

June / July 2015

NZSecurity



GAME CHANGER

Greg Watts, Chief Executive, NZSA

INTERNATIONAL DIPLOMACY

the best defence against home grown terrorism

HIGH WIRING

the man who hacked a plane

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



ISSN 1175/2149

www.NewZealandSecurity.co.nz

your electromagnetic locking specialist!

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

Standard features include:

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

Options include:

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

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



uniview

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

Features:

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



Contact Details:

Craig Flint

Telephone: +64 (07) 868 2703

Mobile: +64 (0) 274 597 621

Postal and delivery address:

27 West Crescent

Te Puru 3575

Thames RD5

New Zealand

Email & Web:

craig@newzealandsecurity.co.nz

www.NewZealandSecurity.co.nz

Upcoming Issues

August - September 2015

Banking, Insurance, Finance,
Loss Prevention, Industry Training

October - November 2015

Professional & Business,
Accountants, Lawyers, Managers
and Consultants

Disclaimer:

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

Copyright:

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

CONTENTS

- 6 An interview with Greg Watts, Chief Executive, NZSA
- 10 Gallagher leads the way with perimeter security technology
- 12 C4 Group Ltd receives first Skills Certified Quality Assurance Mark
- 14 Policy, Procedures and Training to Match
- 18 Completions keep training costs down
- 19 Introducing Schlage NDE and Engage
- 20 Transparency and Security for Efficient Deliveries
- 22 Product Showcase
- 24 Making the Most of Mobile Access
- 28 International diplomacy the best defence against home grown terrorism
- 30 High Wiring: The man who hacked a plane
- 32 Damned if you do, damned if you don't
- 36 Axis Communications opens new Wellington office
- 38 New mobile surveillance cameras ensure best first response
- 42 Hills New Product Range On Fire
- 42 Get a FREE Package of Valuable Accessories when you buy a new FLIR AX8 Thermal Sensor

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

*Standard terms & conditions of sale apply.

Loktronic 0800 367 565
www.loktronic.co.nz

2015

Industry Associations



www.security.org.nz



NEW ZEALAND INSTITUTE OF
PROFESSIONAL INVESTIGATORS INC.

www.nzipi.org.nz



Advancing Security Worldwide™

www.asis.org.nz



www.masterlocksmiths.com.au

Visit Axis at ASIAL

Security Exhibition 2015

Stand C41

Melbourne

Australia



Is this an accident waiting to happen?



False claims are serious business

With a network video solution from Axis, you'll be the first to know if a so-called "accident" was anything but unplanned – and prove it.

Our digital cameras record high-quality images you can use to prevent the unscrupulous from filing false claims – or disprove them in court.

And because claims can legally be filed long after an alleged event, images can be stored for long periods without overloading your system.

Want to learn more?

Put an end to lost liability suits once and for all.
Visit www.axis.com/retail or send an email to contact-sap@axis.com for more information.

Distributed by:

CHANNELTEN
SURVEILLANCE SOLUTIONS

HILLS

AXIS
COMMUNICATIONS

Game changer

An interview with Greg Watts, Chief Executive, New Zealand Security Association

It's not an easy task to get Greg Watts, NZSA's Chief Executive, to talk about himself, which is something of an irony given the extent to which his infinitely varied career has honed his promotional abilities. Nevertheless, New Zealand Security Magazine has done just that, and in doing so has gained Greg's insights into the state of the industry and – importantly – how it needs to adapt to the challenges of the future.

Greg has been described as “impatient and demanding and somewhat arrogant at times”, and having travelled to or worked in over 100 countries, one may get the impression that he enjoys change. But his professional history speaks clearly of a man singularly driven and determined – a man who seeks professional and personal fulfillment not in experiencing change but rather in making it... and making it for the better.

NZSM: What has been your career path in the industry?

Originally I wasn't involved in security at all; I went down the engineering route. I actually have a trade certificate in fitting and turning and various other mechanical and electrical qualifications, but then moved into IT in its early days in the 1980s, completing a certificate in computing at ATI. I worked for a number of companies including Fisher and Paykel, where I project managed large production machinery projects as well as overseeing their IT infrastructure.

Then I travelled abroad and worked in the UK, where I was involved in setting up and supporting computer networks for the likes of the BBC and other large corporates. I also became the ‘go to guy’ when the first threats to IT security hit banks, and was brought in to work with the police and security services to bring things back online after various terrorist activities in London.

After about six years in the UK I returned to NZ, and worked for a company called Computerland. I was able to grow their services business significantly into a highly profitable multi-million dollar business unit, and managed to find time to complete a diploma of business at Auckland University.

In 2000 I headed back to Europe and took on the role of services director EMEA for Network Associates Inc, where I was responsible for 24 countries. I was then employed by RSA security as head of global projects, before changing tack and becoming co-owner of a small IT security services company. After selling my first business I invested in various companies from health and IT to manufacturing and distribution. I raised funds for companies that were in trouble and then proceeded to turn most of them around.



I had spent many years working long hours and travelling constantly for work, so my international exposure was very good, but that comes at a price and the price is family. When my two youngest children got to five and seven, I returned to Auckland with changed priorities.

I wanted to play an active role in my kids' lives, so I put my career on hold for a couple of years. It was quite good for a while, but I soon got bored. I needed more challenges but didn't want to work full-time. I was open to any opportunity that would enable me to use my business skills and knowledge to build something, and the NZSA was looking for someone with a keen business sense to come in and reshape the organisation.

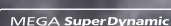
SEEING IS BELIEVING

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



WV-SW598 NETWORK CAMERA

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



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

Droplet formation prevention

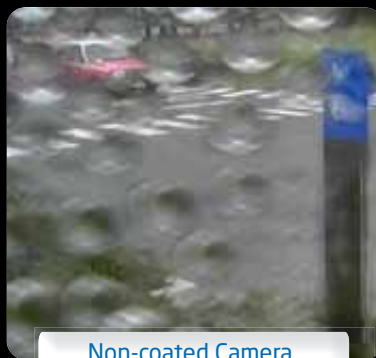
Visibility is maintained due to droplet prevention coating.

Advanced coating technology

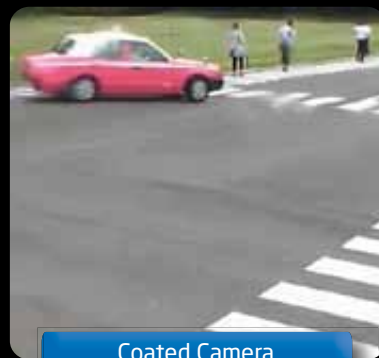
Long-term performance due to advanced coating technology.

Reduced Dirt

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



Non-coated Camera



Coated Camera

NZSM: The passing of the Private Security Personnel and Private Investigators Act was an early challenge. How important was it?

In that first year it was one of my key priorities. At that point, the existing legislation for the industry had been around since 1974, and the NZSA and various stakeholders had been working long and hard with government to write an Act that would be relevant for the industry. My past experience working to overturn an EU directive back in 2005, held me in good stead to assist in the late stages of this legislative reform.

The process was floundering when I joined in February 2010, and my first priority was to help push it along. I worked with various lobbyists and the associate minister and his team to ensure that the NZSA's voice and input in preparing the Act were heard. Once we knew the legislation was to be put through, I negotiated that it be announced at the industry's national conference. It came into law in April 2011.

NZSM: What did it mean for the industry?

The old Act was very loose and there was very little criteria around who could operate within the industry, and on what basis people could be prosecuted for not being licensed, etc. There are now licensing criteria specific to the various functions in the industry, such as guards, investigators, etc. The licensing process means that we now have an industry that's a lot more professional than it used to be.

The key thing the legislation has now is teeth. Under the old Act there was not one prosecution, but under the new act there have been a number of prosecutions in relation to individuals and companies working unlicensed or not fulfilling certain requirements under the act.

But there was a problem. When the Act came into play a mandatory training element was announced, but no criteria or implementation date was given. So from October 2010 many companies simply stopped training their people in anticipation of the new training requirements. A lot of training providers left the industry, so it was a tough time.

I pushed to get the ministry to articulate what the mandatory training would entail, but there was nothing forthcoming. After endless dialog it finally happened in 2013. Mandatory training would be effective from October 2013 and everybody who needed it was required to be trained by October 2014.

This meant a massive three year training backlog had to be cleared in the space of 12 months. This led to my decision to acquire TSSL Training, which some felt was a conflict of interest, but I felt we needed to do it for two reasons: training was an important aspect of what the industry needed in terms of professionalisation, and it also meant we would be delivering training to a very high standard and thus would set the benchmark.

NZSM: What priority have you given to raising the NZSA's profile?

One of the key things that the board in 2010 wanted was for the NZSA to have a stronger profile, and hence I embarked on promotion through various forms of media and events, including a series of radio campaigns. There's a lot more awareness of the NZSA and what we do now. We're certainly high on the list of organisations the media go to now for comment on security related topics.

I've now overseen five annual industry conferences and they've each been successful and profitable. There's no other significant event in the year that brings the industry together.

One of the key things I've focused on is relationships with government and the police, which has been a very positive thing for the industry. For the 2010 Rugby World Cup, I brought the industry and the police together. There had been a traditional lack of trust, but both parties realised that we each had a valid role to play, and the relationship is now stronger than ever.

I've also been able to bring people from the industry together as chair of the technical committee for the Auckland city council CCTV project. And I'm now on the crime prevention partnership, which is the industry and police working together to prevent crime. This would never have happened in the past, and the NZSA has played an important role in making it happen.

The Ministry of Justice refers any questions they receive regarding the PSPPI Act to the NZSA. This comes about by trust. They're not going to send people to talk to us unless they're confident they're going to receive the right message. If the DIA wants to prosecute a company for negligence they come to us. Again, that wouldn't happen if there weren't that trust or respect.

NZSM: You've stated that the NZSA has been criticised as a 'boys' club'. Is this still the case?

Well to be honest, I've never been witness to any activities or decisions that would support that view, and would personally not be involved in the organisation if it were true. However, when I first came on board, our by-laws were such that voting rights were skewed heavily in favour of the big players, so basically the four large companies could control the NZSA and its messages to the industry.

I decided that we had to make it fairer, so I re-wrote the by-laws to cap voting powers, so a large company with 3,000 + employees has no more voting power than a company of 100 employees. There is no way now that there could be a boys club as nobody can bully anybody else into making decisions and nobody has any special powers or privileges.

The other thing we introduced was improved governance, including job descriptions for board members, but we need to do more. Members of the board currently have to come from the industry through our membership, which I believe is wrong. We don't have anyone on the board who can look at the industry from an outsider's perspective, which has been to our detriment. We have to have a mix of industry and representation from other stakeholders.

NZSM: What are some of the key issues facing the industry?

The industry has some very good operators, but there is a shortage of strategic type people in senior management roles. This has happened because existing management tend to come up through the industry from the grass roots, and they're not always equipped with the business, finance and marketing skills as someone who's been through a business degree or worked in other industries in management roles.

I'd like to encourage executives from other industries to come over to the security industry and look at what sort of impact they could have. I've tried to encourage more interaction at that level and to bring people from abroad to talk to people in the industry through strategic training events. It's an area we need to work on more.

As operators one doesn't necessarily see the wood through the trees, and sometimes having a strategic view about what technologies, services and processes we could be using is very important. We need people to be pushing the boundaries of what companies can deliver.

NZSM: What other major challenges do you see?

There's a lot of consolidation going on in the industry right now. Many companies are in acquisition mode, and some of that consolidation involves the sale of all or part of a company to overseas investors. There are positives and negatives to that.

International players are in the process of improving and diversifying their service offerings, and some in the industry won't have the financial resources or skills to compete as these operations mature. Our industry is getting a wake up call right now and needs to look at what's happening overseas and identify what the industry's going to be about in three to five years. It's not going to be as simple as merely providing a security solution.

In terms of residential, people are going to want integrated solutions, so if it's your home you're not just going to want something to control your security but also the temperature in your living room, etc. And commercial's the same; now it's not just about access control, it's analytics and security-based technologies that improve business functions and even generate additional revenue that are already heavily used overseas but not yet here. The companies who will be unwilling to change or adapt will be the ones who don't survive.

NZSM: What can the industry do to maintain its viability?

What does security mean today, and what will it mean in the future? It's not as black and white as it used to be. We need to constantly refine and review the mandatory training, and there are also many parts of the act that need to be amended to bring it into line with emerging technology. There are always areas that need improving. That's what the NZSA is here to do.

The industry is still perceived by many as a transient industry. People don't necessarily see the opportunity of having a professional career within the industry, and we need to change that. We need people to be coming out of universities thinking that the security industry is something that they want to explore.

We need to be pushing for an apprenticeship or cadetship program. There are a lot of people who are unemployed who could be brought into the security workforce through government-funded apprenticeships. Most companies are struggling to find people because the industry is growing. The government could be stepping up and we could be developing an apprenticeship program, and this could provide the career path. We need this, and I'll keep pushing for it.

NZSM: You've done a lot and achieved a lot, especially considering you work part time. What motivates you now?

As long as I'm achieving positive results and making a difference then I'm happy, as soon as it turns into a role of farming - running a steady ship - then it may no longer suit me. But there are a few more goals I want to achieve while I'm here that I'd love to see through, such as more influence in government. I also want to get out and talk to more of our members.

I enjoy assisting with industry mergers and acquisitions, providing business advice, and helping companies develop. I really like that side of it and it's where the industry is lacking somewhat. I've had a number of personal business successes and failures, but I've learned more from my failures. I would like to continue sharing more of what I've learnt to ultimately make the industry a better place.



CAME
AUTOMATION

**Reliable Proven
Quality**

**Now With
Reliable Supply
&
Technical Support**



Gate Automation Direct

Direct To The Trade

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

0508 438 428

Gallagher leads the way with perimeter security technology

Hot on the heels of winning the NZ Engineering Excellence Award in 2014 for their perimeter technology - K20 Tensioner Link System and Z10 Tension Sensor – Hamilton based design and manufacturing company, Gallagher, are seeing continued demand for their innovative perimeter solutions.

“Our approach to scalability and integration on one platform, as well as the synergy with our access control products, are things that really set Gallagher apart in the world of perimeter security,” says Craig Malins, Senior Product Manager for perimeter security at Gallagher.



Craig Malins, Gallagher's Senior Product Manager for perimeter security



Although not a new technology, Gallagher notes a continuing demand from the global market for layered perimeter technology. Gallagher's range of perimeter technologies and ability to integrate technologies onto their security management platform, Command Centre, provides incredible flexibility to meet customers' requirements.

The Gallagher suite of perimeter products focuses on proven, highly developed, innovative technologies that deliver an effective safe deterrent, with low false alarm rates, a high probability of detection, and superior reliability. Gallagher's fence-line technologies can be applied in single or multi-technology

formats to suit customer budgets and security needs. With customers ranging from small commercial sites to highly secure enterprises, including military and corrections facilities, Gallagher has gained a strong reputation as a world leader in the design and manufacture of cutting-edge innovations.

“There are some exciting new product developments in our perimeter suite that will be entering the market in 2015. We're definitely one to watch.” said Malins.



Total site security

Protect your most valuable assets with perimeter security solutions that integrate with CCTV, access control, and more.



C4 Group Ltd receives first Skills Certified Quality Assurance Mark

Registered training provider, C4 Group Ltd, is the first provider in the security industry to be awarded the Skills Certified quality assurance mark.

“This endorsement is so important for our industry and business. It recognises the great performance of our trainers and our training programme and it boosts industry standards across the board meaning students are getting the best training possible,” say C4 Group Ltd Directors, Kathy Wright and Chris Lawton.

Skills Certified is an initiative of The Skills Organisation to measure and benchmark the quality of training delivery by Tertiary Education Organisations (TEOs) across all industries.

Put simply, Skills Certified is an endorsement for any TEO displaying exceptional training at a consistently high level. C4 Group achieved the certification in April 2015.

“We feel very honoured and privileged to be awarded this. It validates our hard work and demonstrates the importance The Skills Organisation places on quality training.

“The evaluation was also great for looking at how we can improve our processes to better service our students,” says Kathy.

What does it take to become Skills Certified?

In order for an application to be considered, the training organisation must have a clear and effective system in place for developing training programmes,



C4 Group Ltd Directors, Kathy Wright and Chris Lawton receive Skills Certified Quality Mark Assurance from Veronica Brajkovich – The Skills Organisation, Quality Assurance Project Lead

have the necessary resources available to students, a coordinated training approach and of course, exceptionally skilled and qualified tutors.

“This criteria definitely gives training providers a challenge and impetus to continue moving forward. It will foster growth and maturity for security industry training and strengthen client confidence in the security industry which is invaluable,” says Chris.

Skills Certified is a step in the right direction for all industries aiming to

benchmark their training and produce exceptional professionals. As training providers are evaluated, the quality of training delivery will continue to rise.

For more information and to register for assessment as Skills Certified endorsed contact The Skills Organisation at skillscertified@skills.org.nz.



Skills Certified



Certificate in Investigative Services

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

The course establishes a base level of professional skills for those wishing to apply for a New Zealand Certificate of Approval (Private Investigator) and commence a career as a professional investigator.

It is consistent with the Australian qualifications 'Certificate III in Investigative Services' and prepares the learner for further study for professional certification with ASIS and ACFE.

Topics include:

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

**Our trainers are experienced investigators and consultants.
Check out our website for more information
www.c4group.co.nz**



Health & Safety Representative

(Security Stage 1)

New Health & Safety laws are coming into effect this year and this legislation will impact on the entire security industry.

C4 Group courses are designed for security companies to meet their legislative obligations and ensure they have an effective Health & Safety Management System.

No matter what size your organisation is a trained Health & Safety Representative will help you reduce accidents and injury as well as save money. NZQA Unit Standards will be awarded on successful completion of the course.

Topics include:

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

**Our trainers are experienced
H & S consultants in both New Zealand and Australia.
Check out our website for more information
www.c4group.co.nz**

Ensure your business is in safe hands

Investigate our First Line Management qualifications now

skills.

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



Policy, Procedures and Training to Match

Good security counters terrorism threat

Last December's Lindt Café attack in Sydney demonstrated that terrorism or terrorism-styled acts can happen where we least expect them to. The event violently thrust small business onto the international terrorism map, and in doing so raises significant implications for the security practices of businesses that may not have previously contemplated the terrorist threat.

Seeking answers to the many questions now being asked by small businesses, we speak with counter terrorism expert and New Zealand Security Association Training Director Stewart O'Reilly. Stewart is a Certified Anti-terrorism Specialist (CAS), and prior to NZSA spent 15 years working in an intelligence role.



NZSM: What type of staff pre-recruitment screening options are available to employers, and how practical are they?

For events such as the Rugby and Cricket World Cups there is an additional level of screening where checks will be run against intelligence agencies' databases. But this is only for big events, and such checking is not accessible for the general screening of employees at a shopping centre.

Even then it's not going to be comprehensive because the risks that we're talking about won't necessarily show up on those databases. When you think about the teenagers that were recently arrested in Melbourne, there was no depth of involvement with a terrorist organisation. It's not like you could have background checked and found them. They're pretty much invisible.

Even Monis, the Lindt Café gunman, who was well known to authorities wasn't on the watch list. He had been on but had been taken off, and there were plenty

of indicators there that this guy was building up to something, not necessarily a terrorist attack.

NZSM: So background checks don't necessarily achieve anything?

It's something that is a relatively simple process worth doing, but it shouldn't give you the satisfaction that you've covered the security bases and that your staff are clean. The likelihood is that if someone was planning a terrorist attack and wanted to get someone into that position, they'd use someone that was very clean who had no history and who would not come to anyone's attention.

NZSM: So, are there any avenues available to an organisation at the employee recruitment stage?

There are additional checks that you can make as part of the initial employment process, but it would be unrealistic to expect employers to do these because of the cost involved. You'd basically have

to be subjecting everybody to a lengthy interview process by someone who knows what they're doing in terms of the questions they're asking. You'd be putting them through a wide range of testing, the kind of psychometric testing done for senior staff in some organisations.

NZSM: Is there anything else that businesses can do in terms of how they're managing their staff?

They can watch behavioural changes. There will be indicators that people are behaving differently, which might be a trigger that they're going to do things. If someone starts to act out of the ordinary it should be something that managers look at – not necessarily an indicator that they're going to blow the place up but that something is happening with that person.

Normal HR practice should be that someone sit down and have a talk with them, and that might reveal stuff. Such a chat in a potential religious extremist example, may elicit comments such as "I've found a new religion." "I'm taking



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

Marc Cisneros

Protector,
Advocate,
Guardian.

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



WD Purple™
Surveillance Storage

WD Blue

WD Green

WD Black

WD Red

See more of Marc's solutions at:
wd.com/choice



absolutely™

my religion more seriously now.” If you look at international experience many of those susceptible to extremist views are not converts but they’re coming back to their religion and are very serious about it; there’s a major lifestyle change.

NZSM: In the media a clear correlation tends to be made between Islamist extremism and terrorism. Is this accurate?

Islam is clearly a religion of peace and those that practice terrorism contradict this. Certainly Islam is not the only source of terrorism. The most notable terrorist attack in this country was carried out by the French Secret Service. Our most recent case was the threat against milk products. These are not Islamic threats.

Eco-terrorists and animal rights activists are actually more likely to be a source of terrorism in this country than Islam. But we’ve got to recognise that the attacks we’re seeing in the media linked to Islamic extremism are happening worldwide and we’re not immune to them.

NZSM: Should the measures that businesses put in place to combat the threat of an extreme event differ according to the type of event?

Each threat requires a response in accordance with the threat, not with the perpetrator. Who makes the threat doesn’t matter except in terms of evaluating whether or not it’s likely to be real. From a security practitioner’s point of view with a person pointing a gun at you it doesn’t matter why.

We would advocate a risk management approach to this. What is the risk and how do we manage it? We’re operating with limited resources and so we can’t manage every risk. We’re operating under social conditions that won’t let us put big barriers around every shopping centre. So, what do we need to do? If you think about a simple risk matrix, you’ve got to measure likelihood against consequence and so a terrorist attack is really low likelihood but extremely big consequence.

Therefore we’ve got to pay it some attention but we’re not going to pay it the same level of attention in a retail environment as shoplifting, which is a day-to-day occurrence. The problem with an extreme event is that it would have major consequences; it doesn’t matter whether its caused by an earthquake or tornado or a terrorist, we’ve still got to plan for it and have mitigation strategies in place.

NZSM: So is it the case that we can’t really plan to avoid such event but we can plan to mitigate what happens if it happens?

No, you can take some steps to prevent it happening to your place. You can’t prevent what’s happening in the minds of the people who have the incentive to do it. People who want to make these attacks may have the intent and the capability, but we can’t influence those things... the government can but we can’t. All we can take care of is our own vulnerabilities, so we can make it harder for them, and if we make it harder for them to attack the target we’ve been charged with protecting, well maybe they’re going to attack somebody else’s target.

NZSM: So for example, if your shop has particularly good security but the one next door to it doesn’t and is a weak link, what can you do?

You’ve always got to take into account your neighbours in terms of your own security. If the office next to you just happens to be the American Consulate, then the level of risk you’re facing from a terrorist attack is much higher than if you’re running your café from anywhere else in the country. Your operational environment has to be taken into account.

The degree to which you can influence what your neighbours do themselves is pretty limited but you have to take into account that they are a weak link in your security. In the retail mall environment, however, there is a degree of consistency because the mall operator provides security and there’d be certain things tenants would also be required to do.

The more you can reinforce the appearance of security the better off you are. It presents a harder target. That’s a general security principle, because in a retail environment you want the shoplifters to go somewhere else, you want the gangs that hang around selling drugs to teenagers to go somewhere else, so you just make it difficult for them.

NZSM: There is an argument that NZ businesses have a relatively high level of complacency in relation to the threat of terrorism. Do you agree?

Security risk management is about evaluation of the risk, and we do face a lower level of risk in New Zealand. The Australian experience has relevance. We have similar populations, and we’re both involved militarily with the Americans.

New Zealand is on the UN Security Council... that’s kind of a biggie in terms of our profile. Regionally and globally, however, they have a bigger footprint so they do attract more attention.

New Zealand is a harder operating environment for a terrorist in terms of distance and the nature of our society: it’s harder to be invisible here, the communities are smaller and they talk to each other. It’s easier to have an overview from an intelligence perspective of the communities here than it would be in Australia because they’re bigger and they’re more spread out.

So we have advantages, but what we’ve got to see is that we’re socially and politically linked to Australia, so what’s a threat to them is a threat to us. The fact is that the Australians have been concerned for years that we’re an easy back door to them. The target may be in Australia but it could be attacked by people resident in New Zealand.

NZSM: Are we presenting ourselves collectively as a rather soft target?

In terms of NZ businesses, there is a degree of complacency. In terms of what’s happening in the world many haven’t made the connection that we’re a part of that world. There’s a degree of ignorance, but the government’s quite keen to not have people panicking about this by saying there’s an extreme threat of terrorism because there isn’t.

Our threat levels have just been raised to ‘very low’ so we’ve just got up off the ground. But the government has stated repeatedly that there are 30 to 40 people on their watch list and I would guess that that’s a conservative figure because you’ve got to look at how many people are those 30 or 40 people talking to. The number is probably much bigger, and if you take that as a percentage of our population it would be a significant figure compared to Australia.

I don’t think there’s a great degree of complacency, but businesses tend to have to see that they are potential targets before they will take action.

NZSM: Are you seeing that businesses in Auckland are taking a greater interest in terrorism-focused security?

You don’t want to be spending your whole time on it because there are more day-to-day threats. However, by looking at awareness around terrorism you’re also picking up on other suspicious behaviours that could indicate someone’s planning a

fire door holding electromagnets



FDH40S

unbreakable universal mounting

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

10 YEAR GUARANTEE*

Designed, tested and produced in New Zealand to AS4178

- A) Wall mounted, 126mm extn. tube (overall 202mm)
B) Wall mounted, 156mm extn. tube (overall 232mm)
C) Wall mounted, 355mm extn. tube (overall 431mm)



FDH40SS

stainless steel surface and flush mounting

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



10 YEAR GUARANTEE*

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



crime. If you're training someone to look for suspicious behaviours, you're actually covering off both things.

NZSM: Do you envisage seeing bag checks at shopping malls in New Zealand any time soon?

No. It would actually take something to happen before it would become a reality. It's going to put people off shopping.

In New Zealand, access to firearms is limited, so bag checking is a pretty useless measure to counteract the most likely attack, which might involve knives. In the case of a shopping centre, you don't even have to bring in a knife in with you; you can just buy once inside the mall.

NZSM: So the incident that occurred at the Lindt Café in Sydney... terrorism or not?

For a security practitioner it doesn't matter in terms of the why's behind it, but it fits terrorism in other ways in that

the gunman hooked onto politically motivated reasons. In this way it echoed the pattern we see in recent lone wolf cases: it's not that the perpetrator is part of a terrorist organisation that's telling them to do something, but rather there are some other issues in their life that have led them to a form of extremist belief.

Nevertheless, I think it's safe to call that example terrorism. And if you think about why he chose the Lindt Café as a target, he did so because it was in camera view of Channel Seven's breakfast television program... be aware of your neighbours!

NZSM: From a business perspective, there's practically nothing that the operators of the Lindt Cafe could have done?

No. You can't stop your customers coming in. If you put measures in place that would make a venue unattractive to come to, you're going to lose customers. So until society recognises the heightened risk, you can't get away with those sorts of measures.

I was living in London when the IRA had a bombing campaign, and it was really fascinating to watch what average people would put up with in terms of the intrusive searching on the tube and at public events. After one attack, the police even conducted door-to-doors. So it intrigued me as to what people tolerated in those conditions, but it was because they recognised that allowing this infringement on their civil liberties would help to protect them.

NZSM: So really the best thing a business can do is to have their training and security protocols in place and to be actively following them.

Policy and procedures and training to match them. And that comes to the defence part where you're trying to spot things potentially going to happen and the response part where something has happened and you need to be able to respond to it effectively. Either way, it's all around those three things: policy, procedure and training to them.

Completions keep training costs down

While the push to complete mandatory training in 2014 saw a surge of training activity, the first quarter of 2015 has seen a steady decline.

The security industry faces a critical year in terms of training performance.



Skills Industry Manager, Wayne Abel

It is important trainees complete their courses and programmes they undertake.

Without growth in programme and trainee completions the training funds available to the security sector will be placed at risk.

Training will become more expensive, with the likely consequence that even fewer personnel will earn nationally recognized qualifications.

Industry Manager Wayne Abel says the industry does not want training costs to escalate out of control.

"It's difficult, we really want to see training in the security industry grow. Customers are aware of qualifications, and they want to know they're getting top quality, skilled people. The way you can show this is through trained staff.

If we want costs to remain at reasonable levels then we need to get serious about the completions of qualifications.

There's no beating around the bush, completions equal funding.

The Skills Organisation is here to support all businesses, employers and trainees in completing their qualifications.

Certification often gives companies a competitive advantage when responding to tenders. By having the ability to offer quality, skilled and certified staff you set yourself apart from other contenders for business.

In addition, you are investing in your staff, giving them tangible gains they can take with them throughout their careers."

skills.

True innovation. Strong value.

Introducing Schlage NDE and Engage

The Schlage® NDE Series wireless lock with ENGAGE™ technology is designed to be easy to install, connect, manage, and use. Developed specifically for facilities that want to upgrade to electronic credentials for improved security and efficiency, it is ideal for interior office doors, common area doors, and sensitive storage spaces with a cylindrical door prep.

NDE Series wireless locks simplify installation by combining the lock, credential reader, door position sensor and request-to-exit switch all in one unit. NDE Series wireless locks utilise the standard 54mm cylindrical door prep and can be installed in minutes with only a Phillips screwdriver; no need to install additional components, drill holes or run wires to each opening.

ENGAGE cloud-based web and mobile apps make it easy to configure lock settings, add users, and view audits and alerts from anywhere. For advanced capabilities including user schedules, auto unlocks & holidays, NDE Series wireless locks can be managed with software from our access control alliance partners. NDE Series wireless locks can be updated manually at the lock with the ENGAGE mobile app, automatically daily

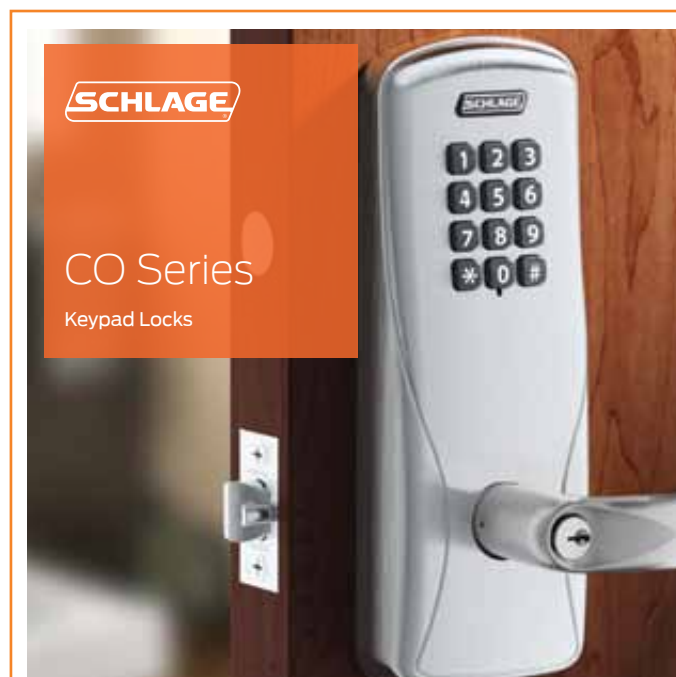


over Wi-Fi 2 or in real-time when connected to an ENGAGE gateway. NDE Series wireless locks with ENGAGE technology are compatible with most proximity and smart cards including aptiQ™.



Quick facts about NDE Series and ENGAGE:

- ENGAGE™ is a connectivity platform that simplifies the ability to connect people and openings to deliver cost effective intelligence and efficiency to any facility.
- Conveniently retrofits into standard door prep without drilling additional holes.
- Installs in about 15 minutes with just a Phillips screwdriver. Compatible with proximity as well as aptiQ™ smart credentials.
- Free cloud-based ENGAGE™ mobile and web apps make it simple to configure lock settings, add users, and view audits and alerts from anywhere.



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

For more information, contact
Allegion (New Zealand) Limited
on 0800 477 869 or visit
www.allegion.co.nz

www.allegion.co.nz



Transparency and Security for Efficient Deliveries

Helping a fragmented logistics industry

Patrik Anderson, Business Development Director for Transportation at Axis Communications

Keep things simple, as we have been told many times. But things are often more complex than we think. For example, our transport and logistics clients are constantly faced with the question: how complex can it get to move goods from point A to point B?

After all that is what the backbone of the global economy is all about. We take it for granted that goods arrive on shelves in stores and customers receive their orders on time, often the next or even same day delivery. Anyone working in the logistics industry of course knows that there are a much more complex process behind this simply order. That the exchange of goods between different stakeholders in the value chain encompasses a variety of different transport modes that stretches across multiple geographies to keep the wheels of the global economy spinning.

Shared responsibilities & value chain roles

Shared responsibilities and specialised roles in the logistics industry are key to getting high efficiency and competitiveness between the various market actors.

Logistics companies work together everyday in this environment with their own assets, shared assets and resources, or no asset at all. Some position themselves as independent freight forwarders. Some also take on the carrier role for parts of geography, a specific route or mode of transport. Independent of such value chain roles, goods travelling from one part of the world to another will eventually be handled by various companies with shared responsibilities. Even for the 3PL giants who have complete end-to-end logistics solutions, there is a need for cross-docking at various points during a route to keep efficiency up and costs down.

Attacks and incidents

Looking at the complex global logistics flows from a security perspective, we have seen an unfortunate increase in attacks against supply chains across all regions and modes of transport. Several organizations and government bodies report the same alarming statistics. Organized crime and everyday criminals have found a new target in the flow of goods as a means to make fast profits.

A key driver for this development is the overall move away from cash in favour of cards and online payments. How can we work against the increasing number of incidents? How can we help protect a lone driver or parked trucks and trailers?

Deviations of goods and transport

Manufacturers have carefully and over a long time built up quality systems to ensure that their products and solutions meet the expectations of their customers. But what happens to products after they leave the boundaries of the manufacturer's quality system? What if something unexpected happens during their transport, when there are a lot of shared responsibilities between different parties? How can the logistics industry more easily and cost efficiently backtrack the series of events that lead to an incident or attack between point A and point B? Lastly, how can precision be improved on a global scale?

Track and trace

One trend within the logistics industry is to increase the use of telematics of various types to track and trace goods along their





journey. Some have started to use this as a post-incident tool to verify the routing of goods. Others use this as a tool to monitor and control both fleets and goods in real time.

This method is based on capturing the identification of passing-through-goods by scanning barcodes or RFID (radio-frequency identification) tags at warehouses, logistics and distribution centers. However it cannot reveal what truly happened to a given shipment, nor the present status of the goods. It doesn't allow us to tell who did what, when, why and how the goods are affected.

Of course one can, just like the great Sherlock Holmes, attempt to make advanced guesses on why unannounced or non-planned stops along a shipment's route have occurred. But what does it really mean, if a barcode is scanned and the shipment is accounted for at a cross-docking station? What does it say about a possible damage or losses of the goods? The scanned data does not allow for a visual post-verification of the goods and thereby not creating transparency.

Visibility but no traceability

So how can we create visibility and remove the costly and time consuming guess work from the investigations of incidents, claims, attacks and deviations of transports and goods?

How can we then gain a crisp clear picture from any warehouse, cross-docking station, logistics center or truck, trailer or delivery van?

The first step would be to simply equip all locations, vehicles and the flow of goods in those locations with smart modern network video cameras. Cameras that can provide not only a high-quality video image in any light, temperature or weather, but also are intelligent enough to detect, for instance, unwanted movements and activities using video analytics. Cameras that also can cooperate and cost-efficiently cover all relevant parts of large outdoor areas and within

the buildings using computer network cabling infrastructure already in place for the barcode scanners & RFID trackers. But is this enough? How would we go through recorded video of millions of individual goods that are shipped every day to find just that particular one that we are interested in? How can we create a complete, visible track of one particular parcel out of all handled on a daily basis?

Clarity and transparency at any given moment

To create a clarity tool for backtracking any individual event around specific goods, we need to integrate the tracking and tracing methods with the visibility tools. Already today any WMS (warehouse management system) or ERP (enterprise resource planning) system keeps track of identification of goods. Any telematics and fleet management system today keeps track of positions at all times of vehicles. If we simply combine video data with the tracking and tracing data to form one common system, we have a winner!

This enables us to track the complete flow of goods and zoom in on individual events in seconds, showing in detail the goods status, who did what and when with the goods and the impact on them. Modern network video systems have this powerful ability to integrate goods identification data with digitally stored video data using crisp clear video quality. Such systems integrate with WMS, ERP, RFID, Barcode and fleet management systems with the VMS (video management software).

Positive business effects and a beginning of a safer and more transparent world of logistics

The positive business effects from network video systems in the logistics world can be grouped into the following areas:

- **Confidence and quality branding**

A much more secure and solid platform to handle any claim, deviation or incident is

now available. The network video system cleverly promotes the existing quality thinking and quality processes already in place so that it can become part of the branding. Users will actually be able to show any and all goods! This will give brands a competitive advantage on the market and act as a great confidence boost for the company.

- **Minimal time & costs for internal and external deviation investigations and claims**

If a follow-up on actual deviations or claims of deviations is needed, we will now have an effective formula-1 tool where the time searching for the origin of the problem, demonstrating the exact sequence of events and implement corrective actions, is now fully integrated and automated in one single system. The network video system will also help provide clear evidence. Usually a deviation research is completely done within minutes, including the evidence making, should it be needed.

- **Reduction of false-claims**

Logistics operators that have implemented modern network video systems into their goods flow, all testify that the level of false claims is reduced to a minimum already in the first months of operation. For many, it is already a thing of the past!

- **Deterrence of supply chain attacks & increased likelihood of solved crime**

Video surveillance and tracking together cannot prevent and solve all types of attacks against the logistics chain. However they will surely as a deterrent and increase the likelihood of solving many of these crimes. Similar to how intelligent surveillance has revolutionized many other areas.

- **Direct bottom-line savings in less lost or erroneous goods, deliveries or shrinkage**

Because of the transparency and clarity of modern network video systems in logistics, the improvements on the bottom line will be direct and continuous through operation. It will act deterring for deliberate shrinkage and it will help to correct quality improvements through organizational learning. The best thing is that it is completely scalable; from very small systems with few strategic network video cameras and goods identification integrations to complete total solutions with hundreds and thousands of connection points in warehouse, distribution centers and vehicles in the fleet. *It really is.*



HCVR7404L/7408L/7416L

Dahua Tribrid Recorder

- Each channel supports analogue / HDCVI / IP video input
- 1x HDMI / VGA / TV video output
- Supports 4 SATA HDDs onboard
- Remotely Accessible by any webbrowser & any smartphone app
- Supports other brand IP Cameras

Distributed by



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



Dahua Customized 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



Dahua 1080P CVI Camera

- Dahua Full-HD (1080P) HDCVI Smart-IR (30m) Weatherproof Camera
- 2.7-12mm Motorized zoom lens
- DWDR, Day/Night (ICR), AWB, AGC, BLC, 3DNR, Auto iris, Auto focus
- Realtime smooth transmission on existing coax or CAT5/6 type cable with HD video baluns

Distributed by



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



ITRON SECURITY & AUTOMATION



Power supply cabinets

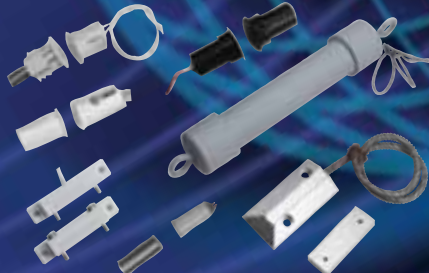
- Mounts for our 5 most popular models of power supplies; 6 key-hole anchor points for easier mounting
- Lift off hinged doors for added convenience
- Louvre ventilation on doors
- Roller ball reed switch provides anti-tamper to front and rear of cabinet
- 6 x 25mm knockouts, 2 each sides and bottom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

Designed, tested and produced in New Zealand.



Loktronic 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_IPSC



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 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.



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



Loktronic for gate locks

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

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


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

Gate locks from Loktronic – a wise choice.

Loktronic

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

20756_BP



Key switches

This versatile product range is produced with two functions

Momentary contact (90°)
Turns 90° clockwise from vertical to turn on

Maintained contact (180°) locked on or locked off
Turns 90° clockwise from vertical to turn on
Turns 90° anticlockwise from vertical to turn off
SPDT switch 5amp rating

Accessories are: Key switch mounting bracket
escutcheon for mounting bracket

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

Supplied random keyed. Can be master keyed.
Client's own key cylinder can be converted.
Front or rear fixing.

Designed, tested and produced in New Zealand by Loktronic.

Loktronic

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

20681_KS

Loktronic Power distribution module



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

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

Comprises

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

Designed, tested and produced in New Zealand.

Loktronic

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

20238_PDM



Panasonic



Exmor
CMOS Sensor

HDCVI

(09) 414 5101 OR 0800 ITRONICS

SALES@ITRON.CO.NZ

WWW.ITRON.NZ

uniview 8 Channel Premium IP Kit



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

Includes:

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

CRK Professional Precision

Ph: 09 276 3271 • www.crknz.co.nz

uniview 4 Channel IP Kit



Perfect for home or business use.

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

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

CRK Professional Precision

Ph: 09 276 3271 • www.crknz.co.nz

uniview 32 Channel NVR



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

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

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

No port forwarding or router configuration.

CRK Professional Precision

Ph: 09 276 3271 • www.crknz.co.nz

Making the Most of Mobile Access

The latest access control systems improve security while enabling mobile devices to be used as credentials, significantly improving convenience while delivering a better user experience. Mobile access control simplifies the secure identity management process for facility access, while also paving the way for solutions that can integrate multi-layered physical access control (PACS) and IT security into unified systems. Other exciting developments include the emergence of gesture technology that makes long-range door opening safe and convenient, new mobile credential form factors such as smart watches, wristbands and other “wearables”, and the emergence of biometric authentication to further improve mobile access security and convenience.

Deployment Considerations

With today’s mobile access technologies, smart devices can be used as universal credentials for accessing multiple buildings, IT systems and other applications using NFC and Bluetooth. These devices provide users with extremely convenient vehicles for opening doors and performing other tasks that require presentation of a secure credential.

There are a number of prerequisites for deploying mobile access control. It is important that the solution support the broadest possible range of phones, without having to insert the phone into a sleeve or slide if it doesn’t support certain features. This ensure that users

can choose freely from among today’s wide range of commercially available devices. Also important is the ability to use a single reader that simultaneously supports existing legacy ID cards as well as Mobile IDs. And finally, it must be easy for system administrators to issue and revoke Mobile IDs using a fast and straightforward process, and for users to download the necessary apps with which to receive them.

Beyond these basic prerequisites, the access control system also must be capable of scaling and adapting as requirements change and security threats evolve. This requires an access control platform that supports open standards, so that organizations can add features and upgrade their security capabilities when necessary.

Today’s solutions meet each of these prerequisites, providing everything that is needed for deployment, along with end-to-end identity management and an easy path to future mobile applications. These solutions enable organizations to immediately begin using Bluetooth Smart- and NFC-enabled smartphones and other mobile devices as an alternative to metal keys and smart cards in today’s increasingly popular BYOD mobility environment. Basic components of these solutions include mobile-enabled readers, Mobile IDs, Mobile Access apps, and access to cloud-based portals that administrators can use to manage users and issue or revoke Mobile IDs over the air. Ideally, readers should also be interoperable with 125 kHz Prox and

Mobile access control simplifies the secure identity management process for facility access.

high-frequency technologies to optimize flexibility for using both cards and mobile devices.

Bluetooth and Gestures

Today’s mobile access solutions also should take advantage of Bluetooth Smart connections and new gesture technology advances so users can unlock doors from a distance.

Physical access control has historically relied on close-range “tap” transactions (directly tapping an RFID card to a reader) to authenticate a user and open a door. Logical access control has used the same tap authentication model, but this precludes such desirable use cases as automatically locking the laptop when a user walks a certain distance away from it. Achieving this longer-distance transaction capability results in a new model that increases security while also improving convenience – two concepts that typically have been mutually exclusive.

Switch to the access control that changes with you.



**Move to HID Global's adaptable iCLASS SE® Platform
and start using the technology of tomorrow, today.**



When it comes to access control, it can be difficult to stay ahead of changing security concerns and technology demands. Go with HID Global's iCLASS SE® Platform—the new standard in access control that positions you for the future with an open, adaptable solution that easily integrates smart cards, mobile devices and whatever tomorrow brings. Join the revolution in evolution and get greater security, flexibility and simplicity.

Make your change by visiting hidglobal.com or contact us at +613 9809 2892 or email at asiasales@hidglobal.com.

© 2015 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, and iCLASS SE are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission.

While the most common RFID card technologies for tap transactions typically have a read range of only 1-3 centimeters (cm), Bluetooth extends the transaction distance that systems can manage from a few centimeters to many meters, making it an ideal choice for the longer-range authentication model with mobile devices. A new and special feature of Bluetooth Smart is the ability to configure this read range allowing the user to determine if a phone should be tapped to a reader in order to open a door, or if longer range activation should be used. When this Bluetooth connection is combined with gesture technology, users can open doors from these longer distances by rotating their smartphone as they approach a mobile-enabled reader. In addition to improving the user experience, gesture-based access control will also increase speed, and minimize the possibility of a rogue device surreptitiously stealing the user's credential in a "bump and clone" attack.

Bringing Wearables and Biometrics into The Mobile Mix

The benefits of mobile access will only grow as new devices are added to the product ecosystem. For instance, adding wearables to the ecosystem will give users the freedom to leave home with nothing but a digital wristband carrying their ID.

Plus, as wearables join smartphones and other mobile devices for access control, we will see greater momentum behind biometric authentication models. We're already seeing the growing adoption of mobile biometrics for payment applications. The latest solutions focus less on technology and more on the user experience, taking a key step toward the long-time goal of killing PINs and passwords by making it easier to know if someone is who he or she claims to be. As this model grows in popularity along with the value of the transactions it protects, there will be new pressures to provide even better security. Sensor advancements will help here, along with improvements in privacy, encryption, tamper protection and anti-spoofing capabilities. Other innovative use cases include "binding" a person to a device such as a key fob with a fingerprint sensor – all without deploying biometrics readers -- for multi-factor authentication.

Meanwhile, as mobile credential delivery and management elevates in importance, we will have the opportunity to use cloud-based solutions into which all entities have been biometrically authenticated. Growing adoption of



mobile access will also drive the move to centralized access control. This will not only make it easier to accommodate a combination of cards, phones, wearables, but also enable organizations to combine secure physical and logical access as part of their facility and IT access strategies.

Mobile Helps Drive Security Convergence

With the adoption of mobile access, cards and phones are already converging into centralized identity management systems. The ultimate objective goes beyond supporting both form factors, though. Even more valuable is the ability to use either form factor -- or both -- to secure access to the door, to data, and to cloud applications, while providing a seamless user experience. Developments in converged back-of-house technologies are enabling strong authentication and card management capabilities for computer and network logon while also ensuring that physical and logical identities can be managed on a combination of plastic cards, smartphones and other mobile devices.

There are numerous benefits to be realized by provisioning IT and PACS credentials to a single smart card or smartphone, using one set of processes. First, it will improve convenience. Second, this approach can greatly enhance security and reduce ongoing operational costs. It also enables organizations centralize identity and access management, consolidate workflows and tasks, and proliferate strong authentication throughout their infrastructure to protect access to all key physical and IT resources.

As both physical and on-line access applications merge onto cards and many types of mobile devices, there are other issues to consider. Organizations

will no longer be able to assign a single ID to each user for all applications. Instead, their systems will need to be capable of managing multiple IDs, for multiple applications, on multiple devices. The coming generation of identify management system will support this requirement, and enable individual groups to independently manage their own application and identity lifecycle needs.

Securing The Mobile Promise

Mobile access has opened a new chapter in the creation and management of digital identities. Moving forward, the adoption of mobile access and new credential form factors such as wearables will create new opportunities for innovative use cases beyond simply opening doors or converged physical security and PC login. Users will be able to tap in to a growing range of applications, and open doors from a distance with gesture technology. At the same time, administrators will benefit from an access control ecosystem that provides a seamless user experience and can flexibly scale and adapt while delivering increased value to the organization. Moving forward, we will also see the implementation of biometric authentication on mobile platforms to further improve security and convenience.

In order to realize this vision, organizations must deploy solutions that support the broadest possible range of available handsets as well as legacy ID cards. These solutions also must be designed using open standards so they can adapt to new requirements and capabilities in the future as the industry quickly moves to a wide variety of new device platforms, biometrics authentication models, and unified cloud-based systems for PACS and IT credential management.

Locked in... no compromise no comparison!

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

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

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

10 year* guarantee

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

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



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

Loktronic

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



International diplomacy

The best defence against home grown terrorism

In a recent interview on the Paul Henry radio show, Otago University International Relations Professor, Robert Patman, made it clear that government overreactions to the threat of terrorism would be counterproductive. “We mustn’t interfere with the lives of people who are law-abiding, Muslim and non-Muslim, in New Zealand, in other words, we mustn’t create a police state in the name of defending everyone against terrorism.”

“Human rights”, he added, “are a strategic weapon in the political struggle against terrorism.”

According to Prof Patman, the Western world’s military and security-

focused actions have done very little to neutralize the political motivations of those using extremism to further their causes. Additionally, as a member of the United Nations Security Council, he says that New Zealand has an historical opportunity to break the paralysis of the UN in providing real solutions to the intractable problems that riddle the Middle East.

Overreacting at home not the answer

Patman’s thinking stems from the idea that the struggle with terrorism, although described in military terms, is actually a political struggle. “The progress of efforts to capture or kill terrorists are rightly considered,” he concedes, “but they are central to the problem and in a sense really what terrorism is against.”

He continues, “The causes generating the rise of the Islamic State can’t be tackled by assassinating or eliminating leaders. It can certainly cause dislocation in their ranks, at the same time drone attacks may inspire for example new recruits into the movement. What we ideally want to do is maintain a vigilant security and military posture against these groups but at the same time begin to attack the ideas that they stand for and discredit them.”

Putnam observes that the Islamic State modus operandi is quite different to that of al Qaeda in that IS are looking to nurture homegrown terrorists. Although the threat of terrorism to New Zealand is

low, he points out that “the fact is that the incidents in Australia were by people born in Australia that have been influenced by Islamic State and the sophistication of IS in social media.

Given this MO, he states that “it’s very important we don’t intrude unnecessarily into the lives of law-abiding people and we don’t create conditions which might inspire people to listen more carefully to listen to the messages communicated in social media by IS.” We must not, he continues, weaken our commitment to human rights and rule of law, “which these groups are dedicated to destroying.”

Military responses have furthered the appeal of extremism

Prof Patman argues that not enough has been done to reduce the appeal of the ideas that inspire Islamist terrorism. The US-led ‘global war on terror’ has, in his opinion, wildly missed the mark in preventing the types of terror attacks that it was ostensibly waged to prevent.

“If you look at the situation since 9/11, the invasion of Iraq for example, which was opposed by a number of commentators – and not least by the government of New Zealand – was a strategic disaster.” By falsely declaring that Iraq was a central front on the war on terrorism, he says, the US has unleashed a whole series of anti-American forces. “The founders of the Islamic State were disgruntled members of the disbanded Iraqi army, and this needs to be kept in mind.”



Otago University International Relations Professor, Robert Patman



He also highlights the link between the attacks on the offices of French satirical magazine Charlie Hebdo earlier this year with the US-led invasion of Iraq. The perpetrators of those attacks, he explains, “were inspired by images that were transmitted internationally from the American detention camp Abu Ghraib.”

Looking for answers, Prof Patman suggests that the western world and the United States in particular needs to be more focused on trying to tackle some of the grievances that the likes of IS cynically exploit. One of these is the failure to achieve self-determination for the Palestinians. “It’s not that groups like IS or al Qaeda care about the Palestinians, because they don’t but they’re happy to exploit the perception amongst even moderate Muslims that the west is indifferent to the plight of the people under occupation.”

The traditional military approach, which assumes that the taking out of terrorist leaders will remove the problem, hasn’t worked, according to Patman. “It is important to keep in mind that ultimately victory over groups like Islamic State will not be achieved by military means alone they will involve shrinking the political base of groups like that, and this takes time.”

New Zealand’s membership of UN Security Council a real opportunity

In an August 2014 stuff.co.nz opinion piece, Patman and PhD student Laura Southgate argued that, New Zealand should use its newly won seat on the UN

Security Council to “remind the world the current veto system in the UNSC no longer serves the interests of international stability or justice.”

To-date, he says, the Security Council has been paralysed by the use of veto, and this is one of the factors that has contributed to the rise of IS. He lists three UNSC resolutions initiated by the Obama administration in 2011 and 2012, each of which was vetoed by Putin government, which had tried to effect peaceful political transition in Syria. “The failure of the international community to deal with the Syrian civil war,” he laments, “has fuelled the rise of the Islamic State, which ironically now threatens both Syria and Iraq.”

This, he asserts, clearly demonstrates that failure to act in someone’s civil war can have major political ramifications even for countries as far away as New Zealand. “These conflicts are not just problems for the peoples involved, these are regional problems, which have global ramifications and New Zealand does need to play a role in getting the Security Council to focus on them.”

According to Prof Patman, given that Foreign Minister McCully had promised that New Zealand would try to restrain the use of the veto when they got on to the Security Council, we need to ‘talk the talk’. “McCully said that he was prepared to upset old friends, and I think he was referring here to the likes of the UK and possibly Britain and France in pressing for the resolution of issues such as the Israeli-Palestinian issue.

Although difficult for a small state to do on its own, Patman believes that there’s a lot of potential support within the UN general assembly if NZ does talk the talk. “Most countries in the world are not great powers, they tend to be medium-sized and small, and they are sympathetic to New Zealand’s agenda,” he explains. “It’s not easy, New Zealand can’t get on to the UNSC and in the space of four months rearrange everything, but I think they’ve got to chip away.”

He sees is as a strategic necessity that the Palestinians get their own state. “I think that’s absolutely essential to the region... it’s not the only problem; there’s a fault line running between the Sunni and Shia communities as well, which is a major issue.”

Dealing with extremism at home

The government already has a range of measures to prevent people travelling overseas to join groups like IS, and under new legislation rushed in towards the end of 2014 these powers have been significantly strengthened. “But there is a longer-term issue,” states Patman, “which is parents who are very concerned about the radicalisation of their children.”

“What is interesting is that [Australian prime minister] Mr Abbot has recently apparently turned his back on the idea of trying to set up a framework to work with families that have children going down that road and trying to actually rehabilitate them before they get further involved.” There are widely held opinions, he says, that such programs are expensive and the results uncertain.

But he maintains that the threat here remains relatively low. With the government having identified a list of between 40 and 80 people with expressed sympathies for Islamic State, “in a country of about 4.5 million people that’s still relatively small numbers.”

With the clock ticking on New Zealand’s temporary tenure on the UN Security Council, and extremist threats continuing to be reported across the Tasman, Wellington is yet to provide any concrete indication of how it actually intends to fight the underlying drivers of violent extremism. Considering the insights of experts like Prof Patman, one hopes that border security legislation and the deployment of troops to train Iraqi forces are not the only strategy cards the government intends on playing.

High Wiring

The man who hacked a plane

The physical hijacking of planes by malevolent passengers and, more recently, by suicidal pilots, has been a major civil aviation issue within the media in recent years. Now, if a case this year in the US involving a hacker, the FBI and an airline entertainment system is any indication, it appears that aircraft can now be potentially hijacked by remote control.

Attacks on cockpit computers have apparently been an issue at hacker conferences for years, but airlines and manufacturers have tended to largely ignore the issue. Now, the FBI is looking into whether Chris Roberts, a US-based IT expert, actually penetrated the in-flight entertainment system of a passenger plane to the extent he managed to manipulate the plane's engines mid-air.

This seemingly unlikely incident has triggered a new debate around a threat that faces airlines and passengers, and comes only months after the US Government Accounting Office (GAO) had highlighted potential weaknesses in air-traffic control in January. According to its report, the weaknesses it identified are likely to continue, "placing the safe and uninterrupted operation of the nation's air traffic control system at increased and unnecessary risk."

Back-seat pilot?

According to the FBI document, Roberts was able to hack into the onboard entertainment systems of passenger planes such as the Boeing 737 and 757 and the Airbus A320. He did so a total of up to 20 times between 2011 and 2014 by hooking his laptop up to the Seat Electronic Box (SEB) (usually located under each passenger seat) using an Ethernet cable.

In mid-April, Roberts, while on board a United Airlines 737, logged onto Twitter via the passenger Wi-Fi network, and tweeted "Shall we start playing with EICAS messages? 'PASS OXYGEN ON' Anyone? :)," (EICAS is the Engine Indicator Crew Alert System that transmits data from the plane's engines to the cockpit)

After Roberts changed planes in Chicago on his way to Syracuse, FBI agents boarded the plane to examine the SEB under his seat. When he arrived in Syracuse, the FBI removed him from the plane and seized his electronic equipment.

It is possible that on other occasions Roberts may have also potentially used the SEB to hack into the systems that actually control the engines. In one case, he told the FBI that he was able to successfully enter the command "CLB," which stands for "climb", and the plane's engines reacted in accordance with the command.

A known whistleblower

Roberts has stated, that "over the last five years my only interest has been to improve aircraft security." And it is clear that his relationship with the FBI has been ongoing for some time. But up until now, no one seems to have cared.

In public presentations going back over four years, Roberts and other experts have demonstrated methods for hacking into onboard computer networks used to operate in-flight entertainment systems. According to Roberts, his research has been shared with aircraft manufacturers, such as Boeing and Airbus, as well as the Federal Aviation Administration.

Despite the ongoing dedication of Roberts and his colleagues to shedding light on these very disturbing apparent vulnerabilities, their research has been met with little interest.

The vulnerabilities of interconnectedness

In a study published in April, the GAO warned against the increasing connectivity of individual airplane components. "This interconnectedness can potentially provide unauthorised remote access to aircraft avionics systems," stated the study. According to one of its co-authors, the findings are particularly applicable to newer planes such as the Boeing 787 Dreamliner and Airbus A350 and A380.

Airlines and manufacturers have been largely silent on the incidents and on possible consequences. Most have refused to comment. A Boeing representative has told Security Week that internal systems access simply isn't possible.

If the recent claims by Roberts are confirmed, it contradicts the claims of airlines and plane manufacturers and provides proof that common airplane models are indeed vulnerable to hacking. This could result in major changes within the industry.

KCS TraceME

INTELLIGENT GPS WILDLIFE TRACKING



Size comparison with a coin

Never lose the ones we love

KCS has extended its successful TraceME product line with the TM-230 module, targeted for tracking wildlife and advancing wildlife science into the Internet of Things era. The TM-230 module is one of the smallest and lightest track-and-trace units in the world. The modules' minimum size of **29.7 x 20 mm** and weight of only **3.5 grams** enable tracking of very small animals e.g. endangered species and small birds. It can be attached easily to various parts of the animal. Successful field trials by wildlife science experts have proven that the unit does not affect the natural behaviour of the animal. Solar powered GPS/GPRS offer long-term accurate location data, to be connected to the Internet of Things era.



www.Trace.ME

All trademarks mentioned herein belong to their respective owners.

Damned if you do, damned if you don't

Preparing businesses for extreme events

Auckland University academic Dr Bridgette Sullivan-Taylor has been in the news a bit lately. In a recent New Zealand Herald opinion piece, she suggested that the day might soon come when terrorism threat levels result in New Zealanders being subjected to bag searches upon entry to shopping malls.

The piece elicited outcry from readers who balked at the idea that malls should be checking shoppers' bags. Ironically, however, Sullivan-Taylor was not suggesting malls conduct checks but rather that businesses need to be taking the threat of unlikely 'extreme events' more seriously rather than just planning for them under the assumption that they are too hard to predict and prevent.

It's about, argues Dr Sullivan-Taylor, strategic decision making – how do you as a company decide what risks you will prepare for, and how do you build resilience no matter what the crisis is?

Taking terrorism out of the 'too hard basket'

In research she started at the Aston and Warwick Business Schools and funded by the UK Cabinet Office, Sullivan-Taylor found that companies in the UK tend to act either defensively in the sense that "we've tried to mitigate the risks as much as possible, practical and affordable", or fatalistically in the sense that "well if it's going to happen it's going to happen and there's nothing we can do about it. If we have an extreme event, particularly terrorism, we'll just have to take the hit. It's just too hard to predict and too hard to prevent."

After 9/11, companies in the UK still felt that terrorist attacks of that kind were an offshore scenario and that they wouldn't

happen on home soil. If it did happen, says Sullivan-Taylor, "then they would respond with the very British bulldog spirit 'keep calm and carry on'." This was a concern to the government because 80% of the public critical infrastructure in the UK is privately owned. So there were big questions around how prepared utility companies were and their level of investment into this.

Private ownership versus public good

Sullivan-Taylor was keen to know whether tourism-related companies in London, such as airlines, airports, convention centres and catering companies, saw themselves as being in a critical public infrastructure supply chain. "Companies may see themselves as being in the hotel or convention centre sector but not necessarily as part of something that's joined up like tourism or something else; but government needs them to see things in this way for safety and security across the whole city.

There is still this expectation among companies, she says, that the government will step in and sort it out and so they don't always prepare beyond a certain point.

The Pitt Review, which followed the 2007 flooding disaster in the UK, found that the scale and damage was so massive that it was beyond the capability of government to cover it. The review resulted in companies being made aware that the government will only help so far. Investing for preparedness, she observes, tends to have to be driven from outside the firm, not inside. "It tends to have to come as a push factor, especially with SMEs."



*Auckland University academic
Dr Bridgette Sullivan-Taylor*

In terms of SME thinking, activities such as counter-terrorism, emergency management and recovery are seen as something of a public good. Businesses tend to have an expectation that they can outsource responsibility for these things to government and that taxes should be put towards protecting them against even the most unlikely of exigencies.

How can companies become more resilient?

"Business Continuity Managers, Risk Managers, and Security Managers in the UK don't usually sit on the company board," says Sullivan-Taylor, and her assumption is that it's the same here. "The frustration is that they do all the analysis and then they have to pass it to someone at board level, and normally the decisions are based on a financial rationale."

"The problem with this," she says, "is that it's so hard to predict the scale and impact of some of these extreme events that the financial people just don't want to go near it." So decisions are made in the



Ultra-Smart & Eco-Savvy
2MP, 3MP, 5MP & 4K IP Cameras



Distributed by



www.itplus.co.nz

Telephone: 09 950 4940 • 8/103, Cryers Road, East Tamaki, Auckland 2013 • Email: info@itplus.co.nz

boardroom to the effect that the risk has been looked at but not further considered. “Every board has a financial director, and there is wide awareness of what they do, but this is not the case when it comes to security.”

But resilience is not something you can really test until it happens, Sullivan-Taylor points out. “Think about Y2K – billions invested but nothing happened... the issue has a taint.” You can either be underprepared or overprepared. “If you’re overprepared,” she says, “shareholders will criticise you for over investing in something you didn’t need to worry about. If you under-prepare, you’re likely to be sacked. You’re damned if you do and damned if you don’t.”

“It’s an endlessly frustrating position to be in unless you have legislation supporting you, or unless insurance companies are influencing businesses to invest in these things, or if reputation or fear or standards are driving it.” She sees it imperative that standards are regarded as the absolute minimum, and that in the context of terrorist threat companies would do more than just the minimum.

There is also the issue of increased regulation leading to the establishment of an audit culture that fails to achieve the cultural change needed to support it. Additionally, “If companies in regulated sectors are doing the bare minimum,” asks Sullivan-Taylor, “then what are companies in unregulated sectors doing?”

How do you make business continuity management ‘business as usual’? People won’t do something they see as wholly hypothetical and a waste of their time; employees won’t leave their screens... call it ‘fire drill syndrome’. “SMEs don’t want to invest in training generally or in anything that’s non-core, and this is something that I’d like to investigate. It’s a real worry.”

Weak links

Echoing her NZ Herald opinion piece, the academic states that “one of the weak links in the chain could be one of those little cafes that sit in train stations or airports, such as Starbucks.” In the case of the Lindt Café in Sydney, she points out, this was a café right opposite a piece of critical national infrastructure, Channel Seven... so being prepared means being aware of the surroundings.

“You could easily be the weak link in the chain, and big corporates need to think about who is in their geographic space, because when you think about Britomart Station or the Beehive, you might be secure but right next to you a little kebab shop could be a weak link.”



London's Canary Wharf

Resources for proactive SMEs

In the UK they have the National Risk Register, says Sullivan-Taylor. “Wherever you are in the country you can go online and look at what the risks are in your area.” Users can see at any time what’s going on in a particular locality, and it’s free. As a result of the Pitt Review, resilience forums have also been set up for each local government area in the country.

“You have to be proactive about finding out about these things”, she suggests. “The NZ Civil Defence website, for example, has the Breakout service where you can get messages and facebook updates. You need to link into these things.”

Rural factor

The UK, she observes, is characterised by a huge London-centric security bias. “Even within London”, she says, “Canary Wharf is like the centre of the universe,” and she thinks the case may be similar here.

Interestingly, she notes that London-based convention centres reported that the biggest threat to them wasn’t terrorism, but foot and mouth. When the disease hit the UK it massively impacted on the tourism industry because not only did people stop coming in from other countries but there was also a halt on domestic movement. “That could happen here,” she opines, “being an agricultural country, that type of biohazard is high on the radar, and if authorities undertake major changes in response, people will respect it.”

“So at the airport where they have that double security of your bags and have dogs all over you, people will put up with it no question.” Returning to the shopping mall example, if it was a biohazard thing,

then you wouldn’t be allowed in with dirty shoes. “You’d have to take them off and there’d be no question.”

But, says Dr Sullivan-Taylor, “It takes an extreme event for it to happen.”

Good risk management and business continuity practices

Being prepared, says Sullivan-Taylor, means being prepared in the light of extremes, not just business as usual. “There is a lack of regard for things that occur at the extremities... their extreme nature and the unintended consequences.”

Secondly, it means thinking beyond your organisation. “Your organisation has an impact in its geographical area,” she says, “and New Zealand has a lack of joined up formalised public private partnerships.” Big corporates are more likely to be doing this, but it’s more about getting SMEs involved. “If you’re part of the wider community in a CBD or a global supply chain, you don’t want to be the one that lets that whole thing down.”

In a general sense, she makes the observation that national security rhetoric tends to be informed by the political sciences and international relations fields, “where they talk about radicalisation and defence stuff, border and heavy serious policy.” But given that 80% of national critical infrastructure is privately owned, she argues that there should be much more input from business disciplines.

If you are interested in participating in Dr Sullivan-Taylor’s research to identify SME best practice between regions and sectors in New Zealand in relation to extreme events, please contact her at Auckland University or Email: b.sullivan-taylor@auckland.ac.nz.

Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

HOLD ON A MINUTE

...OR AN UNRIVALLED 10+ YEARS!

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



PLAY IT SAFE AND LOCK IN
Loktronic quality, every time



FDH40S: Standard, floor mounted



FDH40SS: Flush mounted



FDH40SS: Surface mounted



Designed, tested
and **produced in NZ**
to AS4178

10 year guarantee*

Unbreakable
universal mounting

Floor or wall
mounting options

Superior quality
materials
and fastenings

Full and immediate
on-shore support

Loktronic

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

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

*Standard terms & conditions of sale apply.

Getting in the picture

Axis Communications opens Wellington office

The opening of Axis Communications' Wellington office is just one of many recent developments for the Sweden-based network video solutions leader. New products, new regional leadership and the impending acquisition of the company by Canon have kept Axis well and truly in the news.

Following the Wellington office opening on 31 March, we chatted with Magnus Zederfeldt, Axis' recently appointed South Asia Pacific Regional Director, to find out what the new office means for the company's New Zealand customers, and what we can expect from the market leader over coming months.

The Wellington office adds to an already impressive global footprint. With offices in more than 20 countries, Axis has more than 1,900 employees in more than 40 countries, supported by a network of over 75,000 partners across 179 countries. The company is the global market leader in network video, including security surveillance and remote monitoring.

"We've had a salesperson in Wellington for the past three years," says Magnus, "but our new office gives us more space for receiving clients." Axis has achieved very good growth in New Zealand in recent years, but he believes the local market will continue to increase in double digits, driven by demand and technology shifts.

The Wellington office, managed by Wai King, is also supported by four part time staff in Australia who provide sales,



Magnus Zederfeldt (R) opening the Wellington office

marketing and training support. Magnus sees the new office as a demonstration of Axis' commitment to the market and as evidence of the company's overall geographic expansion.

The company relies on its partner network, which is made up of long-term partnerships with systems integrators - they don't sell to end-users. "Our job in the region is to develop loyal partnerships with systems integrators," explains

Magnus, "... we mean what we say when we want to support them - both pre-sale and after-sale."

In February this year, it was announced that Canon was looking to acquire Axis as part of a forward integration move. Canon already makes its own security cameras, but with Axis it gains a broad range of IP video surveillance products and an open application platform for third-party app development.



Cameras already make up almost 40 percent of Canon's sales, but with smart phones having dampened sales of digital compact cameras, the company has pushed into network cameras. At the same time, Canon's optics technology, such as the 50-megapixel sensor in the new 5DS digital SLR, could also benefit the Axis lineup. "We will have a very financially strong owner," says Magnus, "and they are world leaders in lens technology."

The acquisition process is still ongoing. Echoing reports in the press, Magnus points out that Canon has made it clear that they want to keep the Axis brand name and strategy. "Axis will be an independent unit within the Canon group."

The offer is worth about US\$2.8 billion and has been approved by the three largest shareholders in Axis. It follows a pattern of Canon acquiring companies in the same field that have an edge.

With research and development a major focus in Axis, the company's innovations have given it a major edge. Its Lightfinder technology, which provides colour video in very low light environments, is a combination of Axis' expertise in image processing, in-house system-on-chip development and selection of the best optical components.

Cameras with Axis' Lightfinder technology can deliver colour images in as little light as 0.18 lux, or even lower. "It really differentiates us in a lot of projects," says Magnus. "People want to see colour in low light environments, and

Lightfinder will show video as daylight even if lit by a single candle."

Another Axis technology, Wide Dynamic Range with Forensic Capture, resolves images where there is too much light, such as headlights or direct sunlight. The technology optimises video for forensic purposes by applying advanced algorithms to enable an extremely high level of detail to be visible in both dark and bright areas of a scene. According to Magnus, the technology "can see in the shadows".

Axis' Intelligent Video technology has been around for some years but is only now being commercially employed. Its applications range from analytics, such as video motion detection and audio detection, to more advanced systems, including camera tampering detection, people counting, virtual fences, and vehicle license plate recognition. "It's very simple to install and use," Magnus explains, "but very complex in the background."

Apart from in-house R&D, Axis' technological edge is being bolstered by an open source approach. The Axis Camera Application Platform (ACAP) is an open application platform that enables members of Axis' Application Development Partner (ADP) Program to develop applications that can be downloaded and installed on Axis network cameras and video encoders. Magnus adds, "We give application development partners development and marketing support to develop their products with our cameras".

Although it's already available in some models, Magnus also mentions that Axis' Zipstream Technology-enabled cameras will be launched in spring. Zipstream technology lowers bandwidth and storage requirements by an average 50 percent or more without necessitating investment in new cameras or software. It is fully compatible with the widely adopted H.264 compression standard.

Zipstream technology can be used alongside other Axis network camera technologies, such as WDR - Forensic Capture and Lightfinder. The technology analyses and optimises a network camera's video stream in real time, recording scenes containing interesting details in full image quality and resolution while filtering out other areas.

"With more and more requests for wireless and 4G, the biggest issue is bandwidth," Magnus points out. "Resolution is increasing, therefore Zipstream becomes very important."

Axis' aim in New Zealand, he explains, is to be the market leader and to grow market lead. The company will focus on the retail and government markets where it is seeing a growing demand, and it will boost the sales of its dome cameras portfolio, which has found great success locally. He also sees great things for Axis' latest technology offerings in the quality conscious New Zealand market.

Axis' new Wellington office is located at Level 11, 49 Boulcott St, Wellington 6011.

New mobile surveillance cameras ensure best first response

By Nicholas Dynon, Imran Aziz & Matthew Naylor

Surveillance has perhaps been the most significant legacy of 9/11. The continuing threat posed by global terrorism has driven huge amounts of government investment into electronic surveillance, as well as both wide and targeted physical monitoring systems in our cities. Digitised mobile camera surveillance in particular presents a powerful weapon in counter terrorism and law enforcement, yet this emerging technology remains relatively undiscovered.

The UK boasts the world's most extensive CCTV coverage. It is estimated that most individuals are seen by a camera an average of 340 times per day, and in Central London an individual will be on camera for about 95% of the time. But compared to the UK, CCTV use in other jurisdictions is limited by a range of fiscal, legislative and privacy constraints. Surveillance cameras cannot be everywhere, and thus despite their ubiquity in modern streetscapes they lack the type of panoptic ability decried

by civil libertarians and idealised by Hollywood films such as *Enemy of the State*.

Thus, even if a camera is effective in identifying crime within its own field of view, in all likelihood it has achieved this merely by shifting the crime to a location beyond the width of its lens.

According to the Queen's University Surveillance Studies Centre, the likely consequence of camera surveillance is that "crime and undesirable conduct are displaced into neighbouring areas once cameras are installed in a target location." The centre cited a San Francisco study, which found violent crime decreased within 250 metres of 'open-street' surveillance cameras, but increased beyond 250 metres. Crime, like water, finds the gaps and exploits them.

Filling those gaps is critical, and the introduction and use of new mobile camera technology has been heralded as the solution.

Mobile and body worn cameras

Mobile and body worn cameras have been traditionally used for the same purposes as static CCTV: deterrence and evidence. But it has been issues around use of force, such the 2014 shooting of Michael Brown in the St Louis suburb of Ferguson, and the need to protect both police and civilians that have intensified calls for police to be wearing Body Worn Vest Technology (BWV). It has been recognised that the behaviour of both parties changes when a BWV system is involved.

The first empirical study on the use of body cameras by police was released last December by researchers at Cambridge University's Institute of Criminology. The results from this twelve month study of California's Rialto Police Department indicate a 59 percent drop in use-of-force by officers wearing BWV and an 87 percent drop in complaints against officers. These findings are consistent with those of similar studies.



Nicholas Dynon is an Auckland-based writer focused on security, terrorism and international relations, and his writing has appeared in several international media, business and academic publications. He has served diplomatic postings in Shanghai, Beijing and Fiji during a 14-year career with the Australian Department of Immigration and Border Protection. He has also served in the Australian Army's signals and transport corps.



Imran Aziz is a senior executive with over 16 years of sales, marketing and project management experience in the technology and engineering sectors. His specialist knowledge in remote security, telemetry, fire and technology systems has made him an invaluable resource on strategic projects for major government, corporate and law enforcement agencies globally.



Dr Matthew Naylor has spent the last twenty years with Xiralis (nee Vision Systems) designing, developing and specifying video based technologies for security applications. As senior product line manager for video analytics, his role now involves travel from his home in Australia to the UK, Europe and the US as the company's analytics expert, training and advising designers, installers, and the company's own technical support and sales teams in how to get the best from the Xiralis video analytics portfolio.



time information when responding to suspicious and or intercepting crimes in progress. The majority of video surveillance systems are reactive in nature, in that they record the pictures delivered by video cameras on streets, which are later analysed for evidence or explaining crimes and other incidences. CCTV has been very effective, for example, in the hunt for Boston Marathon bombing suspects, but was of no value in preventing the incident.

Even when remote monitoring systems send alarms in real time to security monitoring centres, they are often poor in quality and require the attendance of a security response vehicle to investigate. According to Luke Percy-Dove of Matryx Consulting, “A very high percentage (95 percent) of all alarm traffic is associated with false alarms, meaning most alarm attendances are a waste of time too.” Typically Police will not attend an alarm event unless it can be validated or the premises carries a high level of priority. “And remember, if 95 percent of all alarm events are false, why would they?”

Digital, or ‘second generation’ technology incorporating video analytics can turn existing technology into a proactive system. This allows alarm-receiving centres to make decisions with real time information, in many cases removing the need for security officer call-out. This results in a significant reduction in costs and false alarms, leading to improved security and proactive responses to situations as they occur.

Once a first responder is deployed to an incident site, however, they still depend on radios to relay information back to central monitoring stations. In most jurisdictions this includes police, who are unlikely to have anything other than radio with which to communicate while on foot. According to Percy-Dove, this means that whoever is in charge of coordinating the response needs to rely on words to understand the situation on the ground. “In this day and age and with the technology available,” he states, “it’s crazy it still happens this way but people don’t know better and what is possible.”

Some first responders have the option of sending images from a car or transmission hub to the control, but this is limited by the necessity of being in close proximity to the hub. “As we all know, when a police officer is dealing with a situation

And quite simply, if police and security personnel were not recording their actions in responding to an incident, then an onlooker with a smart phone/device would undoubtedly be recording their actions. According to the US Office of Community Oriented Policing Services, “given that police now operate in a world in which anyone with a phone camera can record video footage of a police encounter, body-worn cameras help police departments ensure events are also captured from an officer’s perspective.”

Echoing international trends, all Australian state jurisdictions have now run trials of body cameras, but the approach has been one of caution.

“Whether we decide to roll [body worn cameras] out more widely across the organisation is not a decision we are going to rush,” commented Inspector Ian Geddes of Victoria Police via email interview. “Further work is needed to help us to consider the next steps,” he stated, “including considering the outcomes of

other body worn camera trials happening across Australia and the world, as well as the ongoing considerations around evolving technology and data storage needs.”

Indeed, it is the evolving technology that is making law enforcement and security procurement of body worn cameras increasingly complex. While many organisations have trialed and implemented solutions based on transparency, evidentiary and behavioural benefits, emerging second-generation technologies are enabling cameras to do much, much more. The major consideration is now around whether to invest in cameras that can also provide live video feeds, immediate remote response and intelligent analytics aimed at early warning and intervention.

Gaps in first response

Traditional static CCTV and remote monitoring systems have been limited in providing first responders with real





they are not necessarily near or anywhere close to a car or hub,” comments Imran Aziz of safety and security solutions provider Xtralis. “Also, these units will not be able to provide you with GPS information for use with mapping software.”

Additionally, Percy-Dove notes, “some vehicles are now been fitted with video capability, but as far as I know these are recorded only in the vehicle and are not yet broadcast back to the station.” In the case of the Victoria Police, Supt Geddes concedes that not all police vehicles are Mobile Data Network enabled.

First responder solutions

Body Worn Vest technology incorporating live-streaming CCTV can provide the potential answer to the real time intelligence deficit of radio-only communications from first responder to base. “I think it adds real value because at street level you get to a whole different perspective of what has happened,” states Percy Dove, “... the key is always to get the best possible information you can.” But it only works if it is plugged into a system that can transmit audio and video in real time to command and control structures so that the intelligence can be analysed and operational decisions made.

Entering the marketplace are a number of innovative solutions for early and reliable detection, remote visual monitoring for immediate and effective response. The City of London Police (CoLP), for example, has recently commenced a trial of an Xtralis solution that provides live transmissions from police vehicles and BWV to better assess situations and more efficiently deploy appropriate assistance.

According to Imran Aziz, the Xtralis HeiTel body worn solution has the ability to use multiple types of cameras with the same unit. The recording unit is remote from the camera, so if the camera is pulled off the vest by a member of the public the recording remains safe on the vest, thus protecting the evidence. It also possesses a live streaming capability and GPS tracking. Xtralis’ WCCTV Nano technology allows first responders to live stream wirelessly via 3G/4G, LTE and CDMA, as well as satellite, Wi-Fi and broadband networks. Its software allows multiple vests to be monitored at any given time, “giving the commanding officer complete situational awareness.”

The HeiTel mobile technology is also used in other mobile applications such as public transport, cash in transit vehicles, and rental equipment and vehicles. “In principle the car unit will do everything the BWV will do but in

addition it can have up to ten cameras on the unit, connect to panic buttons, blue light engagement, and audio systems to name a few,” says Imran Aziz. “In Europe Xtralis developed a self-contained mobile early fire detection solution called RapidProtector, which utilises the HeiTel mobile technology combined with a compact area smoke detector to create a temporary mobile smoke detection solution for control rooms and base stations. It can be used during construction and upgrades when conventional fire panels need to be switched off.”

In Australia local councils, water and electricity authorities are looking towards mobile video-streaming technology to protect assets and people in areas where there is no traditional network infrastructure available.

Water authorities are using the technology for use in pump stations





or near dangerous drainage systems to proactively prevent unauthorised access. Used in combination with alarm sensors, a central monitoring station can be alerted when unauthorised persons enter a protected area, and an audio warning may be issued to the intruders in order to remove the threat.

Rob Galic, Sales Director at Xtralis says, "Local councils are using the technology for Health & Safety to protect rangers who are driving in remote areas, and for protection of parking officers." According to Galic, its also being used by tow truck companies whose drivers are often the target of aggression by vehicle owners when their cars are being towed from illegally parked areas. "If the tow truck driver is feeling threatened or is concerned that their truck is at risk, they can hit a panic button that will alert a control centre and stream live video while recording the incident."



According to Wayne Trethowan of Hills Industries, when the system is paired with solar backup power units it provides a remote solution for builders and developers of broadacre estates who require video protection of assets and buildings before they become occupied.

Solutions such as these are making traditional mobile CCTV look archaic, and presenting law enforcement, public transport and security procurement departments with the choice between a deterrence and evidentiary tool on the one hand versus all that and a whole lot more on the other.

In essence, it is a choice between a tool that can record a criminal act and a tool that can proactively prevent one. Given the increasing political, social, financial and human cost of crime, and the continuing spectre of terrorism, the latter option is difficult to ignore.

Command and control the scene with live HD video streamed over 3G/4G

CamDisc E/M

Live recording & transmission over 3G/4G, GPS tracking for mobile applications, and integrated monitoring software enables superior alarm handling, bi-directional audio & coordinated response.

The possibilities are endless.



Learn more: www.xtralis.com/CamDiscE
Email: marketing-apac@xtralis.com

HEITEL
by **xtralis**

SUBSCRIBE NOW!

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

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

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

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

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

or email your contact and postal details to:
craig@newzealandsecurity.co.nz

Mr Mrs Ms _____

Surname _____

Title _____

Company _____

Postal Address _____

Telephone _____

Email _____

Date _____

Signed _____

NZSecurity

Hills New Product Range On Fire

Hills has launched its new fire safety product range Quell, which is the complete fire protection kit for home and small commercial premises.

Hills Head of Security and Fire Practice, Kobi Ben-Shabat, said this new range was part of Hills unique ability to provide its customers with new business opportunities.

"The Quell range provides our customers the opportunity to create an add-on business with minimum effort and maximum reward.

"Hills has the unique ability to provide its customers with a value added business and product range. With the Quell range in stock and ready to order, Hills is providing its customers the opportunity to expand its service and product offering today," Kobi Ben-Shabat said.

The Quell system is easy to use and understand with a colour coded system that categorises the complete range.

Products include:

- ◆ Smoke alarms
- ◆ Carbon monoxide alarms
- ◆ Fire blankets
- ◆ Fire extinguishers
- ◆ Fire safety kits

For more information and a product catalogue contact your nearest Hills Branch or visit www.hills.com.au/customer-service.

HILLS™

Get a FREE Package of Valuable Accessories When You Buy a New FLIR AX8 Thermal Sensor

Buy a FLIR AX8 thermal sensor (part number 71201-0101) and receive this free package of valuable accessories:

- PoE injector (part number T199019)
- Ethernet cable, M12 to RJ45 (part number T128390)
- Cable, M12 to pigtail (part number T128391)



Continuous Condition and Safety Monitoring

Combining thermal and visual cameras in a small, affordable package, the FLIR AX8 thermal sensor provides continuous temperature monitoring and alarming for uninterrupted condition monitoring of critical electrical and mechanical equipment.

Limited Time Offer

This offer is valid from 15 May through 31 August 2015.

Request more information:

<http://www.flir.com.au/automation/display/?id=68327>

FLIR®

fired up protection

ViTECH

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



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

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



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

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



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

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



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

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

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



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

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

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

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



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

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

STI-6255 Ref. 720-042

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



STI-6720 Ref. 720-047

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



Battery Tester Ref. 730-100
ViTech rugged steel case 5, 15 and 30 amp battery tester for fire and alarm use.



Fire Brigade Alarm: (Closed/Open) Ref. 730-201
ViTech branded Type X and Type Y models with temperature compensated pressure transducers with digital display showing pressures for defect, fire and pump start.



Anti-Interference Device
Ref. 730-400 series
ViTech AID for sprinkler valve monitoring; fits all ball valve sizes.



ViTech products are designed and produced in New Zealand.

Loktronic

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



HOW SMART IS YOUR COMPANY?

You're (not) smarter than your competitor?

M2M

Machine to Machine and
Internet of Things

LoRa

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

SPECIALIZED IN:

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

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



www.Trace.ME

All trademarks mentioned herein belong to their respective owners