Marketplace providers include ac3, Fujitsu, IBM, Unisys, Deloitte, UXC Red Rock and others.

The creation of a marketplace-driven environment was not originally in DFSI's plan, executive director of government technology platforms Pedro Harris recently told *GTR*, but increasing demand highlighted the opportunity and drove architectural changes that would allow private providers to co-exist within the GovDC environment.

"Traditionally we would do all our development internally," Harris said, "and this signalled a big push toward platform development. We're creating this ecosystem of different marketplaces that allows our users to find the best workloads. Rather than having 160 agencies doing it themselves, we do this and give them the ability to consume.

"We've started partnering with agencies so they can do what they're best at doing — supporting citizens with services — and we can do what we're best at, which is abstracting the complexity and giving them a platform to operate from."

The NSW model has set the pace for government-scale delivery of cloud services, said Oakley, who has been involved in a number of agency-wide deployments and called the state-wide GovDC effort "probably the most innovative group [in government transformation], certainly at a state level. They are doing some really great things."

Such "great things" will be key to helping government bodies realise the potential of digital transformation — as well as meeting a NSW Government edict that they be live within GovDC by August 2017. If the results of a recent Gartner survey are any indication, there's still a way to go — 59% of respondents believe their IT organisation is not ready for the digital business of the next two years.

"The Marketplace project gives government the opportunity to buy on-premises and off-premises cloud services that encourage better efficiencies and better use of government spending."
– Derek Paterson, DFSI

Cloud technologies were nominated as the area that would have the most significant impact on respondents' careers, reflecting the growing importance of initiatives like GovDC to transformation-minded governments.

As well as realising a focus on user experience and user-centric design, the Marketplace portal — which took three months to implement and went "extremely smoothly", Oakley said — is also designed to help agencies monitor and audit their usage of GovDC services, and track their costs as they accumulate.

"The ability to have tenancy in the GovDC Platform, and to stand up preproduction environments within a couple of hours of receiving a purchase order, is critical in getting that time to value and getting the project off on the right footing," he explained.

"The government have had clarity of thought in terms of what they're trying to achieve and gave very clear direction to the project team about the outcomes they wanted."

e-Invoicing the key for Government agencies looking to do business with SMEs

Procurement and invoicing are some of the most highly formalised and standardised workflows, with almost universal applicability across public and private sector organisations. They are also one of the areas where organisations are increasingly facing demands for greater efficiency, transparency and performance.

Completely digitising the handling and flow of formal messages that occur during purchase and invoicing has many significant financial benefits. Human-based interventions can be minimised, greatly reducing administration costs and speeding up routine tasks enormously. For suppliers, this can lead to lower overheads, less need for trade credit, and more rapid and reliable payments. Buyers benefit through improved transaction accuracy and visibility, fewer administrative overheads, and the potential for better pricing from suppliers.

Many large private sector businesses have implemented elaborate technology solutions to try to improve their invoicing workflows. Still the vast bulk of invoices are generated via manual transactions involving small businesses. The Australian economy is estimated to have roughly 1 billion invoices generated each year.

The last twenty years have certainly seen wide-scale replacement of paper documents with PDF equivalents exchanged via email. This is obviously an improvement over purely paper-based workflows, but it still has many inefficiencies and pitfalls. Emails containing PDF invoices are easily lost or misdirected, there is limited verification of the identity of the sender or veracity of the information, and it often involves physical scanning of paper. Worst of all, the PDF workflows used today often require the manual entry of basic invoicing data into electronic systems, even in situations where OCR technologies are in place.

The technologies required to reliably and securely exchange transaction information

> The Australian economy is estimated to have roughly 1 billion invoices generated each year.

between organisations are now very well established, and across the world, are routinely used on a large scale by governments for invoicing and procurement. These systems involve the exchange of structured machine readable data in standardised formats, with automated validation of suppliers and purchasers. Typically, these systems are implemented as open messaging networks that allow access to any participating businesses within the network.

On the world stage, Australia is lagging the rest of the world in automated electronic invoicing. On the flip side, that means there are still significant productivity improvements and cost savings that can be achieved. Countries with the highest market penetration for electronic invoicing between businesses include Brazil, Mexico, and European countries such as Denmark.

In each of these cases, the government-mandated use of e-invoicing has dramatically lifted usage rates and market penetration. Research firm Billentis estimates that in 2015 the average overall adoption rate for e-invoicing across Europe is 28%, while in Australia it is below 15%. In Brazil, it is estimated that more than 90% of all B2B invoicing is handled via e-invoicing.

The slow adoption of sophisticated e-invoicing mechanisms within Australian government agencies has had clear flow on effects to the private sector, and been a major factor in Australia's overall poor e-invoicing performance.

In June 2015, the Australian Bureau of Statistics estimated that 90% of active Australian businesses have four or fewer employees. It is also estimated that approximately 500,000 small businesses are suppliers to Australian government agencies, with the vast bulk of the transaction volume between the public and private sector occurring at a state and local government level.

Given the scale of transaction volumes carried out between Australian government agencies with small and micro businesses, it is clear that any effort to achieve efficiency improvements will require government leadership, to help standardise invoice data exchange formats and foster the use of new e-invoicing mechanisms.

While the Australian Federal Government has indicated they do not currently intend to mandate an e-invoicing standard, as has been done in Brazil, they have encouraged the formation of the Digital Business Council, an initiative which is led by public sector agencies, technology providers and industry bodies.

The purpose of the Digital Business Council is to consult and establish working groups to help create a common interoperable framework for e-invoicing within Australia. Initial data exchange formats and mechanisms have already been documented, allowing pilot projects to commence with both public and private sector participants.

One of the technology providers that has actively led the standardisation process and is participating in pilot projects is MessageXchange, an Australian-developed cloud platform designed to allow businesses to automate the direct exchange of information in a highly secure manner.

MessageXchange has pioneered cloud-based automation of supply chain workflows.

The current MessageXchange platform already handles the exchange of electronic messages for many of Australia's most successful businesses, including Computershare, Australia Post, Telstra, Costco, The Good Guys, and Harvey Norman, transacting more than 100 million messages per year.

According to John Delaney, Managing Director of MessageXchange, the benefits of moving beyond emailing PDF invoices to clients are a no-brainer. "Every level of government in Australia is looking to encourage small, innovative businesses to take part in government procurement. The best way to handle this efficiently is to learn from some of the biggest, most streamlined supply chains in the world — Australia's retailers."

"World class retailers handle this diversity of small business suppliers by providing simple, highly automated cloud-based platforms for their suppliers to use — at no cost to the supplier. This ensures there are low entry barriers for new suppliers, and they can on-board suppliers rapidly, at low incremental cost."

MessageXchange
www.messagexchange.com

HISTORY LESSONS FOR DRIVING **TECHNOLOGY-ENABLED TRANSFORMATION**

THE BIG CHALLENGE FOR TODAY'S ENTERPRISES IS NOT JUST FIXING LEGACY SYSTEMS, BUT FIXING LEGACY THINKING.

Kevin Noonan, Lead Analyst, Government, Ovum

Digital transformation has quickly become one of the IT industry's hot topics, but it is not all good news. While there have been some clear successes, there have also been some high-profile failures. One of the key contributors has been a lack of attention to driving cultural change. Leading change is about leading people. It is about creating alignment, building commitment and constructing partnerships. This is not a new message, and variations have continued to resonate through the ages.

In recent history, much has been written in the media about the potential negative consequences of the internet and social networking. In 2008, Nicolas Carr wrote a popular article: Is Google Making Us Stupid. He argued that people were losing the ability to focus on detail and follow logic, because they had become more accustomed to skim reading information off the internet.

Carr was not alone in maligning the way technology development is affecting the way people are able to think. Indeed, there are many historical equivalents where similar claims were made about technology.

More than two thousand years ago, the classical Greek philosopher, Socrates, complained about the invention of writing, and that it might be having an adverse impact on people's brains. He believed that writing "will introduce forgetfulness into the soul of those who learn it. People will not practice using their memory because they will put their trust in writing."

Complaints about technology's adverse effects have continued throughout history. In 1815, Thomas Clifford Allbutt (famous at the time for inventing the medical thermometer) complained there are "a number of nervous maladies resulting from living at high pressure — the whirl of the railway; the pelting of telegrams; the strife of business; the hunger for riches; the lust of vulgar minds for coarse and instant pleasures…"

Of course, with the benefit of hindsight, we now know the practice of writing did prove to be extremely useful. People did not lose their memory, but gained a valuable tool for recording far more than the human memory could have possibly contained. We also know that telegrams and locomotives did not fry people's brains, and the internet did not create an epidemic of stupidity.

Good leadership needs to draw upon the same underlying qualities of human ingenuity that has helped humanity to adapt and succeed across the millennia. Today, we are again faced with challenges that are not just about managing projects, but also about leading people.

It is also time to consign the phrase "I am not an IT person" to the rubbish bin. This phrase no longer reflects business reality, and it is clear that the next generation of millennials frankly do not even care. Technology has become an inevitable part of the business landscape. It is no longer appropriate to cling to a past where it was the practice to separate the two. The big challenge for today's enterprises is not just fixing legacy systems, but legacy thinking.

10 YEARS MELBOURNE 2007-2016

COMMS 2016 CONNECT

Melbourne

22-24 November

Melbourne Convention & Exhibition Centre

NEW VENUE!

Events for critical communications users and industry

Utilities | Government | Enterprise | Transportation | Resources | Public Safety

CONFERENCE HIGHLIGHTS

Kevin Vinsen
Research Associate Professor
International Centre for Radio Astronomy Research

Bill Schrier
Senior Advisor
US First Responder Network Authority (FirstNet)

Crispin Blackall
Director Global Enterprise Product Engineering
Telstra

Station Officer Graham Tait
Systems Officer, Operational Communications
Fire & Rescue NSW

PLUS: 1500+ users and industry experts | **100+** exhibitors | **75+** speakers
… and so many more reasons that you need to attend and connect with your peers and the 100's of industry experts waiting to offer you the solutions you need.

FREE EXHIBITION ENTRY

8 PRE-CONFERENCE TRAINING WORKSHOPS

- Understanding radio over IP
- Keeping the spectrum clean — ACMA activities and compliance priorities
- Implementation of location services within a radio dispatch environment
- Fleet management cradle to grave utilising OTAP
- Mission-critical communications redundancy
- Integrated operations: beyond IT/OT convergence
- Critical communications, where to from here
- Building a radio network from the ground up

IT'S HOW WE CONNECT

Platinum Sponsors: Hytera, sepura, excelerate

Delegate/Visitor Bag Sponsor: Mingara

Gold Sponsors: tait communications, NEC, ZETRON, simoco, rftechnology, Motorola Solutions, omnitronics

Conference Guide Sponsor: Ericsson

Supporting associations & media organisations: DMR, RFUANZ, TCCA, dPMR, DMR Applications, TETRA Applications, RadioResource International, IWCE, LTE Applications

Lanyard Sponsor: Hytera

Media Partner: critical comms

Association Partner: ARCIA

In conjunction with the ARCIA Industry Gala Dinner
23 November — MCEC, Melbourne
Visit www.arcia.org.au to book your tickets

melbourne.comms-connect.com.au

follow us on

Maximise and secure your Mobile Investment

NETMOTION® WIRELESS

WDS WIRELESS DATA SOLUTIONS

Provide exceptional mobile experiences

NetMotion Mobility is the only intelligent VPN solution for secure connectivity and management of mobile deployments. It's designed specifically for workers who rely on wireless networks and mobile devices to get their jobs done.

Overcome wireless challenges

- Connectivity: Deliver a resilient, "always-on" connectivity experience that exceeds user expectations.
- Visibility: Unleash usage metrics for devices, applications and networks for business intelligence.
- Control: Take management control over network access and enterprise resources to give users a customised mobile experience.
- Diagnostics: Pinpoint and resolve connectivity issues end-to-end – from the mobile device, across any network to your enterprise and cloud applications.

Transform & optimise mobile access

- Control access to applications and devices - for a single user to the entire fleet - based on customisable conditions like the time of day, network type, or even application bandwidth requirements.
- Automatically diagnose connectivity issues and analyse every data hop between devices and application servers to solve the problem.
- Optimise data delivery for faster throughput across even the most bandwidth constrained network.

No one knows mobility like we do

Over 3,500 of the world's most respected organisations, including Australian police agencies and utilities, depend on our software every day to get their jobs done.

Free trial offer

You can try it for free, for 30 days without obligation in a test environment or in production. Try it against your current VPN and see the difference. Call WDS today to arrange your trial.

Wireless Data Solutions Pty Limited
Tel: 1300 937 496 Fax: 1300 937 479
Sales@WirelessData.com.au
www.WirelessData.com.au