

December 2013/January 2014

ISSN 1175/2149

NZSecurity

A Trusted source of information for industry professionals

Professionalism
Key to improving reputation
Retail Security
Brand Security
Showdown over fire
levy freeloaders

www.NewZealandSecurity.co.nz

He's not the only one with
superior night vision.

Introducing Bosch Starlight HD cameras.



Be wise and choose the most light-sensitive HD cameras on the market.

The new DINION starlight HD 720P and FLEXIDOME starlight HD 720p RD/VR are the next real breakthrough in HD security. In poor light these amazing HD cameras deliver a clear colour image where others show only black and white. And in extreme low-light they deliver a black and white image where

others show no image at all! Add the Bosch Video Security app and overcome the bandwidth barrier so you can view HD images from anywhere. See video security in a new light at www.boschsecurity.com.au



BOSCH

Invented for life

ZoneTechnology
Your Security Supply Partner

Email: sales@zonetechnology.co.nz
Web: www.zonetechnology.co.nz

Auckland
Unit 6, 25 Airborne Road
Albany, Auckland
Ph: 09 415 1500

Wellington
35 Abel Smith Street
Wellington
Ph: 04 803 3110

Christchurch
Ph: 03 365 1050

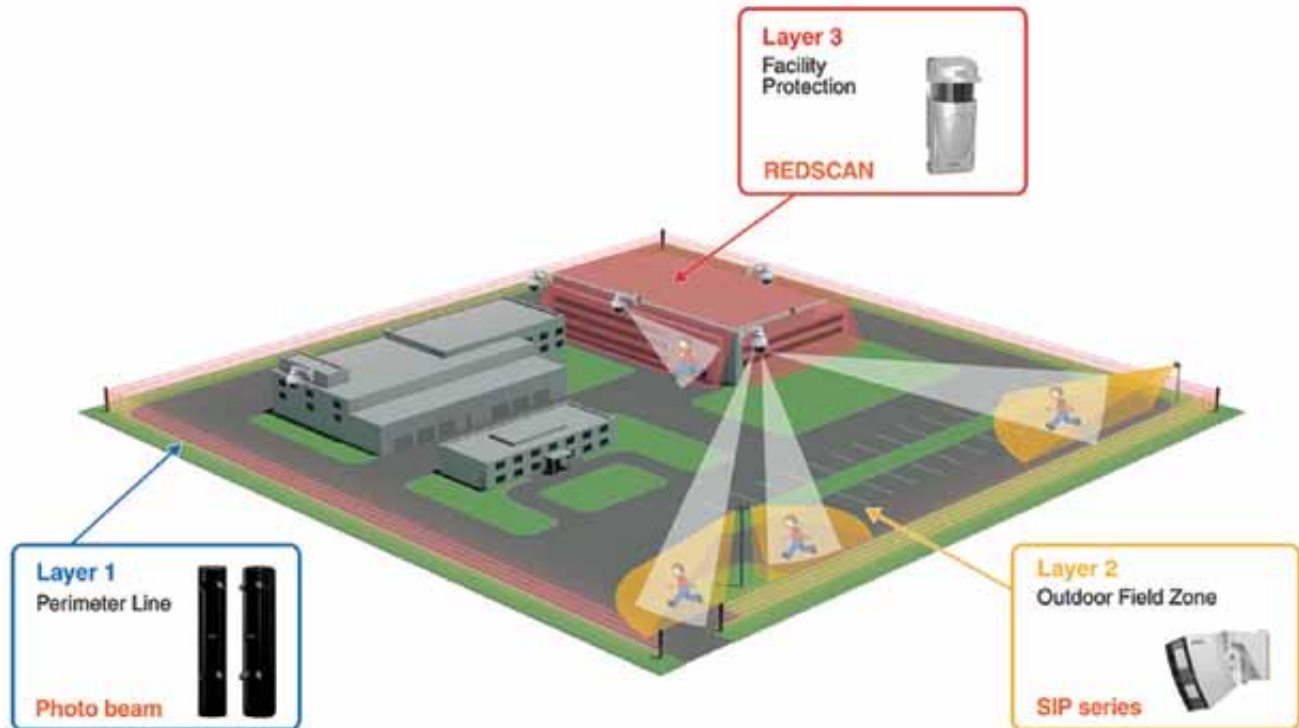
Strengthen CCTV Security with area/barrier detection



Quality detection system for video surveillance

REDWALL®
Unrivalled performance

IP DETECTORS



MULTI-LAYERED PROTECTION SYSTEMS

Redwall IP detectors from Optex are specifically designed for professional video surveillance and offer a complete detection solution for various external perimeter security systems integrated with IP CCTV products. Redwall IP detectors can be connected via Power-Over-Ethernet which allows a powerful “Multi layered protection system.”

KEY BENEFITS:

- Complex virtual wall, fence, ceiling and area protection zones
- Increased reliability of detection
- Vertical protection where cameras cannot work
- Highly reliable sophisticated laser and synthesized
- Intelligent PIR multi-sensor technologies



Available at

For enquiries call your nearest Hillsec branch.



AUCKLAND
Penrose 09 525 8007

CHRISTCHURCH
Sydenham 03 374 6277

WELLINGTON
Petone, Lower Hutt 04 939 9355

www.hillsec.co.nz

Contact Details

Craig Flint

Telephone: (64) 07 868 2703

Mobile: +64 (0) 274 597 621

Postal and delivery address:

27 West Crescent

Te Puru 3575

RD5

Thames

New Zealand

All enquiries to

craig@newzealandsecurity.co.nz

Editorial contributions welcome.

February/March 2014

Building and Construction,
Consultants, Electricians, CCTV
Installers, Architects, Engineers &
Estimators

April/May 2014

All Government Departments,
Access Management, IT Security,
Transport, Tourism

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.

ENJOY a **10** year
guarantee

on Loktronic Indoor
Electromagnetic Locks!

Loktronic

0800 367 565
www.loktronic.co.nz

CONTENTS

Security

- 6 Intek Security Group
- 8 Professionalism of Security Guards
- 16 Murder underlines call for more professional industry
- 17 Challenges ahead for security guard career
- 18 Security fallout from Rugby World Cup 2011
- 20 OSH in the Security Industry
- 22 Leader of well trained team has to deal with 'everything under the sun'
- 24 Red Badge Security - Training for the future
- 26 The corporate travel brief
- 28 Better retail with data
- 30 Thermal Imaging
- 32 HID Global Printer/Encoder
- 36 Retail Security - who can you trust?
- 38 ASIS New Zealand
- 39 NZIPI Association News
- 40 Cyber Threats
- 41 Interview with Colin Slater
- 46 Zone Technology
- 47 MIC Series 612 Thermal Camera
- 48 Bosch unveils AutoDome 7000
- 54 Product Showcase

Fire

- 48 **BROOKS** stand out at Fire NZ 2013
- 50 **Fire NZ 2013**

For a FREE online subscription go to
www.NewZealandSecurity.co.nz

Associations





Knowing when customers are not being served just got a lot easier. Now you can use network video to count people in your store, combat in-store dwell times and monitor queues in real time. So you can better plan staffing levels, boost conversions and enhance customer service. It's all made possible with high quality video feeds, real time alarms and other smart features in Axis' leading network video solutions for retailers.

This is just one way Axis' IP solutions help retail stores minimize loss and maximize profits. Be the first to know how to stay one step ahead.

Get the Axis picture. Stay one step ahead. Visit www.axis.com/retail or send an email to contact-sap@axis.com for more information.



Axis network video solutions for retail integrate our leading network cameras with specially-designed applications from our partners. • Outstanding HDTV image quality • Integration to your existing POS, EAS and IP systems • Scalable, future-proof solutions from standardized equipment

AXIS[®]
COMMUNICATIONS

Distributed by:

CHANNELTEN
SURVEILLANCE SOLUTIONS

Hills
Electronic Security
Since 1968

The Power of One

by Rick Focke

Have you noticed how there has been a recent backlash to the “everything bigger is better” thinking that dominated popular culture and business for a time?

Where once products had to be about supersizing and multiplying and expanding the scope, today’s focus is on procuring what best serves our needs — whether that’s in the fast food lane or security installations.

Part of what is driving these changes is a desire for efficiency of both time and money. Why buy big when small can sometimes do the job better?



How that translates to our field specifically is with the advent of products such as the single-reader door controller.

In an industry that is often all about scalability and how to make things work by thinking in terms of multiples, there is definitely a time and place for a standalone application like a one-reader door controller.

How many times have you encountered an installation where there is a lone door that needs coverage? Or, perhaps the door’s location is such that it cannot be clustered with others?

The current economy has shifted the focus to efficiency and cost competitiveness, so there are times when it can make perfect sense to invest in a one-reader controller for those instances where one is enough.

The other big push for a single-reader controller is the result of an installation shift towards ubiquitous cat 5/6 wiring. Primarily seen in new construction projects, a separate, dedicated cat 5/6 network cable is installed to each door from a central IT area. This design simplifies the overall installation, especially if Power over Ethernet (PoE) is used, and lowers the installation cost by reducing the amount of localized door device wiring.

Although, still offering key functionality of its two- and four-reader counterparts such as PoE to leverage the existing network infrastructure, NIST-level encryption and local storage capability for up to 400,000 cardholders, the smaller controller offers the utmost in scalability to accommodate any installation layout and any budget. Yes, each controller requires an IP address, but the increased system reliability of



Tyco Security Products Rick Focke

having a stand-alone device at each door more than makes up for the possible increase in network management costs.

So when the situation presents itself, it’s OK to think that where two or more are good, one can sometimes be better.

Have you started using a more IP-centric system layout for new projects? Or are your projects more conducive to a centralized approach? Let us know.

For more information on the one reader door control and Intek Security Groups wide range of products and services, go to www.intek.co.nz

or phone

Sales: 0508 4 INTEK (46835)

Tech: 0800 11 HELP (4357)

intek

When you think
IP video



think
American Dynamics

Sure, there are a lot of companies out there with IP video solutions. Some offer cameras at rock bottom prices. Others have systems that look good and promise the world.

So, why should you think of American Dynamics for IP solutions?



- Proven long-term leadership with Intellex legacy
- IP camera portfolio – from standard res to HD – that has tripled in the last year
- NVRs and Hybrid recorders that dispel the “big business only” mentality
- Groundbreaking video management that unifies analog and IP

Now, that's something to think about. **American Dynamics for IP solutions.**

join, visit, share   
www.americandynamics.net
+61 467 763 544
tycosp-apac@tycoint.com



American Dynamics
From Tyco Security Products

intek

© 2013 Tyco Security Products, All Rights Reserved.

Professionalism of security guards key to improving industry reputation

By Keith Newman

The security industry is going to need far more than mandatory basic training for security guard licenses if it's serious about the long-stated desire to oust the cowboys, become more professional, and improve its often tarnished reputation

Those wanting to clean up the industry, known for attracting sometimes dubious characters to the business and the beat, have been lobbying for around 30-years to have a stronger legislative framework that recognises minimum training requirements and qualifications.

While the New Zealand Security Association (NZSA) is attempting to plot a new course where skills and ethical behaviour are paramount, the security industry remains in churn with eroded margins, minimum wages, mergers and acquisitions, a stream of liquidations, and at least one major service provider about to sell off its guard division.

In 2010 the 36-year old Private Investigators and Security Guards Act 1974 was given a makeover requiring all guards, crowd controllers and bouncers to be licenced. The replacement Private Security Personnel and Private Investigators Act 2010, came into force from April 2011.

While candidates can be disqualified for any serious violence, drugs or dishonesty convictions, many believe the long overdue changes still fall far short of the kind of legislation necessary for a first response industry, tasked with protecting life and property.

Before the end of October 2014 all guards and crowd controllers will need to complete three basic NZQA unit standards: conflict management, communication and risk identification and gain a certificate of approval (COA), before being granted a licence.

There are 1537 licenced security companies in the country, mainly small businesses, offering residential, commercial and industrial security patrols, alarm response, crowd control, doormen and bouncers, payroll delivery, prisoner and court custodial and related services.

A large number of the 25,000 or so employees are casual workers on contracts or called on for seasonal events. Although the uniform and job description suggest security guards are part of a trusted profession, a distant cousin perhaps to the police, ambulance and fire service, that's often been exposed as fiction.

In December 2012 the security industry was among those targeted by the Unite Union for treating its workers badly and paying them below the minimum wage.

It claimed security companies were at war with each other, undercutting on price to win contracts and paying among the lowest wages for the "nastiest" work conditions.

It staged a series of protests outside the headquarters of several large security companies late last year and joined the NZSA's call for government regulation that might lead to higher pay and better conditions for guards.



**Deliver
Powerful
Vision in Every
Moment**

Capture the details with
high sensitivity, full HD resolution
and remote pan/tilt/zoom control



LNV7210



LND7210(R)

LND7210(R) / LNV7210(R)

Smart IR(LND7210R/LNV7210R)

Smart IR function enhances the camera IR performance for better image quality



Conventional

LG

Defog

Defog function supports the clear image in any weather condition such as fog, rain and smog



Conventional

LG

Full HD 60FPS

Full HD 60FPS stream allows vivid streaming to users



Conventional

LG

Remote Pan/Tilt

Remote pan/tilt is valuable for easy installation and overcoming the fixed monitoring



Audio Detection

User can detect abnormal sound like baby cries or a loud noise



Face Detection

By face detection, it is possible to detect people in prohibited areas



* Above images are for understanding. There might be difference from actual picture

Sting operations underway

While most players welcome the law change which raises the bar for becoming a security guard, there are concerns about how it will be policed and whether companies can still get away with sharing licences or using loopholes in terminology like calling people ushers or stewards.

The NZSA insists it's already on the case and is taking a strong stand alongside NZ Police and the Department of Internal Affairs (DIA). A number of charges have already been laid and other prosecutions are pending.

"We've already begun sting operations around the country demanding to see people's licences. If security guards are found to be unlicensed there will be prosecutions," says NZSA's Chief Executive Greg Watts."

He says the legislation is an important step toward raising professionalism and driving out poor quality operations which have driven down the value of the industry for decades.

Watts says the NZSA is trying to influence the industry in a positive way through codes of practice, auditing and training, and is "getting its ducks in a row" ahead of ultimately applying for status as a compulsory membership industry group.

Ray Beatson, the NZSA's first full time employee in 1988, says he and others who were fed up with the Government's annual promises to create legislation for the security industry wrote guidelines for the Justice Minister, 23 years ago.

He says nothing happened until the mid-1990s and even then it was simply tweaks in miscellaneous provisions bills, including making it legal for private investigators to take photos.

Beatson, who initiated the industry's first nationally recognised security industry qualifications and negotiated an agreed

system of remuneration with the unions, says the new regulations are a start but there's been "some dumbing down".

At the time Justice Minister Nathan Guy said, it was an important step in cleaning up the industry, improving standards, protecting the safety of the public and ensuring the right people worked in an area which was often volatile with the risk of violence.

Minimum training for security guard licencing was delayed until after the Rugby World Cup to avoid creating problems for those needing to employ thousands of security personnel and crowd controllers.

According to the NZSA there are about 25,000 full time and casual security staff across the country and while the Ministry of Justice estimated there would be around 12,500 applications from current licensees and certificate holders it also expected 9000 new applications for crowd controllers.

"We've already begun sting operations around the country demanding to see people's licences. If security guards are found to be unlicensed, there will be prosecutions."

NZSA Chief Executive Greg Watts

Whistle blowers

Greg Watts says the NZSA has pushed for mandatory training for years. "You can't police something if there's no legislation but now that it's black and white we will see, unprofessional operators disappear from the industry."

Part of that will be self-policing. "We had a flurry of the industry informing on itself six months after the original

legislation was introduced and again last year. We have done a lot of cleaning up of unlicensed operators."

In the past, he said, the NZSA would issue a warning or raise awareness of the need to be licensed. Now it's "get licensed and legal or get out of the industry".

Beatson, CEO from 1988 to 1999, is frustrated it's taken this long, claiming the NZSA dropped the ball after much time and money had been spent getting government agencies, the Insurance Council, the Police and others to agree on a set level of training for licences.

There were insurance incentives and an agreement that you needed to be an NZSA member and abide by its code of practice to get certain kind of work, "but the eye was taken off the ball and things have been staggering along".

Beatson says the use of unlicensed people has encouraged cost cutting and questionable business practices and the NZSA needs to take a stronger lead in raising the professionalism of its members through audits, ethics, standards and compliance.

He says it needs to present a united industry view, taking a lead in educating the public and businesses about security and improving its dealings with the media, rather than what he claims is the fragmented approach of the current NZSA board and staff.

"It needs more of a public profile, with the CEO seen as the go-to person for unbiased media comment or directing the media to experts in specific areas for comment," rather than the random people currently called on for comment.

Lack of maturity

Mike Rutherford General Manager of First Security is also concerned the industry hasn't matured much over the past 40-years. "There's still a relatively high degree of professional immaturity... and little change other than the use of electronics."

Rutherford, one of the first professionals to obtain a COA, says the new legislation still represents a low barrier to entry and while compulsory basic training might offer small improvements, "it's really just window dressing".

He sees evidence of poor practice most days. When New Zealand Security Magazine (NZSM) called, First Security was just taking over a contract in Wellington after a small licensed "fly by nighter" was closed down by the tax department and its guards walked off the job leaving the client exposed.



NZSA CEO, Greg Watts



Former NZSA CEO, Ray Beatson

TruVision®. The new generation of HD.

With more features than ever before, a TruVision solution provides the winning combination of performance, high resolution and style.



Fitted with a motorised zoom lens and auto focus feature, installation and configuration of the TruVision IP Outdoor Cameras becomes significantly easier.

Combine this ease of installation with the high-performance network video recorder (TVN50), flexible bandwidth allocation allows users to maximise recording performance.



Mike Rutherford GM of First Security

“Clients are putting millions and sometimes tens of millions of plant and equipment in the hands of people they don’t really know.”

Rutherford has seen many companies come and go over the years and advises businesses hiring security to first check how long they’ve been around, sight references from previous customers including levels of service, and ensure they’re committed to ongoing training for their personnel.

He recommends membership of the NZSA, which audits its members through codes of compliance, and says checks should be made into the ethics, experience and health and safety record of company management as “they’re the ones you’ll have to deal with if there are any issues”.

Rutherford says First Security, which employs about 1800 people, invests over a million dollars in training annually, however, he knows other companies that “don’t want to know once they get their guards into a uniform”.

While he says bringing bouncers under the Act was brilliant and the new training regime goes somewhere down the right track, “it’s late in the game and light on substance”.

Derailed by indecision

However, Greg Watts says achieving even a minimum standard across the industry would still be on the backburner if he hadn’t applied some serious political pressure.

“It wasn’t going anywhere, and there was no sense of urgency until I met with the minister last year and again applied pressure in May this year so we could announce it at our annual conference.”

He says security training companies waited two years for an announcement and because of the uncertainty some either pulled out of the business, reduced training or stopped it altogether.

“We were going backwards, a number of private training companies went out of

business, staff were not being trained and contractors and people with training skills were disappearing and taking jobs in other industries.”

In the midst of that churn, NSZA acquired private training company TSSL for an undisclosed sum to prevent further skill loss, and now employs its owner Stewart O’Reilly to head its new training programme along with staff member Ngaire Kelaher.

That gives the NZSA a dual role as training provider and co-ordinator of a nationwide programme to ensure training organisations are audited and all security guards get an equal opportunity to sit the tests.

Watts doesn’t have too many grumbles about the legislation although he admits it could have gone further and will need some tweaks, particularly around recognising and exempting those who already have much higher level qualifications.

He says the new regulations are a good stepping stone for higher education and would ideally like to see all security companies have their staff obtain eight more credits for a Nationally recognised Certificate in Security.

“There are some classic examples of members of the association abusing their position, some are known to jump from company to company because there haven’t been any rules.”

Denis Parson, Principal, InDepth Forensics

In the meantime his main concern is that casual security guards and security companies don’t leave it to the last minute to get their staff trained. “If everyone waits until October next year to get their training then we’re all buggered, most of the larger companies are already working on that,” says Watts.

Chris Harris, General Manager of Auckland based Rush Security, says for larger companies with 500 or 1000 staff this could cost hundreds of thousands of dollars but the real issue will be with part timers, he says we worked out a deal to roll over the cost month by month to train our 80 full time security staff.

When NZSM called he was going through the 300 names on his casual staff list, many of whom work for other companies, to see who was going to



Chris Harris, General Manager Rush Security

stick around and who might need some investment to keep them in the game.

The challenge for casual employees, particularly those who only work on events a couple of times a year, is whether it’s worth paying for training. Having to pay for a COA and a security licence doesn’t stack up if you are only going to be employed three times a year, he says.

Harris suggests this will likely reduce the pool of people available, particularly in smaller centres, and require crowd controllers and guards to be imported for Rhythm ‘n Vines, vineyard concerts or sporting events like the Rugby World Cup.

This presents a dilemma for the industry, particularly larger events companies, around who’s going to pay for the training. If it becomes harder to get people, its likely additional costs will be passed on to security guards or the client.

However, he suggests those who pay for their own licences will help raise the bar and they’ll become the cream of the crop.

Red Badge, New Zealand’s largest provider of security for events, with around 2000 staff on call, continues to work on its own growth strategy and raising the level of professionalism among its full time and casual personnel.

Red Badge Group Managing Director, Gary Wilton says his company is on top of the requirements of the new legislation which he hopes will help drive “two bit players out of the market”.

However, Wilton remains concerned at the low barrier to membership of the NZSA which he claims isn’t asking the hard ethical questions, particularly around the financial behaviour of companies with dubious backgrounds that fail then end up “phoenixing” in some other form.

Membership ethics

Denis Parsons, Principal of InDepth Forensics in Hamilton, involved in a number of investigations and liquidations

Elemental storage building blocks for every datacenter.



Build a better datacenter. Enterprise-class datacenter drives from WD® offer end-to-end datacenter storage solutions that are rigorously engineered for the ultimate in performance, reliability and scalability. Learn more at wd.com/datacenter.

absolutely™



of security companies, says security guards and private investigators need to be policed by some independent internal regulatory agency similar to the Police Complaints Authority, the Law Society or the Institute of Accountants.

He says while PIs and security guards are trying to upskill and show they are doing a professional service, they get let down by the one percent. "Ninety nine percent of the time they do a good job under rather stupid legislation and then a few cowboys come along and cause the whole industry to be placed into disrepute."

Parsons goes so far as to suggest there should be a blacklist not just for those who have faced criminal prosecutions but for breaching the ethical requirements they agreed to on becoming a member of the NZSA, for example.

A list of those whose actions have rendered them unsatisfactory to be involved in the industry might remain in effect for five years. "The industry needs to show its teeth by weeding these guys out otherwise they'll continue to run amok."

Parsons, who's both a PI and a former member of the Institute of Accountants investigation panel, says the Institute of Accountants, for example, "can make your life a misery" for breaching standards.

He says members are summonsed to Wellington to appear before a panel of up to 10 peers who "will question you vigorously and if they don't think you are up to it they will suspend you".

Rather than just talking about creating higher standards, the industry should have its own enforcement regime and hopes the recently revised legislation provides a baseline for that.

"There are some classic examples of members of the association abusing their position, some are known to jump from company to company because there haven't been any rules."

Watts says the NZSA is doing what it can within the constraints of its present voluntary membership model including looking at the backgrounds of new companies wanting to join. It also has a complaints process for members who have behaved in a manner "not fitting for the organisation".

He says it's difficult to take action unless there are clear facts about something contrary to the NZSA Code of Ethical Conduct. "There's a lot of hearsay with people complaining about competitors or having personal grievances; we investigate to a certain extent but they are often things the NZSA doesn't want to get caught up in."

While there might be a perception that some companies are doing things inappropriately but when you look into it, it's not actually illegal. "It's a fine line sometimes," says Watts.

A number of companies have, however, been denied membership because of their activities. Darien Rush and Rush Security, for example, were declined membership for a number of years until the dust settled after their many court cases and ongoing media coverage. "We did accept him after receiving letters from lawyers showing various court cases had been thrown out."

If it is proven that a company has acted illegally they would be suspended or their membership terminated, says Watts, although he admits his organisation struggles with ethical issues that fall into legal grey areas such as companies being liquidated then reappearing in some other form, run by "shadow directors" or wives or friends.

"The NZSA should have a more public profile, with the CEO being seen as the go-to person for unbiased media comment or directing the media to the experts in specific areas for comment rather than the random people currently called on for comment."

Ray Beatson former NZSA CEO

"There are legitimate reasons why many companies are liquidated but if we find companies acting inappropriately or there's something untoward occurring among our own members, we will take a stance."

He says the NZSA is looking to strengthen its stand on these matters but has to be careful. "No-one in this industry is squeaky clean and if I took action over every objection or personality clash I would literally have no members."

Watts says most other industry bodies, finance or real estate for example, operate under a legislative framework where membership is compulsory. "The security industry hasn't had that and yet we deal with people's lives and property so it's fair to ask why we weren't among the first to get on board with professionlising?"

He agrees the new legislation and regulations around training are a step toward this goal and as a result membership in the NZSA has begun to grow again.

Watt says his goal has always been to gear the NZSA up to represent the wider industry with the backing of legislation and believe that when that time comes it will be in a much better position.

Compulsory membership would give the organisation more of a stick to deal with anyone contravening its code of conduct or not completing audits in time. "At the moment we have a stick and a carrot because we want to ensure we have an influence over the professionalism in the industry and we have to be careful how we use that stick."

Currently the NZSA represents about 70-80% of the industry by value, including 150 of the larger businesses, although about 1300 of the 1500 licensed companies in New Zealand are small businesses and many aren't members.

Flag guard convictions

Rutherford from First Security says too many people enter the industry with very little business or industry experience, and when they end up struggling, standards don't get maintained. "It's too easy for someone who has worked as a guard to form a company and offer their services."

While it was a good move to take the security guard licence from one to five years; which he says was just a money grab, Rutherford would like it to be harder to obtain one in the first place. "Unless you are in jail or have just come out, it seems you can still get a COA."

He'd also like to see a closer links enabling better communications between the Courts, Police and Justice.

"We came across a situation recently where two people still had their COAs despite the fact one was a pedophile and the other a thief."

Neither had gone to jail, although they had both been convicted of serious crimes. "We only discovered this when we did a serious ground check." When challenged they said no-one had cancelled their licence.

Rutherford says the onus is left to the employer to do a lot more background checking. "A guard with a COA could get arrested for serious offences but there's no flag on the system to say they are a registered security guard. There's no communication."

Chris Harris from Rush Security says he's wanted to see the profile and value of security guards raised for some time. "Many of the people we interview for jobs are already on the minimum wage or less and don't have their licence. I don't know how some companies are getting away with this."

Q-See IP camera and NVR kits



\$1495.00



ON Board POE

Use cameras as stand alone or with NVR



From \$220.00

**4,8 and 16 channel available
Fully supported locally and at**

www.q-see.com

Proprietary APPS for all platforms



**Phone 0800 438 007
www.dcsecurity.co.nz**

DC Security Ltd

He says the first attempt at enforcing the COA legislation will probably drag out and it could be a year or two. In the meantime he says it's imperative the industry police itself until it becomes obvious who's not complying. "All NZSA members should be enforcing this anyway."

Over time, however, he believes security companies will insist employees take courses beyond the COA requirement. "They won't waste their time with those who haven't done that initial training."

Harris believes the COA has the potential to raise the bar and increase pay rates for the whole industry as long as everyone complies. "You are not going to have people pay to gain the COA then receive minimum wages, they'd be better off working at The Warehouse or McDonalds."

Diversification and value

In the mid-1990s Ray Beatson was among those scoping out a list of functions undertaken by NZ Police that could be taken over by private security to free up trained police officers, for example crime scene guarding.

"Instead of having four or five highly trained Police officers keeping people behind the taped line a professional security

"A guard with a COA could get arrested for serious offences but there's no flag on the system to say they are a registered security guard. There's no communication."

*Mike Rutherford,
General Manager of First Security*

guard could do that at a lower cost."

Mike Rutherford of First Security says over the past four years there's growing evidence that clients want more qualified front line officers. "While some companies only see value in a cheap price, others see value in well trained, motivated people."

While the lowest price has typically got the deal in the past, he says there is a greater awareness, particularly among blue chip companies, who realise the value of service delivery.

"We're there to prevent bad things happening and bad things will continue to occur. Prevention is only one step in the process, you need to be able to respond to different events."

While there will always be a need for a physical security response, Rutherford says greater use of remote monitoring and smarter technology will continue to impact the industry, and security guards will have to become more competent and technically savvy.

The way forward he says will see the industry change from gatehouse or premises guarding to multi-tasking, including the technical knowledge needed for facilities management, and ensuring machines are not only secured but running properly.

After years of dog eat dog business practices, bad press and battling to have its own legislation based around minimum training and wages, the security guard business now has a clear opportunity to lift its game.

The challenge is not only to clean up its own patch but to better manage what is often a seasonal price-based business that has shown little evidence of growth or innovation while electronic security and systems automation are eating its lunch.

Changing market expectations, new legislation and a professional industry body that's raising the bar on qualifications and forging stronger relationships with the NZ Police, the Justice Department and Internal Affairs, suggest the tide is turning.

Murder underlines call for more professional industry

The murder of security guard Charanpreet Dhaliwal at a West Auckland construction site in November 2011 served as a serious wake-up call for an industry long plagued with claims of lax standards and unprofessional practices.

NZ Security Association Chief Executive Greg Watts, who was called as an expert witness in the case, says it was frustrating the murdered man's employer CNE Security was let off the hook in the October 2013 court decision.

Watts says Dhaliwal had little previous training or skills and he began his shift in the evening with minimal site awareness or the two hourly phone check which is NZSA standard practice. "They wouldn't have passed the NZSA audit process."



Helen Kelly, Council of Trade Unions

"Leaving Dhaliwal alone in the dark unchecked until four in the morning created an intolerably low threshold of care."

CTU President Helen Kelly

He's aware of companies who still operate this way and used the case in discussions with the Minister of Justice to illustrate the urgent need to have mandatory training for all security guards.

The New Zealand Council of Trade Unions (NZCTU) believes the decision handed down by the Waitakere District Court, exonerating CNE Security from any blame in the death, needs to be challenged by the Minister of Justice.

CNE Security was discharged without conviction on counts of failing to secure Dhaliwal's safety under section 6 of the Health and Safety in Employment Act 1992.

The NZCTU says the court finding, that the company did not need to take further steps to ensure the safety of Dhaliwal, "lowered the bar for all workers".

CTU President Helen Kelly said allowing a 20 minute induction from someone who only had one night's experience as sufficient training for work on a remote building site, then leaving Dhaliwal "alone in the dark unchecked until four in the morning" created "an intolerably low threshold of care".

She said the decision "endorsed the worst kind of sloppy practice", as the company had "no regular checking system... no easy method of communication...and insufficient scrutiny of the employee's ability to safely undertake the job".

Dhaliwal's mother, in the country in late October following the unsuccessful prosecution of the man accused of clubbing him over the head with a piece of wood, was left with the impression there are "serious problems with the New Zealand justice system", as no one has been found accountable for what happened to her son.

NZSA's Greg Watts, says the company acted inappropriately and did not have enough protocols in place to ensure the wellbeing and safety of staff.

He says the "awful and unfortunate event" was an exception and there were many other areas in the industry, for example working on the doors of bars and clubs where security guards faced threats, which highlighted the need for guards to be adequately trained.

"We've been very fortunate not to have seen too much of that here but in the UK there's a high incidence of death and serious injuries in these roles."

— Keith Newman

Challenges ahead for security guard career

While there appear to be plenty of openings for security guards, it's typically been low paid, temporary work, often viewed as a stepping stone to other jobs rather than a career path in itself.

Mike Rutherford General Manager of First Security says, it's a very transient business as reflected in the saying "no-one grows up wanting to be a security guard".

He says the security guard business is typically seen as a feeder for other industries that offer better prospects such as the police or the fire service. "The Police even tell many of their potential

recruits to join a company like ours to get some miles under them before enlisting."

Rutherford says it's difficult to drive a culture of quality and maintain high standards on the low wages many guards are paid. "We genuinely believe we have high standards and while our front line officers work hard, they aren't highly paid so it's difficult to motivate them."

On some employment websites security is still described as unqualified work despite recent legislation requiring a minimum level of skills to get through the door.

According to the Government's www.careers.govt.nz site "there was a good chance" of finding a job as a security officer or guard, patrolling and helping to protect buildings, prevent fires, trespassing and vandalism.

You might even end up involved in investigations on behalf of individuals and businesses or providing personal protection to a client, it says. With one to three years' experience we're told security officers and guards "usually" earn \$14-\$16 per hour which can rise to \$16-\$22 an hour with more than three years' experience.

However, research by NZSM concluded that the low end of the market the rate is typically in the \$11-\$12 range, among the lowest paid 15% of New Zealand's workforce, with work conditions that aren't always ideal.

One contact said guards were expected to work in the rain, get out of bed any time, pay for their own petrol, arrive on time, remain on casual contracts and change sites at the last minute.

About 11,200 people were employed in the field in 2012, about 1000 more than in 2010, although the NZSA suggests the number of people employed in this field could be as high as 15,000.

Those applying for a job in security are advised on the Careers site that they need to be "free of dishonesty, violence or drug convictions in the past seven years".

They also needed a certificate of approval (COA) issued by the Ministry of Justice, which involved a police background check and public notification where objections could be raised. Applicants were told "a first aid certificate may also be useful".

Chris Harris from Rush Security says the old mentality that no qualifications are required and security skills can simply be drummed into people no longer holds water; good security requires a certain kind of person.

The best security staff are those who can provide customer service and act as a peacemaker rather than those who want to rark things up a bit. "We're looking for people that can talk through a situation rather than look like they are going to beat someone up."

Harris says the conflict resolution training in the new industry regulations will be helpful as many recruits are not given the opportunity to learn this. "As security officers that's really what we're there for to deal with conflict."

— Keith Newman

Three course entry challenge

The New Zealand Security Association (NZSA) is working with other private training organisations (PTOs) around the country to co-ordinate workshops and training sessions so no-one misses out on getting the new compulsory qualification.

While a number of new private training companies have "come out of the woodwork" since the regulations were announced, CEO Greg Watts says there are five training companies who are currently qualified, audited or in the process of being audited (*as we go to print*) and have credibility, including its own training arm.

He says those in small areas will get equal opportunity to train as those in the main centres as NZSA and the PTOs are creating economies of scale to reduce costs and provide subsidies to those outside the main centres.

All security guards, bouncers and those involved in crowd control have to complete the new compulsory certificate



An NZSA training session underway

of approval (COA) if they had an existing licence or applied before October 2013. Those who applied subsequent to that date can work temporarily but must complete training within three months to obtain a licence.

Applications for the new licences are being handled by the Private Security Personnel Licensing Authority (PSPLA). The cost of a five-year a COA is \$200 or \$170 online and a full licence could cost around \$300.

To qualify applicants must complete NZQA Unit Standards 27364, 27360 and 77361. These are designed ensure trainees demonstrate knowledge of the security industry in a pre-employment context, demonstrate knowledge of managing conflict situations and an ability to manage conflict situations in a security context.

All holders of licenses and COAs for crowd control, personal and property guards have to complete the mandatory training by 1 October 2014.

The NZSA offers all NZQA recognised security qualifications and assessment standards up to and including the highest qualification currently available, the National Diploma in security (Level 6).

Private Security Personnel Licensing Authority Web: www.pspla.govt.nz



NZSA Chief Executive Greg Watts hands Noel Brown of WD Security his LCP1 (Limited Credit Program) for the NZQA National Certificate in Security Level 2.

Security fallout from Rugby World Cup 2011

While the All Blacks did the country proud at the 2011 Rugby World Cup it was also a defining event for the New Zealand security industry, highlighting the overdue need for a more ethical playing field for crowd control and security personnel and the companies that hire them.

While there were few incidents, the events put some security firms in the sin bin, exposing mismanagement and financial difficulties as they passed on contracts, shared licences, changed names or went broke.

NZ Security Association Chief Executive, Greg Watts, says providing professional crowd management is “a very tough game,” requiring sufficient resources to “scale up and down again when it’s over” and ensuring staff are licenced and trained and have the right aptitude and on-call availability.

Watts, relatively new to his role at the time, brokered a meeting with Rugby World Cup (RWC) organisers, the big security industry players and the Police to discuss “how we could effectively co-ordinate management of these events.”

“It was such a high profile event that they [security companies] realised if they used the wrong people and there were serious incidents, it would reflect badly on them.”

While mandatory training requirements were stalled until after the RWC so as not to reduce the pool of licenced crowd control and security people it was a wake-up call for providers.



While mandatory training requirements were stalled until after the RWC so as not to reduce the pool of licenced crowd control and security people, it was a wake-up call for providers.

Darien Rush Security, the main security operator for the Auckland region, got into deep trouble after buying the contract off Strategic Security in March 2010. Strategic Security was put in liquidation owing \$2 million, including over half a million to the IRD.

After claiming it only acquired the assets of the former contract holder, Darien Rush Security took on crowd control at Eden Park and North Harbour Stadium, and found itself facing liquidation proceedings owing \$2 million in debts including to the IRD.

The action was stalled and the company then changed its name to Northland Services Ltd which was ultimately placed into liquidation in 19 September 2013.

Staff ill prepared

According to the liquidator, Companies Office records and media reports, Darien Rush Security, a former alarm systems company was already embroiled in conflicts ranging from the installation of CCTV security systems and its acquisition of patrol company Magnum in 2008, at the time it acquired Strategic Security.

Security officers employed by Darien Rush Security claimed they were underpaid, understaffed, undertrained and not prepared for the contract.

In January this year the Department of Internal Affairs issued a warning

to Platform 4 Group (P4G), another Auckland security company which picked up a number of Rush clients and managers.

Darien Rush Security alleged the company leveraged another operator for licensing purposes and P4G and its director Aaron Colthurst were questioned by the DIA.

While unsuccessful this was the first investigation into an alleged breach of the Private Security Personnel and Private Investigators Act 2010, requiring private law security firms to be licensed for any security work, including crowd control.

According to the NZ Companies Office, Darien Rush continues to operate as director of Rush Security Holdings registered on 26 November 2012 with co-director Christopher Heremaia Harris.

While frustrated at the low standard of some of the companies working on the RWC contracts, the NZSA's Watts says lessons were learned, particularly about the need for greater professionalism, but the flipside was the improved relationship between the industry and the Police.

He says now that new security industry legislation is in place, including the training regime for all guards and officers, Police have a better understanding and trust and will rely on NZSA members more than they did in the past.

“Our industry relationship and communication with the Police is now better than it’s ever been and that’s meant we’re now involved in the Auckland City Council CCTV project which could roll out to the rest of the country,” says Watts.

What is in your security platform's DNA?



**Security
Center**

**You decide. Strengthen your security;
one building block at a time.**

Start with Security Center unified video, access control and ANPR. Consolidate business systems like intrusion detection, asset monitoring, building management and more. And watch unification evolve.

See what you need at genetec.com/SecurityCenter

Video Surveillance | Access Control | Automatic Number-Plate Recognition

For more information



**Open
Platform
Systems**

OPS New Zealand:
Level 4/17, Albert Street
Auckland 1010
New Zealand

Telephone: +64 9 927 7614
Mobile: +64 21 970962
Email: jason@opsystems.co.nz
Website: opsystems.com.au

Innovative Solutions

Genetec

Health & Safety in the Security Industry

An industry first for Saul Leckey of VIP Security when he received his Site Safe Certification in Safety Management at the Annual Site Safe Construction Health and Safety Awards Gala Dinner in Auckland

“Zero fatalities during the Christchurch Rebuild” was the resounding message taken by attendees from the Hon Simon Bridges - Minister of Labour, during his key note speech to the Site Safe Graduation and Innovation evening on October 30th 2013.

The other message from the evening was Health and Safety is changing, with the Ministry of Business, Innovation and Employment developing a Working Safer reform package.

A large proportion of the attendees were employees of construction companies, but amongst them were Saul Leckey and David Proud from VIP Security. VIP Security is the first electronic security company in New Zealand to have staff attain Site Safe's highest qualification in “Safety Management”.



David Proud Managing Director of VIP Security with Saul Leckey when he received his Site Safe Certification in Safety Management at the Annual Site Safe Construction Health and Safety Awards Gala Dinner in Auckland.

Based in Christchurch and soon to be involved in many of the large projects involved with the rebuild, VIP Security prides itself in training, and not just in products but in health, leadership, project management, background skills (such as CISCO certification) and of course safety.

Often the health aspect in Health & Safety is overlooked. However VIP Security have undertaken several initiatives, one of which is providing all staff with health insurance through Southern Cross Health Society. “We have found that by offering Health Insurance to our staff this has had a very positive impact on our bottom line and staff morale. By assisting our staff with their health which facilitates a speedy recovery and a prompt return to work, which is a win-win situation for everyone.” says David Proud, Managing Director, VIP Security.

Another initiative is that VIP Security have a small gymnasium on-site. Again with safety in mind, a certified instructor gave all staff training on proper use of the equipment prior to opening of the gym.

However, health doesn't need to be a big expense. A good example of this is getting involved in community fun runs which helps to promote both mental and physical health and wellbeing as well as being great fun.

Along with weekly toolbox meetings, VIP Security are committed to first aid training and escalating all field staff in Site Safe training. Along with Saul's top achievement, VIP also have other technicians close to attaining top Site Safety Management certification.

To assist with keeping up to date with changes and correct equipment, VIP Security has developed a strong working



Health doesn't need to be a big expense, an example of this is getting involved in community fun runs which can help to promote both mental and physical health and general wellbeing

relationship with Rita from NZ Safety. The regular updates and checks that NZ Safety has provided has enabled VIP Security to spend wisely on relevant and approved safety equipment.

Safety within the construction industry is facing challenges with the majority of building sites requiring a bigger commitment in time and methodology. Whether it is the restricted use of ladders, mandatory site meetings, site specific safety plans, 5+5's, or audits, the wise contractor must now include and budget for the costs associated with these commitments.

At VIP Security, all staff are recognised as the company's greatest asset, so looking after their health (both physical & mental) and safety are paramount. “Our belief is that every security company can afford to do more for their staff's health and safety, it just a matter of setting your mind to it.” says David Proud

VIP Security is a locally owned business based in Christchurch with a branch in Marlborough. Working throughout the South Island, specialising in corporate, commercial and industrial electronic security solutions.

your electromagnetic locking specialist!

**Underpinned by
22 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
- Chromed through hardened, polished stainless sex nut
- Full protection against transients.

Options include:

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

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

10
YEAR
GUARANTEE



Leader of well trained team has to deal with 'everything under the sun'

As all readers of this erstwhile publication know, working in the security industry can be pressure-filled, demanding, challenging... and a host of other descriptive words and phrases telling us one thing; it's tough out there.

In a series of profiles we will look at some of the individual leaders in this sector: those keeping the lid on the pressure cooker... so to speak.

Want to know more about big roles in the security industry? How about this one? You are managing a team of 40 guards complemented by 20 to 25 full time equivalents and another 800 hours a week to preferred security contractors. You are directly responsible for the safety and security of 40,000 individuals plus a staff of 6,500, the second largest employer in New Zealand's largest city. Your role includes managing security at six sites across the isthmus with over 200 buildings and over 600 CCTV cameras. You can find yourself responsible, on any given day, for the safety of royalty, world leaders, titans of industry and a veritable host of other dignitaries. You are in regular close co-operation with Police and diplomatic protection squads.

Rehan du Toit, Security Services Manager for the University of Auckland's security department, doesn't get a lot of time to put his feet up but he did make time to speak to NZ Security Magazine.



Rehan places a high level of focus on staff development

So in non-emotive security terms, how would he describe his job?

"My role at the university encompasses a wide range of both contracted and in-house services, including contracts for site specific security and mobile patrols, alarm response across four of our six campuses, over 40 in-house security personnel and control room operators.

I am also involved in event planning and, more particularly, providing security risk assessments and advice on security related matters to assist event organisers with successfully running events on campus. I am also involved in security system related projects and I conduct security risk assessment and provide recommendations on how to improve security on campus."

South African born Rehan has been responsible for building and maintaining the university's security relationships with a variety of people, from Police and Auckland City Council along with equivalent personnel from other tertiary institutions. He has developed a strong relationship with Central Police Community Action Team to the extent that they now have a team of constables dedicated to the university to assist with crime prevention advice, training of in-house Security Services officers and both covert and overt crime prevention operations on campus.

With hundreds of events and thousands of classes every day, the requirements placed on the security team are ever-fluctuating. Most pressure comes outside the regular semester programme and the normal hours of operation.

With the huge volume of extended classes, after-hours events, conferences and hire-outs to external parties, access to buildings, maintenance of access to power

and other services as well as the security of people and buildings, is an ever-moving feast that requires detailed levels of organisation and knowledge on the part of Rehan and his team. The event triggered monitoring system, security control room and control room operators are integral to this.

He knows that for this level of security and service provision you need a great team; committed, with great people skills and, above all, highly trained. Rehan says that today the University of Auckland Security Services Department is seen as the flagship for the security industry in New Zealand and everyone in the operation, from his immediate superior, campus operations and security manager Bryan Nicholson on down, is committed to the maintenance of professional standards.

"We place a high level of focus on staff development and have made the level 2 Certificate in Security as well as the Certificate of Approval compulsory for all my staff, although we have exemption. This is now part of their collective agreement. Any new staff member joining us is given nine months after the start of service within which they have to complete their level 2 certificate.

"We also have a number of trained and qualified work place assessors, including myself, who can assess up to Level 3. This year we I have enrolled most of our staff for the level 3 certificate (senior security officer) which they will hopefully complete early next year."

Investing in staff development is a vital part of the maintenance of those professional standards. On top of that, the team at University Security Services Officers are paid 'top dollar' and the

This affects you

Security industry training requirements have changed.

Contact us – we can help get you started.

skills.

The Skills Organisation
info@skills.org.nz
skills.org.nz

chance to be part of a challenging and pleasant work environment. In an industry known for a high staff turnover, guards (Rehan doesn't use that term - he calls them 'security officers') at the University of Auckland Security Services stay an average of seven to eight years; one has been with the university for 32 years!

Rehan says the focus for his staff is on providing good customer service. "With such a disparate range of ethnicities and vocations (from cleaners to professors), excellent people skills are requisite.

This is achieved through a carefully conceived and managed structure. "The staff is divided into five teams of seven members, including two qualified control room operators. In addition there is a dedicated control room team between the hours of 6.30am and 11pm made up of a co-ordinator and three specialised control room operators.

"Each team is led by a co-ordinator responsible for admin, rosters, uniforms, equipment and training," says Rehan.

As is befitting a top-tier educational institution, a defined and achievable career path goes hand-in-hand with the training; vocational achievement with self improvement.

Rehan points to physical fitness and well-being as good examples. "All our team

were enrolled in a six week programme at the University's wellness centre. A full compulsory assessment was made of all personnel including BMI, heart, flexibility etc.

"Security is a tough business on the individual on several fronts. Shift work can make for the formation of bad habits and the hours can be a killer for a normal family life. With the programme, we were given nutritional advice with regular tailored exercises at group session times planned around availability. It has been a notable success with significant gains made in fitness, strength and weight loss goals."

Officers are also enrolled in business communications skills training which adds up to 40 hours of classroom activity per person. A high level of written and spoken English ability is very important, especially with English being a second language for a lot of the team.

For new team members, Rehan views the University of Auckland Security Services department as a great career opportunity, similar to what the Police may be offering. Ideally he is looking for entry level or school leaver applicants who are willing to learn and are free of any pre-conceived notions about the job.

As most involved in the security industry know, today the sector is a constantly



Security for a small city: Rehan with his control room co-ordinators

changing environment. Within the larger university structure, Rehan is part of a strategic group established to plan for the future and to choose the best solutions. He and his team also play an integral part of the university's incident management team, and follow the CIMS model (Coordinated Incident Management System) same as that used by the Police and Civil Defence. As first responders on campus, his team provide emergency management for anything from natural disasters to power outages, water leaks, fire or crime.

So if you did happen to come across the highly unlikely spectacle of Rehan du Toit with his feet up, you are going to know one thing: he earned it.

Controlling the outcome

Red Badge Security is feeling positive about the future – both in terms of the security industry training requirements and national qualifications

Opportunity, options and excitement are three recurring themes Andy Gollings CEO of Red Badge talks about when discussing the mandatory training requirements announced in August.

“Anything that can improve the quality of what we do has to be a good thing. As an industry we suffer at the hand of perception. Anything that increases industry performance while taking away any rogue element has to help.”

Andy believes the three unit standards as a minimum standard strikes a balance and is the right thing for the industry. “As a starting point it’s achievable. It’s then up to individual companies to add value on top of that through their internal training.”

The Red Badge experience

Andy says that even though to a certain extent they saw regulation coming they

looked long and hard about how to approach the training requirements. “We’ve been a Registered Training Workplace for a number of years and we wanted an approach that would work for those staff wanting to achieve the level 2 qualification and for those wanting the three mandatory unit standards.”

Where they have ended up is what Andy describes as a horses-for-courses approach. “We’re giving staff options. There are multiple directions staff can take – whether they choose to complete the mandatory requirements or the full level 2 national qualification.”

“We’re genuinely excited about how this could work out – the recent changes in the level 2 qualification mean it’s more valuable and relevant than before.”

One of Red Badge’s challenges has been how to implement their chosen approach into an organisation that has



Andy Gollings, CEO of Red Badge



From one to another: Registered Workplace Assessor Geoff Randall presented Tracey Cameron with her National Certificate in Security (Level 2) before she too joined the assessor ranks for Red Badge.

a number of regional operations spread across the country. “The most important thing we’ve done is identify the right person in the right place,” says Andy.

For Red Badge staff they start their journey towards achieving the minimum requirements from the time they start their induction.

“Our induction covers some of what is in one of the unit standards. Part of this is about showing staff what is achievable and it’s a way for us to make the mandatory unit standards part of business as usual.”

For the company and the staff having options available means the learner can approach training and assessment with a sense of control as they are using a framework that suits them. Be that through an internal workshop based approach or an independent training provider.

It also means Red Badge are able to prioritise the delivery of the mandatory standards.

Talking to their staff has also been an important factor. "There's no one defined way that's going to work for everyone. Test it with staff," says Andy.

Another lesson from staff is that nothing works better than staff seeing others achieve. Andy describes it in terms of wanting to join a club. "We've had team members who have completed the qualification making themselves available to support others through."

Experience has also shown that for some the fear of starting any type of training is bigger than the fear of not completing it. Andy has been encouraged by the response from staff around the country when delivering training for the conflict management units.

By achieving the minimum standards they are being inspired to look at the full level 2 qualification. "The full qualification is one they realise they can realistically aspire to, they see others completing it."

We want to be a good employer and this one way we can recognise people by giving them this opportunity."

Time is of the essence

For the industry to stay in control of their decisions and make the most of the time available Andy thinks now is the time to get started.

He believes it's key organisations understand what's required and what it will take to get their staff through. One way they can start is by building the learning required into internal training, even integrating it into staff inductions.

"Collectively if we don't do the work now we're only going to hurt ourselves in the long-run. Look at the options available and get involved."

The future

Andy believes by investing in staff now the security industry can benefit most. "There can be more gained than just three unit standards. Training is not just about what the law requires but an opportunity to show staff how as a company you want situations handled."

The mandatory training requirements also work in with the duty of care now placed on security staff under the Sale and Supply of Alcohol Act to ensure the safety of the public as they are leaving licensed premises.

He hopes that by raising the bar the industry will be able to change the perception of others. This, in turn, will

lead to a change in the value placed on the role security officer's play which in time could lead to increased wages. He admits it's an ideal but he sees this as an opportunity to work towards it.

"This is an industry opportunity to invest in more than compliance. We have chosen to look at it as not just a cost centre. There is value in having staff who have achieved unit standards."

Now is the time

With the deadlines set and training options available across the country, The Skills Organisation is encouraging any organisations with staff needing to meet the regulations to be proactive and start now.

Lance Riesterer, Head of Commercial industries for The Skills Organisation is keen for the security industry to be positive in their approach to the training requirements. "We have been working across the industry to make sure these unit standards are accessible to everyone who needs them. There are options available when it comes to meeting them. We know what needs to be done and now is the best time to do this."

The training requirements apply to License and Certificate of Approval holders this includes:

- Crowd controllers
- Crowd controller employees
- Property guards
- Property guard employees
- Personal guards
- Personal guard employees

Three NZQA unit standards need to be gained:

- 27364 - Demonstrate knowledge of the security industry in the pre-employment context
- 27360 - Demonstrate knowledge of managing conflict situations in a security context
- 27361 - Manage conflict situations in a security context

Deadlines

- By 1 October 2014 - if you have an existing and current Certificate of Approval (COA)
- 3 months from joining the industry

"What we want is for organisations to act now to avoid any potential bottleneck later. There's no reason to put your organisation and staff under more stress than you need to. A couple of months ago we were talking about taking the time to prepare, look at the options and talk with others in the industry about

what was happening. Now there are options available so organisations can feel confident in taking that next step," says Lance.

If you have any questions about the new training requirement contact The Skills Organisation – info@skills.org.nz

Training options

The following the organisations have been recognised by The Skill Organisation to deliver the mandatory training requirements. We expect more organisations to be added to this list - for the most up-to-date list of training options go to skills.org.nz

There are also opportunities to complete this training as part of the National Certificate in Security (Level 2).

NZSA

Ph: 09 486 0441
Email: info@security.org.nz
www.security.org.nz

C4 Group

Ph: 09 589 1815
Email: admin@c4group.co.nz
www.c4group.co.nz/

Learning Works

Ph: 07 929 4063
Email: info@primagroup.co.nz
www.learningworks.ac.nz/

Vertical Horizonz

Ph: 0800 72 33 848 or 07 579 5969
Email: info@verticalhorizonz.co.nz
www.verticalhorizonz.co.nz

Skills Update

Ph: 09 275 3155
Email: info@skillsupdate.co.nz
www.skillsupdate.co.nz

HLC

Ph: 0800 368 1095 or 06 368 1095
Email: enquiries@hlc.ac.nz
www.hlc.ac.nz

Individual organisations will advise you of costs, delivery method and course dates.

The corporate travel brief

When organisations send their people to countries where there is a quantifiable risk, they are under the same obligations to protect them as they are in the Auckland office. To show a 'Duty of Care' the most basic measure a company can take is a tailored security briefing to those who will be traveling.

Why brief?

Being in business increasingly means traveling to find new opportunities and markets for our products. New Zealand businesses in particular are encouraged to create value that can be exported; and that means sending people to the far flung reaches of the planet to meet different nationalities and create relationships. Kiwi's are generally well traveled and love the idea of setting out for somewhere new. However, it would be naive to think that a trip to Tokyo carries the same level of personal risk as a trip to Togo.

Organisations need to show a 'Duty of Care' for those in their employ and when asking an employee to go to a place with a proven security risk, a travel brief is the most basic security measure that an

organisation can take. It is forearming the staff member with a little bit of knowledge that could go a long way to preventing a tragic or expensive incident.

Deciding the message

There is normally far too much security information on a country to impart to a traveler in any reasonable time frame. Normally the people traveling are pressed for time; meaning that the briefing must be given quickly and effectively. 20 to 30 minutes is appropriate. After this point, remembering important facts can be difficult as the amount of information begins to mount up. Commonly called, "information overload."

Including information on the country that people generally want to know about, like the weather and how much a New Zealand Dollar (NZD) is worth in the local currency, serves to gain people's attention and can then lead onto key security messages. If a NZD is worth 407 Central African Francs, then the traveler could see that flashing a \$20 note in a market could lead to trouble. Kiwi's don't like to think of themselves as being the target of crime - it's hard enough to come to grips with this in New Zealand - so, we treat all foreigners as innocent until proven guilty. This is a great way to view the world and make friends but, it needs to be applied with some common sense caveats.

Other key messages could be cultural and aimed at avoiding offense that may cause a security incident. Such as, attempting to shake a woman's hand in some Muslim countries. Other key security messages might be what forms

of transport to take to avoid injury or robbery or, what the local view of the United States is. Being obviously Kiwi, and not "acting American", can be good during the times when it is dangerous to be from the U.S. or the U.K. in some parts of the world. These key security messages will be the ones that the traveler is tested on, during or at the end of the brief.

Finally, it's good to leave the traveler with one or two specific scams that are occurring in the target country. A bit of research will normally turn up something that combines a new technology, with a locals need to feed their family and a view of foreigners as rich and entitled.

Where an organisation sends staff to many parts of the world, it makes sense to create a programme for corporate travel briefings that is:

- Expected and standardized
- Delivered and assessed and;
- Seeks continuous improvement

Expected and standardized

For security to be effective in any organisation, it has to be part of the culture. People traveling overseas on company business need to see the travel briefing as part of the process; not something new, foisted on them because they are going to somewhere near the equator. Receiving the travel brief should be as normal as getting your tickets and having meetings to determine the trips business goals. Even if the traveler is going to a very western country, the security scene can change. Who would have predicted the several nights of rioting in London that took



*Carlton Ruffell, ASIS New Zealand
Chapter Chairman*



- 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

www.allegion.co.nz



place in August 2011? Having a travel briefing as standard also means that the traveler starts to become acclimatized to the situation in the country they will be visiting as soon as possible. A big part of corporate travel briefs are dedicated to showing the traveler how to avoid giving offense and causing security incidents. The sooner the traveler can inculcate these local social norms, the quicker they will become 'effective' in the business they wish to conduct.

Like any aspect that we wish to make 'standard' in an organisation; support must come from the most senior of management who will state to those below them that staff safety is important and attention will be paid to this programme. It is impossible for a department to implement these measures and expect the authority to 'trickle up'.

Delivered and assessed

With some travelers you could give them a briefing in a powerpoint form to watch in their own time and they would do this. However, in the wash-up after a security event, the organisation would only have the word of the person that they had viewed the powerpoint and, if the worst had happened and the traveler was dead, the company would have no proof that the information had been seen by the traveler. This would be negligence on the part of the company and a failure to show a Duty of Care. This means that the travel brief should be delivered in person or online. If the travel brief is to be delivered online, then there must be a way of verifying that the person

attending on their computer is the person who will be traveling. An intranet system that requires a password to logon, should satisfy this.

Measuring the impact of the travel brief will be of interest to those wishing to keep company employees safe. Typically the security or Human Resources side of the house. By conducting a test, during or after the briefing, organisations can see if the important messages are getting across. For example; drinking only bottled water with unbroken seals will be pretty standard in most parts of the world while prohibitions on homosexuality, alcohol or talking about politics may be crucial to know in specific environments. Testing also allows the creation of metrics for an organisation to see if travel briefings are getting across to the travelers. Could they be done better, faster or with a different delivery method?

If a traveler fails the questionnaire then this should result in a one-on-one briefing with the briefer. The briefer will need to determine if the briefing was pitched at the right level, if there were language or learning difficulties or, if the traveler is not interested in the security aspects of traveling. If the briefer can confirm in this forum that the main messages have been taken onboard, then there should be scope for them to 'sign-off' on the traveler at that point. If the briefer can confirm that the traveler shows no interest in the travel briefing then they should be stopped from traveling until this can be rectified. Some might say that this specific person is the one required to travel but, if an

incident were to happen, the company would be liable twice! Firstly they knew that the traveler didn't want to know about security and then, they sent them anyway.

Seeks continuous improvement

While companies can provide general travel briefings, it is great from an intelligence perspective, if you can get a brief back from the traveler once the trip is complete. Knowledge gained first hand can be very valuable for security and business. For example, in some parts of India you will need to hide your wallet to avoid having your pockets picked. In other parts, you could leave it on a train and a local would go to extreme lengths to make sure it gets back to you. Including searching the hotels where you might be staying! Knowing this could make a difference in deciding which local economy you would have more faith in investing in.

Conclusion

Working behind the corporate travel brief programme are the responsibilities of the organisation. Showing a Duty of Care in some environments will take extra measures. Things like having a company policy on ransom negotiations, specialist medical evacuation plans, using trusted providers to get secure transport and accommodation for travelers and notifying MFAT on where your travelers are and potentially using specialist travel intelligence companies to provide real-time information to travelers and their companies.

by Carlton Ruffell

Better Retail with Data

Beside loss prevention, security cameras and heat sensing devices can give retailers valuable information about store traffic counts, patterns, dwell times and where they need to improve their store layout.

by Hedgie Bartol, the retail business development manager for Axis Communications

With the trials and tribulations of the holiday selling season approaching, there is not much time to research, vet, test and implement improvements to your retail environment.

Many options are available for each type of improvement and its unique architecture and implementation. Although that may seem daunting, what it really means is that with open, interoperable systems, you have the ability to create the architecture for the improvements that will work in your environment most effectively. Several types of security equipment can be used

to determine which areas of your store need improvement. The following top analytics can drive your sales for 2013.

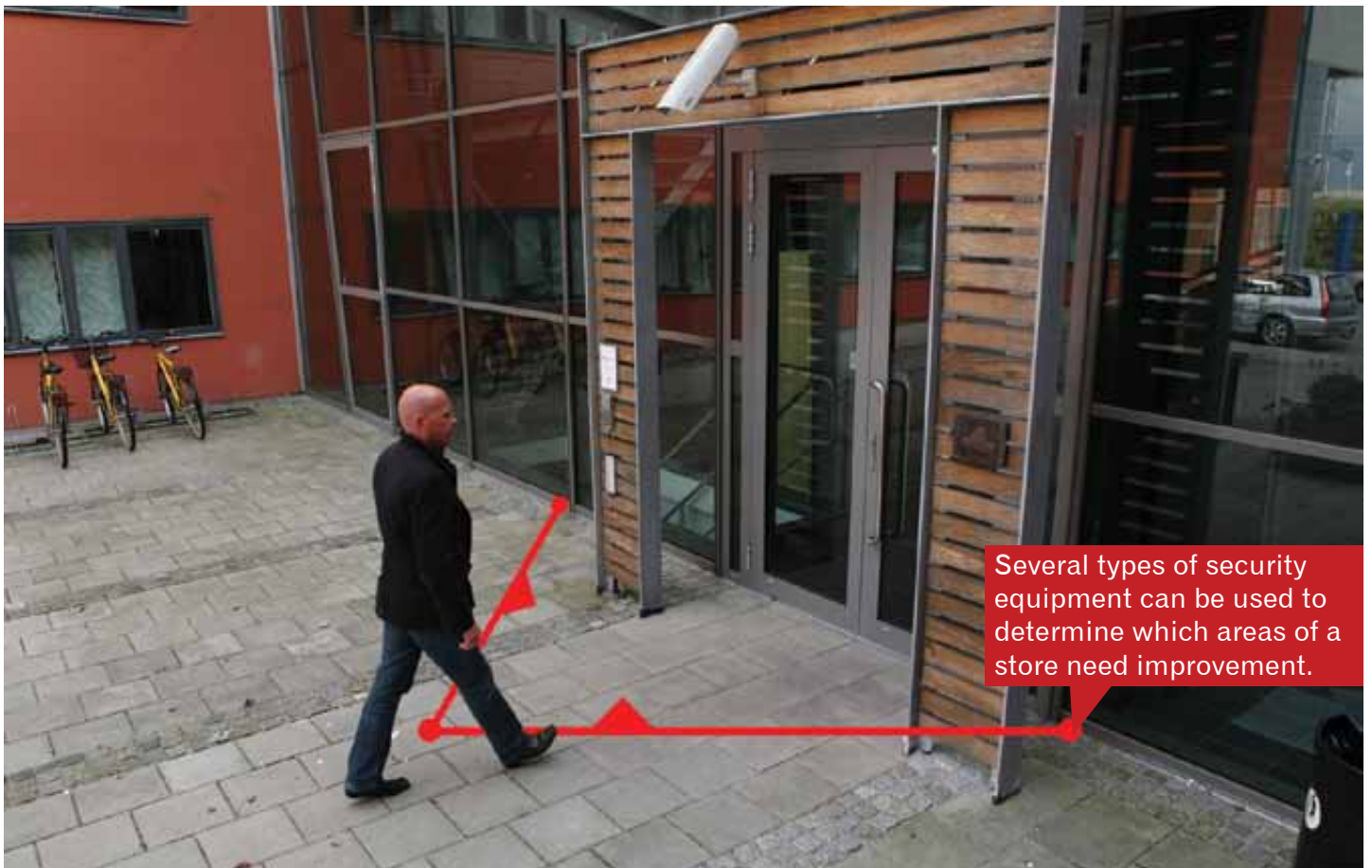
You can count on it

Perhaps the most commonly requested and generally straightforward technology, people counting can help identify what is happening in stores. An effective people-counting solution should allow a retailer to identify the number of people entering a store and compare that to the store's point-of-sale (POS) data for conversion rates.

By using Internet protocol security cameras rather than some traditional

technologies, retailers not only have the opportunity to multipurpose that camera for security purposes, but they also have much greater flexibility in implementation.

Intelligent surveillance can determine the difference between adults and children, be certain that the individual actually entered the store instead of merely crossing the threshold and even have video verification of the activity. Perhaps most importantly, because the cameras are accomplishing this, retailers are not implementing disparate systems but rather multipurposing their investment.



Several types of security equipment can be used to determine which areas of a store need improvement.

Hot or not?

Imagine the benefit of having someone sitting in a store's ceiling, watching and recording everything happening in a store. What would a retailer do with the knowledge of where people are going in the store? What areas are the "hottest" areas and where are the least-active areas? Being able to verify a store design in a quantifiable manner would allow the most effective layout of planograms to be determined to drive sales.

Additionally, knowing where the least amount of activity is could point out areas where people potentially might conceal items, as well. Once again, this multipurpose an existing investment in cameras and utilizes them beyond security.

Keep the line moving

The effective use of staff to serve customers and manage checkout lines and cash registers is critical to customer service and to driving sales. The knowledge of when to open a new cash register and serve the customer keeps a store functioning efficiently and delivering service to drive more sales.

Customers hate waiting in line and the stores that keep them moving through will keep them coming back. Having a system that alerts store managers to lines forming and assists with labour management will streamline operations and enhance the customer experience while driving sales at the same time.

Dwell on the customer

Knowing what displays and end-caps are effective brings huge value to marketing initiatives. By using a dwell-time analytic, retailers can know unequivocally how many people are stopping by displays and for how long.

Presenting that data to vendors can add value to locations with hard data. Once again, use the same cameras and analytic that can warn of a potential theft to pinpoint a customer who is standing for long periods of time in the same area seeking assistance.

No sweetheart deals

Although "sweethearting" may seem like a loss-prevention issue, many times it can be an issue with training. Point-of-sale analytics that identify when items are not scanned properly not only can alert managers to potentially deviant behaviour, but they also can identify when processes are not being followed and a breakdown in operations might occur. Identifying these opportunities can enhance operations and efficiencies at the POS.



Security cameras can zoom in on cashiers, transactions and detect scan avoidance by customers.



Many of these solutions can be tied together into a "dashboard" of sorts. The ability to bring together the data so that retailers can drill down effectively and know what is happening in all aspects of their stores is due to the sheer interoperability of this technology.

Using the data that not only reveals how many people came into a store but also where they went, what they bought, and how effective the store's operations were, can give retailers the knowledge they need to provide and maintain superior operations.

When these systems are used singly or in combination, retailers not only will enhance their operations and drive more sales, but also leverage their investment to increase their security protocols, as well. Multipurposing security cameras adds value to the entire system and gives retailers the knowledge of what is happening in their stores, without having to pull valuable employees out of their roles of customer service.



Hedge Bartol is the Retail Business Development Manager for Axis Communications and a member of the Retail Loss Prevention Council of the American Society for Industrial Security International.

For more information visit www.axis.com

Insulation of commercial walk-in freezers checked with thermal imaging

Enterprises that need to store large amounts of goods at temperatures well below the freezing point of water often install large walk in freezers on their premises. These large freezers are capable of keeping whole rooms full of these goods, usually foodstuffs, at very low temperatures. There is just one downside: cooling requires a lot of energy. It is therefore very important that no outside heat leaks in. To make sure that the freezer's insulation is working properly, thermographers inspect the insulation material with a thermal imaging camera.

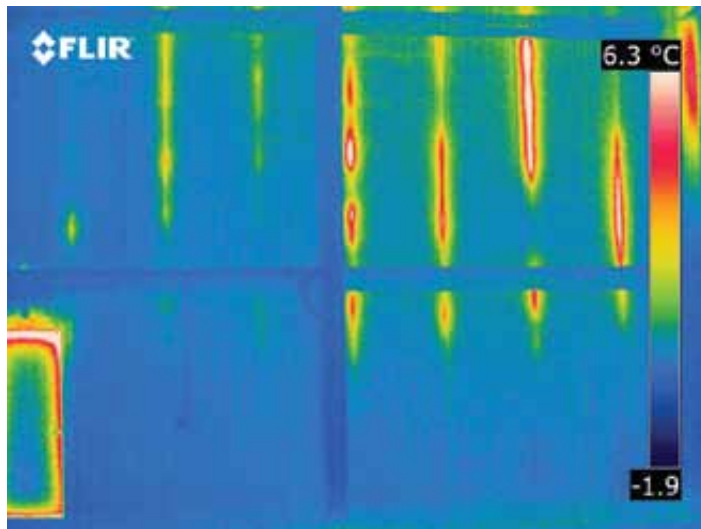
“In essence inspecting walk in freezers, cold rooms and other types of large commercial refrigeration units is very similar to building insulation inspections,” explains Dennis van Est, thermographer at the Uden, Netherlands, based Thermografisch en Adviesbureau Uden. “The only difference is the direction of the heat. With building insulation inspections we generally try to detect heat leaking from the inside of the building to the outside air, but with refrigeration units we want to detect heat leaking inwards. But the mechanism of heat leakage is just the same.”

The thermography consultant is called out to Leeuwarden to inspect two walk in freezers. “If there is any heat leakage this can cause a huge unnecessary expenditure on energy bills,” says Van Est. “Detecting these heat leaks in an early stage allows the owner to fix the insulation defects, preventing soaring energy bills. With the energy prices continually rising, the demand for walk in refrigerator and freezer inspections is also growing.”

Heat bridges

Van Est finds insulation problems in many of the walk in freezers and cold rooms he is hired to inspect. “This particular freezer which I’m inspecting at the moment seems to be very well insulated, but you’d be surprised to see how often newly built refrigeration units have a faulty construction. Sometimes the joints between the insulation panels are not protected properly, creating heat bridges. This can cause a lot of unnecessary energy consumption. In other cases older units might develop insulation faults over time due to wear. In both scenarios the best way to detect these insulation defects is by using thermal imaging cameras. Other methods, like spot pyrometers and such, really are not an option with this type of inspection. It is simply too easy to miss problems that you can relatively easily detect using thermal imaging.”

To Van Est the quality of the thermal imaging camera is crucial for these inspections. “You need high quality thermal images to



Improper welding has caused heat leakage in this section of the freezer insulation, as shown in this thermal image



NEW FC-Series S



Don't call security.
Call FLIR for the complete picture.



Compact D-Series

If your security system is all bells and whistles but can't show you whether it's a possum or a person climbing your perimeter fence then FLIR's new range of thermal imaging security cameras will give you a much clearer picture.

Available in a wide range of performance models including the new FC-Series S and the new Compact D-Series outdoor domes, the FLIR network-ready camera range is now more affordable than ever for your surveillance and security applications.

Whatever mother nature dishes out - blinding sun, fog, smoke, pouring rain or complete darkness - FLIR fixed-mount cameras deliver the sharpest thermal images known to man, day or night.

Here's how:



High contrast scene with standard AGC algorithm applied.



DDE applied – all targets can be observed simultaneously.



Crisp Thermal Images - More pixels allow the user to see more detail in even smaller objects at a greater distance. Choose which resolution of crisp image quality you need: 640 x 480, 320 x 240 or 160 x 120 pixels.



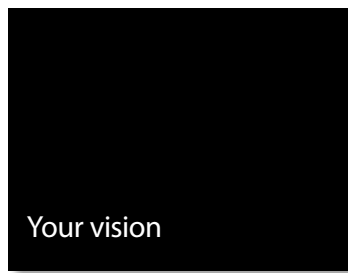
Excellent Range - FLIR thermal imaging cameras can detect targets several kilometres away.



Digital Detail Enhancement - Providing high contrast imagery in almost all weathers optimised for video analytics software.

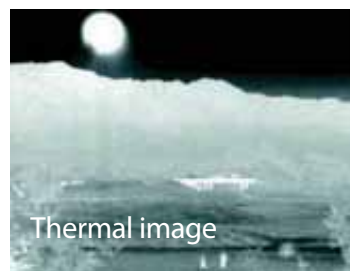


Wide Dynamic Range - Delivering high quality images even when full sun is in the field of view. Ideal for working with video analytics.



Your vision

Thermal image without Wide Dynamic Range (WDR).



Thermal image

Thermal image with Wide Dynamic Range (WDR).

www.flir.com

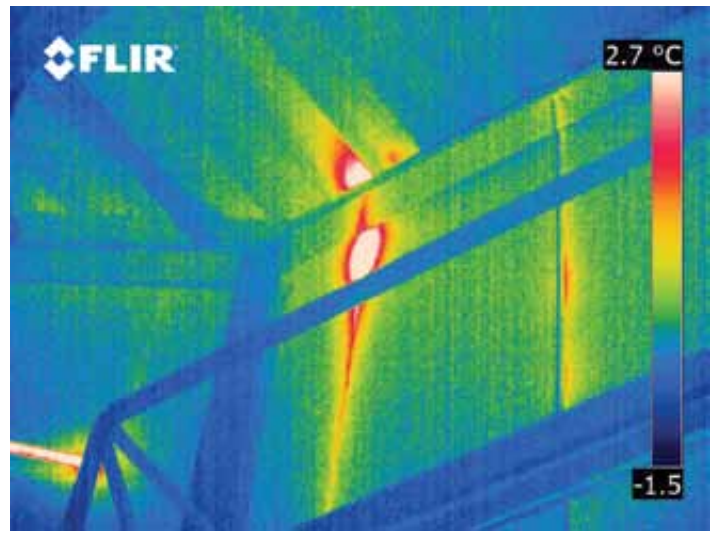
For more information about the about the new FC-Series S and Compact D-Series or any other FLIR thermal imaging camera please contact:

FLIR Systems Pty Ltd. Free Call NZ: 0800 785 492

Email: info@flir.com.au



This thermal image shows an example of improperly connected joints between insulation panels, causing heat leakage



be able to detect warmth bridges in the freezer insulation. The thermal sensitivity and accuracy are both very important, but to me the image resolution is also crucial. You need to be able to interpret what you see in the thermal image and if you are using a thermal imaging camera that produces thermal images at a resolution below the current industry standard of 640x480 pixels then you are missing a lot of information which you need in order to draw the right conclusions.”

Excellent tool

The FLIR P640 thermal imaging camera is an excellent tool for these inspections, according to Van Est. “With an image resolution of 640x480, a thermal sensitivity of 30 mK (0.03 °C) and an accuracy of ± 2 °C or $\pm 2\%$ of the reading the thermal images produced by the FLIR P640 thermal imaging camera are of exceptionally high quality. This thermal imaging camera model is also very user friendly. Especially if you compare it with the cameras of other manufacturers the image quality and user friendliness of the design are far superior. The ergonomic design is also very important to me because you need to prevent back aches and arm strain.”

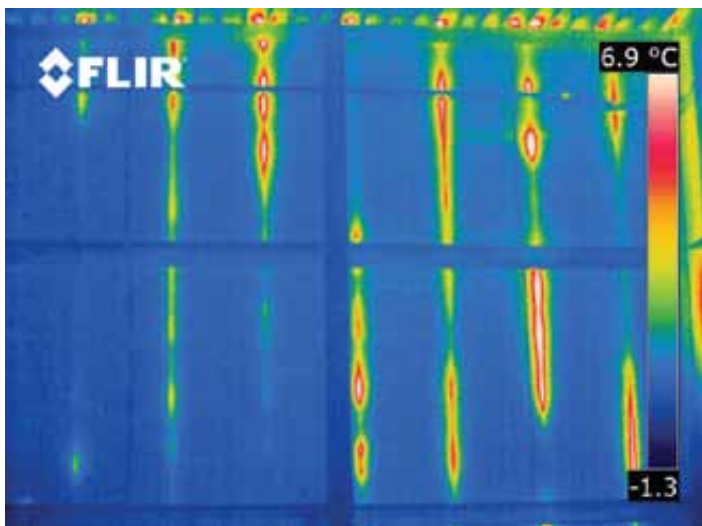
Another important thermal imaging camera feature for this particular application is the calibration range, says to Van Est. “The FLIR P640 thermal imaging camera is calibrated to a minimum temperature of -40 °C. This is very important to allow accurate temperature measurements. Most freezers are kept at

a temperature between -20 °C and -30 °C. However, even at temperatures just below the official calibration range, such as some exceptionally cold freezers that cool down their contents to -50 °C or even -60 °C, the FLIR P640 thermal imaging camera is still quite capable of visualizing insulation leaks.”

The importance of training

A good camera is just half of the solution, however. “Although the quality of the camera is extremely important, the knowledge and skill of the thermographer is just as important,” says Ralf Grispen, Commercial Manager at Thermografisch en Adviesbureau Uden. “We therefore make sure that all of our inspectors have at least a level I thermography certificate from the FLIR Infrared Training Center (ITC) and preferably level II as well. For us this is one of the reasons why we chose FLIR: not only are the thermal imaging cameras of the highest quality; the accompanying training offered by the ITC is also very good.”

“High quality thermal imaging cameras and good training come at a price, but they are definitely worth the money,” concludes Van Est. “We have several FLIR cameras and they are used for a wide variety of applications, including inspections of building insulation, industrial maintenance inspections, HVAC systems, airplane composite materials, water ingress and refrigeration units insulation inspections. In fact these cameras are almost constantly on the move from site to site.”



This thermal image shows heat leakage due to improperly connected joints between insulation panels, causing a lot of unnecessary energy consumption

To find out more about
FLIR Systems and our
product range go to:

www.flir.com or

Phone: 0800 785 492

Email: info@flir.com.au



Intelligence EVOLved.



HID Global's next generation IP-based VertX EVO™ provides the most comprehensive and scalable solution that leverages enterprise networks for building access control.



The VertX EVO™ controller platform combines superior performance with enhanced security and a powerful rules engine to deliver an extended range of advanced and future access control functionality, including interoperability with wireless locks. The open-architecture solution addresses the growing range of customer requirements for building access control, PC logon, and complimentary applications including fire alarm and closed circuit television (CCTV), while ensuring 100% plug-in interoperability with existing HID access control systems and seamless migration from first generation VertX®.

For more information on VertX EVO, visit hidglobal.com/evolved-nzsec or contact us at +64 9537 0279 or email at asiasales@hidglobal.com.

© 2013 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID logo, the Chain Design, VertX and VertX Evo are trademarks or registered trademark of HID Global Corporation/ASSA ABLOY AB in the United States and in other countries.

Loyalty Card Production Enabled with HID Global Printer/Encoder

AwardWallet's OneCard Relies on the Efficient FARGO® DTC4500 Printer/Encoder

AwardWallet LLC provides a free service that helps consumers manage and track loyalty programs, including air, hotel, car rental, and credit cards.

AwardWallet also helps people keep track of award-program balances by accessing program balance information, aggregating data from the various loyalty programs, and then making the information easy to use for the card user.

The company's robust system tracks 432 loyalty programs, roughly four times more than any competitor. More than 82,000 active members depend on AwardWallet to manage over 15 billion miles/points representing \$304 million in value.

By notifying members when their balances change and before their points expire, members can stay on top of their travel assets with minimal effort.

“Every time I use the printer, it blows my mind at how easy it is to produce the cards.”

The Challenge

The average AwardWallet member belongs to approximately 10 loyalty programs. Some belong to as many as 60. Before AwardWallet, carrying around cards and keeping track of the information for every loyalty program was burdensome and ineffective.

AwardWallet's solution is the OneCard, a credit card-sized plastic card that lists up to 30 different loyalty program accounts on a single card. The OneCard also has a magnetic strip that enables users to check in for flights at airport kiosks without using their ID or credit card.

With the introduction of the OneCard and the rapidly growing user base, AwardWallet needed a way to print and encode these cards cost effectively and efficiently.

The Solution

AwardWallet's executives evaluated four printers, including HID Global's FARGO® Direct-to-Card (DTC) printer/encoder; the FARGO DTC4500 was recommended by AwardWallet's security systems integrator, IDESCO Corp.



Top Reasons Why AwardWallet.com Chose HID Global FARGO DTC4500 Printer/Encoder:

1. Robust printer that integrates with existing systems
2. Low cost per print
3. Fast print speed
4. Double-sided printing
5. Ease of use

Introducing Allegion

In early December 2013, Ingersoll Rand Security Technologies will spin-off from Ingersoll Rand to form a new security business; Allegion. The name represents the collaborative, long-term relationships the company forges with customers. It embodies the company's team of experts and their relentless commitment to safeguarding people and property. There will be no change to the high level of service you currently receive from Ingersoll Rand, and no change to the portfolio of strategic brands including Briton, CISA, LCN, Legge, Schlage, and Von Duprin.

The future is bright for Allegion

We are a company with a history of intelligent and industry-defining products. Our people take great pride in putting the customer at the centre of everything we do and have a problem-solving spirit and eagerness to tackle our customers' toughest security challenges. As a global enterprise, we will continue to lead the industry in defining and raising the standards for safety and security everywhere.

The future demands a company that understands the security landscape inside and out. It demands people who can help customers adhere to codes and standards, because they help advocate for and raise those security standards in the first place. Above all, it demands a company that will speak out for safety and security everywhere.



ALLEGION™

That's us. That's Allegion.

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



programmers control over all the features that the company would use, including setting controls for card printing and encoding, diagnostics, upgrades, audits and enabling printer security.

- ◆ **Simple to use.** AwardWallet provides its services to members with a staff of fewer than 15 people. Therefore, it was imperative that the printer be easy to use. The FARGO DTC4500 required only a few quick, simple steps.
- ◆ **Low cost per print and fast print speed.** When compared to the other three printers, the FARGO DTC4500 featured the best cost per print and was the most efficient, which was a critical factor for AwardWallet and their ability to meet the growing demand for OneCards.
- ◆ **Ability to print on both sides of the card.** Many members have so many loyalty programs that a one sided card does not hold all their information. Dual-side printing was a must to serve AwardWallet's clientele.

AwardWallet found that with the DTC4500 printer, they could produce professional-quality, full-colour ID cards with security encoding – all in one print transaction. In one pass, the device can print, encode, fluorescent print, and laminate security cards, single- or dual-sided, in less than half a minute per card. They also found the printer easy to use, and it integrates seamlessly with existing IT networks and databases.

AwardWallet selected the FARGO DTC4500 printer for the following reasons:

- ◆ **Ease of integration with existing system at AwardWallet.** The DTC4500 printer's software gives

Schonzeit, IDESCO Corp. "It's a robust printer that can handle a large volume of card printing while still maintaining the highest quality."

"We're growing rapidly and expect to hit 100,000 users by early 2012," said Alexi Verschaga, co-founder at AwardWallet. "Our supply is quickly depleting, so we just ordered ten thousand more OneCards for our growing demand."

Results

With the HID Global FARGO DTC4500 printer, AwardWallet can produce the new OneCard for their growing customer base, some of whom order two or three OneCards for the entire family. The FARGO printer can keep up with the demand for the OneCards at a low per-card cost, which also enables AwardWallet to continue offering the OneCard as a free value-added service, even as the company expands and keeps track of over 15 billion miles and points for its members.

"Every time I use the printer, it blows my mind at how easy it is to produce the cards," commented AwardWallet's Alexi Vereschaga. "I quickly and easily print cards that not only look very professional but also contain the data that enables our clientele to manage their many loyalty programs."

"Because AwardWallet is anticipating printing upwards of 10,000 cards per year, the best solution out there is the DTC4500 FARGO printer," said Andy

Retail security – who can you trust?

By John Lazo-Ron

New Zealand's retail industry has been one of this country's more booming industries for quite some time.

Shopping for clothing, white ware, electronic devices, jewellery, kitchen ware (the list goes on), is a year round occurrence for Kiwis, and to be quite honest, if there weren't four public holidays where retail weren't legally allowed to trade, retail shopping would be a consumer action that basically never ended.

Even during recent economic hard times, retail still managed to lure thousands of people and their wallets through thousands of stores' doors each day and gets them to spend their money on a wide range of products, with renowned stores such as The Warehouse, JB HI-FI, Glassons and Dick Smiths (to name a few), not only having what people today need... but also what they want.

However, despite the millions of dollars being poured into retail tills around the country by the day, the industry is also losing large sums every day due to a very significant problem that has been around since the first retail store on this planet opened its doors – shop theft.

Shop theft has been a major thorn throughout the global retail industry for decades and is one matter that is not getting any better here in New Zealand.

In spite of improved security technology and employees increasingly being made more aware of this major problem, thieves still manage to get electronically tagged items into their bags and walk through detectors at the door without a noise being made; they still manage to be in and out of a store so quickly with a bag filled with stolen goods they aren't even noticed by staff; and they are so on the money that they know how to avoid getting their shoplifting acts from being caught by security cameras.

And if dealing with these thieves wasn't already a handful, what has made matters much worse for the industry is that it's also had to start combating a rising dilemma

that is internal theft, where many retail staff around the country are basically taking much more from the companies they work for, than they've actually earned.

Spokesperson for the New Zealand Retailers Association Barry Hellberg told the New Zealand Security Magazine that external and internal shop theft has really hurt the retail industry over the past few years and believes the recent economic recession has played a major hand in that.

"Shop theft in its broadest sense is a huge problem," says Hellberg.

"In summary, customer theft and employee theft is estimated to cost retail between \$1-2 million a day in lost sales. If you take an average of \$1.5 million and multiply it by the 361 and half days that shops are legally able to be open, you get a total of over \$500 million in lost sales annually.

"Is it getting worse? I believe it is. In times of economic recession where people are unemployed, the temptations to do things which people wouldn't normally do are enormous. So we've had some challenging times in recent years, particularly in times where people just don't have enough money to meet their requirements. So it's a constant problem and you'll probably see more incidents of it happening leading up to Christmas than in other times."

The broader theft crisis hasn't made things any easier for a retail store owner/manager who now not only have to keep their eyes firmly on the customers that come into their shop, but also on the people working for them.

One manager of a well-known retail store, when approached for comment by New Zealand Security Magazine would only comment if she could remain anonymous for her own safety and security, said the shop theft issue in her store was "quite bad".

She said the store gets 'hit' at least three times a week and that it had got to a point where it had become an extremely difficult

issue to control, especially when she had no doubt the majority of shoplifting from her store was not from the odd school kid who's looking to get something they can't afford, but very much organised crime-related.

"Oh [shop theft is] definitely pretty bad in this store," she says.

"We get scoped out and hit by the gangs quite a lot here. It tends to happen more around weekends, school holidays and Christmas, but there's definitely a black market and we call them the professionals as they definitely know what they're doing."

She said there would always be at least two people working in tandem with a specific plan. First, one would enter the store with the objective of trying to distract an employee away from a certain section of the store where the target items are. Once they did that, another would quietly enter the store to that open free section to take those target items while the employee has their back to them.

"It happens all the time," she says. "It's almost impossible to stop, especially when we normally only have one person on at a time. One time I quickly went to the bathroom and by the time I got back two expensive items had already gone missing! My cover had just started so as I said, [the shoplifters] know what they're doing and know when it's the best time to hit."

The incidence of shop theft started to rapidly increase within the store when they started selling certain extremely popular 'designer products'. She says they are the "it" products, what everyone wants, so demand for these products has always been high which is also why they have become the most popular target for shoplifters – and it has cost the store heavily!

Figures from the store's latest stock take, which they do every six months, are mind blowing, with the store having lost close to \$10,000 in sales and over 500 items during that period – and those figures are just for the designer items!

"I was extremely shocked when I first saw those figures because I honestly didn't think it would be that bad," says the store manager.

"I instantly thought how all that money could have gone towards my budget. That it could have gone to the year's sales figures. But it all simply went out the door because of theft."

She has tried to combat the problem by moving the designer items closer to the counter. The store mirror is also close to the counter which makes it easier for staff to see the items if they were assisting someone away from that section.

She also says her staff generally tends to stick by these designer items and not move, which she advises stores should always do with their 'in demand' products. The store also does bag-checking if they suspect someone may have stolen something.

However, despite the procedures in place, she admits she still hasn't caught one shoplifter thus far.

Also, because she knows the theft is gang-related, it has made it extremely hard for her to say something to someone she suspects may be stealing as she believes doing so could have consequences in regards to her safety.

"I don't tend to say something as I don't want to falsely accuse someone and risk my own health and safety, as I know for a fact other managers have been threatened before," she says.

She also mentioned she wouldn't go after a shoplifter unless she had a security guard with her because she doesn't know who could be waiting for them when they got to their 'take-off' vehicle.

"It's definitely hard because in the end they would be walking away with my stock, but my safety is definitely more important."

As you can see, the store has a big external theft battle on their hands, but their battle with internal theft has been just as big with staff now getting in on the criminal act.

Fraudulent refunds – where staff are doing false refunds under customer's names and collecting the money; False lay-by's – where staff will put on false lay-bys just so it looks like they've made their budget and will end up collecting their monthly bonus; and then giving staff discounts to others – are the main issues she's dealing with.

The manager says it had become "that bad", regular checks on staff were now done on a weekly basis.

"To be honest internal theft boggles my mind more than external theft because I just don't see how anyone could do that to my company. We are well looked after and have been given a job in the first place. It's unbelievable."

Regardless of all the theft problems, she says she still loves her job.

Also, if there was any more advice she could give to other retailers, she would say, "Train staff well. Make sure they have 360 degrees vision at all times; know where the stores blind spots are; stick with customers

all the time, and don't assume that a person isn't a shoplifter because they probably are."

The New Zealand Retailers Association have advisors on their staff purposely to give advice to combat this issue and retailers seeking advice on how to deal with theft, go to www.retail.org.nz.

NZSA Qualification Badges to Provide an Additional Incentive for Training

The new security industry mandatory training, sets a minimum standard for industry; however learners engaged through NZQA qualification based programmes that contain additional units, may also achieve recognition through the award of an NZSA Badge.

The initial white badge will be awarded on completion of a 20 credit limited credit programme (LCP1); as staff continue to progress onto the National Certificates (Level 2 – yellow badge etc) and above they will be awarded higher level badges, up to a black badge for the Level 6 Diploma.

For many in our industry this will be their first success in achieving any qualification, and this badging system will encourage engagement in further

training through the qualification pathway, therefore raising overall industry professionalism and standards.

For employers, and end users of security services, the badging system will enable an instant visual guide as to the skill sets of staff.

This initiative has been well received by NZSA members, Skills Org, The Ministry of Justice and the Police, who all see it as a positive step in professionalizing the security industry.

The NZSA will be investing heavily in the promotion of this badging system nationally, with the intention of it becoming the default recognised standard.

For more information go to: www.security.org.nz/education_training.php

NZSA Qualification Badges



LCP- Limited Credit Program



NZQA National Certificate in Security Level 4



NZQA National Certificate in Security Level 2



NZQA National Certificate in Security Level 5



NZQA National Certificate in Security Level 3



NZQA National Diploma in Security Level 6

Chairman's Annual Report - 2013

I would like to thank the current members of the Executive who have given their valuable time to run this voluntary organisation in 2013. Jeff Brown CPP our Deputy Chairman, Chris Martin our Treasurer, Chris Lawton our Secretary and Alistair Hogg CPP our Regional Vice President. I'd like to single out Chris Martin for his efforts over the last two years in the area of Treasurer. He is unable to continue in this role in 2014. He has really bought our accounting processes up to speed and the person who follows him will have a much easier job to do. Chris has stated that he will provide any necessary support to the person who replaces him and for that, myself and the rest of the Executive, we thank him.

I'd also like to say a particular thanks to Charles O'Donnell who represented ASIS New Zealand at the Crime Prevention Partnership Forum. Having attended one of the meetings I can say that he is having a dramatic effect on this organisation; making it focused and making it work for the attendees organisations, not just the attendees.

Michael Pepper CPP. PSP. continues to do sterling work for ASIS New Zealand and our Chapter website again won the International Website of the Year Award (Group 4) for the fourth year running. His efforts there and in the general organisation of the Chapter are greatly appreciated.

Chapter Business Meetings

This years theme of Physical Security Professional has proved popular with the Membership. Meeting numbers have been consistent where these presentations have been made. I would like to thank all those that have presented at ASIS meetings this year. Their expertise and time are valuable resources and it's great that they can share them with us.

Annual Seminar and Exhibits

In June the Chapter held the draw for the free registration to the Annual ASIS Seminar and Exhibits that was held in Chicago, Illinois in September. Tony McLeish of Intellisec Ltd won this prize,

which came with three thousand dollars towards flights and expenses. I am very appreciative of the membership for passing the rule change at the last AGM to make this prize possible. Harder economic times have made giving away the free registrations to seminars difficult so, the ability to give cash support with this prize has made a great difference to people accepting.

ASIS International Presidents visit

In August we saw the visit of the International President of ASIS, Geoff Craighead CPP to New Zealand. The visit of the President was an honour and the Executive worked to use this to the greatest advantage possible; given that he and his wife Sarah had only one day in the country. After resting following an overnight flight from the United States, Mr Craighead delivered an Executive Briefing on his specialist topic of high-rise security and fire life safety to invited guests at the KPMG offices in the Viaduct, Auckland. The session was very interactive with Simon Davis, senior New Zealand Fire Service Engineering Manager, discussing developments in this country and Mr Craighead sharing his experience of over 25 years protecting high rise buildings. Aashmita Naikar, Risk Manager for Auckland City Council attended the event and was the lucky winner of a signed copy of Mr Craighead's encyclopedic book; *High-rise security and fire life safety*, third edition.

That evening the Chapter held a dinner in Mr and Mrs Craighead's honour at the Sofitel on the Viaduct. Mr Craighead delivered an excellent presentation and a draw was held to pick the winner of a free registration to the ASIS Asia-Pacific Seminar and Exhibits. This prize also came with three thousand dollars towards flights and expenses and was won by Warren Cornor CPP, who is also the Shadow Deputy Chairman for the Wellington branch of ASIS NZ. The event was really well supported by the Membership, some of whom traveled to Auckland to attend. The food and drink was of a very high standard and the

kitchen even delivered a masterpiece in the form of a vegan, gluten free dinner for one of our guests!

Membership

I have failed to achieve my goal of increasing membership to 200 during my tenure as Chairman. Likewise, our organisation still lacks diversity. The Executive of the next few years will have to collaborate strongly in order to decide what our organisations 'value proposition' is and, who will benefit from it. Our organisation may then have to let go of historic norms in order to appeal to this new group.

Personally, I see ASIS New Zealand as the natural home of security managers. To my mind, security managers should be constantly aiming to increase their knowledge and skills and to show this through internationally recognised certifications. These managers should be a senior part of an organisations leadership team and handle the Business Continuity, Risk Management and certain Compliance portfolios. They should meet in a corporate setting and these meetings should be professionally run with the option of connecting online. If we can create this environment and 'brand' then increasing the membership and diversity will follow.

Certification

This year 4 Members and one non-member sat Certification Exams in Auckland. I hope that in 2014, even more Members will take advantage of the learning and recognition offered through ASIS International Certification. Having senior members of the organisation taking study groups and mentoring those sitting has helped increase our numbers taking this exam.

Conclusion

Thank you for allowing me to be the Chairman over the last two years. If our Constitution had allowed it, I would have carried on in the role. I look forward to supporting the new Chairman and Executive in 2014.

Carlton Ruffell CPP. PSP. Chairman ASIS Inc - Chapter 148 ASIS International

NZIPI AGM

The New Zealand Institute of Professional Investigators (NZIPI) held its annual conference in Rotorua on 9 November at the end of a full days workshops. By way of background the NZIPI was established in 1988 at a meeting in Palmerston North and some of the foundation members remain active today with three on our current committee. Although this means that technically our AGM was our 25th, indeed the NZIPI was the evolution of what was first established as an Association in 1982 by 6 members. Phil Roigard our newly elected Vice Chairman was one of those first 6 pioneers.

There are a few special projects planned for this year and it was pleasing to see members take up committee positions to allow specialised working groups to ensure the tasks are completed. An example of our combined strength is evident when you look at a few of our first time committee members.

Stu Bailey, a former detective and well know investigator with 25 years' experience covering the Waikato and Bay of Plenty. Stu is a legend in our numbers known for his interview skills and attention to every detail specialising in catching insurance and commercial fraudsters.

Charlotte Stevens, with over 30 years in law enforcement and investigation, 20 years as a detective in the Metropolitan Police Service in London. The last 10 years in London was spent on the Flying Squad and Regional Crime Squad specialising in combating organised crime. Following her move to New Zealand Charlotte was an investigator with the Serious Fraud Office dealing with complex fraud investigations and now has her own business based in Auckland.

Rod Moratti, has been a PI since 1989 and runs a successful agency specialising in background enquiries, domestic and surveillance work.

Workshops

Detective Inspector Rob Duindam from Police National Headquarters started our day off with a discussion on the industry relationships and the Crime Prevention Partnership Forum. Rob reported progress

This year's elected Committee is

Chairman	Ron McQuilter	Paragon New Zealand.Com Limited
Vice Chairman	Phil Roigard	Risq New Zealand Limited
Secretary	Robyn Robertson	Paragon New Zealand.Com Limited
Treasurer	Charlotte Stevens	D'urville Solutions Limited
Committee	Mike Campbell	Advanced Investigations
Committee	Kevin Dooley	Dooley Associates Limited
Committee	Rod Moratti	Moratti & Associates
Committee	Rob Nicholl	Westland Investigations
Committee	Stu Bailey	Key Investigations
Committee	Brian Goodwin	Ashburton Investigations
Committee	Nick Thompson	Thompson & Clark Investigations Limited

on matters we had previously addressed and was interested to hear from our members on their interaction with Police, good and bad. It is fair to say that our profession has come a long way since the 1980's and our relationship with police at national and local level is in great shape.

Mike Campbell then ran a session on dealing with clients from the very first contact, through dealing with the investigation itself and including the importance of reports and then maintaining ongoing relationships. Everyone joined in and learned something, many had their own ideas to share that demonstrated the professionalism that exists.

Bruce Couper from Risq Consulting travelled to Rotorua and gave a presentation on the PEACE interview methodology of investigation. This method of interview is becoming the only accepted model in most countries including New Zealand.

Phil Roigard ran a session on mobile surveillance; the tricks and the tips; the rights and the wrongs.

Nick Thompson put on a fascinating demonstration of the advances in CCTV technology assisted by two industry technical experts who set up live demonstrations and brought a variety of equipment that can be used by investigators static and in remote locations. It is fair to say the advances in covert CCTV using wireless equipment can only assist our members and in turn our clients.

After our AGM, our day ended with a networking dinner

In summary, NZIPI is in great shape and our members have rallied to ensure that NZIPI maintains its reputation as the industry body for professional investigators with many special projects ahead and a stronger than ever committee.

I am sure that this year, NZIPI will continue to grow with new members already starting to apply from other sectors. The criteria for joining is that an individual must be engaged as a professional investigator in our fields of work as their main occupation, having a PI licence is not necessary.

Ron McQuilter, *Chairman NZIPI*



Ron McQuilter is the current chairman of the NZIPI and is Managing Director of Paragon Investigations

*Ron can be contacted by email:
Ron.McQuilter@paragonnz.com*

Interview with Colin Slater

Partner, Risk and Controls Solutions, PricewaterhouseCoopers New Zealand

Colin Slater joined PricewaterhouseCoopers (PwC) as Security and Technology partner in 2011. In January 2012 he released an opinion piece titled *Tentacles of cybercrime a real threat to blasé NZ businesses*, in which he observed that businesses had a long way to go to protect their interests against cyber crime.

Business leaders and public institutions, stated Colin, “aren’t doing enough, or in many cases anything, to protect their interests as digital crime becomes easier”. In the face of increasing cyber threats, businesses were scrambling to remove traditional security measures to maximise sharing and agility, adopting an “act now, think later”, approach.

In this interview, we ask Colin to what extent – if any – this has changed.

Colin has 17 years of IT security experience both in the consulting and delivery of a variety of project areas, the last 12 years in the local market. From a

background of developing encryption and real-time software in the marine surveying industry, Colin has worked in diverse areas of system development and consulting. He has held senior positions in The National Bank, Sytec and The Risk Advisory Group.

In 2005, he founded Securify NZ Ltd to provide independent IT security and risk management advice, which merged with PwC in 2011. At that time, Securify was credited with being the brains behind a number of major security design and deployments, including an online lottery system and major electricity control systems.

NZSM: In your January 2012 opinion piece you were of the opinion that NZ businesses were blasé in relation to the threats posed by cyber crime. Do you still believe this to be the case, and why?

Colin: Since January 2012 a number of factors have changed. As a direct result of a number of highly publicised incidents there has been a significant focus on security, privacy and risk in the Public Sector, which has also had some knock on effects in the Private Sector. While this focus is long overdue, I still think there is a danger this considerable activity will not result in long-term change, mainly due to the approach that has been taken.

In 2012 we could see the lack of investment and generally lax approach to risk management as a whole, while it would be nice to think that the drive from Public Sector will change that, our observations is that some have taken a very tactical approach and are just addressing short term issues. Our Global Information Security Survey has reported the same issues for the last few years - little investment in strategy, reactive point approaches to issues and challenges measuring the investment return.

Has it changed? While consumer computing has taken over with most

people using smartphones and tablets this has implications for business computing as expectations are high and the requirement to be able to ‘do anything, anywhere, anytime, safely’ poses a serious challenge for all business - private and public sector.

Fundamentally, I still think there is a large amount of PINT theory - Pretend It’s Not There, as the real risks, what they mean for business, how you react and the ultimate impact are so poorly articulated and understood that it’s easier to think it won’t happen to you.

NZSM: Is New Zealand any different to anywhere else in this regard?

Colin: Yes and No. New Zealand has an interesting record in corporate fraud mainly I think due to societal factors such as the small population and the intrinsically trusting nature of Kiwis. This makes no difference whatsoever in the global business environment where we are exposed to exactly the same risks as any other connected country.

Our general view still seems to be that as we are geographically distant then some dissipation of risk happens as a consequence of this. We see exactly the same technical and business risks as our global counterparts and the lessons we learn in New Zealand are applicable all round the world, in fact we seem to be slightly ahead of the curve in certain areas which again will be as a consequence of being a small, nimble, democracy with significantly smaller budgets.

From a purely IT perspective we rely heavily on outsourcing in New Zealand, but still don’t do the basics in terms of asking the right questions to ensure our data and systems are managed securely. For some reason it’s assumed that when you outsource systems and data the provider cares about it the same way you do and the minimum first step of being clear on what is important seems to be missed way too often.



Colin Slater Partner, Risk and Controls Solutions, PricewaterhouseCoopers New Zealand

NZSM: In your view, has the cyber crime threat increased or diminished?

Colin: Cybercrime has definitely increased, but our awareness and ability to not only measure but understand it has also massively increased. Again, the leakage from consumer computing to the business environment means that people are exposed to the same risks outside work as they are inside and this crossover helps and hinders the efforts in thwarting cybercrime.

Truly organised cybercrime, and to a lesser extent hacktivism and similar disruptive elements are now part of the risk landscape and as such need to be thought of the same way as 'normal' risks. Stitching these risks together is where we observe the biggest challenges as the translation of ethereal, hard to quantify and seemingly complex technical risks into the actual business impact is the weakest link.

As we expect more and more services to be available all the time the challenge becomes meshing these risks into the

**Colin's January 2012 opinion piece can be viewed at www.pwc.co.nz/media-centre/opinion-pieces/tentacles-of-cybercrime-a-real-threat-to-blaze-nz-businesses/*

general risk management activities of the organisation.

NZSM: Is there any reason for increased optimism?

Colin: Yes, understanding, managing, treating and mitigating risk, which is what security risks are, has been around for a long time and we need to think about it in these terms. There is no dark art specific to security and cyber risk other than the challenge of understanding the threats and technology you need to be assessing in order to determine the likelihood of something happening.

It can often feel like a never ending chase between the good and bad elements but in actual fact if you adopt a 'back to basics' approach and get the fundamentals in place, then it is much less of a stretch to adapt, respond and react to risks as they are identified.

This basic framework is the part that is most often neglected - if you don't have the structure to manage risks and don't do the basics, then when they are identified

you are in a worse position as the reaction is more likely to be out of step with the threat or issue at hand.

NZSM: Is the threat landscape any different to early 2012? Who and what should businesses be most afraid of?

Colin: Yes some of the technical risks are reasonably exotic but in actual fact these are quite rare. In general terms the threats are always bigger from the inside than the outside.

While it can be hard to accept this, your own people pose the biggest risk to your organisation through even the most innocuous actions.

Privacy of information and the current dichotomy of the expectation of security while not having your privacy invaded will be a long rumbling and difficult to solve. Public expectation has changed, through society, technology and social change, which means that there is a constant tension between the desire to share information balanced with the absolute of privacy.

Blindside: the increasing costs of ignoring the cyber devils within

On the heels of a rough previous 12 months, 2013 was widely forecast to be another bumper year for cyber threats. Of the predictions made in the flurry of reports published early in the year by software, insurance and consulting firms, there was a high degree of consistency: threats growing rapidly in volume and complexity, increasing cyber espionage, terrorist activity and hactivism, and a proliferation of activity on the mobile, cloud and BYOD fronts.

New Zealand's National Cyber Security Centre 2012 incident summary reported 136 cyber security incidents last year, up from 90 in 2011. In an August press release following the passing of GCSB legislation, the Prime Minister quoted the figure for 2013 as 204 and rising. Amy Adams, Minister for Communications and Information Technology, in her 28 May Launch of 2013 National Cyber Security Awareness Week, suggested that this was the "tip of the iceberg".

Within an increasingly complex and threatening cyber security environment, there is wide-ranging opinion on the

sources of the threat. Yet, as wide ranging as it is, popular opinion is linked by its collective externalisation of the issue. Someone else is always to blame. The perpetrators of cyber breaches, we are told, are shady foreign enterprises backed by malevolent states, terrorists developing cyber-weapons of mass destruction, fanatical hactivists hell-bent on undermining the global economy and con artists infiltrating the social media space.

Contrary to this, key reporting metrics indicate that the greatest ongoing cyber danger to New Zealand businesses is our continuing misplaced assumption that threats originate somewhere else or with someone else. What the research is telling us is that the source of our vulnerabilities lies within our borders, within our businesses and – most alarmingly – within our own minds.

Within our borders

According to the NCSC's 2012 incident summary, the bulk (60%) of the incidents reported to the NCSC originated from an overseas source.

Within the national political debate, such statistics give longevity to a post-9/11 discourse that characterizes all threat as alien and pathological. Just last April, John Key reminded us, "there are people within our country who have links to offshore terrorist groups." These people, we are told, covertly attempt to infiltrate and use our science and technology for projects involving weapons of mass destruction.

For some time politicians have presented us with the usual line-up of foreign suspects: unfriendly foreign intelligence agencies, Chinese commercial espionage and Islamist terrorist groups. Yet, as it turns out, what 2013 is revealing to us is that the major cyber espionage threat is more the result of 'friendly fire'. Already this year, the government has been outed for illegally spying on 88 New Zealanders, and intelligence partner, the US, has been exposed for illegal cyber spying on a massive big data scale.

With the recent passing of the GCSB legislation, New Zealand businesses can expect to be further exposed to this type of 'blue on blue' cyber threat. The new

law, states Andrea Vance in the NZ Herald “broadens significantly the powers given to the GCSB to spy on behalf of other agencies”, and it sets no limit on the sharing of cyber intelligence with other countries.

Parallels have been drawn between the new law and the controversial proposed US Cyber Intelligence Sharing and Protection Act (CISPA), which has stalled in the Democrat-controlled US senate amid outcry from privacy and civil liberties groups. Closer to home, the law has been widely criticized as being little more than a vehicle for New Zealand’s ongoing involvement in the ‘five eyes’ security arrangement rather than being a practical enabler for effective cyber security strategy.

Although the legislation now allows the GCSB to provide information assurance and cyber security advice and assistance to public and private sector organizations, just how much of a help the GCSB will be, remains to be seen. As things stand, the bureau is well behind its counterpart agencies in Australia and the UK in engaging with businesses in a genuinely helpful manner.

Within our businesses

Ironically, as much as New Zealand businesses move to protect themselves from cyber incursions and question whether government is a help or hindrance, the reality is that they themselves may in fact be the weakest link.

The Ponemon Institute 2013 Cost of Data Breach Study, which examines the main root causes of data breach globally, found that the main cyber threats faced by business are self-made. Over 37% of incidents involved a malicious or criminal attack, 35% concerned a negligent employee or contractor, and 29% involved system glitches including both IT and business process failures. In other words, malicious attack was the source of only just over one-third of all breaches, with two-thirds attributable to poor in-house procedures and systems.

Telling a similar story, the KPMG Cyber Vulnerability index 2012 found that 78% of Forbes 2000 corporate websites leaked information through document meta-data of potential use to cyber attackers. Banks were the most prolific own-goal scorers, accounting for 30% of all leaks. Other financial, software, technology and telco companies also fared poorly.

Costly blind-spots also exist in relation to procedures relating to the threats posed by employees and trusted business partners. In a 2012 study funded by the US Department

of Homeland Security, researchers found that malicious insiders within the financial industry typically get away with their fraud for nearly 32 months before being detected. Interestingly, non-manager accountants were identified as causing the most insider fraud damage, and they evade detection the longest (41 months).

Of all industry sectors, it is perhaps the legal profession that is most poorly prepared to tackle cyber threats. According to a UK Legal Week Benchmarker study published in May, non-lawyers are far more likely (52%) than law firms (35%) to have a response plan in place for cyber attacks, and they are less likely (35%) to include external cyber security experts than non-lawyers (53%) in their attack contingency planning.

In early 2012, PWC Partner Colin Slater described New Zealand businesses as blasé in relation to cyber crime. He cited statistics indicating that almost 40% of NZ business people hadn’t attended any cyber security training in the preceding year, and that 34% said their organisation lacked an in-house capability to prevent or detect incidents.

Such complacency contributes to the massive costs of cyber crime borne by New Zealand business. In April, Paul Nash of the Department of Prime Minister and Cabinet’s National Cyber Policy Office stated that cost estimates “are hard to verify, but most are in the range of hundreds of millions of dollars”.

Within our minds

The biennial Lloyd’s Risk Index 2013, which assesses attitudes to risk among business leaders across the world, ranked cyber risk as the 3rd highest, up from 12th in 2011. Yet despite this, and as the Ponemon Institute data suggests, there exists a widespread culture of cyber threat complacency and denial among senior executives and within boardrooms across the globe. Why?

Amy Adams “tip of the iceberg” comment in relation to the volume of cyber incidents in New Zealand is probably an accurate characterization due in part to a culture of denial and the associated reluctance of businesses to report incidents. According to the Australian Cyber Crime and Security Survey 2012, an alarming 44% of business respondents across the Tasman did not report cyber security incidents to law enforcement agencies.

Whatever the nature of an incident and whatever its financial implications, the greatest perceived cost of cyber crime is reputational.

The stain of cyber crime is evident in the stigma attached to its victims. Individual victims of such cyber crimes as Nigerian advance fee fraud emails (Dear Sir, We have the pleasure to make this surprising but mutually benefiting business proposal...) are widely regarded as gullible (funnily enough they are referred to in Nigeria by the Yoruba word *maghas*, meaning ‘fool’). Corporate victims are regarded even worse – and often culpable – because the ultimate victims are their clients whose data they have failed to protect.

John Colley, writing for The Guardian, suggests, “embracing a more open dialogue with customers, taking an honest approach when you have been breached and keeping stakeholders updated whenever possible.” It comes down, writes Colley, “to a greater sense of transparency.” Delaying bad news, or having it exposed by someone else, is a proven reputation killer. No one likes a cover-up. It’s a Public Relations 101 no-brainer, yet executives seem to remain willing to gamble their corporate reputations against the statistical certainty that they will eventually be found out.

No one is immune from cyber crime. Statistically, every business will, at some point, fall victim to it. Where a business can set itself apart from its competitors is in developing and maintaining processes to minimise in-house threats and gaps, maintaining systems to identify and respond to cyber incidents and – as a result – being willing and able to openly report on incidents as they occur.

Before this can happen, one needs to embark upon an honest assessment of the threat environment. Identifying the external threats is easy given the number of widely published threat reports available. These make for important general reading, but they tell only part of the story. Identifying the internal blind spots doesn’t come so easily – not for the lack of reports and advice available but for the fact that we persist in externalising the threats to our peril.

Defending against foreign cyber espionage, for example, won’t prevent a crippling customer backlash brought about by a failure to disclose a privacy breach via negligent leaking of information through document metadata. The culprit in this instance is located no further than in the minds of those making decisions in the boardroom.

An assessment of the threat environment begins with an assessment of the threats posed by our own assumptions and attitudes towards cyber security. Step one: look inside, and identify the cyber devils within.

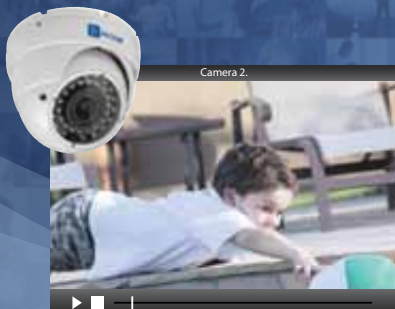
SEE IT. TOUCH IT. RECORD IT.



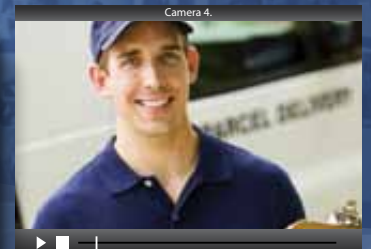
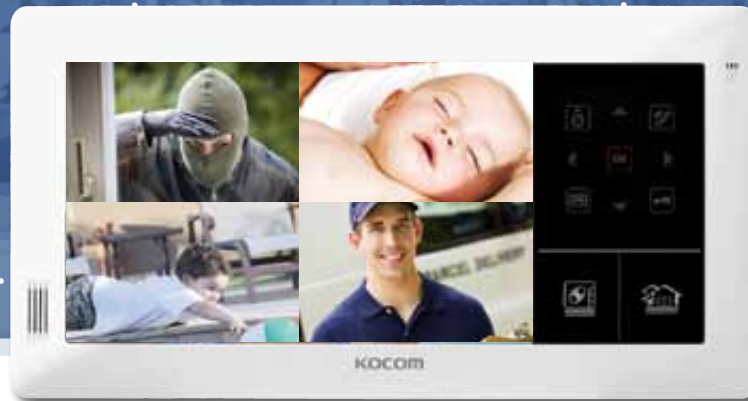
SECURITY



PEACE OF MIND



SURVEILLANCE



CONVENIENCE

KVR-D510 - INTEGRATED INTERCOM, CCTV & DVR SOLUTION



View and record live footage
With a built-in 4 channel (up to 4 cameras) digital video recorder (DVR), you can view and record live footage and playback any recordings.



Digital Photo Album
Turn your intercom into a digital photo album by displaying and sharing your favourite photos.

"Delivery for Mrs Smith"



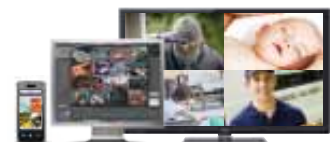
Communicate With Visitors
Conveniently see and communicate with visitors through the intercom feature without opening your front door.



High Resolution Touch Screen LCD
Experience clear images and videos at your fingertips through the wide, 10 inch, touch screen display.



Multiple Storage Options
Supports SD card, external HDD and network data storage options.



Remote Viewing Capabilities
Monitor live footage whilst you're away from home or away from the device through a smartphone, computer or TV.

Available at:

Are you sure your brand is secure?

by John Lazo-Ron

Name, image and reputation – Some of the most influential life details nearly every person in this day and age looks to have.

Whether it's for personal profile, career, and in particular business, having a renowned name, excellent image and great reputation, are factors most would consider vital and essential.

Only when it comes to business, the naming of a brand is not just vital, it's extremely vital and basically all that matters, as in the commerce world what you end up naming your business can simply make or break the life of a company.

A strong name not only gets a business into the game on their particular playing field, and eventually gets them well-known; it's also what lays down the foundation for a business' future success.

Apple, Samsung and Vodafone are



Michelle Calder is an Australian-based New Zealand trademark consultant

just a few of the big companies around the world whose names and icons make a huge impact on today's markets and consumers.

When people want and start looking for a computer, a music device, or mobile phone – some of today's necessities – it'd be fair to say that their names, along with iPad, iPhone, iPod, as well as Galaxy Phones, are at the top of the consumer's shopping list, which eventually brings about the purchase of one of these products.

As a result, a business's brand name plays a significant part in a business's success.

For that reason, with brand naming being such a crucial aspect to a business, having your brand name legally secured is one of the most important and wisest decisions you can make when starting up a business; as the last thing you'd want is someone taking your brand name or idea and using it for their own business benefit.

However, despite brand security being exceptionally fundamental to a business, its one element many business owners surprisingly don't look into and sooner or later experience heavy costs and consequences.

And it's not the big companies that end up paying the price for their lack of security by having their name, brand or reputation stolen or misused (as they normally have the strong legal teams that take care of that side of things), it's the smaller businesses who suffer and are more at risk - and it actually happens more often than you would think.

One of the biggest legal matters that has a tendency to pass by significantly under the radar is brand security.

A recent survey of 30 businesses in the Wellington area found that only one sole trader had trademarked their business, while close to 90 percent of the un-trademarked traders surveyed were under the belief they had brand protection just because their business was registered.

Australian-based New Zealand trademark consultant Michelle Calder says countless cases concerning businesses fighting others over the rights to a specific brand name, reputation or product, take place on the legal scene on a daily basis.

You simply just don't hear about them as brand security is an issue that won't normally get the media excited unless it was a case that involved a major company such as Samsung or Apple.

Calder, who has been practising in trademark law for almost three years (two years within the NZ government and one in the private sector), says during her time in practise, she has seen numerous businesses steal other business' names, while at the same time working and reaping off their reputation and getting away with it. She also said people constantly come in asking if a particular business they've taken an interest to has been trademarked, so if it hasn't, they can snatch it up for themselves.

"There are so many traders who don't want to put in the effort of marketing and building up their reputation, so what they will go and do is basically copy another brand," says Calder.

A guide to getting a trademark and some interesting facts

- When you start a business and come up with a name, do your homework (Google search) and see what else is around.
- Always keep that name close to your chest.
- Visit a trademark consultant or IPONZ and get them to do a preliminary search to see what other trademarks are out there so you are fully aware of similar brand names or trademarks.
- Then ask them for advice of what you can do so you have a full idea of what you're getting into.
- There are 45 different classes of trademarks between goods and services.
- In New Zealand you can apply for a 'combination mark' which allows you to have a logo.
- You can also trademark unique smells (smell marks), shapes (shape marks) and sounds (sound mark).
- Trademarks last for 10 years before they need to be renewed.
- Trademarks are a form of property and add value to your business.

"We had one guy come in recently who said he liked another guy's business and wanted to copy it so he wanted us to see if they had protection. Luckily for that business they did have trademark protection so that guy wasn't able to do anything, but wanting to copy other trader's businesses happens a lot.

"Other traders will simply come in the side, do something very similar to another business as well as have a similar logo and name and also make their website to look the same. And if the business they're copying isn't trademarked, they'll do it themselves, and it happens every day!"

One recent case Calder used as an unfortunate example and described as 'heartbreaking', was a client her boss was dealing with who lost everything because he hadn't trademarked his business.

Out of nowhere another trader started using his brand name and had gone ahead and also trademarked it. Once they had done that they dealt the killer blow sending a Cease and Desist letter to him – a Cease and Desist being a letter a lawyer sends to another party on behalf of their client informing them of their infringements – and demanded that he stop trading under that name, despite it originally being his business name and idea...and there was nothing he could do about it.

Calder says the man was in tears as it was his livelihood and that they tried everything they could do get his business name back, but it was simply too late as he had no protection, so there was nothing they could do.

"We feel for people like this and this is what motivates our firm in particular to protect people," says Calder.

"It doesn't matter whether they're a multi-national firm or a sole trader, everybody needs to protect their trademark and their brand because we don't want to see people like that in tears."

Calder did say that people can have common law rights where they can fight for their name through litigation, but she admitted it was a costly and time consuming process where there are no guarantees.

Calder also mentioned that business owners can be a little naive at times, with many believing another business that has a similar name and service, but is based out of their city or town, will be of no threat to their business, therefore not seeing the need for a trademark. Yet, she's seen tonnes of cases where another business had decided to expand into another region and begins to leech off another company's name and clientele in that area, ultimately bringing that business' movements to a halt.

"A lot of traders tend to think because another business is in another region or even in another country that they're not going to affect them," says Calder.

"However, there's nothing stopping a business out of region or country from changing locations, expanding, or franchising, which a lot of businesses are doing as many want a license that makes their business more mobile and covers more ground.

Because a business is based in Auckland, that doesn't mean they won't license someone in Wellington, Christchurch or Dunedin to do the job. It works between New Zealand and Australia as well where a business in New Zealand can license a business in Australia to do work for them."

Calder believes the main reason why so many businesses go through brand security problems is simply due to their lack of knowledge in the matter.

Day after day, Calder says her office sees numerous clients come in not having the slightest idea that a trademark is the ultimate protection for their business, believing when they registered their business (which all businesses have to legally do) was all they had to do to keep their name secure.

"Many people are unaware of the importance of trademarks", Calder says. "They think that a business name that they came up with gives them the rights to the name. We've had clients come in saying, 'nobody told me about trademarks. I thought my business was protected'.

They think that just because they've registered their business, they've got protection. But registration is basically just

for tax purposes. It doesn't actually give you any legal rights to the name."

Given that many are well uneducated in the importance of trade marking a business, Calder says it's crucial that businesses start looking into it immediately, as a trademark could be what ends up saving their company's life.

Having a trademark is crucial for every business," she says.

"Once you've started up a business, you invest so much time and money into it, especially the name, and the name is pretty much what everyone remembers. So if you don't have that protected, someone else can come along and take it from you.

The quickest, easiest and most cost-effective way to avoid all that is to get a trademark. It basically secures your brand and stops other traders from sneaking in on your turf and working off your reputation. It makes sure your brand is your brand and when customers see it they only think of you."

The New Zealand government has also seen the importance of this matter and this year launched ONECheck under its business website (www.business.govt.nz). ONECheck allows businesses to check for existing trademarks as well as educates people by promoting the fact that if you're looking to start a business that getting a trademark is essential and will help you avoid potential costly court cases.

Calder again stressed the importance of getting a trademark for any business, saying everyone needed brand protection from as high as Apple and Google, right down to Bob the Plumber.

MIC Series 612 Thermal Camera

- ◆ User-switchable (single) or simultaneous (dual) thermal/optical video output.
- ◆ Two thermal imager options: standard resolution with 35 mm (includes on-screen temperature display with alarm) or high resolution with 50 mm lens.
- ◆ Human detection range up to 1500 m (almost twice the range of previous MIC thermal models).
- ◆ Video and control over IP when powered by MIC IP Power Supply (sold separately).
- ◆ Robust design rated to an industry-leading IP68/NEMA 6P/IK10.

The MIC Series 612 camera has been designed to offer an extremely reliable, robust and high-quality surveillance solution for security applications that demand the very best performance. Precision engineered to exacting standards, the camera offers the most ruggedized dual optical/thermal image capture solution available on the market today. When powered by a MIC IP Power Supply, the MIC camera becomes an IP-enabled device with extra features such as Intelligent Video Analysis (IVA), and the ability to record video on a network-attached RAID iSCSI storage device or locally on a user-supplied SD or SDHC card (32 GB maximum). The optional “hybrid” operation provides video and control of the MIC camera over both analog (Bilinx over coax) and IP connections simultaneously. For more information, see the MIC Series IP Power Supply datasheet on the online Product Catalog at boschsecurity.com.

System overview

High-performance camera with simultaneous thermal/optical video output

Image control and quality are integral aspects of any PTZ camera, and the MIC612 delivers. A high-quality day/night camera core with 36x optical zoom lens and a full 12x digital zoom and a high-performance, uncooled thermal imaging core sit side-by-side within the housing. Each MIC612 has two video

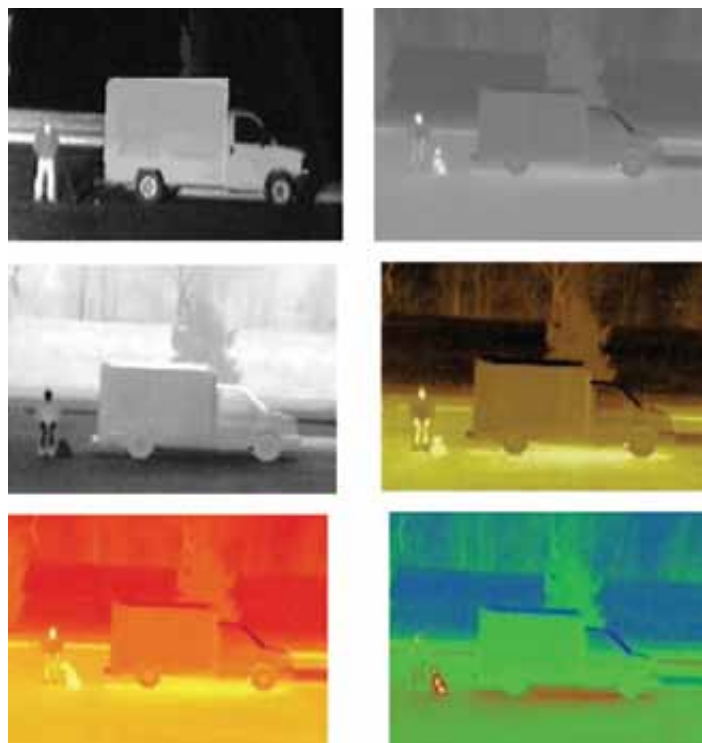
outputs – one for the optical camera, and one that is user-switchable between the optical camera and the thermal imager.

The optical camera provides 550 TVL of horizontal resolution for outstanding clarity and image detail and incorporates Wide Dynamic Range (WDR) that dramatically improves the dynamic range by 128 times and results in clear image reproduction in extreme high-contrast environments. Features of AutoScaling (proportional zoom) and AutoPivot (automatically rotates and flips the camera) ensure optimal control.

Day/night capabilities and outstanding sensitivity make the MIC612 an exceptional performer in all lighting conditions. In low light, the optical camera automatically switches from colour to monochrome by removing the IR filter to boost sensitivity, while maintaining superior image quality. For operation in the darkest conditions, the SensUp control feature automatically reduces the shutter speed to as little as one second. This increases sensitivity by more than 50 times. In addition to low light applications, the optical camera is also an exceptional performer when viewing under a sodium vapor lamp (for example, a street lamp or tunnel lamp) which normally gives a yellowish tint to images. The camera automatically compensates and restores objects to their original colour.

The thermal imager has user-selectable colour options including White Hot, Black Hot, and many others and built-in sun protection that allows the camera to selfheal if pointed directly at the sun. Standard-resolution models include a user-selectable on-screen temperature display (spot meter) feature. These models allow users to set high or low thermal temperature limits and then to use the measured temperature value from the spot meter to trigger alarm functions based on those limits.

Examples of optical and thermal modes



Optical image / Thermal image, White Hot mode;
(middle) Black Hot / Sepia; (bottom) Globow / Rainbow



Bosch unveils AutoDome 7000 with Intelligent Tracking technology

- ◆ Accurately track objects even in scenes with challenging light and weather conditions.
- ◆ Proactively alert operators to potential risks with Intelligent Video Analysis.
- ◆ Deliver flexibility in system design with advanced streaming and recording options.
- ◆ Simple and easy onsite installation.

Bosch Security systems introduces the AutoDome 7000 family of Pan-Tilt-Zoom (PTZ) cameras with intelligent features that are major asset to security surveillance.

Built-in intelligence

Bosch's embedded Intelligent Video Analysis (IVA) software automatically processes video signals and alerts operators to security risks. A single AUTODOME PTZ camera can analyse up to 10 different scenes for loitering, line crossing and other criteria. Customisable to address the specific concerns of each customer, IVA enables earlier threat detection and improved overall security.

Bosch's unique Intelligent Tracking technology uses advanced flow detection algorithms to monitor scenes for motion and to automatically track objects. Customers can define conditions that will instantly activate tracking—such as a vehicle moving through an area in a specific direction. Now, operators can also trigger tracking by clicking on a moving target within live video to prompt the camera to keep it in the scene. The camera dynamically re-tunes zoom settings to capture the most useful, highly-detailed images of objects of interest as they move through the camera's field of view.

AUTODOME 7000 family sets a new benchmark for intelligent tracking algorithms, as it resumes following a target after it passes behind a privacy mask or if it is temporarily concealed by a stationary object—even when swaying trees or other background noise is present. AUTODOME continuously tracks the target when it reappears or if motion is detected along the same trajectory—ensuring activities are always captured.

High performance

AUTODOME 7000 brings imaging to the next level with improved sharpness, more accurate colour reproduction and more detailed low-light images. The standard definition IP camera offers 28x or 36x zoom, and the HD camera delivers 1080p resolution, 30 images per second (IPS) and 20x zoom. The HD camera also supports high-speed 720p resolution at 60 IPS for capturing fine details of fast-moving objects in traffic and city surveillance, gaming centres, toll plazas, gas stations and similar applications.

Designed using Bosch's latest firmware release CPP4, the camera supports quad-streaming to perform live monitoring and recording using up to four independently-configurable streams. While customers can record and monitor in HD resolution, the camera can also deliver reduced resolutions for bandwidth-friendly remote viewing. The new firmware provides a common software platform for many Bosch IP camera models, making it easier to install and maintain Bosch systems.



The cameras also support edge recording in combination with central storage for dependable performance. With up to two terabytes of storage via SDXC or 32 gigabytes with SDHC, the cards can be used for short-term or local alarm recording.

Designed for ease

AUTODOME 7000 is simple to use and install. It comes with five pre-configured settings for capturing optimal image quality in the most common applications and 256 preset positions for viewing critical monitoring areas at the touch of a button. Pre-terminated, colour-coded wiring and a quick-connect system between the camera and mount make AUTODOMES faster and simpler to install than other PTZ domes. And, a fiber optic kit includes a unique media converter module installed directly into the power supply box.

Dependable operation

AUTODOME 7000 family includes indoor and outdoor dome cameras with an extended operating temperature range of -40 to +55 degrees Celsius (-40 to +131 degrees Fahrenheit). Their tamper-resistant aluminum housing is rated to IP66 and NEMA4X for uncompromised functionality even in most dusty or wet environments—ensuring years of reliable performance. In addition, AUTODOME's power supply design supports simultaneous use of 24VAC and High Power over Ethernet (HPoE) for continuous coverage. If one power source fails, the other takes over seamlessly without going through a reboot cycle.

ZoneTechnology
Your Security Supply Partner

Email: sales@zonetechnology.co.nz

Website: www.zonetechnology.co.nz

Auckland:
(09) 415 1500

Wellington
(04) 803 3110

Christchurch
(03) 365 1050

BROOKS stand out at Fire NZ 2013

Brooks once again exhibited at this year's Fire NZ Conference and Exhibition held at the Viaduct Events Centre in Auckland on the 22nd and 23rd of October 2013.

The theme of this year's conference was 'Adding Value is it Worth It', which was quite an interesting topic and one which I am sure every manufacturer, supplier and contractor struggles with to some extent – putting a dollar value on the extra services they provide and the customer expects. From a supplier perspective most offer some form of 'added value' which could include items such as customer visits and site visits with the contractor, system design, commissioning assistance, training etc. We know how much it costs but is it chargeable or more a cost of doing business and creating a competitive advantage.

The Brooks exhibit this year focused on the total solution Brooks can provide for residential, commercial and industrial markets. Our stand layout reflected this with one side showcasing our extensive range of smoke, heat, carbon monoxide alarms and the NEW multi sensor alarm for the residential market through to emergency and exit lighting, passive illumination, sight and sound. The other component of our stand focussed on the new or upgraded range of Analogue Addressable C.I.E's and other fire system solutions.

Brooks continue to advocate **Wireless Interconnection** between Smoke, Heat, Multi Sensor Alarm and Carbon Monoxide Alarms. Wireless Interconnection enables alarms to be connected to each other without the need for cabling. This is the ideal solution for residential buildings with a common floor/ceiling, for heritage buildings and for out-houses and sheds. You could see how effective interconnection is particularly when using a combination of alarms. Using RF (radio frequency) signals, when one alarm activates, they all activate providing the earliest possible warning signal. Wireless Interconnection is available through Brooks New Zealand and Brooks Australia. We also had our new range of Emergency and Exit lights, Active and Passive Illumination and Sight and Sound Products.

Brooks also featured the recently approved **Firetracker FT1020G3**, which will replace the popular FT512 giving **advanced functionality** and **double the device capacity** (1020 devices over 4 loops). The **FT128 was also on display** and the **version 2 software** will **double the device capacity** of this unit as well providing the user with a **single loop 250 device capacity**. Brooks also displayed samples of their Warning Lights and Sounders, Hard of Hearing Alarms and the latest products and solutions from Xtralis which included OSID – Open



Area Smoke Imaging Detection System and the newly released refrigerated storage sampling product.

The Chairman and Founder of Brooks, Peter Brooks and Managing Director, Cameron Brooks also attended this year's Fire New Zealand and both see New Zealand as a key market for Brooks. Along with the Sydney Opera House, Brooks also **this year celebrate 40 years** in the Electrical Engineering and Fire Protection business.

If you have any questions about the products on display or the services Brooks can offer, we would be happy to come and see you or send you any information you may require. **You can contact Lester Easton on 0800 220 007 or visit our new website: www.brooks.co.nz.**



fire door holding electromagnets

Standard, floor mounted, wall to door distance 114mm



FDH40S

unbreakable universal mounting

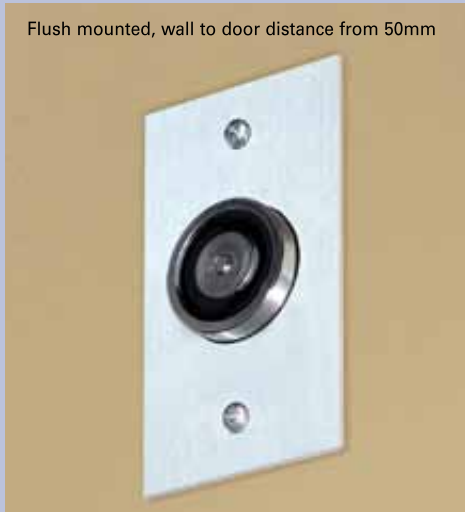
- Low power consumption - low operating temperature
- One product suits floor and wall mounting
- Universal armature - offsets to 55° to suit doors opening past 90° • Wall mount extensions available
- 12 VDC models and 24 VDC models • Push off button with no residual magnetism • Oversize armature for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

Designed, tested and produced in New Zealand to AS4178

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



Flush mounted, wall to door distance from 50mm



Surface mounted, wall to door distance 70mm



FDH40SS

stainless steel surface and flush mounting

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

10 YEAR GUARANTEE*

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



BOTH options are packaged in the same box



Slow showdown over fire levy freeloaders

By Keith Newman

Loopholes in legislation continue to encourage deals where insurance brokers, big businesses and even the Government get away with making minimal or no contribution to the running the NZ Fire Service.

The 2012 Fire Review Panel, which made recommendations for the proposed Fire Services Reform Bill, urged “sustainable, stable and equitable funding for fire services, with the sources of that funding aligned with the functions that they perform.”

However, when the contents of the Bill was announced in September, those clauses dealing with funding had been dumped. The Bill itself, originally due to go before Parliament before the end of the year, has now been shunted out to early next year.

Concerns around how the NZ Fire Service is funded, the subject of several reviews seeking legislation change over the years, have again been sidelined for further research and consultation.

According to the Insurance Council (NZIC), New Zealand is operating “an international anomaly” by continuing to rely on an insurance-based model to fund fire fighters when most other governments have moved to general rating or taxes.

NZIC Chief Executive, Tim Grafton, says the current system leaves the way open for corporate and even Government agency freeloaders to avoid paying their fair share for the fire service.

Grafton says the Fire Services Reform Bill clarifying the broader role of the Fire Service will establish that all New Zealanders benefit from its services,

paving the way for a fairer, more “stable and equitable” funding base.

He says it’s now firmly established that taxation on insurance is inefficient, inequitable and unsustainable. Most Australian states had shifted to some form of general taxation, consolidated revenue, or a property based levy and “its time NZ followed suit”.

Further funding frustrations

United Fire Brigades Association (UFBA) Chief Executive Rick Braddock, while pleased with much of the content of the proposed Bill, is frustrated the funding issue was “pushed out to another time”. He would have preferred to see “more progress around the inequities and inequality of how the fire service is generally funded”.



Tim Grafton, Insurance Council CEO



Rick Braddock, UFB Association CEO



Chris Tremain, Minister of Internal Affairs

He says the issue has been tossed around for many years including recommendations to shift to a rates-based or assessed system “where those who require assistance are levied on a fair and reasonable basis”.

Internal Affairs Minister Chris Tremain, in advising NZ Security Magazine that the Fire Services Reform Bill is not likely to be introduced until early in 2014, said it’ll still need to go through a robust Select Committee process which may result in further amendments.

“I am confident, however, that the measures in the legislation are reasonable and necessary, and build off the consensus generated by the report of the Fire Review Panel.”

The Bill modernises 40-year old legislation unsuited to an era where 30 percent of fire service time is spent as first responder to car crashes, domestic accidents, hazardous substances, severe weather events and search and rescue operations.

The Bill will legitimise a full range of fire and non-fire services and protect firefighters from legal and insurance liability when attending calls. “Everyone’s been waiting for this for a long while. It’s just sensible, it means they’ll no longer be operating outside of their mandate,” says UFBA’s Braddock.

The funding issue, however, will be looked at as part of further legislation in 2014, although the sceptical doubt it’ll get any traction during the current election term.

Reform long overdue

Tremain admits reform is long overdue and while there’s talk of tweaking the levy, unless dissenters are required to make a contribution it won’t address the fairness issue, leaving the majority of insurance premium holders effectively subsidising non-payers.

Although Fire Service funding is currently in surplus, Tremain says there’s a need to focus on long term sustainability. “It’s vital to get this right and there will be a lot more consultation and discussion on this before any final decisions are made.

He says the review will look at issues including “insurance constructions” that minimise levy payments. “It is my aim to address any loopholes which corporate organisations use to significantly reduce their fire service levy which they should fairly pay.”

The bulk of funding for NZ Fire Service comes from a Fire Services levy on household and business insurance

The Bill modernises 40-year old legislation unsuited to an era where 30 percent of fire service time is spent as first responder to car crashes, domestic accidents, hazardous substances, severe weather events and search and rescue operations.

premiums. Most businesses take two forms of fire cover, an indemnity policy and an excess policy for any shortfall in replacement cost.

The levy is charged at 7.6 cents for every \$100 of insurance to fund 95 percent of the cost of the country’s fire stations and full time firefighters

Meanwhile the NZIC, the UFBA, the Fire Services Commission (FSC) and others remain concerned loopholes continue to be exploited. Many building owners are prepared to take the risk of not insuring their premises, are self-insuring or legally “seek to structure their arrangements to minimise their costs” and avoid paying, says the NZIC’s Grafton.

One of the major culprits are Crown agencies. “You get voluntary payments from some Government owned property but quite a lot don’t pay. Basically they use the Crown as a backstop if things go down or use the self-insure option.”

If a Government department such as a prison institution catches fire they expect the Fire Service to be there but “they’re not making an equitable contribution” leaving the burden of the levy on those who pay insurance.

“If everyone is a beneficiary and it’s a public good then we have to find a way to enable everyone to make a fair contribution. Applying it to insurance which is voluntary is always going to lend itself to a freeloader situation which is inequitable,” says Grafton.

Court supports avoidance

An important element in the decades old debate is currently before the court system. At publication date a High Court ruling was in place effectively stating that

avoidance schemes cobbled together by insurance brokers to reduce fire levies for big businesses were acceptable.

The test case bought by the Insurance Brokers Association (IBANZ) and insurance company Vero against the FSC, asked the courts to endorse the use of composite policies after several ports, including the Auckland Council-owned Ports of Auckland, signed a collective insurance agreement lowering their total cost for indemnity and significantly reducing fire levies.

Justice Paul Heath found in favour of the plaintiffs, saying case history favoured a levy calculated on indemnity cover and the Fire Services Act 1975 did not contain anti-avoidance provisions.

The FSC is appealing that December 2012 decision and preparing a legal challenge, claiming it could have long-ranging consequences, including further minimising levy payments.

Fire Service National Commander Paul Baxter weighed in with his concerns that if such schemes were allowed to continue, homeowners would have to pay more for emergency services. It was unfair and would result in millions of dollars being paid by others.

He believed Parliament did not intend large corporates to arrange their insurances to minimise their contribution to the fire service and said in February this year that the Fire Service had better uses for its funds than trying to shut down insurance schemes trying to reduce fire levies.

He and others hoped the Government would close the loopholes and opt for a more equitable levy base for all of the country as recommended by the Fire Review Panel.

Wider public good issue

Insurance Council Chief Executive Tim Grafton believes that once it is establishing that the NZ Fire Service is now legally mandated to do far more than putting out fires, it will be clearer that all New Zealanders not just those who pay insurance are the beneficiaries.

The ICNZ has made a number of “strong submissions” pointing out the existing insurance-based method of levy collection is outdated, no longer relevant or in-line with international best practice.

Like fellow advocacy group the UFBA, it believes the collection method is unfair. “Significant numbers of New Zealanders do not purchase insurance and therefore contribute nothing... yet continue to receive the same protection and benefits as those who pay for it.”

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 \$50.00 plus GST you can ensure that you receive a 1 year subscription (6 issues) by filling out the form below and posting to:

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

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

Mr Mrs Ms _____

Surname _____

Title _____

Company _____

Postal Address _____

Telephone _____

Email _____

Date _____

Signed _____

nzSecurity Magazine
A trusted source of information for industry professionals

The New Zealand Fire Commission in its 'Statement of Intent for 2013-16', while admitting it's in a strong financial position, says there's significant risk to its income base as private and public sector agencies with large property portfolios sought to "shield their insurance arrangements from liability to pay (the) Fire Service levy".

The report said the Commission had taken "prudent action" to minimise this risk while new funding arrangements were being considered, although it remained confident it would not need to increase insurance levies.

The Commission revealed that while it had tightened its budget, and has cash, committed reserves and receipts from Christchurch earthquake insurance settlements approaching \$80 million, it needed to invest an estimated \$50 million in capital works to strengthen its stock of fire stations and other critical facilities to new seismic standards.

Political will essential

Much hangs on whether the Commission's challenge to the High Court test case can shut down avoidance schemes and how seriously Minister Tremain or his successor take the challenge of closing loopholes in the law.

Any alternatives that link levy collection to property rates or general taxation are also likely to face hurdles without the political will to follow through. To support its case the ICNZ has commissioned work from the New Zealand Institute of Economic Research (NZIER).

It claims spreading the cost of the NZ Fire Service across all ratepayers instead of just those who insure, shows a net benefit for everyone. Similar work "in the commercial space" has also been commissioned.

CEO, Tim Grafton, says ideally the levy should be coming from general taxation so everyone who benefits contributes. "The beauty of the rates system is that it is already in place in relation to properties and it's very difficult to avoid." However, there has to be a willingness from local authorities to collect this tax.

Since the announcement that the funding issue has been dropped from the proposed legislation, the UFBA's Braddock has continued to meet with Minister Tremain, the FSC, the NZ Fire Service and his own board.

While he says the Fire Service has reserves to call on, he's unsure whether that would be sufficient to deal with another disaster like the Christchurch earthquakes. "We would expect the

"If everyone is a beneficiary and it's a public good then we have to find a way to enable everyone to make a fair contribution. Applying it to insurance which is voluntary is always going to lend itself to a freeloader situation which is inequitable."

Tim Grafton,
Insurance Council CEO

government to assist in times of crisis."

He says there will always be tension and disagreement between Government entities like the Department of Internal Affairs, the Minister's Office, the Commission and the NZ Fire Service in respect to the UFBA.

"That's why we are in existence and are always looking at ways to advocate for our volunteer movement about better ways of doing things."

While it's never going to be a perfect world, Braddock says, the fire brigade will continue to turn out with adequately trained and resourced people irrespective of the requirements "although we don't like false alarms and cut fingers".

Minister Tremain still has the task ahead of him of promoting the Fire Service Reform Bill through its passage and before he focusses further on the funding fiasco he wants to ensure any decisions are based on solid information and is therefore "taking a more measured approach".

Does that mean general taxation is an option or that Government departments and large corporations who currently use loopholes to avoid paying the Fire Service levy will now be required to pay it?

Tremain wants to "develop an accurate picture of where the fire service is currently allocating resources across its different activities". Then there'll be a "more fundamental review" later next year. "It is therefore too early to say which options are on or off the table.

fired up protection

ViTECH



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



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

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



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

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



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

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



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

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

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



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

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

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

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



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

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

STI-6255 Ref. 720-042

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



STI-6720 Ref. 720-047

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



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



Fire Brigade Alarm: (Closed/Open) Ref. 720-102
ViTech branded Type X and Type Y models with temperature compensated pressure transducers with digital display showing pressures for defect, fire and pump start.



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



ViTech products are designed and produced in New Zealand.

Loktronic

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






Loktronic control buttons and plates

Each pushbutton has SPDT contacts, one breaks the power and one signals the system of an authorised egress. Options are: 12VDC LEDs for illumination or status; coloured button shrouds to increase weather resistance.

Designed, tested and produced in New Zealand by 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 20682_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.

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 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

Auckland: (09) 415 1500 • Fax: (09) 415 1501
Wellington: (04) 803 3110
Christchurch: (03) 365 1050
Email: sales@zonetechnology.co.nz
www.zonetechnology.co.nz



FUJINON

GSP
DIGITAL VIDEO SECURITY SYSTEMS

IR LAB
SURVEILLANCE TECH

LOCKWOOD
ASSA ABLOY

THE EVOLUTION ...CONTINUES...



Introducing the new EVO Series 3 cameras. These new cameras utilise the Effio-E™ & P™ DSP from Sony and come in Full Body, Internal Dome and External Dome

EVO Series 3 Features:

- 700TVL resolution
- Full Body, Internal Dome and External Dome models
- Base models feature Effio-E™ DSP and full featured version use Effio-P™ DSP
- Flush and Surface mount
- Varifocal, IR, Fixed lens, and WDR features on various models

Now available at your local Hillsec branch.



For all product information visit
www.hillsec.co.nz

KOCOM®

SEE IT. TOUCH IT. RECORD IT.



KVR-D510 - INTEGRATED INTERCOM, CCTV & DVR SOLUTION

- View, record and playback live footage • Built-in DVR
- Connect up to 4 cameras (3x cameras, 1x door station)
- Video intercom functionality • 10" touch screen display
 - Multiple storage options (SD, HDD & Network)
- Remote viewing (via App, computer & spot monitor)
 - Digital photo album • Digital calendar

Now available at your local Hillsec branch.



For all product information visit
www.hillsec.co.nz

tecom Challenger10™

Now available



An advanced security solution designed for the most demanding security applications.

Challenger10 utilises a modern, 32-bit processor with high-speed memory, designed to accommodate the ever-changing needs of your site's security solution.

- Fully compatible with Challenger V8 peripheral hardware
- Superior scale to meet the ever-increasing security demands
- Connectivity options with IP, USB, RS-232 and dialler as standard
- Simultaneously communicate with up to 10 monitoring stations
- Multiple holiday types configured to span multiple days and repeat
- Efficient switch-mode power supply with advanced diagnostic capability and resettable fuses • Link multiple internal areas to a perimeter area to control your site's entry/exit procedures
 - Flash upgradable firmware

For more information, or to schedule a product demonstration, please contact Interlogix or your local Hillsec branch

Now available at your local Hillsec branch.



For all product information visit
www.hillsec.co.nz



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

2023B_PSC

Pacific GSM

Presents

Jablotron 100

Revolutionary Alarm System
Easy – Smart – Flexible



Bus and wireless system combination
Multi-use system for all your needs
Free access from anywhere

Come to our stand #31 at NZ Security Conference & Exhibition 22-23 August 2012 to see Jablotron's great new JA-100 Alarm System

www.pacificgsm.co.nz sales@pacificgsm.co.nz

09 948 4762

HTS Group Ltd



BARRIER GATES

Performance Guaranteed

- 2 year warranty
- 4 - 6m arm
- Extremely low power use
- Durable construction
- Tested to 10 million cycles
- Two Inbuilt loop detectors
- Ethernet control option
- RS485 control option

We are looking for distributors!

0800 487 476

www.htsgroup.co.nz

NETGEAR



BOSCH ZoneTechnology
Your Security Supply Partner

Go DirectIP to Faster Setup



With four new models and a whole new plug-and-play protocol (DirectIP™), the SmartIP range of NVR's from Pacom are unrivalled in the industry for performance and ease of use.

SmartIP Features:

- User-friendly Graphical User Interface (GUI)
- Real-time recording @720P all models and 1080p real-time on the -8SD and -16PD - Multiple Recording Modes
- Audio Recording and Audio Playback
- 8 x in-Built PoE (Power over Ethernet) connections
- Third party camera support (Axis, Panasonic, ONVIF™ profile "S")
- IR Remote Control

Now available at your local Hillsec branch.



For all product information visit
www.hillsec.co.nz

CRK Professional Precision

Ph: 09 276 3271 www.crkennedy.co.nz



Real Time IP Kit Plug & Play!

Ganz Real - Time High Definition recorder has everything on board (Built inDHCP, POE) - enabling a quick plug and play system. Eliminating the need for external switches and complicated Networks.

- 1 x Ganz 4CH NVR
- 2 x Ganz HD Dome Cameras
- 1 x 22" LG HD Monitor
- 1 x 4GB Usb flash-disk
- *Optional Cable available

iPhone, Android and Windows compatible.



CRK Professional Precision

Ph: 09 276 3271 www.crkennedy.co.nz



LG LNV7300 3 Megapixel Camera

LG IP camera provides better surveillance, thanks to its higher resolution image quality. The newly launched LG XDI ISP is engineered to complement the IP in image quality through megapixel technology.

- 3 ~ 9 mm Vari-focal Lens, F1.2
- 20 fps @ 2040 x 1536, 30 fps @ 1920 x 1080
- H.264 (High Profile Supported) / MJPEG
- Dynamic Profile (Up to 7)
- Region Of Interest Streaming
- Video Analytics Embedded
- IP66 / Vandal Proof

iPhone, Android and Windows compatible.





Axxon Next: Open-Platform Video Management Solution from AxxonSoft

Next-generation open-platform video management software (VMS). Thanks to exciting innovations from AxxonSoft, the Axxon Next platform has reached a whole new level of performance, reliability, efficiency, functionality and accessibility.

Featuring:

- Advanced Video Analytics free of charge included in every channel.
- Unique tools for fast video footage retrieval including Time Compressor and MetaData search capabilities.
- License Plate Recognition Capture & Search.
- Face Recognition Capture & Search.
- Tag & Track feature.
- Video Wall Management included at no extra cost.
- Multi-Domain Monitoring (Federated Architecture).
- Interactive 3D Mapping.
- Expandable to an unlimited number of cameras, servers, workstations and remote clients.
- iOS, Android and Web remote client applications.
- Support for more than 1,000 IP Cameras plus ONVIF & PSIA Integration.
- Flat pricing - full functionality in system of any scale.
- Zero Maintenance and on -going charges: free support and free updates.
- Free 16 Channel version available for immediate download.



Experience the NEXT®

For more information about Axxon Next please contact:



ITPLUS Communications Ltd
T: +64 9 950 4940
E: info@itplus.co.nz
www.itplus.co.nz



viewtech™
SURVEILLANCE TECHNOLOGY

Viewtech Ltd
T: +64 3 423 1635
E: sales@viewtech.co.nz
www.viewtech.co.nz