

NZSecurity

Swings & Carousels

In Airport and Border Security

Off the Rails

Calls for Police on Auckland Trains Continue

FREAK Show

How the Politics of Data Encryption keeps Internet Transactions Vulnerable to Attack

www.NewZealandSecurity.co.nz/free-magazine

download a free copy of the latest nzSecurity Magazine to you ipad, notebook or smart phone.

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



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

Found at 103 metres distance!

Ideal solution for
commerce and industry



Multifocal sensor technology

innovative - unique - cost-effective

In contrast to single sensor cameras, the multifocal sensor technology provides a guaranteed constant resolution of at least 125pix/m. This makes it possible to monitor large areas from a distance from a single location, achieving this in real time with a uniform image resolution, high dynamic and constant focal depth.



Integration into common management systems.

Sign up for a free on-site
Panomera demo.

To register email
panomera@crknz.co.nz

 **Dallmeier**

Phone: 09 276 3271
Email: cctv@crknz.co.nz • Web: www.crknz.co.nz

CRK
Professional Precision

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

RD5

Thames

New Zealand

Email & Web

craig@newzealandsecurity.co.nz

www.NewZealandSecurity.co.nz

Upcoming Issue

June - July 2015

Wholesalers and Manufacturers

Perimeter Protection,

Alarms and the use of fibre optics

August - September 2015

Banking, Insurance, Finance,

Loss Prevention, Industry Training

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.

CONTENTS

- 6 Gallagher helps Businesses Reduce their Carbon Footprint
- 8 Swings and Carousels in Airport and Border Security
- 12 Interview: Bill Sillery, Global Project Coordinator for TT Services
- 14 Panomera® from Dallmeier ensures enhanced Security at Naples Airport
- 16 Countering Violent Extremism for the Common Good
- 18 Opening Doors and Gates with Smartphones, Bluetooth Smart and Gesture Technology
- 20 Product Integrity and Personal Integrity go Hand In Hand
- 21 New Zealand Security Conference and Exhibition
- 24 Hills: The Future is Happening Now
- 26 Off the Rails: Calls for Police on Auckland Trains Continue
- 28 Trends in Incident Management for Public Transport Operators
- 31 Maintaining Motivation
- 32 Identity Theft Support Service iDcare Launches in New Zealand
- 34 Advanced Crime Analytics Connect the Dots
- 36 International Bodyguard Training Standards now available in NZ
- 37 Recognising Innovative Product Excellence in the NZ Security Industry
- 38 FREAK Show: How the Politics of Data Encryption keeps Internet Transactions Vulnerable to Attack
- 41 World Leading Security Research moves offshore because of TICSAs
- 42 It's Academic: Why the debate between Security and Privacy in NZ is important yet irrelevant
- 46 National Home Safety Service: Securing Homes against the scourge of Domestic Violence

NewZealandSecurity.co.nz

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

*Standard terms & conditions of sale apply

Loktronic

0800 367 565

www.loktronic.co.nz

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



One day. 124 incidents.

124 right decisions.



When you're responsible for the safety and security of an urban public transport system involving thousands of buses, the amount of incidents to detect, evaluate and act on every day is staggering. That's why we've made sure our network video solutions can handle it all. So you can make the right decision. For every incident.

Get the details at www.axis.com/buses
or send an email to contact-sap@axis.com

Distributed by:



Gallagher helps businesses reduce their carbon footprint

Now, more than ever before, businesses are sharpening the focus on their energy consumption as we all become more conscious of the carbon footprint we leave in our wake. In addition to providing total site security and protecting businesses from crime – particularly that committed by the competent insider – security systems innovator, Gallagher, has opened the door for a number of businesses to operate smarter, more energy efficient environments which result in distinct cost savings.

Through automated and integrated systems that are driven by Gallagher's Command Centre central management platform, businesses are able to monitor and report on a range of site operations, that together, contribute to an organisations overall awareness, and commitment to reducing energy use.

Control of systems can be based on occupancy. For example, when an area is unoccupied, Command Centre notifies the Building Management System (BMS) which can turn off building services such as lighting, heating, and air conditioning -

ensuring that valuable energy is not being wasted. System integrations also enable resources, such as meeting rooms, to be booked via an online schedule. Building services are then activated in real-time in line with the schedule.

Integrating business systems can have a substantial impact on the bottom line and as yet, there is unlimited potential for Command Centre's ability to reduce energy consumption.

A major state university in Australia, through integrating their sports ground lighting in Command Centre, saved over AUD 60,000 in power costs within the first year. An international private school in New Zealand utilises Command Centre to manage their indoor pool, where the system has been configured to monitor and control the temperature, humidity, chlorine level, and more.

Energy savings have also been observed at an internationally recognised financial institution where their energy star rating increased due to the powerful monitoring, and reporting function of Command Centre.

For more information on Gallagher systems and integrations:

📄 security.gallagher.co

✉ info@security.gallagher.co

☎ 07 838 9800



It's new. It's fresh. It's here.

Introducing Command Centre v7.30,
Gallagher's next generation security
management platform.



- Extend security management with mobile application
- Produce dynamic reports identifying security and business trends
- Improve efficiency through advanced system administration

security.gallagher.co/latest-releases

Swings and carousels in airport and border security

Managing borders is no easy task. From Queensland fruit flies to illegal workers posing as tourists, international criminals to terrorist fighters carrying photo-substituted passports, allowing the good folk in and keeping the bad folk out, is a 'round-the-clock' challenge for border authorities.

On the one hand, people demand watertight borders, yet on the other they want hassle-free – and preferably visa-free – travel and immigration clearance procedures. On the one hand, we insist that authorities conduct the necessary checks to prevent criminals from breaching our borders, yet on the other we abhor the intrusion into privacy that comes with bag checks, laptop data scrutiny and immigration interviews.

In the middle of this are immigration, customs and quarantine authorities and airport and airline staff. With worldwide airport passenger numbers in 2013 totalled 6.3 billion, and volumes set to double in the next 20 years, border security threats are not going away.

Just what are border authorities around the world doing to meet the challenge of keeping borders secure while handling the massive throughput? We take a look.

Biometrics at the border – ePassports and fingerprints

More than any other recent development in border security, biometrics personifies the tug o' war between airport convenience and visa application hassle, passport security and passport holder privacy.

Biometric information can include photographs, finger prints, iris scans and even voice recognition. New Zealand's



Passports bearing the ePassport symbol

Immigration Act allows for the collection of photographs of a person's head or shoulders, fingerprints, and iris scans from foreign nationals, for immediate use and storage for future use. It also allows biometrics to be collected from New Zealand citizens on arrival in NZ. Where the person's identity and citizenship is confirmed, the information is disposed of and is not stored.

A biometric passport, also known as an ePassport, contains biometric information that can be used to authenticate the identity of its holder. In accordance with Civil Aviation Organization (ICAO) specifications, the passport uses contactless smart card technology, including a microprocessor chip and antenna embedded in its front or back cover or centre page.

The critical information of the passport and its holder is printed on the data (photo) page of the passport and stored in the chip. Public Key Infrastructure (PKI) is used to authenticate the data stored electronically in the chip making it difficult to forge. Counterfeits are prohibitively expensive, and gone are the days when one might get away with a good photo substitution under the data page lamina.

The potential 'frontline' use of biometrics in countering terrorism was recently revealed in Australia. New biometric collection measures enabled by powerful legislation can now identify returning terrorist fighters – including any child suspected of involvement in terrorism – at the border by crosschecking their fingerprints at

**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



absolutely™



An Emirates A380 rests on Auckland Airport's tarmac

airports against watch list data from international agencies.

But privacy advocates have been scathing in their criticism of ePassports, the vulnerability of their wireless RFID technology to interception, and the possibility of data being shared between governments and eventually falling into the wrong hands.

Immigration New Zealand (INZ) already shares biometric and other information relating to foreign nationals with Australia, the US, UK and Canada under the Five Country Conference (FCC) Data Sharing Protocol. This arrangement has been in place since 2011 and has been highly successful in managing immigration risk. But sharing arrangements will likely expand beyond the FCC within a matter of years... if not by INZ then by any one of its FCC partners.

The other big sore point for travellers is the hassle of having to endure the collection of their biometric data – usually fingerprints and photographs – when they apply for a visa to travel to any one of the growing list of countries that require it. Even though the visa application process for many destinations is at least part online, enrolling one's biometrics as part of the application process necessitates in-person finger printing at an often inconveniently located enrolment centre.

Better security and a faster breeze through the airport?

But there is an upside to all this. If you've flown across the ditch in recent times, you'd know that SmartGate

ePassport readers have been installed at arrivals in Australian airports and departures in New Zealand airports. SmartGate performs the customs and immigration checks normally made by a Customs Officer, and they're making immigration clearance for ePassport holders of several nationalities much quicker.

Similar systems are popping up at airports around the world. At the end of 2014, a total of 74 e-gates were in place at the German airports of Frankfurt, Munich, Dusseldorf and Hamburg airports, and will almost double by the end of the year to 140. It is claimed that this facial recognition-based system reduces the processing time for each passenger to less than 18 seconds.

US Customs and Border Protection's (CBP) Global Entry program takes this a big step further. This program allows expedited clearance for pre-approved, low-risk travellers upon arrival in the US by using automated kiosks located at select airports. Pre-approval entails background checking and an in-person interview.

Program participants proceed to Global Entry kiosks, present their machine-readable passport or US permanent resident card, place their fingertips on a scanner for fingerprint verification, and complete a customs declaration. The kiosk issues the traveller a transaction receipt and directs the traveler to baggage claim and the exit.

Similar technology allowing low-risk travellers to breeze through screening from "kerb to aircraft door"

is being slated for Melbourne Airport. It will become the fourth airport, after Heathrow, Amsterdam's Schiphol, and Doha's Hamad, to test the new Smart Security program.

A trial with Qantas to start at the airport this year will see people register as 'known travellers' after being cleared via background checks by security agencies. Avoiding the normal airport screening, advanced facial biometric technology will link them to their travel documents and communicate a risk assessment to the boarding gate.

These passengers will potentially walk through streamlined checkpoints without having to remove shoes and hand in laptops and mobile phones. Devices would scan for banned items and prohibited amounts of liquid.

Pre-vetting, online checking and remote baggage drop

Other innovations already arrived or due to land at your airport sometime soon include one of the many self-service bag drops being trialed by airlines. These include solutions that can be installed either in the terminal building or offsite, allowing passengers to identify themselves using their boarding pass and then print out their bag tags. If installed in a hotel lobby or airport car park, these units can make navigating luggage trolleys into a terminal a thing of the past.

It will also soon be likely for passengers to track their checked-in bags via mobile phone apps in much the same way as one might track a courier parcel. The technology is already here, and it probably won't be too long before airlines and airports will start rolling it out to their travelling customers.

Ultimately, there exists strong evidence of a trend of cooperation towards a more seamless coordination of security, baggage and immigration clearance processes at airports, well, major airports at least. Developments will largely focus on the streamlining of such processes for pre-vetted passengers deemed to be of 'low risk'.

Those with the wrong type of passport, a blemished immigration or criminal record, or some other attribute that doesn't satisfy a border authority's low-risk threshold, will likely find themselves on the wrong side of the biometrics revolution. High-risk 21st century jet setters may well have to continue to settle for a more 'traditional' 20th century destination airport welcome.

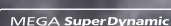
SEEING IS BELIEVING

Trust Panasonic rain-wash-coated PTZ Dome Cameras to ensure you have the best visibility possible, even when it's wet and wild. Delivering clearer images and long-term durability, our specially coated dome covers can provide up to 1080p HD images in the harshest New Zealand conditions.



WV-SW598 NETWORK CAMERA

- 1080p HD images up to 30 fps
- 360 degree endless Panning
- Advanced Auto Tracking
- Ambient Operating Temperature -50 °C ~ +55 °C



THE EFFECT OF RAIN-WASH COATING: LESS DIRT, CLEARER IMAGE

Droplet formation prevention

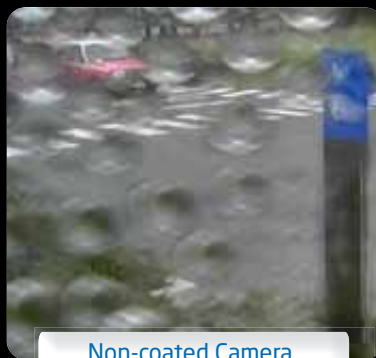
Visibility is maintained due to droplet prevention coating.

Advanced coating technology

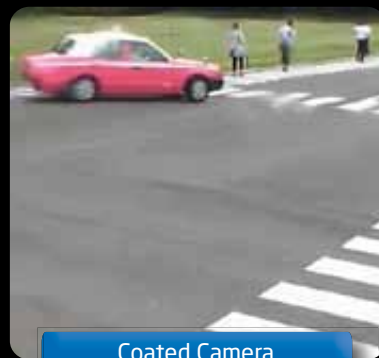
Long-term performance due to advanced coating technology.

Reduced Dirt

Dirt is easily washed off the dome cover by rain water due to self-cleaning design.



Non-coated Camera



Coated Camera

Developments in biometrics at the border

Biometric security for passports and visas is fast becoming a ubiquitous aspect of international travel. The collection of travellers' biometric data – including fingerprints and iris scans – is an increasingly unavoidable part of the process of travel – from applying for visas to passing through immigration clearance at international airports.

For expert insight into the fast-developing world of biometrics, NZ Security Magazine had a chat with Bill Sillery, Global Project Coordinator for TT Services, a leading provider of integrated visa processing solutions for governments and diplomatic missions. TT Services is currently a service delivery partner of Immigration New Zealand (INZ), and operates visa application centres on behalf of INZ in 15 countries across the Pacific, Asia, Europe and North America.

Prior to joining TT Services, Bill was senior advisor to Citizenship and Immigration Canada for its Temporary Residents Biometric Project. Before this, he was solution architect for the UK visa biometric enrolment system and UK National Identity Cards scheme, and was also a member of the ISO SC37 working group on biometric standards, part of an all-country biometrics rollout for the UK.



Bill Sillery, TT Services

NZSM: How does the collection of traveller biometric data enhance border security?

Bill: Biometric border controls using photographs have actually been in use since the First World War, and have always been unpopular. Lt. Commander Kenworthy, MP for the English constituency of Kingston-upon-Hull had this to say in Parliament back in 1922: “You have to get a passport, a photograph, and you have to pay your fees. We all know that photographs untouched are not flattering things on a passport. You have to stand in a queue among the ducks in St. James Park, and it is all an infernal nuisance...”

Nonetheless, the League of Nations agreed to implement passports in their more or less modern form rather than return to the pre-war days of passport free travel, and the era of biometric travel checks began. Almost 100 years later, the same check of the face in the passport continues to be the predominant means of admission at the border.

The days of post-9/11 travel have seen rapid change, as advances in technology have permitted a wider range of biometric tests to be performed, the most important of which is the ability to use fingerprints to rapidly search vast repositories for matches. This has been readily adopted by security minded governments so now it is relatively normal when applying for a visa to be expected to attend an application centre to give your fingerprints.

The early implementations of fingerprint checks by the US and UK amongst others proved very successful in identifying persons of interest, ranging from those previously deported travelling under false identities, to individuals using multiple identities to access state benefits. They were very popular in parliament they worked and made for good press releases. As such they have caught on and many other governments have followed or are following suit.

NZSM: How has it made a difference in terms of visa and passport integrity?

Bill: Alongside the rise of biometric checks for visas, we've also seen the increasing uptake of what rather inevitably have been termed ePassports. These include a chip containing data about the authenticity of the passport, and an enciphered biometric record of the holder. There are the usual issues with compatibility of the early versions, but the intent is to deliver a uniform implementation that includes the face, fingerprints and iris of the holder.

ePassports are, for now, beyond the reach of the more accessible forms of tampering and forgery, and the inclusion of biometrics offers great potential to check the legitimacy of the holder.

Until ePassports have universal uptake, and even then probably for the foreseeable future, destination governments will want to maintain their own independent biometric record of all visitors. This will be frustrating for the traveller who has gone to the trouble of giving biometrics when they applied for the passport but will continue to need to do so whenever they travel.

NZSM: What are the major challenges facing the implementation of biometrics collection for border authorities.

Bill: Collecting biometrics – particularly fingerprints – is currently an inherently physical process, which typically needs to take place in a controlled environment using specialist equipment and trained staff. Without biometrics, visa applications would by now almost certainly have been purely online, but for now a trip to a diplomatic mission or outsourced visa application centre is a necessary part of travel. The challenge for governments is to find a balance in a three-way contest between cost, accessibility and security when providing points of enrolment for visa applicants.

Panomera® from Dallmeier ensures enhanced security at Naples Airport

The international airport at Naples, Napoli Capodichino Airport, is used by 6 million travellers every year. With the introduction of the Panomera® multifocal sensor system from Dallmeier, security in both the apron and the airport forecourt areas is enhanced further still by the very latest in camera technology.

Napoli Capodichino offers direct connections to 50 domestic and international destinations. It is managed by GESAC SPA, a member of the F2I Airports Group, an airport management company known for the excellent quality of its services and for its culture of continuous improvement. GESAC works constantly to find efficient solutions and satisfy the requirements of its passengers and field operators, particularly with regard to personal safety and environmental protection.

Innovative multifocal sensor technology

GESAC's security engineers saw the Panomera® multifocal sensor system from Dallmeier for the first time at the "Sicurezza" trade fair in Milan in 2010, and were very impressed by the performance capabilities of this ground-breaking video technology. Unlike conventional cameras, which have a single focal lens, multifocal sensor technology is based on a multi-sensor platform with several lenses, each

with different focal lengths, creating the unrivalled Panomera® effect. This innovative system provides surveillance of large areas with extremely high resolution, all from a single installation site.

The contact at the trade fair was followed by an intensive planning and design phase, during which the staff at Dallmeier Italy worked closely with the "Infrastructure Development & Flight Operations" department of GESAC, under the direction of Alessandro Fidato. Representatives of Dallmeier Italy visited the site several times so that they could adapt the new video system precisely to the requirements of the airport management company.

Safety for apron, runways and forecourt

For GESAC, two major zones of the airport site were of paramount importance: the area in front of the airport buildings ("Panomera® Forecourt" project), and the apron and runways ("Panomera® Airfield" project).

In the airport forecourt and concourse, Panomera® monitors traffic and pedestrian flows between the multi-storey car park, Terminal 1 and the network of feeder roads and paths by which people arrive at and leave the airport, either in motor vehicles or on foot.





The customer also wanted to obtain complete coverage of the movements of all vehicles and aircraft anywhere on the entire airfield, including the ramps and aprons, taxiways, and takeoff and landing runways, so that incidents could be reconstructed if necessary, wherever they occurred on the site.

The cameras of the Panomera® system for this airfield project were installed at a considerable height, close to the roof of the APRON tower at about 13 metres; three Panomera® systems installed in a semicircle provide a panoramic view through 228°. The Panomera® Viewer workstation was located inside the

APRON Tower to provide security staff with a unique and full panoramic view of the entire airfield.

“With Panomera® technology, distant objects can be captured with the same quality as those in the foreground. The extremely high resolution over the entire area of interest and intuitive operation of the system led us to choose Dallmeier”, says Giuseppe Musto, Head of Innovation & Automation Development for GESAC.

Another important difference between Panomera® and conventional PTZ cameras is that the whole area to be monitored with Panomera®, is recorded

Sign up for a free on-site Panomera demo.

To register email
panomera@crknz.co.nz

continuously, so the high resolution images enable important, single details to be examined even after the event. With PTZ cameras, the general overview image is lost while the camera is recording a detailed area.

Reliable recording

Recording is based on the Dallmeier DIS-2/M NSU blade technology – this ensures maximum availability and reliability of the recording. Each blade unit is equipped with a redundant hard disk. The units are powered via a rack for 19” slide-in modules with redundant power supply units. The rack system can accommodate up to 10 single modules, so that even relatively large systems can be installed in compact and cost-efficient manner. The modular structure of the system guarantees high availability of the overall solution.

Complete success

Alessandro Fidato, Director of the Infrastructure Development & Flight Operations department, describes the video system as a resounding success: “With these two projects, GESAC confirms its orientation towards innovative solutions that ensure high standards of security and simplify management arrangements. We are very satisfied with this cooperation.”

Pierpaolo Piracci of Dallmeier Italy responds: “I am very proud to have been personally involved in these highly innovative projects, and I would like to thank Alessandro Fidato and Giuseppe Musto of GESAC SPA for the confidence they have shown in our technology and professionalism.”



Countering violent extremism for the Common Good

Last December saw Parliament passing legislation aimed at stopping would-be foreign fighters from leaving New Zealand to join Islamic State (ISIS) in Iraq or from carrying out terrorist acts in New Zealand. It followed claims by the Prime Minister that up to 80 New Zealanders were being monitored due to links to ISIS, fundraising for ISIS or attempting to radicalise others.

The Countering Terrorist Fighters Legislation Bill amends three existing laws to give the Security Intelligence Service (SIS) greater surveillance powers and the Minister of Internal Affairs greater powers to suspend and cancel passports. The SIS can now conduct surveillance for up to 24 hours on terrorist suspects without a warrant, conduct video surveillance on private property in relation to suspected terrorism, and gain access to Customs data in relation to suspected terrorism. The Minister of Internal Affairs can now suspend passports for up to 10 working days and cancel them for up to three years.

Although Labour supported the bill, they've nevertheless condemned the manner in which it was rushed through the House, arguing that it denied New Zealanders a real say. Phil Goff described the handling of the bill as an "absolute travesty", and Greens MP Kennedy Graham said the manner in which it was rushed through was a "procedural abomination."

Opposition spokesperson on foreign affairs, David Shearer, commented that when representatives of the Muslim community appeared in front of the bill's select committee, their basic message was: "When we hear about these it is in our

interests as New Zealanders and as New Zealand Muslims to ensure that they get picked up on", and I think what they were saying was: "Yet we are not listened to sufficiently."

Dr Anwar Ghani, president of the Federation of the Islamic Associations of New Zealand (FIANZ), said that while the legislation was technically non-discriminatory, its introduction could alienate and stigmatise New Zealand's small Muslim community. The hurried legislation, combined with the government's recently announced contribution to military action against ISIS in Iraq, will do nothing to prevent a paranoid atmosphere in which ordinary New Zealand Muslims are perceived as a threat.

As hurried as it was, the legislation's passing by a bipartisan majority reflects a consensus that the threat posed by terrorism is real. The Government's New Zealand Intelligence Community website describes the threat succinctly: "Given the degradation of Al Qa'ida networks, possibly the greatest threat of a terrorist act in New Zealand comes from "home-grown" radicalisation or a so-called "lone-wolf" attack. While the risk of such an attack may be low, its consequences could be severe."

Are we following international best practice?

Less than three weeks before the passing of the Countering Terrorist Fighters Legislation Bill, Jim McLay, New Zealand's ambassador to the UN Security Council, delivered a statement at the Open Debate on International Cooperation on Combatting Terrorism and Violent Extremism. In his address,

McLay urged other countries to enact the Global Counter Terrorism Forum's (GCTF) best practices for countering violent extremism and terrorist fighters.

Good Practice #1 of GCTF's Memorandum on Good Practices for a More Effective Response to the Foreign Terrorist Fighters (FTF) Phenomenon encourages governments to "invest in the long-term cultivation of trusted relationships with communities susceptible to recruitment, considering the broader set of issues and concerns affecting the community." Authorities that engage communities whose members are vulnerable to becoming FTFs, it suggests, "should conduct outreach on a broader set of issues, such as national foreign policy, to cultivate trust and address the core needs and concerns of the communities."

While its ambassador to the UNSC was busy preaching to other states the virtues of engaging with and cultivating trust with communities susceptible to FTF recruitment, it appears that our Government was busy rushing through domestic counter terrorism legislation without any meaningful engagement with the very communities in New Zealand that are particularly susceptible.

Interestingly, these best practices go on to explain the varied ways in which engagement with susceptible communities can support counter terrorism. "Governments should consistently engage youth, women, families, and civil society", states Good Practice #4, "providing them with relevant and functional training on building counter-narrative content, outreach, and communications."

It is through collaboration with communities, states the document, that positive and convincing alternatives may be provided to those contemplating travelling to destination countries to support terrorist groups or otherwise commit terrorist acts. “Systematic, tailored mentoring programs”, it continues, “can also be very effective, particularly for youth at risk of radicalization, because they offer individual attention.

This is a point that resonates with Dr Rob Roche, a member of the New Zealand Peace Foundation and retired Auckland-based medical practitioner, who has previously led groundbreaking work with patients suffering from alcoholism and serious drug addiction. Although acknowledging the role of security and law enforcement, he believes that the government is approaching the issue of radicalisation and violent extremism with one eye open.

According to Dr Roche, New Zealand should look to complement its security efforts with a program taking its lead from those currently operating in Europe that are countering radicalisation with tailored mentoring of those at risk. As he sees it, a mentoring program would incorporate the very elements that have served him well during decades of professional practice: community and family engagement, trust building and compassion.

Community mentoring – winning hearts and minds

“There are two successful rehabilitation programs in operation overseas that are worthy of consideration”, states Dr Roche. “In Denmark, law enforcement officers have been working since 2007 on an evolving program designed to prevent radicalisation and to rehabilitate potentially violent extremists.”

At the centre of the program, he explains, is Infohus (Information House), which is a contact point where people are encouraged to make anonymous reports on individuals who may be at risk of radicalisation or extreme acts of violence. Most of the cases that are referred to Infohus involve young people despairing over global events and inequalities and who may have lost their private battle for self worth and acceptance by society in general.

“Infohus then uses a network of parents, social workers and teachers to collect information before therapeutic steps are taken”, Dr Roche explains. “After identification and assessment of someone deemed to be at risk, an



Dr Rob Roche, is a member of the New Zealand Peace Foundation

appropriate support team is put in place, which can provide one-on-one counselling by social workers and religious leaders. Where there is financial disadvantage, job training and housing assistance may be provided.”

“To be effective, any program for the rehabilitation of extremists must be based on love, truth, trust and mutual respect”, insists Dr Roche. “It will have a better chance of success if it is non-judgmental and where there are no elements of confrontation or fear of physical punishment or condemnation.”

Another program based in Germany has been in operation since 2011 and has so far dealt with almost 500 cases. Called Hayat (Arabic for ‘life’), it is supervised by Daniel Kohler, director of the German Institute of Radicalisation and Deradicalisation and a leading figure in counter-radicalism.

“Kohler stresses the importance of treating a radicalised individual as a patient”, explains Dr Roche, “so that appropriate psychological counselling and other specialised services can be provided when needed.” And the identification of the at-risk person as someone ‘in need’ rather than a mere target of state surveillance or law enforcement action is a key ingredient for Dr Roche. “The object”, he stresses, “is to generate a sense of wellbeing and self-worth so that the patient is well equipped to find a rewarding place in society.”

“The process of rehabilitation may start with an anonymous call to a 24-

hour hotline from a worried friend or family member. Counsellors can then work with families as equal partners in the therapeutic process. An important early step is simply to resolve any ongoing family problems.”

Hayat now belongs to a network of four similar organisations funded by the German government. Recently Hayat Canada has been launched, and a proposal is under consideration by the Australian Government. Across the Tasman, however, there are concerns that \$13m in federal government funding allocated in October to fund community-based deradicalisation programs has remained unspent.

A Sydney Islamic leader has recently commented that community leaders there are refusing to counsel young Muslims vulnerable to being radicalised because they fear security agencies will target them as collaborators. Therein lies the risk of a lack of meaningful government-community engagement: without official backing, those most qualified and capable of identifying and supporting at-risk individuals are likely to be too afraid to help, and we all remain exposed.

According to Dr Roche, government backing of a community-based deradicalisation program is what’s needed to fill the gap left by Wellington’s surveillance-centric approach. Cancelling passports no doubt has its place, but winning back the hearts and minds of at-risk New Zealanders surely is a more desirable endgame for us all.

Opening Doors and Gates with Smartphones, Bluetooth Smart and Gesture Technology

The latest access control systems offer more secure and sophisticated credentials, while introducing new credential form factors including mobile devices that make it more convenient to open doors and gates. Mobile access control also delivers a simple and user-friendly secure identity management process to access facilities, while paving the way for integrated, multi-layered physical access control (PACS) and IT security solutions down the road.

One of the most attractive opportunities for access control solutions on mobile devices involves the use of Bluetooth Smart connections and gesture technology. Bluetooth combined with gesture technology enables users to open doors from a distance by rotating their smartphone as they approach a mobile-enabled reader. Using gesture technology in this way significantly improves the user experience while adding an authentication factor to the existing access control rule set that goes beyond something the cardholder “has”

(the card) to include a gesture-based version of something the cardholder “knows” (like a password or personal identification number, or PIN).

Gesture-based access control will also increase speed, and minimize the possibility of a rogue device surreptitiously stealing the user’s credential in a “bump and clone” attack.

Entering with a Twist of the Phone

In much the same way that mouse technology was a disruptive innovation that revolutionized the computer interface, gesture-based technology is poised to change how users open doors today and perform many other access control tasks in the future.

In a mobile access control environment, gesture-based access control technology leverages a smartphone’s built-in accelerometer feature to enable a simple twist of the phone to unlock doors. For instance, a user presents the phone to a reader,

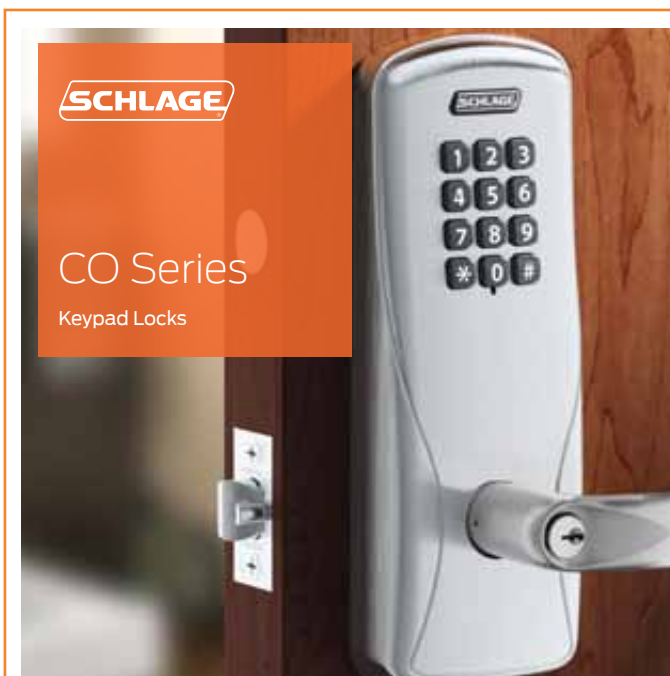
rotates it to the right, and then returns it to the original position so that the credential inside the phone can be read, and access can be granted. The smartphone knows how the screen is oriented because its accelerometer senses movement and gravity. Adding gesture capabilities to a wireless connection gives users a great deal of control over how they interact with the access control system.

Making the Connection

There are two choices for communications technology that enables smartphones to “present” credentials to a reader: NFC and Bluetooth Smart. NFC technology has taken the lead for tap-in strong authentication use cases, enabling users to gain access to resources by simply tapping a smart card to a tablet or laptop for authenticating to a network or application.

In order to implement gesture technology, however, Bluetooth Smart is required because of its longer reach.





- 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**



ALLEGION

www.allegion.co.nz

HID Global recently piloted gesture technology with Bluetooth-enabled smartphones at Vanderbilt University. There were approximately 15 participants that used their smartphones to open doors at one or more of six possible campus entry points, including one parking garage. Each entry point was equipped with mobile-enabled iCLASS SE readers that were configured to work with existing iCLASS® smart cards as well as HID Global's Mobile IDs. A survey of participants highlighted the speed and simplicity of installing and registering the HID Mobile Access App. Most respondents said it required no more than a minute to complete the process and was a self-explanatory and intuitive experience. Respondents also cited the convenience of using their phones to open doors and gates, including the added benefit of not even having to roll down their window as they approached. They also appreciated how mobile access control provides a backup measure in case of a lost or forgotten access card.

Rolling out Mobile Access Solutions with Gesture Technology

Mobile access control and the ability to use gesture technology smart devices requires rethinking how to manage physical access credentials, and to make them portable to smartphones. It also requires an open and adaptable secure identity solution that can turn mobile devices into trusted credentials.

An example of this is delivered with HID Global's HID Mobile Access solution, which includes everything necessary for organizations to

immediately begin using Bluetooth Smart and NFC-enabled smartphones and other mobile devices as an alternative to keys and smart cards in today's increasingly popular BYOD mobility environment. The solution also makes it possible for users to unlock doors and open gates from a distance using the company's patented "Twist and Go" gesture technology. It is implemented with the company's mobile-enabled iCLASS SE® and/or multiCLASS SE® readers, and includes Mobile IDs, HID Mobile Access Apps and access to the HID Secure Identity Services™ portal for managing users and issuing or revoking Mobile IDs. The mobile-enabled readers are also interoperable with 125 kHz HID Prox and high-frequency technologies including iCLASS Seos®, iCLASS SE, standard iCLASS®, MIFARE®, and MIFARE® DESFire® EV1, which optimizes flexibility for using both cards and mobile devices.

As mobile access control solutions are deployed, their benefits will drive many companies and organizations to seriously consider incorporating a combination of secure mobile physical and logical access into their facilities and IT access strategies. In addition to receiving digital credentials and "presenting" them to readers at doors and parking gates, smartphones will also be capable of replacing passwords for computer login, and generating one-time passwords for accessing network or cloud- and web-based applications. In other words, the same phone used for building access will also be used in conjunction with a personal tablet or laptop to authenticate to a VPN, wireless

network, corporate intranet, cloud- and web-based applications, single-sign-on (SSO) clients and other IT resources. In some cases phones will replace cards, but in many others they will supplement cards to deliver a more secure and user-friendly experience. The objective is not simply to substitute one credential form factor for another across isolated use cases, but rather to leverage mobile platforms and associated technologies to build unified solutions for ensuring secure access to the door, to data and to cloud applications.

The introduction and accelerating adoption of mobile access solutions is one of the most important industry developments of the past few years. New mobile technologies such as gesture-based access control using the phone's Bluetooth connection are an important ingredient as smartphones become an integral part of the ecosystem for the creation, management and use of secure identities. Just as mouse technology revolutionized the computer interface, gesture technology is expected to change how users interact with access control systems. Used alone or in tandem with other authentication factors, gestures offer the potential to significantly improve privacy and security. Plus, gesture technology helps offer an improved user experience along with new and more convenient ways to open doors and gates.



Product integrity and personal integrity go hand in hand

Our profile for this month is a well known identity on the supply side of the security industry in New Zealand. Until recently he has been the manager of a specialist electric locking hardware distribution company, selling major imported brands, but also designing and manufacturing local product under the Loktronic and ViTECH brand names.

In an industry that is full of characters and unique individuals, Peter Calvert stands out. Not because he makes the most noise, has the biggest business or runs a hefty steamroller over those in his path.

Peter is far more modest. As he will tell you, he was born in “the latter part of the first part of last century.” Running a business now is very different to those halcyon days. We all know the modern business world is as tough and as uncompromising as it has ever been. The wolf is often scratching at the door and those with compromised motives abound. But Peter aims to stick to the fundamental principles of honesty, integrity, truthfulness and full disclosure, adding up to no surprises and reliability in a business sector that demands these attributes along with the essential knowledge, expertise and professionalism required.

Today Peter describes himself as a humble ‘consultant.’ For health reasons he now restricts his working life to three days a week and there is already a mapped out succession plan for the business, Loktronic Limited. But such is his knowledge and expertise in the highly technical and specialist world of electronic locking, you can bet his phone is always handy on those ‘off’ days and he is checking his in-box for any blips on the radar.

The first iteration of the Loktronic name and brand goes back to 1989 when Peter formed Loktronic Industries Ltd to cater for a dearth of products in this market sector and to develop a catalogue system to source and sell from. But like many good operators he had tried a



Peter Calvert says “putting intelligence into the lock” and offering new levels of sophistication are the keys to Loktronic’s success

couple of other paths before arriving at his final destination.

Born in the central Waikato, after concluding his university studies he joined the family business, Geo. Calvert & Co Ltd, which was an iconic retail business in Cambridge. In 1913, Peter’s Yorkshire grandfather George had purchased a small clothing and outfitting business which dated back to the 1890’s. Peter’s father Maurice joined in 1928 and took ownership in 1956. Over the decades the business expanded significantly employing more than 20 people and became famous for its mix of clothing, textiles, manchester, haberdashery and quality period furnishings as well as the unique ‘Lamson Cash Railway System,’ at the time one of the big tourist attractions in the small town.

While Peter stuck at the retail life for 10 years with some two years away gaining experience in textile manufacture, he admits he was less interested in the women’s fashion side of the operation. He yearned for something a bit more “nuts and bolts” as he says. With a keen interest in biological sciences, he took up a position with pharmaceutical company, Beecham Research Laboratories as a medical detailer.

With some 45,000 employees in 120 countries, Beecham was then one of the biggest players in the ethical drug production market worldwide. Peter worked his way up through the organisation taking national and international supervisory and managerial roles. By 1989 Beecham was in the throes of merging with an equally well established business, Philadelphia-based SmithKline French Corporation and it was time for Peter to again scratch an itch for new fields of endeavour.

Another area of special interest for him was in the area of mechanics and engineering. It had become clear in discussions with experts and locksmiths that there was a strong move towards electronic locking solutions, particularly in large construction and commercial applications. He was the co-developer of some locking concepts that would help turn a range of technical inspirations into reality.

He and his small team developed a very smart product that he describes as “putting intelligence into the lock” and offering new levels of sophistication. When a conventional lock with a mechanical locking system did not meet

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



requirements with regard to security or convenience, electronic door deadbolts as a supplementary locking device were often the best solution and were also recommendable as an additional security measure due to their compact design. The many different installation types and slim designs enabled these deadbolts to be fitted to nearly all types of doors, from standard doors through to glass doors.

Adjustable between 12 and 24 volts, Loktronic's early iteration, the intelligent drop bolt known as the LB25R, was enthusiastically adopted by the large German manufacturer Eff Eff which was taken over in 2000 by Assa Abloy, the global leader in door opening solutions.

On a purely business front, it has been a rocky road at times for Peter and his various permutations of the Loktronic brand. But through it all he and the company have survived based on some basic concepts relevant to all small business operators. With a dedicated fighting team of four, Loktronic is a mean, lean locking machine. Peter's stated business mantra is, "Quality, service, reliability, and competitive prices which collectively add up to value."

Today Loktronic specialises in electric locking hardware and accessories and has become universally known as New Zealand's leading port of call for advice, sales, service and repairs to the widest range of products. The company stocks all the leading brands and some less well known ones too.

As an expert supplier to the security and access control installation industries Loktronic distributes electric locking and security products nationwide from its Mt Eden showroom, offices and warehousing facility. Between the four members of the highly motivated team they can boast decades of experience.

Sandi Hewlett has 26 years of service with Loktronic and manages the day to day office and accounting functions; as the daughter of the late Sid Pemberton, one of Auckland's pioneer locksmiths, she came to Loktronic with a wealth of practical knowledge. Eilish O'Brien fills the demanding technical sales and support roles and her two degrees in marketing and business management equip her well for the additional support that she gives. Peter Sheehan is a registered electrician and manages the ViTECH division of Loktronic. He specialises in the design and development of the highly innovative range of fire protection products further described below. Together the team see their role

as supplying and supporting installation companies and systems integrators.

Their task is to help in the selection of the most appropriate products to fulfil the needs of a diverse range of clients initially at the design level but also through to commissioning and on-going after sales support. Peter's philosophy is never to sell anything to anybody by withholding information knowing that if you gave them 100 percent of the information, they wouldn't buy the product.

"If we do not have the most suitable product in stock for a customer's needs we will do our best to obtain it for them," says Peter. "If we cannot source it we will advise them where they can obtain it. We are trade suppliers only and do not sell to the public or undertake installations; however we can arrange installation through partner companies."

If the above all sounds a little altruistic, rest assured that tyre kickers and information pumpers can get short shrift at the Loktronic counter or on the phone. If its information you want in order to buy or solicit the lower price elsewhere, then think again.

The company's Loktronic-branded products comprise electro-magnetic locks for indoor and outdoor use, fire door holders, key switches, exit buttons, power distribution modules and power supply cabinets. All these are manufactured and assembled here in New Zealand. The Loktronic-branded indoor locks and fire doors holders carry a 10 year guarantee. 25 years' evolution in the design and manufacture of electromagnetic locks means the Loktronic product has become the standard by which others are measured, becoming famous here and in certain overseas countries. A wide range of accessories, finishes and custom lengths means that this range is favoured by discerning specifiers and installers alike.

The wholly owned ViTECH division of Loktronic designs and produces a leading edge range of fire protection products including anti-interference devices, battery load testers, Type X and Type Y fire brigade alarms.

The feature rich and keenly priced Loktrenz range of products Peter and his team now offer are sourced from outside manufacturers and the Loktrenz branding gives assurance that they are tested and meet the stringent requirements which the company lays down when contracting for supply. Loktrenz products include a wide range of electric locks, electromagnetic locks and accessories, gate locks and power transfers.

Peter says it is worth noting that

Loktronic stocks a wide range of electric lock agency products including strikes, drop bolts and mortice locks with many famous brands: Abloy, Allegion, eff-eff, FSH, Interlock, Lockwood, Cisa, Trimec and others.

All electric locks require power to operate and Loktronic has met this demand by stocking a wide range of power supplies from Powerbox and Meanwell with well over 30 models to suit a customer's requirements.

Not content with just locks and accessories, Loktronic has a complete range of Rosslare key pads and Prastel door controllers, Reed switches by Flair and Securitron, the complete range of Trojan EmRex, ProxRex devices, relays and timer boards, Trencab key switches plus a huge range of STI stoppers, protective cages, alarmed housings, wireless transmitters and strobes. As Peter will tell you, the range really is exhausting! But you can generally rest assured that whatever your problem, they will have a solution or be able to find it and have it delivered the next business day anywhere in New Zealand.

Some time ago Peter came to the realisation that the supply of these types of product had to come with the highest levels of professionalism and integrity. You will find his products providing security and safe access in the busiest airports and the biggest hospitals in the country along with banks, schools and other major institutions.

To this end in 2012 Loktronic applied for and gained ISO 9001:2008, the world's leading ISO management system standard. This independently audited standard has been implemented by over one million companies and organisations in over 170 countries.

The principles upon which ISO 9001:2008 are based are crucial to Loktronic and include: customer focus, leadership, involvement of people, process approach, system approach to management, continual improvement, factual approach to decision making and a mutually beneficial supplier relationship.

It wouldn't be too much of an exaggeration to say Peter Calvert loves the industry he is involved in. It is a long way from the ever-changing women's fashion world of the family business he worked in all those years ago. In this industry, while the market is always changing and developing, products are not obsolete overnight; just right for a pragmatist who likes to say, "Is the client always right? No. But it's always got to be right for the client."

New Zealand Security Conference and Exhibition

The 2015 New Zealand Security Conference and Exhibition will be held on Thursday 19th November, Friday 20th November and Saturday 21st November.

The venue

ASB Showgrounds

Green Lane West, Greenlane, Auckland

The Theme

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.



*Timothy L. Dillon, Vice President
Oracle Global Physical Security*

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.

The Speakers

As usual we will feature a range of international and local experts delivering presentations around our theme.

We are pleased to announce the first of our keynote speakers, Timothy L. Dillon, Vice President Oracle Global Physical Security. Timothy will focus on how to maintain a level of safe and secure operation for facilities and people in areas of high threat or risk. He will concentrate on the following areas:

- The branded value of security services: Personnel Protective Services (including executive protection for corporate officers), Travel Security (proactive, ongoing tracking while in high risk environment), Threat and Risk Analysis, GSOC (Global Security Operations Centers) and the role they play.
- Strategies for global security support in regions or areas of high threat/risk and the relationship between their partners on the ground, the GSOC and the management team, as well as methodologies that are used to determine locations of high risk.
- Tools & Technologies used to support the above programs, how they efficiently establish where their threats and risks are, and how these are communicated to personnel globally.

Registrations open 1 April 2015.

For further information on exhibiting or sponsoring for this event call us on 09 486 0441 or email Kirsty Reid at Kirsty@security.org.nz



The future is happening now

Examining the key security risks for government and business.

While malicious cyber activity has seen significant growth, it does not replace traditional threats.

The security environment is changing globally on an almost daily basis. The world is experiencing real increases in threats to individuals, critical infrastructure and trusted environments such as airports, schools, hospitals, public transport, utilities, businesses and the home. Australia is not immune from the uncertainty, which we saw when our own terror threat level was lifted from medium to high by ASIO last year.

These security threats are being driven by several factors:

- Geopolitics.
- Globalisation of crime.
- Terrorism.
- Physical and cyber piracy.
- Organised crime and anti-social behaviour.

In an increasingly connected economy, these threats are real, prevalent and affect the bottom line.

In a constantly evolving environment these threats present risks to governments and business and place new and increasing demands on the security industry. Responding to them must be a priority for government and business in Australia.

For our governments and most Australian businesses the emphasis has been on cyber, virtual and internet security. While malicious cyber activity has seen significant growth, it does not replace traditional threats.

The changing environment and evolving threat level demands a shift in our response.

The implications of this new environment for governments and businesses are far-reaching and have an

impact across many aspects of business, public policy and social life:

- Risk management.
- Continuity and insurance planning.
- Finding the balance between privacy issues, security surveillance needs and data retention requirements.

For some governments and businesses, significant upgrades of physical surveillance infrastructure will be

required to protect staff, customers and operations. These issues suggest a need to refocus efforts in physical security.

Advances in technology within the security industry will lead the way to improved security awareness, tracking, threat detection and protection through:

- IP networking.
- Mobility.
- Ultra-high definition video surveillance.
- Real time location services.





- Big data analytics, including video.
- New face and iris scanners.
- Video synopsis.
- Unmanned robotic security systems.
- Advances in secure identity systems.

These tools will facilitate security services' evolution from incident capture to real-time assessment of threats that can lead to incident prevention.

The integration of disparate

security systems such as alarm, access control and CCTV as part of bundled security solutions with fire and building management systems is emerging as a strong push within the security market. This will see traditional security providers joined by new players such as telecommunications companies, who will offer active monitoring and surveillance services to governments and enterprises alike. These security services may be part

of a broader security framework covering network and cyber security.

So what steps should enterprises and businesses take?

Risk assessment and management is critical. At the simplest level this involves a review of the risk management framework within the organisation to ensure it identifies risks, rates likelihood, potential business impact and then outlines mitigation strategies. At the most comprehensive level, it requires detailed threat assessments and an exhaustive review of the potential vulnerabilities of physical assets, virtual assets and systems.

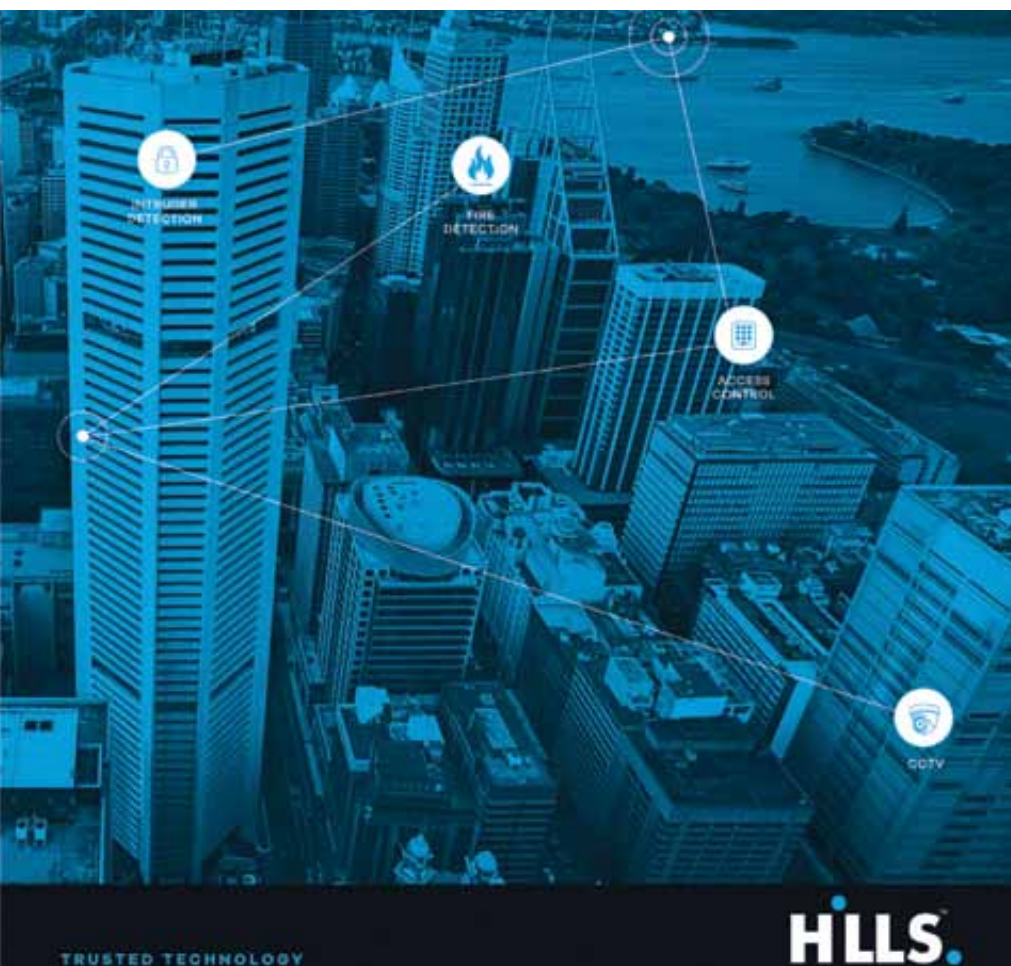
Improvements to IT security, entry procedures and physical security are all part of this process. Given the speed of developments in cyber espionage and sabotage, risk management must be an ongoing process.

The effectiveness of any organisation's defence against security threats is directly related to the drive and leadership of senior management and directors to address risks.

Complacency is not an option. Business continuity depends on best practice leadership action to assess insurable risks and obtain appropriate policy cover. Above all, remain vigilant.

Emerging security trends

- Bundled security solutions - alarm, access control and CCTV.
- Migration from passive analog security to an IP video centric security model.
- Integration and unification of all solutions into a single platform – PSIM/Command and Control.
- Move to cloud based storage and processing, which will allow for increased collaboration across a range of sensors and devices.
- Migration of legacy security systems away from PSTN to IP monitoring, putting existing business models under stress.
- Self-monitored security solutions will become the 'norm' until the current security monitoring industry is able to re-invent itself and offer new compelling services.
- Telco providers beginning to offer security services as part of a broader 'connected home' strategy.
- Emergence of new ultralow profile and HD microdome cameras, high contrast thermal imaging cameras as detectors.
- Integration of geo-location.

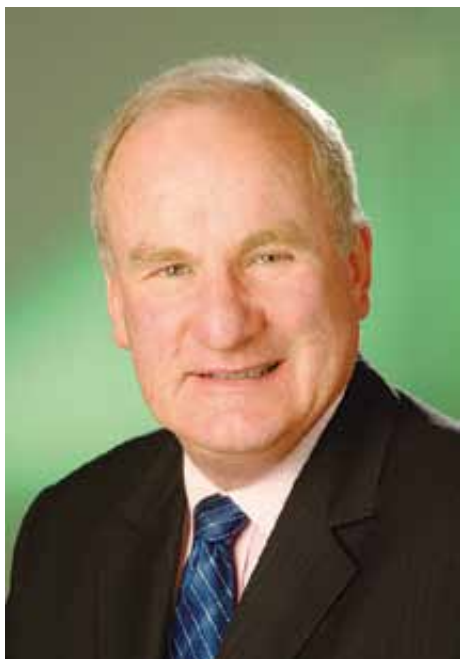


Off the Rails

Calls for police on Auckland trains continue

On the evening of Saturday 13 December, nearly 100 brawling youths disrupted train services following Christmas in the Park and the Ragamuffin music festival. 15 security guards and Maori wardens struggled to contain the crowd. The brawl was over quickly, but violence at Glen Innes the same night resulted in \$20,000 damage to a train.

In July, in an Auckland Council press release, Manurewa Local Board chairperson Angela Dalton had commented that the Police had been



George Wood is an Auckland councillor and former policeman

warning Auckland Transport for months about problems with unsecured train stations. "In light of failed ad hoc solutions such as contracted ticket inspectors and security guards operating from time-to-time", stated Ms Dalton, "a more radical response may be required."

That same month, press reports covered the news that a proposal for transit police to patrol Auckland trains was being considered by Auckland Transport as a "long-term option" to curb violence on trains. In one such report, Auckland councillor and former policeman George Wood was quoted as saying that transit police were "long overdue".

The Britomart incident has only served to intensify calls for policing on Auckland trains, with Cr Wood again expressing to the NZ Security Magazine deep concern over the increasing examples of violence and theft in the rail system. "The number of incidents is very high", argues Cr Wood, "and Britomart is likely not the worst".

"Unfortunately, security officers don't have any powers, so they can't intervene. We have been lobbying Auckland Transport into doing something for well over two years, and the situation hasn't improved. There doesn't seem to be any end to the problem of the lack of intervention by Auckland Transport and the police."

The Land Transport Act provides for spot fines of \$150 and court penalties of up to \$500 for fare evaders on any form

of passenger transport service, but that requires police intervention. And despite the introduction of lapel-mounted cameras for fare inspectors in mid-2014, fare evasion appears to have been on the increase.

Cr Wood observes that according to Auckland Transport estimates, 6% of passengers are not paying. Other estimates suggest the figure is at least 11%. According to a March 2014 post on transportblog.org.nz, rising fare evasion "seems to be the result of more and more people realising the chance of getting caught without a ticket is low and even if they do get caught, the ticket inspectors are powerless to do anything."

A lack of gates at stations has also been blamed for promoting fare evasion, and perimeter gaps along the rail network are being blamed for encouraging damage and vandalism to Auckland Transport property.

"There needs to be more coordination", argues Cr Wood. "With no police on platforms and in trains it can be a long time before security staff receive police backup when they need it." He points out that there were no police at Britomart on 13 December.

"Police are always telling us how stretched they are. The New South Wales police have 600 dedicated officers for the rail system. I would like to see Auckland follow the New South Wales model, but the cost of this would be more than what the government would be prepared to put in."



Greg Watts, Managing Director of the New Zealand Security Association

The NSW Police Force took over policing of that state's public transport network on 1 May 2012. The Police Transport Command (PTC) was established to provide high-visibility policing across the transport network. According to the NSW Police website, PTC officers are trained in counter-terrorism, criminal detection and

conflict resolution and are empowered to arrest anyone who breaks the law on public transport.

In addition to uniform patrols, special teams operate in plain clothes targeting identified problem areas and graffiti vandalism. PTC officers detect and prosecute offenders for a variety of matters including malicious damage, graffiti and trespassing in the rail corridor. The PTC also provides an intelligence-based response to transport crime during busy times and at hotspot locations. This includes a focus on special events such as New Year's Eve celebrations, Anzac Day and major sporting events.

Apart from the rail network, the PTC makes patrols of bus interchanges, bus stops, bus patrols and routes, ferries and wharves, ferry patrols, and taxi ranks and pick up points.

But Greg Watts, Managing Director of the New Zealand Security Association questions the need for more police on Auckland trains. "The first question I'd ask is what are the numbers? There needs to be some statistics around this."

Greg suggests that there are other things that Auckland Transport could be doing to improve security around its network, and for less money.

"Council could place increased security at certain times and during big events", he suggests. More security staff could also be deployed to violence hot spots. "Some incidents could possibly be deterred by greater CCTV surveillance, as has been the case in London."

On the question of how an Auckland model might be funded, Cr Wood points out that "Policing is a government responsibility." Greg's not too sure about that. "The Police don't have the budget to be putting more police on trains and platforms", he points out.

Despite the ongoing debate around the state of security in the rail system, however, calls for greater policing of Auckland trains appear to be falling on deaf ears with neither Auckland Council nor the central government prepared to throw more funding on what has become an ongoing public transport security issue.



Health & Safety Representative (Security Stage 1)

New Health & Safety laws are coming into effect this year and this legislation will impact on the entire security industry. C4 Group courses are designed for security companies to meet their legislative obligations and ensure they have an effective Health & Safety Management System. No matter what size your organisation is a trained Health & Safety Representative will help you reduce accidents and injury as well as save money. NZQA Unit Standards will be awarded on successful completion of the course.

Topics include:

- Role of Health & Safety in the workplace
- Health & Safety Representative roles and responsibilities
- Motivational & behavioural factors behind Health & Safety
- Legal compliance requirements for today and the future
- Employee participation and good faith
- Risk management (*Hazard avoidance*)
- Emergencies (*Reduction, Readiness, Response, Recovery*)
- Accident reporting and Investigation
- Health & Safety training requirements (*Internal & External*)
- Injury management
- Promoting effective Health & Safety

**Our trainers are experienced
H & S consultants in both
New Zealand and Australia.**

**Check out our website for more information
www.c4group.co.nz**

Certificate in Investigative Services

This course is designed for people involved in the investigations process including criminal, fraud, internal, Health & Safety and anybody who conducts workplace investigations.

The course establishes a base level of professional skills for those wishing to apply for a New Zealand Certificate of Approval (Private Investigator) and commence a career as a professional investigator. It is consistent with the Australian qualifications 'Certificate III in Investigative Services' and prepares the learner for further study for professional certification with ASIS and ACFE.

Topics include:

- Develop investigative plan
- Provide quality investigative services
- Conduct interviews and take statements
- Gather information by factual investigation
- Conduct surveillance
- Locate subjects
- Compile investigative report
- Prepare and present evidence in court
- And more...

Our trainers are experienced investigators and consultants.

Check out our website for more information

www.c4group.co.nz



Trends in Incident Management for Public Transport Operators

The article discusses the trend towards system integration (fire, access control, video surveillance) and resulting advantages for public transport operators to be able to more efficiently respond to incidents.

In a larger transit system, more than one hundred security-related incidents can occur every day. Typical incidents include pick-pocketing, violence, illness, a lost child and graffiti. In the past, public transport operators have used video surveillance mainly forensically for investigation purposes after an incident had

occurred. Moving forward and already a reality today for transit authorities in some cities, live video is becoming instrumental to all stages of an incident lifecycle.

We see both Physical Security Information Management (PSIM) and Video Management System (VMS) vendors offering professional incident

management modules which integrate with modern network video camera systems. This development is underlined by a general trend to integrate previously separate systems such as fire detection, access control and video surveillance into a common security and safety system using network and IP technologies based on open standards.



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

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.

Advanced video analytics can automatically detect incidents as they occur

Advanced video analytics, or intelligent video, is a technology area that has matured significantly and become more robust lately. Such capabilities can now be embedded directly into smart surveillance cameras. This enables the cameras to automatically alert the security center in cases of, for instance, unauthorized access at rail yards, bus depots or tunnels. As a result, the transit authorities can get early warnings for potential incidents such as graffiti, metal theft, sabotage or tunnel trespassing. Modern video analytics applications can be used in both very light sensitive cameras and thermal cameras, making them invaluable in very low-light conditions or even in complete darkness, around the clock.

IP-based video surveillance systems can stream live video to multiple users

A network-based video surveillance system is an ideal platform to distribute live video during an incident to first responders and incident coordinators to create a common operating picture of what is going on. This type of real-time information is valuable in helping remotely evaluate and prioritize the specific incident, allowing better and more effective management of resources and to implement an appropriate response. When the security center and/or first responders receive an alarm – whether from a fire detector, security officer or a passenger in panic – they have to decide on what actions to take. With access to live video from the scene, it becomes much easier to make the right decisions regarding an appropriate response. This not only helps resolve the incident quicker, but also ensures that it is done as cost-effectively as possible.

As multiple video streams can be generated from one network camera the video quality can be adopted for mobile devices that are connected wirelessly. This is particularly helpful for responders driving to the incident location to understand how the scene develops, people involved etc. Additional responders can be called to the incident. There may be a medical emergency such as a man suffering a heart attack as well as a very crowded platform situation. Before responders arrive at the scene they can call upon the transport operator to ensure a rescue pathway is cleared by station personnel.



Public transport operators can upgrade older security systems in stages

When planning to upgrade older security systems, public transport operators should work towards a centralized security system with real-time capabilities, with the ultimate goal to connect the complete transit system to one central security center. This makes it possible to efficiently act on incidents as they occur. Such a system can be implemented incrementally, adding new stations, depots, fleets, etc. over time.

Public transport operators should steer away from proprietary solutions and instead invest in equipment based on open standards. This warrants a future-proof, scalable and cost-efficient solution. Modern network cameras provide crisp clear image quality in HDTV, even under very low-light conditions. This allows for quick visual identification of incidents

and the appropriate resources deployed to address them. Image quality also plays a major role should video footage serve as evidence in court.

The latest advancements in video analytics enable early incident detection and can be a cost-efficient alternative to patrolling security guards. A modern incident management system can manage the whole incident lifecycle; from detection, prioritization, response, re-prioritization, investigation and follow-up.

**By Patrik Anderson,
Director Business Development
Transportation, Axis Communications**



Maintaining motivation

It's incredible to think we are a quarter of the way through 2015 and the change of season is a great time to take stock of how well things are going so far this year.

Is your team motivated? Or are they just hanging out for the next statutory day off work?

If your workplace sounds like the latter don't worry, there are things you can do to change this.

The good news is you've probably hired people you want to work with, you know they want the job, you know they can do the job – it's just a case of regaining that "new year" energy. Here are a couple of tips to help kick-start things.

One hugely underrated motivator is listening to your employees. Organise some one-to-one time with your team members – head out for a 15 minute coffee together.

This isn't about wasting time at work but in fact opens the door to chat about new ideas they may have, work concerns



Lance Riesterer, GM of Specialist Trades and Business, The Skills Organisation

or personal situations they may need to talk about and which might be negatively impacting on their work.

Another motivator is taking a genuine interest in the future of your employee's career. Imagine coming into a working environment where you know your boss

wants you to succeed, and is actively involved in helping you become the best you can be.

Lance Riesterer, GM of Specialist Trades and Business, The Skills Organisation says having your team trained through a proper certified programme shows willingness to invest in them.

"There are some great courses offered by training providers associated with The Skills Organisation. It is not just a case of putting employees on training courses though, the real point of difference is to have them complete the course.

"There is a sense of accomplishment and they have tangible proof of their development which they can keep for their entire career.

Certification also gives your customers assurance of quality, skilled workers. It's a win-win for your business," he says.

For more information call 0508 SKILLS (0508 754 557) or visit www.skills.org.nz.

Ensure your business is in safe hands

Investigate our First Line Management qualifications now

skills.

The Skills Organisation
0508 SKILLS (0508 754 557)
skills.org.nz



Identity theft support service iDcare launches in New Zealand

Thursday 19 March saw the national launch of iDcare at New Zealand's Parliament House. Presiding over the launch was Minister of Justice, the Hon Amy Adams, along with Mr David Philp, General Manager Identity Services at DIA, and Dr David Lacey, Managing Director of iDcare and Senior Research Fellow in identity security at Queensland's University of the Sunshine Coast.

With its Australian operations officially launched in Brisbane last year, iDcare is Australia and New Zealand's national identity theft support service. Their service is anonymous and free, supported by a number of sponsors and members across government and business that view their involvement as a means of demonstrating their commitment to protecting their clients and customers. Several of these, including the IRD, New Zealand Police, the banking ombudsman, and a number of telcos and banks, were present at Thursday's launch.

iDcare provides personalised support to individuals that are concerned about their personal information, and works with government and industry (large and small) to independently assess their capacity to respond to contemporary and emerging identity theft and misuse risks – physical or online. iDcare operates a national toll-free number (0800 201 415) and an online presence at <www.idcare.org>.

According to MD, David Lacey, iDcare works with clients to build specific response plans to their situation. It is a one-stop-shop, states David, providing “practical guidance on what organisations across the public and private sectors require their customers to do in response to risks to their personal information.”



David Lacey (L), Minister Adams and David Philp (R) at the iDcare launch

iDcare's counsellors specialise in identity security and they work with people in crisis to build their confidence and a clear pathway on what to do moving forward. The key, says David is that “as soon as you become aware that personal information has been put at risk, act. Don't wait. Call iDcare and we'll work with you to build your resilience and countermeasures.”

Overseas criminals, local victims

According to iDcare data, the current top three sources of personal information compromise in New Zealand and Australia involve:

1. Scams (21%) (investment scams, phishing emails, internet scams, etc).
2. Physical theft of documents (19%).
3. Email hacking (17%) (as result of malware).

“All of the phishing and internet scams forwarded to us by clients originate overseas in areas where law enforcement has limited effect,” says David. “Because scams are the largest source of identity theft we see, international trends have a significant impact on New Zealand and Australian ID crime.” The documents requested during these scams are typically driver licenses, taxation details and credit/debit card details.

“There is no doubt the online nature of a lot of this crime enables criminals the opportunity to impact the community without having ever hopping off a plane in New Zealand,” observes David. It's a sobering thought.

“Most of the telephone scam compromises feature both a local and an international dimension, for example, a local landline diverted to an international criminal call centre,” he explains. “It's

fair to say domestic and offshore feature prominently as a source of compromise.”

Although overseas actors are the main perpetrators of scams, physical theft is the local aspect... and often more traumatic for victims. “With physical theft,” says David, “victims tell us things like, ‘I’m afraid to go home because they know where I live’.”

Approximately 190,000 New Zealanders experience some form of identity compromise every 12 months, which puts them at risk of further misuse. According to David, iDcare’s client engagement indicates that retail purchases, accessing of financial services, and obtaining government services are the three most common forms of misuse resulting from the compromise.

Gone... in 72 hours

According to iDcare’s data, over 72% of New Zealanders ‘self-detect’, which means they are the first to detect that their identity has been compromised or misused. “The takeaway here,” says David, “is that for complex identity crime matters, the victim is typically the first one to know. Secondly, it means that either organisational controls are not as effective as we hoped, or organisations may know, but choose not to tell the victims.”

On average it takes individuals around 16.2 days to detect the event, but criminals only 72 hours to misuse the information. Hacking events are particularly worrying, adds David, “where organisations (government and business) can take weeks to tell impacted staff and customers.”

How the compromise occurred, he says, really matters. If it was online, then the chances are a number of identity credentials and forms of personal information are at risk. “It’s not good enough for institutions to think that the problem is solved if they merely work with a customer to replace a credit card or monitor an account. Identity information is part of a much broader identity ecosystem, and as such, responses must be holistic.”

Is New Zealand any different?

According to David, all parts of the New Zealand community are impacted upon by identity theft. “iDcare speaks daily with clients of organisations across business and government, from large to micro, from Auckland to Invercargill.” Despite this, the victimisation from identity crime in Australia and the US is approximately three times more prevalent than in New Zealand. “This is largely to do with the federated nature of these countries,” he explains, “criminals love to swim in the crevices between organisations and jurisdictions.”

However, New Zealand’s natural defence is also its weakness. New Zealand’s size and structure means that it provides a tighter social media and online community where, says David, “a large identity crime event can quickly reverberate across the country.” Taking the Sony Pictures, Target, and Anthem hacks as examples, he continues, “iDcare received calls from clients in New Zealand impacted by all three of those data breaches.”

The organisational response to each of those examples varied dramatically from offering staff and customers services that were already available and free to them, through to acting quickly and identifying the need to build the identity resilience of those at risk. “iDcare is increasingly working with organisations as a key feature of their data breach response processes,” says David. “As can be seen from our data, the first 72 hours matter, and there is a lot that can be done to make an identity unattractive for future misuse.”

For more information on iDcare, visit their website, www.idcare.org

The logo for iDcare, with 'iD' in blue and 'care' in green.

Protect your Identity Don't become an identity theft victim!

According to the Department of Internal Affairs’ website, “identity theft is more likely to occur if you make it easy for someone to take and use your identity information.” It’s a simple message, but it’s one that so many of us take for granted... often to our detriment.

According to the DIA, there are a number of things you can do to protect your identity information:

- Be careful with your identity information, how much you give out and who you share it with.
- If someone asks for your identity information, ask why the organisation or individual needs it, and what they intend to do with it.
- Keep key identity documents (eg. birth certificate and passport) in a secure place.
- Make sure you properly dispose (shred or burn) of bank statements, electricity bills and any piece of correspondence with your name and address on it. Consider receiving these online as opposed to via snail mail.
- Be careful about publishing personal information in public places (eg. date of birth posted on a social networking website).
- Don't log in to internet banking from a shared or public computer, such as an Internet café.
- Remove all personal information from computers before you dispose of them.
- Be suspicious of anything that looks strange, such as unexpected letters from creditors or bank transactions you can't remember making. These could be the result of identity crime.
- Request an access register report from Births, Deaths and Marriages at the DIA. This is a free service that allows people to find out who has applied to access their records since 25 January 2009.
- Request a credit report.

For more information, visit www.dia.govt.nz/Identity---How-to-protect-yourself-from-identity-theft

Advanced crime analytics connect the dots



The application of advanced crime analytics can optimise operations by focussing investigations in areas of most value

Cybercrime, drug smuggling, human trafficking, serious fraud, money laundering and terrorism are often transnational by nature requiring participation from criminals located in different countries. Organised crime gangs also operate across jurisdictions within countries.

For law enforcement agencies, like those in New Zealand, that share information in accordance with international and domestic laws, the challenge is sharing the information contained in different systems to join the data and connect the dots.

The historical approach to combating multijurisdictional crime requires a lot of time and effort to gather information; with detectives individually usually calling multiple police forces in other areas to elicit the necessary information. The alternative method that has proved successful is the establishment of task forces. These teams focus on a specific problem that impacts a range of agencies. They serve as an information

fusion centre, collating information and distributing it as required.

One of the challenges with traditional information systems is that they were not designed to get any information out of the system. This means that often the only way to extract information is via a time consuming manual extraction process.

Wynyard Group, an international market leader in risk management and crime fighting software with offices in New Zealand, has deployed advanced crime analytics for use across jurisdictions through a secure web application. This allows structured and unstructured automatic data feeds from numerous sources including existing evidence and open source data from websites, news feeds, chat rooms, blogs, and social media to be loaded and processed in one location with the analysis and results available elsewhere. Additional data can be manually added to update the model, for example witness statements or the results of investigations and this allows

new relationships to be added to help complete the picture.

Task force investigators can learn about connections and relationships between criminals and suspects. If an investigator was doing this manually back in the old days, there would be a massive whiteboard going through and drawing all these connections. With analytics software agencies are able to quickly search and find those connections they weren't able to see before.

By applying advanced crime analytics technology law enforcement agencies and private investigators can optimise their operations by focussing their efforts where they will get the most value. They can use the system to help prioritise their patrols, plans and budgets. This means that they can solve crimes and prosecute and convict offenders faster and with less resources. They can also develop effective strategies and tactics that help prevent future crimes and this allows the benefits of information sharing and cross border collaboration to continue after the task force is dissolved.

fired up protection

ViTECH

LOKTRONIC's expansive product range has just become even wider with these first class **EGRESS** and **FIRE PROTECTION DEVICES** and **PROTECTIVE COVERS**.



STI-1130 Ref. 720-102
Surface mount with horn and spacer
255mm H x 183mm W x 135mm D

STI-13000-NC Ref. 720-090
Flush mount, no horn
200mm H x 135mm W x 65mm D



STI-13510-NN Ref. 720-092
Surface mount, horn and label optional
200mm H x 135mm W x 100mm D

STI-1100 Ref. 720-054
Flush mount with horn
255mm H x 183mm W x 84mm D



STI-6518 Ref. 720-060
Flush mount, no horn
170mm H x 95mm W x 49mm D

STI-13210-NG Ref. 720-094
Surface mount, horn and label optional
200mm H x 135mm W x 100mm D



All **STI 'Stoppers'** are made of tough, UV stabilised polycarbonate. Many can be supplied with or without a 105 dB horn. Other models and sizes available including weather resistant options.

STI-WRP-R-11 Ref. 720-059R

Resettable call point surface mount, DPDT. Positive activation mimics the feel of breaking glass. Visible warning flag confirms activation. Simple key to reset operating element - no broken glass. **IP 67**



STI-RP-WS-11/CN Ref. 720-052W

Resettable call point surface mount and flush, DPDT. Positive activation mimics the feel of breaking glass. Visible warning flag confirms activation. Simple key to reset operating element - no broken glass.

STI-RP-GF-11/CN Ref. 720-051G

Resettable call point surface mount and flush, DPDT. Positive activation mimics the feel of breaking glass. Visible warning flag (pictured) confirms activation. Simple key to reset operating element - no broken glass.



STI-RP-RS-02/CN Ref. 720-058

Resettable call point surface mount and flush, SPDT. Positive activation mimics the feel of breaking glass. Visible warning flag confirms activation. Simple key to reset operating element - no broken glass.

STI-6255 Ref. 720-042

Mini Theft Stopper discourages inappropriate use of equipment. Sounds a powerful 105 dB warning horn when activated. Tough, ABS construction. Reed switch activation for cabinets and display cases or unique clip activation for freestanding equipment. Does not interfere with use of protected fire fighting equipment. Compact design 85mm H x 85mm W x 25mm D.



STI-6720 Ref. 720-047

Break Glass Stopper. Keys under plexiglas. Protects emergency keys from inappropriate use. Keys remain visible. Fast, easy installation. Simple, inexpensive plexiglas. 3 year guarantee against breakage of the ABS housing within normal use.



Battery Tester Ref. 730-100

ViTech rugged steel case 5, 15 and 30 amp battery tester for fire and alarm use.



Fire Brigade Alarm: (Closed/Open) Ref. 730-201

ViTech branded Type X and Type Y models with temperature compensated pressure transducers with digital display showing pressures for defect, fire and pump start.



Anti-Interference Device

Ref. 730-400 series

ViTech AID for sprinkler valve monitoring; fits all ball valve sizes.



ViTech products are designed 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
mail@loktronic.co.nz www.loktronic.co.nz



International Bodyguard Training Standards now available in New Zealand

Close protection or bodyguard training has always been recognised as 'high end' training courses or qualifications in the security industry. Due to the nature of the risks being managed in these operations, this training needs to sit at the highest level.

"The introduction of a world class standard in New Zealand represents a maturing of the security training industry in this country," says C4 Group Ltd CEO, Chris Lawton.

Internationally recognised certified professional bodyguard training is now available in New Zealand through a joint venture between The Professional Bodyguard Association (PBA), and C4 Group Ltd (C4), New Zealand's leading security training company. PBA is an approved provider of the United Kingdom Security Industry Authority (SIA).

The course delivered in New Zealand is approved by the SIA and accredited by Pearson Education (leading UK awarding body registered with Ofqual).

The Professional Bodyguard Association

The Professional Bodyguard Association is the only legitimate registered United Kingdom non-profit organisations expressly set up to further the profession of bodyguards or close protection operatives as it is often known. In the words of the CEO & President of the Professional Bodyguard Association, Craig Knowles, "the organisation seeks to further the profession, the interests of individuals engaged in the profession, as well as ensuring the public interest is maintained. As a group of people in a learned occupation we are entrusted with ensuring the legitimate practice of the occupation and to protect the public by upholding and maintaining standards of training and ethics in our profession. To achieve this goal we work in tandem with our Affiliated Partners, each a specialist organisation in its own right and renowned for the outstanding reputation for providing excellent service."



ELC

The MOD's Enhanced Learning Credits Scheme (ELC) is an initiative to promote lifelong learning amongst members of the British Armed Forces. The ELC scheme provides financial support in the form of a single up-front payment in each of a maximum of three separate financial years. ELC funding is only available for pursuit of higher level learning, i.e. for courses that result in a nationally recognised qualification at Level three or above on the National Qualifications Framework (NQF) (England and Wales), a Level six or above on the Scottish Credit and Qualifications Framework (SCQF) or, if pursued overseas, an approved international equivalent qualification. In certain circumstances this initiative to promote lifelong learning is available to retired members of the British Armed Forces too.

SIA

The UK Security Industry Authority (SIA) is an independent body reporting to the Home Secretary, set up in 2003 to regulate the security industry. Their initial drive was the compulsory licensing of those working in the security sector, something we are still establishing in New Zealand. **PBA representative in New Zealand** Murray Tume, the PBA Regional Officer in New Zealand has considerable recent experience operating in both Iraq and Afghanistan. Security operators working

in these countries are required to have a recognised qualification in close protection. Many companies stipulate the UK SIA qualification together with an FPOS certification.

C4 Group Ltd

C4 Group Ltd, as the leading security training company in New Zealand has a wealth of experience in delivery of training and international operations in the field of body guarding and close protection. Chief Executive Officer Chris Lawton was heavily involved in training New Zealand Police protection teams during his 20 years' experience in weapons and tactics training. His role as team leader in specialist search teams and time served on the Armed Offenders Squad enhance the knowledge and delivery of high end training. His experience in East Timor,



which included the safe evacuation of United Nation staff and local staff from townships and eventually from East Timor to Darwin, provided real world knowledge of operating in hostile environments.

He has also spent time in the Middle East (Iraq, Jordan, Kuwait), and travelled to various parts of the world managing security operations for super yacht owners and their families.

As an NZQA Private Training Establishment C4 will ensure the standards of training are met for both the SIA as well as for NZQA. Managing Director Kathy Wright says, "We will also be able to award the NZQA unit standard 6530 - Protect Persons At Risk, As a Security Operator. This will establish a standard of training for the New Zealand national market as well as the international scene."

Operating internationally requires a wide set of skills that can differ from job to job. Obviously working as a security operator in Iraq is different to protecting a celebrity or high net-worth family while holidaying on their super yacht. It is essential that the training received is appropriate. The IHCD/FPOS (First Person on Scene Intermediate) qualification is a SIA approved course for emergency medical response and is a compulsory aspect of any training for the SIA approved close protection qualification.

"I have come across some horrific injuries after people were attacked with machetes while I was in East Timor and skills such as FPOS are essential when working in these types of environments. PBA recognises this and embeds it into their courses." says Chris Lawton.

As part of the development team for the new NZQA Emergency Medical Responder qualification Kathy Wright is able to provide an international benchmark against the FPOS course which has been accredited by the Royal Edinburgh College of Surgeons.

Successful course participants will be awarded a BTEC Level 3 certificate for Working As A Close Protection Operative Within The Private Security Industry (QCF) – and BTEC Level 2 award for First Person On The Scene (Intermediate).



For more information check out the websites

**www.c4group.co.nz
www.the-pba.com**

Recognising innovative product excellence in the New Zealand Security Industry



The NZSA is excited to announce that our Conference and Exhibitions 2015 will be held over 3 days being Thursday 19 November, Friday 20 November and Saturday 21 November

The venue this year is the ASB Showground's – 217 Green Lane West, Greenlane, Auckland.

The final day, Saturday 21 November is dedicated specifically to new products, innovations and security solutions which are considered remarkable in their ability to improve security.

Exhibitors are invited to present their latest range of products and solutions to a broad range of potential clients. Speaker sessions will be 45mins which includes question and answer time.

Please note that only exhibitors are invited to present these seminars. This will be on a first come - first serve basis and since we have only 8 sessions available, you need to HURRY and book.

Please invite your customers, colleagues, clients and friends to come along, the sessions are FREE to attend and are open to the general public.

In closing on Saturday, we will present our Innovative Product of the Year Award 2015. This award honours the most outstanding product development achievements in the local security industry. The criteria used to judge this award will be:

- Innovation
- Ease of Use
- Unique advantages
- Value and Impact

We look forward to seeing you at the exhibition.

For further information please contact Kirsty Reid at Kirsty@security.org.nz or call us on (09) 486 0441.



FREAK Show

How the politics of data encryption keeps internet transactions vulnerable to attack

FREAK, or ‘Factoring Attack on RSA-EXPORT Keys’, is the most recently uncovered security flaw threatening millions of Internet users. It affects SSL/TLS protocols used to encrypt data as it is transmitted over the web, putting at risk private information such as passwords, banking and credit card information.

Although it’s actually existed for many years, FREAK was uncovered just a few weeks ago by French researchers at the INRIA computer science lab in Paris. The researchers notified governments and companies around the world as soon as they found it, but it was only made public in early March.

The flaw allows an attacker to intercept HTTPS connections between clients and servers, forcing them to use weakened ‘export-grade’ encryption, which the attacker can break in order to steal or manipulate data. This type of hacking is called a ‘man-in-the middle attack’ and is used to steal and unencrypt what the victim believes is protected, encrypted communications.

Vulnerable browsers include Internet Explorer, Chrome on Mac OS, Chrome on Android, Safari on Mac OS, Safari on iOS, Stock Android Browser, Blackberry Browser and Opera on Mac OS. According to freakattack.com, a University of Michigan research team that tracks the impact of the attack and helps users test whether they’re vulnerable says patches are now available for most of



these browsers but plenty of servers are still at risk.

HTTSP servers that remained vulnerable as of 26th March included 8.5% of those at Alexa Top 1 million domain names (down from 9.6% since 3rd March, and 6.5% of those with browser-trusted certificates (down from 36.7%), among others. Interestingly, 11.8% of all HTTPS servers remained vulnerable (down from 26.3%) at the time of writing.

Chrome for Windows and all modern versions of Firefox are known to be safe. However, even if your browser is safe, some third-party software, such as some anti-virus products and adware

programs, can expose you to the attack by intercepting TLS connections from the browser. If you are using a safe browser, it’s best to assume that you’re vulnerable.

In addition to browsers, many mobile apps and other software products use TLS. These are also potentially vulnerable if they offer RSA_EXPORT cipher suites or rely on unpatched libraries.

How to protect against FREAK

Self-diagnosis is a good first step. Freakattack.com offers an SSL FREAK Check tool and Qualys SSL Labs an SSL Server Test, which can identify FREAK and other security issues.

fire door holding electromagnets



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)



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**



According to the Michigan University researchers, if you run a server you should immediately disable support for TLS export cipher suites. You should also disable other cipher suites that are known to be insecure and enable forward secrecy. They recommend the Mozilla security configuration guide and SSL configuration generator, and testing your configuration with the Qualys SSL Labs SSL Server Test tool.

If you use a browser, they suggest ensuring that you have the most recent version of your browser installed, and check for updates frequently.

If you're a systems administrator or developer, they recommend that you ensure that any TLS libraries you use are up to date. Ensure that your software does not offer export cipher suites, even as a last resort, since they can be exploited even if the TLS library is patched. Google has released an updated version of its Android OS and Chrome browser for OS X to mitigate the vulnerability, and Microsoft has released a Security Advisory that includes a workaround for supported Windows systems.

HTTP Strict Transport Security (HSTS) addresses the threat

Starting with Windows 10, Internet Explorer will allow users to access some websites only over SSL-encrypted connections using the HTTP Strict Transport Security (HSTS) policy. Strangely, it's the last major browser to get support for HSTS. Google Chrome has had HSTS support since 2009, Firefox since 2010, Opera since 2012 and Safari since 2013.

HTTP Strict Transport Security (or HSTS) is a header that allows web servers to require that web browsers and other user agents only interact with it using secure HTTPS connections, not HTTP. Once a browser sees such a header for a website, it will remember the preference and only accept HTTPS connections for that site in the future.

HTTPS, therefore, provides protection against SSL stripping, downgrading and certificate mismatch attacks against secure HTTPS websites by turning encryption failures into failures that can't be bypassed. No more FREAK.

Also, some sites that use HTTPS might load content from third-party servers over plain HTTP. This is known as mixed content and while it's discouraged practice from a security perspective it's nevertheless accepted by browsers. With HSTS enabled, mixed content is no longer allowed.

Backdoors and national security

Back in the early 1990s when SSL was in its infancy, the US maintained a rigorous regime of export controls over encryption systems. In order to sell software outside of the US, companies were required to weaken the strength of encryption keys. For RSA encryption, the maximum allowed key length was 512 bits.

According to Mathew Green, a cryptographer and research professor at Johns Hopkins University, "the 512-bit export grade encryption was a compromise between dumb and dumber." In theory it was designed to ensure that the NSA would have backdoor 'access' to communications, while allowing encryption that was still adequate for commercial use.

Steve Weismann, writing for USA Today, comments that "the reason for this was that the federal government wanted to make it easier for federal intelligence agencies to spy on overseas software users." Following years of rumblings from the technological community, the restrictions were ended, but many software developers continued to use the weaker encryption.

Weismann comments that the discovery and discussion of this security flaw is particularly timely "in the light of FBI Director James Comey's announced desire that software developers should specifically build in backdoors in the security of their products so that intelligence agencies can readily decrypt data for reasons of national security."

The obvious dilemma, writes Weismann, is the risk that if such backdoors are built into the software that we use, "it will not be merely intelligence agencies exploiting these defects in the furtherance of national security, but also the possibility that criminal hackers or foreign countries will do the same thing to the extreme detriment of everyone." And, he states, this is "without even getting into the risk of misuse of these backdoors by our own national security agencies."

According to Keeper Security Senior Network Engineer, Patrick Tiquet, "There is no justification for any secure website to support the RSA export cipher suites, now, or even for the past five years." The justification for doing so has been to maintain compatibility with old clients or browsers that only supported the 512-bit ciphers.

Supporting these ciphers on a website, explains Tiquet, was previously considered 'best-practice' to support the widest number of web browsers possible.

"However, most of those export-cipher-only browsers ceased to exist about 15 years ago," he observes, "when export restrictions on encryption technology were eased by the US Government." A web browser from 2000, he quite rightly states, isn't capable of displaying most content from contemporary websites – so there really is no place for a continued compatibility mentality.

According to Nathaniel Mott of the Pando Daily, FREAK has proven critics of policies of weakening encryption to be right "Misguided laws or restrictions don't just affect people today," he points out, "they create problems which come back to haunt users more than a decade later."

Cold war in cyberspace

The FREAK flaw is a sobering reminder of the extent to which state espionage has shaped and continues to shape cyberspace. Commenting on the timing of the flaw's discovery, Mott writes, "it's fitting that FREAK has been rediscovered as governments around the world, from the United Kingdom and France to China and the US, have sought access to tech products. They want backdoors; they want encryption keys; they want to undermine basic security."

Even more ironic, given the US government's role in the apotheosis of FREAK, are President Barack Obama's vehement criticism and threats against the Chinese government over its proposed anti-terrorism legislation. This legislation will require technology companies operating in China to install special backdoors in their security systems and hand over encryption keys to Beijing.

The draft law stipulates that any tech company operating or selling products in China would be required to give authorities encryption keys and allow back doors for law enforcement to access data. The US fears that exposing companies to this type of access by Beijing will leave their customers personal information and communications open to abuse.

Beijing has been quick to show Washington the mirror, pointing out that the law is not so different from the blocking of Huawei and ZTL's telecommunications products from the US and Europe due to fears of cyber-security exposure. The Chinese state-run newsagency, Xinhua, has quite fittingly used this as an opportunity to say to the Americans: hey, at least we're being open about it!

World leading security research moves offshore because of TICSA

Currently six of New Zealand's universities are submitting their final bids for a share in the 2014 budget's \$28 million worth of new funds for new ICT graduate schools. According to Tertiary Education Minister Steven Joyce, this initiative will connect tertiary education and industry to deliver more of the ICT and cyber-security skills New Zealand needs by lifting the training of our next generation of high-tech professionals.

Potential post-graduates may be wary though, because the Telecommunications (Interception Capability and Security) Act (TICSA), which was put in place under urgency last year, has prevented research and investment into what is arguably the next generation of new technology and one where, until the passage of the Act, New Zealand had a head start.

An article by technology writer Juha Saarinen from a recent edition of NZ Herald says that this country was at the forefront of software defined networking and network functions virtualisations (SDN/NFV) – essentially the technology is the development of virtual internet routers.

However Saarinen says TICSA mandates that telecommunications service providers and public network operators must register with the Government Communications Security Bureau (GCSB) and its sidekick, the National Cyber Security Centre (NCSC).

Furthermore, telcos and network providers must notify the agency which is tasked with upholding the country's IT security if they make significant changes to their networks.

Computer science academics at Victoria University were going to be working on a virtual networking project with US companies including Google. It was an opportunity that arose because the NZ academic research network (REANNZ) had carried out some world leading early investigations. However because of the uncertainties of the TICSA provisions, including fines of up to half a million dollars a day for not complying with the legislation, the potential investors have relocated to Australia.

Another company director has told Saarinen that he is keeping his company turnover below \$10 million per annum

and subscribers below 4,000 “just to avoid dealing with TICSA hassles.”

Software defined networking and network functions virtualisations are going to be a multi-billion dollar industry worldwide in the next few years. They will form part of the infrastructure of the next stage of the internet which is being called ‘the internet of things’.

There are big challenges (including serious additional risks to privacy and of surveillance) as well as huge opportunities as these new technologies develop and an important discussion to be had about what kind of society we want to create. But if the TICSA bill remains unchanged it's not a future that our local researchers and entrepreneurs can take any part in shaping.



Recent Act passed into law under urgency may cost the country its research and security expertise

ADPRO[®] PRO

**Award-Winning
Longest Range
Passive Infrared (PIR)
Detector
in the Industry**



WINNER OF



xtralis
The sooner you know[®]

• Tel. 03 9936 7000 • Email: marketing-apac@xtralis.com

www.xtralis.com

It's Academic

Why the debate between security and privacy in NZ is important yet irrelevant

Surveys shed light on our willingness to accept state snooping of our private data

It was the major 2014 pre-election issue that fizzled: state mass surveillance. Kim Dotcom, Nicky Hager and even a cameo by Edward Snowden had whipped up a frenzied political debate that preoccupied New Zealand for a few brief moments. That same debate turned out to fall curiously short of making any dent on the national election result.

Surely government surveillance of our personal communications – whether legislatively justified or not – is a big issue. Surely we, as citizens, have some quantum of interest in whether the state – and who knows who else – is siphoning our personal communications into a pool of countless other texts, emails and lovingly sent emoticons for possible analysis in relation to who knows what. Apparently not.

New Zealanders, it appears, just don't give a byte about the potential for intrusions – either well intentioned or not – into their personal space. Is it because we just don't have anything to hide? Is it because we've come to view our telecommunications and social media accounts as public space anyway? Or is it because most of us accept that protection from terrorism and enemies of the state are more urgent ends than protection from the state itself?

Surely most of us would find the idea of mass surveillance somewhat irksome, but is there simply an implicit acceptance that it is necessary, or at least better, than the alternative? No one likes the prospect of visiting the dentist for a tooth extraction, but we accept its necessity nevertheless.

And is it just us? Revelations in February that New Zealand was surveilling the communications of our neighbours in the Pacific had all



the ingredients for diplomatic stouch, but there was barely a ripple in the pond. Even Grant Bayldon, Executive Director of Amnesty International NZ, commented in a March New Zealand Herald opinion piece that “News of New Zealand’s mass spying on people in the Pacific is just the latest instalment. But there’s been little real political fallout.”

New Zealanders’ attitudes surveyed

A recent poll, commissioned by Amnesty International, questioned 15,000 people from 13 countries across every continent. It sheds some interesting light on the attitudes of both us and the publics, of NZ’s spying partners on the issue of state mass surveillance. The survey, conducted in early February, included 1,000 respondents from New Zealand.

According to the poll, 63% of surveyed New Zealanders are opposed to the government monitoring and storing

their internet and mobile communications data. By contrast, only 22% supported mass surveillance practices.

53% of respondents disapproved of the use of electronic surveillance technologies being used by New Zealand against other countries. But 43% were comfortable with surveillance against foreigners in New Zealand – as opposed to 40% against.

Interestingly, the survey found that only 7% of people would be less likely to criticise the government on email, private messaging or social media if they knew the government was listening in. More interestingly, it found that 15% indicated they’d be more likely to criticise the government in their private communications.

7% are less likely to criticise the government but 15% are more likely to. Maybe there’s a few of us out there that perhaps view state surveillance as another avenue for the airing of complaints... at least the government’s listening!

On a serious note though, these statistics do not suggest great fear of the surveillance state nor of the prospect of a retaliatory government turning on dissident voices. On the contrary, they suggest that surveillance may actually inspire an emboldening of behaviour against intrusive government rather than a retreat to quiet acquiescence.

In other words, the results appear to indicate that New Zealanders do not see the spectre of domestic state surveillance as impacting on the democratic fabric of our political system. They do not view a 'big brother' scenario as necessarily part of a slippery slope towards totalitarianism or anything resembling that.

Despite our views on mass surveillance, there appears to be a begrudging acceptance of it... perhaps helped along by a popular assumption that more intrusive government snooping doesn't necessarily reflect a weakening of our democracy and the checks and balances that come with it. Tracy Watkins commented in a February Dominion Post op-ed that it's all about trust. "We put our faith in our elected governments to not give agencies like the GCSB or Security Intelligence Service free rein and to understand where we, as a nation, would draw the line at activities conducted in our name."

How well placed is our collective belief in the benevolence of our government and the robustness of our democracy? How well placed is our relatively higher acceptance of surveillance against foreigners? And how do the attitudes of New Zealanders compare in this regard to those of the publics of other countries?

How did we compare internationally?

Across all 13 countries surveyed, there was no majority support for surveillance – only 26% of all respondents agreed that a government should monitor the communications and internet activity of its own citizens. A similar number of respondents overall – 29% - were of the opinion that their government should monitor overseas citizens.

In all surveyed countries, more people were in favour of their government monitoring foreign nationals (45%) than citizens (26%). In some countries those in favour of spying on foreign nationals was more than double that of citizens. In Canada only 23% believed their government should monitor citizens compared with 48% for foreign nationals, and in the US the differential was 20% compared to 50%.

According to Chris Chambers, writing for The Guardian, "These results suggest the presence of a social ingroup bias: surveillance is more acceptable when applied to 'them' but not to 'us'. New Zealanders' 'ingroup bias' wasn't far behind that of Canada and the US, and was significantly higher than that of the likes of the UK, Australia, South Africa, France and the Philippines.

Surveillance doesn't appear to be stifling criticism of governments. In almost all the surveyed countries, most people (60% on average) said that surveillance would not change their tendency to publicly criticise their government. And, interestingly, for those people who indicated that it would change their behaviour, surveillance was usually associated with more criticism rather than less. This pattern was greatest in Brazil, Spain, New Zealand and South Africa.

Negative feedback does not a political movement make

While the survey suggests that a majority of New Zealanders may prefer no government mass surveillance of their personal internet and mobile communications, this clearly hasn't translated electorally. For New

Zealanders and many of the publics questioned in other countries, the survey tells of a clear underlying trust of one's own government, coupled with a relative underlying distrust of foreign governments and foreign nationals.

The reasons for this may be many and complex, but the key question remains: should we care about mass surveillance?

Although the security vs privacy battleground is usually seen as a case of pitting two polar opposites against each other, Grant Bayldon argues that it's not the zero-sum game that we tend to think it is. The security and privacy imperatives can – and should – coexist, providing for settings that balance security measures with assessed threat levels and that provide the checks and controls that characterise a robust democratic political system.

The ongoing debate in New Zealand is important because without it the state is not provided with a gauge of public sentiment on issues that may not ultimately loom large come election time. Democracy is not just about elections, and it is perhaps the debates and sentiments expressed in the three years between them that more truly define us as a democratic country.

KCS TraceME expands Internet of Things era by integrating LoRa™



KCS BV, based in Dordrecht (NL) 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. The module will be available in Q2/2015 and other variants in the high/mid-range and budget-line will follow shortly after.

Please visit www.trace.me for more information.





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 Securitron 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

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

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

20239_PDM



ITRON SECURITY & AUTOMATION



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



IP Video Intercom

- Wide range of single villa to multi-apartment stations options
- Wide range of control panels with/without phone handsets
- 1.3MP camera on station units
- Control panels also capable of communicating with Dahua IP CCTV cameras
- 2 years 2b2 warranty

Distributed by



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



Dahua ultra-smart IPC

- 8xxx series 3MP PoE IP cameras -> full-body box, IR bullet, day/night dome, IR dome models
- Includes smart features such as: regions of interest (RoI), corridor mode, Electronic image stabilization (EIS) & scalable video coding (SVC)
- Includes smart-detection and intelligent analytics features such as: tripwire, intrusion detection, abandoned/missing, scene-change, defocus, facial detection, audio detection etc

Distributed by



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



Dahua PTZ

- Dahua Full-HD (1080P) Network Auto-Tracking IR PTZ Dome Camera with Wiper
- Powerful 30x optical zoom
- Defog, DWDR, Day/Night(ICR), Ultra DNR, EIS, Auto iris, Auto focus
- Max 240°/s pan speed, 360° endless pan rotation
- IR Distance up to 150m

Distributed by



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



(09) 414 5101 OR 0800 ITRONICS

SALES@ITRON.CO.NZ

WWW.ITRON.NZ

Canon VB-S900F Compact Full HD IP Camera



- Best in class low light performance
- Advanced intelligent functions
- Exclusive dual processing power
- ONVIF S compatibility
- H264 multi streaming
- Auto smart shade control
- RM-Lite software

Canon

CRK Professional Precision

Ph: 09 276 3271 • www.crknz.co.nz

Canon VB-S30D Compact Full HD PTZ IP Camera



- Smallest Full HD PTZ on the market
- Best in class low light performance
- Advanced intelligent functions
- Exclusive dual processing power
- ONVIF S compatibility
- H264 multi streaming
- Auto smart shade control
- RM-Lite software

Canon

CRK Professional Precision

Ph: 09 276 3271 • www.crknz.co.nz

Canon VB-H41 Full HD PTZ IP Camera



- Wide angle lens with 20x optical zoom & auto focus
- ONVIF S compatibility
- Class leading low light performance
- On board video analytics
- Exclusive dual processing power
- Image stabilisation
- Auto smart shade control
- Auto day / night capability
- Built-in SD memory card slot
- RM-Lite software

Canon

CRK Professional Precision

Ph: 09 276 3271 • www.crknz.co.nz

National Home Safety Service

Securing homes against the scourge of domestic violence

Domestic violence continues to constitute a major social and law enforcement issue in New Zealand. 33 to 39% of New Zealand women experience physical or sexual violence from an intimate partner in their lifetime. It is one of the leading causes of injury and death to women, and it leads to health problems such as mental illness, and problems with sexual and reproductive health.

Although the Treasury estimates the economic cost of domestic violence to be in the vicinity of \$4 billion annually, other studies estimate the cost to be closer to \$8 billion. Violence within New Zealand families is resulting in an average of 29 deaths every year, up to half of all police time is taken up dealing with domestic violence, and around half of all violent offence charges in the court system relate to domestic violence.

Police commenced around 95,000 family violence investigations last year, an increase of 7,000 on the previous year.

Early March saw the award of the \$3.6 million contract to deliver the Government's National Home Safety Service to the National Collective of Independent Women's Refuges (NCIWR) on behalf of the 41 affiliated member Women's Refuges in partnership with Shakti New Zealand and the Pacific Island Safety and Prevention Project. The contract will commence on July 1.

The service, which will boost security in the homes of domestic violence victims, is the meeting of an election promise to support 400 women and their children escaping violent relationships. According to Justice Minister Amy Adams, who awarded the contract, "too many people continue to be re-victimised, even when a protection order is in place."



Justice Minister Amy Adams (left) and NCIWR representatives at the awarding of the National Home Safety Service contract

A pilot of the service, running in Auckland since 2008 and expanded to Tauranga and Christchurch, provided practical safety measures such as strengthening doors and windows, replacing locks and installing safety alarms. 150 house upgrades were provided each year at a total cost of \$500,000 a year. The pilot saw no reported re-victimisation of participants.

Commenting on the contract win, Women's Refuge acting Chief Executive Cheryl Gibbs said, "We are exceptionally well placed to deliver this service. Not only do we have over 40 years' experience in the domestic and family violence sector in New Zealand, but we also have Refuges throughout the country, offering 24/7 support."

The partnership of NCIWR with Shakti New Zealand and the Pacific Island Safety and Prevention Project provides an opportunity to provide

specialist, expert-led services across the country, which can be tailored so that the services are responsive to cultural needs. It is intended that the approach will effectively integrate domestic violence expertise with culturally appropriate responses for Māori, Pacific and migrant women.

"Within the end-to-end integrated holistic services that this partnership provides, the home safety project will be an integral part of our initiative to keep vulnerable women victims and their children safe", commented Shakti New Zealand Senior Advisor Shila Nair.

"While Women's Refuge is most commonly recognised for our response in emergencies", said Mrs Gibbs, "we do a significant amount of work in our communities focusing on prevention and stopping re-victimisation. This new contract will allow us to do much more in this space."



Move to the secure platform that grows with you.

**Leverage HID Global's extensible iCLASS SE®
Platform to keep your access control optimized,
today and tomorrow.**



With constantly evolving access control concerns and demands, how can you ensure your investments today will be operable tomorrow? Go with the new standard in access control—HID Global's iCLASS SE® Platform, the open and adaptable solution that easily integrates smart cards, mobile devices and whatever tomorrow brings, for greater security and flexibility. Now no matter where technology goes, your access control is always growing with you.

Learn more about the iCLASS® SE Platform's advantages at hidglobal.com or contact us at +613 9809 2892 or email at asiasales@hidglobal.com.

© 2014 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, and iCLASS SE are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission.

HOW SMART IS YOUR COMPANY?

You're (not) smarter than your competitor?

M2M

Machine to Machine and
Internet of Things

LoRa

TraceME can check and update your machines, pumps, systems etc. Worldwide within seconds!

SPECIALIZED IN:

GSM	GPRS	LBS
SMS	GLONASS	GPS
LoRa™	BLE	4G
iBeacon™	RFID	Wi-Fi
M2M	SENSOR	Bluetooth®
EXTREME LOW POWER AND OTHER TECHNIQUES		

One of the biggest Telecom companies on earth is selling and exporting our M2M devices to many branches of industries. Please have a look for more specs at our TraceME website or for examples have a look at www.demo.tv



www.Trace.ME

All trademarks mentioned herein belong to their respective owners