

NzSecurity

ISSN 1175/2149

June / July 2016



SECURING BETTER
qualifications for industry

INSTITUTE TAKES A STAND
against unlicensed investigators

AUTOMOTIVE CYBERSECURITY:
is car hacking really a thing?

www.DefsecMedia.co.nz

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





IPS 10000

SMAVIA Appliance for up to 100 Channels and 36 TB of storage

- The appliance IPS 10000 combines the proven and extended VideoIP software SMAVIA Recording Server with a reliable and high-performance server hardware.
- Best matched components ensure high storage speed and thus allow the recording of up to 100 HD video channels in real-time.
- The integrated RAID 6 storage system already provides a high storage capacity and can be expanded by an external RAID 6 and JBOD system. Thereby this appliance is the optimal recording system for large video installations in Stadiums, Shopping malls, Casinos or Convention Centres.

Storage System

Eight easily accessible HDD bays, RAID 6 storage capacity of 36 TB can be achieved and can be expanded by additional 60 TB.

SeMSy® III Integration

Optimised for SeMSy® III Video Management System.

SMAVIA Viewing Client

View footage over the network. It can be run on any workstation running Windows 7/8/10.

DMVC Server

The integrated DMVC Server Software permits access with the mobile app Dallmeier Mobile Video Center, that is available for iOS or Android operating systems.

Open Platform

Together with the according licenses, third-party network cameras can be recorded with motion detection ONVIF protocol.

Contact Details:

Craig Flint

Telephone: +64 (07) 868 2703

Mobile: +64 (0) 274 597 621

Postal and delivery address:

27 West Cresent

Te Puru 3575

Thames RD5

New Zealand

Email & Internet:

craig@defsecmedia.co.nz

www.defsecmedia.co.nz



www.facebook.com/
defsecmedia/



www.twitter.com/DefsecNZ



www.linkedin.com/company/
defsec-media-limited

Upcoming Issues**August / September 16**

Banking, Insurance and Finance
Loss Prevention, Industry Training.

October / November 16

Conference issue:

Professional & Business. Accountants,
lawyers, managers and consultants

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 Note from the Editor
- 8 Strategies For Success
- 9 Security Industry Awards 2016
- 10 Things seem to be moving along apace at Loktronic
- 12 Trust Mark to set standard for responsible use of biometrics
- 14 Driving Innovation Eyes on Dahua's Complete Range of Solutions
- 18 NZ banknotes awarded for design and security
- 20 Synology Storage & Surveillance management software
- 22 Made in China security robot causes a stir
- 24 NZSA training evaluation result raises questions
- 26 Institute Takes A Stand Against Unlicensed Investigators
- 27 Securing better qualifications for industry
- 28 Excellence in Physical Security: A Human Systems Approach
- 30 Security In The News
- 34 New Zealand to finally get a Computer Emergency Response Team
- 35 Automotive cybersecurity: is car hacking really a thing?
- 36 Australia Round-up
- 38 Showcase

Industry Associations



www.security.org.nz



www.asis.org.nz



www.masterlocksmiths.com.au



www.biometricsinstitute.org



www.nzipi.org.nz



www.skills.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

Innovating for a **smarter, safer world.**

Axis offers a wide portfolio of
intelligent security solutions:



Video encoders



Network cameras



Physical access
control



Network video
recorders



Video management
software



Audio and
accessories

Visit www.axis.com or send an email to
contact-sap@axis.com for more information.

Note from the Editor

Welcome to the June issue of NZ Security. I'm just back from the annual Biometrics Institute's Asia-Pacific Conference in Sydney, where the issue of privacy took centre stage. The ever-present yet evolving need to achieve an acceptable balance between security and privacy is a challenge across the industry, from biometrics to surveillance to cyber security.

Whether or not there are the right legislative safeguards in place to manage this tug 'o' war, fundamental to maintaining public confidence is the idea of trust. Do people have trust in how government – or any organisation – will use their personal information and keep it safe? The Institute's development of a 'privacy trust mark', which we cover in this issue, is a strong example of how industry is working to get on top of this.

A story that will no doubt be read with interest by many within the industry is the piece on the NZSA training division's NZQA External Evaluation and Review (EER) result. The training arm of the Association received a "not yet confident" rating in relation to educational performance, and this has understandably raised some question marks.

To be sure, it's a sub-standard result for an organisation that promotes itself as a standards setter in the industry, but the review took place back in 2014, and the key question now is what's the current state of play. We pose this question – and more – to NZSA CEO Gary Morrison.

Ultimately, there are much bigger questions facing the guarding sector in relation to training. As the reports in our NZ and Australia news round-ups continue to indicate, guards are ill-equipped to manage situations involving violence. Mandatory training does not provide adequate guidance on what to do when a punch is thrown or when a guard is faced with the real threat of unavoidable violence. It's an industry Achilles heel that's begging for proper treatment.

Writing for us in this issue is Jas Qadir, a postgraduate engineering student at AUT. In a thought provoking article, he asks do the policies and work culture of an organisation drive its physical and access security needs? His research suggests an apparent over-emphasis within organisations on the technology of access control to the neglect of enforcing security-minded behavior among employees.

On the cyber security front, we take a look at the NZ Government's announcement of \$22 million for the establishment of a new national Computer Emergency Response Team (CERT) to combat cyber-attacks and cybercrime. It's welcome news, but New Zealand is a very late entrant to the international 'CERT club', and there are plenty of voices claiming that it's a case of "too little too late".

As always, we are very keen to get your feedback. And if you have something to say, we'd like to hear from you.



Nick's professional background is in government and the military. He was posted to Shanghai, Beijing and Suva as a diplomat during a 14-year career with Australia's Department of Immigration and Border Protection, and has also served in the Australian Army's Signals (RASIGS) and Transport (RACT) corps. He holds Masters degrees in Asian Studies and International Relations from the Australian National University and the University of Sydney respectively, and he is a graduate of the Royal Military College of Australia. Nick's research has been published in several peer-reviewed journals and for the Washington-based Jamestown Foundation on international security, cyber conflict and terrorism. His writing has also appeared in international affairs publications including The Diplomat, National Business Review, Global Times and World Policy Institute Blog. His insights are regularly sought via interview by outlets such as CNN and Agence France-Presse (AFP).

www.defsecmedia.co.nz



The World's Largest Supplier of Video Surveillance Products and Solutions

One-Stop-Shop for Your Security Needs

Finding the right solution for your needs is an important decision. Hikvision is a worldwide Leader focused on security and excellence; its products are installed and operating across a broad spectrum of industries, including the City Surveillance, Retail, Banking and Finance, Transportation, Education, Commercial and Residential among others, in over 100 countries and regions. Look to Hikvision to provide end-to-end solutions, no matter what industry you're in.

Address:
1/44 Greenpark Rd,
Penrose, Auckland

W: www.nfs.co.nz
P: 09 580 1576
E: sales@nfs.co.nz

NFS 
NATIONAL FIRE & SECURITY
LOW VOLTAGE ELECTRONIC SUPPLIER

STRATEGIES FOR SUCCESS

2016 EDUCATIONAL SEMINARS & AWARDS DINNER

1.45 to 2.00 Registration

2.00 to 2.45 **Rebecca Cook** – Strategic Solutions to Health and Safety Management

2.45 to 3.00 Break

3.00 to 3.45 **James Yearsley** – Succeeding in the Public Sector

3.45 to 4.00 Afternoon Tea

4.00 to 4.30 **Steve Vermey** – Strategies to create a winning tender

4.30 to 5.00 Networking

6.30 to 11.00 **Awards Dinner** – Recognising Excellence in the Security Industry



REBECCA COOK



JAMES YEARLEY



STEVEN VERMEY

Rebecca has over 15 years' experience in all areas of Human Resources and Health and Safety offering full HR and health and safety services to clients across a range of industries, including telecommunications, retail, manufacturing, banking, construction, IT, seafood exporters and residential care providers. My Health and Safety came about when company founder Rebecca Cook, investigated the online Health & Safety solutions available for businesses and organizations for whom the new Act will have major impact.

Businesses are looking to partner with suppliers who do not present any additional Health and Safety risk. Clients are increasingly looking for evidence that you have a Health and Safety system that exists, is actively used by your people, and is adequately managing the risks. Learn how your investment in Health and Safety can actually help you win jobs, and can be a successful marketing strategy in its own right.

James is a former officer in the British Army with over 20 years experience in security around the world and has served in many locations around the world including operational tours in Afghanistan and Northern Ireland. He has a wealth of experience in security engineering and consultancy including; the risk assessment and design of physical protection measures for facilities and assets; research and development into physical protection measures against various threats; and the instruction and training of risk assessment and security engineering.

James presentation will focus on the PSR and the trend towards a threat driven, risk based and holistic approach to security. In 2012, the New Zealand Government had a number of high profile security breaches. The Information Privacy and Security Programme was a response to these breaches. The PSR sets minimum standards which can be tailored and enhanced to meet the agency risk environment and agencies are able to implement it in a way that is appropriate to their circumstances. It pushes the idea that there is not a 'one size fits all' solution to protective security; it must be designed around risk management principles.

Steve is one of the founding Directors of BMV Solutions and has prepared and reviewed thousands of tenders across the world. Steve has led BMV Solutions to prepare over \$16bn worth of tender submissions with its clients across numerous industries. Steve has a unique ability to analyse requests for tender documentation, lead bid management teams, prepare tender documents and critique submissions for compliance and completeness.

Both Private and Public purchasers have a vested interest in achieving value for money for the goods or services they are procuring. They will also have other key drivers influencing their decision to award a contract. It is the supplier's responsibility to know their potential client, understand how they think and to convince the evaluators of their value for money proposition – generally speaking, this is not done well in industry. The "Strategies to create a winning tender" session will present five key strategies to create winning tenders.

SECURITY INDUSTRY AWARDS 2016

PROUDLY SPONSORED BY THE SKILLS ORGANISATION

RECOGNISING AND CELEBRATING EXCELLENCE AND
OUTSTANDING SERVICE PERFORMANCE IN THE
NEW ZEALAND SECURITY INDUSTRY.

FRIDAY 26 AUGUST 2016, ROTORUA

- 13 AWARDS CATEGORIES
- WORLD CLASS VENUE
- FANTASTIC NETWORKING OPPORTUNITY
- EDUCATIONAL SEMINARS (FRIDAY AFTERNOON)
- ACCOMMODATION & ATTRACTION PACKAGES

For more information and to book your attendance:

Email: nzsa@security.org.nz

Ph: +64 9 486 0441

Fax: + 64 9 486 0442

www.security.org.nz

NEW ZEALAND SECURITY ASSOCIATION



Things seem to be moving along apace at Loktronic

In the last issue we reported on an interview detailing a range of updates and improvements on their flagship range of New Zealand made Loktronic brand electromagnetic locks.

When we spoke with Loktronic this month we were updated on a significant array of just-released improvements in their range of Fire Door Holding electromagnets (FDHs), also made here in New Zealand.

We learned that over the years technicians have frequently asked for various models of the FDH but have not known whether the site was configured for either 12 VDC or 24 VDC, or as sometimes occurs, both. It is not uncommon for products to be ordered without the technician having visited the site, hence the dilemma of which voltage to choose. Usually both voltages would be purchased and the unused version returned at a later stage, involving unbudgeted time and cost.

That set the Loktronic techno-boffins thinking and a new product range has resulted.

New voltage selector

Firstly, the standard FDH40S now incorporates a nifty little PCB where the voltage can be easily selected between 12 or 24 VDC by the repositioning of two small jumpers. Although there are four power wires entering the PCB there are just two, non-polarity sensitive connectors so that wiring errors in the hook up procedure are eliminated.

Secondly, the 12 VDC power consumption has been reduced to a low 110 mA with the 24 VDC remaining at a low 55 mA so that the continuous power draw is minimal. There is no great operating cost here!

Thirdly, an extender PCB with colour-coded cables has been developed to enable the voltage selection option to be maintained when extension tube sets are used thereby avoiding the bunching up

of cables in the base unit of the standard product. Installing technicians will quickly recognise what a real advantage this is.

New Surface and Recess mounted models

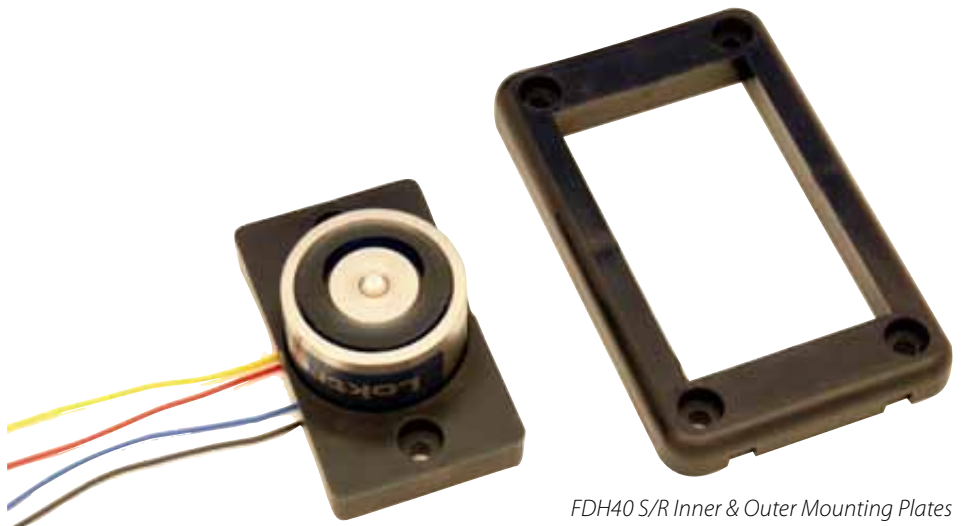
Loktronic have designed a completely new model from a clean sheet of paper, as it were! An unbreakable nylon base plate is made in one piece and is used as supplied for the Surface Mounted option. Responding to demand for optional colours and finishes, Loktronic now offer covering dress plates (escutcheons) in satin aluminium, gloss black or gloss white and these clip over the top of the nylon base plate. As for the FDH40S model, the FDH40S/R incorporates the 12 or 24 VDC selector option.

When Recessed Mounting is desired, the same components are used though with a small modification. The Mounting Plate is separated into two parts by cutting the four joining lugs. The Inner Mounting Plate is used as a template to cut out a matching sized hole in the wall board and is secured to a stud or similar solid point. The Outer Mounting Plate is then positioned over the electromagnet and secured, leaving only the chosen escutcheon to be clipped into place for an easy and attractive professional finish. *Now that's easy!*



FDH40 S/R Surface Mounted in White

In line with other New Zealand made Loktronic brand products, all models are guaranteed against breakage for 10 years. When asked what other product upgrades were in the pipeline we were met with a smile and a wait and see!



FDH40 S/R Inner & Outer Mounting Plates

NZ made

Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

fire door holding electromagnets 12 & 24 VDC selectable



Standard, floor mounted, wall to door distance 114mm



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 & 24 VDC selectable • 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

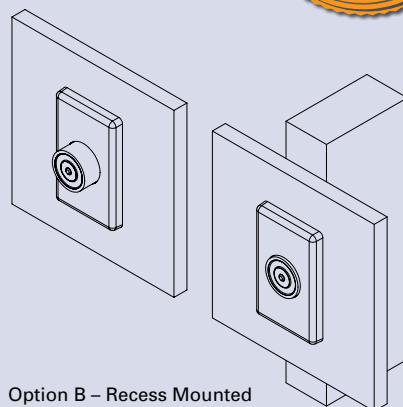
10 YEAR GUARANTEE*

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)



Option A – Surface Mounted



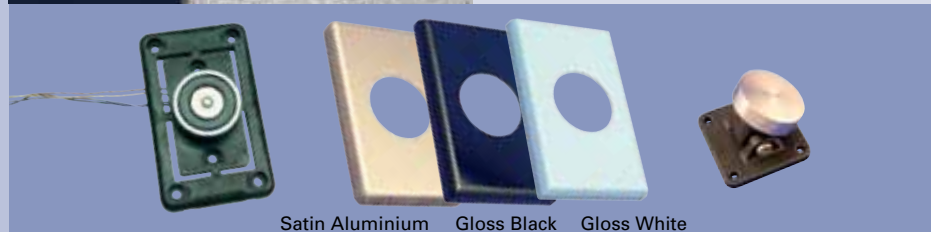
FDH40S/R

Surface and Recess 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 a choice of 3 covers for optimum aesthetic appeal and durability. The installer can utilise one device for surface mounting or for recess mounting.

10 YEAR GUARANTEE*

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



Satin Aluminium Gloss Black Gloss White

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



*Standard terms & conditions of sale apply.

Trust Mark to set standard for responsible use of **biometrics**

To mark Privacy Week 2016 in May, the Biometrics Institute released a Privacy Trust Mark Summary Paper, which provides an update on and next steps for its proposed Privacy Trust Mark. To be issued for a biometric product or service, the proposed trust mark is envisaged as a way to reassure consumers of the responsible use of biometrics and to make privacy compliance easier to understand.

According to a 13 April Biometrics Institute media release, the trust mark project aims to deliver “a mechanism by which businesses can provide assurance to consumers that they meet an accepted standard of good privacy practice and therefore can reasonably protect biometric information collected and/or used.” It is intended to be applicable internationally and be broadly compatible across jurisdictions.

The need for a trust mark appears driven by the rapidly increasing use of biometric systems in sectors beyond government and security, including banking and finance, communications, social media, general business and retail. According to the Institute, there is an increasing call “within the industry as well as by privacy and consumer advocates, for mechanisms to ensure current and future use on biometrics is appropriately and proactively governed.”

“As a peak industry association, we have a key responsibility in educating people about the convenience and security biometrics can offer and in raising awareness of best-practice around the responsible use of biometrics,” stated the Hon Terry Aulich, Head of the Biometrics Institute Privacy Expert Group, in the 13 April media release.

The Privacy Week summary paper gives an overview of the two stages of the project completed to date: stage one, which delivered a feasibility study and roadmap; and stage two, which delivered a self-assessment questionnaire and Privacy Impact Assessment template to be trialed as part of stage three of the project.

The trust mark by stages

It was in October 2014 at its annual show in London that the Institute first announced its intention to develop a Biometrics Institute Trust Mark. In February 2015 it announced that it had awarded a contract to Lockstep Consulting to write a landscape report about the feasibility of a trust mark.

Constituting ‘stage one’ of the project, the landscape report included interviews of more than 20 user and vendor representatives, and concluded that there was strong overall support and appetite for a trust mark, with most stakeholders seeing it as an important way to provide consumers with increased confidence and comfort in the responsible use of biometrics.

The report recommended that a wholly owned subsidiary of the Institute should eventually be established to issue the



Biometric Iris scanning equipment used by the US Marine Corps in Iraq

trust mark and that it must be prepared to police it, address unauthorised use of it, and actively revoke a mark where required. In the longer term, the most respected form of trust mark should be externally audited. In the short term, a self-assessed mark is feasible (if the criteria and substantiating documentation are all public) and it should be piloted.

In August 2015 the Institute received funding from the Australian government to progress the trust mark’s development. The second stage of the project continued with the development of the proposal for an initial self-assessed trust mark that would be augmented by an independent Privacy Impact Assessment, and this was completed in March 2016.

This second stage recommended that self-assessment should be via a questionnaire, with responses required to be substantiated with publically available documentation, and that National Strategy for Trusted Identities in Cyberspace (NSTIC) Fair Information Practice Principles (FIPPs) should form the basis of the trust mark criteria, as they are aligned to most international data protection regulations.

Stage three of the project will involve a small set of trials using the proposed self-assessment criteria to test the viability of the draft questionnaire and evaluation process.

The proposed initial model provides a future pathway to an externally assessed and open standards-based accreditation scheme.

“This project is very exciting as it will help us work out how the process could work later and importantly, what needs to be in place in order to effectively manage and govern such a trust mark” said Isabelle Moeller, the Institute’s Chief Executive. “Several of our members have already expressed an interest in participating in a trial which could potentially lead to the issuance of a pending Trust Mark.”

4K

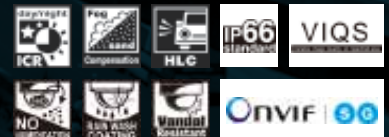
IT'S IN OUR DNA

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



WV-SFV781L VARI-FOCAL CAMERA

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



OUTSTANDING CLARITY

THE PANASONIC VARI-FOCAL OPTICS AND 12MP SENSOR

4K OFFERS IMPROVED CLARITY

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

FALL OFF REDUCED

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

12M PIXEL MODE

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



WWW.PANASONIC.NET/SECURITY

Panasonic

Driving **Innovation** Eyes on **Dahua's** Complete Range of **Solutions**

2015 was a year of success for Dahua Technology, which streamlined its operations, pushed its global branding strategy, expanded research on innovative products and solutions, and explored new areas of business. Due to these efforts, Dahua was able to survive its most difficult period since founding and make a turnaround: last year its total sales were US\$1.6 billion, a growth of 37.45 percent from 2014. Net profit was \$0.22 billion, a growth of 20.1 percent. On a&s's Security 50 list, Dahua's ranking jumped from No. 6 in 2014 to No. 5 last year. Meanwhile, Dahua is continuing its globalization campaign as the company builds more presence in the world. Besides North America, Europe, Dubai and LATAM where Dahua already has subsidiaries, more established subsidiaries and offices in APAC and other regions of the world will begin operation this year.

A Pioneer in Technology

At the end of the day, Dahua is still a technology-driven company that leads the market and appeals to users with its cutting-edge innovations. The company has over 3,000 R&D professionals and devotes 10 percent of its annual sales to research and development, with the goal of developing advanced, high-quality, and reliable solutions for users. In fact, Dahua's commitment to growth and innovation has won the trust of China Development Bank (CDB). On February 17, Dahua and the Zhejiang branch of CDB signed a financial cooperation agreement, with the amount of financing totaling 10 billion RMB (approximately \$1.6 billion) between 2016 and 2021. "We thank CDB's support and approval of Dahua," said Fu Liquan, President of Dahua Technology. "Our signing of the agreement with CDB represents both sides' commitment to



Fu Liquan, President of Dahua Technology

further collaboration, which is sure to help Dahua make a giant leap forward." As for its technology development this year, Dahua will focus on two aspects: HD analog and "true" 4K.



BUILDING SECURITY SOLUTION

One step to smart secured building

- Integrated Video Surveillance, VDP, Access control, Alarm
- Unified/centralized management for all sub-systems to reduce OPEX
- Industry leading design and high reliability
- Customizable and scalable



Video Surveillance



Access Control



Unified Management Platform



Video Intercom



Intrusion & Alarm



Video Surveillance

- Advanced video collecting and analyzing
- Wide coverage w/o blind angle



Access Control

- Various identification method
- Secured and convenient



Intrusion & Alarm

- Linkage between alarm and other system
- Flexible alarm reporting



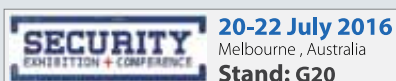
Video Intercom

- Support both IP and Analog
- Exquisite design



Unified Management Platform

- High reliability with low running cost
- Scalable and customizable



CE FC CCC UL ROHS ISO 9001:2000



Add: Unit G 701 Great South Road Penrose
Auckland 1642 New Zealand
E-mail: andrew@swl.co.nz
Web: www.swl.co.nz



DAHUA TECHNOLOGY CO., LTD.

Tel: +86-571-87688883 Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity.com

DAHUA TECHNOLOGY AUSTRALIA PTY LTD

Add: Unit 8, 39 Herbert Street St Leonards, NSW, 2065
E-mail: sales.oc@global.dahuatech.com

A Complete Range of Solutions

Over the years, Dahua technology has not only established itself as a leading video surveillance solutions provider with presence in various parts of the world but also expanded its portfolio. As part of its technology development this year, Dahua will focus on two aspects: HDCVI 3.0 and 'true' 4K.

HDCVI 3.0

As a pioneer in the HD-over-coaxial technology, Dahua rolled out HDCVI back in 2012, a breakthrough technology that delivers HD video — long associated with IP — over the user's existing coaxial cable. After HDCVI 1.0 and 2.0, this year Dahua launched the new generation of HDCVI — HDCVI 3.0 — at ISC West in April. According to Fu, a defining feature of HDCVI 3.0 is the HDCVI 3.0 DVR supports not only HDCVI but also HDTVI and AHD edge devices, a major innovation for users who are no longer limited by the type of camera they can choose.

"For a long time, for the end user choosing a particular HD analog technology, they have to side with a particular alliance. That's no longer the case with HDCVI 3.0," Fu said. "For HDCVI 3.0, we'll add interoperability or multi-mode features into storage. That



means the HDCVI 3.0 DVR supports not only our HDCVI but also other signals, including AHD, TVI, and IPC. For users, it protects their investment, as with our DVR you can choose whatever type of camera based on your own preference or your own use scenario."

But what truly sets HDCVI 3.0 apart from its predecessors is its high-definition and intelligent features. In terms of high definition, the maximum resolution currently supported by analog is 1080p, and HDCVI 3.0 seeks to change that. "For HDCVI 3.0, we'll introduce 4-megapixel





cameras, and research and development work is currently being done on 4K cameras, which we plan to announce in the second half,” Fu said. Further, Dahua will incorporate more intelligent features into HDCVI 3.0. These include facial recognition, people counting, heat mapping, and fisheye-dome smart tracking whereby the user can zoom in and out on an area of interest on a panoramic view. These are features that are otherwise found in IP solutions.

“Dahua believes that high-definition and intelligence should not be reserved for IP only. They should be applied to analog as well,” Fu said. “For the overwhelming existing analog install base, they want extendibility and continuity of their infrastructure. Technology can evolve, but infrastructure can’t be replaced overnight. And for these users, we believe they also have the need for higher resolution and intelligence. That’s what motivated to roll out HDCVI 3.0 and push the HD analog technology forward.” And according to Fu, HD analog is here to stay, and HDCVI 3.0 will even prolong HD analog’s lifecycle. “For the longest time, IP claims to be a superior technology over analog due to its high-definition and

intelligence, and we agreed that these were the defining features of IP,” Fu said. “But with HDCVI 3.0, analog and IP are now on the same footing, and HD analog’s competitiveness will increase. This, plus analog’s usability and simplicity, will make it stay longer.”

“True” 4K

As for Dahua’s IP offerings, it will offer what it calls “true” 4K, rolling out solutions for each part of the video surveillance process, namely image capturing, transmission, storage, and display. At the end of last year, the company already launched a series of 4K cameras including 12-megapixel bullet and IR dome cameras. But a challenge facing customers these days is bandwidth and storage management, amid ultrahigh-resolution images captured by 4K cameras. Compression, therefore, becomes critical.

Dahua uses two approaches to compression: either the equipment is H.265-ready, or it supports Dahua’s own Smart H.264+ technology, which builds upon and optimizes the existing H.264 architecture. The technology uses various algorithms to lower bitrates, one

example being motion-still extraction that extracts the still portion of the image and does more compression to it. “The end result is compression by as much as 70% for still images, as well as 40 to 50% for daylight images with moving objects,” Fu said. Aside from these, Dahua also has 4K display solutions that are especially helpful in city surveillance projects. One example of how this has helped end users is a solution for police in China’s Jiangxi Province, where the police monitoring station comes equipped with a giant TV wall made up of 500 60-inch panels, allowing operators to pinpoint every minute detail shown on the screen. “What we offer is not only the front-end capturing of image, but also everything from transmission to storage to display. This capability to offer true end-to-end 4K solutions is what sets us apart from others,” Fu said. “For our competitors, their end-to-end 4K may cover the frontend and the backend, but to add display ... not a lot of players can do that,” Fu said.

Future Growth

Already with operations in different parts of the world, Dahua also set up professional local teams staffed with local experts who will not only sell our products but also provide further support and service to customers as well as partners. Technology-wise, Dahua will boost its HDCVI offerings, at the same time positioning itself as a true end-to-end 4K solutions provider. Already ranking the world’s second largest market share according to the IHS 2015 report and 5th on a&s’s Security 50, Dahua is set to see continued growth in the years to come.



NZ banknotes awarded for design and security

New Zealand's new five-dollar note - featuring a range of new and enhanced security features – has won the International Bank Note Society's prestigious banknote of the year award. The award recognises outstanding achievement in the design, technical sophistication and security of a banknote or banknote series.

Twenty banknotes from around the world were nominated for the award, and the winner was voted by IBNS members. The IBNS says New Zealand's \$5 note was the competition's "clear winner", with Sweden's 20 Kronor note, Russia's 100 Ruble note, Kazakhstan's 20,000 Tenge note and Scotland's (Clydesdale Bank) 5 Pound polymer note voted the runners-up.

Reserve Bank of New Zealand Deputy Governor Geoff Bascand says the award is testament to the hard work and innovation by RBNZ and its partners that went into developing the note. The upgraded \$5 and \$10 bills went into circulation in October last year, packed with security features designed to make spotting fraudulent banknotes easier than before and to maintain NZ's strong track record against counterfeiting.

"We are proud of all of New Zealand's new banknotes, but to have our \$5 note recognised internationally is very special," said Mr Bascand. "The note incorporates some of the world's most advanced security features, yet still beautifully showcases New Zealand's history, culture and heritage."

Although it is a New Zealand note, it was actually designed and printed by the Canadian Banknote Company (CBN). Established in 1897 to supply security-printed products to the Canadian government, CBN manufactures a range of documents and systems that are common targets of counterfeiters and fraudsters, including currency, birth certificates, driver's licenses, Id cards, passports, postage stamps and lottery systems.

In recent years, CBN has also supplied machine readable passports used within Caribbean Community (CARICOM)



New Zealand's new - and award-winning - \$5 note

countries. The CARICOM common passport regime has been lauded as promoting easy travel within the Caribbean Single Market and Economy (CSME).

Since New Zealand's current banknotes were first issued in 1999, security features and the technology for designing and printing banknotes have all advanced considerably. And while counterfeiting rates here in New Zealand are low compared to the rest of the world, the Reserve Banks stresses the need to stay one step ahead of the game.

To give industry time to prepare for the new banknotes, they have been rolled out in two phases: (i) \$5 and \$10 notes were released from October 2015; and (ii) \$20, \$50 and \$100 notes were released from April. As the existing notes pass through the cash handling process, they will be replaced with the new series. RBNZ anticipates it will take up to 18 months for all of the existing series to be rotated out of circulation.

The new notes bring with them a number of new and updated features that will help people identify legitimate notes, including:

- A larger clear window features a more detailed holographic metallic element
- The native bird icon changes colour as the note is tilted, and a 'rolling bar' can be seen moving through the space
- A small 'puzzle number' lines up to form a numeral when the note is held up to the light
- Raised ink is still used on the large denomination number.

On its 'Brighter Money' website, the RBNZ provides guidance on what to do if you've been handed a note you think does not have all the security features.



The Bank says it's important to avoid handling it (so the police can trace the counterfeiter). "Either refuse to accept the note or store it in a bag or envelope, then inform the police immediately."

The RBNZ suggests the following steps when dealing with a suspicious note:

- Make sure you are familiar with the security features. It's easy to quickly check the colour changing features in the windows when accepting a banknote.
- If you are a cash handler, make sure you are familiar with your company's procedures for handling suspect and counterfeit banknotes.
- Please check all notes that you receive.
- If you suspect a note may be counterfeit, compare it with a genuine one. Use the RBNZ's guide for checking your banknotes if you need help. Make sure you are familiar with the security features of the previous polymer banknotes.
- If you haven't accepted the banknote yet, politely refuse to accept it.
- Under no circumstances should you take actions that may jeopardise your safety or that of others.
- Report to the Police that someone potentially attempted to pass a counterfeit note.
- If you are in possession of a suspect note, store the note safely and handle it as little as possible. Note all relevant details such as date, time and place of receipt, car registration number and whether you have CCTV.
- Please hand suspect notes to the Police as soon as possible.

**For further information, contact:
The RBNZ at rbnz-info@rbnz.govt.nz
or visit their website:
<http://rbnz.govt.nz/>**

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 179mm W x 135mm D

STI-13000-NC Ref. 720-090
Flush mount, no horn
206mm H x 137mm W x 69mm D



STI-13B10-NW Ref. 720-092
Surface mount, horn and label optional
206mm H x 137mm W x 103mm D

STI-1100 Ref. 720-054
Flush mount with horn
255mm H x 179mm W x 86mm D



STI-6518 Ref. 720-060
Flush mount, no horn
165mm H x 105mm W x 49mm D

STI-13210-NG Ref. 720-094
Surface mount, horn and label optional
206mm H x 137mm W x 103mm 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-WRP2-RED-11 IP67
Ref. 720-062R
Also available in White.



STI-RP-WS-11/CN
Ref. 720-052V
Available in White, Green, Blue & Yellow.



STI-RP-GF-11/CN
Ref. 720-051G
Available in White, Green, Blue & Yellow.



STI-RP-RS-02/CI
Ref. 720-058
Cover included.
Flush Mount Available.

- Approved to EN54-11
- **Current Rating:** 3 Amps @ 12-24V DC, 3 Amps @ 125-250V AC
- **Material:** Polycarbonate
- Comes with Clear Cover
- 2 x SPDT switches
- Positive activation that mimics the feel of breaking glass.
- Visible warning flag confirms activation.
- Simple polycarbonate key to reset operating element - no broken glass.
- **Dimensions:** 87mm Length x 87mm Width x 23mm Depth (Flush Mount) & 58mm Depth (Surface Mount)

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. 730-101
VITECH, strong, lightweight aluminum case, 5, 15 and 30 amp battery tester for fire and alarm use. Weight: 500gms, Size: 165mm x 90 x 70mm.



Fire Brigade Alarm: (Closed/Open) Ref. 730-202
VITECH branded Type X and Type Y (illustrated) 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



Synology talks **storage** and **surveillance**

Synology, along with authorised distributor VST NZ Ltd, recently hosted their 2016 Auckland storage workshop. The Sky City Conference Centre event was the latest in a series of workshops, following hot on the heels of similar events in Sydney, Melbourne and Brisbane.

Synology has long been a well known name in the IT and surveillance industry, boasting the number one NAS box in the industry and the award winning DiskStation Manager (DSM) data storage platform. Found on every NAS, this powerful intuitive web-based system also comes with free surveillance management software that allows the user to manage the IP cameras in their network.

It's a well-established trend: IP camera solutions are becoming more popular and more affordable. With the switch to IP solutions and higher resolution cameras there are ever increasing demands on storage. To add to this, we're also witnessing unprecedented demand for management software with intelligent video analysis.

With big storage and software being what it does best, Synology appears to have the Surveillance side well and truly covered – for projects big and small.

From small retail to big corporate

DSM's Surveillance Station provides a simple plug and play solution, which supports over 4300 models of IP cameras from 90 brands, giving the user the ability to integrate with their existing solution or to choose the camera they desire. With easy to use cross-platform software support, recorded and live footage can be managed and played back via a browser-based interface.

The DS Cam smart phone application allows for footage to be viewed from anywhere for easy remote access.

DSM's live view feature supports a 64 channel live view feed at 720p and a wide range of intelligent video analytical features that can send the exact kind of alerts or locate the exact footage needed in a flash. It also has 'action rules' and I/O module integration that effectively provides an automated surveillance system. Tasks can be automated to be carried out when a predefined event occurs, reducing the need for human intervention.

Pay as you grow solution

The Central Management system (CMS) capability provides an easy to scale up solution, allowing users to expand their surveillance capabilities. Starting small, the user can add more Synology



Synology storage workshop recently held in Auckland's Sky City

NAS to their deployment as the need arises. This allows the user to pay as they grow and split resources and data to different units, but still monitor and manage video feeds and cameras as well as receiving notifications on a single screen. Even for massive architecture with hundreds of cameras, everything is unified and readily available.

Finding and playing back footage on a large deployment can be painful and time consuming, and this is when DSM's Smart Search features really come in handy. With Smart Search, the user is able to track any change during their IP camera's watch time, and customize search parameters to narrow down a search to avoid false alarms.

Alerts can be set for motion detection, camera occlusion, missing objects, lost objects, foreign objects, and for objects that stay in the camera's no-idle zone for over a set period of time. Utilising the Timeline panel, a user can select a date and time and then play back recordings and from up to 64 channels concurrently or non-concurrently. With on-screen tools, customizable layouts, and many other features, events can be pinpointed with relative ease.



The Central Management system enables you to "Pay as you grow"

As one accumulates an enormous amount of recordings from multiple cameras over time, Surveillance Station provides tools that allow the user to manage their recordings and to choose what can be deleted or archived.

Simple to use, cutting edge technology

Solutions with all the bells and whistles are sometimes either too good to be true or require a PhD degree to operate, but the Synology Surveillance Station 7.2 comes with a GUI befitting even the most technologically challenged user. Easy to setup and not demanding in-depth product knowledge, it minimises the learning curve by providing well defined functions.

On the administration side, remote setup can be established allowing the user to interface via web browser.

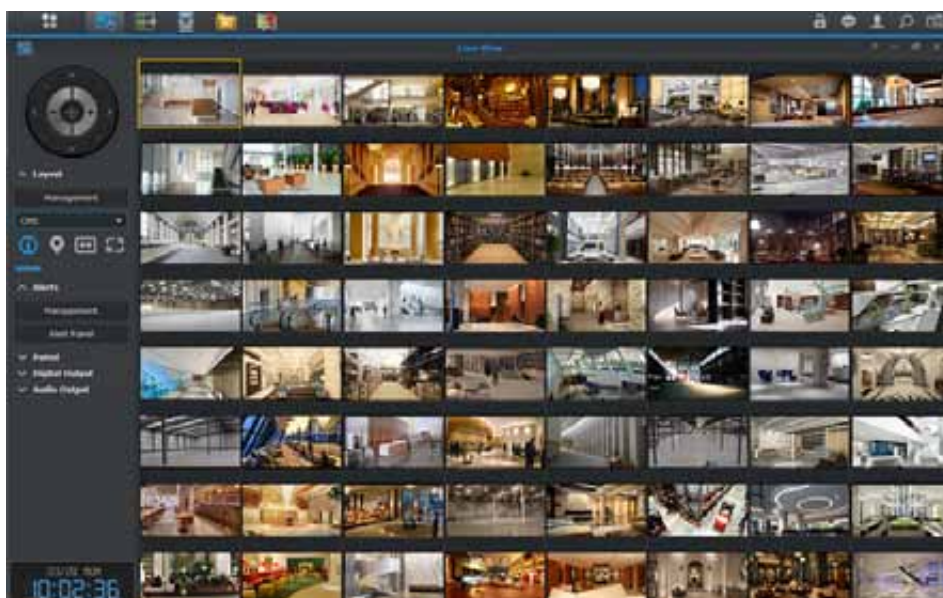
All Synology units come with free periodic updates that you can download manually or automatically, so staying up to date with the latest Synology software features is hassle free and has no price tag.

I already have my own VMS or surveillance software

Adopting a Synology doesn't mean that you have to discard your current surveillance system. With the coming of age of HD recording, the demand on storage has increased dramatically, and one has to consider a range of potential issues, including stress on hard disks due to excessive heat and vibration.

Synology has that all covered. Ranging from a 1 to 180 bay solution, they have overcome some of the most demanding storage challenges of data protection and overheating. With a NAS unit as core, the system supports SMB/CIFS, AFP and NFS protocols, allowing the system to be mounted easily to a surveillance server.

Synology also supports iSCSI protocol, affording the ability to setup an iSCSI target and mount it on a server with



The award winning data storage platform DiskStation Manager (DSM)

ease. Synology NAS systems support the automated RAID management system, Synology Hybrid RAID (SHR), giving you the benefit of easily upgrading your hard drives when more disk space is required.

With the ability to scale up by equipping expansion chassis on some models, running out of storage space is a worry of the past. The folk at Synology recommend running at maximum capacity and maximum bandwidth using Link Aggregation, which is supported by most Synology units.

Protect your surveillance footage with Synology

Rather than focusing on surveillance applications, the Sky City workshop was more squarely focused on storage, providing insight to new innovations that provide market leading data replication, disaster recovery and business continuity solutions.

Synology has a comprehensive backup solution to ensure data safety. With the new DiskStation Manager 6.0, released in March, users can benefit from the new Hyper Backup and Snapshot Replication

features, which provide the capability to back up data to another Synology unit either on or off site.

Hyper backup is an advanced feature that supports the ability to back up the Synology NAS to different types of destinations such as other Rsync servers or public clouds, so that the user can choose a strategy best suited to their needs. This feature also has a cross-version de-duplication capability to minimise storage usage.

Snapshot replication is another beneficial feature that is designed to help replicate data to another Synology unit every five minutes. This feature provides a super efficient way to back up data offsite, so that when disaster strikes you can regain access to the data within minutes.

The specs are impressive, and one can visit www.synology.com to check them out. What they amount to is a system that allows businesses to start with a lower upfront cost and to scale up storage capacity as requirements grow, all the while investing less time on storage management. As such, it's a compelling package.

Synology boasts the number one "Network-attached storage" in the industry



Made in China

security robot causes a stir

Built by the National Defence University in China and promoted on social media by the Chinese Communist Party mouth piece People's Daily Online, news of China's new "intelligent security robot" has been received with widespread concern by netizens in the West. Considering international trends in the robotisation of security, is such roundly negative reaction actually justified or is it just a case of pananoid China bashing?

Unveiled at the 12th Chongqing Hi-Tech Fair in April, the robot is 1.49 metres tall and weighs 78 kilograms. It claims a top speed of 18 kilometres per hour and an operating duration of eight hours

between charges, and is equipped with a remotely operated "electrically charged riot control tool" and an SOS button for people to notify police.

It has been dubbed 'AnBot', a transliteration of the Chinese 'an' (security) and 'bao' (to protect). The researchers say that the robot is designed to be used to patrol airports, train stations, shopping malls, hotels, banks, government buildings, warehouses and port facilities. It has already undergone test runs at a military camp, airport and museum in the inland Chinese city of Changsha with "very positive" user feedback.

According to the People's Daily Online, "AnBot represents a series of breakthroughs in key technologies including low-cost autonomous navigation and intelligent video analysis, which will play an important role in enhancing the country's anti-terrorism and anti-riot measures."

The report states that AnBot is able to patrol autonomously and "protect against violence or unrest."

According to a report by Xinhua, China's state newsagency, "Wei Quansheng, an officer from Beijing Municipal Public Security Bureau, said the robot guard can be used in many





public places such as airports, stations and subways to help with police officers' anti-riot missions."

Despite its immense size, Communist Party-ruled China is one of the most internally surveilled countries on earth. Party organs operate from the national level all the way down to individual neighbourhoods, streets and workplaces, and a collection of security services that are either government run or controlled combine to make China an unrivalled police state. In cyberspace, the infamous 'Great firewall' epitomizes the extent of surveillance and censorship in the People's Republic.

It is, however, a police state that has faced tough security challenges in recent years, with increasing worker and social unrest and frequent mass demonstrations arising from a range of collective frustrations. Resentment over growing inequalities in wealth and opportunity, environmental problems, government corruption, forced evictions and failed petitions, gangster activity and personal disputes, has fuelled the trend.

Taser-enabled police robot slammed

It is perhaps the mention of its playing a role in China's "anti-riot and anti terrorism measures" and protecting against "unrest" that has caused a number of international commentators to raise alarm bells over the new robot. Social media users have been quick to liken AnBot to Dr Who's Daleks, Robocop's ED-209 and other cinematic icons of mechanised dystopia.

Frances Eve, a researcher at NGO China Human Rights Defenders, is quoted by CNBS as commenting "Continued political interference in China's law

enforcement bodies leads to the real worry that these robots could quickly become an Orwellian surveillance tool deployed against the population."

But there is also concern that such robots could be used by an authoritarian state for the carrying out of violence that would otherwise be beyond the pale for flesh and blood security officers. And such concerns are not altogether misplaced.

In its infamously bloody suppression of Tiananmen Square activists in June 1989, the central government in Beijing resorted to trucking in military personnel from distant provinces to mow down unarmed members of the public. The deployment of mechanised security officers would take this one step further by removing the humanity element altogether and ensuring officer compliance.

The People's Daily Online news site tweeted a photo of the robot, which was then shared by American intelligence whistleblower Edward Snowden with the caption: "Surely this will end well".

Popular Science's website covered the story under the headline 'China's new security Dalek is a bad idea', also published under license in Business Insider as 'China debuts this awful taser-armed police robot'.

Rather than expressing concern over the possible state uses of the machines, many social media users saw the lighter side. According to Hong Kong Free Press, Chinese netizens have been quick to cast ridicule on the new robot: "Poor people can no longer even get the security job available," said one. "I don't believe it. Try and catch me, catch me! Do you know how to go down staircases?" said another.

Is the criticism fair?

The release of security robots over the years has kept us both entertained and enthralled. It's now been a decade since Secom developed the Robot X, a six-wheeled outdoor surveillance robot designed to be either remotely controlled or pre-programmed to chase intruders, take high definition video pictures, issue loud warnings and release a dense, billowing cloud of smoke to frighten off the bad guys.

2012 saw the release of South Korea's Robo-Guard, a five-foot tall robot designed to patrol prisons on thick rubber wheels and equipped with cameras, including 3D, a microphone and speaker, and software designed to evaluate and report on out-of-the-ordinary inmate behaviour.

In comparisons of AnBot to actual existing security robots, it is the Knightscope K5 that it is said to most closely resemble. As reported in February's NZ Security Magazine, the five-foot tall, 300-pound security robot has been turning heads on the streets of Silicon Valley since 2014, and was received in the media with largely positive curiosity.

The aesthetic similarities of the two robots are clear, but it's what's under their respective hoods that makes them markedly different. According to Popular Science, "K-5 is a mobile sensor platform that actually shares its data with the general public during emergencies. Anbot, on the other hand, can interact with the public, respond on scene to crimes, and has weapons to knock out human troublemakers."

Previous security robots have offered little more than a deterrent effect to would-be perpetrators of crime. The AnBot takes things to an altogether new level due to two of its characteristics – the first one technical, the other policy. Firstly, it introduces an offensive capability through an electric – presumably taser-like – weapon. Secondly, it is the first security robot intended to perform anti-terror, anti-riot and anti-unrest functions.

AnBot fails to overcome the well-documented limitations of existing security robots, including the inability to negotiate a wide range of terrain and weather scenarios, and as such its role remains limited to very little beyond providing a prototype for what is possible. Ultimately, however, it is the robot's very role as such a prototype that makes the AnBot a most justified object of dystopian discomfort.

NZSA training evaluation result raises questions

By Nick Dynon

In an NZQA Report of External Evaluation and Review of February 2015, NZSA's Training Division received a 'Not Yet Confident in educational performance' result. It's a surprising result for an organisation that describes itself as having "taken a leading role in raising the quality of training being offered across the industry."

But before the alarm bells start ringing, it's worthwhile noting that the result was based on the performance of the NZSA's Training Division during 2014. EERs occur around once every four years, so it's a long time between reviews and it should also be noted that the EER result for the NZSA's Training Division was "Confident in capability for self-assessment".

One would assume that things have moved on since then and that issues have been addressed, but the result nevertheless poses questions of an organisation accredited for delivering Mandatory Training (unit standards 27360, 27361, 27364), National Certificate in Security Level 2 (LCP1, LCP2), National Certificate in Security Level 3.



Gary Morrison NZSA CEO

NZQA external evaluation and review

The New Zealand Qualifications Authority (NZQA) is responsible for managing the NZ Qualifications Framework in order to ensure that kiwi qualifications are regarded as credible and robust. As part of this, the Authority is responsible for ensuring that tertiary education organisations continue to comply with "statutory policies and criteria after initial programme approval and accreditation and/or registration is granted." It achieves this via the external evaluation and review (EER) regime.

According to the NZQA's website, each EER "provides an independent judgement of the educational performance and capability in self-assessment of all non-university tertiary education organisations (TEOs)." By 'educational performance', what NZQA means is "the extent to which the educational outcomes achieved by the TEO represent quality and value for learners and the wider community."

NZQA reports its judgements as one of four levels of confidence: Highly Confident, Confident, Not Yet Confident and Not Confident. So, how is it that the NZSA Training Division received its 'Not Yet Confident in educational performance' result, and what does it mean? NZ Security Magazine spoke with NZSA CEO Gary Morrison to find out.

EER findings valid... but no longer valid?

"The NZSA places a very high focus on raising standards across all areas of the security industry and including the content and delivery of training to industry," said Mr Morrison. "We do accept that having the NZSA Training Division receive an assessment of "not yet confident in educational performance" from the EER is not a good look, however we stress that

the assessment was conducted in early 2015 and using data from 2014, and the issues raised at the time have all been addressed."

In relation to unit standard 27364, the EER noted NZQA's concern over "questions marked as correct but the answer is incorrect' and vice versa" – instances that the NZSA's own moderation processes had identified. Although it is to NZSA's credit that it had itself picked up these errors, their existence clearly raised question marks.

According to NZSA, the inaccuracies can be attributed to having to contract temporary instructors/facilitators to meet the massive surge in demand for mandatory training in 2014. "The NZSA has always been transparent with its moderation processes and had become aware through its own moderation that several assessors employed on a temporary contract basis in 2014 were not consistently meeting required standards", stated Mr Morrison.

The NZSA provided further coaching and training to these assessors, but eventually terminated their contracts due to ongoing performance concerns. According to Mr Morrison, since 2015 all assessments have either been conducted at a senior management level or subjected to a 100 percent verification process by senior staff.

"We also note that the Skills Organisation has stated within the same external post-assessment moderation visit report that NZQA refers to regarding the 27364 results that "Your assessors are following best assessment practice and the NZSA has robust internal quality assurance procedures in place," he said.

No time to manage training?

In its findings, NZQA noted that NZSA training directors/managers "were heavily involved in frontline training delivery and



- 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

www.allegion.co.nz



ALLEGION

lacked the time, capacity and resources to manage and reflect on training management and operations.”

This, it suggested, was the likely reason behind areas of concern that included the NZSA’s lack of a policy to support priority trainees as identified by the government, the abovementioned assessment errors, and that the association was “yet to enhance its information systems and further harness the value of the qualitative data it collects.”

Mr Morrison doesn’t agree with this statement. “Whilst the NZSA does not necessarily accept the validity of this statement,” he stated, “subsequent structural changes within the organisation have ensured that this is no longer a concern. We also note that the NZQA found NZSA’s capability in self-assessment effective and that the association is moving in a positive direction”.

The structural changes he refers to include the full integration of the NZSA Training Division into the organisation from a previous model that had it operating “as a stand alone entity within the Association and without the ability to call upon other resources as and when required.”

Addressing EER recommendations

In conclusion, the EER presented a number of recommendations, including that the NZSA consider how it can contribute (and demonstrate its contribution) to the government’s Tertiary Education Strategy, especially in relation to priority trainees [Maori, Pasifika] which is required of all training providers regardless of their source of funding.

Mr Morrison stressed that the NZSA has always acknowledged and supported the government’s Tertiary Education Strategy and especially in relation to its dealings with priority trainees. “It is important to note that the NZQA were looking solely at the Mandatory Training, and that is an area that is set by regulation that we cannot change, but we do strive to give all learners the best

Mr Morrison stressed that the NZSA has always acknowledged and supported the government’s Tertiary Education Strategy and especially in relation to its dealings with priority trainees.

possible opportunity to meet the required standard. As an Association we ensure that our programmes are reflective of New Zealand’s cultural and ethnic diversity”.

He also confirmed that the NZSA had addressed the EER’s recommendation that the association “explore ways to analyse its quantitative data, identify trends and use the findings to inform continuous improvement decisions.” In

2015, he said the NZSA implemented a new student management software package that has enabled it “to produce a range of reports that support the identification of trends and continuous business improvement.”

Invited to make general comment on the issue, Mr Morrison told NZ Security Magazine that at both a CEO and board level, the NZSA’s leadership has “utmost confidence in the current state of the NZSA Training Division and in our ability to achieve an improved assessment in future external evaluation reviews.”

“Over the last eighteen months we have made significant changes to the structure of the training division and implemented system and process changes that have provided improved quality and business controls. We are also very confident that ongoing Skills Organisation moderation assessments will continue to identify that we operate to best practice standards and that our processes and procedures are robust and appropriate.”

To be fair, the EER identified a whole bunch of things that the NZSA was doing well. The report, in reality, is littered with “Adequate” and “Good” ratings, with a good deal of positive comments throughout.

“As the peak body of the security industry,” states the report, “NZSA is leading a lot of changes in the sector, particularly in advocating a cultural change so that training and qualifications are valued. This is not a simple mission. The association has good representation on the Targeted Review of Qualifications and appears well prepared for designing new programmes that lead to the replacement New Zealand qualifications when the time arrives.”

Institute Takes A **Stand** Against Unlicensed Investigators

by Ron McQuilter, New Zealand Institute of Private Investigators Chairman

In May it was reported in the media “Private Investigators escape prosecution for working without a licence”. Read the article here <http://www.stuff.co.nz/business/79602896/private-investigators-escape-prosecution-for-working-without-a-licence> Typically, we again see the actions of a few individuals tarnishing the good work done by the majority of professional investigators.

The case in point related to an individual who put forward a defence that he was not a usual private investigator but a “specialist” carrying out “scientific” work in relation to crash and fire insurance claims and that he could have simply been an “assessor”. Yet, it was obvious to everyone that his conduct, investigating claims, interviewing claimants, taking recorded statements, creating scene reconstructions, etc is actually duties of an insurance claims investigator, an insurance assessor quantifies the loss.

Compounding this matter was the fact the investigator had been touting for work and been instructed by AMI Insurance on a domestic fire related claim, with a supporting background of having attended a 1 week course in fire investigation. The investigator had even joined the Fire Investigators Association although the president Ken Leggat said “Most fire investigators completed a range of qualifications that did enable them to claim they were professionally trained, but

the course at Charles Sturt was not one of them”. It is not known what other fire qualifications the investigator has. When the insured complained to the insurer and then decided to take legal action, the recorded statements he had provided in support of his claim to the investigator got erased. The upshot was that the insurer got slammed and had to pay the insured – see the article here <http://www.stuff.co.nz/business/money/6753517/10-000-payout-over-AMIs-failures>

So the question remains, why did this individual escape prosecution and why has no-one been prosecuted since the new laws were introduced in April 2011? Licensing of Private Investigators in New Zealand first came into force in the 1974 PISG Act. Under the old Act the Registrar could only deal with licensed private investigators, anyone acting without a licence had to be investigated by the Police. The new Act commencing 2011 was supposed to rectify this anomaly with the Department of Internal Affairs tasked to hold to account both licensed and unlicensed operators. In the case above, it is reported that the DIA recommended the individual be prosecuted but the chief investigator decided to hold off to “encourage compliance” That is all very well, but what about those that have properly jumped through all the licensing hoops and paid their fees for years.



Ron McQuilter, CFE is Managing Director of Paragon New Zealand now based in Tauranga and can be contacted by email ron.mcquilter@paragonnz.com

Just what message are the DIA sending in a profession that is entirely based on a person’s ability to know the law. Investigating an insured’s claim is not to be taken lightly and if you cannot work out you are breaking the law yourself by being there in the first place, how can you possibly expect to achieve any sort of proper outcome for all sides.

In closing regarding the above case, it is truly remarkable to read that in these times, an insurance company such as AMI opted to instruct an unlicensed investigator given their knowledge of the Privacy Act and their obligations relating to the conduct of their agents.

To be accepted as a member of NZIPI a private investigator must agree their application is copied to every other member and that the committee encourages feedback, the applicant must also agree to a credit check being performed and any other relevant enquiry, plus they must provide evidence of their PI licence or COA. Our members agree to work to a Code of Ethics giving the public reassurance they are dealing with an accredited and accepted professional investigator.

NZIPI has strived for over 30 years to support a strong licensing regime and proper conduct in our profession. It is disappointing to read media such as that above.



Securing **better qualifications** for industry

by Wayne Abel

It is crucial that workers in any industry have access to a range of nationally recognised qualifications covering the latest standards. To this end, The Skills Organisation has been busy over the past couple of years reviewing the qualifications available to those in the security sector.

The targeted review of qualifications (TRoQ) for this industry commenced in early 2014. This involved a Sector Review Group – consisting of industry, associations, subject matter experts, the ITO (The Skills Organisation), and training providers – proposing a potential suite of qualifications.

This suite covers a broad span of security qualifications, including both certificates and diplomas ranging from levels 3 to 6.

What can employers expect?

The main outcome from this review is likely to be a simplified qualification structure, with a graduate profile that

indicates what security graduates are expected to 'be, know, and do'.

These qualifications should also equip employees with skills that can be transferred across a wide range of security contexts, with only 'top up' training required to fill in job-specific skill sets.

Where are we now?

The proposed suite of qualifications has been approved by NZQA to commence development. Meanwhile, the Sector Review Group has been tasked with further developing details around the qualification to ensure they are what the industry requires.

The next steps are for the Sector Review Group to critique these draft qualifications, and once this is completed, they will be posted on The Skills Organisation website, where the public will be invited to submit feedback over a two-week period.

When this process is completed, the qualifications will be resubmitted

to NZQA. Once accepted, they will be finalised and published on the New Zealand Qualifications Framework.

The Skills Organisation anticipates that this process will be completed by September 2016.

It is important to also note that the qualification itself is not a training programme. Going forward, training providers will need to develop programmes that can meet the requirements of the graduate profile.

This may be done through unit standards, provider modules, or a mixture of the two, depending on what the training provider wants to do. Part of NZQA's reasons for such a substantial change in qualification development was to provide more flexible training and delivery methods for qualifications.

The Skills Organisation looks forward to the qualification being finalised, and invites the industry to submit their ideas and feedback regarding its development.

Wayne Abel



Achieve long term business success

Invest in workplace training

skills.

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

Excellence in Physical Security: A Human Systems Approach

Jas Qadir, a Masters in Engineering Project Management candidate at AUT University, asks do the policies/work culture of an organisation drive its physical and access security needs? This article draws from his research.

We all have, at least once, propped open doors for house staff carrying cups of coffee as a matter of courtesy in our workplace. We have also propped doors open for colleagues in the work place who might have forgotten their access cards at home. These innocent acts of courtesy – and other very human and seemingly harmless practices – can, of course, be exploited and result in breaches of security.



Masters in Engineering Project Management candidate at AUT University, Jas Qadir

In other cases, we have security systems in our workplaces that generate ‘goal conflicts’ between the security practices and productivity levels demanded. Such systems effectively force staff to abandon or to interfere with the system in order to meet targets. Again, this opens opportunities for either casual or planned incursion.

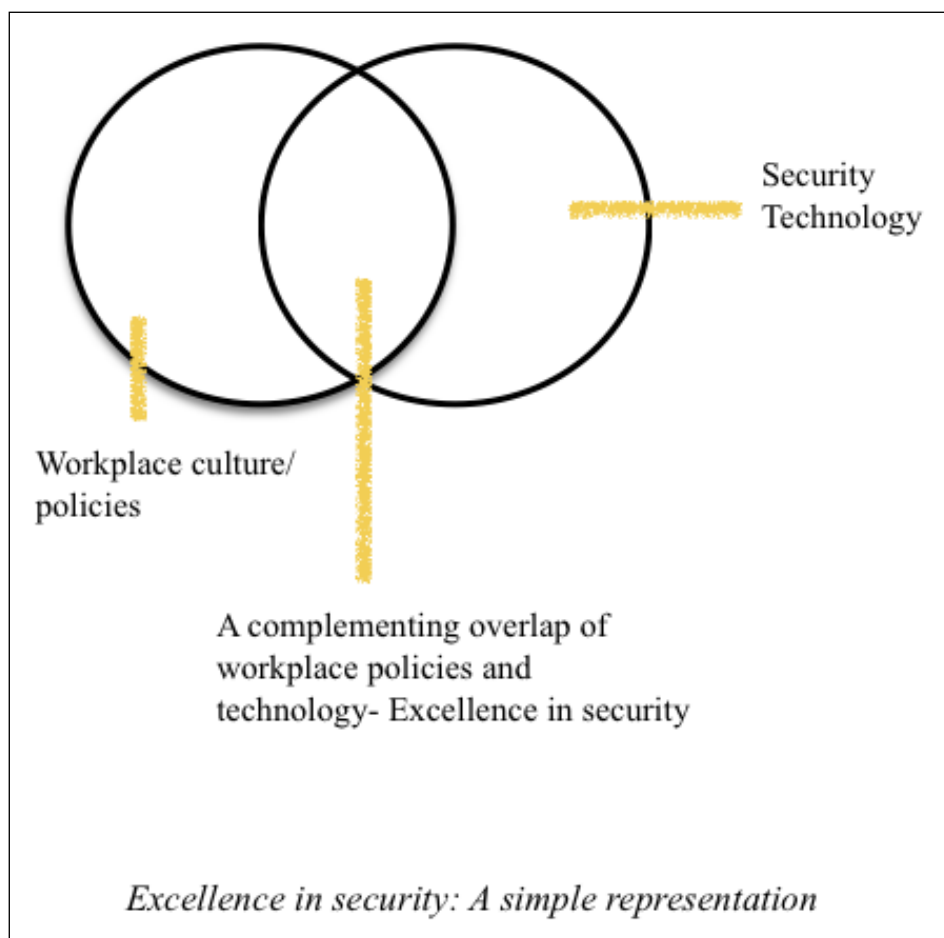
As part of my Masters in Engineering Project Management degree at AUT, I decided to look at the ways in which these potential breaches occurred, and to find out what we can do about avoiding them. My approach was to firstly look at the internationally published research on this, and then to talk to people in New Zealand workplaces to see if the same problems and solutions were suggested locally.

I was surprised to find that according to the published research, physical security is compromised more often by people taking advantage of an employee’s trusting nature than through hacking of technology. Such breaches are also more common than breaches by computer virus or systems breakdown. The data collected within NZ supported this, with tailgating and piggybacking of colleagues and visitors to workplaces noted as the most common forms of compromise.

Participants in the study suggested that in comparison to overseas countries they detected an overly complacent approach here: the “we are safe and secure” New Zealand attitude. The study findings suggest a culture among employees in NZ that is too tolerant of unauthorised entry into premises and the creation of multiple identities in access systems’ databases.

I was also surprised to find that employees struggled with their workplace’s security policies and found it uncomfortable to ask security related questions to their colleagues on matters such as mandatory ID compliance. The goal conflicts created in these situations were due to the ‘authority gradient variation’ or cultural conflict involved, ie. the discomfort felt in the thought of challenging colleagues for their identification or their purpose for entering the premises.

The research has shown that in many workplaces, the people responsible for security place a higher importance on technology rather than on ensuring the implementation of appropriate security policies in the workplace. Further research has also shown that there is an absence of critical “third-party” perspectives that can assess the security requirements of an organisation based



on the work culture and accordingly find the technological solution required. This means that opportunities to identify cost and time efficiencies are lost.

Global research on best practices has also shown that technological access control methods such as access cards and biometric scanners are increasingly effective when the culture and policies of a workplace can successfully integrate with them.

So what can we do about it? There appears to be three major areas where extra focus could reap rewards:

1. Design process – The people who actually operate physical security systems are the real experts about what is practical and sustainable. These subject matter experts can assist in a number of ways, for example by identifying high risk / high pressure scenarios where the system will be most severely tested. These scenarios can then be used in trial simulations.
2. Prioritisation and channelling of resources, and measuring improvements – Many security systems become discredited in the eyes of the users because it is apparent that the organisation has abandoned attempts to control the

more difficult problems and is simply enforcing the easy rules. To break this cycle, it has to be possible to measure the impact of interventions, the changes made to try and improve security performance in key areas.

3. Organisational learning and systematic continual improvement – No technology-based system lasts forever, but neither should they be left to degrade to laughable levels of leakiness before they are replaced.

The consequences of physical security breaches can be monumental, in terms of loss of life, revenue, clients and/or reputation. The answer does not lie in technology alone, but in pragmatic and constantly evolving human-systems security integration.

As the next step towards completing his Masters in Engineering Project Management at AUT, from July 2016 Jas is keen to move into a role that allows him to continue to develop his understanding of the market and its emerging opportunities. He is looking forward to working with industry experts to make security management efficient.

Jas can be contacted on 022 391 2198 or at jas.qtk@gmail.com.

GREAT NEWS!

**NZ'S
finest
electromagnetic
locks
are now
possibly the
world's
best
with our...**

4

**point
2016
upgrade.**

**Simply
the best!**

**Buy Loktronic.
Made in New Zealand.**

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

21516

Security In The News

Advanced Security Group acquires Concord Security

Nationwide security integrator Advanced Security Group has acquired Concord Security. "We continue to invest in the security sector," said CEO Mike Marr, "and the Concord Security business reinforces several of our existing geographic regions."

Brian Fleming, Concord Security MD said he is very pleased to see the amalgamation of Concord Security and its staff into the Advanced Security Group, and that it will provide added opportunities ahead.

Advanced Security is New Zealand's largest dedicated corporate and industrial electronic security provider, with a range of corporate and government clients and supported by 13 branches across the country. This latest acquisition follows six others, including South Island integrator Struthers Electronics & Security in late 2014 and Systems.Com in 2010.

"We must be located where our customers are and we will continue to reinforce existing Advanced Security branches as well as establishing new branches around New Zealand," said Mr Marr.

Concord was founded in 1976 and operates across the Auckland, Waikato, and Bay of Plenty regions. Founded in 2002, Advanced Security continues to maintain an average growth rate of 30 percent per annum.

Northlanders asked to review firearm security after burglaries

According to a 26 April Fuseworks Media report, Northland Police are reminding firearms licence holders to review their security, regardless of their remote location, after three separate burglaries involving stolen firearms over one weekend in late April.

Between Sunday 24th and Monday 25th April, four shotguns were stolen from a Ruawai property. The report noted that the firearms were brand new and not stored securely.

Between Friday 22nd and the following Monday, three firearms and ammunition were stolen from a gun-safe

at a Ruatangata West property, and two air rifles were also stolen from a Mangawhai property, the air rifles had been stored behind an office door.

As well as the obvious concerns about unsecured firearms being stolen by criminals, if license holders fail to secure them they run the risk of having their licence revoked" said Snr Sgt John Fagan, Prevention Manager, Whangarei/Kaipara Police.

Public attitudes to data sharing cautious but shifting

According to a recent report by UMR Research Ltd, approximately two-thirds (65%) of New Zealanders continue to be concerned about privacy. This result is statistically unchanged from previous surveys in 2014 and 2012. The public opinion survey, commissioned by the

Privacy Commissioner, was released to mark the beginning of Privacy Week.

Nearly half of New Zealanders (46%) are more concerned about individual privacy issues over the last few years. This was particularly so for young people aged 18-29 years (55% more concerned), and those with university education (55%). "This sort of result tells us that we need to revisit the perceived wisdom that is out there about how younger people view privacy," said Privacy Commissioner John Edwards.

A large majority of respondents (75-81%) were concerned about issues related to identity theft, credit card and banking details, businesses sharing personal information and security of information.

Respondents expressed a decreased level of concern about the way government (59% concerned) and health organisations (47% concerned) are sharing information. This represents a decrease of 8% and 6% from 2014 respectively.



In a new part of the survey, respondents were asked about their attitudes to personal data being shared between organisations. A majority (62%) felt “We should not share data as the risks to people’s privacy and security outweighs the benefits”, while 38% had a view closer to “We should share all the data we can because it benefits the services and me.”

Significantly, respondents were more open to data sharing when safeguards were put in place. A majority were willing to share data as long as they could opt out if they chose (57%); there were strict controls on who can access the data and how it is used (59%), and data is anonymised and they couldn’t be identified (61%).

NDS provides pedaling guards for Hatea Loop

Early on the morning of 6th May, security guard Josh Rapata patrolled Whangarei’s Hatea Loop on bicycle. It was the first daily two-wheeled patrol of the loop by Whangarei-based Northern Districts Security (NDS).

At the behest of the initiative’s instigator, general manager Jean-Pierre Dignon, NDS employees will cycle the

Loop regularly in an attempt to make people feel safe after an attack on a young female jogger the preceding Friday.

“We are so proud to announce our latest patrol. NDS wants to “Give back” to our community,” stated a post on NDS’ Facebook page just hours after the initial patrol. The post has been ‘liked’ by 2,600 social media users and shared 1,113 times so far.

The 113 comments elicited by the post were overwhelmingly positive: “Awesome idea hopefully there will be patrols after dark? Because that is the most dangerous time”, stated one; “Cameras be good too. Is such a shame it has come to this tho”, stated another. “Needed and appreciated. Bicycle patrols are quick, effective and inexpensive,” commented another thankful local.

Police Station security to be reviewed

According to the NZ Herald, Police announced in April that 105 stations have been identified as needing increased security following an attack on a volunteer manning a public counter in Counties-Manukau. It is also in the wake of an



Northern Districts Security

May 6 at 8:27am · 🌐

We are so proud to announce our latest patrol. NDS wants to "Give back" to our community. Meet Josh. Josh wants you to take back the loop. We'll be patrolling the loop daily, Can we get a "like" and a "share" for Josh ?
#takebacktheloop #looppatrol #givingback #Whangarei



👍 Like 💬 Comment ➦ Share

Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

your
electromagnetic
lock

**UPGRADE
DETAIL**

1

The 6 mm **wider armature** allows for a greater margin of misalignment in the vertical plane. PLUS, the MBS will not falsely report misalignments.

Standard features include:

- Field-selectable 12 & 24 VDC options
- 550 kg holding force
- Slimline styling
- Instant release
- Stainless steel fitting hardware
- Through hardened, polished stainless sex nut
- Full protection against transients.
- Door Position Switch
- End-to-end Magnetic Bond Sensor

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

21516

incident where a man fired shots inside the Palmerston North police station in August last year and a more recent attack on a police officer at the Hamilton police station.

“Acting Assistant Commissioner District Operations Bruce Bird said tonight that the exact locations will not be revealed for operational reasons,” stated the 21st April report. Police confirmed a nationwide initiative to improve station security would include immediate security improvements for 105 smaller stations.

Assistant Commissioner Allan Boreham said potential security improvements may include issuing staff with safety alarms and adding more CCTV cameras. Police also announced some volunteer-staffed kiosks have been temporarily closed and will remain so until the completion of a more comprehensive audit.

According to the Herald, independent sources and Labour MP and Auckland Mayoral candidate Phil Goff, several Auckland City, Counties-Manukau and Waitakere police stations are due to be closed as a result of the review. Police Minister Judith Collins and the police have spoken out against such claims, saying they are incorrect.

Win for council contract cleaners and security guards

In a 16 May media release, the union E tū's has congratulated the Wellington City Council for “sticking to its guns” and securing the Living Wage for its contracted cleaning and security staff.

This follows talks between the council and the Chamber of Commerce which in March agreed to drop legal action related to implementing the Living Wage for its contract staff. Last week the Chamber met with the Council to discuss its threat to seek a judicial review of the council's decision to pay the Living Wage to contract workers.

E tū's Assistant National Secretary, John Ryall says the result entailed the Chamber agreeing that remaining contracts for this year would provide the Living Wage to contractors.

The increase is effective from 1st of July, and will mean a big pay rise for about 15 security guards and around 20 cleaners. “This is a marvellous victory that's been a long time coming,” said Mr Ryall. “It means a pay rise of about 25 per cent for these workers.”

Police drop bouncer assault charge

In a 7 May report in Queenstown's Mountain Scene, Police have dropped an assault charge against the daughter of an election candidate – more than 18 months after the incident.

“Zoe Veint, 22, was accused of repeatedly punching a bouncer who was restraining her boyfriend Nathan Proctor at 1.30am in Searle Lane on 20th September 2014,” stated the report. “Later that morning, her father, James Veint stood on the Ban 1080 Party ticket.”

Mr Proctor's arm was broken in a scuffle after he had left a bar of his own accord despite initially refusing to leave. He was jointly charged with assaulting bouncer Neil Kirk. Mr Veint told Mountain Scene at the time that the two attending bouncers had been “heavy-handed”, but Allied Security boss Ed Stott denied this.

No assault charges were laid against security staff. Both Mr Proctor and Ms Veint pleaded not guilty.

Police withdrew the charge against Ms Veint and downgraded the charge against Mr Proctor to disorderly behavior, having taken into account the level of the charge, the costs involved and the likelihood of a conviction.

Mr Proctor admitted disorderly behaviour and was fined \$500.

Z Energy faces violent robbery epidemic

A 13 May Radio NZ report has described an “epidemic” of highly-orchestrated and violent robberies that have targeted Z Energy service stations in Auckland. The company says its workers have been victims of a number of robberies involving ram raids and sledge hammers.

Chief executive Mike Bennetts stated that Z Energy is now elevating its security protocols, upgrading hardware and posting security guards on their sites at night.

This news comes just under two months after Z announced it was rolling out licence plate recognition software to keep its sites, staff and customers safe.

The 19 February news item published on Z's website stated that the licence plate recognition software is the latest in a string of state-of-the-art security measures implemented by the company, which include smoke cannons, SelectaDNA mist and an \$8 million digital CCTV network on each site.

“This technology, coupled with Z's cutting edge digital CCTV technology, is already making a huge difference on Z sites, particularly in preventing ‘drive-offs’ which cost Z around \$1.5 million per year,” said Z's General Manager of Retail, Mark Forsyth.





“When we identify a vehicle involved in a drive off, the number plate is captured in the system and if that vehicle comes onto any Z site again, the technology immediately recognises the plate, focuses cameras on the vehicle and driver and turns the pump on to pre-pay, preventing the vehicle from filling up without paying.

“Additionally, the quality footage we now get through this software and digital CCTV aids the police in identifying people and increases the odds of catching them. Already in this pilot we’ve reduced drive-offs by up to 80 per cent at some sites,” he said.

Mr Forsyth said Z had partnered with Auror, an Auckland-based company developing an innovative crime prevention platform, and Focus Digital Security, an implementer of ANPR technology, to deliver this solution across the country.

He said that the three companies were also working on applying the technology so that if a stolen vehicle comes onto a Z site an automatic alert is sent directly to Police alerting them to the vehicle’s location. “We want to get the message out loud and clear that we’re not going to stand for anything that makes our sites, our staff or our customers unsafe,” he said.

The ‘epidemic’ of recent violent robberies suggests that this message hasn’t yet made its way to Auckland’s organised crime community.

Spike in weapon seizures at Christchurch courts

Radio NZ reported on 24th April that more weapons are seized outside Christchurch courts than anywhere else in New Zealand, “yet there will be no security report on the city’s new justice precinct.”

According to the report, about 45 percent of the weapons seized at courts last year were from Christchurch. “There were 39 weapons, mostly knives, seized outside Christchurch courts last year, 45 percent of the national total,” it stated. This constituted three times as many as was seized in Auckland, Waitakere and Manukau courts combined.

Despite these statistics, documents revealing the seizures obtained through the Official Information Act, also showed that the Ministry of Justice did not have a security report prepared into its new Christchurch precinct.

“A ministry spokesperson said the new justice and emergency services precinct’s design had taken into account the threats facing each of the agencies that would use it, including the courts,” stated the report.

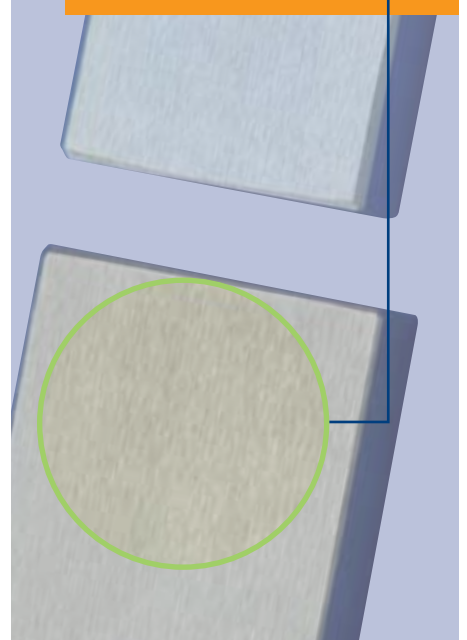
Of the 100 or so weapons seized by security at New Zealand courts last year, 95 percent were knives. Air pistols, a tomahawk and a crossbow have also been discovered by court security.

Loktronic
SECURITY • TECHNOLOGY • RELIABILITY

your
electromagnetic
lock

**UPGRADE
DETAIL 2**

Unightly galvanic action on plates is eliminated through BOTH Electromagnet and Armature being **Electroless Nickel Plated.**



Options include:

- 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

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 21516

New Zealand to **finally** get a **Computer Emergency Response Team**

The Government has announced that it will invest \$20 million of operating funding over the next four years on a new national Computer Emergency Response Team (CERT) to combat cyber-attacks and cybercrime, with an additional \$2.2 million of capital for set up.

A CERT is an organisation that receives cyber incident reports, tracks cyber security incidents or attacks, and provides advice and alerts to its customers on how to respond and prevent further attacks. CERTs also work closely with international counterparts to prevent and respond to cybersecurity incidents, and address cybercrime.

Over 100 countries already have CERTs, and Australia's has been operating for more than two decades. The recent CERT announcement is widely seen as a case of New Zealand joining the CERT club very late in the piece.

"Establishing a national CERT means New Zealand joins an international network of CERTs, improving our access to information on potential or real-time cyber-attacks. It will help us play our part in a global effort to improve internet

security," stated Communications Minister Amy Adams.

"Our national CERT will be a key piece of New Zealand's cyber security architecture. It will be the central place for businesses and organisations to go to for help and information when they're experiencing cyber-attacks," said Ms Adams. The CERT also becomes a core part of the government's Cyber Security Strategy and Action Plan launched last December.

With cybercrime having cost the New Zealand economy \$257 million and having affected more than 856,000 New Zealanders in 2015, the CERT announcement has been broadly welcomed by industry. There are differing views, however, on whether the government's preference towards an optional – rather than mandatory – regime for the reporting of cyber breaches by organisations is the right approach.

Symantec's technology strategist, Mark Shaw, for example, was cited in a recent Interest.co.nz article as saying "the CERT is toothless without it being mandatory for organisations to report significant cyber security breaches." He is not alone.



The Hon Amy Adams, Minister for Justice, recently announced the new CERT

Minister Adams has also announced the creation of an Advisory Board to advise her on setting up the CERT.

"There is substantial experience in cyber security in the private and non-government sectors – and I intend to tap into that as CERT NZ will not reach its full potential without a strong voice representing our private sector guiding its establishment and operation," she said.

"We know from our international partners that that involvement of the private sector is critical to success of the CERT."

The Board will have up to nine members, constituted by a mix of cyber security experts from the private and public sectors. It will provide advice on the establishment, operation and longer-term organisational form of the CERT and the transition to it. The Board will also be expected to build strong links with the CERT's key customers.

The CERT will initially be established as a separate unit in the Ministry of Business, Innovation and Employment and is expected to commence operations in the first quarter of 2017.



Automotive cybersecurity: is car hacking really a thing?

NZ Security Magazine's June 2015 issue carried a story about US-based whistleblower and IT expert Chris Roberts, who allegedly manipulated an airliner's engines mid-air by hacking into onboard systems via the in-flight entertainment unit ("High wiring: the man who hacked a plane"). The FBI took Mr Roberts' claims very seriously, and since then have also turned their attention to emerging concerns over car hacking.

In a Public Service Announcement (PSA) issued on 17th March, the FBI officially bought into the emerging issue of car hacking, confirming that security researchers evaluating automotive cybersecurity were able to demonstrate remote exploits of motor vehicles. "The analysis demonstrated the researchers could gain significant control over vehicle functions remotely by exploiting wireless communications vulnerabilities."

The PSA cited an August 2015 whitepaper in which researchers were able to accomplish a number of vehicle function manipulations, including: engine shutdown, brake disabling and steering (in a target vehicle travelling at 5-10 mph); and door locking, turn indicating, and tachometer, radio, HVAC and GPS operation (in a vehicle at any speed).

In another 2015 case, researchers Charlie Miller and Chris Valasek were able to control a Jeep Cherokee remotely from kilometers away by exploiting the car's entertainment system, which was connected to the mobile data network. The pair were able to fiddle with the vehicle's air conditioning, transmission, and even its steering controls. Following this, Fiat Chrysler launched a safety recall of 1.4 million recent model cars deemed vulnerable to remote exploit.

Automotive hacking, we are being told, is a natural consequence of cars becoming 'connected'. While connected

cars offer innovative features and services, such as keyless entry, ignition control, tire pressure monitoring, diagnostic, navigation, and entertainment systems, there is a potential downside. According to Argus Cybersecurity, "these new features also increase vehicles' cyber attack surface, so the more sophisticated modern cars become, the more vulnerable they are to cyber attacks."

In late April, two bills were sponsored into the Michigan senate that would regulate that state's emerging connected and autonomous vehicle industry. Under the proposed legislation it would become a felony to "intentionally access or cause access to be made to an electronic system of a motor vehicle to willfully destroy, damage, impair, alter or gain unauthorised control of the motor vehicle." Transgressors could face up to life in prison.

Such jail time may seem excessive, but, after all, we are talking Michigan, home to the 'Motor City' of Detroit, the headquarters of the US automotive industry and the home of General Motors, Chrysler and the Ford Motor Company.

But not everyone's convinced that car hacking poses a real threat. According to tech journalist David Pogue in a recent article in Scientific American, it generally takes expert teams several months to successfully hack into a vehicle. "Here's the simple truth. No hacker has ever taken remote control of a stranger's car. Not once. It's extraordinarily difficult to do. It takes teams working full-time to find a way to do it," he wrote.

Chris Valasek, the expert hacker who was part of the team that eventually pulled off the Jeep Cherokee hack, told CNBC, "I'm more afraid of someone texting and driving and running into me than I am of someone hacking my car."



Is it really possible that a car hack could do this?

Loktronic
SECURITY • TECHNOLOGY • RELIABILITY

your
electromagnetic
lock

**UPGRADE
DETAIL 3**

Dislodging of the
Door Position Switch
is now almost
impossible through
the **flexible** (non-rigid)
fastening technique
adopted.

Standard features include:

- Field-selectable 12 & 24 VDC options
- 550 kg holding force
- Slimline styling
- Instant release
- Stainless steel fitting hardware
- Through hardened, polished stainless sex nut
- Full protection against transients.
- Door Position Switch
- End-to-end Magnetic Bond Sensor

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

21516

Australia Round-up

Australian security personnel in fatal Baghdad shooting

According to a Nine News report, former Australian soldier Sun McKay is in custody at a military base in Baghdad after a fatal shooting at the Australian Embassy in Iraq. The victim, 34-year-old fellow Unity Resources Group employee Chris Betz, was fatally shot in the head.

Foreign Minister Julie Bishop refused to comment on the incident, saying that an investigation is being conducted. She did, however, state that the death was not related to the broader security situation in Baghdad.

Unity Resources Group, a Dubai-based Australian security company, is contracted by the Australian Government to guard the embassy. The purpose-built facility, situated in the city's 'green zone', was initially guarded by ADF troops but with the withdrawal of Australian forces from Iraq, URG was hired to provide security. Many of URG's personnel are former Australian special forces soldiers.

The provision of security at Australian embassies is big business. In February 2015, the Sydney Morning Herald reported that the Australian government had spent more than a quarter of a billion dollars on private military contractors to protect high risk diplomatic posts.

According to the report, two private military companies had earned more than \$237 million dollars for guarding Australia's Kabul and Baghdad embassies and providing "close personal protection" for Australian diplomats in Afghanistan and Iraq over a five-year period. Another \$26 million had been committed to security and guarding services over 2014-16 for the Australian High Commission in Port Moresby.

Australia's Cyber Security Strategy

According to a 21 April prime ministerial media release, the Australian Government's Cyber Security Strategy will deliver improved cyber security through 33 new initiatives, funded by over \$230 million directly resulting in more than 100 new cyber security jobs.

The investment complements the \$400 million over the next decade - and roughly

800 specialist jobs – committed by the government to improve Defence's cyber and intelligence capabilities through the 2016 Defence White Paper.

"If we are to fully realise the social, economic and strategic benefits of being online, we must ensure the Internet continues to be governed by those who use it—not dominated by governments," Mr Turnbull said. "Equally, however, we cannot allow cyberspace to become a lawless domain. The private sector and government sector both have vital roles to play."

Among the strategy's initiatives is the relocation of the Australian Cyber Security Centre from the ASIO building in Canberra to make it more accessible to the private sector. The details of the new location have not been disclosed.

\$30m will be deployed to build a Cyber Security Growth Centre with the private sector to coordinate a national cyber security innovation network. Another \$47m will be spent to establish joint intelligence sharing centres in state capitals.

A combined \$41m is also being allocated to enhance the capabilities of Australia's Computer Emergency Response Team (CERT Australia) and recruit more cyber security specialists to the ranks of the AFP, Crime Commission, and Australian Signals Directorate.

Woman urinated on at festival criticises 'patronising' security response

A woman who claims she was urinated on during the 'Groovin the Moo' music festival in Canberra has criticised the response of security guards. According to a 27 April ABC News report, she said she had received a "patronising" and "inadequate" response from security guards after she was urinated on by a man who was "drunk or high".

The woman was sitting with her children at the festival when she sensed a man behind her. She turned to discover that the man had urinated on her. Eventually she was approached by security who took the man away.

She then noticed a group of guards laughing and patting the man prior to letting him walk away. She approached

them only to be told by one of the guards, "if you don't shut up you'll be chucked out". She also accused a female security officer of telling her that she was "at fault" for bringing her children to the event.

Ms Perkins also tried to involve a police officer at the festival, but was told unless she wanted to lay charges against the man, it was not a police matter. She said she planned to file a formal complaint with the security company and had filed a complaint to police about their duty of care.

Australian Capital Territory police confirmed they had received a complaint about an officer's conduct, and said police had provided advice to Ms Perkins on how to make a complaint against the security officers at the festival. Festival security provider ISEC declined to comment on the incident.

Perth man allegedly bashed by security in Bali

A 33-year-old said he was attacked at around 1am on 2 April while partying at Sky Garden Nightclub in Bali with a friend. The man has since returned to Australia after undergoing surgery in Bali to have surgery performed on his skull and broken nose.

According to a 20 April report in WA Today, an off-duty freelance Australian cameraman claimed he had found the injured man "covered in blood and beaten to a pulp" near the notorious nightclub. Still dazed from the attack, the Perth man told the cameraman he had been attacked by nightclub security guards.

"I've just seen one of my mates getting beaten up, I don't know what for, I tried sticking up for him," the man said. "It didn't work out very much in my favour because there were at least 12 guys and they just took me down and then they handcuffed me and beat the shit out of me."

Sky Garden denied in a statement on Wednesday that its security guards were involved in an altercation with the man but rather that guards had halted the incident by handcuffing the individuals involved and escorting them out of the nightclub. Kuta police chief Wayan Sumara supported the nightclub's version of events.

Jail for coward punch security guard Viko Sausoo

A Western Sydney magistrate has sent a coward punch offender to jail following a violent attack on State of Origin night last year. According to the Daily Telegraph, magistrate Karen Stafford sentenced 38-year-old Viko Sausoo to 12 months in prison with a non-parole period of eight months in Parramatta Local Court on 12 May.

Mr Sausoo punched Sebastian Rodriguez Chamorro, aged 22, at Parramatta's Albion Hotel about on the evening of 27th May after telling his girlfriend and their family at 9:50pm that they had to leave the venue because they had children with them (the pub was not allowed to have children inside after 10pm).

Mr Chamorro walked out of the venue and got into a discussion with Mr Sausoo in relation to being required to leave the venue prior to the end of the game. He was then hit by the guard on the left side of his face, knocking him to the ground.

Mr Chamorro's injuries included three fractures to the cheekbone as well as bleeding on the left eye causing blurred vision. Mr Sausoo pleaded guilty to assault occasioning actual bodily harm on March 18.

CCTV from the venue was submitted to the court by the police prosecutor, which Ms Stafford watched twice before delivering the sentence.

"The blow comes so suddenly, this man had no time to see it coming," stated Ms Stafford. "Security guards are often the victims of assaults. This is not one of those cases."



Australian Criminal Intelligence Commission to combat criminal and national security threats

New criminal intelligence and information agency following the successful passage of the Australian Crime Commission Amendment (National Policing Information) Bill 2015 through Parliament, according to Minister for Justice, Hon Michael Keenan MP.

The legislation creates a new Commonwealth law enforcement and criminal intelligence agency to be known as the Australian Criminal Intelligence Commission (ACIC). It will focus on targeting emerging criminal and national security threats, and will bring CrimTrac and the Australian Crime Commission (ACC) together under one banner.

The ACC is the Commonwealth's national criminal intelligence agency with specialist investigative capabilities. CrimTrac delivers and maintains national information-sharing solutions that enable Australia's police and law enforcement agencies to share information across state and territory jurisdictions.

"This merger is vital because our law enforcement and protection agencies need accurate information and intelligence to respond to immediate threats," stated the minister. "The nation's law enforcement agencies will be able to use a single data entry point to feed in and out of the ACIC's IT capabilities where research, operational data and intelligence will ultimately provide a big data view of law enforcement information including imminent threats. The agency will be operational from 1 July 2016.

Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

your
electromagnetic
lock

**UPGRADE
DETAIL 4**

Substantially improved
DPS Reed Magnet
fastening is extremely
secure, making the
product much more
Vandal proof.



Options include:

- 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

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

21516



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.

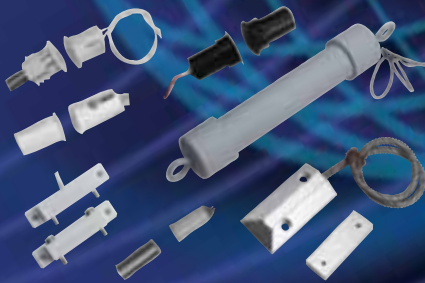


Loktronic



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



ITRON SECURITY & AUTOMATION



Loktronic for gate locks

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

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

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

20238_PDM



Wireless IP Surveillance

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

Distributed by



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



Customized CCTV Kits

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

Distributed by



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



Open Platform VMS

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

Distributed by



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



(09) 414 5101 OR 0800 ITRONICS

SALES@ITRON.CO.NZ

WWW.ITRON.NZ



DF5200HD-DN

- Full HD Box Camera
- 1080p @ 25/30 fps
- 720p @ 25/30 fps
- 1080p @ 120 fps optional
- Motor-driven Lens
- Wide Dynamic Range
- Day/Night with ICR
- Ultra Low-Light
- P-Iris Control
- PoE (Class 0)



Ph: 09 276 3271 • cctv@crknz.co.nz • www.crknz.co.nz



DF5200HD-DN/IR

- Full HD Box Camera
- Day/Night with ICR
- Integrated IR Illumination 25m
- Motor-driven Lens
- One-Push Autofocus
- P-Iris Control
- PoE (Class 0)
- IP66 Rated



Ph: 09 276 3271 • cctv@crknz.co.nz • www.crknz.co.nz



DF4820HD-DN

- HD Box Camera
- 3-Megapixel
- Full High-Definition
- 1080p/30
- H.264
- Day/Night (ICR)
- Motor-Driven Varifocal Lens
- One-Push Autofocus
- P-Iris
- PoE (Class 0)



Ph: 09 276 3271 • cctv@crknz.co.nz • www.crknz.co.nz



SECURE ACCESS. NO CARD REQUIRED.

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

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

YOUR SECURITY. **MOBILE** | Visit us at hidglobal.com

