

# NZSecurity

August / September 2015

## Conference 2015

Safe & Secure Cities

Why Safer Cities?

Making Privacy Easy

Privacy Good Research Fund

NZ \$7.95 inc. GST  
Aus \$8.95 inc. GST



ISSN 1175/2149

[www.NewZealandSecurity.co.nz](http://www.NewZealandSecurity.co.nz)

Image supplied by the Office of the Privacy Commissioner and is an acrylic on canvas "No Privacy in the Bathroom" by artist Shar Young of Vincents Art Workshop



**Loktronic**

SECURITY • TECHNOLOGY • RELIABILITY

# *your* electromagnetic locking specialist!

**Underpinned by  
25 year's  
experience  
and service with  
integrity.**

**Standard features include:**

- Field-selectable 12 & 24 VDC options
- 300/550/750 kg holding force options
- Slimline styling
- Instant release
- Stainless steel fitting hardware
- Through hardened, polished stainless sex nut
- Full protection against transients.

**Options include:**

- Door Position Switch
- End-to-end Magnetic Bond Sensor
- Header extension angle bracket
- Custom full width housings
- Z/L brackets for inward opening doors
- Frameless glass door brackets
- Powder coated or anodised colours
- Stainless indoor, outdoor and gate locks

For expert advice and assistance with **your** security locking needs, trust in Loktronic, call us on **0800 367 565**

**10**  
YEAR  
GUARANTEE



**Loktronic**

Loktronic Limited Unit 7 19 Edwin Street Mt Eden Auckland  
P O Box 8329 Symonds Street Auckland 1150 New Zealand  
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK  
mail@loktronic.co.nz [www.loktronic.co.nz](http://www.loktronic.co.nz)



Your **guaranteed supplier** of  
**Lockwood** and **Trimec** products.  
**PLUS!** Large stock and  
numerous models available.

**uniview**

# IPC6242SL-X22(G) 2MP 22x Laser IR Network PTZ Dome Camera

## Features:

- Accurate and fast focusing
- 22x Optical Zoom (4.7 ~ 103 mm)
- Combined IR LED and laser, up to 500mtr IR distance
- Build-in Varifocal Laser generator
- Optical glass window with higher light transmittance
- IR anti-reflection window to increase the infrared transmittance
- Hydrophobic Im coated, water and dust repellence
- ONVIF Conformance



## Contact Details:

Craig Flint

Telephone: +64 (07) 868 2703

Mobile: +64 (0) 274 597 621

## Postal and delivery address:

27 West Crescent

Te Puru 3575

Thames RD5

New Zealand

## Email & Web:

craig@newzealandsecurity.co.nz

www.NewZealandSecurity.co.nz

## Upcoming Issues

October / November 2015

Professional & Business,  
Accountants, Lawyers, Managers  
and Consultants

December 2015 / January 2016

Retailers

The largest retails in the country by  
number of employees

## Disclaimer:

The information contained in this publication is given in good faith and has been derived from sources believed to be reliable and accurate. However, neither the publishers nor any person involved in the preparation of this publication accept any form of liability whatsoever for its contents including advertisements, editorials, opinions, advice or information or for any consequences from its use.

## Copyright:

No article or part thereof may be reproduced without prior consent of the publisher.

ENJOY a **10** year guarantee\*  
on Loktronic Indoor Electromagnetic Locks!

\*Standard terms & conditions of sale apply.

**Loktronic** 0800 367 565  
www.loktronic.co.nz

2015/1

# CONTENTS

- 6 The New Zealand Security Conference And Exhibition  
"Safe And Secure Cities"
- 8 Panasonic Launches 4K Network Cameras with 4K Ultra Engine
- 10 Practical training produces qualified professionals
- 12 Gallagher's T20 Terminal continues to turn heads
- 14 Why Safe Cities?
- 18 Enabling smart cities - The role of network video
- 20 Successful, Savvy Security Companies Ensure Safe Cities
- 21 NZ Government Protective Security Requirements (PSRs)
- 22 Privacy safeguards driving secure information destruction
- 24 From Loktronic Ltd - New generation electronic locking...
- 26 Rise of the machines - drones a new weapon for the Kiwi burglar
- 28 Wet dogs and new tricks - Axis turns up the innovation
- 30 Making Privacy Easy - the Privacy Good Research Fund
- 32 Something to CROW about- the 2015 NZ Cyber Security Challenge
- 34 Secure Identities Move Beyond Smart Cards into a Growing Smart Device Ecosystem
- 38 Biometrics Conference - trustworthiness critical to broad acceptance of biometric technology
- 40 2015's most and least reliable countries to do business in
- 42 Australia Round-up
- 44 Product Showcase
- 46 Proving "Competency" for Security Consultants

## Industry Associations



www.security.org.nz



NEW ZEALAND INSTITUTE OF  
PROFESSIONAL INVESTIGATORS INC.

www.nzipi.org.nz



Advancing Security Worldwide™

www.asis.org.nz



www.masterlocksmiths.com.au





# The power to protect, detect and patrol.

Threats can come from anywhere. You need to be everywhere to counter them. You don't need super powers to manage the security of your site and the safety of your employees. With Axis video surveillance products you can protect everything from your outer perimeter to the inner core of your plant.

Take a closer look, visit [www.axis.com/criticalinfrastructure](http://www.axis.com/criticalinfrastructure) or send an email to [contact-sap@axis.com](mailto:contact-sap@axis.com) for more info.

Distributed by:

 **CHANNELTEN**  
SURVEILLANCE SOLUTIONS

**HILLS**

**AXIS**  
COMMUNICATIONS

# THE NEW ZEALAND SECURITY CONFERENCE AND EXHIBITION

## ***“SAFE AND SECURE CITIES”***

Will be held in Auckland on:  
Thursday 19th November  
Friday 20th November  
Saturday 21st November.

The venue is the ASB showgrounds  
217 Green Lane West, Greenlane, Auckland

The Conference theme this year is  
*“Safe and Secure Cities”*.

The safe-city concept presents a number  
of challenges:

- The sharing of information effectively to reduce crime and disorder
- The integration of smart intelligence-

gathering solutions with existing systems  
to offer a common platform for monitoring  
and dealing with situations at all levels

- Regulatory obstacles including data protection laws
- Delivering a return on investment when funding is required

We will also look at how technology has evolved and made it possible for government agencies, emergency services, public sector officials and professionals across the security industry to work together in order to deliver safe and secure cities which protect people and safeguard critical national infrastructure.

## Sponsorship Opportunities

### Awards Dinner Sponsor

Gold Investment: \$10,000 plus GST

The Security Industry awards dinner is a special and popular event, with many of the Industry's leaders attending. *(taken)*

# skills.

### Keynote Speaker Sponsor (A)

Silver Investment: \$5,000 plus GST for our major international keynote

This is an opportunity for sponsors to participate in the proceedings by sponsoring our major international keynote.

Miki Calero  
*“Securing Cities  
the Smart Way”*



### Security Personnel Sponsor

Gold Investment: \$10,000 plus GST

This is an opportunity for sponsors to provide guards and promote their guarding services for the duration of the conference.



### Keynote Speaker Sponsor (B)

Silver Investment: \$5,000 plus GST for our international keynote

This is an opportunity for sponsors to participate in the proceedings by sponsoring our second international keynote.

Peter Houlis  
*“Safe city: a security  
integrators view, lessons  
learned, more challenges  
and how a safe city should  
function in 2016”.*





# Sponsorship Opportunities

## Drinks & Nibbles Reception Sponsor

**Silver Investment: \$5,000 plus GST**

Sponsors of the drinks and nibbles will be provided the opportunity to strategically place their banners in the proximity of this event.



## Industry Breakfast Sponsor -

**Bronze Investment: \$2,500 plus GST**

This is an opportunity for sponsors to strategically display their banners in the breakfast venue and to introduce the speaker at that breakfast presentation.



## ID Badges & Lanyard Sponsor

**Bronze Investment: \$2,500 plus GST**

This is an opportunity for sponsors to participate in sponsoring the ID Badges & Lanyard. (taken)

# HILLS<sup>TM</sup>

## Session Sponsor

**Bronze Investment: \$3,000 plus GST per session**

This is an opportunity for sponsors to display their banners in the seminar room and to introduce the speaker for that presentation.



## Lunch Sponsors -

**Bronze Investment: \$2,500 plus GST per lunch**

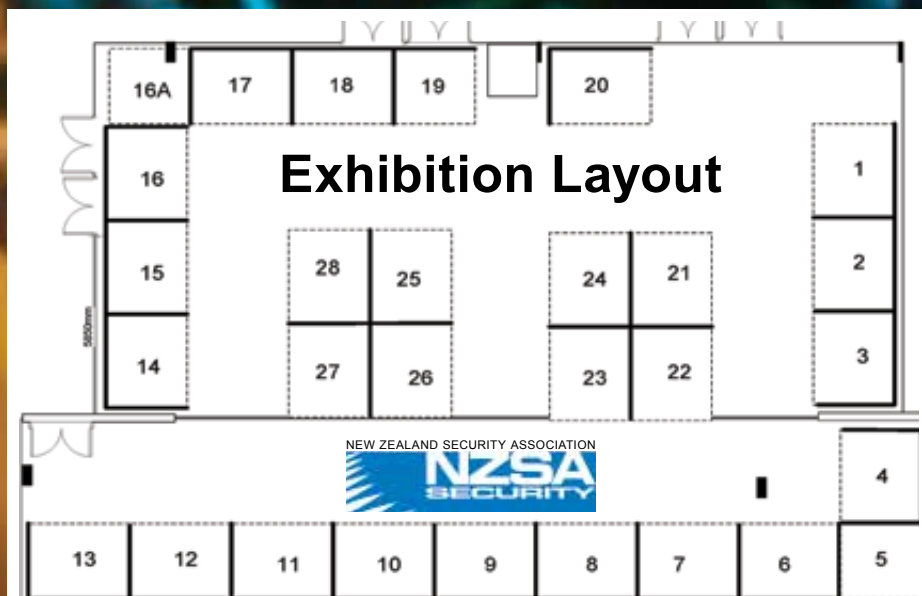
This is an opportunity for sponsors to strategically display their banners around the lunch venue and they will be formally announced as the lunch sponsor.



## Tea-break Sponsors

**Investment: \$1,500 plus GST per break**

This is an opportunity for sponsors to strategically display their banners around the tea venue and they will be formally announced as the tea sponsor.



**Contact the Sponsorship managers**

Email [greg@security.org.nz](mailto:greg@security.org.nz) or [Catherine@security.org.nz](mailto:Catherine@security.org.nz)

Telephone +64 9 486 0441 • Facsimile +64 9 486 0442

# Panasonic Launches 4K Network Cameras with 4K Ultra Engine

Last week saw the official release of Panasonic's latest true 4K network surveillance cameras at the Panasonic Systems Expo at Eden Park. It was the perfect location to unveil a camera range that pushes all weather, wide-angle image taking to unprecedented new levels of clarity and reliability.

The 4K standard is the latest in HD video technology, supporting resolution four times higher than full HD 1080p. Equipped with a 4K Ultra Engine, 1/1.7-inch high-sensitivity image sensor, Panasonic large diameter lens (F1.6), 6x optical motorized zoom, built in IR illuminators, the WV-SFV781L and the WV-SPV781L cameras enable clear identification of people and objects with 4K resolution. With a built-in IR LED, they capture clear images in low light or complete darkness.

What sets the new WV-SFV781L and WV-SPV781L apart, according to Paul Grey, Panasonic's Auckland-based Product Manager / Sales Engineer, is that the cameras are 'all Panasonic'. "We designed for 4K from the ground up; we developed all the components, from the lens to the memory card", he said. "It's end-to-end Panasonic 4K."

Total control over the manufacture of the cameras translates into complete belief in the reliability of their product,



*Last month Panasonic released its 4K network surveillance cameras at the Panasonic Systems Expo at Eden Park*

evidenced by Panasonic's three-year warranty. "If there is a problem – with a chip for instance – we can communicate directly with the engineer that designed it", explained Paul. In addition Panasonic's in-house testing ensures that the cameras are tested to standards well in excess of the label standards.

The WV-SPV781L's 3-drive lens system provides an impressive 17 (tele) to 97-degree (wide) horizontal angular field of view in 16:9 mode and 18-101 degrees in 4:3 mode (the WV-SFV781L boasts similar figures). The wide angle of view, delivers ultra detailed 4K images ideal for surveillance applications requiring wide area coverage, such as intersections, airports, railway stations, parking lots, factories, warehouses, port facilities and stadiums.

According to Paul, the high resolution and wide angles can result in less cameras being needed to cover large areas. "Fewer cameras means lower installation costs,

cabling costs, power, data and maintenance costs", he said. Panasonic's VIQS (Variable Image Quality on Specified area) and VMD (Video Motion Detection) technology also pushes down total cost of ownership. Both technologies deliver absolute clarity on footage areas that matter while decreasing image quality elsewhere, thereby keeping bandwidth consumption low.

The cameras' other image enhancing features include Panasonic's HLC (High Light Compensation) technology, which reduces strong light sources, such as vehicle headlights, to prevent the camera being blinded, fog compensation and SCC (Super Chroma Compensation), which delivers colour reproducibility even in low illumination. The unique Rain Wash function ensures that the all-powerful motorised variable focus 4K Panasonic lens remains obscurity-free.

For those blown away by the performance of the WV-SFV781L and WV-SPV781L at Eden Park, the superiority of these cameras was amply demonstrated on the field. Truly great performers are born, not made, and with these latest offerings from Panasonic, 4K excellence is in their DNA.

**For more information about Panasonic video surveillance cameras and solutions, please visit <http://security.panasonic.com/pss/security/>**



*Panasonic's new 4K network camera WV-SFV781L*



*Panasonic's new 4K network camera WV-SPV781L*



# 4K

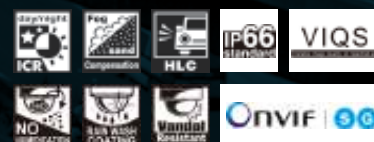
## IT'S IN OUR DNA

The new Panasonic WV-SFV781L Camera embodies Panasonic's Security DNA philosophy. We provide True 4K from the Panasonic made optics to the chipset and black box technologies, such as the rain wash coating. The WV-SFV781L is designed from the ground up to provide the best 4K experience.



### WV-SFV781L VARI-FOCAL CAMERA

- 4k images up to 30fps
- Ultra wide 6x motorised optical zoom
- 12.4 Mega pixel sensor
- Rain wash coating
- Fog compensation



## OUTSTANDING CLARITY

### THE PANASONIC VARI-FOCAL OPTICS AND 12MP SENSOR

#### 4K OFFERS IMPROVED CLARITY

With 4x the resolution of FHD more details can be seen.

#### FALL OFF REDUCED

The Panasonic 4-25mm optics insure the image stays sharp right to the edges.

#### 12M PIXEL MODE

The WV-SFV781L Can provide a 12M Pixel output at 15Fps.



[WWW.PANASONIC.NET/SECURITY](http://WWW.PANASONIC.NET/SECURITY)

# Panasonic

# Practical training produces qualified professionals

When it comes to professional development, FIRST Security's National Training Manager Mike Moriarty makes it clear where he stands. "If training doesn't change you then it's not working," he says. "It's supposed to change you; to make you a better person."

When he first came to security after a career in the New Zealand Police (Armed Offenders Squad and Special Tactics Group), Mike noticed glaring skills deficits in the industry. "I came from a structured, directed, specialised environment," he recalls, "and in 1998 when I started getting involved in security training, the industry had only just started embracing the national qualification model."

But that model seemed a mismatch right from the start. "It was theory/academic classroom-based training with competency-dominated teaching in an environment where the audience were officers doing 60 hours a week shift work", explains Mike. "It just didn't make a whole lot of sense to me."



*Mike Moriarty is First Security's Training Head*

So in 2007, he wrote a professional development workbook based on what he had identified as the various skills recruits needed in order to develop a professional profile. It was to become the centerpiece of FIRST Security's practice-based Professional Development Course (PDP).

"A good 95% of learners in our industry are kinetic learners, so I tried to make it as practical as possible," says Mike. "I wanted a training mechanism that actually did what training is supposed to do: develop the learner and give them the confidence and competence to do what they're meant to be doing."

Made up of five stages, Stage One of the workbook is "Basic Skills", which includes elements such as use of radio telephones, communication etiquette, how to use log books, and patrolling. Mike also created an officer's notebook so that officers had something to write on that possessed integrity for court purposes and that also provided an aide memoire for what to do when confronted with a scene.

Stage Two, or 'Advanced skills' focuses on health and safety, employers' statutory requirements, customer service, and basic investigation skills. "OHS stuff tended to talk about slips and spills", he recalls, "but the biggest risks faced by security officers is their fellow man: coming across an intruder in a building or someone taking your car or keys".

According to Mike, basic investigation skills isn't about trying to emulate the police but rather about using observational skills to assess a scene so that when police officer arrives they can be well briefed. "It's about giving police the information they require to carry on their investigation with confidence that they have been given the information they need", he explains. "Overall the industry has suffered a negative perception because we haven't provided this level of information."

The similarities and differences with the police is also a key theme of Stage Three 'Legal Skills', which focuses on topics such as arrests. For that particular topic, it's about getting security officers away from an arrest orientation. "Our people don't have the tools, skills and the mandate; how often do they come across a person who needs to be arrested? Not often."

Stage Four, which deals with personal and professional skills, focuses on issues such as time management, setting standards, accountability, leadership, goal setting, life balance, and who one associates with. According to Mike, "a lot of people who come into the industry are undercooked in terms of these skills". He sees 'ownership', or going to work as if you have a stake in it, as playing an important role. "There's a whole different pattern of behaviour that comes with that if our guys embrace it."

Taking the learning from each of the four stages together, trainee officers are then required to apply it to the site that they are working at. The idea being that skills are applied at different sites in different ways: a noise control officer's patrol, for example, requires a different mix of skills to that of a person doing a patrol at a retail outlet. "Skills are interwoven," says Mike, "and the problem with the existing qualifications was that the skills were all treated in isolation."

150 staff completed FIRST Security's PDP prior to the imposition of mandatory training last year, and since then FIRST has worked fast to blend its winning approach to training with the new requirements. Says Mike, "We want our staff to be trained in a particular way to meet a particular standard and which is in line with the national standards."

First thus took it upon itself to train its staff. "We put 25 supervisors and managers through the 4098 workplace





assessors course and a three-day train the trainer element with an accredited trainer, and then we delivered the course through our branches.” And importantly, they sought national level recognition of their in-house PDP, now called the “Officer’s Qualification Course” (the OQT).

“This year we worked alongside the NZSA to integrate the workbook with components of the national qualification unit standards so that now the officers introduced to a training component like patrols are given information about it, then practices it in the workplace. He then says to his boss he can take him on a patrol, walks and talks through what he does, then answers a number of questions, and then gets the national level certificate as a result of this assessment.”

“For FIRST, we faced a major challenge in melding together their own existing training, and the national qualifications, to ensure consistency of outcomes,” says NZSA’s head of training Stewart Reilly. “This exercise was not easy; but will have a long-term benefit for all concerned.”

Mike attributes a big part of the success of the program to NZSA’s input and expertise.

According to Stewart, NZSA has been working closely with client companies to make the generic qualifications work for them, which means injecting flexibility into delivery methods so that training can be more accessible to learners in security workplaces. “We see this flexibility as the future of training for our industry.”

It’s a line right out of Mike’s song sheet. “We wanted to give our staff a mechanism to show that they could do it”, he notes. “This is people’s employment... we should be lifting people and their sense of self-worth and capability.”

The demonstration-based nature of the program is perhaps its defining feature. Mike had originally envisaged the program’s assessments to be entirely demonstration due in part to the importance of clients seeing that officers were being trained at their sites. “Clients don’t care if you can talk or write about it”, explains Mike, “they just want to see that you can do it.”

An assessors guide explains how the unit standards merge with the demonstration-based assessments, while an assessment schedule keeps it all on track. Mike suggests that because officers are doing the work on a day-to-day basis, each unit should take around a week. The assessment schedule ensures that the 21 assessments are conducted over a period of 25 weeks.

The training has only just started, commencing with six branches, and the implementation plan has been ‘small groups, little bites’. But Mike seems quietly confident that the program will not only produce better security officers but will also evolve to offer more components in the future.

Ultimately, it’s about ensuring a quality basis to being the best in what is a competitive industry. As Mike puts it, “to be the provider of choice, we need to be the employer of choice.”

## Simple, Reliable, Stylish...

Commercial & Residential Intercom Systems  
using the latest 2 wire technology



**bticino**

From simple solutions to complex  
multi-site applications with integration to  
access control and cctv...



UNLIMITED  
COMBINATIONS  
FOR EACH INSTALLATION  
REQUIREMENT

**INNOVATION  
CENTRAL**  
*Wholesale Technology*

[www.intercom.co.nz](http://www.intercom.co.nz)

[info@incnz.co.nz](mailto:info@incnz.co.nz)

Phone: 0800 34 88 88

Mobile: 021 666 502

# Gallagher's T20 Terminal continues to turn heads

New Zealand owned security technology leader, Gallagher, is continuing to win attention around the world for its intelligent physical security systems. A significant award win at the ISC West security exhibition in the United States this year, has added yet another accolade to Gallagher's growing trophy cabinet. Winning Gold in the access control devices / peripherals division, Gallagher's T20 Terminal with Alarms impressed the judges and outperformed other entries across 12 categories including: quality, design, impact in the security industry, scalability and technical advancement.

Gallagher's T20 Terminal with Alarms received praise for its ability to deliver outstanding performance as a high-traffic card + PIN terminal and system management gateway, along with its ability to extend operator control of alarms management functionality right

to the door. The IP66 ingress rated T20 Terminal surpassed other entrants in the category with its impressive additional features including the IK08 impact rating for durability.

Throughout the industry, the T20 Terminal is gaining attention for its exceptional decision-response speed of up to 200 milliseconds, and its superior authentication and security with IT grade encryption levels delivered by Gallagher's HBUS communications protocol.

"Our T20 Terminal with Alarms is easy to use and can be configured to meet a wide range of user preferences. It has been very well received by both new and existing customers" said Marty Blake, Access Product Manager at Gallagher. "The T20 provides a high-security solution suitable for both large enterprise sites and small commercial businesses."



Further information about Gallagher's award winning T20 Terminal with Alarms can be found on their website: [security.gallagher.com](http://security.gallagher.com)





# Total site security

Protect your most valuable assets with an access control solution that enables you to manage alarms and enforce business policy directly at the door.





# Why Safe Cities?

Cities are the home and workplaces to millions of people. Therefore it is now more than ever that we need to collaborate and work together to create an environment where people of all ages and backgrounds feel safe at all times.

The concept of making a Safe Cities is complex but it often starts with some serious issues. For example the Henderson CBD was rocked by four deaths in a short time in 2014. This prompted the Henderson-Massey local board to develop a safe city approach. Initial responses were an increased police presence as well as the installation of CCTV cameras. The longer term approach was to consider designing out crime and creating a safe environment for the community.

Internationally the concept of safe cities and communities is not new. Both the World Health Organization and the United Nations have given serious support to the concept.

## **International Safe City Accreditation**

Safe Communities is a World Health Organization (WHO) concept that recognises safety as “a universal concern and a responsibility for all”. This approach to safety promotion and injury

prevention encourages greater cooperation and collaboration between non-government organisations, the business sector, central and local government agencies and creatively mobilises local community members to action. The WHO Safe Communities model creates an infrastructure in local communities through the building of local partnerships. It is a programme that was initiated in Sweden by the WHO Collaborating Centre on Community Safety Promotion.

Many New Zealand Cities and communities are part of the international Safe Community Movement. The safe community model was established for injury prevention and safety promotion at local level for all age groups, environments and situations.

The World Health Organisation supports the safe community programme and promotes the declaration that ‘Every person has the equal right to have all the advantages of a healthy and safe life’.

Progress of the strategies are measured and reviewed every year to ensure International Safe Community standards are achieved to maintain accreditation. This requires inter-agency cooperation, leadership from within the community and defined stakeholder commitment

as well as an understanding of criminal activity and the drivers of crime.

## **UN-Habitat**

Creating safe cities is part of a global movement, where The Global Network on Safer Cities, an initiative of the UN-Habitat was created with the goal of equipping local authorities and urban stakeholders to deliver urban safety, thus contributing towards securing the urban advantage for all.

## **What is a safe community?**

A community can be defined as a delineated geographical area, groups with common interests, professional associations, or the individuals who provide services in a specific location. The principles of a safe community will change accordingly, from place to place.

For individuals and families there is continued quality of life, ongoing participation in work, leisure and educational activities, and preservation of income and assets. For organisations and businesses the benefits of preventing injury include reduced disruption to their operations, increased productivity, retention of valued staff and reduced levies. The wider community has a lot to gain from





**Your security,  
our storage.  
The power of choice.**

## Marc Cisneros

Protector,  
Advocate,  
Guardian.

362,512 hours recorded,  
15,643 cameras strong,  
7,453 sequences stored,  
2,423 businesses secured,  
1,512 clients protected,  
**1** surveillance solution.



**WD Purple™**  
Surveillance Storage

WD Blue

WD Green

WD Black

WD Red

See more of Marc's solutions at:  
[wd.com/choice](http://wd.com/choice)



**absolutely™**

having a safer, positive and more productive population, and from less demand being placed on the health care and justice systems due to injury and violence.

Creative methods of education and environmental change joined with appropriate legislation and enforcement are an important beginning for the safety of a community. No single approach is sufficient for changing existing behaviour patterns.

## Government

The safety of the community is a responsibility of central government. Recognising the successes of safe community initiatives internationally, the Ministry of Justice has supported safer communities with funding and support with initiatives. The Ministry also recognises that while they hold responsibilities, in practice it is the community itself that needs to put it into effect and to do so in a sustainable way.

The Police put a lot of resources and effort into smarter policing. Police mobility (IPad and iPhone), access to real time information as well as the 'Prevention First' strategy has resulted in a reduction in crime. Between 1998 and 2007 the NZ crime statistics showed that police had become more effective at resolving crimes with resolution rates going from 36% to nearly 50%. Police report that they are likely to have a homicide resolution rate close to 100% in the near future.

The Police vision statement includes the words - 'Safer Communities Together' reinforcing their understanding of the need to 'work in partnership with individuals, communities, businesses and other public sector agencies'.

## How do we make a City Safe?

This problem was faced by the largest city in the United States. In the early 2000s New York recorded the biggest drop in violent and safety crimes in all the large cities.

Murder, robbery, burglary, theft and rape rates dropped significantly over a period of 20 years from 1990. For example the homicide rate went down 82 percent. A change in policing strategies and the removal of public drug dealing were cited as two of the primary reasons for the 'miracle' reduction of crime. But policing was not the only answer to the creation of a safer New York.

It requires a diverse range of security and safety professionals to come together with people from the community to discuss innovative and solution based ideas that are specific to that particular community.



A safe city approach must also be ongoing. Changes in the community can have an effect. Economic downturn, unemployment, disasters, changing demographic patterns, police availability as well as lifestyle changes all play a part.

Concepts for a safe city approach are almost endless, but include;

- Designing, building and planning
- CCTV surveillance technology, data storage and retrieval
- Public transport, road and pedestrian safety
- Crime prevention (CPTED) strategies and the understanding of the criminal mind
- Institutions and infrastructure safety: campus, schools, hospitals, aged care and shopping centres
- Safety initiatives for vulnerable groups: child, youth, mobility and mentally impaired, women, elderly, refugees
- Graffiti removal
- Late night safety
- Research, policy development and licensing laws
- Resilience to disasters
- Public awareness
- Restorative Justice

Education is also at the forefront of changes. Sir David Curruthers, head of the Independent Police Conduct Authority says there is evidence that reducing crime rates in New Zealand is partly caused by the reduction in the number of teenagers being expelled, suspended or leaving school early.

One emerging important aspect of a safe city concept is the use of technology and the sharing of information, much of it required in real time.

Safe cities and communities need support from specialist industries such as the security industry. Support usually comes in tangible items such as professionally installed and monitored CCTV systems, bollards, fencing and glazing etc. In particular, support in technological based systems including, intelligent detection systems, thermal imaging, facial recognition, license plate tracking, are proving to be intrinsic parts of a safe city approach.

## Public perceptions of crime

Public perceptions of crime is also an important factor with people feeling safe in their communities. Studies suggest that many New Zealanders hold 'inaccurate and negative' views on the crime levels in their communities. Yet, the Global Peace Index (2011) placed us as a country at the top after considering aspects of society including corruption, violence as well as the overall crime rate.

A forum held at Parliament in 2009 identified many socio-economic factors that contribute to crime. The government's response to these was the Better Public Services document outlining four priority areas to reduce crime which will be covered in the next issue of New Zealand Security Magazine.

## Community Volunteer Groups

Crime prevention in safe cities is not all about paid specialists from government or private business. Community volunteer groups in all communities assist emergency services. Community Patrols of New Zealand (CPNZ), Neighbourhood (NSNZ), Auckland Asian Safety Patrol (ASP), Pacific Wardens as well, as the Maori Wardens are recognised for their valuable contribution.

Other specialist community groups such as Woman's refuge, suicide survival support organisations along with numerous cultural specific support groups provide valuable intervention or support to those in need.

## Conclusion

It is more important than ever to create safe cities, urban areas and communities. We must recognise the safety issues and collaborate, improve or create safe environments. It is now vital to develop our knowledge to assist with mitigating dangers within our communities.

This is the first of a series of three articles focussing on safer communities. Written by Chris Lawton CEO of C4 Group Ltd and Chairman of the Trust Board for Community Patrols of New Zealand.



# THE ANNUAL NEW ZEALAND RISK MANAGEMENT LEADERS FORUM

A premier platform bringing New Zealand's leading industry practitioners together to share best practices in risk management strategies & frameworks across industry sectors

**Auckland | 09-10 November 2015 (Conference)**

**11 November 2015 (Post-Conference Workshop)**

## Featured Speakers Include:



**Roger Estall,**  
*New Zealand Representative,  
ISO Working Group*



**Katrina Felton,**  
*Director of Operations,  
McDonald's Corporation*



**Steve Gordon,**  
*Head of Risk Assessment and  
Assurance,  
Reserve Bank of NZ  
2014 RiskNZ Awards of  
Excellence*



**Steve Clark,**  
*Head of Risk and Assurance,  
Fisher and Paykel*



**Paddy Davies,**  
*Chief Risk Officer, Consumer NZ,  
GE Capital*



**James Turner**  
*Head of Risk and Audit,  
The Warehouse Group*



**Matt Cullum,**  
*Chief Risk Officer - Retail,  
Marketing & Wealth,  
Bank of New Zealand*



**David Middleton,**  
*Head of Crime and Business  
Continuity,  
Auckland Council*



**Karl Armstrong,**  
*Chief Risk Officer,  
IAG New Zealand*



**David Toyne,**  
*Group Risk Manager,  
Carter Holt Harvey*



**Nigel Edmiston,**  
*Chief Risk Officer,  
Vero Insurance NZ*



**Vanessa Johnson,**  
*Group Manager, Corporate Risk  
and Assurance,  
Inland Revenue NZ*



**Gillian Dudgeon,**  
*General Manager, Shared Services  
/Chief Risk Officer,  
Earthquake Commission*



**Adrian Sparrow,**  
*Group Risk Assurance Manager,  
Datacom*



**Doug Widdowson,**  
*Chief Risk Officer,  
TSB Bank*



**Christine Young,**  
*Head of Internal Audit,  
Kiwibank*



**Shane Bidois,**  
*Chief Risk and Safety Officer,  
MetService*



**Warwick Williams,**  
*Group Manager Risk and Analytics,  
Genesis Energy*



**Toby Beaglehole,**  
*Chief Executive Officer,  
New Zealand Oil Services*



**Aaron Davis,**  
*Planning and Preparedness  
Deployment Manager,  
Group Resilience and Risk,  
Fonterra*

The Annual New Zealand Risk Management Leaders Forum is a premier platform bringing the nation's most influential risk management leaders together to provide you with the latest industry thinking, topical issues and practical risk strategies.

Delivered by an esteemed line-up of CROs and Heads of Risk from the nation's leading organisations, this forum will provide you with an unrivalled networking opportunity, updates on the next ISO 31000 standard, awareness of the most pressing risk management issues and the opportunity to benchmark against industry best practices.

**Don't miss the Post-Conference Workshop:**  
How to manage risk more effectively



**Wednesday, 11 November 2015**

*Masterclass Leader:*

**Grant Purdy**

*Associate Director  
Broadleaf Capital International*

**REGISTER NOW!**

[info@aventedge.com](mailto:info@aventedge.com)

+64 9 306 8908

REGISTER ONLINE  
WITH VIP CODE **MP-NZSecurity**  
AND GET 10% EXCLUSIVE DISCOUNT!

[www.riskmanagementleaders-nz.com](http://www.riskmanagementleaders-nz.com)

Media Partners:

**NZSecurity**



Organised by:

**Aventedge.**





# Enabling smart cities

## The role of network video

The city of the future will be a smart city. Network video systems will have an important role to play in this - beyond today's safety and security installations

Around the world, town councils and municipal authorities are working on projects to make their cities smarter places to live in. While there are many slightly different definitions of the 'smart city', the main idea behind it is to use digital technologies to improve the quality of living for its inhabitants, reduce environmental impact and make everyday services run more smoothly.

Easy and efficient city management, optimized energy consumption, water and waste management, improved mobility, pollution and noise reduction, easily accessible online services, and intelligent buildings that attract tourism and new businesses, are all important components of the smart city of the future.

Security and safety plays a key role too, as it is impossible to develop a smart city where the citizens do not feel safe, and are restricted in what they can do and where

they can go. Crime statistics are one thing but it is important to understand the citizens' perception too as they may feel they are not well enough protected. A smart city has to be a safe place.

With city populations growing, there is a clear relationship between urbanisation and increasing incidence of crime. The centers and peripheries of cities are the biggest crime hotspots; population size and density are directly proportionate to crime rates. Cities are becoming more crowded, and return on crime is likely to be higher in larger cities due to the greater concentration of wealthier victims and a more developed black-market network for the disposal of stolen items.

To exacerbate the issue, the chances of stopping crime or arresting a criminal are typically lower in larger cities because they tend to have a lower budget per capita for law enforcement, and see lower

levels of community cooperation with the police. Of course, local and international economic factors also affect crime rates but are more difficult to control by the individual city.

To improve safety, crimes against people, property and public order have to be addressed at street level. Many towns are already using video cameras to help prevent, detect and investigate crime. City surveillance not only helps citizens feel safer, but video cameras can also be used to protect facilities and critical infrastructure both from natural and man-made threats.

Beyond safety and security, network video cameras will increasingly take on the role of smart sensors; facilitating components that provide important data to inform and enable the smart city – from improving traffic flow to supporting on-demand utility management services.





The smart city of the future will rely even more on digital and connected technology. It will be built on a system structure that is made up of four technology layers, with sensors forming the first of those layers. These sensors can be machine to machine terminals, wireless and mobile sensors, cameras that record video and audio, and even participatory sensing where the community contributes data and information, for example, about traffic congestion.

All these sensors connected by a city network via the communication infrastructure represent the second layer, the Internet of Things. Already in 1995, Axis Communications talked about “Internet of things” with their vision of Access to Everything. As Axis co-founder Martin Gren puts it: “Axis’ network cameras were certainly among the world’s first internet-of-things devices that were shipped in volume with embedded Linux, the AXIS 2100.”

Data and applications converge into a common operating platform, the third layer where the information processing and analysis takes place. The collected data is turned into usable intelligence, information becomes interactive, and citizen engagement is facilitated. Finally, the fourth layer is where the understanding of the data – both

real-time and historical data – powers smart city applications such as energy management, traffic optimization, noise reduction, and safety and security initiatives. With network cameras as sensors, entirely new applications will be possible that include controlling the effects of heavy rain or snow, adjusting street lighting according to the actual lighting needs and thereby reducing energy consumption and even managing bike or car sharing stations.

New applications will also help engage citizens more and allow them to be an active part of the city’s ecosystem. Smart mobile phones and apps enable citizens and tourists to provide information related to security and safety to city management. With citizens actively adding data and information about themselves or the city, and sharing it on social networks, city management can be informed about early traffic jams for instance, and use video and analytics to verify the situation, monitor actions needed and confirm responses, to put the citizens right at the heart of the smart city.

The four-layer model may sound complex, but the good news is that existing network video infrastructures can already scale for a safe city today and a smart city tomorrow. With security as the starting point, camera installations

today will become the foundation for the sensor networks of the future. The cameras will act as a hub for other sensors to be connected into a network of intelligent devices – for example, flood sensors, weather sensors, traffic and gate control systems. Many network cameras also come with built-in multi-purpose applications on board – number plate recognition, people counting and vehicle tracking, to name a few. This turns them into intelligent devices that can process data right at the edge of the network and share actionable information across the network. In this way, they will form the backbone of the city’s Internet of Things, provided they are built for easy integration and with an open architecture.

In the future, network cameras will play an important role above and beyond safety and security, as an open platform for the development of smart city applications, and an important source of open and big data. After all, a city can only be smart if you see it.

*By Andrea Sorri, Business Development Director Government, City Surveillance and Critical Infrastructure, Axis Communications.*

**AXIS<sup>®</sup>**  
**COMMUNICATIONS**

# Successful, Savvy Security Companies Ensure Safe Cities

They say that the best way to start the day is to get up nice and early and have a good breakfast. New Zealand Security Association's 3rd July Networking Breakfast ticked both of those boxes, with attendees kicking off the winter frost to enjoy a 7am breakfast at Takapuna's Blankenberge Belgian Beer Café.

Once the last of the lattes were drained, the breakfast became a case of 'food for the mind' as we made our way to the NZSA's new offices at 132 Hurstmere Rd where guest Speaker Mark Windust of Mastermind gave an insightful presentation on Business Development. It was something of a sneak preview, as Mark will also be speaking at this year's New Zealand Security Conference & Exhibition in November.

With plenty of experience in sales, marketing and business development for start-ups, big players and everything in between, Mark has plenty of wisdom when it comes to getting one's message out there. "Business development is challenging in any industry," he says, "and the security industry is no different."

According to Mark, there are so many changes with compliance, technology and legislation "that the customer doesn't know what they don't know and they are often making decisions based on ignorance, price or habit." In order to win new customers and develop new markets, he suggests, security businesses must first educate the market. "This challenge creates opportunities for those security companies that can evolve from a product selling approach to an educational selling approach."

Asked if there's one piece of advice he'd give to business operators to grow their business, Mark states "one of my mentors used to tell me, 'if in doubt, sell something!'" Putting is somewhat more elegantly, he continues "focus on a profitable customer segment (the narrower the better), get to know that customer type better than your own family and go to that market and 'sell something.'"

"Too many companies dilute their offering by trying to be all things to all people and rely on the market to come to them. Switch that mindset by going narrow and going to them."

After returning to New Zealand from a stint overseas, Mark had found that the sales and marketing capabilities of many Kiwi businesses were comparatively underdeveloped. This inspired him to launch Mastermind as a sales and marketing consultancy. "Now our focus is to help growth-focused kiwi companies to build their sales capabilities and become leaders in their space."

In line with its 'Safe and Secure Cities' theme, Mark reveals that he plans to talk at this year's New Zealand Security Conference & Exhibition on "how to safeguard and secure your future by building your sales capabilities."

"Building your sales capabilities is a function of strategy, systems and skills," Mark explains. "I'll go over the keys to an effective sales strategy, how to create your sales process by taking an educational approach and the sales skills you need to develop in your business to be successful in today's world."

"The audience can expect something different to what they



*Mark Windust of Mastermind*

have been taught in sales courses in the past, which is based on American techniques that worked in 10 years ago. My approach is a big shift from the traditional approach and focuses on what works in New Zealand today."

The New Zealand Security Conference & Exhibition is a three-day event staged by the NZSA. It is the single largest gathering of security professionals in the country, attracting between 100 and 150 delegates and aiming to have over 100 security organisations coming together in one location.

This year's conference theme of 'Safe and Secure Cities, presents a number of challenges. These include the sharing of information to reduce crime and disorder, the integration of smart intelligence-gathering solutions with existing systems to offer a common platform for monitoring and dealing with situations at all levels, regulatory obstacles including data protection laws, and delivering a return on investment when funding is required.

Presentations will also consider how technological evolutions have made it possible for government agencies, emergency services, public sector officials and professionals across the security industry to work together to protect people and safeguard critical national infrastructure.

Achieving safe and secure cities is possible only with a security industry comprised of professional and profitable businesses. Learning from the market wisdom of business masterminds like Mark, businesses can look to develop their sales and marketing capabilities and become leaders in their space.



# NZ Government Protective Security Requirements (PSRs)

The New Zealand Intelligence Community launched its Protective Security Requirements (PSR) website on 15 December 2014. Despite this and the overall importance of the requirements to security service providers, very few providers know of them.

The PSRs reflect a different way of doing business when it comes to security services to government agencies. Much of the following information is taken from the PSR website supported by security and training consultant Chris Lawton - [www.protectivesecurity.govt.nz](http://www.protectivesecurity.govt.nz).

‘The PSR aims to provide better guidance and support to enable New Zealand Government to meet core requirements in the areas of protective security governance, personnel security, physical security and information security. It’s the product of extensive collaboration with a number of New Zealand Government agencies.

The purpose of the PSR is to help agencies:

- identify their individual levels of security risk tolerance
- achieve core requirements for protective security expected by government
- develop an appropriate security culture to securely and effectively meet their business goals’

Earlier this year the government ran a series of sessions for commercial service providers to update them on the PSRs, the government’s approach to protective security and information to enable service providers to provide services that will meet the requirements.

‘It will enable service providers to understand the security-related contractual criteria that will be a condition of outsourced services.’

One of the reasons for the PSRs are situations such as the Ashburton Work and Income tragedy. WorkSafe NZ laid one charge against the Ministry of Social Development (MSD) in relation to the shooting at the MSD Ashburton office on 1 September 2014 in which two Work and Income staff were killed and another was injured.

The charge (under section 6 of the Health and Safety in Employment Act) alleges that the Ministry of Social Development failed to take all practicable steps to ensure the safety of its employees while at work.

The invoking of Health and Safety legislation is a sign of future times with the new legislation criminalising failures to ensure staff safety. Legislation will go hand in hand with the PSRs for protecting staff at risk.

Information security is also detailed in the PSRs. ‘New Zealanders need to have trust and confidence in the way their information is being managed and used by government agencies.

The government takes all aspects of privacy and security very seriously. In the PSRs agencies will find guidance and resources to build their capability in managing privacy and security.’

The leadership shown by government in development

standards (PSRs) and the future regular auditing of the standards set by crown entities and other associated organisations, is a significant step up in security across both the government and service provider realms.

Many security service providers will already meet the standards required by government but in my view there will be two important considerations falling out of the PSRs.

Government agencies will need to upskill or employ qualified people as Chief Security Officers. It will also see a number of them join professional organisations such as ASIS an international organisation focussing at security management level.

Security service providers will have to meet the requirements with respect to training of security staff, whether they are guards, supervisors or managers. Security providers that attain recognised qualmark certification will ultimately obtain more contracts than those that don’t reach those standards.

Chris Lawton, CEO of C4 Group Ltd is an experienced security and training consultant. For more information email [psr@nzsis.govt.nz](mailto:psr@nzsis.govt.nz) or contact the author [chris@c4group.co.nz](mailto:chris@c4group.co.nz).

## Diploma in Security Management

### Specialist Programme in Protective Security Requirements (NZPSR)

New Zealand’s only Diploma level security course specifically designed for Chief Security Officers  
Modules include;

- Operational Security Plans
- Legal Issues
- Security Risk Assessments
- Security Surveys
- Develop Policy and Procedures
- Security Management Principles

As the only ‘Skills Certified’ security training provider in New Zealand C4 has the Security industry Standard Setting Body support for its programmes.

The National Diploma in Security Level 6 is currently under review and C4’s Diploma, focussing on the PSRs, will map directly to the new qualification.

Chris Lawton (CEO C4) is directly involved in the review of this qualification at a Skills and NZQA level.



For more information go to [www.c4group.co.nz](http://www.c4group.co.nz)

# Privacy safeguards driving secure information destruction

---

In a 23 February 2015 media release, Freightways Limited Managing Director Dean Bracewell commented, "Privacy of business information will continue as a key driver of demand for secure document destruction services." Information destruction is looming as a growth industry of the future as consumers become more protective of their privacy rights and governments move to legislate accordingly.

Whereas in the past information destruction simply meant putting sensitive documents through the secure paper shredder, the information revolution has changed all this.



*Bob Johnson, CEO of National Association for Information Destruction (NAID)*

According to Recall's New Zealand website, hard drives and media tapes contain much more confidential information than paper documents. "One LTO4 media tape can store 800 gigabytes of data," states the site, "which is equivalent to 18 tractor-trailer loads of paper."

## **The easy part: document destruction**

There are essentially two different methods used for physical document destruction: on-site (mobile) and off-site. With the mobile option, a business fills secure bins with documents that need to be destroyed. Once the bins are filled, an appointment for destruction is scheduled. A truck equipped for shredding arrives and the documents are destroyed, usually under supervision.

In the case of off-site paper shredding, a business either arranges for pickup or delivers the files directly to a destruction facility. Once they arrive, the documents are placed in a locked area for same day destruction. Clients witness either the documents being placed in a locked container at drop-off or the actual destruction process itself.

The mobile method is generally considered the most secure option as documents have very little opportunity to fall into the wrong hands, but it's also relatively expensive.

## **It's complicated: data destruction**

Protecting the privacy of clients, customers and others by destroying paper records is one thing, but what about

electronic records? Electronic, or digital, records could include information held in computers, on storage devices or even on internet servers that may or may not be owned or controlled by the business in question.

And even the most accessible of data can be difficult to erase. According to Auckland-based IT Recycle, data such as passwords, digital photos, personal documents and online histories "are eternal unless they are physically destroyed or wiped using intensively high level formatting." Then there is data remanence, which is the residual representation of digital data that remains even after attempts have been made to remove or erase the data.

As with document shredding, several standards exist for the secure removal of data and the elimination of data remanence. These include standards by professional bodies such as the National Association for Information Destruction (NAID), which is the international trade association for companies providing information destruction services and the GCSB through the 2015 New Zealand Information Security Manual.

Just how tricky information destruction can get is evident in the cases investigated by organisations such as the Office of the NZ Privacy Commissioner (OIC) and various ombudsman bodies. A September 2013 complaint to the OIC against a recruitment agency that had failed to remove all personal information of a client from an old online profile is evidence of this.





*The pieces of a physically destroyed hard drive. Source: IT Liquidators*

After the client advised the agency he no longer wanted to use its services and asked to have his profile removed, the agency removed the man's name and photo from the online profile and removed the link to his profile from its website. However, the rest of the profile, which included other details about the man, was left online.

The man was no doubt surprised when he subsequently discovered that the edited profile was available in Google when he searched his name.

The Privacy Commissioner found that although the man's name had been removed from the profile, it could still be considered to be personal information that identified him because of its detailed nature and because it was still being linked to his name through Google. The agency accepted this and, as a result, removed the remainder of the profile from its website.

According to Bob Johnson, CEO of NAID, "When examining data protection compliance around the world, the trends definitely favour more stringent regulations and stronger penalties. Lawmakers in countries such as the US and the UK have learned the hard way that organizations require clear direction and stiff consequences in order to take privacy seriously.

"While we have seen some recognition of this in New Zealand and Australia," he continues, "regrettably they still rely on a more conciliatory advisory position. The good news for the public is that sooner or later all jurisdictions eventually intensify their approaches largely because it is the only thing that works."

The trend towards ever-stricter legislative requirements around privacy means that it is in the interest of businesses to review their information destruction policies and processes... and to look at establishing these if they don't already have them.



*Electronic waste dump at Agbogbloshie, Ghana, where organised criminals commonly search drives for information to use in local scams*



# CAME

## AUTOMATION

### Reliable Proven Quality

### Now With Reliable Supply & Technical Support



### Gate Automation Direct

### Direct To The Trade

Enquires to  
**Info@gad.co.nz**

**0508 438 428**

# From Loktronic Ltd

## New generation electronic locking...

Award-winning innovators, FSH (Fire & Safety Hardware Ltd) have long been recognised as world-leaders in electromechanical locking and security solutions. Recently acquired by Allegion, FSH's range of revolutionary electromechanical locking and security products complement Allegion's existing range of security solutions available here in New Zealand.

### A greener future

With an eye on protecting our natural resources and helping to reduce carbon footprints, FSH's team of engineers embarked on a project to redesign a selection of locks, strikes and drop-bolts to provide the same level of hold and security as their previous models, but with a much lower power consumption. This innovative project led to the new EcoLine™ series – a range of energy saving electromechanical locking devices.

The EcoLine range of devices have a lowered energy consumption of up to 80% - a significant reduction in power draw – and still offer the same, if not better, holding force than larger, less power efficient models. A lower power consumption also results in energy cost savings, an important consideration for future mapping.

### Smaller and more powerful

Reduced power consumption in turn, reduces the wiring size and stand-by battery capacity requirements of standard magnetic locks. Designed as an alternative to older

models of magnetic locks, the innovative, slimline MEM2400LP Mechanical Electro Magnetic Lock retains all the features of a much bigger lock, but is 75% smaller than a standard 600kg magnet.

This smaller size is especially suited to situations where door height or narrow profile door frames create installation restrictions, or when appearance is of paramount importance.

Alongside the reduction in physical size, the MEM2400LP has a high holding force of up to 1000kg and releases under side loads of up to 70kg.

Added security features of the MEM2400LP include an "Early Warning" alarm, FSH's patented Anti-Tamper Bracket and the lock is fire rated to AS standards of four hours.

### Pre-load capability

Part of the design process for the unique EcoLine Drop bolts was engineering pre-load capability into the mechanism. The patented EcoLock™ VE1260 motorised drop bolt is a high torque, motor-driven drop bolt with up to 35kg pre-load capability. It achieves this by consuming an in-rush current of 290mA @ 12VDC only during locking and unlocking action. During Sleep mode, the drop bolt only consumes a current less than 15mA @ 12VDC.

The VE1260 can be installed vertically in the door frame (lock style) or horizontally in the frame header and has a symmetric dead-bolt mechanism to allow the drop bolt to be used on 180° swing through doors. With a holding strength

of 1000kg, the VE1260 can be fully monitored and is operational on multi voltage from 12 to 30VDC.

### High security, less power

Combining both pre-load capability and high security locking into one device, the patented FES90M-P High Security Electric EcoStrike™ is a revolutionary electronic locking solution. With 35kg of pre-load capability, the FES90M-P features minimal energy consumption in Sleep Mode (less than 15mA @ 12VDC) and has a holding strength of up to 1300kg. This strike is guaranteed shock and hammer resistant!

A motorised locking device, the EcoStrike FES90M-P accepts voltages from 10 to 30 VDC and consumes current less than 300mA @ 12VDC at full 35kg pre-load only during locking and unlocking action.



FES90M-P

High Security Electric EcoStrike™

### A safer future

Securing our safety while reducing our carbon footprint has become much simpler with FSH's EcoLine™. As part of FSH's commitment to quality, all EcoLine products undergo stringent testing to ensure continued, robust and reliable function. Innovative design features, pre-load capabilities and enhanced product performance of each EcoLine device utilise advanced technology and reduced power consumption ensure greater levels of security with minimal ecological impact.

An investment in EcoLine is a commitment to a safer and greener future.

FSH's standard range of electromechanical locking solutions, as well as the EcoLine series, are available from Loktronic, an authorised Allegion distributor.



MEM2400LP

Mechanical Electro Magnetic Lock



The patented EcoLock™

VE1260 motorised drop bolt



# Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

# HOLD ON A MINUTE

## ...OR AN UNRIVALLED 10+ YEARS!

**Not all products are created equal.**  
Take Loktronic's premium quality Fire  
Door Holding Electromagnetic FDH40...  
they are simply the best in their field.



**PLAY IT SAFE AND LOCK IN**  
Loktronic quality, every time



FDH40S: Standard, floor mounted



FDH40SS: Flush mounted



FDH40SS: Surface mounted



Designed, tested  
and produced in NZ  
to AS4178

10 year guarantee\*

Unbreakable  
universal mounting

Floor or wall  
mounting options

Superior quality  
materials  
and fastenings

Full and immediate  
on-shore support

## Loktronic

Loktronic Limited Unit 7 19 Edwin Street Mt Eden Auckland  
P O Box 8329 Symonds Street Auckland 1150 New Zealand  
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK  
mail@loktronic.co.nz [www.loktronic.co.nz](http://www.loktronic.co.nz)

For expert advice and  
assistance with **your** security  
locking needs, trust in Loktronic,  
call us on **0800 367 565**

\*Standard terms & conditions of sale apply.

# Rise of the machines

## drones a new weapon for the Kiwi burglar

---

Drones could soon become the weapon of choice for Kiwi burglars, according to Marsden Hulme, GM of home security company Vivint. International reports highlight the use of drones or unmanned aerial vehicles (UAVs) by thieves around the globe to target private homes and New Zealand's current lack of regulations is making our houses vulnerable.

Given their extensive use by military and law enforcement, the harnessing of drone technology by those on the other side of the law seems something of a grand irony. Numerous cases of thefts thwarted by crime fighting drones have been widely celebrated in the international press, but now it seems that criminals are also discovering the airborne technology's utility.

### **A disturbing international trend**

Three years ago, Rodney Brossart became the first American citizen to be arrested with the help of a drone after allegedly stealing cattle. As recently as May, a convenience store robbery and auto theft suspect was captured by police thanks to a borrowed drone in the US state of Wisconsin. In Saurashtra, India, authorities facing a drinking water crisis deployed drones along canals to check water pilferage.

As perhaps we see all too often in the security industry, however, this technology has now been appropriated to support the misdeeds of those up to no good.

Last year reports emerged of a new hacker-developed drone capable of lifting

a smart phone's private data from its GPS location without the user knowing. Drones carrying the Snoopy software were able to intercept Wi-Fi signals when mobile devices attempted to find a network connection, posing an identity theft threat to their users. In the US, a theft ring dubbed the 'Tub Gang' have allegedly been using drone surveillance to 'case' properties for theft in New York and New Jersey.

This disturbing international trend could take root in New Zealand if regulations do not take potential criminal activity into account, says Marsden Hulme. He explains that increasingly affordability of the technology has meant it is now easy for drones to be purchased by criminals who use the devices to fly over properties and collect footage.

According to Marsden, a drone is able to give its operator detailed intel in real time on who is home, what doors or windows have been left open, and even images of what there is that might be worth stealing.

UAVs are also becoming increasingly agile, able to be flown over electric gates and wire fencing, under low hanging branches and to hover outside windows. Using drones, thieves can determine if a property is vacant, identify security weak spots, determine property layouts, identify alarm systems, and to monitor police activity in surrounding areas.

Marsden says that camera-mounted drones overseas have been recovered with footage of various homes and commercial



*Marsden Hulme, GM of home security company Vivint.*

properties that was used to identify burglary targets, and police in those countries were warning homeowners to report any suspicious drone activity in residential areas.

"Right now these devices are easy to buy, relatively cheap, and there are very few regulations on their use," he explains. "They are also getting lighter and quieter as the technology evolves."

"Small drones fall under model aircraft rules, and there is nothing to stop someone flying a drone with a camera on it over





- Keypad, proximity cards and magnetic stripe card options available
- Convenient and secure
- User friendly
- Open platform
- Up to 2000 users
- Stand alone, full access control

**For more information, contact  
Allegion (New Zealand) Limited  
on 0800 477 869 or visit  
[www.allegion.co.nz](http://www.allegion.co.nz)**

  
**ALLEGION**

[www.allegion.co.nz](http://www.allegion.co.nz)



your property to film, which could present a fairly serious privacy and security risk.”

Drone operators can face criminal charges in the case of drones used to commit a criminal offence. However, it can be difficult to determine the identity of the person flying the drone due to the fact that drones are remote controlled and do not have any licensing or identification attached to them.

### Big gaps in the law

According to Marsden, drone legislation in New Zealand has been driven by the Civil Aviation Authority (CAA), which has understandably been focused on keeping our skies safe. However, this focus means that there are no provisions



in current legislation nor in the coming August 2015 amendments that addresses public safety and privacy concerns.

“Legislation needs to be expanded to address public safety and privacy issues,” he argues, “which requires widening of Police powers to investigate and prosecute criminal activity under this proposed new legislation.

To effectively address all three concerns of aviation safety, safety of the wider public against potential criminal activity as well as addressing privacy concerns, legislation needs to be drafted with input from Civil Aviation Authority, Police and the Privacy Commission.”

For the time being, there appears to be no indication that legislation changes will look to address wider public concerns of protection against criminal activity or privacy breaches. According to Marsden, this leaves us exposed. “People want to be able to have a BBQ in their backyard with friends and family without this private event being spied upon and recorded by some unknown party with potential devious intent.”

### Keeping an eye on the sky

Marsden suggests that we need to make ourselves more aware of this technology and its capabilities. Increasing public awareness means strengthening community watch practices, “including the establishment of community Facebook pages where the wider neighbourhood community can be alerted to such sightings and immediately report to the Police any sightings of strange and foreign objects flying around your neighbourhood.”

At the household level, he suggests greater vigilance in security checks when leaving the house, even if it is only for a short time. “Professional burglars,” he warns, “can clean a house out within a couple of hours.” He also recommends installing and actively using a quality home security system, but again warns that less than 20% of home systems are regularly used by their owners.

Ultimately, the best available approach to foiling this invasive technology is somewhat more ‘last century’ than 21st century. “When you go away on holiday, tell a trusted neighbour, family member or friend. Give them a key to the house and ask them to check on the property regularly if not daily. Make sure your letterbox is cleared everyday. Have your neighbour use your driveway regularly so it looks like there is someone home.

“Have your curtains opened and closed each day - again make your house look as though it is being lived in. Have the neighbour put your rubbish bins out on the same night as everyone else and taken back in again the next day. Ask your neighbour’s kids to play on your property. Have someone mow the grass if you are going to be away for any length of time.”

Marsden observes that drone technology is becoming less and less expensive, more and more sophisticated and easier to acquire, which means that its use will become more pervasive amongst the wider criminal community. As crime evolves with the technology, it is incumbent upon lawmakers to play catch-up... and upon the public to be keeping at least one watchful eye on the skies above.

# Wet dogs and new tricks

## Axis turns up the innovation

---

The New Zealand Security Magazine recently caught up with Wai King Wong, Axis Communication's Melbourne-based Oceania head. Talking about Axis' recently opened Wellington office, Wai King also shed light on the company's recent product offerings, including innovations that take their inspiration from some of the most unlikely of places.

For the last 12 or so years, Axis has operated throughout Australia, New Zealand and the Pacific. This year, however, saw an expansion of its existing office network of Melbourne, Sydney, Brisbane and Perth to include a two-staff office in Wellington. It was, says Wai King, a strategic location move. "We selected Wellington mainly because it's the capital, and our main income is at the enterprise level."

Having been back and forth across the ditch more time than he'd probably care to remember, we asked Wai King about what he saw as the key differences between the NZ and Australian markets.

"Both countries are quite similar in terms of requirements, technology and the way business is done," he observes. "What a lot of people don't understand is that a camera is a camera. Thus the most expensive cost of a project is the labour component, and this is a similarity between Australia and New Zealand."

According to Wai King, one of main reasons why Axis has found success in this high labour cost setting is that it has provided integrators with ease of installation. Reliability is also a key.

"Each time you go out to replace a camera it already costs 200 dollars. We can never change labour costings or the economy itself, so the camera has to be advanced in order to keep costs down."

### **Zipstream: reducing the costs of storage**

Cameras tend to account for 20 to 30% of total cost, but storage, says Wai King, is an ongoing cost. Storage means moving parts, and a hard drive typically needs upgrading every three or so years. Axis' recently introduced Zipstream technology, he claims, enables customers to reduce the cost of storage by 50%. It's a big claim, but one that's been proven in testing.

Zipstream reduces data use and therefore storage by focusing on the images that matter. For areas that are still and don't require high resolution, Zipstream reduces compression and puts its efforts into focusing only on moving objects. According to Wai King, the difference between a Zipstream and normal image is minimal. "Performance in low light is good, and lower bandwidth does not mean picture quality degradation where it counts."

"Moving forward, all our products will have Zipstream technology," he explains. The technology will essentially come free, built into camera models across the Axis range. "We have a range of cameras from entry level to high end, and we are very competitive price wise. Anything released from today onwards will be Zipstream compatible – it's built into the firmware."



*Axis Communications' Oceania head, Wai King Wong*

The benefit of lower bandwidth for the enterprise customer is a smaller storage requirement. Some enterprises can spend millions of dollars on storage alone and will stand to save up to 30% with the technology. For remote monitoring, the savings are potentially huge, especially where real time data is being transmitted over 4G and even 3G networks.

Zipstream is designed to work seamlessly with Axis' other innovations, such as Forensic Capture, a technology designed to capture persons' faces and provide the best facial recognition possible. According to Wai King, multiple technologies have been employed to enhance capture on the facial side. After all, as he points out, "you need to see the person who is doing something."



## Back to the future: keeping analogue alive

Axis' stable of recent developments includes its M7011 video encoder. The encoder converts from analogue to digital, allowing customers to effectively go digital without having to replace their existing analogue systems altogether. By bridging the analogue-digital gap it can provide for big capital cost savings.

It's mainly designed, explains Wai King, for customers recently invested in analogue technologies. While it has its resolution limitations, people go with analogue mainly for cost saving. Analogue cameras continue to possess some security value, not least their deterrent factor.

The system is particularly useful for those who have existing infrastructure constraints, such as premises in heritage buildings, and are not able to otherwise move to the internet. "We can power the analogue camera to run high definition IP by inserting the converter," says Wai King, who suggests that some big case studies are on the way to showcase the technology.

## Outsmarting criminals... and competitors

Asked what sets Axis apart, Wai King was light on superlatives, preferring to continue talking through the company's impressive list of recent innovations.

Next on the list was Axis' just-released free software called Access Camera Companion. Suitable for a 10 camera or below type customer, the recording of DVR function is in the camera so all you need is an SD card and software for your mobile device. "The beauty," he says, "is you don't need a box."

"Imagine you have multiple cameras and a 4G tablet. The existing ways of doing it is quite tedious with TCIP requirements. We overcome this with access software we install in the camera, which talks to a server and creates an



*An Axis Q61 camera keeping watch over Wall Street*

encryption tunnel linked directly to your device, removing the need for port forwarding or an IP address. It's basically plug and play. It auto searches for you and auto assigns an IP address for you."

"When people break into a shop or house the first thing they look for is a box so they can stop the recording. They can't do that anymore."

And it's been tested thoroughly. "We do a lot of tests on quality controls... we try and smash it. In our R&D we actually have shot guns... we see if it still works after a couple of shots."

Last week, Axis released its own 64-gig SD card storage, produced in collaboration with SanDisk. It's a high performing edge storage solution optimised for video surveillance applications, which allows for flexible storage solutions, enabling video recording directly to an SD card.

The card combines the market and technology know-how of SanDisk, a global leader in flash storage, with Axis' unrivalled security systems credentials. And importantly, notes Wai King, "the difference between this one and the standard Sandis you get from the shops is a three year warranty and we guarantee that the recording is constant."

And what sort of reaction has Axis been getting from the market to all this? According to Wai King, the reaction has been audible. "Today is not the best time to be spending as much money as you can," he says, and Axis' new offerings have altered cost factors and changed how customers look into their overall costings. "A customer who could be running six frames per second for recording can now double up their recording and utilise the same storage they were using today. That's a big plus, particularly for enterprise customers."

## Wet dog leads to hot innovation

In terms of what's over the horizon, Wai King suggests that we keep an eye on the impending launch of the Q61, a new PTZ dome camera with Speed Dry function. "When it rains, you tend to get water droplets around the glass surface of a unit, so what people usually do to minimise this is to spray it with something," he explains. "We've designed the Q61 so that the unit is able to shake off the water."

It's a mechanical solution in which very high frequency vibrations shake off the water... a concept that takes its inspiration from nature. Picture a wet dog emerging from a swimming pool poised to rid its coat of excess water and you'll get the idea.

"If you put a wiper on a camera, you end up needing to replace it. Cameras are often mounted high up and therefore difficult to access. The design of the mechanics is very high speed and durable. Wear and tear is not a factor, and backed up with a three year warranty."

All this is evidence, says Wai King, that Axis is doing things differently to the old ways of doing things. After all, he says, "we are a technology company." For more details of Axis' security solutions visit [www.axis.com](http://www.axis.com).



*An Axis M7011 video encoder*

# Making Privacy Easy the Privacy Good Research Fund

---

New Zealand's Privacy Commissioner is calling for applicants for a new privacy-related research funding programme worth up to \$75,000. Successful applicants will receive project funding of up to \$25,000 to conduct privacy-related research and public education or awareness raising initiatives.

The Privacy Commissioner's Office, which administers the Privacy Act 1993, especially welcomes applications that might assist with "making privacy easy" for agencies or individuals or contribute to "better public services". Any applications for public education and awareness raising initiatives should address privacy promotion and the protection of personal information.



*John Edwards, Privacy Commissioner*



*No Privacy in the Bathroom. Acrylic on Canvas by artist Shar Young. Image supplied by the Office of the Privacy Commissioner*

It's the first year the Privacy Good Research Fund is being offered and the closing date for applications of 21 August 2015 is fast approaching.

According to a Privacy Commissioner's Office media release, the types of organisations

that are eligible for funding include academic institutions, non-profit organisations (including education institutions and industry and trade associations, consumer, voluntary and advocacy organisations) and for-profit organisations.



# Build your team, build your business

Upskill your team today

## skills.

The Skills Organisation  
0508 SKILLS (0508 754 557)  
[skills.org.nz](http://skills.org.nz)

The fund was established to capitalise on existing privacy research capacity in the academic and non-profit sectors; generate new knowledge and support the development of expertise in privacy and data protection; increase awareness among individuals and organisations of their privacy rights and obligations; and promote the application of research results by relevant stakeholders.

In order to find out more about the fund, we approached the Privacy Commissioner's Office with a number of questions.

**NZSM:** How did the fund come about? Are there similar programs operating overseas?

**PCO:** The Privacy Good Research Fund is a research programme similar to the Contributions Program run by the Office of the Privacy Commissioner of Canada. The concept of a privacy research programme took shape when Assistant Commissioner Blair Stewart had an opportunity to be seconded to Canada.

He was delighted to see the research outcomes of the Canadian Contributions Program and thought a research programme like this would be a good way to encourage privacy research across disciplines. The objective of the Privacy

Research Fund is to stimulate privacy related research, public education or awareness raising initiatives.

**NZSM:** How much interest has there been in the fund in terms of enquiries, and what sort of response are you expecting by the 21 August deadline?

**PCO:** This is the first time our office is running the Privacy Good Research Fund, so we hope to get a variety of interesting and compelling applications.

The Research Fund has generated a lot of interest both nationally and internationally. We have had over 360 views of our Privacy Good Research Fund webpage and over 60 downloads of the applicant guide.

**NZSM:** Is there a deficit in knowledge and awareness in NZ in relation to privacy rights and obligations?

**PCO:** While we are certainly always looking for opportunities to raise awareness for New Zealanders about privacy rights and obligations, this fund isn't really about trying to address any particular deficit. Rather it's about trying to encourage privacy research more widely to extend and deepen knowledge and expertise about privacy in general.

**NZSM:** When it comes to privacy, who are the "relevant stakeholders"?

**PCO:** This depends on the specific nature of the project proposed. However, the stakeholders are likely to either be individuals generally (who obviously have an interest in knowing about how their personal information should be / is being treated and what their rights are in terms of managing or protecting their information), or agencies which collect and use personal information.

**NZSM:** With the intrusive capacities of technology, is privacy becoming an increasingly contested domain?

**PCO:** Developments in technology, particularly with respect to the ability to collect large amounts of personal information from an increasing number of sources, present both a challenge and an opportunity with respect to privacy.

**NZSM:** What are the specific requirements for applications for the fund?

**PCO:** All relevant information about application requirements can be found on our website.

# Something to CROW about the 2015 NZ Cyber Security Challenge

---

Following a highly successful event last year, the Cyber Security Researchers of Waikato (CROW) is again hosting the NZ Cyber Security Challenge at the University of Waikato. The Challenge, which will also include an internship fair, guest lectures and talks by industry partners, will take place on 17-18 September.

Last year's Challenge, which was built around a zombie-themed capture-the-token style game, saw participants battling a bio-war inflicted zombie-virus across challenges of varying degrees of difficulty.



According to the head of CROW, Dr Ryan Ko, last year was more of a pilot to test how much traction such an event might gain. "Last year's challenge was opened to Waikato University students only, but managed to attract over 70 students for the training session and over 40 students for the actual challenge."

There was strong support from the National Cyber Policy Office and from the industry last time around, both in terms of sponsorship and the sending of staff to the challenge. "Some of our participants were eventually scouted by the industry partners," noted Dr Ko, "while the students realise that the cyber security industry was actually more than the typical stereotype of 'hacking'."

This year, the Challenge is not only going national, but is also expanding to two rounds and four categories: High School, Undergraduate, Postgraduate and



Open/Industry. “We are starting to gain interest from several high schools, not just from the Waikato but from several other regions as well.”

Once again, government and industry are coming to the party. “The National Cyber Policy Office’s Connect Smart Initiative and the Interpol are supporting our event,” commented Dr Ko, “while industry is supporting us in terms of sponsorship, training and speaking engagements and experience sharing.” Both groups will be assisting in validating the Challenge scenarios and participating in a job and internship fair.

For industry professionals, the Challenge is an opportunity to get to see some of the emerging talent coming out of universities as well as keeping up-to-date with what students are learning and what they are thinking about in terms of career options.

“This year, we are happy to have PwC and HP as platinum sponsors, while Aura Information Security is sponsoring as an



Official Training Sponsor. Several other sponsors are confirming soon. We are very appreciative of such strong support, and we aim to make this challenge a great experience for all.”

**If you and/or your organisation or institution are interested in participating, please register at: <https://cybersecuritychallenge.org.nz>.**

## 12 months on an update on the STRATUS project

This September sees 12 months since the announcement of government funding of \$10.6 million for the development of the Security Technologies Returning Accountability, Transparency and User-centric Services in the Cloud (STRATUS) project. The project is headed up by Dr Ryan Ko of the University of Waikato,



and the *New Zealand Security Magazine* got in touch with him for a one-year update.

For its submission last year, the STRATUS project (a consortium comprising the University of Waikato, the University of Auckland, Unitech and the Cloud Security Alliance) received the third largest grant in the Ministry of Business, Innovation and Employment’s (MBIE) science investment round. The grants will ultimately see a total of \$139 million invested over six years in new science research programmes.

**NZSM:** What’s been happening in the project during its initial 12 months?

**Dr Ko:** STRATUS was kicked off with quarterly meetings between the scientific research team and the industry partners in Hamilton and Auckland. It is our goal to engage industry from day one, as it is critical for the success of cloud security research.

A lot has happened since then; the project is wrapping up the hiring of researchers, and continuously recruiting top research students. Most recently in June, we did a demo session by all

research partners, and industry partners were able to visualise how the science can link to their strategies and products and [they were able to] provide feedback to researchers.

In July this year, STRATUS will have a session in InternetNZ’s NetHui to engage the users of the Internet, so as to gain grassroots feedback on the actual need of users. In November this year, with the help of MBIE, we will be holding our first STRATUS Forum in Wellington to engage the industry and showcase our research progress.

**NZSM:** What will be happening in the STRATUS world over the coming year?

**Dr Ko:** The goal for Year 1 is to build a strong team, and align industry and academic research towards technology transfer. I believe we are well on track to achieving that. Next year’s goal is to integrate the technology into actual products and kickstart a chain of NZ-led cloud security services which will return control of data to users.

The long term goal is to create an industry around such products and services – generated from NZ.

# Secure Identities Move Beyond Smart Cards into a Growing Smart Device Ecosystem

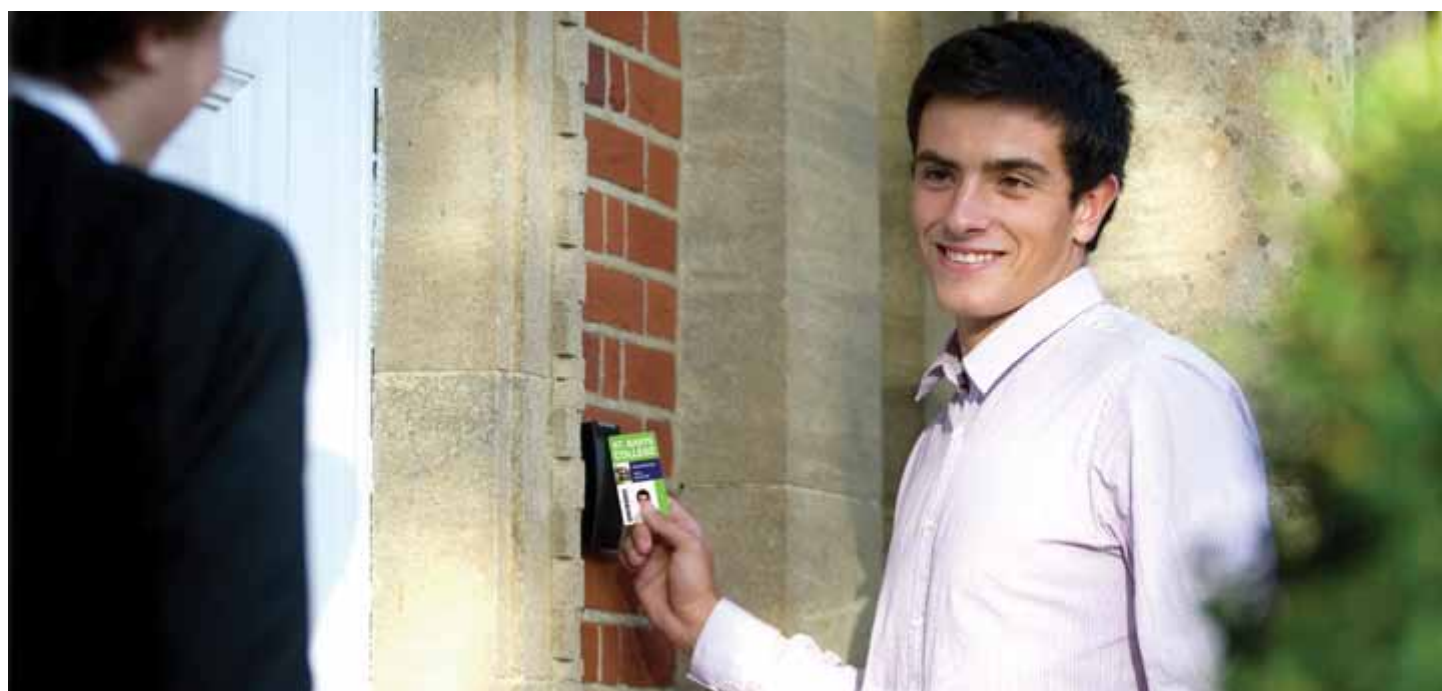
---

Today, any smart device – whether a traditional card or a device with wireless technology such as Bluetooth or NFC – can become a trusted credential used for recognizing, identifying and authenticating individuals. Meanwhile, advances in converged back-of-house technologies are enabling strong authentication and card management capabilities for computer and network logon, while also ensuring that physical and logical identities can be managed on a combination of plastic cards and smartphones, and that printer systems will support both. The result: a single card – or phone – can now carry multiple

identities and replace all previous mechanical keys and dedicated OTP hardware, within an access control system that provides a seamless user experience while delivering growing value to the organization.

The ultimate objective is a unified solution for ensuring secure access to the door, to data and to cloud applications, that uses an off-the-shelf appliance or cloud-based service to create, manage and use secure identities. All the technologies for achieving this objective are already here. Today's access control platforms deliver more sophisticated credentials, new credential form factors including

mobile devices, and many other useful capabilities. Perhaps most importantly, these platforms are based on open standards that enable organizations to evolve beyond current abilities, add features, and adapt to continuously changing security threats. With the proper foundation and planning, organizations can solve today's challenges, prepare for new capabilities such as mobile access control, add a diverse range of new applications over time, and pave the way for integrated, multi-layered PACS and IT security solutions that span all of the organization's networks, systems and facilities.







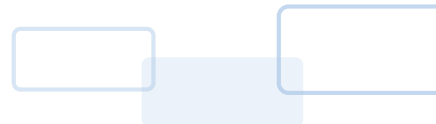
# SECURE ACCESS. NO CARD REQUIRED.

Secure mobile access solutions by HID represent a revolutionary breakthrough in next gen technology by combining convenience, flexibility and the power of Seos. With a simple tap or use of our patented "Twist and Go" gesture technology, you'll experience the most innovative way to make an entrance—no card required. And because it's all powered by Seos, issuing, managing and revoking access couldn't be easier—or more secure.

You'll call it the most advanced way to use your mobile device.  
We call it, *"your security connected."*

Contact [asiasales@hidglobal.com](mailto:asiasales@hidglobal.com) or **+613 9809 2892**

YOUR SECURITY. **MOBILE** | Visit us at [hidglobal.com](http://hidglobal.com)





### A Solid Foundation

Today's access control systems enable the use of smart cards, mobile devices or both within a PACS and IT security infrastructure, as part of an open ecosystem of interoperable products and services including card credentials, readers and a backend infrastructure to issue and revoke credentials.

Choosing an open technology platform is critical in order to support any piece of access control data for both current and future requirements, and to turn any smart device (cards, phones, key fobs, wristbands, watches, etc) into a trusted credential that can securely exchange identity information with readers, locks, printers and other access points. For the optimum combination of security and user convenience, the system should use contactless high frequency smart card technology that features mutual authentication and cryptographic protection mechanisms with secret keys. Also important is a secure messaging protocol that is delivered on a trust-based communication platform within a secure ecosystem of interoperable products. Another essential for interoperability is a generic, universal card edge, also known as the card command interface. This ensures that solutions will work with a broad ecosystem of products within a trusted boundary. With these capabilities, organizations can ensure the highest level of security, convenience, and flexibility, along with the adaptability to meet future requirements.

The bottom line: organizations need dynamic solutions that are adaptable to their changing needs and industry

best practices. Legacy security solutions simply can't deliver adequate security or new capabilities over time, because they often use proprietary, static technology that makes them easy targets for attack, and precludes their evolution beyond current abilities and security levels. In contrast, the latest open and adaptable platforms deliver flexibility and interoperability, they leverage important industry communication and connectivity standards, and they aren't anchored to obsolete software, devices, protocols and products. They also provide a single, media-independent and mobile-ready solution for all applications and environments, and they minimize migration disruption to day-to-day workflow through the use of multi-technology smart cards, readers and encoders.

ID card personalization is also important. Today's credentials can include elements that enable more trustworthy visual authentication while helping deter tampering and forgery. These visual elements may include higher-resolution images and holographic card overlaminates, as well as permanent laser-engraved personalization attributes that are difficult, if not impossible, to forge or alter. Ease of personalization must also be considered, and today's inline smart card personalization processes reduce this to a single step, enabling users to submit a card into a desktop printer equipped with an internal smart card encoder that personalizes the card inside and out. Today's ID card printers also support multiple types of electronic personalization, across many card types to simplify migration to new technology and new encoding options as security requirements increase.

### Moving to Mobile

With the latest access control platforms, smartphones can receive digital cards and keys and "present" them to readers. The same handsets also can generate One Time Password (OTP) tokens for securely logging on to another mobile device or desktop computers for accessing the network or cloud- and web-based applications.

Support for open standards is particularly important for mobile access control. For instance, systems that use phones to open doors and parking gates will likely need to accommodate multiple short-range communications technologies used by today's commercially available devices. While Near Field Communications (NFC) was initially thought to be the primary short-range communication technology for mobile access control, the industry is also deploying solutions that use Bluetooth Smart because of its wide availability and a simplified deployment and identity provisioning model. To accommodate a broad spectrum of mobile platforms including iOS, Android and Windows devices as well as the growing range of wearable devices, the access control platform will also likely need to support both communications technologies, as well as NFC Host Card Emulation (HCE) technology (which simplifies deployment as compared to NFC, but is not currently supported on Apple devices).

Another advantage of Bluetooth Smart is its longer reach, which means a smartphone wouldn't necessarily have to be close enough to be tapped to a reader in order to open a door, as with NFC technology. A big opportunity here is to incorporate gesture technology into a Bluetooth-based smartphone



solution, so that the phone can simply be rotated or “twisted” as the user walks up to a mobile-enabled reader. Gesture technology will deliver a new way to open doors and parking gates, while laying the foundation for a wide range of additional future applications.

Identity provisioning is the final piece of the mobile access control system. The task is simplified using today’s comprehensive, automated management portals for issuing and revoking mobile IDs.

A cloud-based identity provisioning model eliminates the risk of credential copying while making it easier to issue temporary credentials, cancel lost or stolen credentials, and monitor and modify security parameters when required. The system manages the seamless and secure over-the-air provisioning of encrypted credentials so that smart mobile devices can receive digital keys and present them to interoperable, mobile-enabled readers to perform many common tasks. All identity provisioning and authentication transactions are secured independently of the communications layer between reader and device, to protect against sniffing and replay. Additionally, the encrypted credential can only be decrypted by the access control reader, and each transaction is unique to ensure privacy.

### **Adding Secure Identity Applications**

Today’s access control systems also support the ability to combine multiple applications on a single card or smartphone. This eliminates the need for employees to carry separate cards or devices for applications including opening doors, using time-and-attendance and secure-print-management systems, and making cashless vending purchases. Other applications that can be added include biometrics, which is particularly effective on smartphones. Storing fingerprint, iris and other biometric templates on a smartphone will simplify system start-up, reduce installation costs by eliminating the redundant wiring requirements for traditional biometric template management on plastic cards, and speed authentication since the access control system can be continuously reading the biometrics data as users approach the door.

Combining applications on a single card or smartphone delivers a significantly improved user experience while maximizing access control investments beyond simply opening doors. Consider the modern healthcare institution, with its diverse community spanning patients,

staff and affiliated doctors, students, contractors, visitors and volunteers. Today, ID cards or phones can be used not only for access to the main door, emergency room and pharmacy, but also for specialized requirements such as vaccination compliance tracking and infant protection systems - all with a single convenient and cost-effective solution. Hospitals also can integrate visitor management into their access control system, replacing manual logs with a solution that enables visitors to be screened, badged and tracked. Solutions also support features such as real-time patient feeds using Health Level 7 (HL7) integration so that the system has all patient status and room information, so no visitor is sent to the wrong location, or to see a patient that has already been discharged. Today’s visitor management systems also support integration with access control systems for the most efficient badging.

In addition to physical access control applications, organizations also can seamlessly add multi-factor authentication, also known as strong authentication, for accessing data resources. Consider the benefits for the healthcare facility that was mentioned earlier. An affiliated doctor might typically carry as many as 20 OTP tokens in order to access networks and cloud- and web-based applications associated with multiple hospitals. Now, it is possible for the doctor to carry a single smart card containing a software One Time Password (OTP) token, which can simply be tapped to a personal tablet or laptop for authenticating to VPNs, wireless networks, cloud- and web-based applications and single sign-on (SSO) clients. Bluetooth Smart is expected to provide the connectivity for this capability on smart cards. In the future, this same “tap in” authentication capability can be delivered on a smartphone carrying software that generates OTPs on the device. No password entry is required, or separate card readers, or additional devices to issue and manage. As this tap-in authentication capability moves to smartphones, a combination of Bluetooth Smart and NFC Host Card Emulation (HCE) connectivity technologies may also be used here, as well.

As new physical and logical access control applications are added to an organizations cards and phones, the administration of these applications can all be centralized into one efficient and cost-effective system. The result is a fully interoperable, multi-layered security

solution across company networks, systems and facilities. This convergence of access control applications will yield important benefits, today and in the future.

### **Benefitting from Convergence**

Provisioning various IT and PACS credentials to a single smart card or smartphone, using one set of processes, improves convenience and can greatly enhance security and reduce ongoing operational costs. It also centralizes identity and access management, consolidates tasks and enables organizations to quickly and effectively use strong authentication throughout their infrastructure to protect access to all key physical and IT resources.

Organizations are increasingly adopting this new model, in which multiple access control use cases and identities can be supported on a single card or smartphone, thus eliminating the need to remember passwords, or carry multiple cards. This capability will start with smart cards and will then move to smartphones and other smart mobile devices and wearables, and will create a seamless user experience when securing doors, data and the cloud, while also improving how organizations create, manage and use identities on both smart cards and smartphones for network and physical access.

Beyond convenience, the convergence of credentials onto a single smart card or other smart mobile device can greatly improve security and reduce ongoing operational costs. And because there is a single process for provisioning and enrolling both IT and PACS identities, it becomes possible to apply a unified set of workflows to a single set of managed identities for organizational convergence. This also centralizes identity and access management, consolidates tasks and enables organizations to quickly and effectively use strong authentication throughout their infrastructure to protect access to all key physical and IT resources.

The latest secure identity technologies enable organizations to meet difficult security challenges while enhancing the end user experience, using smart cards and other smart devices in a growing ecosystem of interoperable products and applications. Today’s cards and phones can replace all previous mechanical keys, physical access cards and dedicated OTP logical access authentication hardware, as part of an extremely flexible, centralized access and identity management system that can adapt to evolving threats and requirements, and deliver increasing value over time.

# Biometrics Conference

## trustworthiness critical to broad acceptance of biometric technology

The Biometrics Institute Asia-Pacific Conference was held in late May at Sydney's Dockside conference venue with the theme 'Identity, Security & Trust – Creating a seamless customer experience in the physical and digital world'. Indeed, trust and the customer experience became dominant themes as speakers started taking their turns at the lectern.

Keynote speakers included Australia's Immigration Minister, Peter Dutton; Michael O'Connell, Director, Operational Police Support Directorate, Interpol; and Clarence Yeo, Commissioner, Immigration & Checkpoints Authority, Singapore. Joining them were a range of expert

speakers, including Mandy Smith, Head of Agency Services & RealMe, Kiwibank, and Arron Baker of Immigration New Zealand.

In his keynote address, Minister Dutton suggested that wider adoption of biometric technology can reduce identity crime, which in Australia is estimated to affect around one million people and cost \$1.6 billion annually. "To put it in perspective, identity crime is more common than assault, robbery, break-ins and motor vehicle theft.

It also holds grave danger for us as a nation – as terrorists and organised crime groups adapt and adopt increasingly sophisticated counterfeit techniques

to produce false identity papers and credentials to evade detection at borders or law enforcement or national security agencies."

### Security important, as is client experience

At airports, although biometrics tends to be focused on securing borders against a high risk, non-bona fide travelling minority, speakers suggested that its utility will eventually be most keenly felt in helping to manage the ever growing numbers of low-risk passengers move briskly through border points.

According to Ms Hinds, Director, Law Enforcement Policy at the Australia's Immigration Department, "biometrics is crucial for handling the growing movement throughput."

And Aussie travellers seem to be increasingly okay with this application of biometrics. According to a Unisys Security Index survey, 71% of Australians support the use of biometrics as an ID check for frequent travellers deemed to be a low security risk. Interestingly, the survey also revealed that in the wake of the Flight MH370 disappearance 75% of Australians would support the use of biometrics to confirm passenger identity when boarding a flight.

Ms Hinds noted that although privacy is a "limited commodity" in the border context, there nevertheless is a need to ensure that biometrics collection adheres to principles of proportionality and are fit for purpose. "For the overwhelming



*ePassport gates: the increasingly familiar new face of airport border control. Image courtesy Home Office (UK)*





*The action at the Sydney Biometrics Institute Conference*

majority of travellers, the collection of just one biometric – a facial image – is necessary.”

Interestingly, surveys indicate that public acceptance of biometric collection – and particularly the taking of fingerprints – tends to be highest among younger respondents. Older generations perhaps associate fingerprinting with criminality given that the practice has traditionally been depicted in the media as part of formal arrest and incarceration processes. For youth, providing a fingerprint is what one does to access their smart phone.

A key aspect of biometrics’ power is its convenience. With just one facial image

capture or one fingerprint scan, a person’s identity may be known, stored and used for any number of potentially malevolent purposes. As the conference’s discussion session on ‘biometrics and privacy’ identified, “with convenience comes temptation”, and the biometrics industry is struggling with how to handle this.

### **A Trust Mark for responsible use**

The Biometrics Institute recently released the results of its 2015 Industry Survey, which, according to the institute’s Chief Executive Isabelle Moeller, “confirm that the current and significant issues around Privacy and Data protection and the need to build consumer trust in biometrics is at a critical stage in the adoption of biometrics.”

To this end, the institute has been working on the development of an industry Trust Mark, with the aim of giving consumers confidence in the responsible use of identity products and services. “Creating consumer trust in why their biometric information is being collected and how it is handled, stored and potentially deleted is essential for the success of this industry.”

The institute has been consulting with its members and key stakeholders on privacy and the Trust Mark proposal. A feasibility study for the proposal has been approved by its Board of Directors,

The Biometrics Institute was itself established to promote the responsible use of biometrics technologies, and it promotes itself as the independent and impartial international forum for biometrics users and other interested parties. With currently have over 185 member organisations including government agencies, financial institutions, health service providers and vendors of biometric products and services, its membership has been growing as quickly as the technology is evolving.

An institute Member Meeting is scheduled to take place in Wellington on Thursday, 27 November 2014, and it already boasts an impressive line-up of speakers from the institute, the Australian Department of Immigration and Border Protection, NEC New Zealand and Datacom New Zealand.

**Details via the Biometric Institute website [www.biometricsinstitute.org](http://www.biometricsinstitute.org)**

## **Government and banks not trusted by Kiwis to protect their data**

A recently released study by Unisys Corporation has found that New Zealanders are deeply untrusting of telcos, government agencies and banks when it comes to protecting their personal data. Kiwis believe that these organisations are more likely than many other types to suffer an accidental or malicious breach of their personal data over the coming 12 months.

The Unisys Security Insights survey asked consumers in a dozen countries about the likelihood that their personal data held by seven types of organisations (airlines, banking/finance, government, healthcare, retail, telecom, and utilities) would be accessed by an unauthorised person, accidentally or deliberately, within the next year.

As part of the study, 503 adults in New Zealand were surveyed by Newspoll during April 2015. Of those surveyed, 53% expected a breach of their personal data held by a telco within 12 months, 51% expected a breach by government and 50% by their bank.

By comparison, only 35% believed that their data held by an airline would be the subject of a breach.

### **% of New Zealanders expecting a data breach in the next 12 months by industry**

<b>Spark</b>	<b>53%</b>
<b>Government</b>	<b>51%</b>
<b>Banking &amp; Finance</b>	<b>50%</b>
<b>Retailers</b>	<b>45%</b>
<b>Healthcare</b>	<b>45%</b>
<b>Utilities</b>	<b>42%</b>
<b>Airlines</b>	<b>35%</b>

“Consumer trust must be earned,” said Mr Steve Griffin, Unisys New Zealand’s country manager. “To build public confidence, an organisation needs to not only take preventative measures, but also communicate to their target customers that they have taken those measures. Such

an investment can offer a competitive advantage between brands within a category.”

“Many Kiwis have experienced a data breach or have seen media reports of breaches by telcos, government and banks, so they expect data breaches in those organisations. However, telcos and government would do well to learn from the way banks quickly communicate breaches to their customers to minimise the impact and rebuild confidence,” Mr Griffin continued.

That trust needs to be earned is an important message. Research indicates that consumers will look to change providers if they are unable to trust them to protect their personal information.

“Previous Unisys research revealed data breaches impact a consumer’s willingness to deal with an organisation,” explained Mr Griffin. “The majority of New Zealanders surveyed in 2011 said that they would stop dealing with an organisation if their data was breached. This highlights that public confidence in an organisation’s ability to protect data needs to be a business priority, not a mere IT issue.”



*Telcos and banks at the top end of town not trusted when it comes to data [Queen Street, by Ed Kruger]*

# 2015's most and least reliable countries to do business in

For New Zealand companies sourcing international suppliers, opening overseas offices and conducting transactions across borders, knowledge of the risks they face in the locations they do business, is of critical importance. While e-commerce has brought the world to the fingertips of local entrepreneurs, just how appraised are they of the stability of the business environments they're connecting with?

The 2015 FM Global Resilience Index (GRI), a ranking of 130 countries by insurer and loss prevention giant FM Global, provides country-by-country insights into this risk. The GRI ranks the resilience of countries to supply chain disruption so that managers can evaluate and manage unknown risks in the countries their business depends upon.

Managers might use insights from the GRI, for example, to assist in: informing strategies for selecting suppliers based on the supply chain risk/resilience of the countries in which they are located; locating facilities and evaluating the resilience of the countries hosting existing facilities; and assessing the supply chain resilience of countries where customers' facilities are based.

FM Global's methodology groups nine key drivers of supply chain risk into three categories: economic, risk quality and supply chain factors.

The drivers include:

1. GDP per capita
2. Political risk including terrorism
3. Oil intensity (the possibility a country will experience an oil shortage)
4. Exposure to natural hazards
5. Quality of natural hazard risk management (a country's disaster preparedness)
6. Quality of fire risk management
7. Control of corruption
8. Quality of infrastructure
9. Quality of local supplies

The GRI uses a number of respected sources to inform its assessments. The International Monetary Fund, U.S. Energy Information Administration and the World Bank's Worldwide Governance Indicators provide the data under the 'economic' heading. The World Economic Forum's Global Competitiveness Report



*Risk of natural disasters pulls a country's ranking down: flooding in Venice, Louisiana, after Hurricane Katrina, courtesy of the U.S. Geological Survey*

is the source of the data on infrastructure and local supply chain quality.

The data on risks and natural hazards, on the other hand, comes from an algorithm that FM Global developed to calculate risk at the more than 100,000 commercial properties it insures globally.

The field of country risk supports an entire industry of economists, political scientists and actuaries, informing anything from government policies to credit worthiness to insurance premiums. And one may well ask: do we need another ranking system on top of the myriad others that already exist?

The counter argument to this is that the GRI is probably more useful than most. It is, by design, a simplified, summary measure of resilience. The structure of the index enables managers to identify the sources of strength and vulnerability in a country's supply chain both at a bird's eye level and also in more detail across the nine drivers.



*Risky neighbourhoods: damage to the US Embassy in Beirut caused by a terrorist bomb attack*

It essentially gives managers a data-driven picture of how they can seek to improve their company's supply chain risk profile in a particular country... and what countries to avoid.

In this year's GRI, the top 25 countries include Ireland, Luxembourg, Germany, Finland, Belgium, Denmark, Sweden, the US, UK, New Zealand, Australia, Hong Kong, Singapore and Qatar, among others. Topping the list is Norway, followed by Switzerland and the Netherlands... no surprises there given northern Europe's perennial domination of such rankings.

According to the GRI, Venezuela tops the list of least reliable countries, with its unstable macroeconomic environment, high inflation and public debt, and malfunctioning markets. The country also scores poorly in terms of risk quality and supply chain factors.

The FM Global list fails to include around 60 countries, including many of the most unstable, disaster-prone countries in the world, such as Haiti, Syria, Yemen, Iraq and the Sudan – simply due to a lack of data. The big limitation of the index for our neighbourhood is that no Pacific island country made it to the list despite the many forms of risk that characterise the region.

The index is viewable interactively via the FM Global website [www.fmglobal.com](http://www.fmglobal.com).



# Locked in... no compromise no comparison!

**LOKTRONIC** proudly continues to be a leading supplier of New Zealand and international electronic locking hardware brands, including....

Abloy Electric Locks • Abloy, Effeft & IR Power Transfers • Effeft Electric Strikes • Egress Buttons • Flair Reed Switches • Haze Batteries • Imported Electromagnetic Locks • Legge Electric Mortice Locks, accessories and furniture • Lockwood Electric Mortice Locks, accessories and furniture • Loktronic, Cisa, Effeft and Asian Gate Locks • Loktronic and Trencab Key Switches • Loktronic Power Distribution Modules • Loktronic Power Supply Cabinets • Powerbox Power Supplies • Prastel Door Controllers • Roller Door Locks • Rosslare Keypads • Trimec Drop Bolts • Trimec Electric Strikes • Trimec V-Locks • Trojan Em Rex & Prox Rex Devices • Trojan Relays • STI Secure Housings for Keypads, Fire Alarms and Exit Devices • ViTech Anti-Interference Device • ViTech Battery Tester • ViTech Fire Brigade Alarms, Type X and Type Y • And many others.  
Plus, a wide range of spares and accessories.

Designed and made in New Zealand, our famous **LOKTRONIC** electromagnetic locks and Fire Door Holding electromagnets carry a solid

# 10 year\* guarantee

And, our **LOKTRONIC** outdoor electromagnetic locks continue to stand the test of time!

**25 years service and experience.**  
A future of secure growth and development.



\* **Sales** \* **Spares and accessories** \* **Repairs** \* **Advice**

**Loktronic**

Loktronic Limited Unit 7 19 Edwin Street Mt Eden Auckland  
P O Box 8329 Symonds Street Auckland 1150 New Zealand  
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK  
mail@loktronic.co.nz [www.loktronic.co.nz](http://www.loktronic.co.nz)



# SUBSCRIBE NOW!

Readers of NZ Security include those working directly and indirectly in the domestic and commercial security industry. From business owners and managers right through to suppliers, installers and front line staff.

Among our readers are IT security experts, surveillance professionals and loss prevention staff.

Our readers take their job seriously and make an active choice to be kept informed and up to date with the industry.

For only \$75.00 plus GST you can ensure that you receive a 1 year subscription (6 issues) by filling out the form below and posting to:

New Zealand Security Magazine  
27 West Crescent, Te Puru, 3575  
RD5, Thames, New Zealand

or email your contact and postal details to:  
[craig@newzealandsecurity.co.nz](mailto:craig@newzealandsecurity.co.nz)

Mr Mrs Ms \_\_\_\_\_

Surname \_\_\_\_\_

Title \_\_\_\_\_

Company \_\_\_\_\_

Postal Address \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Telephone \_\_\_\_\_

Email \_\_\_\_\_

Date \_\_\_\_\_

Signed \_\_\_\_\_

## NZSecurity

# Australia Round-up



## Citizenship law changes

In late June, the Australian government introduced amendments to the Australian Citizenship Act 2007 to parliament that would not only prevent dual nationals involved in terrorist acts overseas from returning to Australia, but also strip them of their Australian citizenship. The amendments will be voted on by parliament.

According to the government, of the around 120 Australians fighting with Islamic State (IS) overseas, about half hold dual citizenship. The government has cancelled 120 Australian passports in order to prevent people participating in conflicts in the Middle East.

Under the current Citizenship Act, dual citizens are automatically stripped of their Australian citizenship if they serve in the armed forces of a country at war with Australia. In the case of so-called 'foreign fighters', the concept of allegiance is not so straight forward, and the proposed changes have sparked fierce public and political debate.

The changes would widen the scope of section 35 of the Citizenship Act to automatically strip dual nationals



*Tony Abbot speaking at a citizenship ceremony on Australia Day 2015, image courtesy Nick-D*

of their Australian citizenship if they "engage in various kinds of conduct inconsistent with allegiance to Australia". Such widening has unsurprisingly raised questions over just what "conduct inconsistent with allegiance to Australia", might constitute.

## 2015 Security Exhibition & Conference

The 2015 Security Exhibition & Conference held 15-17 July has been described by ASIAL as "the most successful event in the show's 30 year history", with around 5,000 security industry professionals converging on Melbourne's Exhibition and Convention Centre for the spectacular.

This year's theme of 'Where to next? Future challenges and opportunities for security' was well reflected in the conference program, which included cyber security, corporate information and social media security among its topics. According to ASAIL, "speakers challenged the readiness of the Australian security industry for a host of threats, both physical and online."

The program also squeezed in a half-day executive briefing on crisis communications, presented by crisis management expert Bruce Blythe, Chair of Crisis Management International.

Mr Blythe, who has had direct involvement in a number of major crises, including Hurricane Katrina, the Oklahoma City bombing, 1993 World Trade Center bombing, workplace shootings, fires, earthquakes and reputation scandals, was just the man to shed light on an area that requires significantly more attention than what the industry tends to give it.



# Countering Violent Extremism Regional Summit

**Australia's Regional Summit to Counter Violent Extremism convened over 11-12 June 2015 in Sydney. Following on from the White House CVE Summit held in Washington DC in February, the Sydney summit brought together key stakeholders from government, civil society and industry across the region focused on building capacity to address the threat posed by violent extremist groups.**

According to the Commonwealth Attorney General's Department, the summit provided an important platform for participants to collaborate on the shared challenge posed by the dissemination of terrorist propaganda. "Participants recognised that the online environment has no borders and terrorist propaganda can reach everyone in the region online, a collective effort is required to counter this threat."

This summit is one of a number of regional events planned for 2015 to

build on work being done globally to implement the United Nations Security Council Resolution 2178 to prevent the "recruiting, organizing, transporting or equipping of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning of, or participation in terrorist acts."

Summit outcomes will inform future contributions to a leaders' event, which will be held in the margins of the UN General Assembly in September 2015.

Ministers and officials from 24 countries, the European Union and the United Nations, as well as representatives from civil society and the private sector met on the 12th for the ministerial component of the summit. In an Official Statement, delegates expressed approaches to CVE that departed significantly from the Australian Government's law enforcement and border security-centric approach.

The Communiqué acknowledged "that effective strategies to counter the threat of online radicalisation require governments to act beyond legislative and law enforcement measures to engage with the community in partnership with industry to promote positive messaging and counter misleading and harmful terrorist narratives."

It also emphasised that "effectively preventing the spread of violent extremism includes empowering those who are best placed to facilitate change, including youth, women, families, religious, cultural and education leaders and community groups."

Strategies, it stated, need to be holistic "from addressing the underlying conditions conducive to the growth and spread of violent extremism and building community resilience to radicalisation through education and support, to early intervention and rehabilitation programs, and implementing appropriate legal regimes and codes of conduct."

---

## Security in Government 2015 Conference

**The National Security Resilience Policy Division of the Australian Attorney-General's Department, will host the 27th Security in Government (SIG) Conference at the National Convention Centre in Canberra from 31 August to 2 September 2015.**

The conference theme is 'Security risk management—getting it right!', which will consider the evolution of security risk management, focusing on case studies, best practice and current and emerging strategies available for doing security risk management well.

An extensive trade exhibition attached to the conference will feature over ninety security-related service providers who work closely with both the government and private sector to provide solutions to protective security issues.

According to an Attorney General's Department overview, "the conference is targeted at senior executives responsible for managing security in agencies, officers from all levels of government who contribute to the development of security capability and response,

security practitioners from the public and private sectors who provide services to government and critical infrastructure providers," in the areas of physical, personnel and information security,



*Duncan Lewis AO, DSC, CSC, Australia's Director-General of Security. Image courtesy Department of Foreign Affairs and Trade website – [www.dfat.gov.au](http://www.dfat.gov.au)*

information and communications technology, and government policy."

Undergraduate and postgraduate students undertaking studies in security policy, capability development, incident response and policing, are also encouraged to attend.

The conference's varied line-up of speakers includes Duncan Lewis AO DSC CSC, head of the Australian Security Intelligence Organisation (ASIO), who will speak on Australia's current security and intelligence operating environment. Lewis is also a former Australian Ambassador to NATO, Secretary of the Department of Defence, and Major General and Commander Special Forces in the Australian Army.

Chris Moraitis PSM, Secretary of the Attorney-General's Department, is slated to talk on Managing personnel security risk. He, along with Paul Jones of the Australian Nuclear Science and Technology Organisation (ANSTO) who will discuss managing risks at a nuclear facility, are just a small selection of the speakers confirmed for the event.

## uniview 8 Channel Premium IP Kit



Featuring an 8 Channel NVR with built in PoE, 2TB HDD fitted, plug and play setup with no port forwarding or router configuration.

### Includes:

- 4 x 2MP Domes, IP66
- 23" Full HD Monitor
- 4GB USB flash drive
- 100m of Cat5 cable
- HDMI cable

**CRK** Professional Precision

Ph: 09 276 3271 • [www.crknz.co.nz](http://www.crknz.co.nz)

## uniview 4 Channel IP Kit



Perfect for home or business use.

The NVR has built in PoE and comes fitted with a 2TB HDD, featuring plug and play setup with no port forwarding or router configuration required.

The kit also includes four 2MP IP cameras with 30m IR and are IP66 rated for outdoor use.

**CRK** Professional Precision

Ph: 09 276 3271 • [www.crknz.co.nz](http://www.crknz.co.nz)

## uniview 32 Channel NVR



A 16-32 Channel NVR with 200Mbps total bandwidth available and 8 hard drive bays, comes with 3TB fitted.

The NVR is capable of 16 channels at 1080p or 32 channels at 720p and includes 2 Gigabit Ethernet adaptors.

Easy to setup by QR code for remote access, support for Windows, Android and iPhone.

No port forwarding or router configuration.

**CRK** Professional Precision

Ph: 09 276 3271 • [www.crknz.co.nz](http://www.crknz.co.nz)



**ITRON SECURITY & AUTOMATION**



## Loktronic for gate locks

Choose from a comprehensive range of 23 models of electric gate and outdoor locks for a wide range of applications.

6 models from the famous Loktronic stable, and 7 imported models with holding forces from 300kg, 550kg, up to 740kg; all locks complemented by accessories to facilitate fitting.

7 models of strikes by Trimec and eff-eff, Rim mounted locks from CISA, and a versatile range from Securatron and Interlock.

Gate locks from Loktronic – a wise choice.

**Loktronic**



Unit 7 19 Edwin Street Mt Eden Auckland  
P O Box 8329 Symonds Street Auckland 1150 New Zealand  
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK  
[www.loktronic.co.nz](http://www.loktronic.co.nz)

20756\_BP



## Key switches

**This versatile product range is produced with two functions**

Momentary contact (90°)

Turns 90° clockwise from vertical to turn on

Maintained contact (180°) locked on or locked off

Turns 90° clockwise from vertical to turn on

Turns 90° anticlockwise from vertical to turn off

SPDT switch 5amp rating

**Accessories are:** Key switch mounting bracket  
escutcheon for mounting bracket

**Suitable for:** Access control, air-conditioning,  
lifts, lighting.

Supplied random keyed. Can be master keyed.

Client's own key cylinder can be converted.

Front or rear fixing.

**Designed, tested and produced  
in New Zealand by Loktronic.**



**Loktronic**



Unit 7 19 Edwin Street Mt Eden Auckland  
P O Box 8329 Symonds Street Auckland 1150 New Zealand  
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK  
[www.loktronic.co.nz](http://www.loktronic.co.nz)

20681\_KS

## Loktronic Power distribution module



**The Power Distribution Module** allows the removal of power to a group of doors on a fire alarm activation whilst conforming to regulations. Provision for individual fused power supply to each door lock.

Red and black uncommitted terminals to facilitate distribution from power supply or battery, to load.

### Comprises

- Fire Drop Relay DPDT 12 VDC • 6 x 2 Amp FU 500
- Terminals with LED Indication • 2 x Red Terminals
- 2 x Black Terminals • 1 x DIN Rail
- All terminals are labelled.

**Designed, tested and  
produced in New Zealand.**



**Loktronic**



Loktronic Limited Unit 7 19 Edwin Street Mt Eden  
Auckland P O Box 8329 Symonds Street Auckland  
1150 New Zealand Ph 64 9 623 3919 Fax 64 9 623 3881  
0800 FOR LOK [www.loktronic.co.nz](http://www.loktronic.co.nz)

20239\_PDM





## Power supply cabinets

- Mounts for our 5 most popular models of power supplies; 6 key-hole anchor points for easier mounting
- Lift off hinged doors for added convenience
- Louvre ventilation on doors
- Roller ball reed switch provides anti-tamper to front and rear of cabinet
- 6 x 25mm knockouts, 2 each sides and bottom
- Medium cabinet holds 5 x 7 A/h batteries
- Large cabinet holds 14 x 7 A/h batteries
- Cam lock for security
- Front lip to retain batteries and for additional strength
- Removable shelf and removable back plate to facilitate easy bench mounting of equipment
- Lip return on door for greater rigidity
- Durable powder coated white finish
- Heavy gauge 1.2mm steel

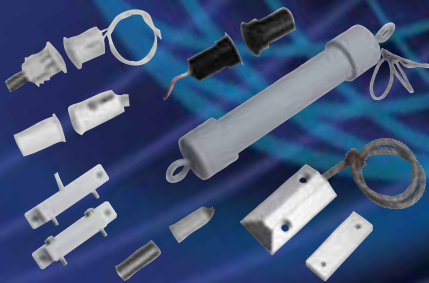
**Designed, tested and produced in New Zealand.**



**Loktronic**

Loktronic Limited Unit 7 19 Edwin Street Mt Eden  
Auckland P O Box 8329 Symonds Street Auckland  
1150 New Zealand Ph 64 9 623 3919 Fax 64 9 623 3881  
0800 FOR LOK www.loktronic.co.nz

20238\_PSC



## total reed switch solutions from Flair

**From closed loop, open loop to SPDT, we've got the lot.**

Talk to Loktronic now about our comprehensive range of Flair Reed Switches. Not only for "standard" use, but also for specialty applications, from taught-wire types to waterguards, from collared to stubbies, from overhead door with offset to floor contacts, from latchguard to sub-miniature, from push-fit to surface mount.

**Flair reeds from Loktronic: an unbeatable combination.**

**Loktronic**

Loktronic Limited Unit 7 19 Edwin Street Mt Eden  
Auckland P O Box 8329 Symonds Street Auckland  
1150 New Zealand Ph 64 9 623 3919 Fax 64 9 623 3881  
0800 FOR LOK www.loktronic.co.nz

20237\_FL



## Loktronic for power supplies

Source all your power supply requirements at Loktronic and choose from a range of over 20 ex stock options, with 100's more to select from.

Complete range of monitored security PSUs in 12 and 24 VDC from 2.5 A - 20 A. DIN rail units in 12 and 24 VDC from 10 - 100 watts. Plus, inline and Plug packs and DC/DC converters.

**Power supplies from Loktronic – a great deal.**

**Loktronic**

Unit 7 19 Edwin Street Mt Eden Auckland  
P O Box 8329 Symonds Street Auckland 1150 New Zealand  
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK  
www.loktronic.co.nz

20757\_BP



**Panasonic**



(09) 414 5101 OR 0800 ITRONICS

SALES@ITRON.CO.NZ

WWW.ITRON.NZ



### Wireless IP Surveillance

- Cost effective high performance wireless access points for outdoor use
- Stockists of AirMax, AirFiber, AirVision, UniFi & mFi series products
- ITPLUS are a Ubiquiti certified and trained partner

**Distributed by**



Ph: 09 950 4940 | E: info@itplus.co.nz  
www.itplus.co.nz



### Customized CCTV Kits

- We supply fully customized complete CCTV kits in form of Hybrid, Tribrid, IP, CVI etc
- Complete kits are a great way of reducing costs and getting the whole package from one place
- Receive FREE support\* including remote connection assistance

**Distributed by**



Ph: 09 950 4940 | E: info@itplus.co.nz  
www.itplus.co.nz



### Open Platform VMS

- Award winning best open platform VMS
- Advanced Built-in Video Analytics
- Micromodule crashproof software architecture
- Includes powerful features such as Modern GUI, Video Archive, Green Stream, Time Compressor, Interactive 3D Map, Autozoom etc.

**Distributed by**



Ph: 09 950 4940 | E: info@itplus.co.nz  
www.itplus.co.nz

# Proving “Competency” for Security Consultants

## The Current Situation

The Private Security Personnel and Private Investigators Act 2010 defined “security consultants” as: *a person who for valuable consideration, either by himself or herself or in partnership with any other person, carries on a business—*

- a) entering any premises that are not owned or occupied by himself or herself or his or her firm or any of his or her partners for the purpose of selling or attempting to sell any device of the kind referred to in paragraph (a) or (b) of section 6(1); or
- b) entering any premises that are not owned or occupied by himself or herself or his or her firm or any of his or her partners for the purpose of advising the owner or occupier of the premises on the desirability of having installed on the premises any, or any further, such device; or
- c) entering any premises that are not owned or occupied by himself or herself or his or her firm or any of his or her partners for the purpose of advising the owner or occupier of the premises on the desirability of having guarded the premises or any other property that may from time to time be on the premises or dispatched from the premises.

Following the introduction of Mandatory Training for the manpower sector (Crowd Controllers, Property Guards and Personal Guards) by Regulation in 2013; the Private Security Personnel Licensing Authority (PSPLA) began advising applicants in other categories that they were also required to prove “competence”. The PSPLA website explains this as:

*“The following permit classes Private Investigator, Security Technician or Security Consultant are of a specialised nature and you must provide suitable evidence that you are:*

- competent or trained
- receiving appropriate training

*The evidence of competency for Private Investigator, Security Technician or Security Consultant can be:*

- letter from previous/current employer as to work history
- letter from previous/current employer that you are an apprentice
- qualifications gained
- member of the NZ Institute of Professional Investigators (NZIPI)”

The last bullet point is a little confusing as membership of NZIPI is not really relevant to the Security Technician or Security Consultant classes.

The PSPLA’s requirement for the proof of competence is currently impacting on new applicants, and the “solutions” suggested will not work for many. If, for example, your company hires a highly skilled sales person from another sector, what evidence could they provide to enable them to work as a “consultant”? This issue will become a bigger problem in 2016 when it will also impact on thousands of COA holders who will have to provide evidence of competence before their COA’s are renewed.

## NZSA Provides the Solution

There is no clear pathway to enter our industry for a career as a security consultant. This is partly because the Act’s definition and partly because there is no “gateway” training linked to the CoA process. With the manpower categories the PSPLA determined that an initial block of three unit standards from the National Certificate in Security (Level 2) would be sufficient as the mandatory training requirements for the issuing of a Certificate of Approval. They have made no such determination for the other sectors.

We have developed a short course package of training that will provide proof of “competence” for Security Consultants in the same way as the Mandatory training package does for manpower training. Successful

completion of this training will result in an NZSA Certificate of Competence. The programme will comprise 3 one day seminars, with some pre-reading and assignments to be completed in the learners own time.

## Module One: Introduction to Risk Management and Security Surveys

This covers the basic concepts of Risk, Threat, Vulnerability, and Likelihood, and Consequence. Learners will be trained in the use of Risk Assessment and Security Survey templates. Assessment is by way of a practical exercise completed after the seminar.

## Module Two: Introduction to the Operational Security Requirements

This covers the process of selecting appropriate security services and equipment to meet client need. This process would be based on the Operational Security Requirement process that is already referenced in NZSA’s Codes of Practice. Assessment is by way of a practical exercise completed after the seminar.

## Module Three: Compliance Requirements

This covers the requirements of Legislation, Regulation and industry best practice (PSPLA, OH&S, Privacy, NZSA Codes of Practice). Assessment would be by way of a written test included in the seminar.

The PSPLA has responded in a very positive way to our solutions, and we will be offering the courses from August this year.

**To book or find out more information please contact NZSA on 09 4860441 or via email to [nzsa@security.org.nz](mailto:nzsa@security.org.nz).**



# fire door holding electromagnets



Standard, floor mounted, wall to door distance 114mm



A)

B)

C)



## FDH40S

### unbreakable universal mounting

- Low power consumption - low operating temperature
- One product suits floor and wall mounting
- Universal armature - offsets to 55° to suit doors opening past 90° • Wall mount extensions available
- 12 VDC models and 24 VDC models • Push off button with no residual magnetism • Oversize armature for easy alignment • Emergency release button
- Electroless nickel plated armature and electromagnet
- Stainless fastenings • Full local support and back up

### 10 YEAR GUARANTEE\*

Designed, tested and produced in New Zealand to AS4178

A) Wall mounted, 126mm extn. tube (overall 202mm)

B) Wall mounted, 156mm extn. tube (overall 232mm)

C) Wall mounted, 355mm extn. tube (overall 431mm)



Flush mounted, wall to door distance from 50mm



Surface mounted, wall to door distance 70mm

## FDH40SS

### stainless steel surface and flush mounting

This device enhances an outstanding range of unbreakable products which conveniently hold open fire doors. When a smoke/fire alarm is activated the magnet instantly releases the door to the closed position to prevent the spread of smoke and fire. These units feature satin finished stainless steel covers for optimum aesthetic appeal and durability. To allow maximum flexibility the electromagnet is pre-assembled onto a plated steel mounting plate. The installer can utilise one device for surface mounting or for flush mounting.

### 10 YEAR GUARANTEE\*

For expert advice and assistance with **your** security locking needs, trust in Loktronic, call us on **0800 367 565**



**BOTH**  
options are  
packaged  
in the  
same box



# KCS TraceME

2G 3G 4G LBS

LoRa™ BLE M2M

Iridium Sensor

Bluetooth™

SMS



iBeacon™

Glomass GPRS

RF GPS



Internet of Things



## LoRa™ Internet of Things

KCS has extended their successful TraceME product line with an advanced module, targeted for worldwide mobility in the Internet of Things era. The latest development of the TraceME GPS/GPRS Track and Trace module will combine the RF location based positioning solution with the LoRa™ technology. This combination offers 'smart objects' being even smarter, since LoRa™ enables long range, battery friendly communication in a wide variety of (M2M) applications. Supporting GPRS/SMS and optional 3G, Wi-Fi, Bluetooth LE, ANT/ANT+ and iBeacon™ provides easy integration with existing wireless networks and mobile apps. Other variants in the high/mid-range and budget-line will follow soon.

## ANTI-THEFT module based on RF

KCS TraceME product line offers an intelligent location based positioning solution for indoor and anti-theft applications. The solution is based on RF with an intelligent algorithm of measuring the propagation time of transmitted (proprietary protocol) signals. Unique features are: minimum size (46x21x6.5mm), weight (7 grams for fully equipped PCB) and a standby battery lifespan of more than 10 years. 'Listen before talk' algorithm makes it practically impossible to locate the module, which secures the valuable vehicle or asset. Supporting GPRS/SMS and optional 3G, Wi-Fi, Bluetooth LE, ANT/ANT+ and iBeacon provide easy integration with existing wireless networks and mobile apps.

[www.Trace.ME](http://www.Trace.ME)

All trademarks mentioned herein belong to their respective owners.