

NZSecurity



December 2015 / January 2016

Perspectives on Starting Out in Security

**Christchurch Bar
Security Staff Result**

**The Retail Sector –
Where Safety and Security Collide**

**The Man Who Gave Us
the Networked Camera**

www.NewZealandSecurity.co.nz

Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

your electromagnetic locking specialist!

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

Standard features include:

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

Options include:

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

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

10
YEAR
GUARANTEE



Loktronic

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



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

uniview

Better Security, Better World.

CRK

Professional Precision

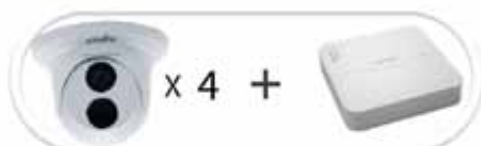
YOU CAN COUNT ON ME

UNIVIEW HD IP KIT, YOUR PERSONAL SUPER GUARD

- View anywhere
- Alarm real-time push
- Easy connection & installation



Products included:



IPC3612SR3-PF28

NVR201-04LP

IPC3612SR3-PF28

2MP Network IR Mini Bullet

Up to 30m IR

Triple streams

IP66

NVR201-04LP

4-ch 1 HDD PoE Network

Video Recorder

HDMI/VGA output

USB3.0 interface

4 x 10M/100M PoE interfaces



HD IP KIT

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

February / March 2016

Building and Construction:

Consultants, Integrators,

Electricians, CCTV Installers,

Architects, Engineers & Estimators

April / May 2016

Government, Transport, Tourism,

Access management, IT security

threats

Disclaimer:

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

Copyright:

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

CONTENTS

- 6 Perspectives on starting out in security: Mandatory training
- 8 Actions of Christchurch bar security staff result in controversy and questions
- 10 Coroner delivers findings into the death of Charanpreet Dhaliwal
- 12 Take a closer look at the latest on offer from Gallagher
- 14 The Retail Sector – Where Safety and Security Collide with Personal and Legal Consequences
- 18 HID Global Helps Simplify Access to Critical Data for Retailers
- 20 See What You're Missing: Mining Your Surveillance Video for Real-time Business Intelligence
- 24 Meet the new NZSA board
- 26 Why Safe Cities?
- 28 What you need to know about drones
- 30 The man who gave us the networked camera
- 34 Facilities Integrate Expo here to stay
- 36 The challenge of integrating security and facilities management within an organisation
- 37 Australia Round-up
- 39 Experts point to payment systems threats in 2016
- 40 Showcase
- 42 Paris attacks: NZ businesses need to 'join up' to be resilient to threats

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

*Standard terms & conditions of sale apply.

Loktronic 0800 367 565
www.loktronic.co.nz

20651

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

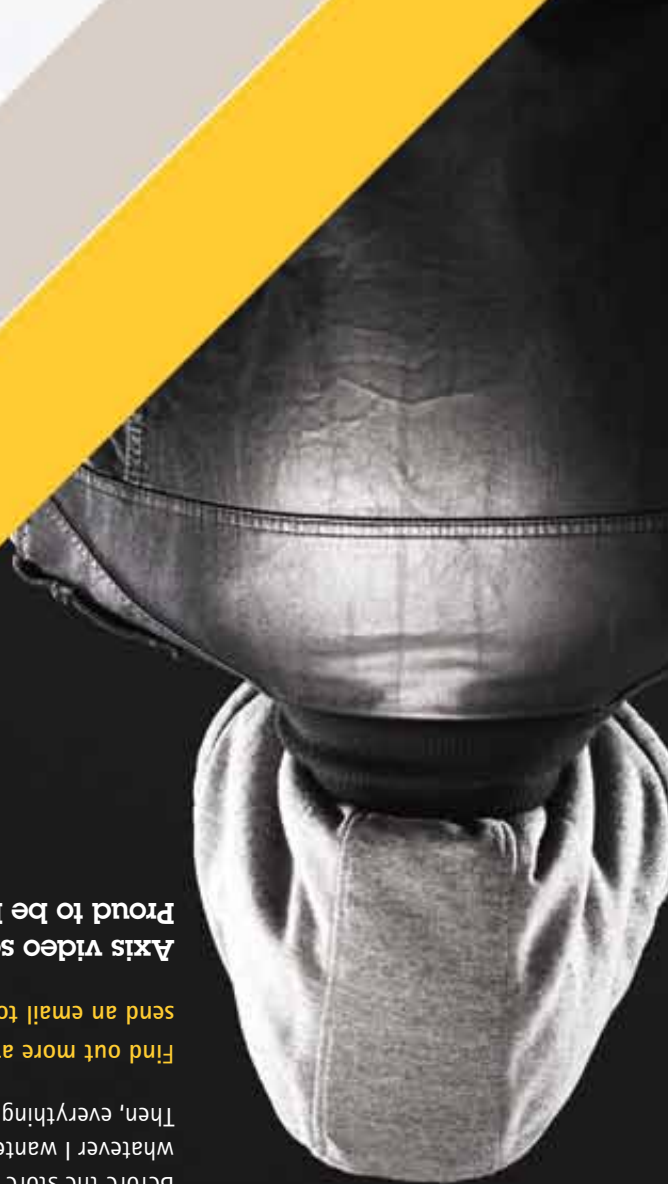
www.NewZealandSecurity.co.nz

I'm a Lover.

Thanks to Axis video solutions, we've gained valuable business insight. Now, we can analyze customer flow, optimize store layout and measure buying activity. Our customers are happy – and so are we.

Find out more at www.axis.com/lovehate or
send an email to contact-sap@axis.com for more info.

Axis video solutions for retail.
Proud to be loved.



I'm a Hater.

Before the store got Axis video solutions, I'd take
whatever I wanted and never pay so much as a cent.
Then, everything changed – and now I'm paying the price.
Find out more at www.axis.com/lovehate or
send an email to contact-sap@axis.com for more info.
Axis video solutions for retail.
Proud to be hated.

Perspectives on starting out in security: Mandatory training

Mandatory training is the entry point into the security industry, bringing together people from disparate backgrounds as they take their first steps toward a career in security. For the many trainees that have not had any prior experience related to the industry, it is also the point at which whatever ideas they had of a career in security start to become real.

In this article, we meet four trainees who've not only bravely decided to give security a go, but who have also bravely agreed to share their initial thoughts on the industry with us. In a few months time, we'll check in on them again to see how they are progressing and whether or not a career in security is turning out in accordance with their hopes and expectations.

We caught up with them during a break in their National Certificate in Security (Level 2) course, and in between practical drills for Unit Standard 27361 – manage conflict situations in a security context.

Samantha Draper

Sam currently works as a stewardess on a super yacht “doing laundry and polishing a lot of silver.” Her goal is to get a berth on a cruise ship, she says, “so I can work my way up, see better places, and have more interaction.”

She sees mandatory training as providing a qualification, but also sees herself actually working in the industry. “I see it as somewhere that can take me further with the qualifications I do have.” In particular, she points to the potential variety of guarding locations as a plus, such as at events, in airport security or at

marinas. There's definitely a travel theme running through her plans.

Interestingly, security is a role that Sam sees as embedded within and relevant to other types of occupations, particularly in the service and travel industries. “It's all around us, in so many different forms.”

Twelve months from now she aims to be working on a commercial cruise liner either internationally or coastally. “That's where I want to be. If I have to get ground experience first in a bar to get that experience, that's great.”

Artisha Gates

Artisha is quick to stress that her interest in security is about people. “I'm willing to help others as much as I can. Being a security guard is not just about being around people but getting to know their personalities while you're working.”

“The job tends to seem easy to others because all they see is someone standing there. But there's a lot more to being a security than just standing there... People are all different, and you're having to maintain control whatever is happening, which is challenging, very challenging.”

Artisha has her sights set on law enforcement. “In 12 months from now I'm really hoping to be in the police force. I just want the experience of being a security officer because it's quite similar.”

I wouldn't mind working in a mall as a security officer, because you're around people every day. It's challenging to me to be amongst people instead of working on my own. It's about confidence building for me. Being in a situation where there's a lot of people, my confidence is going to grow because I'm in that situation instead of avoiding it.



Samantha Draper



Artisha Gates



"If I like being a security officer I might just move myself up instead of giving up on a career that got me into the industry in the first place," she suggests. "I might actually really enjoy it." But if she does achieve her goal of joining NZ Police, she wants to work in the youth side. "There are a lot of youth issues in this generation. I enjoy working with youth about their struggles, to help them keep out of trouble."

Despite her focus and enthusiasm, Artisha found the training to be no walk over. "The training is a lot more challenging than what I thought. It teaches you a lot in the three days. The practical was definitely worthwhile. It keeps us safe knowing our roles before going out there. We do not want to get hurt, so having this training helps us before going out there and actually starting."



Dylan Torr

Dylan Torr

Dylan hadn't considered the security industry as a career option until recently. "It looked fairly interesting and a career that has a bit of progression to it... not just a nine to five job. You can get to go different places with it, and there seems to be plenty of room to grow and expand in the industry."

He too found the training to be a lot more thorough than what he thought it would be. "People look at security guards and sometimes they don't look like much from the side of the road, but the work is actually quite tricky."

In twelve months time, he hopes to be potentially working towards prison escorts or anything out of the ordinary. "I just think prison escorts would be interesting, he says. "Seeing prisoners and being the people that are in charge of transporting



Earl Hardcastle

them around is just something different.

"When people ask me what's your job I'm not going to be saying some boring old thing; I'm going to be able to say that I'm a prison escort."

As for what his expectations are of a security career, Dylan's keeping an open mind, but guarding a shopping mall isn't on his radar. "I want to go with it and see where I can get to."

Earl Hardcastle

Earl's interest in security stems not necessarily from a deep attraction to the industry itself but rather from seeing whether he could actually do the type of work that security involves. "It's totally different to what I've done," he says. "My general background is IT helpdesk, where it's about customer service."

He sees the customer service similarities between the helpdesk and security, but the face-to-face nature of the latter presents a new dimension. "I've done customer service before but that was over the phone, not face-to-face." You can see people's reactions, facial expressions, body language as well [face-to-face], but on the phone its more the tone of their voice, you can sort of hear the anger in their voice through the phone.

As for the training, "I think its been brilliant," he says, and not just for a strictly security context. "You learn so much valuable stuff for when you're out with friends and for how you can diffuse situations." He hasn't found the theory to be too much of a stretch, although, as he points out, "It's hard to visualise what's being said on paper until we do the practical component."

In 12 months time, Earl sees himself still in the security industry, and learning more. "All our lives we're learning, and I will continue to learn and grow with the company." Looking further down the track, he sees himself sticking with the industry long term. "It's more about finding out where I'd like to go, but its cool to know that there's a lot of growth in the industry."

Although convinced of a long-term career in the industry, he's not yet clear on a particular pathway within it. "From the first day of the training, I see that the industry is so diverse and there's so many things you can get into. I haven't looked into all of it."

In a few months time, we'll check in again on our four trainees to see whether they've progressed from mandatory training to new careers in the industry and, if so, what their reflections are as early-career security officers.

Actions of Christchurch bar security staff result in controversy and questions

Video footage showing two men being rendered unconscious by bar security staff outside Christchurch's Strange's Lane bar precinct on the night of Saturday 10 October has created instant controversy within the security industry. The appropriateness of the bouncers' actions have been hotly debated in the days and weeks since, raising a number of questions that go well beyond the incident itself.

The footage shows the two men arguing with the bar security staff after being ejected from the bar. After several minutes, the exchange becomes more heated and a bouncer places one of the men in a headlock. After the other attempts to intervene he is thrown to the ground unconscious. The head locked man is put into a choke hold and is also rendered unconscious. Both are then placed in the recovery position.

Lasting little over two minutes, the footage provides no insight into what may have happened prior to the altercation or following it.

Media reports indicate that police were called to the incident and that after being picked up off the pavement the patrons spent the night in custody before being released. An ambulance was called to the scene at 12.20am, but was stood down soon after as the men were being cared for by police. They did not suffer serious injuries.

The owners of the bar are standing by the bar's security staff, and it appears that no complaint has been laid. Nevertheless, the incident has triggered a polarised debate across social media and among key figures within the industry.

Criticism of bouncers' actions

Head of Training at the NZSA, Stewart O'Reilly, interviewed by the news media,

was critical of the use of force employed by the bar's security staff. According to Stewart, there was "no justification" for it. His public chiding of the bar's security staff has drawn criticism from some within the industry and praise from others.

"The interview they did with me for the press was when I was watching it live, and they told me that my reaction was that I'd said "Good grief", says Stewart. "I still stand by what I said in terms of the actions being inappropriate. I have real difficulty in anyone defending these actions."

"That was not the appropriate thing to do in the situation. It takes place outside the venue, so I don't know what legal ground they're claiming. The bar owner said that it was because there were death threats being made. It's about whether or not those people had the capacity to carry out those threats, and they clearly didn't.

Self-defence, he points out, is clearly defined in the Crimes Act, and from his perspective there was no indication from that video that they were defending themselves.



Stewart O'Reilly, Head of Training at the NZSA

"Somebody making death threats to you is not an excuse for taking self-defence action. You've got to believe that the person is capable of carrying out the threat there and then, and to believe that the person has the current capability to carry that threat out there and then... and I'm sorry, but they didn't.

Although the carotid hold appeared to be applied effectively in this instance, Stewart states that the hold has a slim margin of error, which is why the police no longer use it. "It's banned police procedure, and we shouldn't be doing things the police don't do." This view appears to be shared by Quinton Swanson, a self-defence trainer and former police officer, who was quoted in Stuff.co.nz as being "confused" by the decision to apply the carotid hold.

"From what I'm seeing those bar security officers are assaulting people, but I'm not in a position to comment on the totality of the situation," commented Stewart.

"Other people in the industry in Christchurch – including some security staff – have said "thank God somebody has said something because these guys



Chris Lawton, Director of the C4 Group



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

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

www.allegion.co.nz



ALLEGION

are out of control,” Stewart points out. He doesn’t believe that what aired on the footage is in any way representative of standard practices within the industry there.

He also acknowledges the often dangerous operating environments that bar security staff work in, pointing to another piece of recent footage from Sydney that shows a disgruntled man king hitting a security guard to the ground then running away. Guard Fadi “Fred” Taiba ended up in a coma for 19 days and had to have part of his skull removed.

A post on the NZSA facebook page linking to the news item on the 7 News/ Yahoo website stated, “For anyone who was confused by our media comments last week - NZSA is not “anti-bouncer”, they do a difficult job and many do it very well. I would have no issues with restraining this guy.”

A tough gig

It’s a sentiment shared by Chris Lawton, former policeman and director of the C4 Group, who was otherwise scathing in his criticism of the NZSA’s comments on the Christchurch incident. “There’s some fantastic work being done out there at the coalface,” he says. “That’s the hard yards, where people don’t see it, and that’s why I think we should be supportive of them as an industry because they’re the ones who are surrounded by people who are drunk, drugged, angry and just want to have a fight.”

“I wouldn’t say [the industry has] a bad name, but [bar security] is the part of the industry that’s criticised the

most because it’s at the sharp end where these guys have to use force; they have to remove people on a nightly basis from many pubs, and it’s at some of these locations where the big fights are, where the gangs come together to fight. “At other sites, he points out, guards can back off, but bar security are employed by bars to remove people behaving antisocially... they are required to confront and eject.”

From Chris’ perspective, the Christchurch bouncers demonstrated good individual skills. “In my view they were calm, they were pretty clear, and working together as a team.” Graeme Spinks, a self defence and judo expert who has worked in security, was quoted in the media as saying that in his view “the strangle was not excessive and to KO someone in that environment was actually helpful to those people.”

“Clearly in the Christchurch incident, there had been something going on,” said Chris. “When guys are drunk or drugged or violent, the dynamics change quite dramatically very fast. They can be dangerous and then change again. Their behaviour’s irrational so you can’t judge it from a short video.”

“Death threats ramp things up considerably... You have to do something to minimise threat to self, and that’s self-defence.”

Ultimately, Chris views the NZSA’s comments on the incident as prejudicial. “You don’t see the police saying “oh, that was bad”, they don’t comment until they have all the evidence. Why should our industry comment without the evidence?

“I’ve had phone calls from people in

the industry saying that the comments by the NZSA were unfair. ... it takes the police to charge them and a court to convict them for it to be assault. Up until then it’s an allegation, that’s all.”

Training gaps a factor?

The NZSA’s apparent lack of support is viewed by Chris as a double slap in the face for bar security. He is firmly of the view that the curriculum of the industry’s mandatory training is inadequate for bar security staff, and that the NZSA and its advice to the Ministry of Justice in the formulation of that curriculum is to blame. “It didn’t help that part of the industry that needed it the most. They needed more of what to do when standing and saying “get back” doesn’t work and you have to use force.”

“So you’ve got this same training that doesn’t teach you anything about what to do when the basic verbal and physical projection doesn’t work. Yet that’s day-to-day work in bars. They have to remove people. They have to use force. We don’t teach them anything like that because it’s not in the curriculum.

In an industry that operates largely off the minimum wage, individuals are unlikely to invest in their own training to fill that gap. “The opportunity was there to make it mandatory but the industry did not push it,” comments Chris. “Maybe a graduated training system would do a far better job.”

“So here we are criticising two security guards when the industry didn’t support them with training, and the only way to do it is with mandatory training... we lost an opportunity.”

Coroner delivers findings into the death of Charanpreet Dhaliwal

On 23 October, Coroner Peter Ryan delivered his findings into the death of security guard Charanpreet Singh Dhaliwal. Aged 22, Dhaliwal was found dead in a pool of his own blood after being attacked while working on a west Auckland construction site in November 2011.

It was his first night as a security guard for CNE Security. A group of drunk young men broke into the construction site where Dhaliwal was working. After he confronted them, he was struck in the head with a piece of wood. He had moved to New Zealand a year earlier to study.

In 2013, the man accused of his murder was found not guilty by a jury.

While the report provides some closure to the years-long struggle for justice, it has been a long time coming – so long, in fact, that most of the recommendations put forward by the coroner had been implemented within the industry some time before they made it into his report.

The coroner's findings

Among his findings, Coroner Ryan suggested that had Dhaliwal received appropriate training he may have decided against approaching the group. "Due to his lack of training and experience, Mr Dhaliwal left the relative security of his motor vehicle... this was contrary to accepted industry best practice," he stated. "It is unlikely that Mr Dhaliwal was aware of this."

The coroner also pointed out that if there had been a system of half-hourly welfare checks in place at that time, "then it is likely medical assistance would have been sent much sooner." He stated that there was a case for security guards to be equipped with technology enabling them to call for assistance at the press of a button.

He also recommended that a code of practice be introduced after consultation with the security industry, requiring formal risk assessment of work sites, the introduction of radio telephones for lone night guards and regular welfare checks.

Stakeholder reaction

In a 23 October media release, the NZ Council of Trade Unions (CTU) welcomed the coroner's findings.

"The CTU thanks Coroner Ryan for his work on this case and his recommendations," states Jeff Sissons, CTU General Counsel. "We intend to work with security guards, their unions, the security industry and WorkSafe to honour Charanpreet's memory by making the industry safer. The recommendations form a good base to do so. We have spoken to WorkSafe and they have agreed to meet to discuss the next steps."

The CTU also used the findings to push for the inclusion of the security industry in the list of high-risk industries for the soon to be enacted *Health and Safety at Work Act*.

"A sad irony is that while the Coroner and all parties acknowledged the high risk



Charanpreet Singh Dhaliwal killed on his first night at work

nature of security work, this industry has not made Minister Woodhouse's draft list of high risk industries. A working people in a small firm like CNE Security would be unable to ask for a health and safety representative under the draft law. The CTU is also calling on the Minister to include security work in the list of high risk industries."

There is no indication yet as to whether or not this recommendation will be given any serious thought in Wellington.

For the New Zealand Security Association (NZSA), the coroner's report hits the mark. "The coroner's report says mandatory training should be in place; it already is," says Stewart O'Reilly, NZSA's head of training. "All of the things raised



Focus your energy on the things that matter.



The fuel card that helps you run things your way

Find out more at mobilcard.co.nz

Energy lives here™

Mobil™

An ExxonMobil Brand

MOB1621_NZS

by the coroner's report which says that there should be a code of practice for the industry – they are all in the existing NZSA Codes of Practice.”

According to O'Reilly, NZSA has had Codes of Practice since they were first written in 2004/5. They were last reviewed in 2012 and are currently being reviewed again. Mandatory training has also been implemented industry-wide.

One recommendation that O'Reilly believes is problematic is the suggestion that the three-month temporary Certificate of Approval be removed, preventing guards from working until they've been trained.

“There's a financial reality here, were talking about a low paid occupation. We're already putting a barrier of around the \$500 plus mark to get into the industry to work in a low paid occupation. We're now going to say that you are not only going to have to spend that money but now you can't work until you've completed the training? It's another barrier to entry.”

He suggests that the alternate option of having people on temporaries being required to only work alongside an experienced officer is feasible. It is something the NZSA would support – and consistent with provisions already

existing within their Codes of Practice.

“No matter what we do,” he says, “there are risks within the occupation, but there are things that any responsible employer should be putting in place to mitigate those risks and keep the majority of our staff safe.” And although the NZSA requires its members to comply with its Codes of Practice, he points out that they cannot require it of non-members.

According to O'Reilly, NZSA has an 80% share of the industry in terms of membership. There are 595 companies licensed as property guards and 242 individual (owner/operator) license holders. 80% of these 595 companies are not members, but the handful of companies that employ the majority of guards are. There are 22,000 current Certificates of Approval for property guards.

Although some small operators are with NZSA, O'Reilly points out that many of them are not, and these would also be the least likely to have the capacity to follow their Codes of Practice.

“People who rely on winning contracts on the lowest price are not going to be able to put these things in place, because you are going to put an inexperienced guard out there without a supervisor because you can't afford to be paying two salaries. You won't spend the time

training, you won't have the skills, experience and time to conduct a risk assessment of the site before you deploy a guard.”

O'Reilly says that many companies mistakenly assume that clients are wanting the cheapest possible solution. “Clients don't want the legal implications, they don't want the reputational problem. The clients are a lot happier if you're actually providing a professional service.”

“We say that you should do a risk assessment, do an operational security requirement, identify what the best way of meeting the clients needs is, so you're showing them that you're thinking and demonstrating a professional service.” The optimal solution, he says, might not be to deploy a guard 24/7, but rather a mixture of risk management processes that could involve security lighting, a new lock on the door, etc.

It's about providing a risk management solution, not simply a guarding solution. “Guarding is just one aspect of the solution that we provide. This means that for NZSA members that they need to network with other members to provide total solutions. They need to keep themselves upskilled as to what's happening... You're not selling guards by the hour, you're selling a package of solutions.”

Take a closer look at the latest on offer from Gallagher



There's product evolution then there's product revolution. The latter of which best describes Gallagher's latest generation in electric fence control. The just launched F3 Series Fence Controllers are fast becoming the new standard in electric fence management. Pushing the boundaries of functionality and design is what Gallagher do best and the F3 Series delivers on both. Providing a great range of flexibility, versatility and visibility, the F3 Series is capable of working as either stand-alone or fully networked perimeter technology. The design of the F3 Series allows the controller to suit a wide range of environments as it can be mounted in either portrait or landscape orientations. The LED Icon display allows operators to view at a glance the alarm state and voltage output capacity

of the controller while the Magnetic Key, sold with each unit, allows operators to clear historic alarms.

Gallagher haven't forgotten about their security management software either releasing a new version of Command Centre v7.40 that is brimming with additional features. The overhaul of Command Centre includes a new scheduling function that prevents a site switching to free-access mode until a privileged card holder is on site. Visitor Management and Gallagher's award winning T20 Terminals got a piece of the action as well. The upgraded T20 now allows an operator to manage perimeter alarms in the field through the terminal allowing for overrides, maintenance and repairs to the fence line. Gallagher's Visitor Management Client and Kiosk gained

new hardware in the form of a barcode scanner which significantly speeds up the entry and exit process for visitors while automation of some previously manual inputs reduces the interaction required from on-site hosts.

For more of Gallagher's latest products watch their videos





New generation. New possibilities.

Unleash the potential of your site with Command Centre v7.40, the latest in security management software from Gallagher.

Find out more at security.gallagher.com/latest-releases



2015 WINNER
PRODUCT OF THE YEAR
ACCESS CONTROL



The Retail Sector – Where Safety and Security Collide with Personal and Legal Consequences

Much has been said about the significant changes about to occur with the Health and Safety at Work Act 2015, which comes into law from April 2016. For the first time, all people within a business will have responsibilities to keep themselves and others safe from harm. This includes everyone from directors and managers to floor staff.

Although not listed among the high-risk range of industries, such as forestry and construction, where there have been many well-documented tragedies, retail sector occupations are exposed to significant 'people versus people' risks. Such risks relate to the behaviours of robbers, thieves and other angry or disaffected people, some of whom may be impaired by alcohol or other drugs, and can be the cause of serious harm.

This is where personal safety and security collide in the workplace, sometimes with the worst of outcomes.

All organisations that are open to the public and handle cash are at risk of robbery. So are businesses that stock or handle valuable and desirable commodities such as liquor, cigarettes, jewellery and electronics, among others.

In 1990, when Bruce Couper started developing and delivering training for at-risk people on how to prevent robberies and similar events, as well as how to stay safe should such an event occur, companies who provided this training to their staff did so because they had experienced incidents that went wrong. As with many security issues, it is only when people have been victimised that they appreciate the need to increase safety measures and train for dealing with risks.

The same moral obligations to keep everyone safe still apply today, but there will be an increased duty of care owed by employers to all employees come April 2016. The penalties for non-compliance

are increasing significantly and there are now significant prison sentences for individuals who recklessly shirk their responsibilities under the new act.

So what can be done to make all employees in the retail sector safer from such risks? As always, it starts with having the right policies in place, supported by appropriate security procedures to both prevent incidents from occurring and to guide staff in taking actions to heighten safety. Staff then need to be trained on how to carry out the procedures.

Bruce recalls when he was first involved in creating safety training solutions in the 1990s, at least one of the country's largest financial sector organisations had training materials for their tellers that read, "In the unlikely event of a robbery: Go slow. Look them in the eye. Give them the small notes first." These are some of the most negligent things I have ever seen, but sadly not the worst.

4K

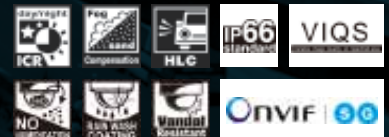
IT'S IN OUR DNA

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



WV-SFV781L VARI-FOCAL CAMERA

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



OUTSTANDING CLARITY

THE PANASONIC VARI-FOCAL OPTICS AND 12MP SENSOR

4K OFFERS IMPROVED CLARITY

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

FALL OFF REDUCED

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

12M PIXEL MODE

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



WWW.PANASONIC.NET/SECURITY

Panasonic



We've come a long way since then. Our observations are that companies in the retail sector today aim to keep their staff safe as a matter of utmost priority.

What can be a struggle is how to do this efficiently and cost-effectively, allowing for operating changes and staff turnover.

RISQ New Zealand was engaged as the subject matter expert for Foodstuffs North Island early in 2015 to create video-based training materials that were relevant and accessible and could be used across their many stores and brands. The development of distinct training videos for all staff and for managers and supervisors covered all issues, including:

- Preventative measures
- Safe actions during a robbery
- How to look after people and the scene immediately after an incident
- Carrying out a critical incident debrief within 72 hours of an incident and supporting all affected staff

Cash Converters and Mitre 10 MEGA New Zealand have recently embraced this concept, with the latter having their own branded material developed and distributed to their network to allow a roll-out of training to take place.

Robbery safety training provides people with the knowledge of what the

risks might be in any scenario. It is about providing them with tools and new coping skills that they can practice so that they can safely respond in an emergency or threatening situation.

The training is encapsulated in our simple mnemonic COOP: Calm yourself – Obey the robber's orders – Observe only when safe to do so – Preserve life and evidence.

Online versions of the training are currently being finalised, but all such material is now available on other media, such as generic or branded USB flash drives (email bruce@risq.co.nz). With these resources, all at-risk staff can be trained upon induction and can undergo annual refresher training and testing.

What about other situations?

While an armed or aggravated robbery in the workplace is possibly the most dangerous event in retail, there are far more common day-to-day situations that also endanger retail staff. Some call it dealing with Difficult Customers/ People and Difficult Situations. We refer to this area as personal safety and conflict management.

Customers or any member of the public can become a danger to staff for a number of reasons. When a person is in a distraught, aggressive or in a heightened

emotional state, being able to recognise these signs and listen to what they are saying is vitally important. Having some simple response and de-escalation tools is crucial for all retail staff.

Equally important is understanding that your personal safety is of paramount importance, so that when you are feeling really unsafe it should no longer be about managing the conflict or building rapport, but rather about "how do I make myself safe?" This can then manifest in verbal skills, calling for assistance from others, creating a safe space or fleeing the situation.

These situations occur in the retail sector many times every day across New Zealand.

RISQ New Zealand have been training in this environment for many years and now they are developing video-based and online resources on these specific risks.

RISQ New Zealand, based in Albany, Auckland, has been providing training and/or robbery safety kits for a number of major retailers and the feedback from both management and staff has been very positive.

There are an ever-increasing number of New Zealand's retailers wanting video-based resources so they can induct and train their staff on an ongoing basis.



*Bruce Couper
is the Managing
Director of RISQ
New Zealand Limited*

Background

Bruce spent 11 years in the New Zealand Police and during that time worked across a range of uniformed duty roles. The last four years of his service were in the Criminal Investigation Branch as a detective.

Upon leaving the NZ Police, Bruce founded The Couper Group Ltd, which became the largest provider of investigative and security consultancy services in NZ by the time it was sold in 2002.

Since 2002 Bruce worked in a senior strategic role with another security and investigative consultancy before spending 15 months working exclusively as a specialist trainer in the Australian market. He was engaged as a contractor to an RTO delivering qualification based training courses to federal and commonwealth agencies on fraud control and

investigations across Australia. Bruce then founded RISQ New Zealand Ltd in 2008 to provide Training, Risk Management and Investigation Services.

Experience

Bruce has been developing and delivering specialist training in the areas of fraud prevention, personal safety and conflict management for more than 20 years. He develops and delivers such training programmes for a number of NZ companies and government agencies.

Bruce spends considerable time managing client relationships and developing new strategies to optimise client results and benefits.

Qualifications & Professional Associations

Bruce is a former chairman and now a life member of the NZSA (New Zealand Security Association). Bruce is a former chairman for ASIS International (NZ Chapter 148).

Performance affects funding

The Skills Organisation (Skills) is proud to partner with the security industry and we look forward to continuing this strong partnership.

For Skills to continue providing resources and invest in equipping security personnel; lifting performance is critical.

Skills funding is determined by the Tertiary Education Commission (TEC) who look primarily at completions and performance to determine the level of investment into industry training.

Stronger performance will ensure we can continue to invest in helping your people stand out from the crowd.

Education Performance Indicators (EPI) Update

Completing qualifications is the first step on the road to improving performance.

Qualifications provide your personnel with an achievement and a tangible record of their on-job training leading to engagement and quality service.

To date, 26% of trainees have completed their qualifications. We still have a fair bit to achieve to reach our target of 60%. The CCR (Credit Completion Rate), which indicates the rate of ongoing training activity sits at just 36%. This is down from 53% in 2014.

The clear solution and benefit to you as an employer, is to ensure that trainees are better engaged in ongoing training.

If we don't reach the target, funding will eventually be cut altogether. Let's work together to get back on track.

Private Security Personnel Licensing Authority (PSPLA) Update

In a recent briefing to the industry, the PSPLA expressed training is still an area of concern.

Between 5,000 and 10,000 security personnel are still yellow-card holders. Due to this figure, the PSPLA advise security companies to increase their level of commitment to training.

As of March 2016 yellow-card holders who have not completed their mandatory training and apply for renewal of their Certificate of Approval

(CoA), will be declined without any exceptions or exemptions offered.

While the PSPLA has attempted to regulate with a gentle hand, the crunch has now come.

If you have any concerns about your trainee progress, want to register for My Skills, or just have a query - we're here to help. Get in touch with on 0508 SKILLS (0508 754 557) or support@skills.org.nz.



Wayne Abel
Industry Manager - Security
The Skills Organisation



Achieve long term business success

Invest in workplace training

skills.

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

HID Global Helps Simplify Access to Critical Data for Retailers and Enterprise Organisations with Authentication Solution for Microsoft Office 365

- Retailers can improve service and enhance security by enabling floor staff to access the information they need by simply tapping a smart card to their tablet.
- Healthcare organisations simplify electronic prescription signing and enterprise users have easier access to cloud applications as HID Global and Microsoft continue to collaborate on improving the security-enhanced experience across mobile devices.
- HID Global hosted a webinar on mobile authentication, mobile trends, and the results from a mobile study; the two companies will jointly host part two of the public webinar series later this year.

HID Global®, a worldwide leader in secure identity solutions, is collaborating with Microsoft to make enhanced cloud app security as simple and convenient as tapping a smart card to a laptop, tablet, smartphone and other NFC-based mobile devices. HID Global hosted a webinar on mobile user authentication and how HID Global's new solution, ActivID® Tap Authentication, can benefit users of Office 365 and other cloud-based applications in their daily work. The two companies will jointly host part two of the public webinar series later this year. This will build on the foundational meetings with key Microsoft ISVs at Microsoft WPC in Orlando that took place earlier this year.

"We are excited about our collaboration with Microsoft and the potential to take the industry to a new



level of security-enhanced convenience and simplicity," said Ian Lowe, senior manager of product marketing, Identity Assurance with HID Global. "Retailers will be able to use ActivID Tap Authentication to more easily access inventory control and payment systems from the store floor. Healthcare professionals and enterprise users who often log-in 20 or more times daily can now replace complex passwords with a more simple and security-enhanced tap-in experience. We continue to explore many new opportunities with Microsoft to bring ActivID Tap Authentication to a growing range of users and applications."

"Microsoft is excited to be collaborating with HID Global to offer our mutual customers a great new option when accessing Office 365 and other cloud apps and web-based services," said

Jen Field, Senior Program Manager with Microsoft. "The combination of HID Global's ActivID Tap Authentication solution and Microsoft's Active Directory Federated Services (ADFS) will help our retail and other customers make it easier for their users to access corporate cloud applications, data and services anywhere, at any time, from the mobile device of their choice, with the same smart card they use to open doors."

Introduced in April, ActivID Tap Authentication for Microsoft is powered by Seos® and tightly integrated with Windows Server 2012 R2 Active Directory Federation Services and the HID Global Authentication Cloud Service. It supports Microsoft Windows 7 laptops and desktops, Android™-based tablets and other mobile devices via NFC.

SWIPE TAP TWIST POINT TOUCH OR PUSH WITH CONFIDENCE.

Technology is evolving and words like “interoperability” are taking on entirely new meaning. HID Global is leading the industry by developing the world’s broadest portfolio of truly scalable, fully interoperable secure identity solutions. We are connecting people to places with physical, mobile and virtual access solutions like never before—and we’re doing it with the most advanced layers of security anywhere on the planet.

You’ll call it seamless end-to-end solutions. We call it, “*your security connected.*”

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

See What You're Missing: Mining Your Surveillance Video for Real-time Business Intelligence

When retailers think of video surveillance, it is usually in the context of loss prevention and security. But there is a whole other arena where surveillance video provides enormous value: gathering real-time in-store intelligence to help you improve your margins.

With the embedded analytics in network video cameras, you can not only observe customer behaviour in-store, but garner real-time statistics to help you improve store layout, product and display placements, and even identify bottlenecks and dead areas on the shop floor. Unlike the hit-or-miss approach of customer surveys and mystery shoppers, network video offers you an accurate and unbiased report of the immediate situation and of changes over an extended period

of time. You get a clear view of how customers move along the aisles, making it possible to optimize shop floor plans and merchandising strategies to drive your sales and profitability.

Sharing intelligence across channels

Because the surveillance video is streamed over the network, multiple departments can securely share views of store activity in real-time. Store managers can compare analytics between multiple stores for a range of activities – from customer traffic to sales statistics. You can even download and share select video with your supply chain to improve inventory levels, merchandise selection and stock turns.

Optimizing shop floor plans

A network-based video surveillance system makes it easy to identify a store's hot spots, dead zones and bottlenecks. You can easily program the system to generate heat maps that portray customer traffic for selected time periods. These maps provide valuable input for improving store design to facilitate more inviting access to merchandise. You can also combine mapped traffic patterns with point-of-sale statistics to immediately evaluate the impact of any changes you make to the floor layout – customer flow, items sold and the average sales amount.

Improving end caps and displays

Another way to leverage video intelligence in your retail operation is in the area of product placement and display strategies. Store managers can record video of customer interactions with different displays and then review the heat maps to see how effective those displays are at attracting shoppers to purchase the featured merchandise. You can also use video surveillance to compare traffic flow and sales figures between stores with or without a particular end cap or display.

Evaluating advertising and signage

Similarly, you can test the effectiveness of promotional campaigns, in-store advertising and signage by studying the customer flow captured on surveillance video. With advanced video analytics you can even measure the dwell time



Heat maps enable retailers to identify store hot spots, dead areas and bottlenecks

What you can learn from video surveillance

Question: *Is my shelf display attracting customers?*

Answer: *A single network camera focused on a shelf location can measure:*

- *Number of people passing by the shelf*
- *How long each person lingers at the shelf*
- *The direction people are coming from when approaching the shelf*

Question: *Is my store layout inviting to shoppers?*

Answer: *Several high-mounted network cameras focused on movement across all aisles can detect:*

- *Dead spots where customer traffic is too low*
- *Hot spots where customer congestion occurs*

customers spend in front of a sign or display. Intelligent video analytics applications provide a number of key performance statistics, including average viewing time, distribution of viewing time and number of shoppers viewing during a selected time period.

Placing video surveillance intelligence where it does the most good

Watching hours and hours of store video can be an extremely tedious and inaccurate way to mine valuable data. And yet customer traffic patterns can reveal a lot about your patrons. With strategic deployment of intelligent network cameras throughout the store, however, you can slash that viewing time by allowing the camera to automatically analyze the video data and glean the useful information for you. Intelligent video surveillance systems use complex mathematical algorithms to extract moving objects or other recognizable forms from the recorded video, while filtering out irrelevant images or movement. Intelligent decision-making rules govern the data search to determine if the activity recorded in the video should be flagged for further review.

There are numerous advantages to processing as much of the video as possible inside the network cameras. For instance, putting intelligence at the edge helps you:

1. **Minimize bandwidth usage** – Network cameras can be programmed to only transmit video when they detect motion in a defined area of a scene. This dramatically reduces bandwidth consumption and the number of operators needed to review
2. **Reduce server costs** – In a centralized video surveillance architecture, servers typically process four to 16 video streams. When network cameras do the processing, servers can handle more than 100 video streams. For people counting applications, for example, the resulting data (rather than the video stream) can be sent directly into a database, further reducing the load on servers.
3. **Improve video surveillance analysis** – When network cameras process raw video data before it is degraded by a compression format, the quality of analysis greatly increases. This configuration also reduces the number of servers required to process the transmission because fewer video packets are actually sent along the network for uncompressing or transcoding prior to processing.
4. **Lower operating costs** – With fewer servers needed, power consumption and maintenance costs drop. This also removes the burden from environments without server rooms to build special facilities to support their video surveillance system.
5. **Lower equipment investment costs** – Reducing network bandwidth usage by streaming only essential information (metadata and snapshots)

transmissions. For instance, network cameras can extract a head count from a frame and send just the essential data with a few snapshots instead of consuming bandwidth with several hours of unfiltered video.

gives retailers the option to deploy more moderately-priced network components that can easily support reduced data rates.

Combining video intelligence and POS

Because network video systems are generally built on open standards, they can be easily integrated with your other retail systems to provide a higher level of intelligent analysis. For example, by combining data from your point-of-sale registers with your video surveillance analytics you can determine a store's conversion rate down to an item level. Trends in employee performance such as daily efficiencies can also be tracked, indicating the need for additional training or other factors impacting cashier effectiveness.

Impacting the bottom line

Retailers who continue thinking of video surveillance strictly as a loss prevention tool are missing a huge opportunity to leverage some truly powerful in-store intelligence. Network video systems provide an efficient and unbiased way to analyze customer behaviour and shopper traffic. The technology makes it possible to evaluate and compare merchandising and marketing initiatives at a single store or throughout a chain. With strategic application, network video gives your store managers the real-time insight they need to optimize store layout, product placement and advertising to enhance your shoppers' experience, which will inevitably boost your bottom line.

*by Trevor Westhead, Business Development
Retail South Pacific Region
Axis Communications*



RED WOLF

HIGH LEVEL MONITORING



RED WOLF SECURITY GROUP

Red Wolf Security Group is an industry leader in high level security solutions. We partner with all sectors including; government, corporate, commercial and residential. We develop partner specific solutions combined with strategic planning to future proof and add value.

We specialise in electronic security solution design, installation and asset management, security network operations centre services, systems monitoring, outsourced systems management services, and security consulting.

Red Wolf is proudly New Zealand owned and managed.



THERE WHEN YOU CAN'T BE

RED WOLF HIGH LEVEL MONITORING

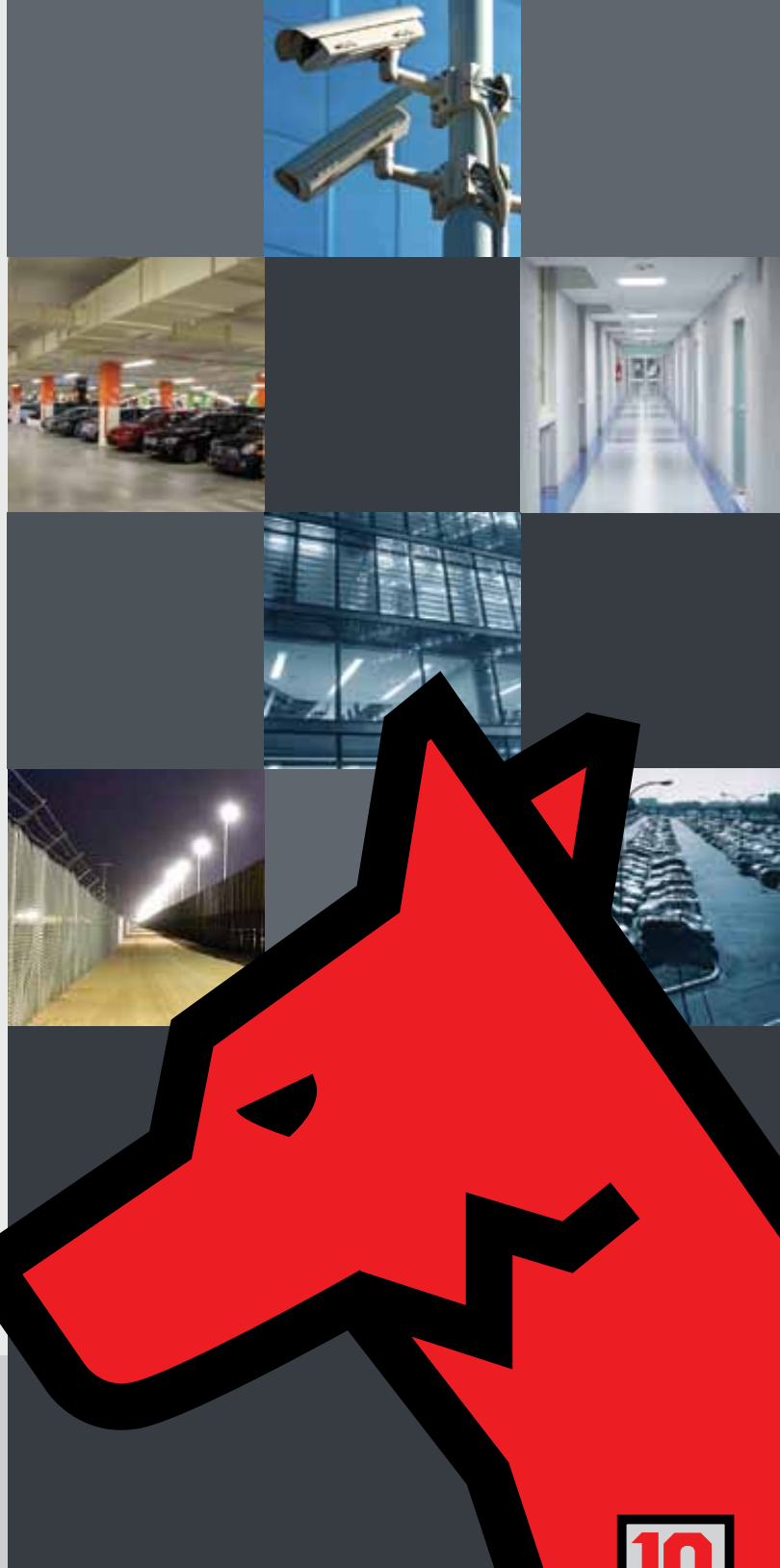
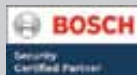
Although we have provided monitoring for some time, Red Wolf High Level Monitoring Ltd has developed a state-of-the-art Grade A Security Network Operations Centre (SNOC).

Our operations centre in Wellington provides monitoring for a diverse range of security solutions and systems throughout New Zealand and abroad. This facility has the latest technology incorporated within its self-contained secure bunker. This allows a comprehensive range of monitoring solutions and services to fulfil all of our business partners' requirements.

MONITORING SERVICES INCLUDE:

- Integrated alarm monitoring for a diverse range of systems and solutions
- Intruder detection
- Plant alarms
- Duress alarms
- Man down health and safety alarms
- Lone worker
- Perimeter protection alarms
- Access control system monitoring
- Systems and card database management
- Closed circuit television monitoring
- Closed circuit television virtual patrols
- Operations centre fail over

OUR PARTNERS:



Call: 0800 REDMON (73 36 66) or visit: redwolf.net.nz



Meet the new NZSA board



Doug McCormick, Chairman

Has been employed in the security industry for 30 years until moving to semi-retirement during 2014. His appointment to the NZSA Board for the past 3 years and into the future is through employment with the Gallagher Group.

Doug has worked in the Gallagher NZ, UK and USA offices. While in the UK, he was a member of the BSIA Access Control working group and is currently a member of the IEC international working group responsible for preparing a new set of Standards for access control and associated systems. He is also the NZ delegate to the IEC Technical Committee 79 (Alarm and Electronic Security Systems).

My vision for the NZSA is to further develop customer growth for NZSA members through initiatives that explain and promote benefits of choosing NZSA members for their security requirements, which include the benefits of established standards and training.



Bronwyn Paul

Operations Manager at Electra Monitoring Ltd trading as Securely

Entering 5th year on the NZSA Board. Immediate Past Chair 3 years.

Key aim is to work with Stakeholders and end users to position NZSA members as providers by choice for provision of security services contracts.



Ben Marsh

Ben is the Principal of Marsh Security Consultancy Ltd.

He joined the board in August 2014 and is passionate about professionalism and ethical conduct within our industry.

His objectives on joining the board is to continue to enhance codes of practice and standards of auditing.



Mark O'Brien

General Manager, Manned Services – Armourguard Security

Mark has been a board member for 3 years.

Although there has been positive progress in the industry significant effort is still required to lift standards. The team at the NZSA is working hard to continue that progress on behalf of all of our stakeholders.



Ziso Avram

Ziso is the Managing Director of Guardforce Security Ltd.

He has been a board member for the past 12 years.

His contribution to the NZSA has been to promote a high level of integrity amongst NZSA members and to provide solid guidance to the NZSA operations, particularly financial management.



Marsden Hulme

Country Director & General Manager Vivint NZ

Board Appointment: November 2015
Former NZ Police Officer
25 years in senior management roles in ICT and Business Process Outsourcing in NZ, Australia and US.

"My aim is to offer my time and whatever talents and experience I may have for the betterment and benefit of this industry that we are all fortunate enough to be a part of".



James Sutherland

Northern Regional Manager for FIRST Security Guard Services Limited.

James has been on the Board of NZSA for 5 years.

Over the past five years I have seen some significant changes within the security industry and the association. There are more expectations for the NZSA than ever before to step up and be the voice of the industry.

I believe that there has been significant progress made in this area with relationships with government and the delivery of added value to the membership including the establishment of NZSA Training and the fuel card initiative. I look forward to see NZSA continue to deliver more benefits to the NZSA membership and be the voice of the industry.



David Proud

David began his security engineering career in 1987 and founded VIP Security.

David's contribution to the board is as a person well versed in most aspects of electronic security, company management and strategy. David is committed to continuously raising the standards and quality within the industry.

He has previously served on the NZSA board. His aspirations are to work with the board for the overall benefit of all members (small, medium, large and corporate) and ensure good governance and teamwork within the board and that it keeps true to the set goals.



Kerry Heard

Kerry is the New Zealand General Manager for Hills Ltd.

He has been a board member for the past 4 years.

His vision is for the NZSA to be the voice of the industry, setting recognised standards and helping members achieve them, educating the public at large about the value of security and adding value to members.



www.security.org.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.



Why Safe Cities?

In this final of three articles by Chris Lawton of C4 Group we will look at how CPTED and other community programmes have reduced crime in three important cities of New Zealand. Hutt City, Christchurch and Henderson Auckland.

Christchurch

The Institute for Economics and Peace, 2012 stated that Christchurch New Zealand as one of the safest cities in one of the most peaceful countries on earth. This title was of course destroyed as was a large part of the city and environment.

In rebuilding the city Crime Prevention through Environmental Design (CPTED) has made a remarkable contribution to ensuring that the 'new' city is as crime free as it can be.

There has been a significant effort put into incorporating CPTED into the rebuild of Christchurch

The Design, methodology, approach is detailed in a paper written by Sue Ramsay, a Crime Prevention Team Leader, based in the Community Support Unit, Christchurch City Council, Christchurch, New Zealand. This is available online and should be read by all upcoming CPTED enthusiasts.

The paper is a case study and discusses the author's experience of working within Christchurch before the earthquake and describes her involvement in the rebuild of Christchurch post-earthquake.

The paper identifies the principal establishments;

- There has been significant process made in incorporating CPTED into all projects.
- A formal mandate to consider CPTED is included in the Central Christchurch Recovery Plan.
- CPTED is used throughout public and commercial rebuild projects.
- The need to increase practitioner capacity.
- CPTED is being included earlier in planning and design.
- The Christchurch rebuild may be the most extensive application of CPTED yet.

- It is hoped that Christchurch's experience can be used as a model for other cities to increase their use of CPTED.
- Funding is required to widen the uptake of CPTED and create a positive and informed understanding within the community.

Benefits of the CPTED programme were;

- The provision of a formal "home" for CPTED in community safety.
- Access to expert advice.
- Building local capacity through training.
- The Design Out Crime Advisory Service was formed.
- Information Seminars are provided to professional and community groups to introduce the concept of CPTED and its benefits.
- Building capacity through the CPTED Practitioners Group.
- CPTED Clinics are run monthly and are open to anyone who would like CPTED Advice.
- Funding from the Crime Prevention Unit of the Ministry of Justice: this funding has been essential to the growth of CPTED in Christchurch.

CPTED principals in Crime Prevention considers the Context, Connection and the Spatial analysis. The principal of a 'little, early and often' ensured CPTED practices were incorporated from inception to post-construction. In this way, CPTED can be involved in a project at appropriate junctures and those involved can be offered input from brief conversations to written plan reviews.

'Involving CPTED early and often is the most cost effective way of including CPTED. It is much less expensive to make changes on a plan than to make the same changes in a physical environment'.

The CPTED approach taken in Christchurch consisted of a CPTED programme lead by the Crime Prevention Team, acting in conjunction with the community as well as partner organisations, acting early in the design and management of development projects, carrying out appropriate interventions whether a conversation or a full CPTED assessment by experienced practitioners.

The use of CPTED in the Christchurch rebuild identified some issues with it. Firstly that the perception of CPTED was that it is less complex than it really is. The need for a sustainable pool of competent practitioners as well as the strengthening of policy framework in which CPTED and crime prevention operates.

The gains of a CPTED programme were a greater awareness of the benefits of CPTED, providing a focal point for Crime prevention; CPTED was ingrained in more projects, multiagency collaboration; IPTED (Injury Prevention Through Environmental Design) development and of course a safer and more liveable city.

Henderson City Crime Prevention Project

After a spate of murders and the recognition of an ongoing reign of petty crime Henderson City is now the subject of a crime prevention project lead by Auckland Council and Police.

Unlike a city rebuild such as Christchurch, Henderson is an established and functioning city. The development of 'designing out crime' is not just a matter of rebuilding.

The importance is also to build community confidence and a feeling of safety.

This project requires a lot more involvement of people. The police have increased both foot and mobile patrols in three city area. More than that there is now a consistent approach in the use of Community based security groups. These include Maori and Pacifica wardens, as well as Neighbourhood support and in particular Community Patrols of New Zealand. Of particular importance is that Henderson City area does not have a patrol itself. The patrols are conducted by neighbouring areas such as Te Atatu - Glendene, Swanson - Ranui. Patroller show at the call from the Police patrol certain areas at night and day to decrease opportunities of crime.

And the response is not only in front line policing. Police youth experts are seeking to work with youth and prevent them offending. Groups such as Waitakere Anti-Violence Essential Services work behind the scenes with social deprivation issues. Foundation for Youth development work with siblings of youth offenders in attempts to stop the cycle.

The Henderson Lincoln Business Association works with the local business community as well as key stakeholders and community groups to be a strong voice to leverage and influence change that will reduce crime and feelings of insecurity and be of economic benefit to the Henderson-Lincoln Road area.

The Association's key aims are: Provide a safe and secure environment for economic activity; Increase visitor numbers to the area; Create a sense of business community – bring the heart back into the community!; Create a brand awareness for the area through events and project management.

In a recent media release Vanessa Neeson, Henderson Massey Local Board stated that the West had come together in response to what has happened in Henderson.

This is the most important aspect. The community comes together under leadership of Police and Council to assist people living in other areas of their city. We are likely to see more of this over the coming years.



NZ's #1 security training provider – a one-stop shop for all your security training needs. The only security training provider to be awarded the Skills Organisation quality assurance award 'Skills Certified'.

We are able to offer the following courses and programmes.

NZQA COURSES:

- National Certificate in Security Level 2
- National Certificate in Security Level 3
- National Certificate in Security Level 4
- National Diploma in Security Level 6
- Certificate of Approval Mandatory training
- Conflict Management Instructor training

NON-NZQA COURSES:

- Professional Investigator
- Port Facility Security Officer
- Bomb Threat
- IED
- Armed Robbery
- Security Consultant
- Control and Restraint
- Calming and Restraint (Health)
- Close Protection (Body Guard)
- Self Defence
- Baton and Handcuff training
- Aviation Cabin Crew training

For more information go to www.c4group.co.nz

Hutt Safe City

The Hutt Safe City Group is administered by a Charitable Trust acts as an umbrella organization that provides administrative, financial and other relevant co-ordination support to various safety focussed groups throughout the Hutt Valley.

The Trust has a seven-member Board that deals with governance, financial and policy matters and meets bi-monthly. Management Committee meetings are also held monthly to discuss co-operative, operational and information matters. These are attended by representatives of the following:

- Community Patrols of New Zealand (6 patrols throughout the Hutt Valley, 100 volunteers).
- Neighbourhood Support (259 groups).
- CCTV Camera operators (32 volunteers monitoring cameras located across the Hutt Valley).
- Hutt Valley Police.
- Hutt City and Upper Hutt City Councils.

They also work closely with other groups in the safe community's area such as the Wellington Regional Emergency Management Office, Safe City Ambassadors etc, have an open welcome to approaches from other like-minded organizations. Hutt Safe City and its constituent groups are all volunteers, with the exception of three staff.

Civic minded volunteers that care about their community are crucial to achieving our objectives and are always very welcome. There are differing roles in the various groups (such as Camera volunteers, Community patrols, Neighbourhood Support etc) that would suit most people and after a security vetting process, full training is provided. Contact the Hutt Safe City Manager for further information or visit www.huttsafecity.co.nz



What you need to know about drones

In recent months we've seen growing media and industry chatter about the growing market for drones – or UAVs – in New Zealand

An increasing number of players within the fledgling NZ drone industry are forging partnerships with developers overseas and commencing their own R&D and assembly capabilities locally. The recent Facilities Integrate and New Zealand Security trade shows attracted drone exhibitors, and over 2016 we're likely to be hearing, well, the 'drone' of UAVs more frequently than ever.

A recent NZ Security article featured the warnings of Vivint CEO Marsden Hulme in relation to the potentially malevolent use of UAVs by criminals in NZ. In this issue, we discuss the positive consumer and commercial applications of drone technology with Tactical Solutions' Ross Taylor.

Based on Auckland's North Shore, Tactical Solutions formed in 1999 to offer military, law enforcement, security and public safety departments and personnel access to the world's best operational equipment. Tactical Solutions is a leading provider to New Zealand's law enforcement agencies and supports customers in Australia and the region.

Where does NZ sit relative to other major markets in terms of the uptake of drone technology?

At the consumer level UAVs have seen a huge increase in their popularity and their widespread uses are being applied across the country more and more.

Drone racing, aerial photography and commercial use have increased dramatically.

We are probably further behind in the full size and military UAV technologies – as far as I am aware at least, I would believe this to be because we don't have a high interest in drones as national assets in the same way other nations, such as the US, do.

What do you see as being the major applications of UAV technology for New Zealand? Who will want drones?

Because of the versatile nature of UAVs and the different systems that can be attached to them, there is almost literally an unlimited amount of uses for them. The main addition to a UAV is a camera.

There are many uses for a UAV once it has a camera attached, including (but not limited to):

Facilities Management: exterior building inspections, roof inspections, large interior inspection (think inside of a stadium), landscaping overview/site photography.

Transport: infrastructure inspections, bridges, retaining walls, railways, roads and expansion planning (via aerial maps / images).

Agriculture: standard cameras can be used to view large crops remotely and quickly. UAVs can also be programmed to take repetitive photos to assess crop growth rates and provide a visual indication of their health.

Hyperspectral Imaging cameras can be used to assess the health of crops and to identify anything that might be harmful to plant life. Whilst previously high cost, the ability to mount these cameras onto relatively cheap drones are making them more and more accessible. Pesticide and fertilizer payloads can be delivered via UAVs.



Ross Taylor and David Wright of Tactical Solutions

Search and Rescue: The use of a thermal camera on a drone can vastly decrease the time required to locate a missing persons. The drone could also be equipped with a droppable payload containing vital necessities such as a trauma kit or emergency food and water. Using a drone to clear large areas of open land could also help increase time spent on focus areas. For disaster response, microphones mounted to drones can be used to detect people buried in rubble. Video feed can be used to direct ground forces to those most in need.

Police: Immediate traffic accident evaluation and congestion assessment, crime scene photography, locating missing persons and foot pursuits. Drones are cheaper and potentially far more localised

than police helicopters. STG/AOS use, thermal/regular aerial mapping of compounds, entrance testing and threat identification.

Photography and 3-D mapping: Drones can be used to take photographs and to quickly scan areas and the images be used to create 3D maps.

There will obviously also be people who want drones purely for the science, the tinkering required to build them, or the enjoyment of flying them. It is, after all, marketed as a recreational piece of equipment at the consumer level.

Drones appear to be a mixed bag. What makes for a quality drone solution?

There are a number of different types of drones. The most common being fixed wing planes, helicopters and quad (or more) rotor drones. All of these come in sizes ranging from fighter jets to ones that fit in the palm of your hand. Most consumers in NZ will probably never have the ability to purchase and fly a military grade full sized fixed wing drone. They are cost and law prohibitive. Most will purchase small helicopters and quadcopters for recreational use.

A quality solution once you are purchasing an off the shelf drone is something which is GPS stabilised. This means that a connection to the Global Positioning System keeps the drone as best it can, in the place where you last told it to be.

A GPS stabilised drone will resist wind trying to move it out of place, and are by the far the safest for beginners to use. The most popular of this style of drone are the DJI Phantoms, arguably the most recognisable drones behind military

Predators. Off the shelf micro drones are considered to be toys, and don't have many uses outside of giving the dog something to chase or scaring the cats, for most people.

The other option is to build your own drone. The most powerful and bleeding edge drones will always be produced in this way, however they are not necessarily going to be "quality" as they have not endured the product testing required when a company releases one to the market.

Do we have any reason to fear UAVs? Is it likely we'd see them being used malevolently in NZ?

As with the different quality levels of drones, I think there is nothing to be afraid of at the general consumer level. Micro UAVs and anything without a camera should pose very little threat, and would at most be a nuisance if they were to drop on you or hit your car/house.

Higher consumer level drones pose the ability to invade privacy, as most are now fitted with high-resolution cameras. While most people use them responsibly with no ill intention, it would be foolish to think that everyone is going to behave.

At this higher level of UAVs, there is the potential for payloads to be attached and rigged to drop. This can be beneficial, fertilising a crop, or harmful, dropping contraband into a prison yard.

Hopefully with the work I am doing in investigating prevention solutions there won't be the ability for drones to be used maliciously at critical places across the country (airports, prisons, sensitive locations, etc).

Is legislation keeping pace with the technology and the demand for drones among their varied applications?

I think previously it has lagged behind a lot, but is not doing too badly anymore. As I said at the start, I have focused mainly on the prevention and detection technologies, which come into play when people are ignoring laws in the first place.

Given the extremely varied uses for attachments placed onto drones, I can imagine it is an extremely hard task to keep it all controlled under law. The focus currently, to my knowledge, has been on the flight restrictions, not the attachments themselves.

The Civil Aviation Authority has a good amount of information on their website about UAV flying regulations and an extremely informative FAQ - www.caa.govt.nz/rpas/rpas_faqs.html.



The man who gave us the networked camera

For virtually all individuals and businesses operating in the global security industry today, a networked camera system is ubiquitous. That ubiquity would probably not be as universal as it is without the technological breakthroughs and product advancements of one man and the organisation he co-founded.

Martin Gren, was recently voted as number three in the IFSEC global '50 most influential' in security and fire in 2015.

He took some time out to speak to *New Zealand Security Magazine* (NZSM) on a recent visit to the South Pacific and talk about his company, the future for security technology, some key issues and product development.

Headquartered in Melbourne for the Oceania region, Axis has sales offices across Australia and in Wellington. These locations are not any sort of distribution hub though. Axis prides itself on a unique distribution system based on a 2-tier channel business model. "We never sell direct," Martin tells (NZSM). "We have distributors worldwide that manage our logistics and integrators that make sure the system works."

Mikael Karlsson, Keith Bloodworth and Martin founded Axis Communications in 1984 while Martin was still a student at the University of Lund in Sweden. He has acted as chairman of the board and still sits as a senior board member. He has an impressive background of 31 years of engineering and entrepreneurial experience and has played an important executive role in establishing Axis' products, including IBM-connectivity products, print servers, CD-ROM servers

and camera products in particular the network cameras, with sales of almost 100 percent of the group's turnover. Today Axis has more than 2,200 dedicated employees in more than 40 countries around the world, supported by a network of over 75,000 partners across 179 countries.

While still heavily involved in product development and innovation, ask what Martin's designated role is within the group and he has another of his good natured chuckles. "What do I do? That is a good question. I get it all the time and I never know how to answer. I do a lot of speeches and presentations as well as helping to drive development in the new product section; such as the IP video door station."

Embracing IoT

But back in 1996, he launched the world's first network camera to little fanfare and much market scepticism. Ten years later, it was the fastest growing segment in surveillance and has now surpassed the sales of analogue cameras. It took the security industry nearly a decade to realise the added value of network-connected security and surveillance video products.

Today a large part of Martin's role as an industry leader, innovator and representative is talking about innovations, the future and key issues.



Martin Gren: the man who gave us the networked camera

The top-of-mind topic currently is around why the security sector should embrace the internet of things (IoT) and smarter connectivity.

When international IT security organisation ISACA recently surveyed consumers and professionals about the IoT they found a disconnect. Most consumers aren't worried, ISACA said. It found 64 percent of respondents were confident they could control the security on their own IoT devices. But in a parallel survey, ISACA asked IT security people if they felt sure they could control who had access to data collected by IoT devices in their homes.

The results were flipped: 65 percent said no, they didn't feel confident about that.

Martin and his company were working on IoT long before it was known as such. As is the way of things, he says that what goes around generally comes around and old ideas often resurface in newly imagined ways.

"The concept behind IoT is actually rooted in yesterday's thin client and thin server technologies popular in the mid 1990's. While physical security pundits may wonder how IoT will affect the industry going forward, they only need to look to the past. As more IP-based security devices inevitably replace aging analogue systems, security products manufacturers face the ongoing challenge of helping users integrate the growing wealth of information generated by the IoT into meaningful business intelligence."

Looking Back on a Forward-Thinking Trend

Martin says the framework for designing smart network devices began in 1995. "Back then thin-client technology was a growing trend driven primarily of Oracle and Netscape. It gave companies a way to deliver greater processing power to multiple users by having them share a common high-capacity server. A thin-client solution not only reduced the total cost of ownership for the overall system, relying on a central resource was an easy way to maintain a high level of computational services across the enterprise."

Axis re-imagined that 'thin' concept and invented something they called 'thin server technology'. According to Martin; "Our goal was to make the network smarter so that devices sharing the infrastructure would not only be more economical to own but easier to manage as well. It was a logical next step for broadening our business, which at the time focused solely on print servers – small network-enabled devices that connected printers to networks. Thin server quickly became the framework for developing server apparatus for connecting almost anything to the network – optical storage and home automation systems, even model trains and Christmas tree lights."

But the most important thin server products Axis were developing back then were the networked cameras and video encoders because they eventually reshaped an entire industry. Today tens of millions of network video devices have been installed around the world from a



vast array of manufacturers. Thanks to the networking abilities it became practical to deploy video over larger areas which made city surveillance an affordable application everywhere.

Martin says, "Looking back on the white papers written 20 years ago, I discovered a remarkable similarity between early thin server technology and how IoT is trending today. In hindsight, the millions of print servers we shipped in the late 90s were probably the first IoT devices deployed in volume."

The first network cameras were introduced in 1996 and by 1999 they were embedding LINUX to create an open architecture that would finally make network surveillance devices practical solutions for the security industry. This open approach to system development not only became the Axis business model, it launched an entire network video revolution.

Martin is of the belief that with the excitement around IoT technology heating up, there is an opportunity for security products that can collect and automatically share useful data with other IoT devices. As network-based devices they could be monitored remotely. And the connectivity between devices would provide end users more complete situational awareness across multiple locations.

"To that end comes IP-enabled access control system that could transform a door into an intelligent IoT device. With its IoT ability, the network door controller can be configured for a cloud environment where access control becomes part of a hosted system.

This operating model is particularly suitable for environments with many remote doors that need the added security of integrated video. The network door controller capitalises on the benefits of 'Power over Ethernet' to decrease installation costs and increase system reliability. Overall, an IP-based door controller is less complicated to maintain, offers greater flexibility and scalability and a lower total cost of ownership than its analogue counterpart.

To augment the cameras and network door controllers accessory and enhancement devices such as IP speakers and horns can be added. Being yet another IoT device, for example, the horn speaker can be triggered automatically by video motion detection and intrusion sensors to play a pre-recorded audio message which can be useful for preventing graffiti or keeping parks empty at night.

When integrated with a video management system, a remote operator can even speak directly to any intruders saving cities lots of money. Because of the IoT capabilities and industry open

standards, it easily integrates with other open standards IoT device. Best of all, with speakers that supports SIP can be assigned a regular phone number like any other VoIP telephony device.”

Other technology game changers for IoT

While basing IoT devices on open standards has certainly changed the physical security landscape, Martin says that one of the biggest game changers when it comes to system costs has been Power over Ethernet. Being able to use the same cable to both power the IoT device and transmit data has significantly reduced installation costs by decreasing the amount of cabling needed for the project and shortening the amount of man-hours needed to install devices.

“With PoE there is no need to home run expensive coaxial cables to a recording device or a security monitoring centre as you would with analogue video cameras, card key systems and intercoms. With PoE in the network topology you just run a single cable from the IoT device to a centralized PoE switch. The PoE switch runs a single cable back to the recording device or security centre to stream the data from all its connected IoT devices.

“Another significant game changer has obviously been cloud-connected services. As network-based technology IoT devices are excellent candidates for managed services. The only up-front investments end users have are the IoT devices themselves. The service provider handles

the rest of the system – data storage, a secure web portal for user access, system upgrades, authorised user directories, ongoing maintenance, etc. – for a fixed monthly fee.”

IoT is everywhere

IoT has certainly proliferated in the consumer world. Smart thermostats send homeowners alerts while they are away on vacation. Nanny-cams let parents keep an eye on their children while still at work. There are even smart refrigerators that automatically order groceries for the household when supplies run low.

Martin says, “In the security world, IoT is helping businesses manage all their security systems – from intrusion sensors and fire alarms to video surveillance, access control, loudspeakers, emergency stations and video intercoms – as a single cohesive platform. IoT monitoring devices are even being linked to environmental controls to ensure that a building’s HVAC systems operate within set parameters.”

Compression technology in video surveillance applications

With the mounting plethora of network cameras come other technological issues. Martin says Axis is heavily involved in the development of better image quality, multiple image sensors in the one device and multi directional capability.

“With all this collection, storage and transportation of data and the addition of more and more devices, new compression technologies have been vital.”

Axis has developed Zipstream technology allowing customers to benefit from reduced bandwidth and storage requirements without having to invest in new cameras or software. Zipstream is fully compatible with the widely adopted H.264 compression standard. The technology has been developed specifically for video surveillance applications and lowers bandwidth and storage requirements by an average 50 percent or more.

“Significant progress towards better image quality with higher HDTV resolutions and increased low-light performance has also increased the requirements on the network and storage infrastructure. With Axis’ Zipstream technology we enable our customers to drastically reduce bandwidth and storage needs without compromising on important image details. For example, more than twice the video footage can now be stored on SD cards or NAS’s in small systems built on AXIS Camera Companion as well as other edge recording applications.”

This technology analyses and optimises the network camera’s video stream in real time. Scenes containing interesting details are recorded in full image quality and resolution while other areas are filtered out, to optimally use available bandwidth and storage. Important forensic details like faces, tattoos or license plates are isolated and preserved, while irrelevant areas such as white walls, lawns and vegetation are sacrificed by smoothing in order to achieve the better storage savings. Customers can use Axis’ Zipstream technology alongside other Axis network camera technologies such as Wide Dynamic Range - Forensic Capture and Lightfinder.

The development and growth doesn’t stop for Martin Gren and his team. “Today, we’re focusing on a new wave of innovation. We’re continuously making advances in light sensitivity, dynamics, colour reproduction and resolution in our network cameras. Beyond that, we’re also successfully moving into new markets, such as access control. We’re driven by our vision to come up with new, innovative, smart solutions that meet user needs – and we’ll expand our portfolio to keep achieving that.”

Embracing IoT with safety

The Information Systems Audit and Control Association (ISACA) has highlighted some ways security professionals can advise clients to safely embrace IoT devices in the workplace to keep competitive advantage without becoming susceptible to breaches:

- Ensure all workplace devices owned by organisation are updated regularly with security upgrades.
- Require all devices be wirelessly connected through the workplace guest network, rather than internal network.
- Provide cyber security training for all employees to demonstrate their awareness of best practices of cyber security and the different types of cyber attacks.

When it comes to manufacturers of IoT devices, ISACA says there are various best practices to abide by:

- Require all developers who build software to have appropriate performance-based cyber security certification, to ensure safe coding practices are being followed.
- Insist all social media sharing be opt-in.
- Encrypt all sensitive information, especially when connecting to bluetooth-enabled devices.
- Build IoT devices that can be automatically updated with new security upgrades.





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

Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

Your FSH Electric Locking
range includes...

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



MEM2400LP



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

MEM2400LED-LZ

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

FES20M



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

FES 10 and FES 10M



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

VE1260



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

FEL990M



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

Loktronic

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

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

Facilities Integrate Expo here to stay

October-November has been conference season in Auckland, with NZSA's New Zealand Security Conference and Expo, the New Zealand Risk Management Leaders Forum, and newcomer, Facilities Integrate 2015, all vying for our attention. Held at ASB Showgrounds on 15 and 16 October, this latest entrant appears to have had a successful first outing despite the congestion.

Billed as providing a unique showcase for businesses that operate, maintain, and upgrade buildings, facilities, and infrastructure, or design, install, and integrate AV and ICT systems, the show was a promotional platform for the industry focused on making commercial buildings more intelligent and efficient.

According to Dona White, CEO of organiser North Port Events, the show is based on an overseas concept that's growing. Although there are separate Integrate and Total Facilities expos across the Tasman, North Port went for a combined approach. "We also felt," said Dona, "that with all the money going into commercial refurbishments, building and infrastructure, that this is right and these two groups fit really nicely together."

Supporting the event were a number of industry players, including the Facilities Management Association of NZ (FMANZ), Energy Management Association of NZ (EMANZ), Building Services Contractors (BSC), KNX and ASIS.

A first-year success

According to Dona, the expo hit the mark, meaning it won't be a one hit wonder. In fact, organisers were overwhelmed by the response. "We had a personal goal of having a thousand of the right people a day in year one," she stated, "... and we succeeded in that."



Dona White speaking at the Facilities Integrate 2015

"By and large we judge the success of the show on whether we get a re-sign, and we've had about 50% re-sign, with everybody enlarging their stands. We feel really positive about it."

Although they're satisfied they delivered value to their support associations and exhibitors, the organisers identified some gaps that they'll be looking to fill for next year. They got some architects through the door this time around, but there's plenty of work to do to get more through next time. Also, despite having ASIS on board as a supporter, the expo had been unable to secure support from the NZSA.

Interest from the security industry

"Of all the groups that attended the show we had really positive feedback from the security industry," stated Dona. The lack of interest from NZSA, therefore, seemed something of an irony.

With little more than a month separating Facilities Integrate and the

Security Conference, there was concern that the former might take away from the latter. Nevertheless, she remains hopeful. "We'd love to work with them... and I will be reaching out to them again to see if we can collaborate next year."

What can we expect next year?

North Port is aiming for plenty more content in next year's show, potentially involving some accreditation and learning. According to Dona, this is especially important for the architects, whose participation is in turn important for the integrate side of things. "For all sectors, to make the show compelling it's all about the content and having things that people are really wanting to see."

"We haven't had the post show survey yet, so we'll see what that comes back with," she suggests, though feedback to date points to the need to be pulling more interest from the South Island. A targeted buyers program, or perhaps an awards function or an international speaker might be on the horizon.



Panel discussion on “Facilities management and integration in the design process”, which featured Martin Leitch, Richard Harris, Mark Sinclair, Stephan Goodhue, Glen Gordon and Charles O'Donnell.

Messages for potential exhibitors

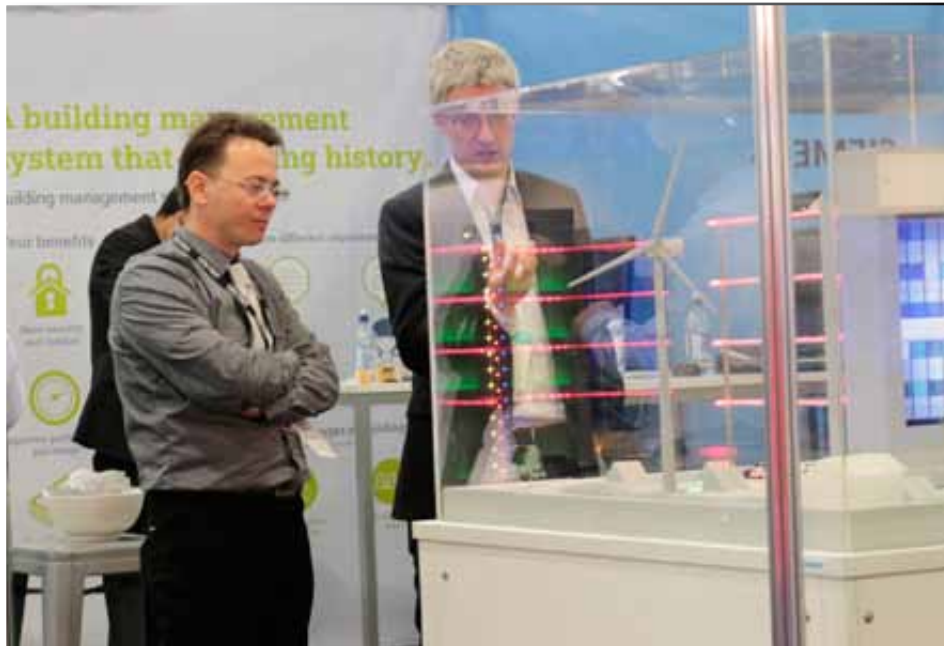
Dona suggests to keep an eye on the Facilities Intergrate website. “We’ll be sending out details soon of the results of the survey, and that will have information about what kind of business is done. Our thing is showing your product three dimensionally. We are masters of the PR that goes around it.”

“It’s the one time a year you can show your product three dimensionally. You can demonstrate face to face with your exact target audience. It’s really great for lead generation; it makes the difference. We’re the face-to-face – or experiential – component.”

With \$10 billion worth of new projects in construction and refurbishment currently planned for

Auckland, and 142 projects valued at 570 million going on in Christchurch, there are compelling numbers for this kind of show. Construction is set to continue well into the future with Auckland’s population tipped to grow by 30% over the next 10 years.

Added to this, states Dona, is the fact that facilities management is now seen as a strategic function rather than as a reactive one, and facilities and building management are becoming increasingly professionalised. “We’ve got a really good window for this of 10 to 15 years. We may find that facilities will ultimately sit on its own and integrate will sit on its own, but right now they sit really nicely together and they’re really happy with each other.”



Siemens stand Facilities Intergrate 2015

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 Cresent, 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

The challenge of integrating security and facilities management within an organisation

One of the highlights of the Facilities Integrate 2015 expert seminar program was a talk by Charles O'Donnell of ASIS New Zealand on "Current developments in the security industry of relevance to facilities managers".

Charles' talk covered the changes taking place within organisations that are shifting the operational responsibilities between security and facilities management, as well as technical issues, including integration, the importance of product selection and the need for professional engineering oversight.

Charles is principal consultant and company director at RISQ New Zealand Ltd. With a total of 29 years security industry experience here and in Australia, he has worked for multinational corporates including IBM, Westpac and the National Bank of New Zealand. He has also held the position of Departmental Security Officer for The Treasury.

Changing organisations

"If you walked into any corporate environment today, you'll have a security manager who sits somewhere down the middle of the food chain, and they'll report to somebody in audit, risk, HR, legal, and quite often finance. They're pretty much a one-man band with one system." This, according to Charles, describes where the security manager sits... but it's changing, and changing rapidly.

"Although the responsibility for traditional security functions lies with the security manager, constraints in resources and budgets mean that we're having to do more with less," he says. This has led to facilities managers taking over a number of operational security responsibilities. Systems and security guards are thus increasingly being managed by facilities managers, property managers and even outsourced providers.

This means that much of the ongoing work is managed by the facilities manager, leaving the reporting, risk assessments and all the governance aspects to the security manager. It's already happening in the

commercial property space, he says, "and it's seen as being an economically feasible way of running security."

According to Charles, this is a good thing. "But the question that arises is are those people equipped and have the experience to actually deploy the security skills required to mitigate the security risks that an organisation may encounter? And who determines those risks and how?" It's a bit of a science, he says, and it requires experienced people to do it.

Given that risk is mitigated to the level that it is assessed, problems can arise when those managing risk don't actually understand it. "If people are securing buildings without that knowledge," Charles warns, "they may be over-securing them, they may be spending too much money, and they may not be getting value for their."

Timely mitigations and treatments to identify security gaps and prevent incidents need to be instigated on a prioritised and risk assessment basis. "You really need to understand your business, understand your priorities and justify your expense," he points out. "Are those the types of skills that our facilities managers have today to take over some of the security parts of the business? I put it to you that it is questionable."

A good fit – doing what we're good at

Whatever questions are being posed by these changes, Charles, sees the idea of facilities people taking over security services as making good sense. Security managers, he says, should focus on their core security activities, risk assessments, procedures and so on, and "let the experts in security systems deal with security systems."

In doing so, we now have a facilities area that has security obligations. "And what we put on them is the management of our operational security resources and our systems, our security guards, our access control systems, our camera systems and our alarm systems," he explains. "Essentially we're giving them



Charles O'Donnell is principal consultant and company director at RISQ New Zealand Ltd and a member of ASIS New Zealand

the key to the building so that they can manage it on behalf of the security department."

While this means some shedding of operational security responsibilities away from the core security function, organisations need to ensure that they approach this judiciously.

"If responsibility for security strategy and the development of a security culture and implementation of security training and awareness is placed into a facilities department, are they necessarily equipped and skilled to take you through that security strategy and implement the security program? Unlikely."

In the integrated model, the organisation should expect more than ever its security managers to develop and articulate security and risk management strategies. The organization should also ensure that its security managers maintain an accountable role in working with relevant business units to achieve the best operational security solutions.

"Security is no longer a clandestine unit sitting on the 12th floor behind mahogany doors," says Charles, "it's now an open and transparent organization that

is out there in the business, understanding the business, working with the business and working with the facilities management team to ensure that the operational services are being looked after.”

The challenge today, says Charles, is how do we take the traditional security knowledge to the facilities team? Collaboration, he points out, is key. It’s about working together and working as a team instead of consistently locking horns with each other trying to get a dollar for it.”

Managing procurements and lifecycles

The collaborative approach Charles suggests is one in which although facilities managers may be responsible for systems, security managers must help to develop the systems and specifications based on predetermined security standards. Decisions around procurement and product selection should never be unilateral.

It takes a collaborative approach to identify a suitable plan for capital, operational funding, and servicing of assets, and to look at what he refers to as “the lifecycle management of the security program”.

“It used to be 20 or 25 years ago that you could stick a security panel on a wall and walk away and leave it... your investment in security might have been 10K in 1990, and today

if your wanting to replace that same panel your investment is going to be significantly higher.” This is, as Charles is quick to point out, far from the truth these days.

“Those involved in systems, systems development or IT will know that a security product these days is a piece of IT equipment. It is depreciating and its lifespan is 3-4 years.”

Nevertheless, he suggests that there are many buildings in New Zealand that still run old security systems, which are not necessarily performing in terms of meeting today’s business needs, today’s risks and what today’s market can provide.

“At the end of the day it’s about managing that lifecycle, and I believe that facilities managers are extremely good at that function. They’re dealing with equipment and kit every day and they want to get the best performance out of it, but they’re also wanting to make sure that that performance and maintenance of that product is not costing a lot of money.”

The moral of the story? The integration of security and facilities management functions within organisations is happening, and it will continue to happen. How successful an organisation is at integrating these functions will depend on the extent to which it recognises the specific skills sets of each side of the equation – and the extent to which each side communicates and collaborates to ensure that facilities – and the people that work in them – are kept safe and secure.

Australia Round-up

Spectators and security guards brawl at A-League game

NSW Police were investigating a fight between soccer fans and a security guard during the tail end of the Newcastle Jets’ 2-1 loss to the Western Sydney Wanderers on Saturday 07 November.

Mobile phone footage shot from within Hunter Stadium shows a security guard pushing a white shirted spectator away from a section reserved for Wanderers’ fans, reported the Newcastle Herald. The security guard is then seen punching the man, hitting him on the left side of the face.

A black shirted spectator is then filmed leaping on top of the scuffling pair, attempting to bring the security guard to the ground. As this man and the security guard exchange

unpleasantries on the ground, the security guard appears to throw a series of punches.

The man in the white shirt then lands a number of punches on the guard’s head, causing a cut under his eye. Several more guards then converge on the scene in an attempt to defuse the situation, and the man in the white shirt is dragged away by headlock.

According to Police, a total of six people were ejected from the stadium during the game, including the two men involved in the scuffle. They were both issued with a ‘failing to quit a venue’ and one issued with an infringement notice for offensive language. Police were reviewing CCTV and mobile phone footage as part of their inquiries.

New gun laws pass NSW Parliament

Laws introducing tougher penalties to target the illegal firearm trade passed the NSW Parliament on 17 November.

Deputy Premier and Minister for Police and Justice Troy Grant said the Firearms and Weapons Prohibition Legislation Amendment Act 2015 will deliver on a commitment by the NSW Government to crack down on those who endanger the community.

“These laws have a clear focus of hitting the illegal firearms trade because it’s clear the illegal gun market presents the threat to the community,” Mr Grant said. “This means tough new 14-year penalties for a range of illegal firearm offences, including a new offence of possessing a stolen firearm.”

The laws create a new offence for the possession of a stolen

firearm, which will carry a maximum penalty of 14 years’ imprisonment. They also increase the maximum penalty for defacing or altering any identifying mark on any firearm or firearm part, or for possessing a defaced or altered firearm or firearm part, from five years to 14 years’ imprisonment.

Consistent maximum penalties of 14 years’ imprisonment will apply to a range of other offences relating to unauthorised possession, use, supply, or acquisition of firearms where the firearm involved is a pistol, a prohibited firearm, or is defaced, unregistered or stolen.

The laws also ban possession of digital blueprints that enable firearms to be manufactured using 3D printers and milling machines for anyone without an appropriate licence.

Big increase in counter-terror unit interventions

According to a 20 November press release from the Minister for Immigration and Border Protection Peter Dutton, there's been a significant increase in the number of interventions Counter-Terrorism Units are making at Australia's international airports.

Since July, 199 passengers have been offloaded from flights by CTU officers for national security reasons, concerns about their intended travel destination or other suspicious behaviour – a significant increase in total offloads.

The CTU program is part of the Government's \$630 million funding package for agencies involved in counter-terrorism activities. Mr Dutton said that since the CTUs began operating at airports in August 2014 there had been a total of 535 passenger offloads, 194,660 real time assessments nationally and more than 13,000 patrols.

"Maintaining strong security at our borders is critically important in stopping those with evil intent or impressionable

young people who have fallen prey to terrorist propaganda from leaving Australia to join murderous terror groups like Islamic State," said the minister.

"Many passengers subject to offload are able to continue their journey at a later time, but a significant number of people of national security concern have been detected during the CTU offload process.

"Much of the work these units do cannot be made public, but the instance of five young men prevented from travelling to the Middle East revealed in August this year is not an isolated case," he said.

"Recently Australian Border Force officers formed a suspicion that a minor was potentially travelling to join conflicts in the Middle East. After questioning and an examination of his baggage he was prevented from travelling and referred to other agencies for investigation. Again this is not an isolated incident."

Australia loses ground in ASPI 2015 cyber maturity report

Australia scored 79.9 out of 100 in the Australian Strategic Policy Institute's recent report, while the US was rated at 90.7. Despite a third ranking in 2014, Australia has now been pushed down to fifth, with the US, Japan and South Korea leading the way.

According to the report, Australia has a well-established legal framework that continues to be adjusted in response to contemporary cyber issues. It has also sustained its role as a regional leader in multilateral forums on cyber security, and interacts with Australian businesses through the expansion of a reciprocal cyber-dialogue.

There remains, however, "a paucity of coherent national cyber policy", states the report, although this would likely improve if the Australian Government delivers and implements its promised Cyber Strategy. The areas where Australia received its lowest scores were in the areas of governance, military and business:

Governance: at the official opening of the Australian Cyber Security Centre in November 2014, the then Prime Minister Tony Abbott announced a review Australia's cyber security strategy, but "it's yet to be seen what the review will deliver and what changes will be implemented as a result." Australia's score, suggests the report, could improve with the release of the strategy.

Defence: the Defence Department, states the report, "struggles to engage beyond traditional intelligence partners on cyber security issues". Australia's score could improve with further clarification of the ADF's roles and responsibilities.

Business: as part of its cyber security review, the Government has engaged strongly with the business community. Beyond this, there's sustained two-way dialogue between government and key sectors such as banking, telecommunications and CNI, although, argues the report, this could be deepened and widened to incorporate more sectors.

YPB Group Limited wins ePassport contract

Australian listed brand protection solutions company YPB Group Limited has been contracted to provide its proprietary VariSec technology to a significant Southern African country. This follows YPB's recent contracting by a major first world economy to supply the VariSec technology for application in 15 million ePassports.

The technology was developed by YPB's recently acquired subsidiary Intellectual Product Protection (IPP), and the recent contract win is seen as strong validation of the purchase. It also substantially increases YPB's penetration into the area of ePassport security.

The VariSec technology can be customised or individualised to suit different government's uses and specifications. "We are building momentum in government document security as

evidenced by these orders in recent weeks," commented YPB CEO and Executive Chairman John Houston.

"As previously stated this is an excellent opportunity for YPB to gain increased exposure to government agencies for our entire suite of anti-counterfeiting solutions. We are continuing to develop products that will assist governments and businesses and these recent deals for VariSec are a great advertisement for us that should lead to wider acceptance of our solutions."

ICAO's Technical Advisory Group on machine-readable travel documents (MRTD) published an information paper in January 2013 on ePassports worldwide disclosing that 101 states and economies issue ePassports; an estimated 489,522,100 ePassports have been issued worldwide; and an estimated 483,929,100 ePassports are currently in circulation.

Experts point to payment systems threats in 2016

Among the 14 key areas of threat identified in Intel Security's recently released 2016 Threat Predictions report was that of payment systems, and in particular the proliferating scourge of online credentials theft.

The report, published by McAfee – now part of Intel – listed payment systems along with cloud services, wearables, automobiles, hactivism and ransomware as an area under threat over the next 12 months. A skewed focus on card transactions and the rise of alternate payment methods, says the report, have left many companies napping.

New systems, new avenues for theft

According to the report, we continue to place a significant security focus on vulnerabilities associated with credit and debit card transactions. This makes sense given that most digital transactions use these forms of payment, although there's been little change in relation to how these vulnerabilities are exploited.

"Most attacks approach payment card theft in the same way they have for the past 10 years," it states, "by attacking payment mechanisms or the databases containing card data." Once attackers have obtained the card data, they sell it on as quickly as they can.

"Today, the number of alternate payment methods is rather dizzying," the report observes, "from Bitcoins, ApplePay, credit cards, and debit cards, to online payment services." This growth in alternate payment methods means that the number attack surfaces have multiplied, increasing the number of possible targets open to cyber thieves.

"Given the plethora of payment methods, most of which still require usernames and passwords, credentials have become very valuable," it says. To steal credentials, the cybercriminals are targeting the consumers directly because they are "both the source of the credentials and the weakest link in the payment process."

Intel predicts that in 2016, payment system cybercriminals will increasingly focus their energies on stealing credentials from consumers. "We think that they will leverage traditional, time-proven mechanisms including phishing attacks and keystroke loggers, but new methods will emerge too."

ATMs, POS and mobile payments at risk

In its 2016 Security Predictions: The Fine Line report, Trend Micro suggests that it will be in the mobile space where payments are most exposed. Trend Micro states that next generation payment methods will "pique the interest of online criminals from EMV credit cards to mobile wallets, challenging supposed 'safer' payment platforms." Mobile malware is expected to grow "given the lax user behaviour and the availability of third-party app stores in China."

In its 2016 predictions, the Kaspersky Security Bulletin highlights the many examples of attacks on point-of-sale systems and ATMs over the past year, including the Carbanak heist that pilfered up to one billion US dollars during a two-year period. A multinational gang of cybercriminals from Russia, Ukraine and other parts of Europe, and China was allegedly responsible for the crime.

"In the same vein," says the Kaspersky report, "we expect cybercriminals to set their sights on novelties like alternate payment systems (ApplePay and AndroidPay) whose increasing rate of adoption should offer a new means of immediate monetization."

Remove enrolment from the equation?

PwC's Global State of Information Survey 2016 points out that there are lessons to be learnt from the roll out of ApplePay and similar services. Some of the initial challenges of Apple Pay, it suggests, weren't necessarily issues with the security of the phone or the credentials, but rather the process around enrolment.

"When you have these new payment models, you have to look at the end-to-end lifecycle of enrolling a user, transactions that flow through the system and de-enrolling users," Joe LoBianco of CIBC stated in the report. "When there are new processes, the bad guys will try to exploit human weaknesses just as much as technological weaknesses."

The transmission of tokens to merchant systems is one approach that the survey considers to be fundamentally secure because it avoids the need to store and transmit credit card information. While this may be the case, it suggests that completely removing the payment process from the user experience is the ideal end state.

In this regard, it quotes Guido Sacchi of Global Payments as citing the seamless process used by ride-hailing service Uber – where the merchant uses a payment card on file, and customers' cards are automatically billed. "If there is one thing that is a takeaway from all this," says Sacchi, "it's that you need to look at both security and user experience. The winners in the market place are going to be those that strike the best balance between the two."

Picking up on these pressing themes, the annual Payment Security Summit will take place on 26 and 27 April 2016 in London. The summit will bring together the entire payments ecosystem to showcase the range of tools and avenues for addressing cyber security threats specifically in the emerging and alternative payment markets.

The amount of reporting and information being produced internationally about these emerging issues reflect disquiet in relation to the extent to which criminals are exploiting new payment technologies ahead of the identification of adequate security countermeasures. As more new payment platforms emerge, it appears that fortune will most likely continue to favour the cautious.



Power supply cabinets

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

Designed, tested and produced in New Zealand.

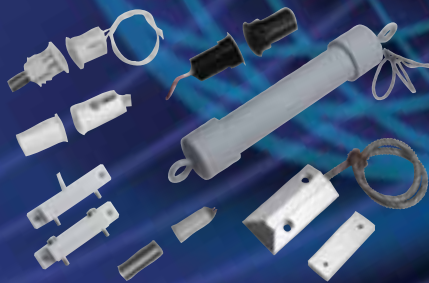


Loktronic



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

20238_PSC



total reed switch solutions from Flair

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

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

Flair reeds from Loktronic: an unbeatable combination.

Loktronic



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

20237_FL



Loktronic for power supplies

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

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

Power supplies from Loktronic – a great deal.

Loktronic



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

20757_BP



ITRON SECURITY & AUTOMATION



Loktronic for gate locks

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

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

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

Gate locks from Loktronic – a wise choice.



Loktronic



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

20756_BP



Key switches

This versatile product range is produced with two functions

Momentary contact (90°)

Turns 90° clockwise from vertical to turn on

Maintained contact (180°) locked on or locked off

Turns 90° clockwise from vertical to turn on

Turns 90° anticlockwise from vertical to turn off

SPDT switch 5amp rating

Accessories are: Key switch mounting bracket
escutcheon for mounting bracket

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

Supplied random keyed. Can be master keyed.

Client's own key cylinder can be converted.

Front or rear fixing.

Designed, tested and produced in New Zealand by Loktronic.



Loktronic



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

20681_KS

Loktronic Power distribution module



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

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

Comprises

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

Designed, tested and produced in New Zealand.



Loktronic



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

20239_PDM

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



Panasonic

**HD
CCTV**

**Exmor
CMOS Sensor**

HDCVI

(09) 414 5101 OR 0800 ITRONICS

SALES@ITRON.CO.NZ

WWW.ITRON.NZ

**UBIQUITI
NETWORKS**



Wireless IP Surveillance

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

Distributed by

ITPLUS
SECURITY TECHNOLOGY

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

**dahua
TECHNOLOGY**



Customized CCTV Kits

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

Distributed by

ITPLUS
SECURITY TECHNOLOGY

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

axxonext
www.axxonext.com



Open Platform VMS

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

Distributed by

ITPLUS
SECURITY TECHNOLOGY

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

Paris attacks: NZ businesses need to 'join up' to be resilient to threats

The recent terror attacks in Paris, security responses by authorities in Belgium and blanket adverse international travel advice by the US government to its citizens have again heightened the spectre of indiscriminate terrorism. Although New Zealand is far removed from traditional theatres of terrorism, extreme events expert and Auckland University lecturer Dr Brigitte Sullivan-Taylor suggests that we're not as removed as we might think.

Dr Sullivan-Taylor, who has recently fielded New Zealand Herald and television media questions on terrorism resilience following the events in Paris, notes that the frequency of such events has increased, "and that's probably concerning in itself."

According to Sullivan-Taylor, "the American response is showing how interconnected we all are. They're not in France or Belgium but they are clearly concerned." This poses questions around what risk managers and business continuity specialists in New Zealand's private sector – and those with civil defence and emergency services responsibilities in the public sector – should be doing.

Dr Sullivan Taylor acknowledges the very effective work done by authorities in New Zealand to raise natural disaster awareness, but believes that the time has come to be thinking about broadening it out to other types of extreme events.

"Essential government campaigns and support has been there for earthquakes, resulting in high profile awareness," she says. This assists in communities becoming more aware of what to look out for and what to do in the case of an event and – essentially – to operate in a more 'joined up' way. "In the case

of earthquakes the focus is the local community, but [for other events, such as attacks] the business community within an immediate geographical area is important."

Identifying vulnerabilities and who is important in the case of an event is key. In the UK, says Sullivan-Taylor, local councils joined with private sector and CNI organisations to work through exercises to achieve coordination and agreement on specific roles. Additionally, a risk register for each city – accessible via the web – informed these exercises, making them location-targeted.

"A similar approach could be applicable here," she suggests, "because in different regions there would be different risks, such as flooding, earthquakes, biohazards, etc."

But identifying who might lead this joined up approach is the challenge. In the UK it's the Civil Contingencies Secretariat that performs a leadership role, and in the US it's the Department of Homeland Security. In New Zealand, Sullivan-Taylor suggests that it is also the case that the responsibility best resides with government.

The private sector, she observes, already understands and engages with risk and business continuity planning, but the focus tends to be internal. In order to work towards a 'joined up' approach, risk and continuity managers need to be looking beyond the company to their "wider supply chain and corporate partners and neighbours."

A good start would be to consider whether your business exists within a multi-tenanted building context, and the extent to which you coordinate and joint-plan with other security and facilities managers within your building. At the



Extreme events expert and Auckland University lecturer Dr Brigitte Sullivan-Taylor

next level, is the building management 'joining up' with their counterparts in neighbouring buildings? To what extent does your local Chamber of Commerce or business association promote locality-based resilience and business continuity programs?

Dr Sullivan-Taylor is leading an International Comparative Study into extreme events best practice at Auckland University, partnering with the Aston and Warwick Business Schools in the UK. Given that it was private sector business continuity and risk professionals who informed the UK study, she is looking for participants from within the NZ private sector to make the project work. If you are interested in participating, please contact her at Auckland University or email b.sullivan-taylor@auckland.ac.nz.

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 • Cobalt 90 & 180 degree Locks • Effeff Electric Strikes • Egress Buttons
• Flair Reed Switches • FSH Electric Mortice Locks, accessories and furniture • FSH Electric Strikes
• FSH Electromagnetic Locks • FSH VE Locks • Haze Batteries • Lockwood Electric Mortice Locks, accessories and furniture • Loktrenz, Abloy, Effeff & IR Power Transfers • Loktrenz Electromagnetic Locks • Loktronic and Trencab Key Switches • Loktronic, Loktrenz, Cisa, Effeff and Securitron Gate Locks • Loktronic Power Distribution Modules • Loktronic Power Supply Cabinets • Meanwell Power Supplies • Powerbox Power Supplies • Prastel Door Controllers • Roller Door Locks • Rosslare Keypads • STI Call Points • STI Secure Housings for Keypads, Fire Alarms and Exit Devices • Trimec Drop Bolts • Trimec Electric Strikes • Trimec V-Locks • Trojan Em Rex & Prox Rex Devices • Trojan Relays • 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**

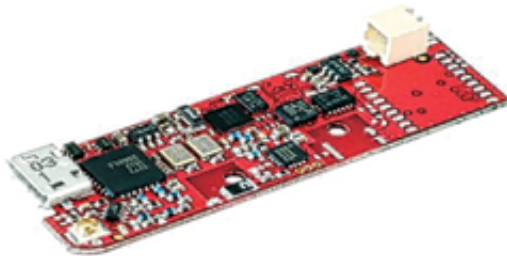
Loktronic

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



KCS TraceME

KCS TraceME TM-900 / N1C1 GPS/RF-module / OEM-version



The TM-900 / N1C1 is a budget product line member of KCS' advanced TraceME track and trace modules. The TM-900 is targeted for remotely tracking and tracing a variety of objects, even livestock, and for personal use.

The TM-900 offers excellent long range RF coverage and is equipped with a low-power GPS receiver.

The module is equipped with multiple on-board sensors, low-level I/O-connectivity and a solar (*) rechargeable integrated battery. It offers accurate location based position data to be connected to any existing worldwide server application.

Key Features

- Excellent satellite coverage
 - GPS
 - Glonass/GPS (*)
- Very small, only 49.6 x 15mm
- Lightweight: 3.4 grams for a fully equipped PCB
- Standby battery lifespan of more than 10 years.
- OEM version
- Excellent GPS accuracy, internal antenna.
- Integrated 2.45GHz. radio for special functions and peripherals.
 - Short range, up to 30m (*)
 - Long range, over 1 km range, line of sight
- LoRa™ technology, up to 10km, line of sight
- Excellent indoor and outdoor performance with accuracy up to 1.5m
- 3 LEDs for user interaction.
- 1 switch for user interaction.
- Onboard sensors:
 - Temperature sensor ($\pm 0.5^{\circ}\text{C}$)
 - 3D accelerometer up to 16g.
 - Humidity sensor (*)
- Wide operating range: $-20^{\circ}\text{C} \dots +85^{\circ}\text{C}$
- Multiple watchdog levels for maximum stability.
- Solar cell powered (*)
- Versatile interfacing:
 - Digital I/O
 - Serial, 3V
 - iButton™ / 1-Wire™
- Buzzer
- Event based free configurable module to fit any job.
- Remote maintenance. Both firmware and configuration files can be updated over the air.
- Runs local user scripts via .src files.
- Supports integration into third party networks.

Applications

- Object protection, up to 10 years of standby on a single lithium AAA-battery.
- Logistics, M2M
- Animal tracking, asset monitoring
- Security and surveillance
- Remote control and diagnostics
- Anti-theft

www.Trace.ME

(*) Optional, please contact sales for more details.

All trademarks mentioned herein belong to their respective owners.