

NZSecurity

December 2016 / January 2017



PRIVACY IN THE AGE OF BIG DATA

**MISSING TASER CALLS WEAPON
SECURITY INTO QUESTION**

**BUSINESS CONTINUITY MANAGEMENT
AN INTEGRAL COMPONENT OF PROTECTIVE SECURITY REQUIREMENTS**

www.defsecmedia.co.nz

Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

your electromagnetic locking specialist!

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

Standard features include:

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

Options include:

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

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

10
YEAR
GUARANTEE



Loktronic

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



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



IPC6852SR-X44U-F

Worlds First 44x Zoom HD Starlight Camera

- 250m Infrared Range
- Starlight Illumination
- Ultra Fast Focus
- H.265 Recording
- Triple Streams
- 128GB onboard Storage

44x



Contact Details:

Craig Flint

Telephone: +64 (07) 868 2703

Mobile: +64 (0) 274 597 621

Postal and delivery address:

27 West Crescent,
Te Puru 3575, Thames, RD5,
New Zealand.

Email & 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

February/March 17

*Building and Construction
IQP's, Consultants, Electricians, CCTV
Installers, Architects, Engineers, Integrators
& Estimators*

April/May 17

*Government, Transport, Tourism, Access
Management, IT security threats*

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 From the Editor
- 8 Dahua Technology Launches HDCVI3.0
- 10 Privacy in the Age of Big Data
- 12 RealMe: Realising privacy and trust via digital identity
- 14 New Zealand needs a cultural shift to keep data safe
- 16 Missing Taser Calls Weapon Security into Question
- 20 Aotea Security WINS the 2016 Hikvision Flying 5000 Go Karts
- 21 No holiday from retail cybercrime
- 22 Wish you an 'app-y' Christmas shopping
- 24 Trailblazer: Ngaire Kelaher setting the standard
- 26 Business Continuity Management
- 28 Automating asset maintenance with simPRO
- 29 NZSA & FPANZ forging close working relationship
- 30 Martin Jetpack: First response game changer?
- 32 nzSecurity in the News
- 34 Australia Round-up
- 38 iSANZ Awards winners announced for 2016

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.

20851



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.

From the Editor

In this December/January issue of NZ Security, we focus on the latest and emerging cyber security themes and – as we head into the holiday shopping season – we take a close look at retail cyber security in particular.

On 12 December, the 2016 Privacy, Security and Trust Forum comes to New Zealand for the very first time. Hosted by Unitec, the event will bring to Auckland a collection of international expert speakers on a wide range of cyber security and privacy topics. We were lucky enough to seek the insights of two big names from the line-up: eminent computer scientist Dr Ali Miri and RealMe pioneer Mandy Smith.

In our interview with Dr Miri we discuss some of the opportunities presented by the use of Big Data and the security and privacy issues they present, while with Mandy Smith we explore the insight and learnings that RealMe provides around how one can give consumers and organisations confidence around privacy and trust via digital identity.

We also cover Massey University's Future NZ event held on 10 November in Auckland. The event's speaker, Dr Andrew Colarik, a cybersecurity expert at Massey's Centre for Defence and Security Studies, argues that New Zealanders need to better understand the risks of prioritising user features over security when it comes to the many internet-connected devices we use.

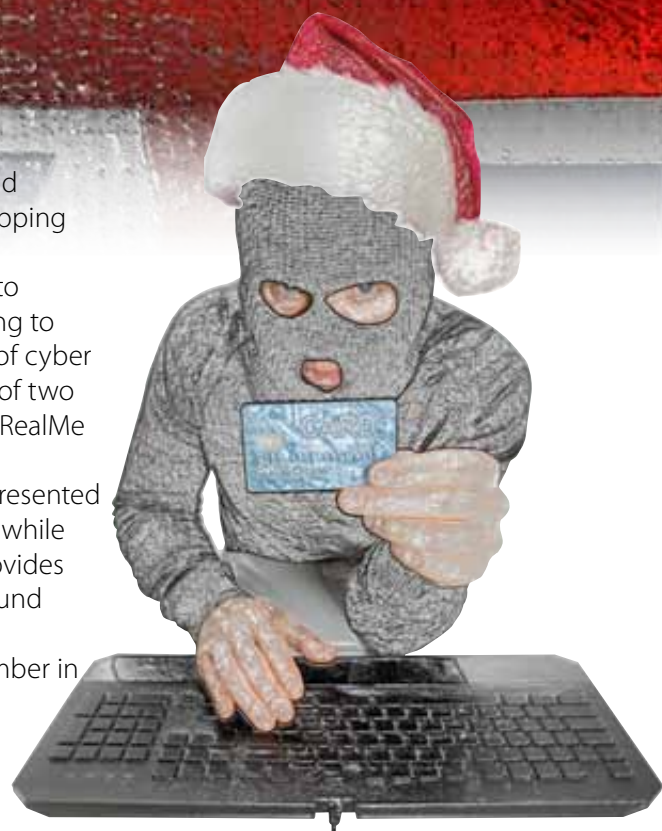
In his regular feature, Gary Morrison, NZSA CEO, revisits the Protective Security Requirements (PSR), this time zeroing in on the requirement to have an effective business continuity management programme in place. With natural events taking over news bulletins since the 14th November Kaikoura earthquake, his message is particularly timely.

We also look at the issue of Police Taser security. 5th November saw the loss of a Taser during a struggle between NZ Police officers and youths in Gisborne, and the weapon is still yet to be found. Is Taser security what it should be, or does there need to be a ramp up in the way that our law enforcement protects its 1,500-strong cache?

Also in this issue, we return to the theme of mechanisation in security, and have the pleasure of learning about the Kiwi-developed Martin Jetpack. This Optionally Piloted Hovering Air Vehicle, or OPHAV, looks like something out of the pages of science fiction, but it also presents real possibilities for revolutionising the work of first responders. We ask Martin Aircraft Company about the potential enterprise security applications of its amazing machine.

As we continue to profile outstanding individuals in the New Zealand security industry, in this issue we profile Ngaire Kelaher, ASIS NZ Secretary and NZSA Deputy Director of Training. A trail blazer for women in security, few have had such a profoundly positive impact on the professionalism of the industry.

The NZ Security team looks forward to bringing you the best in security industry news and analysis in 2017, and in the meantime we hope you have a very happy, safe and secure festive season.



Nick Dynon
Managing Editor

Nick has written for *nzSecurity* since 2013. He writes on all things security, but is particularly fascinated with the fault lines between security and privacy, and between individual, enterprise and national security.

His research has been published in several peer-reviewed journals and in reports 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*.

Prior to *nzSecurity*, Nick was posted to Shanghai, Beijing and Suva as a diplomat during a 14-year career with Australia's Department of Immigration and Border Protection. He has also served in the Australian Army's Signals (RASIGS) and Transport (RACT) corps.

Protect what's most valuable



The new Avigilon™ H4 Fisheye camera line offers a complete, high-resolution, 360-degree panoramic view with no blind spots. This cost-effective, easy-to-install solution is designed to provide broad coverage with fewer cameras.



- Available in 6 and 12 megapixel resolutions
- High Definition Stream Management (HDSM)™ technology
- 360° control with Avigilon Control Center (ACC)™ software
- LightCatcher™ low-light technology
- Integrated with content adaptive IR technology

Learn more at avigilon.com/H4Fisheye



Security Wholesale 2001 Ltd

Unit G, 701 Great South Road, Penrose, Auckland 1061
09-580-1147 | sales@swl.co.nz | www.swl.co.nz

Dahua Technology Launches HDCVI3.0, Next-Generation Analog-To-HD Solution

Now With Greater Compatibility and Intelligent Features

Dahua Technology, a world-leading manufacturer of video surveillance products, today announced the release of HDCVI 3.0, its next-generation analog-to-HD video surveillance solution.

HDCVI, also known as high definition composite video interface technology, is technology developed and introduced by Dahua in November 2012 to address an industry need. Since then it has become a standard for HD-over-coaxial-cable video transmission that allows reliable, cost-effective long-distance HD transmission, offering powerful performance and functionality.

Dahua HDCVI3.0 technology includes full compatibility with a wide range of industry platforms and technologies, higher video resolutions such as ultra HD and 4K, as well as intelligent functions equal to those in IP systems.



“The worldwide adoption of Dahua HDCVI technology is testament to its ability to address an industry need,” said Liquan Fu, President of Zhejiang Dahua Technology Co., Ltd. “With nearly two hundred million analog security surveillance systems deployed globally, HDCVI 3.0 is expected to have a far-reaching impact on the security industry for years to come.”

Full Compatibility

Dahua HDCVI 3.0 effortlessly integrates with five popular industry platforms—HDCVI, AHD, TVI, IP and analog—and can accept input from IP systems. DVRs equipped with HDCVI3.0 technology can act as an access point to integrate with external passive infrared sensors, smoke detectors and other types of sensors, to further provide comprehensive security services.

Ultra HD

Dahua HDCVI3.0 delivers a true end-to-end ultra HD experience to existing coaxial systems. It is the first technology that realizes 4-megapixel resolution over coaxial cabling. Meanwhile, it also offers Dahua Starlight night vision technology that includes 2-megapixel resolution at 0.008 lux illumination and 120dB WDR. Additionally, it features H.265 compression standard that allows the system to save up to 50% bandwidth.



Intelligence

Dahua HDCVI3.0 features rich intelligence including facial recognition, people counting, heat map, smart tracking, and smart scene adaption. Other basic smart features include intrusion, virtual tripwire, missing object, abandoned object and scene change. Defogging and a voltage overload alarm are also included.

Simplicity

HDCVI 3.0 systems offer the same simplicity and ease of installation as analog systems of the past, as the cameras can be plugged into the DVRs using coaxial cable. HDCVI 3.0 systems are low-cost and easy-to-build. Video travels long distances with no delays/latency and power can be directly supplied over coaxial cable.

Another advantage of HDCVI 3.0 is the transmission distance compared to other analog systems. When transmitting general media, the signal can be extended as far as 1,200 meters by using 75-5 cable, with a low signal distortion rate.

HDCVI 3.0 not only offers high definition across long distances, but also features no-latency capability for outstanding real-time performance, because there is no compression processing required to maintain its original effect, resulting in vivid image quality.



Re-empower the coax with Dahua revolutionary **HDCVI 3.0**

- **Full Compatibility / Convergence**

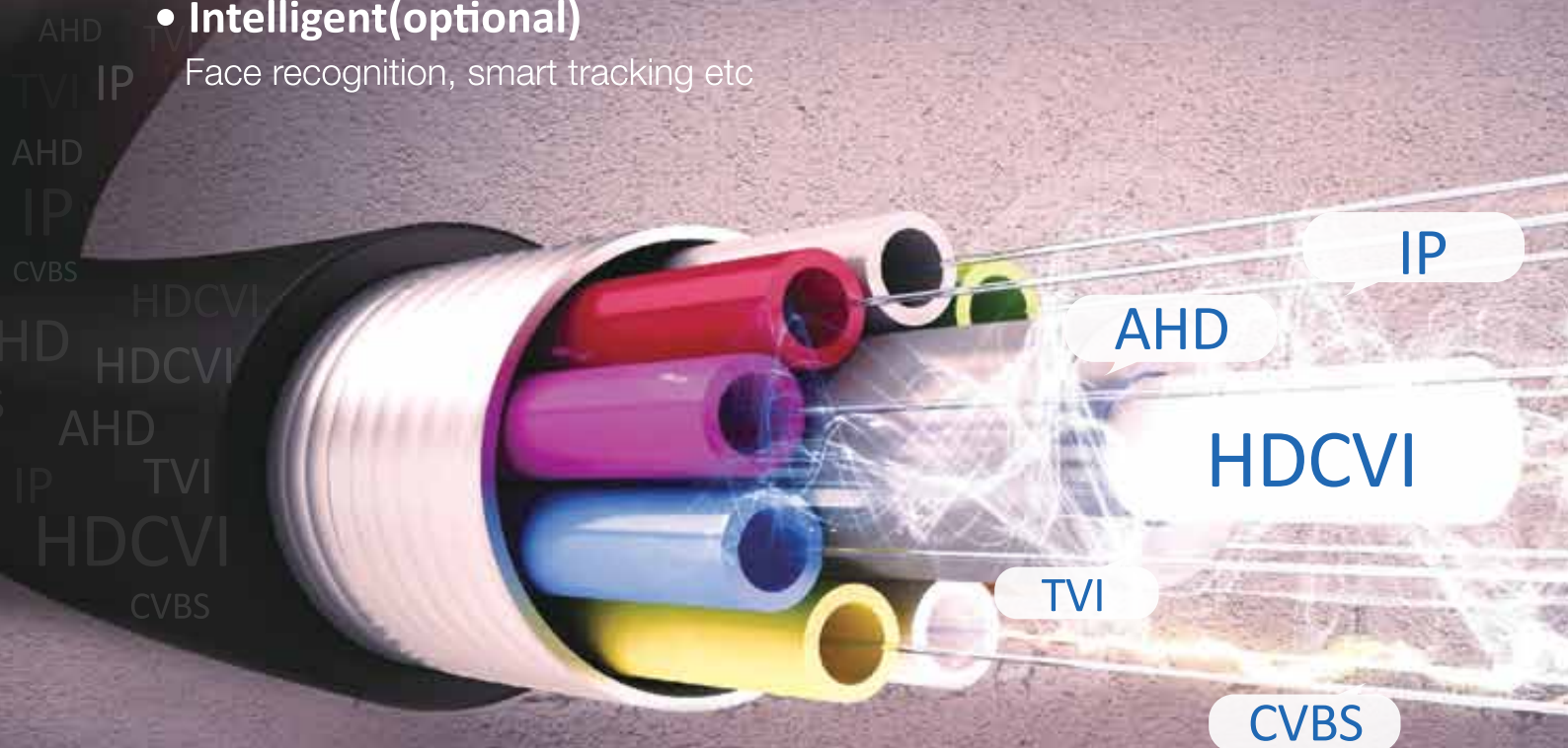
Penta-brid: HDCVI/TVI/AHD/CVBS/IP

- **Ultra HD**

4 megapixel/4K, night vision, WDR

- **Intelligent(optional)**

Face recognition, smart tracking etc





INTERVIEW:

Privacy in the Age of Big Data

The 2016 Privacy, Security and Trust Conference is jointly organised by the High Tech Trans-Disciplinary Research Network at Unitec and the University of New Brunswick, and will be held in New Zealand for the first time from 12 to 14 December in Auckland.

The first day of the conference will host a Cybersecurity Summit/Industry Day for government and industry experts, industry groups and academics to discuss privacy, security and trust and associated industry issues. Joining the line-up of day-one presenters will be computer scientist Dr Ali Miri, who will speak on privacy in the age of big data.

Mobile computing, cloud/client infrastructure, the Internet of Things, and other advanced technologies have led to the creation of dynamic, diverse and distributed datasets, commonly referred to as Big Data. Advances in computing, data mining, and analytics, when used together with Big Data are promising to enable new discoveries and innovations that would have otherwise been thought to be impossible.

Current laws and practices, however, were not designed with Big Data in mind, and many of the technical tools needed are still in their infancy. Governments and industry are now scrambling to fill the gap.

In his talk, Dr Miri will discuss some of the opportunities presented by the use of Big Data, the security and privacy issues inherent in these opportunities, and some of technical, legal and policy-based solutions that can and should be considered.

Dr Miri is Professor at the School of Computer Science, Ryerson University, Toronto. He is the Research Director of the university's Privacy and Big Data Institute, at Ryerson University, a member of the Standards Council of Canada, Big Data Working Group, and a member of the Ontario Center of Excellence's College of Reviewers.

NZSM: What are the security and privacy issues we face with Big Data and its use? How concerned should we be?

AM: With great opportunities comes great risk. The latter is what we are facing with the expansion of big data analytics into more and broader applications. This technology is developing faster than our current laws and practices, which have been unable to keep up.

This gap in technology and policy has led to a number of security and privacy issues, including maintaining end to end data security throughout the big data lifecycle. This sense of trust is key. Many big data applications in areas such as healthcare, the smart home, or industrial environments require the ability to query and process data and extract knowledge from incredibly large and complex datasets.



Dr Ali Miri is a computer scientist, who will speak on privacy in the age of big data at the Cybersecurity Summit/Industry Day in December

Designing systems that can establish trust among end users, IoT devices, and the applications themselves is a significant issue. Currently, many vulnerabilities exist that enable theft of personal information and access to vulnerable infrastructures. We should be concerned to the extent that we need to be more knowledgeable of the use and collection of our personal information. We must be more aware and educated on available methods to secure our information in our online world.

NZSM: The abstract to your talk states "Current laws and practices were not

designed with Big Data in mind, and many of the technical tools needed are still in their infancy." Can you describe the main tools needed?

AM: The volume of data collected, stored, and processed is increasing every day. As a result, this is challenging technical tools that were never designed with these pressures in mind. Some of these are policy based, such as modern and intelligent access management policies. Most are technical, focusing on new methods of encryption and anonymisation, such as homomorphic encryption.

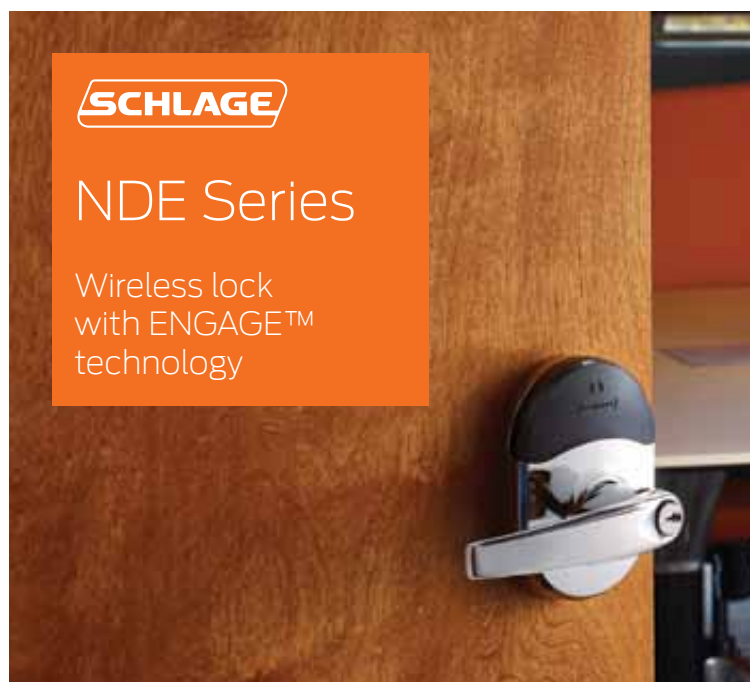
Another technical challenge is the storage and processing of encrypted data and developing methods to use the data while maintaining its security. In other words, developing 'smart' keys that can allow users access while maintaining the overall security of the database.

NZSM: How would you describe the New Zealand government's efforts to fill legal and policy gaps in relation to the use of big data, compared to other governments?

AM: While I'm still learning about the government of New Zealand's efforts regarding big data, I can speak to the efforts of the United States and Canada. In the US and Canada, there are efforts to recognise that online privacy should be afforded the same protections as in the physical world.

In addition, there is a recognition by US and Canadian authorities that big data can be dangerous when it comes to fairness and discrimination, encouraging applications to recognise that disadvantaged communities may not be as connected as wealthier ones, and therefore the data collected may skew towards privileged groups.

Where the US and Canada, and many other jurisdictions, fall short is the use of big data for government surveillance. This is especially obvious when we see authorities clamp down on private sector usage of personal information, but no mention is made of their own use of data collection. Of course, government policies can change drastically with administration changes and shifts in political power (ie. the United States).



- Easy to install, wireless solution for access control ideal for interior office doors, common area doors and sensitive storage spaces
- Uses ENGAGE™ technology - allows users to manage lock configuration settings via web or mobile apps

Activation

- Re-programme at the lock using mobile phone (Apple iOS or Android), iPad, iTouch
- Update remotely when lock is connected via Wi-Fi

For more information,
contact Allegion on
0800 477 869
or visit allegion.co.nz





INTERVIEW:

RealMe: Realising privacy and trust via digital identity

Mandy Smith, Head of RealMe for New Zealand Post, will discuss the application of digital identity at the 2016 Privacy, Security and Trust Conference in Auckland on 12 December. NZ Security spoke with her ahead of the event.

RealMe verified identities are designed to allow customers to prove to businesses and government departments who they are, without having to hand over physical documents such as passports, driving licenses and utility bills. Launched in 2013, RealMe is a collaboration between the Department of Internal Affairs and New Zealand Post.

With over 200,000 New Zealanders already having a RealMe identity, and growing at nearly 10,000 or more per month, it appears that consumers are seeing the benefits of having a single trusted digital identity.

As Head of RealMe Mandy Smith leads the third party identity verification services strategy for Kiwibank and is the New Zealand Post group business lead for the RealMe partnership with the Department of Internal Affairs

(DIA). She sees digital identity as a key enabler of the digital economy, allowing organisations to reimagine their services to be delivered digitally while still providing trust and privacy for their customers.

Mandy's presentation at the upcoming PST Conference will explore some of the existing use cases for the application of digital identity verification and how it is helping to not only reduce the costs associated with identity fraud but helping consumers keep their information private.

NZSM: Can you provide further insight into your upcoming PST Conference presentation?

MS: RealMe gives really good insight and learnings around how one can give consumers and relying parties confidence around privacy and trust. And when I talk

about trust I talk about it being two-way.

One of the big challenges today is if you're in the analogue world and handing over your identity documents, even though it's happening within the context of a genuine relationship, you have no control over who handles the copies of those afterwards. And because organisations go for less friction they end up getting more [information] than they needed to actually do the transaction.

The individual is thus relying on that organisation to do the right thing, which on the whole works fine... but not always. That's what we see in terms of how the various forms of identity fraud start to happen.

In the digital world, one of the things with RealMe is that you're always in control of what you're sharing, and it's designed in such a way that only what needs to be shared is shared. If you have



Mandy Smith, Head of RealMe for New Zealand Post

a case where somebody just needed to prove that they were of age, you can just confirm they are of age and nothing more. You don't need to know date of birth or place of birth or anything else about them because you're not requiring information about a whole identity.

NZSM: How do you achieve that?

MS: What happens is that the consumer enrolls into RealMe and we verify their identity – there's four core attributes that we hold about them that are held in different systems. When a relying party comes in and says I would like to determine that a person is of age, all it needs to know about her is her full name and date of birth, or that she has turned 18, and we provide the logic to say that's all we're going to share with you.

What creates the trust is the customer sees what's going to be sent to the relying party. What's great about that is that in your account you also have a record of where you have asserted your identity, whereas in the analogue world you don't have that – it's up to your memory as to where you may have provided your identity documents.

In your personalised RealMe account you can identify where you have verified information to an organisation. RealMe does not have a central database, so when attributes are shared they are shared from the relevant source, and that's due to the

privacy-by-design principles used to build RealMe.

NZSM: Is privacy-by-design a little over-the-horizon in terms of general uptake, or are we already seeing it?

MS: Within core government functions and designs it is absolutely foremost. There is a lot of discussion about privacy guidelines. I think the awareness is coming up and I think anyone now designing a solution involving someone's identity is very much aware of the different privacy guidelines and what they mean in terms of the way you design a system.

NZSM: What's the end-state for RealMe, in, say, five to ten years' time?

MS: We're really seeing some momentum in enterprise and relying party adoption. My view is that ideally [your RealMe identity] is your most common form of identity used. The timing of adoption is around individual relying parties' capability to offer digital services.

So for us to get our marketplace going, we need to have organisations able to interact with their customers in a digital fashion irrespective of the channel. For example, if you walk into a retailer and you want to apply for finance with them, they need to have the ability to receive a RealMe decision, such as

“Mandy Smith is who she says she is”.

If you think about five or ten years' time, in order to address customer friction most organisations will have moved into the digital space and will have acquired the ability to use that type of platform. Consumers with their adoption of mobile devices will already have the ability to do this.

So on the one hand it's about the attractiveness of – and confidence in – RealMe itself, and on the other it's about the capability of the market to adopt.

NZSM: Where does NZ sit globally in terms of this?

MS: It's interesting because we have quite a unique model in the way that we've done this compared to other markets. If you look to European nations, many already had national identity systems and quite a strong philosophy of compliance around those. If you look at Norway and the Scandinavian countries, they've been able to establish these programs quite quickly and efficiently due to their consumer philosophies.

But in terms of ease of experience, what we've got in New Zealand is pretty unique. Once you have a verified identity in RealMe, proving your identity digitally is very simple and quick. The system has been around for a few years now, the technology continues to advance and we're working with it.

Australia still hasn't gotten anything moving, and some of that's to do with the challenges of federation in terms of having both state and national governments. The UK is on a journey, but at the moment they are only servicing the government sector. The US less so, and Canada – in terms of authentication – is probably on a par. So I think we're doing well.

If you're going to address the privacy and trust components, so long as you can demonstrate the benefits [of the system] around privacy and trust then I think the majority of the population will decide to opt in over time.

ENJOY a **10** year guarantee*

on Loktronic Indoor Electromagnetic Locks!

Loktronic 0800 367 565
www.loktronic.co.nz

*Standard terms & conditions of sale apply.



New Zealand needs a cultural shift to keep data safe

November 10th saw the staging of Massey University's Future NZ Forum on Cybersecurity, held at Auckland's Aotea Centre. NZ Security was there to hear from Dr Andrew Colarik, a cybersecurity expert with the university's Centre for Defence and Security Studies.

New Zealanders need to better understand the risks of prioritising user features over security when it comes to the many internet-connected devices we use. That's the message Massey University senior lecturer Dr Andrew Colarik wants NZ businesses to understand.

Dr Colarik warned that New Zealand hasn't invested heavily enough in infrastructure to make the country resilient against denial-of-service attacks, or to keep data safe. The problem, he says, is the infrastructure we have built is scaled for New Zealand's population, but that same infrastructure connects us to the rest of the world.

"Everything we do in this country is now so dependent on the free flow of information and the connections that we maintain. Any disruption to that will have huge, cascading effects," he said.

"A large denial-of-service attack could shut down communications to the whole country quite easily. If targeted for competitive or political reasons, there are very few organisations that would be resilient to that sort of attack."

He pointed out that both individuals and organisations need to understand that communications infrastructure, by its nature, is not secure. "There are only measures of security," he said. "The

notion that the internet is secure is just salesmanship."

He asked how many of us really think about the access we give to our information when we download an app or a game. "Pokemon Go! has the right to take all your pictures, all your contacts, basically everything on your phone and send it to the mother company", he commented. "The company that owns it, their net worth increased by billions – how is that possible if the data isn't worth something?"

In this digital landscape, New Zealand's economic livelihood faces real threats, Dr Colarik warned. New competitors are emerging all the time – and some will have the know-how and motivation to extract information for competitive advantage.

"What happens when an organisation's own information is used against it? Customer details, costing and pricing structures, and other intellectual properties are all there for the taking if not properly protected."

It's a national security problem that, Dr Colarik argued, is more than just the government's responsibility to address.

"Sure, more investment in infrastructure is helpful, but what we

really need is a cultural shift to strike the right balance between user features and security, and data usage and privacy. You can't have your cake and eat it too.

"This needs to be done at a whole-of-society level. We all need to take responsibility for the level to which we share our personal data, and we need more education and greater discussion about who owns and controls our information. A genuine public/private partnership is essential for ensuring everyone's prosperity in our digital future."

After his speech Dr Colarik was joined by a panel of industry experts to discuss the strategic cybersecurity issues facing New Zealand. They also acknowledged there was a lack of capability in New Zealand for dealing with cybersecurity issues, but also identified it as an opportunity for the future.

Panelist Kendra Ross, director and co-founder of Duo, pointed to the enormous potential in New Zealand's human capital. "There is a global skills shortage – 1.5 million cybersecurity roles currently unfilled globally," Ms Ross said. "We have an ability here to actually build a workforce that we could be exporting in terms of skills and resource capability."

People Counting**Heat Map**

smart solution 2.0
for Shop

Maximize Business Efficiency and Intelligence

Hikvision Smart Shop Solution Offers Modern Surveillance Beyond Security

The Hikvision Smart Shop Solution is a modern, state-of-the-art IP surveillance system to reduce your loss and provide better service for your customers. The solution employs video analytics that can provide an accurate report of customer traffic flow and heat mapping to show the most active in-store areas. These analytics help businesses understand customer behavior, assess conversion rates, and improve management efficiency. The Smart Shop Solution is designed for independent shops, department stores, and chain stores.

- High video quality
- Excellent nighttime visibility
- WDR performance
- Wide coverage





Missing Taser Calls Weapon Security into Question

Recently a Police Taser went missing in Gisborne after a struggle ensued between Police and a group of youths. It's yet to be found. With the Taser now a standard weapon carried by all level one police responders, just how secure is NZ Police's cache of 1,500 Tasers?

On 31 July 2015, New Zealand Police Commissioner Mike Bush's announcement that all police responders would routinely carry Tasers was greeted with some controversy. More than a year down the track, the increase to the Police's cache of 1,000 Tasers by 400-600 new units has attracted little attention.

Figures released on 2nd September, show that of the 1,949 allegations made against police between January 1 and June 30, there were only eleven use of force complaints related to the deployment of Tasers. That's four less than the number of complaints relating to police dog bites.

But the loss of a police Taser during a struggle between police and youths in Gisborne on 5th November has sparked concerns over the implications of a Taser in the wrong hands. The missing weapon remains unaccounted for.

It is believed the Taser and holster may have become dislodged from an officer's belt clip when he attended a fireworks related incident on Waikanae beach. Police had been called to an incident involving a large group of youths reportedly shooting firecrackers at passers-by.

While escorting the group from the area, one of the officers was hit in the arm by a firework, and a struggle ensued when Police tried to stop the youths from running off. It is during this struggle that the Taser is believed to have become detached from the officer's belt.

"Police are continuing to make inquiries to locate the Taser and are doing this through a range of channels including social media," said Inspector Sam Aberahama, Area Commander Tairāwhiti.

Responding to an enquiry from NZ Security, Inspector Aberahama stated that data on the number of times equipment has been misplaced or lost in each District is not held centrally. However, Police say that incidents where 'appointments' (batons, OC Spray, Taser etc) are misplaced or lost are "rare".

"When not in use, a Taser is secured in a holster which is clipped onto the officer's belt, so instances where they become detached or lost are uncommon," stated Inspector Aberahama. "However, due to the nature of Police work officers are often faced with a range of situations including physical contact or activity, which may result in uniform items being displaced or detached."

"A review into the incident is ongoing and when this will be completed and how findings of the review will be shared publicly are still to be determined," he said.

NZ made

Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

fire door holding electromagnets 12 & 24 VDC selectable



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

Standard, floor mounted, wall to door distance 114mm



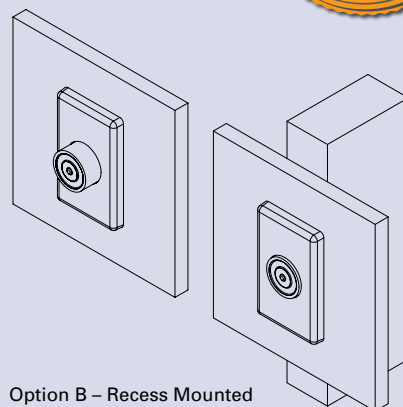
10 YEAR GUARANTEE*

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



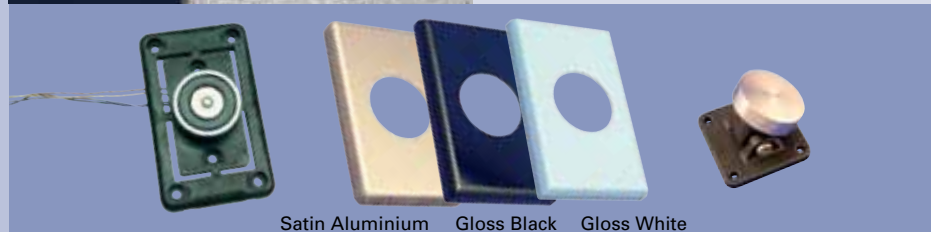
FDH40S/R

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.

While lost Tasers may be uncommon in the New Zealand context, a global snapshot suggests that the compromising of Taser security as a result of altercations in the line of duty is more commonplace than one might assume. In many cases, missing Tasers were recovered only after they had been used in the carrying out of crime.

On 25 September, the Canadian Global News reported that Winnipeg police had found a Taser that had been lost by an officer weeks earlier. The Taser had been drawn and then dropped by the officer during a struggle with a crowd while he and another officer had attempted to assist a man who had been stabbed.

Police were called to the same area three weeks later after receiving reports that a man was threatening people with a Taser outside a bar. They arrested a 19-year-old they say had taken it three weeks earlier.

In another example, a Taser that had been mistakenly left behind by a police officer during a drug search in Burnsville, Minnesota, in January 2013, turned up six weeks later when three 19-year-olds allegedly used it to rob a Subway restaurant in Burnsville.

Alarmingly, international reports indicate that a good number of Tasers are also lost through sheer officer carelessness rather than in the heat of crowd scuffles and drug searches.

In May 2015, in Manheim, Pennsylvania, police placed charges against a woman who admitted to picking up a Taser and giving it to a friend after a township police officer had inadvertently left the device on top of his police vehicle and drove away.

Investigators reviewed footage from surveillance cameras and saw a vehicle stop along the road where they believe the Taser had fallen. Police identified the owner and charged her with theft of lost property. Although charges were laid, the weapon was not recovered.

In November 2015, a Queensland Police Service Taser went missing after an officer mistakenly left it on top of his car while leaving a crime scene. An extensive search of the area initially failed to turn up the missing weapon, but it was later found.

One wonders whether a police officer would as easily forget about a firearm – such as a pistol or rifle – he/she had just placed on the roof of a police vehicle. Probably not.

Perhaps the relative carelessness afforded to the Taser by its user is a consequence of its apparent non-lethality relative to a conventional sidearm. That



Tasers are commonly referred to by authorities and the media as ‘devices’ or ‘appointments’ rather than ‘weapons’ is certainly not helpful in fostering a mindset of Taser security among users.

The Taser is certainly less lethal than a ballistic weapon, but even in trained hands it has – at times – proven lethal. Trained use by a police officer is unlikely to result in serious injury or death, but malicious use in ‘the wrong hands’ is unlikely to prove so harmless.

Looking ahead, the problem with this is that the release of new versions of the Taser – capable of inflicting more harm – is just around the corner.

In the UK, it was reported in November that a two-shot Taser is on the verge of being approved for use by British police officers. Following extensive testing by government scientists of the new product, the British Home Secretary is expected to make a decision within weeks.

The new Taser holds two cartridges each containing twin metal barbs that are propelled at more than 160km per hour before delivering a five second shock. It also comes with twin laser sights designed for more accurate aiming.

According to the Daily Mail, “the device can hit two targets or offer officers

a second chance of incapacitating a suspect without reloading” if the first set of barbs do not pierce the skin. The two-shot would also enable a lone officer to shoot ‘multiple targets’.

This new Taser will, no doubt, provide police in the UK with a more effective ‘non-lethal’ weapon option, and depending on which side of the Taser camp one sits, this is either a good or a bad thing. An enhanced Taser in the wrong hands, however, can never be a good thing.

One Taser lost due to a lack of holster security or officer carelessness is one Taser too many. While a Taser in police hands may be appropriately described as a ‘device’, in the hands of people on the wrong side of law enforcement a Taser can only be described as a ‘weapon’ that can kill.

This is why NZ Police stating in response to our enquiries that “incidents where ‘appointments’ (batons, OC Spray, Taser etc) are misplaced or lost are rare” just doesn’t really cut it. Training, procedures and organisational cultures of accountability relating to Taser security must be commensurate with that afforded to conventional firearms, and if they aren’t – which such responses suggest – they should be improved.

High Speed Gate Automation

Do you need a fast opening sliding gate for commercial or secure locations with high traffic volumes, does the gate need to open in a hurry to get a vehicle off a busy road quickly?



Withington Electrical Limited have designed and manufactured a range of commercial gate automation with simplicity in mind for over 15 years. The proven durability of these robust products has seen this automation installed in prisons, police stations, embassies as well as everyday commercial sites around New Zealand.



We design and manufacture all our automation products in Wellington.
We supply and service motors and automation throughout New Zealand.

For more information and trade enquires contact:

Simon on 0274 488 506 or visit www.highspeedgateautomation.com

We wish all New Zealand Security members a safe and happy holiday season.

We look forward to another great year in 2017.

skills.

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

Proudly supporting the New Zealand security industry.



Aotea Security WINS the 2016 Hikvision Flying 5000 Go Karts

The Annual Flying 5000 sponsored by Hikvision was held on November 16 at Supa Karts Indoor Raceway in Christchurch.

The defending champions, Advanced Security, were very confident going into the event but there were a lot of teams either out for revenge from last year or teams that wanted to get their names on the trophy for the first time.

Atlas Gentech security account manager Brent Stokes says “the Flying 5000 has been around for 17 years which I have been a part of for the last 15 years. It’s all about everyone coming along and having some fun with friends and competitors alike. It’s also a great chance to showcase your driving talents, being enthusiastic to fellow team mates/companies and having a great time.”

Leaderboard:

- First place went to Aotea Security who came back after third place last year so great effort by these guys to sustain the pressure of the racers chasing hard behind them.
- Close in second was a team that was formed by a number of racers from 3 separate companies which I called the All Stars team - although most of them had actually worked with each other in earlier times.
- Third place was Alarm Solutions, they were leading for most of the race but just fell short at the finish line and due to a penalty within the last few laps that gave away second place. These guys made a great effort and have been trying since 2001 to get their names on the trophy for the first time.

Thank you to Mark Underwood from Hikvision and we managed to get him into a team. He found out very quickly that there was no mercy shown to him even though Hikvision were our sponsor. Fortunately for him the back of his seat stopped the front of the car behind him.

Special mention also has to go out to our ladies that raced; we had 3 in the field and after speaking to them they really enjoyed themselves and had a great time. They are keen to come back next year.

Shop online with Atlas Gentech: www.atlasgentech.co.nz



No holiday from retail cybercrime

According to IBM's Security Trends in the Retail Industry report, retailers should have a cybersecurity game plan for the holiday shopping season. While it's shopping time for consumers, it's hunting season for cybercriminals targeting smaller sitting-duck businesses

Attackers use the holiday season to their advantage via spam, phishing and compromised websites, and according to IBM's retail-focused report, there is an increase in malicious holiday-themed activity at this time of year. But whether it's holidays or not, retail remains one of the most attacked sectors in the economy.

The report also notes a tactical shift among attackers, with an increasing number of smaller businesses being targeted. This may be due to the fact that in a large compromise, the retailer provides all the affected credit card numbers to the bank, which deactivates them immediately, whereas when a small company is targeted the breach may remain undetected for longer and the compromised cards might stay active until they're caught individually.

Then there's the incidence of 'own goals'. "The discovery that end user behavior leads to a massive volume of cyber security risks within retail is both a concerning and addressable revelation for leaders in a retail enterprise," states Joe Ferrara, CEO of Wombat Security Technologies. "Many of the security pain points retail organizations are experiencing today can be addressed and

negative impacts significantly reduced with greater security awareness.

While increased retail activity may be one reason for the relatively high incidence of attacks during the holiday season, it is also the case that business owners often switch off in terms of cyber-vigilance over this period when they really should be switching on. And it appears that cyber criminals are well aware that a busy retail season means less retailer focus on security house-keeping.

IBM suggests there are some things that businesses can do to prepare for cyber attacks before and during the holiday season:

Keep patching: Don't ignore patches during the holidays, and ensure that all systems dealing with financial data are patched appropriately. "Criminals have a lot to gain if they're successful, and patching can keep them away from the new vulnerabilities they want to exploit."

User education: Consider implementing a phishing awareness campaign ahead of the holiday season to test users' ability to identify phishing attacks. Employees should be armed with the skills they need to identify suspicious activity both on the phone and in-store.

Prepare holiday staff: Those employees left to manage the store during the holidays don't have time to figure out the appropriate escalation path during a crisis. Ensure your incident response plans are up to date.

Encourage smart shopping: Warn your consumers about the potential for a lurker to be using a mobile phone to record their debit card PINs at checkout.

Monitor for false brand advertisements: Work with law enforcement or service providers to get fraudulent brand advertisements removed, and alert customers to active scams using your brand name.

Consider contactless POS systems: These allow consumers to use their chip-and-PIN credit cards without the need for physical swiping or reading – reducing the risk of attackers skimming the data.

Consider point-to-point encryption (P2PE): P2PE encrypts card data at the point of interaction and does not decrypt this data "until the data reaches the solution provider's secure decryption environment."

Key Benefits Of Leasing:

- Conserve cash and manage cash flows
- No CAPEX approvals necessary
- Flexibility to update to new technology
- Payments are tax deductible

GUARANTEED PAYMENT WITHIN 48 HOURS

Simply Leasing
TECHNOLOGY WHEN YOU NEED IT

Freephone 0508 LEASING | www.simplyleasing.co.nz



An 'app-y' Christmas for cyber criminals

Just in time for Christmas, the online shopping public can expect the festive season to usher in a new cohort of retail cyber threats. This year, shoppers will be kept on their toes by a range of fake mobile retail apps designed to elicit credit card details.

As the pre-Christmas shopping season gets underway, some scammers in the US are creating their own fake mobile retail apps in order to defraud consumers who think they're doing business with reputable companies. With more users than ever turning to Android and iOS apps to avoid the rush and get gifts delivered on time, it's a potential goldmine for scammers and a big threat for retailers.

The fraudulent apps are appearing in mobile app stores and impersonating even big-name brands, such as Footlocker, Puma, Jimmy Choo and Christian Dior. According to Retail Dive, two-thirds of retailers are yet to develop official mobile applications, leaving the door wide open for malicious actors.

iOS not immune

Google's relatively liberal app submission policies have allowed this type of problem to plague Android for years, but scammers are now finding ways to get around Apple's acceptance process as well. Some have even used Apple's new paid search ads to elevate them to the top of the rankings when users search for specific brands in the App Store.

According to the New York Times, Apple tends to focus on blocking

malicious software rather than routinely checking if the thousands of apps submitted to the iTunes store every day are legitimately associated with the brand names they claim to be. After recent media reports, however, a cohort of fake apps has been quickly taken down by Apple.

Although the goal of those scammers is to steal credit card and other personal information by causing consumers to think they are submitting it as part of a retail transaction, there are potentially darker implications for corporates.

An attacker infecting a dual-purpose mobile device with malware via a fake retail app could, for example, gain access to company data such as usernames and passwords, emails and financial sensitive commercial information. A ransomware infection could lock a user out of their work device or delete critical files.

Tips for consumers

Accompanying the proliferation of fake apps has been a wave of advisories providing tips to help consumers tell the difference between fraudulent and legitimate apps and what to do to avoid being stung. These include:

- Look at app store reviews. If the app has no reviews under its profile, it's

likely to be fraudulent. An established retail app will have a long history and plenty of reviews behind it.

- Look for poor grammar and links to other mobile web pages or online destinations. Many fraudulent apps originate from countries where the developers may not be English speakers, which makes them easier to detect.
- Be wary of linking your credit card to any app. If the app turns out to be counterfeit, fraudsters can have easy access to your financial information.
- Never click on a link in any email to download a new app. Go to the retailer website and click on links to download their mobile retail apps directly.

If any of the warning signs are present, avoid downloading the app.

With apps becoming more popular as a way to shop, it makes good sense for brands, retailers and developers themselves to monitor for fakes and report them. A fake app affecting a whole bunch of customers is the last thing a retailer needs at the business end of the year.



**World leaders in
revolutionary Electric
Locking Design
and Craftsmanship.**
Proudly stocked and
supported by NZ's
leading authorized
distributor...

Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

Your FSH Electric Locking
range includes...

- **ELECTROMAGNETIC
LOCKS**
- **STRIKES**
- **DROP BOLTS**
- **ELECTRIC MORTICE
LOCKS**
- **5 YEAR WARRANTY**



MEM2400LP



- Suits low door height or narrow profile frames
- High holding force up to 1000kg
- Releases with up to 70kg of side pressure; early warning alarm
- Supplied with anti-tamper bracket
- 12/24 VDC, low power consumption
- 4 hour fire rated
- Lock Status & Door Status Sensors

MEM2400LED-LZ

- Features as for MEM2400LP with L/Z Bracket for inward opening doors

FES20M



- High security stainless steel strike rated up to 1490kg holding strength
- Quick and easy Power to Lock/Power to Open interchange
- Mounting kit with adaptor tabs
- 12VDC 220mA; 24 VDC 120mA; 36 VDC 80mA
- Door, Lock & Frame status monitors
- Pre-drilled for extension lips, 25mm & 50mm available

FES 10 and FES 10M



- Stainless steel faceplate & keeper rated up to 1300 kg holding strength
- FES 10 is IP56 rated
- Dual voltage capable; 12VDC 200mA, 24VDC 100mA
- Pre-drilled for extension lips, 25mm and 50mm available
- FES 10M has door latch monitor

VE1260



- High security, 1000 kg holding force, 35kg pre-load capability
- Accepts 12-30 VDC
- Door status & Lock status monitors
- Square & radius edge models
- Pre-taped glass door housing available for radius edge version
- Special strike plate caters for up to 12mm door misalignment

FEL990M



- Multi-functional and field changeable
- Vestibule or combination
- Fail Safe/Fail Secure
- 12/24 VDC
- Left or Right hand
- Key override
- Monitors: Door, Lock, Key & REX

Loktronic

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

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

Trailblazer:

Ngaire Kelaher setting the standard

In this issue we profile ASIS NZ Secretary and NZSA Deputy Director of Training Ngaire Kelaher. In an industry more male dominated than most, peer feedback suggests that Ngaire is setting the standard not just for women in security but for the industry in general.

Ngaire Kelaher holds the distinction of being the only female CPP and PSP dual certification holder in Australasia. Add to these acronyms a Diploma of Adult Education and a 'Highly Commended' award as a Security Trainer at this year's NZ Security Industry Awards and one starts to form the picture of one driven security training professional.

According to Scott McNaughton, Chairman of the New Zealand chapter of ASIS and Senior Manager, Protective Security, ASB, there are only five dual or more ASIS International certification holders in NZ (four with two and one with three), including Ngaire. There are just 42 dual (or triple) female ASIS International certification holders worldwide (31 with two and eleven with three).

Scott, who has known Ngaire for about two years through their respective positions in ASIS, describes Ngaire as a pleasure to work with, personifying the Kiwi attitude of being low-key in celebrating her achievements. However, he says, "that modesty and self-deprecating approach is underlined by a strong and determined individual who is very competent and capable."

"Ngaire's passion for training is clearly evident to all who are fortunate enough to be instructed by her in her 'day job', as Deputy Director of Training with the NZSA."

"Ngaire has an enthusiastic approach to everything she does and this enthusiasm is infectious to all exposed to it," comments Scott. "I have never met a busier person with huge commitments around work and personal life – even with those commitments she has always been prepared to take on more work."



Long-time colleague, Security Consultant Lincoln Potter, thinks of Ngaire as more of a "Tomb Raider without the guns". Recalling his first meeting with her at a Close Protection Training delivered by former NZSAS Sargent Glenn Berridge, he comments that even though she was regarded as an experienced educator, "she suffered with the rest of us under training, [and] you don't forget training at this level."

Describing Ngaire as a gifted educator and formidable field officer, Lincoln points to the ripple effect of her work, with her expertise having rubbed off on many others, including himself. "She has enriched my life as an educator giving me insights and guidance that have paid off in my teaching of other security officers."

"What people don't know is that she is an expert / specialist on documentation regarding NZQA, file builds and associated Ministry of Education, audits and Skills and all the crap that goes along with it."

"What's it like to work with Ngaire? easy really, [but] don't upset her! She can be rather dangerous!," warns Lincoln. "I do recall the time when she said she was going to kill me, cook me and eat me."

According to Scott, Ngaire has broken through a glass ceiling in what has traditionally been a male dominated sector, "and would now have to be considered one of the most qualified security practitioners in New Zealand."

"She is indeed a trail blazer for women in security and we are all watching with considerable interest as to what her next achievement will be."

4K

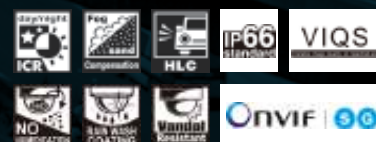
IT'S IN OUR DNA

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

Business Continuity Management:

An integral component of Protective Security Requirements (PSR)

New Zealand Security Association CEO Gary Morrison continues his focus on PSR, this time zeroing in on the need to have an effective business continuity management programme in place. Given the events of November, the message couldn't be more timely.

In my article “Protective Security Requirements (PSR) – An opportunity to professionalise the security industry” (NZ *Security*, Aug/Sep issue), I noted that although the PSR are initially focused on government agencies, they are intended to be relevant to the wider public sector and the private sector. As such, we can expect them to be widely implemented in the near future, with larger corporates being early adopters.

Within the PSR's governance directives, GOV 8 requires agencies using contracted security providers to ensure that the provider is also PSR-compliant and that this be covered within the terms and conditions of the contract between them. Furthermore, assessment visits (or audits) must be undertaken to ensure compliance is demonstrated and maintained.

It is critical therefore that security providers who are currently working for government agencies – or who may wish to in the future – are aware of and operating in compliance with the PSR.

The focus of this article is GOV10, which requires that agencies (providers) “establish a business continuity management (BCM) programme to provide for the continued availability of critical services and assets, and of other services and assets, when warranted by a security threat or risk assessment.”

Prudent business owners and managers will be aware of the need to plan for emergency situations, and will already have procedures and contingency plans in place. Unfortunately, it is often the case that these plans are neither tested nor updated to reflect technology and business changes. This was evidenced by the Christchurch earthquakes when the planning for many organisations was found to be inadequate.

In his book *A Guide to Business Continuity Management* (copies available from NZSA) author Brian Doswell presents a ten-step plan for developing a robust and effective Business Continuity Management Programme/Plan, and they are well worth considering:

Step 1: Project Initiation and Management

Establish the need for a Business Continuity Plan, including obtaining management support and organising and managing the project to completion within agreed upon time and budget limits.

Step 2: Risk Evaluation and Control

Determine the events and environmental surroundings that can adversely affect the organisation and its facilities with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimise the effects of potential loss. Prepare and provide cost-benefit analysis to justify investment in controls to mitigate risks.

It is essential that all risk assessment work has the full cooperation of senior managers in order to ensure acceptance of outcomes.

Step 3: Business Impact Analysis

Identify the impacts resulting from disruptions and disaster scenarios that can affect the organisation and techniques that can be used to quantify and qualify such impacts. Establish critical functions, their recovery priorities, and inter-dependencies so that recovery time objective can be set.

To assess the impact of any business problem, consider how much time there is to correct the problem before it becomes



Gary Morrison CEO,
New Zealand Security Association

critical to the adequate function of the business. The principle objective of BCM is to minimise the potential failures that might lead to a critical/fatal result.

The impact analysis should be as realistic as possible, as appropriate planning and allowance will only occur where senior staff can identify and understand the significance of the impact.

Step 4: Developing Business Continuity Strategies

Determine and guide the selection of alternative business recovery operating strategies for recovery of business and information technologies within the recovery time objective, while maintaining the organisation's critical functions.

Where risks are identified, there should be an appropriate corporate response from the directors/senior management stating how they intend to address their impact.

Step 5: Emergency Response and Operations

Develop and implement procedures for responding to and stabilising the situation following an incident or event, including establishing and managing an Emergency Operations Centre to be used as a command centre during the emergency.

The BCP should coordinate emergency plans with those of emergency services that may be in attendance.

Step 6: Developing and Implementing Business Continuity

Design, develop, and implement the Business Continuity Plan that provides recovery within the recovery time objective.

The BCP should provide information and guidance to those who are nominated to implement the plan and set out the processes and procedures to be followed during business disruption. The plan would ordinarily be presented in the form of action plans and checklists and provide all required information, including a list of key contacts.

Step 7: Awareness and Training Programmes

Prepare a programme to create corporate awareness and enhance the skills required to develop, implement, maintain, and execute the Business Continuity Plan.

It is important that those nominated to respond within the scope of the BCP are given the opportunity to

understand the rationale for their role and to explore how best to rehearse their response to the plan. The BCP should be understood and accepted as a “housekeeping” issue.

Step 8: Maintaining and Exercising Business Continuity Plans

Pre-plan and co-ordinate BCP exercises, and evaluate and document BCP exercise results. Develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the organisation's strategic direction.

Testing is essentially important when third party contracts are an essential part of plans and the ability to control or influence the contracted service is limited or non-existent.

Step 9: Public Relations and Crisis Co-ordination

Develop, co-ordinate, evaluate and exercise plans to handle the media during crisis situations. Develop, co-ordinate, evaluate, and exercise plans to communicate with and, as appropriate, provide trauma counselling for employees and their families, key customers, critical suppliers, owners / directors, and corporate management during a crisis.

Step 10: Co-ordination with Public Authorities

Establish applicable procedures and policies for co-ordinating response, continuity, and restoration activities

with local authorities while ensuring compliance with applicable legislation or regulations.

Summary

In conjunction with the steps above, there are a number of Business Continuity Management Plan templates that can be sourced online (or via the NZSA on request) that provide excellent guidance on how a BCMP should be presented.

Whilst GOV10 specifies the need for businesses to establish and maintain a BCMP, the recent earthquakes in the South Island provide a stark reminder of our vulnerability against events outside of our control and provide ample justification that robust and effective BCMP's are a must-have.

It is also critical that all staff, and in particular those nominated to respond within the BCMP, understand the rationale of the plan and are trained and practiced in their response to the plan.

A comprehensive, well documented – and tested – BCMP can be the difference between survival and business failure by mitigating business risks in the event of a disaster or disruption and including costs and implications that cannot be insured against. BCMPs also provide surety to customers, suppliers, investors and insurers that business planning is robust and as such they potentially offer a competitive advantage over less prepared competitors.



CONNECT YOUR PHONE IN OUR CLOUD

Improve your business phone system and cut costs with our Cloud PBX solution.

- Recurring Revenue
- Simple Installation
- 24/7 Dealer Support - Engineer Direct
- Dealer Training - Technical & Sales
- Solution Design / Configuration Assistance

Automating asset maintenance with **simPRO** job management software

NZSecurity Magazine caught up with simPRO at their stand at the recent 2016 Fire and Security Expo, learning of the software company's just-struck partnership with NZSA to offer association members its cloud-based job management solutions.

Job management software has enjoyed increasing popularity among trade service businesses. By streamlining processes, businesses are seeing a boost in staff productivity both in the office and in the field. For many security businesses, being able to monitor and manage preventative and reactive maintenance of customers' equipment is an essential part of everyday business.

simPRO's job management software enables users to undertake a range of tasks, such as quoting and scheduling installations, managing planned maintenance and more, without mountains of paperwork and complicated audit trails. For businesses, this potentially means time and money savings.

Preventative maintenance made simple

The simPRO Maintenance Planner add-on provides visibility on what's to be tested and when – and what specific test is required. The add-on alerts when assets fail and require rectification, and when critical failures occur that need to be rectified quickly. Jobs and quotes can be created and assigned directly from the planner to get the job done fast.

With comprehensive business management system, simPRO Enterprise, detailed records of all equipment serviced can be kept in the one place – secure in the internet cloud. This means just one centralised platform to store all data, such as service history, details of upcoming services, attachments such as manuals or photos, and so on... and it's available at the click of a button.



Security business such as Allied Alarms has realised the benefits of streamlining processes to boost staff productivity and enjoying a new level of profitability with simPRO

The beauty of the cloud is that all this information can be shared in real time with office staff, field technicians, and even customers and external parties.

Easy asset testing in the field

While on the job, technicians can use the simPRO Connect mobile app to capture test readings, register new equipment, follow service level checklists, report defects, make notes, and even take photos.

Not only can field employees update times, materials, job details, and photos in real time, as well as issue invoices and collect payment on site as soon as a job is complete, but through simPRO Enterprise, all of this information can be viewed in the office. For a business, this office-to-field connection means reduced travel time and an increase in billable hours.

Better service = more customers

It's well known that customers who have a positive experience with a business will recommend its services to others in the future. Allowing professionals to manage jobs in real-time with always accessible cloud-stored data, simPRO's suite of job management software oozes customer satisfying efficiency.

"By offering a comprehensive trade business tool to NZSA members, simPRO aims to support the ongoing growth and efficiency within the industry," says Richard Pratley, simPRO Software New Zealand General Manager.

For more information on the simPRO-NZSA agreement partnership, see the news item on page 40, contact the simPRO Software team on 0800 100 854 for a free demonstration or visit www.simprogroup.com

NZSA & FPANZ

forging close working relationship

Having taken their relationship to new heights over the past year, NZSA and FPANZ are now moving in together. In this report, the NZSA suggests that the benefits go far beyond the sharing of office space.

Whilst there has always been a close alignment between the security and fire protection industries, the same can't necessarily be said for their respective industry associations. That, however, has changed dramatically over the last year under the respective stewardship of NZSA CEO, Gary Morrison, and FPANZ Executive Director, Scott Lawson.

Gary and Scott have recognised that both associations have a number of commonalities including a continued focus on working for the good of their respective industries and members, and that a quick phone call can often tap into a wealth of experience and knowledge and avoid the need to reinvent the wheel.

This has also enabled a common sense approach to be followed in relation to areas where there has been some cross over and confusion between fire and security providers over legislative and compliance requirements.

In November, the two associations worked together to host the Fire and Security Exhibition at ASB Showgrounds that ran alongside the Fire NZ Annual Conference. The inclusion of security industry exhibitors and attendees helped turn an already successful event into the largest event of its type ever held in New Zealand with 70 exhibition stands and in excess of 500 attendees over the two days.

In another demonstration of the close relationship, the FPANZ office will relocate to the NZSA office at Level 2, 132 Hurstmere Road in Takapuna in early December.

According to Scott, the FPANZ needed to shift from their current location in Albany, and the NZSA were able to offer a suitable area in their office at a favourable rental and terms. "This offers both parties an immediate financial saving and, going forward, the opportunity to further consolidate our infrastructure and resource requirements," he said.

Already very positive towards the benefits already achieved through the relationship, Gary can see significant value in developing similar opportunities with other industry associations such as Master Locksmiths and ECANZ during 2017.



simPRO
SOFTWARE

Serious Job Management




ENTERPRISE

Take control of your security business with powerful cloud-based job management software – **seriously.**

FREE EVALUATION

Features to make your work flow

-  Estimating & quoting
-  Service & project management
-  Asset maintenance
-  Scheduling
-  Invoicing
-  Payment processing
-  Field mobility with  **CONNECT**
-  GPS vehicle tracking with  **SIMTRAC**
-  Accounting software integration ...and much more.

Get your FREE evaluation!

simprogroup.com/enterprise

or call 0800 100 854 for a **free demo.**



Martin Jetpack: First response game changer?

nZSecurity caught up with Michael Read, Martin Aircraft Company's VP Sales & Customer Delivery, as he boarded a flight to the US to spread the Martin Jetpack word. We asked him about the jetpack's potential for security industry applications.

Mention 'jetpack' and it immediately conjures images of the liquid-fuelled rocket packs that emerged out of the pages of science fiction and into mainly US prototype programs in the 1960s. Despite its name, the Martin Jetpack shares little in common with these except for its potential to totally revolutionise aviation.

The jetpack is, more accurately, a OPHAV, or Optionally Piloted Hovering Air Vehicle. It can be flown manned, unmanned or networked and tethered as a mule. "Mule allows people to fly manned but then also bring along equipment or an unmanned aircraft that you can put someone in," Read explained. "That ability to force multiply is the game changer."

Established originally as a research and development company, the Christchurch-based Martin Aircraft

Company has evolved to become a world leader in Jetpack development and commercialisation. The company is publically listed on the Australian Securities Exchange (ASX).



Initially conceived to bring the fantasy of personal aerial transportation to reality, the Martin Jetpack concept has evolved to one focused on the real world mission of saving lives. Indeed, with potential applications such as providing high-rise 'lifeboats' for hotels, the invention turns science fiction imagination into life saving reality.

The aircraft was named as one of *Time Magazine's* Top 50 inventions for 2010, and this triggered a number of queries from the First Responder community who were interested in using jetpacks as a rapid response vehicle.

"We've got the statement 'saving lives', and that is the 'why' about what we're doing," said Read. "We are approaching specialist organisations that are involved in saving lives, from counter terrorism to special response police units, special response fire, and certain military organisations, all of which have the goal of saving lives."

In mid-November, Read was in Auckland to exhibit the Jetpack at the New Zealand Defence Industry Association Annual Forum, and there was no shortage of interest. “Just like the helicopter, we can’t just go straight into the commercial space,” he explained, “we have to go via organisations that know what they’re doing... that’s just part of introducing a new type of aircraft.”

These specialist organisations have the ability to gain approval from the regulator in the public or national interest to experimentally fly the aircraft in its intended roles prior to permission being granted via a type certificate, which, Read explains, “is kind of like the rubber stamp that you need to go and access the commercial markets.”

As for the potential for the Jetpack to take on commercial security applications, he says this is something they will look at once they get their type certificate, which is a couple of years away yet.

Once units start coming off the production line early in 2017, they will be available for purchase to eligible organisations as a package of capability. “As part of the package we’ll offer training, through life support, after sales support, documentation and – most importantly – involvement of the customers in what they want to see in the next iteration of the aircraft,” Read said.

But they’re not just selling to anybody. “We’re being very strict about the type of customers we work with,” explained Read. Currently limited to specialist organisations, Martin’s client list will also



be limited to those who constitute a neat strategic fit.

By the time the Jetpack makes its commercial application debut you can expect it to have further benefitted from a couple of years’ additional fine tuning. The soon-to-be released Series 1 is an impressive looking model, even more so than its predecessor. Its beautiful lines and eloquent engineering belying its high-powered performance and robust aeronautics.

For those few who have had the pleasure of piloting the Jetpack, it is apparently one of the easiest aircraft to fly either manned or remotely, with a fly-by-wire system that allows hands-free hover and position hold. Its advanced safety features include a ballistic parachute that can open at low altitudes.

Sci-fi-like mechanisation in the security industry is nothing new, but it

has made very limited inroads. Security robots, such as the Secom Robot X, Knightscope K5 and the Chinese AnBot, have presented fascinating possibilities, but their application scope remains desperately limited. Drones, or UAVs, have also caught our imagination, but their payload is limited by size and regulation. Moreover, their use by malevolent actors, such as burglars and intruders, has made them as much a threat to security as an enabler.

The Jetpack OPHAV presents entirely new possibilities for the industry that push way beyond the terrain limitations of robots and the payload restrictions of UAVs. As full commercialisation of the aircraft draws nearer, security solutions providers would do well to consider the potential applications of this impressive feat of New Zealand ingenuity.

Key Benefits Of Leasing:

- Conserve cash and manage cash flows
- No CAPEX approvals necessary
- Flexibility to update to new technology
- Payments are tax deductible

GUARANTEED PAYMENT WITHIN 48 HOURS

Simply Leasing
TECHNOLOGY WHEN YOU NEED IT

Freephone 0508 LEASING | www.simplyleasing.co.nz

NZSecurity in the News

NZ facing security skills shortages

16 October: New Zealand is facing a security skills shortage, according to NZTech chief executive Graeme Muller. His comments came ahead of the New Zealand security summit held in Wellington on 17 October, and in the wake of a report from Cisco claiming a global cyber security skills shortage of more than one million people.

“In New Zealand the government and the tech sector have recognised this growing global problem and have created a collaborative private-public sector taskforce to proactively initiate solutions within New Zealand such as the introduction of specialist tertiary degrees and the inclusion of cyber security in the new school curricula,” he said.

“Ironically this could present a wonderful opportunity for New Zealand. If we can maintain our international reputation as a safe and secure country and produce world class cyber professionals, security could become a significant export earner over the next decade.

“Skills shortages in any industry mean that salaries will always be high and cybersecurity is no exception. The demand for talent is so acute that US cities are offering huge salaries to attract the right people and skills.” The effective and safe use of IT has the potential to deliver big benefits to the NZ economy by enabling greater efficiency and productivity.

Cyber Security Skills Taskforce established

8 November: Communications Minister Amy Adams announced the establishment of a Cyber Security Skills Taskforce to address the shortage of cyber professionals in New Zealand. The Taskforce will focus on increasing the number of cyber professionals to help defend against cyber attacks, which cost the NZ economy \$257 million last year.

“We know there is a lack of New Zealanders entering the profession at a

sub-degree level, so the taskforce will focus on working with academia and industry to develop a level 6 course, with industry supported internships,” says Ms Adams.

Many New Zealand universities have developed specialist cybersecurity degrees and postgraduate courses or are in the process of developing them. The Cyber Security Skills Taskforce will establish a pathway for junior analysts, including a level 6 qualification and industry-supported internships to be developed in 2017.

“There is a growing global shortage of cyber security professionals. It’s estimated that there will be a global workforce shortfall of between one to two million positions by 2019,” said Ms Adams. The eight-person Taskforce will be led by David Eaton and include representatives from academia and industry.

Rush Security in receivership

20 October: According to the Government Gazette, security company Rush Security Holdings Limited has been placed into receivership. The company has appointed Grant Bruce Reynolds of Reynolds and Associates as receiver and manager under The Receiverships Act 1993.

According to the National Business Review, the business was placed into receivership owing \$1.5 million to a finance company. Rush Security Holdings Limited was established in 2012.

Darien Rush, director of Rush Security, told NBR that it is likely the assets of the business will be sold as a going concern but that he is also looking for equity partners to refinance it.

Official crime stats for September 2016 released

31 October: According to Police Minister Judith Collins, the official crime statistics for September 2016 show that Police recorded 1,390 more victimisations for the month compared to the same month last year. For the 12-month period, 30 September 2015 to

30 September 2016, the total number of victimisations increased from 261,748 to 276,098.

There were 6,361 burglary victimisations in September, a month-to-month drop of 290 from August. In this crime category, there were 72,776 victimisations in the 12 months to September 2016 – a rise of 10,979 (17.8 percent) from the previous 12 months.

“Burglaries, particularly dwelling burglaries, is a concern and a priority for Police,” Ms Collins said. “This is why an extra focus was put on attending house break-ins from the end of August.”

“While a review of the new Police policy that staff are expected to attend all dwelling burglaries will be conducted in December, provisional data show more than 90 percent of scenes were visited by Police in September. “Across all crime types, Police have increased the number of proceedings against offenders - rising by 3,076 to 175,772 over the year.

simPRO and NZSA partner to benefit members

21 November: simPRO Software has partnered with the NZSA to deliver a suite of job management solutions and training to NZSA members. The partnership will offer financial concessions to members including free licensing options for simPRO Service and concessions on simPRO Enterprise, the company’s flagship cloud-based job management solution.

The partnership will offer a range of professional and financial resources for members, including exclusive education and support from simPRO, such as objective industry advice on how to remain competitive in their markets and gain control and visibility over business operations.

“This partnership will provide enhanced value and support to NZSA’s membership base along with comprehensive trade business software tools for better business automation and increased performance, and making them more competitive in the market,” said simPRO Software New Zealand General Manager Richard Pratley.

“We are very focused on raising integrity, standards and professionalism within the industry, and also providing our members with exceptional support and access to world-class business partners,” NZSA CEO Gary Morrison said.

14 new high tech drug analysers for Customs

26 October: NZ Customs is deploying 14 new FirstDefenders, a mobile substance identification device, to enhance its capabilities to protect the border, according to Customs Minister Nicky Wagner.

“FirstDefenders use a laser to analyse a substance, often without the need to open the packaging. It matches this against a database of over 11,000 illicit and legal substances to provide an accurate result within seconds,” Ms Wagner said. The FirstDefender database can be upgraded to include new and emerging drugs.

“These devices will be a fundamental piece of equipment for frontline officers, making drug identification quicker, safer and more efficient,” Ms Wagner said. “Customs will also be sharing this latest capability with partner agencies to help with broader drug enforcement work,”

The devices are portable, making them ideal for district ports, and they can be used for Customs’ search warrants and taken on board vessels undergoing search. They will be rolled out to 12 Customs locations: Opuia, Auckland, Tauranga, Napier, New Plymouth, Wellington, Nelson, Christchurch, Timaru, Dunedin, Queenstown and Bluff.

Intelligence and Security Bill safeguards could go further

03 November: The NZ Law Society supports the New Zealand Intelligence and Security Bill, but says safeguards could go further. It believes legislation to improve the transparency and oversight of New Zealand’s intelligence and security agencies is a positive development, but recommends strengthening some of the proposed safeguards to enhance public confidence.

The Law Society presented its submission on the New Zealand Intelligence and Security Bill to the Foreign Affairs, Defence and Trade select committee on 3rd November.

“The bill provides some additional protections for personal privacy which

the Law Society welcomes, but considers that in some areas the bill should go further,” Law Society spokesperson Jonathan Orpin said. The Law Society recommends a number of changes to strengthen safeguards in the bill.

“For instance, the Law Society believes that intelligence should be collected using the least intrusive means possible and open source collection of information is preferred where possible, and recommends this general principle is added to the bill”, said Mr Orpin. “It would also enhance transparency and public confidence if the bill required the intelligence agencies to report yearly on their direct access to other government agencies’ databases.”

Wynyard announces voluntary administration

25 October: The Board of Wynyard Group has informed shareholders that it has placed the company into voluntary administration. KordaMentha partners, Neale Jackson and Grant Graham, have been appointed as administrators of the company.

According to a media release, the Board considered all available options including potentially raising additional capital and drawing on the \$10 million loan but concluded that neither raising further equity nor incurring debt was in the best interests of the company, its shareholders or other stakeholders.

“The Board believes this is the right decision under the circumstances, in order to ensure an environment where all options can be fully explored to retain the value in the business,” stated the media release. “The Board acknowledges the significance of its decision for shareholders, staff and customers; and will work with KordaMentha to support these parties as it moves quickly through this process.”

According to a Circular to Creditors from the Joint Administrator, VA is a short-term measure that effectively freezes the Companies’ financial position, giving creditors the opportunity to consider – and eventually vote on – the future direction of the Companies.

Legislation enables Police to recover vetting costs

1 November: According to Police Minister Judith Collins, NZ Police will soon be able to recover the cost of vetting services, with the Policing (Cost Recovery) Amendment Bill passing its

third reading in Parliament. Cabinet has agreed to a fee of \$8.50 per vetting request, allowing Police to recover over \$3 million each year.

“The new legislation amends the Policing Act 2008 to enable regulations to be made that allow Police to recover costs for certain policing services that fall within the definition of a ‘demand service’,” she said. “Police Vetting is considered a demand service because the service is provided on request from organisations for their direct benefit. For example, the vetting of a prospective employee or volunteer.”

However, the Regulations will provide for a range of fee waivers. Agencies making 20 vetting requests or fewer per year will not be required to pay, and registered charities will be exempt. Fees may also be waived for agencies facing extreme hardship and in cases where there are exceptional circumstances.

The Police Vetting Service is also facing significant growth. Police are being asked to vet over 500,000 people a year. Demand has increased by over 100,000 vets since 2012/13, with a nine percent increase in vetting requests in 2015/16 alone. This growth is forecast to continue, particularly with the phasing in of workforce safety checks under the Vulnerable Children Act 2014.

InternetNZ welcomes NetSafe as approved agency

21 November: InternetNZ has welcomed NetSafe to its new role as “approved agency” under the Harmful Digital Communications Act 2015.

“The Internet has enabled much easier communication and sharing. This creates significant benefits, but also some risks and challenges,” said InternetNZ’s Chief Executive Jordan Carter. “NetSafe has been helping New Zealanders to manage these challenges for the last 20 years - and this experience will be valuable in running the agency.”

InternetNZ expects that the approved agency function will allow for timely and education-focused responses to harm online, whilst maintaining the Internet’s role as a medium for free expression.

As the approved agency, NetSafe will listen to people’s concerns about online harm, and guide them through the options for responding. This role requires an agency that understands what people value about being online, and that can help parties to work through the issues.

Australia Round-up

Government announces Academic Centres of Cyber Security Excellence

8 November: Education Minister Simon Birmingham and Minister Assisting the Prime Minister for Cyber Security Dan Tehan announced approval for Academic Centres of Cyber Security Excellence. The announcement was part of a \$3.45 million commitment to help address Australia's shortage of skilled cyber security professionals

The centres are intended to produce work-ready graduates to increase the country's cyber security workforce and cutting-edge research on cyber security, as well as providing executive education programs for industry and government.

The announcement came as a just-released survey of Australian millennials found that two-thirds had never discussed a career in cyber security at high school. Mr Tehan said Australia needed to work harder to encourage young people into cyber security careers.

"There is growing demand for cyber security professionals and it is an exciting and challenging career," he said. "Australia also needs talented cyber professionals to help protect our national and business interests online and to encourage innovation."

"The Centres of Excellence extends the Government's work encouraging young people into cyber careers through the Australia Cyber Security Challenge and Women in Cyber networking event."

"In an important next step," added Mr Birmingham, "we will also appoint a working group to review the courses currently on offer at universities and the eligibility and selection criteria for establishing the Academic Centres of Cyber Security Excellence."

Man jailed for drunken attack on McDonalds' security guard

9 November: According to an ABC News report, a man who assaulted a security guard, dislodging three of his teeth, during a brawl at a McDonald's restaurant in Adelaide has been sentenced to three months' imprisonment.

Demeon Magrowski, 38, pleaded guilty to one count of aggravated assault

at Adelaide Magistrates Court, where it was heard that he had pushed, punched and threw chairs at a security guard at the fast-food restaurant in June.

The victim was hospitalised to repair three dislodged teeth and he had also suffered facial bruising, swelling and a black eye. He believed he could have been killed during the assault, and suffered psychological issues including post-traumatic stress disorder, depression and nightmares as a result.

In a previous court appearance, Magrowski's step-brother was sentenced to four months' jail for his role in the assault.

Magistrate Lynette Duncan imposed a partially suspended sentence of five months and 18 days' imprisonment, ordering Magrowski to serve only three months in prison. He will be subject to a two-year good behaviour bond after release.

New Australian Ambassador for Cyber Affairs

10 November: Minister for Foreign Affairs, Julie Bishop, and Minister Assisting the Prime Minister for Cyber Security, Dan Tehan, announced the appointment of Dr Tobias Feakin as Australia's inaugural Ambassador for Cyber Affairs.

The government's decision to establish the position of Ambassador for Cyber Affairs was one of the principal initiatives of the \$230 million Cyber Security Strategy, which is aimed at encouraging collaboration between Australian government, business, academia and communities to improve cyber security.

The Ambassador for Cyber Affairs will lead Australia's international cyber effort, working closely with the Special Adviser to the Prime Minister on Cyber Security Alastair MacGibbon, who became the first person to assume that role in May 2016. The Ambassador will support regional cyber capacity building, advocate against state censorship of the Internet and promote Australia's view that opportunities provided by the Internet should be available to all people.

Dr Feakin was a member of the Independent Panel of Experts that produced Australia's Cyber Security Strategy. He has been the Director

of National Security Programs at the Australian Strategic Policy Institute, and has held a number of research and advisory positions, including with the Royal United Services Institute for Defence and Security Studies, the Oxford University Global Cyber Security Capacity Centre, and the Global Commission on Internet Governance.

ASIAL 2016 Security Award winners celebrated

21 October: The 2016 Australian Security Industry Awards Ceremony & Dinner was held on 20th October at The Westin in Sydney. The awards have been an initiative of the Australian Security Industry Association Limited (ASIAL) for the past 21 years.

A big individual winner at the Awards was Hailey Page of Chubb Fire & Security who took out both the Outstanding Female Security Professional Award and the Technical Security Award. Rick Beddoes of Meridian Protection Group took out the General Security Award, and Roger Pearce of Sydney Building Technology Brokers was awarded Outstanding Security Consultant.

Winners among the collective awards included the Star Casino Asset Protection Team for Outstanding In-House Security Team, Wilson Security in partnership with Department of Defence for Outstanding Security Partnership, Tactical Training Australia for Outstanding Training Initiative, and Wilson Security for Outstanding Risk Management Solution.

In the Product of the Year awards, Gallagher Security won the Access Control category, Genetec won CCTV, Fire & Security Hardware won Alarms, and Sylo picked up the Communications/Transmission System category. For other awardees, visit the ASIAL website.

Legislation to strengthen telecommunications security

10 November: The Australian Government has introduced legislation that strengthens ties with the telecommunications industry, enabling authorities to better identify and respond to national security threats.

The Telecommunications and Other Legislation Amendment Bill 2016 has been designed to enhance the existing security framework to better protect Australia's telecommunications networks.

"Australia's national security, economic prosperity and social wellbeing increasingly depend on the security and resilience of telecommunications services," stated a government media release. The government, claims that the draft legislation will provide greater certainty for the industry and will better protect telecommunications networks from national security threats.

The Bill is the result of extensive public consultation and responds to recommendations from the telecommunications industry. The Government will refer the Bill to the bipartisan Parliamentary Joint Committee on Intelligence and Security for public inquiry. The proposed legislation reflects the approach previously recommended by the Committee.

Guards face daily racism and violence in Northern Territory

19 October: According to a NT News report A security guard involved in a fight with a group of teens at Palmerston Shopping Centre has told of daily violence and abuse against guards protecting staff and patrons at the retail venue.

Police have asked for the public's help after one of the youths filmed the incident involving Wilson Security guard Forkpah Ballah and posted the footage on social media. A group of teens were apparently involved in another incident with a second security guard only hours later. That guard was taken to Royal Darwin Hospital with head injuries.

Mr Ballah said he and other guards subjected to the daily taunts were considering quitting the industry over the escalating violence. He said teens from the area would often provoke them and then post the videos of occurrences online.

In the footage, a teen can be heard inciting his peers to use force as the security guard attempted to protect himself. Mr Ballah was punched in the head, knocking him to the ground.

According to the report, Wilson security guard Forkpah Ballah stated that abuse and violence occurred daily. A spokesman for Wilson Security, however, said violent incidents involving guards were not a regular occurrence at the shopping centre.

Trans-Tasman collaboration on cyber security

03 November: New Zealand and Australia are working together on practical initiatives to boost trans-Tasman cyber security, according to Communications Minister Amy Adams, who recently returned from Australia where she met with her counterpart, Minister Assisting the Prime Minister for Cyber Security, Dan Tehan.

During a meeting in Sydney, Ministers agreed to work together on a range of initiatives to benefit both countries. Areas of interest include boosting cyber skills, building the cyber capability of small and medium-sized businesses, and co-operating on joint awareness raising campaigns.

"Many New Zealand businesses operate in Australia and vice versa, and our citizens travel regularly between the two countries. We're committed to cooperating at a practical level to help our communities be safe online and ensure they're making the most of the digital economy," said Ms Adams.

"Collaboration and close international partnerships are a key part of implementing New Zealand's 2015 Cyber Security Strategy. Working alongside like-minded countries, such as Australia, is important to ensure we are cyber secure."

New study reframes Australian cyber security skills shortage

Companies that fail to recognise the importance of cyber security expertise within their organisation might be contributing to the view that Australia has a cyber security skills shortage, according to new research by the Australian Information Security Association (AISA).

The recently released study by AISA suggests that the skills shortage is better characterised as a failure of some organisations to resource appropriately, rather than the belief that there are not enough people to fill available jobs. Conducted over four months, the study included a member survey, analysis of job ad's and interviews with key stakeholders.

Seventy-eight percent of AISA members surveyed believe that there is a shortage of qualified cyber security workers for available positions in Australia, however, further analysis of the data suggests that the problem is deeper than demand simply outstripping supply.

AISA members believe a large

proportion of organisations are not putting the right number of people with the right skills into appropriate positions, although many acknowledge there are several organisations which do support well-resourced security teams. This problem is fuelled in part by a failure on the part of management to appreciate information security risks, according to AISA members. This failure may in turn be a consequence of the relative immaturity of the Australian cyber security skills market.

From the supply side, there is evidence of high levels of frustration from those looking to enter the cyber security work force, with too much focus by employers and recruiters on prior experience and detailed knowledge of very narrow and specific areas, which unnecessarily narrows the pool of available candidates.

The reluctance of many employer organisations to invest in development of entry level cyber security workers is a particular concern, given the average Australian cyber security worker is 36 or older, with a large number looking to retire in the next 10 to 20 years. It also raises questions about the career prospects of graduates from vocational and tertiary courses, more of which are being rolled out to address the perceived crisis.

AISA CEO Arno Brok said there are several organisations in the Australian economy that do cyber security well while many do not even have cyber security on their radar or see it as irrelevant to their business. "Those who are doing it well have the budget and understanding of their own requirements to recruit and train the people they need," said Mr Brok.

Ms Siganto, AISA's Director of the Cyber Security Academy (CSA) believes a more mature appreciation of how important information security is to ensuring trust and protecting organisational reputations will help raise the profile of the profession and provide a more clearly marked pathway for cyber security workers.

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

Loktronic 0800 367 565
www.loktronic.co.nz

20851

*Standard terms & conditions of sale apply.



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.

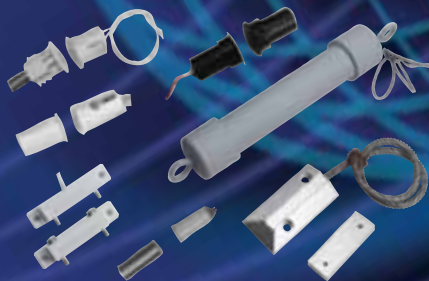


Loktronic



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 Securiton and Interlock.

Gate locks from Loktronic – a wise choice.



Loktronic



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

20756_BP



Key switches

This versatile product range is produced with two functions

Momentary contact (90°)

Turns 90° clockwise from vertical to turn on

Maintained contact (180°) locked on or locked off

Turns 90° clockwise from vertical to turn on

Turns 90° anticlockwise from vertical to turn off

SPDT switch 5amp rating

Accessories are: Key switch mounting bracket
escutcheon for mounting bracket

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

Supplied random keyed. Can be master keyed.

Client's own key cylinder can be converted.

Front or rear fixing.

Designed, tested and produced in New Zealand by Loktronic.



Loktronic



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

20681_KS

Loktronic Power distribution module



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

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

Comprises

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

Designed, tested and produced in New Zealand.



Loktronic



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

20239_PDM

NVR301 SERIES



**POE+300M
RANGE**

- 4/8/16 POE+ channels
- 1x VGA, 1 x HDMI 4K outputs
- Supports H.264/H.265
- 1x HDD up to 6TB
- Onvif Support up to 8MP
- Support P2P, UPnP, NTP, DHCP,
- Supports up to 80Mbps
- Support mobile access



EZ Cloud

CRK
Professional Precision

ph: 09 276 3271
sales@crknz.co.nz

3 Hutunui Drive
Mt Wellington, Auckland, 1060

NVR302 SERIES



**POE+300M
RANGE**

- 8/16- POE+ channels
- 1x VGA, 1 x HDMI 4K outputs
- Supports H.264/H.265
- 2x HDD up to 16TB total
- Onvif Support up to 12MP
- Alarm i/o support
- Support P2P, UPnP, NTP, DHCP
- Supports up to 320Mbps
- Support mobile access



EZ Cloud

CRK
Professional Precision

ph: 09 276 3271
sales@crknz.co.nz

3 Hutunui Drive
Mt Wellington, Auckland, 1060

IPC312/314SR SERIES CAMERAS



- 1080P/2MP/4MP Resolution
- Supports H.264/H.265/UCode
- Smart IR 15m distance
- Triple Streams
- Onvif Compliance
- IP66
- Microphone built in
- Micro SD Card up to 128gb



EZ Cloud

CRK
Professional Precision

ph: 09 276 3271
sales@crknz.co.nz

3 Hutunui Drive
Mt Wellington, Auckland, 1060



Panasonic



(09) 414 5101 OR 0800 ITRONICS

SALES@ITRON.CO.NZ

WWW.ITRON.NZ



Wireless IP Surveillance

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

Distributed by



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



Customized CCTV Kits

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

Distributed by



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



Open Platform VMS

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

Distributed by



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

iSANZ Awards winners announced for 2016

A 200-strong contingent of professionals from New Zealand's information security community gathered in Wellington on 15th November for the second annual iSANZ Awards.

The goal of the iSANZ – or InfoSec Awards NZ – is to inspire, promote and reflect on the New Zealand InfoSec industry and its people, and its mission is to formally recognise the achievements of outstanding New Zealand InfoSec professionals, companies and initiatives or events.

Celebrating the achievements of those working with information security, judged awards were handed out in four categories. A nominated Hall of Fame Award was also presented – recognising one organisation's enduring contribution to the industry.

iSANZ Board Chair Kendra Ross says this year saw a full slate of high quality entries – representing highly-skilled and dedicated professionals and organisations from across the public and private sectors.

“Information security is a complex and multifaceted area, and much goes on behind the scenes to protect and secure networks from cyber attack. It's clear that New Zealand has leaders and innovators in InfoSec the equal of anywhere in the world, and we're pleased through the Awards to be able to honour their contributions.”



The winners in the 2016 iSANZ Awards are:

Best Security Awareness Campaign - PwC, for its Game of Threats simulation game – an interactive simulation of the real-world challenges of a cyber security incident. This category is open to companies or organisations who have successfully implemented a formal security awareness program covering outreach, education and assistance in order to raise internal and/or external awareness of InfoSec nationally.

The judges noted that Game of Threats “has enabled not just one company but many to experience the real threat of a security breach. The creation of a reusable software experience has had a multiplier effect on the cost effectiveness and reach of this campaign.”

Game of Threats simulates the real world challenges of a cyber-security breach from the perspectives of both an attacker and the leadership of an organisation. “The digital experience is a head-to-head strategy that challenges you to make quick, high-impact decisions to either launch attacks to reach your objective or counter those attacks with preparation, response and remediation,” said Steve McCabe, a PwC Partner, in a media release.

Best Security Project / Initiative - Air New Zealand, for its organisation-wide security transformation programme. This category is open to companies or organisations who have successfully implemented an InfoSec security project or initiative. It is also open to companies or organisations who have successfully initiated best InfoSec practices - identifying security gaps, and implementing specific security measures to a successful outcome.

Best Security Company - RedShield. This category is open to security companies with superior security products or solutions that help customers tackle today's most pressing InfoSec challenges.

Best International Superstar - Kate Pearce of Cisco, for her contributions in raising awareness and educating people about cyber security, including among many global communities of interest. This category is open to individuals who achieved significant results in the development or promotion of work that has had a high international profile.

Hall of Fame Award - NetSafe, for its many and varied efforts over the years in helping keep New Zealanders safe online and providing cyber security advice and assistance. Sponsored by Datacom, this award is open to a person, event or company who has made a significant contribution to the wider InfoSec community.

The 2016 iSANZ Awards were sponsored by Check Point (Gold sponsor), Arbor Networks, Blue Coat, Context, Quantum Security, HPE, Carbon Black, Aura Information Security, Sailpoint, Cogito Group and Datacom. Supporting organisations included 1st Tuesday, ConnectSmart, Domain Name Commission, Duo NZ, InternetNZ, Izard Weston, TechDay Security Brief, NZITF, SiteHost and Stephenson Thorner.

iSANZ is a non profit organisation, set up to formally recognise the achievements of outstanding New Zealand InfoSec professionals, companies and initiatives / events. In doing so it aims to inspire, promote and reflect on the New Zealand InfoSec industry and its people.

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




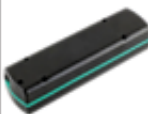




KCS TraceME









hello! TraceME
LoRa™ Technology

VEHICLE TRACKING

PERSONAL TRACKING

| premium | high-end | mid-range | budget | budget | mid-range | mid-range | budget |
|---|--|--|--|--|---|--|--|
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| <u>TM186/R9A10</u> | <u>TM201/R9U10</u> | <u>TMR9B3/R9A10</u> | <u>TM178/R9H7</u> | <u>TM203/R9F4</u> | <u>TM189/R9P4</u> | <u>TM179/R9Q1</u> | <u>TM206/R9D5</u> |

and goodbye GPS?
OBJECT TRACKING

| high-end | mid-range | mid-range | budget | budget | budget |
|---|---|---|--|---|---|
|  |  |  |  |  |  |
| OEM | OEM | OEM | OEM |  |  |
| <u>TM202/R9C7</u> | <u>TM202F/R9C5</u> | <u>TM230/R9M1</u> | <u>TM202B/R9C5</u> | <u>TM900/N1C1</u> | <u>TM901/N1C2</u> |

www.Trace.ME

All trademarks mentioned herein belong to their respective owners.