

NZSecurity Magazine

A trusted source of information for industry professionals

December 2010 - January 2011



**Gallagher Security Management Systems
Winner of the 2010 New Zealand International
Business Awards \$10-50 million category**

The **new** Dinion Camera from **Bosch**

Revealing every detail with 2X technology



Camera image

Warehouse entrance or exit.

Brings out the details with our high sensitivity solutions using smart BLC.

No more setting up Back light mask boxes on the screen. Let the Bosch Smart BLC do it for you automatically and save you time & money.



High quality Dinion 2X camera image



Other cameras



Human eye

Use a **Dinion 2X solution** for your application

The clearest images, day or night

- CCTV 20-bit image processing
- See more in harsh lighting conditions using pixel by pixel analysis
- Smart backlight compensation (BLC)
- See clear images both day and night as the 2X image
- processing dynamically adapts to scene changes.
- Compensation for IR illuminations

Find out more about **Dinion 2X** and **FlexiDome 2X** by contacting our offices below for a product demonstration or for more information on these exciting new products visit www.zonetechnology.co.nz.

ZoneTechnology
Your Security Supply Partner

Auckland

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

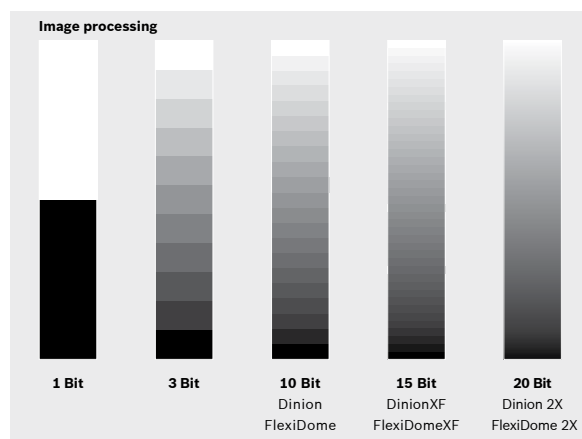
Wellington

35 Abel Smith Street
Wellington
Phone: 04 803 3110

Christchurch

L1, 70 Gloucester Street
Christchurch
Phone: 03 365 1050

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



BOSCH
Invented for life

INFINITY LENS™ CCTV LENSES MASSIVE DEPTH OF FIELD

GBO's innovative InfinityLens™ product range delivers a breakthrough in optics. With extended depth-of-field and edge-to-edge sharpness, these unique mega pixel rated lenses enhance your system's ability to provide more useful information.



High Quality
Conventional Lens



InfinityLens™



Available at:

nz Security

NZ Security Magazine Limited

Contact:

Telephone: + 649 409 2018
P O Box 4, Ahipara, Northland
New Zealand 0449

Editorial enquiries to:

craig@newzealandsecurity.co.nz
Editorial contributions welcome

Advertising enquiries to:

Craig Flint on 09 409 2018
craig@newzealandsecurity.co.nz

Subscription enquiries to:

craig@newzealandsecurity.co.nz

Deadline for copy

February / March 2011
issue is the 15th January 2011



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.

NOW a 10 year guarantee
on Loktronic Indoor Electromagnetic Locks!

Loktronic • Innovationz
0800 367 565 www.loktronic.co.nz

16462_ELS

CONTENT

December 2010 - January 2011

6	INUKSHUK - COMPANY PROFILE
10	PSPPI ACT 2010
14	PSPPI GLOSSARY
16	UNHAPPY STAFF RISK TO COMPANY DATA
18	CONCEPT DEALER NETWORK (CDN) UPDATE
20	AIPHONE'S NEW DOOR STATION
22	ONE-ON-ONE WITH IAN ANDERSON
24	RETAIL VIDEO SOLUTIONS
26	MOBILE FORENSICS
32	GALLAGHER'S SUCCESS AT NZ INTERNATIONAL BUSINESS AWARDS
34	ASSOCIATION NEWS - MLAA
36	ASSOCIATION NEWS - NZIPI UPDATE
38	ASSOCIATION NEWS - ASIS
39	ASSOCIATION NEWS - NZSA
40	TERRORISM
46	THE FINE LINE BETWEEN FEELING SAFE & UNSAFE
47	COLLABORATION GATHERS PACE
48	NEXT STEP TO TRUSTED IDENTITY
50	POWERFENCE™ SOLUTIONS
52	SECURITY GUARDS IN NZ
56	NEW BOSCH RECORDING STATION
58	CFATS
62	PRODUCT SHOWCASE

For all the information you need on Editorial and Distribution for upcoming issues as well as a comprehensive archive of back issues, please visit

www.newzealandsecurity.co.nz



Help keep your stores
focused on customer satisfaction.

A good video surveillance system does more than just record events. It improves your ability to prevent and control them – allowing you to focus on your actual business.

Combine the new Axis range of compact affordable M-line network cameras with AXIS Camera Station, or with a video management solution from one of our partners, to create a truly effective HDTV surveillance system.



www.axis.com/focus

AXIS M11, AXIS M32 and AXIS M10 network cameras, combined with AXIS Camera Station, provide a complete network video solution for up to 50 cameras that supports HDTV, H.264 and Power over Ethernet.

Easy to install and operate, an Axis IP-Surveillance system delivers image quality that really proves your case, and the flexibility and scalability needed to accommodate your changing needs. So you will rest easy with a trouble-free video surveillance choice that lets you focus on what's important for you.

Get the Axis picture. Stay one step ahead.
Join the Axis Channel Partner Program today!
Register at www.axis.com/partner

AXIS®
COMMUNICATIONS

Axis Authorized Distributors:

 **CHANNELTEN**
SURVEILLANCE SOLUTIONS

 **Hills**
Electronic Security
New Zealand

Inukshuk -

a secure path to a Class 5 act

An alarm system is only as good as the people who can respond to it. But if they don't know to respond – because a phone line has been disconnected or there is a line fault – then the alarm can't dial out to the monitoring company.

And while there are some firms offering wireless solutions to circumvent this issue, Ron Taylor's company Inukshuk Secure Pathway, Inukshuk SP for short, has taken the whole issue of secure monitoring three steps up, with the internationally used UHS products (British Telecom Red Care and Telstra Secure AU are UHS product / platform users).

The UHS product family include the ¹UltraConnect® UC-351-G/GH and the UltraConnect® UC -372-AS3GE with inbuilt router. Taylor says both units have battery back up for all system functions and the ability to run over ADSL and/or 3G as primary pathway with 2G GPRS and PSTN service as backup.

"The system is unique in New Zealand," he says.

At the heart of this service is a highly secure and encrypted private wireless network within the Vodafone system. A

¹UltraConnect®, Ultra-Agent, UltraVideo, are Trade Marks and Copyright of UHS PTY Ltd

network that is ring fenced from all the other traffic the mobile phone company handles.

"What we are offering," says Taylor, "Is alarm signal transport to Class 3, 4 and 5 meeting AS/NZ 2201.5:2008 standard over our own private VPN – that operates within the Vodafone 3G Network."

"The VPN can only be accessed with Inukshuk's authorisation and is segregated from the rest of Vodafone's traffic."

"It means that if the general Vodafone network was slowed down or is interrupted for any reason, it would not impact at all on the secure services we provide. There would have to be a catastrophic failure at Vodafone before our system was compromised."

What Taylor's firm has done is to contract a section bandwidth from Vodafone, a VPN, in the same way that other mobile phone companies have done, but on an appropriately smaller scale.

He says: "Anyone deploying an intruder alarm system over the Inukshuk service has the security of knowing their system is monitored for its integrity and condition and is not reliant on landline cables to function. The system can be monitored up to six times a minute, dependant on the plan chosen."

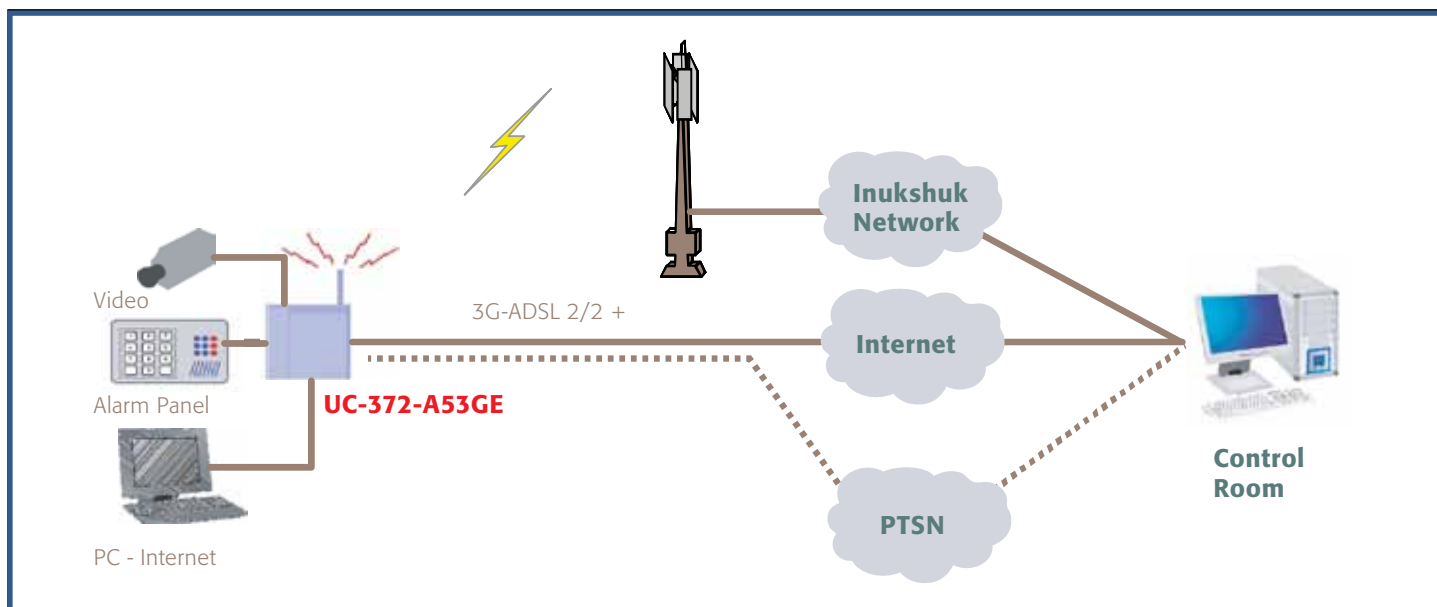
As soon as something goes amiss, the software within the server will transmit a message to the monitoring station. All the data transmitted is coded and encrypted and compatible with CMS (Central Monitoring Station) automation systems.

Normally alerts are created by things such as intruder activation, tamper, mains fail and low battery. The UHS software will also notify the CMS if 3G network or ADSL failures to poll, within seconds of occurrence.

In the case of a failure on the 3G network, the UHS unit will switch to the next platform of Vodafone services. If the ADSL or 3G pathway fails, GPRS polling frequency increases.

Dialler systems can be a lottery, because if your telephone line has been cut – or is down due to a fault – your alarm can't call anywhere. But the advantage of the Inukshuk solution is that the communications are constantly managed, between, the Central Monitoring Station and the alarm system.

Some existing dialler monitored alarm systems only poll once a day – which provides a huge window of opportunity for burglars to cut communication lines. But with Inukshuk SP's system, as soon as



Why use Inukshuk's wireless monitoring?

- Inukshuk runs over a 3G VPN.
- Inukshuk meets AU/NZ 2201.5:2008 Class 3, 4 and the highly secure Class 5.
- Full path diversity and server redundancy.
- Polling over wireline (ADSL) 3G IP, GPRS.
- Fixed lines are often used for other purposes such as fax, answering machines and modems etc that can create disturbances to lines used by alarm systems.
- An Inukshuk wireless connection is solely used for the intended purpose – thereby securing best possible alarm connectivity.
- Using off-the-shelf wireless equipment can reduce installation time and cost.
- Accommodates increasing demands for more advanced alarm functionality such as notification by confirmation picture/video.
- Manufacturing support is well in line with high-capacity mobile networks for data and voice communication.
- Inukshuk's network is monitored 24/7 by a dedicated team making sure your security devices remain connected.

something happens to the communications with the alarm panel, the monitoring station is informed that the UHS unit has lost communication within a polling cycle.

Depending on the monitoring station options the customer has selected, a security guard or key holder service could be dispatched to the alarmed premises to check what's going on within minutes."

Taylor says the Inukshuk system polls, and if this fails, polls again immediately to verify the pathway integrity before signalling the poll status to the Inukshuk SP servers. It all sounds complicated, but it is a double belt and braces approach to alarm monitoring. This repeat polling removes spurious alarms hitting the monitoring station if the network hiccups.

Taylor is offering four levels of service; a Residential & Small Business package; then three plans that have, using the UHS equipment and platform, been independently accredited to meet CLASS 3, 4 and 5 of AS/NZ 2201.5:2008

- Class 3 report in 120 seconds
- Class 4 report in 60 seconds
- Class 5 report in 20 seconds

Class 5 monitored on an ADSL line, backed up with a wireless 3G, polling frequency increases when ADSL/IP path fails.

Taylor says: "Operating on the Vodafone 3G networks with fallback to 2G/GPRS in the event of disruption to the 3G network means there are parachutes for Africa, and no other system I know of in the country can offer this.

"As far as I can see, this secure alarm pathway is unique in New Zealand because I do not know of another one that is running UHS equipment over a virtual private network within Vodafone as opposed to a public network.

The risk of being on the public network is that during high traffic times, the alarm monitoring could be compromised. The Inukshuk system is well away from all that, on a secure private network – that is a huge advantage for people who need to know their alarm is going to do its job.

If the Vodafone network is overloaded for any reason, it will not affect the Inukshuk SP private network.

Mobile network encryption, combined with a Private Link, creates a highly secure connection into your organisation's enterprise network. All users are authenticated before entering the Inukshuk network. Private access point names give complete control over who connects to the Inukshuk network."

And because the system is designed to run over the ADSL and 3G network, it can handle video too. The UHS equipment supports a low cost video surveillance capability, with access to live and recorded video from CCTV and IP cameras at the premises viewable at the central monitoring stations or over a authorised pathway over the web.

"The team at UHS in Sydney consistently monitor international markets and are in frequent communication with their expanding international client base working on new solutions and innovative methods of transporting critical wireless data," says Taylor. "One such opportunity is the monitoring of people – particularly the elderly with known medical conditions – at home."

All these innovations will be available to the local market through Inukshuk SP's close partnership with UHS.

Taylor says: "The bottom line is, this system meets leading European, Australian and New Zealand standards, reliability is superior to what many companies are used to in New Zealand and the cost is really affordable."

With more than 30 years in the security industry, it's not surprising Taylor and the team at Inukshuk SP have "trust our pathway" as their tag line. Security is a high priority for them.

For more details contact Ron Taylor on
Phone: +64 21 775 902
Email: ron@inukshuk.co.nz
On the web: www.inukshuk.co.nz

trust our pathway



ALERT 5 SEC 10 SEC 15 SEC 20 SEC **ACTION!**

Inukshuk Secure Pathway Limited P.O Box 115 Te Kauwhata Waikato 3741 New Zealand
t +64 7 826 3332 f +64 7 929 2859 e mail@inukshuk.co.nz w www.inukshuk.co.nz



Win new customers and grow your business

“Make sure your message gets through to the key companies that sell your product to end users.”

IN NEW ZEALAND THERE ARE OVER 2000 SECURITY COMPANIES THAT RESELL PRODUCTS AND SERVICES TO END USERS.

Unless your business successfully reaches each one of those companies that should be selling your security products and services, you are missing out on growth.

Before they recommend you and your products to their customers, they must believe in you and what you can do for them.

There is now a unique way to reach out and gain the trust of the key people and companies who can help you grow your business: a NZSecurity Magazine Profile.

Your specially written NZSecurity Magazine Profile will put you in front of a highly targeted network that has been developed by NZSecurity Magazine over 15 years. The only specialised network of its type in New Zealand, it covers all regions and all sectors incorporating all the key people you need to reach.

The profile is a double page story written for you to engage the readers, your resellers and customers, in a way that they can relate to, building trust and knowledge as they get to know you and your products.

It's easy. You tell us your story and our experienced professional writers will shape it until it works for you.

Your story will reach thousands of readers of NZSecurity Magazine, raising your profile even further among end users, staff and other security industry personnel by positioning your story in a highly desirable position in the magazine.

To take advantage of this cost effective opportunity you need to book early because space in each issue is limited.

CALL CRAIG FLINT ON 09 409 2018

Cost effective

A profile costs less than posting out A4 brochures, even if you had all the up-to-date addresses in your own database.

You could pay someone to create and constantly update a database – a hugely time consuming job. You could pay someone to stuff thousands of envelopes. You could find and engage a professional writer. You could find and engage a professional layout designer.

And once you did all that, a large percentage of all your hard work could be binned by the company's receptionist, along with the junk mail.

But there is another way: you can save all that money and hassle, and count on your message getting past the front desk to the people you need to reach.

Convenient time saver

A single call will set the project going, leaving you to concentrate on managing your business. Call Craig Flint at NZSecurity Magazine, save time and hassle and get your message in front of the people who can help grow your business.

Credible

With a NZSecurity Magazine Profile you have the opportunity to be associated with the highly credible and trusted NZSecurity Magazine name and reputation built up over many years. NZSecurity Magazine will not devalue its own brand or your company by profiling inferior companies, products or services.

Tell a story

In a NZSecurity Magazine Profile, you will be telling your story focusing on the benefits for the reader. That is what sells. It is not a brochure filled with technical specifications, it is not marketing puffery, and it is not a highly stylized advertisement. It is a story about your company, your products, your services. Mostly it will be a story about people, who you are, and why you are worth the customers' business. What benefit there will be to them if they choose your products and services. Even better, if you have a happy customer – let them help tell the story for you.

This kind of profile engages the reader in a way no other sales and marketing document can, building trust in you and your products and services.

Increase the power

Increase the power of the message with a companion display advertisement (optional). Let the profile tell the story, and the advertisement showcase the product.

This combination adds up to far more than the value of either individual approach because the profile and advertisement reinforce each other making it ideal for launching new products and services.

Most effective of all is to use a NZSecurity Magazine Profile to launch a campaign, for your company or new product. Follow up with a program of advertisement over subsequent NZSecurity issues reinforcing the value of the profile over a period of months.

A combination story and an advertisement package brings you a stronger marketing message, yet the combinations cost you less.

CONTACT CRAIG FLINT ON 09 409 2018
or by EMAIL: craig@newzealandsecurity.co.nz
and ask about a NZSecurity Magazine package deal.



Easy process

1. Decide what the focus of your profile will be - your new product, your company, your new team, your new premises or any combination.
2. Make a simple phone call to Craig Flint at NZSecurity Magazine.
3. Our writers will call you or meet with you in person to uncover the story you want to tell. You don't need to have material all polished up and ready or worry about what you need to say. Our professional and experienced writers will walk you through it, their job being to tell your story.
4. A draft will be emailed to you and it will not go any further until you are 100% happy with it.
5. A layout will be emailed to you for final approval. This can also be used to order extra printed copies to use as your own flyer, or added to your website.
6. Standby for results.

Now the hard work begins

The enactment of the Private Security Personnel and Private Investigators Act 2010, more than two years after first being introduced into parliament, might seem like the end of a long process.

Many organisations and individuals made submissions on the bill but if you were not directly involved it was quite easy to put the new law at the bottom of your list of things to think about.

Not anymore. In about four months, on 1 April 2011, the Act will come into force and everyone in the industry will start to feel the effects starting from that date. Even some who don't yet regard themselves as part of the security industry, will be drawn in over time.

The new Act builds on the Private Investigators and Security Guards Act 1974, but some of the terms from that Act that appear familiar now have new meaning.

For example, to work in the industry you will still need licences and certificates of approval, but they will apply to specific classes of work, and they will have more stringent requirements than in the past.

(For details see the NZ Security plain English glossary on page 14).

The point of the new law is to raise the bar. This means that some businesses or individuals may no longer qualify to work in the industry.

Some of the new requirements will, in time, include mandatory training and qualifications, but these details are not spelled out in the Act itself.



Hon Nathan Guy
Associate Minister of Justice

Instead this information will be specified in regulations that will be issued by the government at a date that has not yet been announced.

Happy timing

The new Act was passed just as the 2010 New Zealand Security Conference was held in September. It was happy timing that ensured the Associate Minister of Justice Hon Nathan Guy got a positive reception. The industry welcomed the bill, but had been growing weary of waiting for it to pass into law.

The new Act dispenses with the term 'security guard' from the old Act, splitting it into several classes of security personnel. At the same time it extends coverage to the new classes of 'crowd controllers,' 'personal guards' and 'confidential document destruction agents.'

The old Act specifically excluded people who kept order at licensed premises but the new Act draws them in.

"The definition of crowd controller includes bouncers at bars and pubs," says Mr Guy.

"Crowd controllers will need a licence or certificate of approval, even if they are directly employed as in-house security by a bar or other business.

This means, for example, that a bouncer employed directly by a bar, instead of a security firm that is contracted by the bar, will require a certificate of approval.

This approach reflects the significant risk of harm with unsuitable people performing this type of role, which by its nature can involve physical confrontation."

The Hospitality Industry Association, representing 2370 members, were opposed to this measure, but their concern that ordinary bar managers or restaurant owners might need a certificate of approval has been addressed in the new law; if crowd control is just an incidental part of another job, say as a bar manager, then you will not need a certificate of approval.

Not needed in-house

Apart from crowd controllers, in-house staff will not need a certificate of approval. According to the Associate Minister this is because employers have an incentive to check the suitability of their employees and monitor their performance, and are in the best position to do so.

Although this is no different to the old Act, it means if you are a property guard for your own or your employer's property you will not need a certificate of approval.

This could be a cheaper option for some firms if the cost of training and certification climbs under the new Act and in any case could leave unregulated and untrained security personnel dealing with the public.

It's not what the industry wanted. In its submissions to the bill The New Zealand Security Association recommended that everyone who guards property open to members of the public on a day to day basis should be required to obtain a certificate of approval. They cited shopping centres, tertiary education institutes and universities as examples.

Rugby World Cup

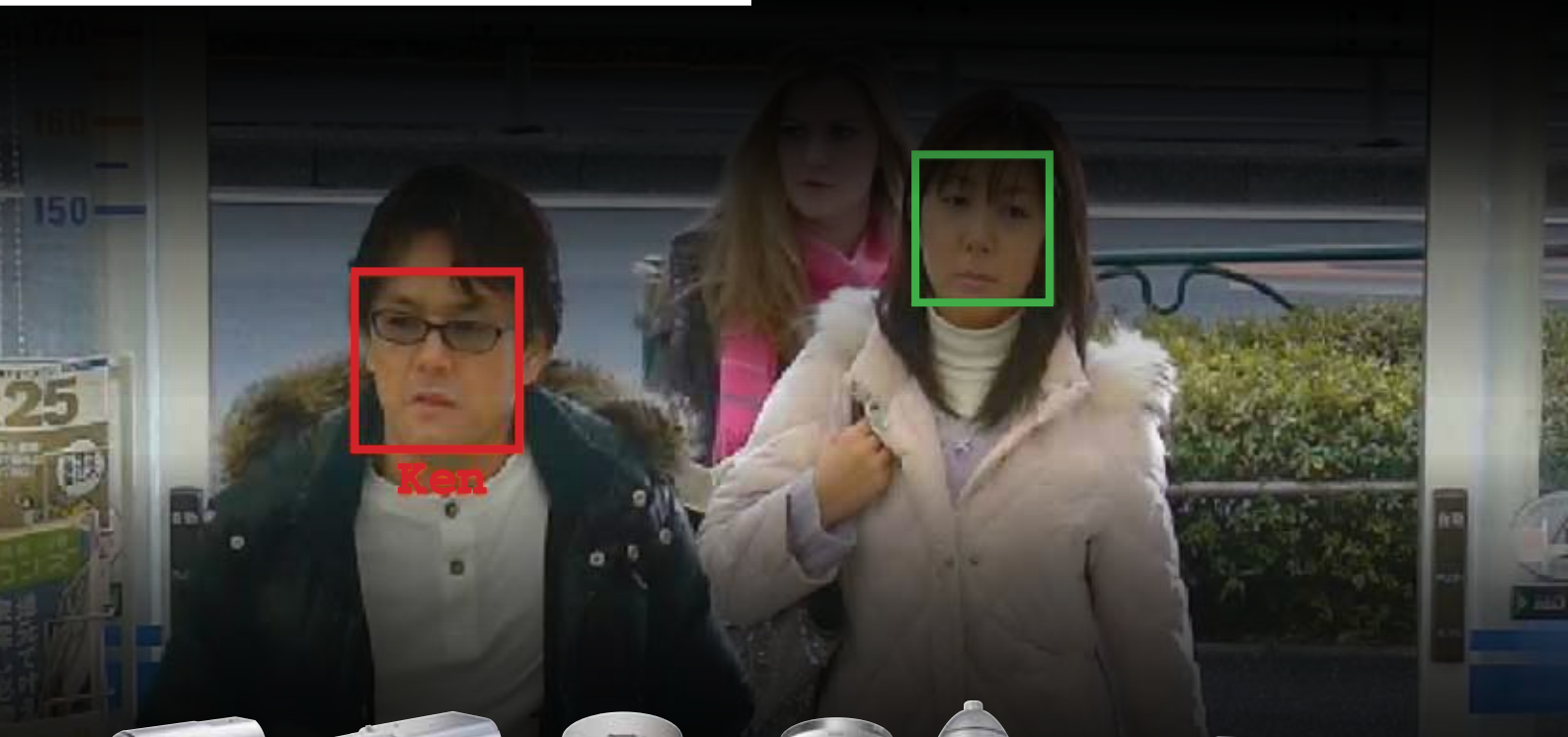
Employing in-house security guards is not the only area that the government has left wiggle room. If things get tight, the Rugby World Cup also has an escape clause.

For one thing volunteers will not be captured by the regime - although this is a practical measure that means parents can still kick gate-crashers out from their teenager's birthday party or school ball without fear of being pinged by the Act. But under section 20 of the new Act the government can - without passing any new law or regulation - use an Order in Council to exempt certain property guards, personal guards or crowd controllers from the Act.

If the Minister takes this step on the grounds of a general public benefit, he will have to consult affected parties. But if it is a major event like the Rugby World Cup or associated events, and there is not enough property guards, personal

SMILE

PANASONIC REAL-TIME FACE RECOGNITION



WV-SP105

VGA/1.3MP
Simple day/night
PoE



WV-SP306

1.3MP
True day/night
Wide Dynamic Range
Auto Back Focus
Face Detection
PoE



WV-SF336

1.3MP
Simple day/night
Wide Dynamic Range
Auto Back Focus
Face Detection
PoE



WV-SC385 / WV-SW395

1.3MP
True day/night
Super Dynamic
Face Detection
PoE/ PoE+
ONVIF



WJ-NV200

16 Camera NVR
PC Less Operation (mouse & monitor)
Real time face matching
Easy set-up and operation

- **FACE DETECTION/MATCHING**
- **FULL HD**
- **SD/SDHC RECORDING**

Panasonic has developed unique i-pro Smart HD cameras with on-board Face Detection combined with the new WJ-NV200 NVRs Face Matching feature. This allows real time face matching against a stored database - providing quick and easy identification and recognition of registered faces.



Panasonic New Zealand Limited
350 Te Irirangi Drive, East Tamaki, Manukau 2013, New Zealand.
Telephone: 9 272 0100, Facsimile: 9 272 0138

Panasonic

ideas for life

panasonic.co.nz

guards, or crowd controllers for the event, then the Minister is not required to consult anybody, he can simply waive the requirements of the Act.

Training in time

Still, the Minister may not need to go that far if he gets nervous about the country's ability to bring security staff up to the new training standards in time for the Rugby World Cup. The Government has the option to simply delay the introduction of the requirements until a more convenient time.

It is the new regulations that will impose training requirements and qualifications for the various classes of security personnel. They will be a key factor in raising standards, but still need to be worked through in another round of consultations.

Mr Guy says the timing of the introduction of the requirements will be determined when the regulations are developed.

But according to a Ministry of Justice spokesperson, a decision has not yet been made, even on the consultation process for the regulations. He says the Ministry's website will be updated with any announcements.

But once the regulations are introduced, in time for the Rugby World Cup or not, then there will have to be sufficient time for the actual training itself.

"Decisions on when people must complete their training will take into account the nature of the requirements and how long is reasonable to allow people to comply," says the Associate Minister.

Nor does the Act specify the date by which personal guards, crowd controllers or their employees are even required to hold licences or certificates. Under section 126 of the Act that date is left up to the Government.

The Government has not yet made a decision on when this date will be or when

it will be announced, but the Associate Minister says it will be announced well in advance, and will not be any earlier than 1 June 2011.

That is the day by which almost 13,000 licences and certificate holders will need to re-apply to continue working in the industry.

It is a fair bet that it will be some time after that date, because to have the new and numerous class of crowd controllers all apply at the same time, even if the regulations were in place, would risk overwhelming the licensing authority.

Some training

The Government has said that at this stage it will be just personal guards, property guards and crowd controllers that are required to undergo training.

"It is inevitable that people in these roles will, from time to time, find themselves involved in situations that could result in a physical confrontation," says Mr Guy.

"It is in the best interests of everyone that they are properly equipped to deal with such situations. This new requirement will benefit not only the public, but also the staff themselves, by protecting their safety and increasing the value of their licence or certificate."

Code of conduct

One date that is spelled out in the Act is the date for the new code of conduct for private investigators. The regulations must create this particular code of conduct by 1 April 2011. The Government has the option of creating further codes of conduct for other classes if it wants to.

Wayne Newall, National Manager Tribunals, Ministry of Justice says at this stage it is intended that there will be a code of conduct for private investigators only.

"However, if this was to change we would notify interested parties who would be able to input into any code of conduct development through the Ministry's

consultation process," he says.

The code of conduct will be enforceable, and will, at a minimum, regulate surveillance of individuals by private investigators and private investigator employees.

The current legislation prohibits private investigators from taking or using photographs and making or using audio-recordings without the subject's written consent - severely restricting legitimate private investigations, sometimes for the Government's own agencies. These clauses have been dropped from the new Act, thanks in part to a submission by the Government's own advisors, the Law Commission, who recommended the code of practice.

However, in future private investigators will probably not only have their code of practice to comply with. The Law Commission is proposing to recommend a new Surveillance Devices Act based on Australian state laws and offering general protection against surveillance. It would add to the protection afforded surveillance of subjects by the Crimes Act, making it an offense to trespass on a property to install a surveillance device, to conduct visual surveillance of private areas, or to install a tracking device.

Unnecessary costs

According to Mr Guy the new Act will also reduce unnecessary costs and bureaucracy because licences and certificates of approval will now only have to be renewed every five years, instead of annually.

"This will be a relief for license holders who currently have to advertise in newspapers every year they want a renewal," he says.

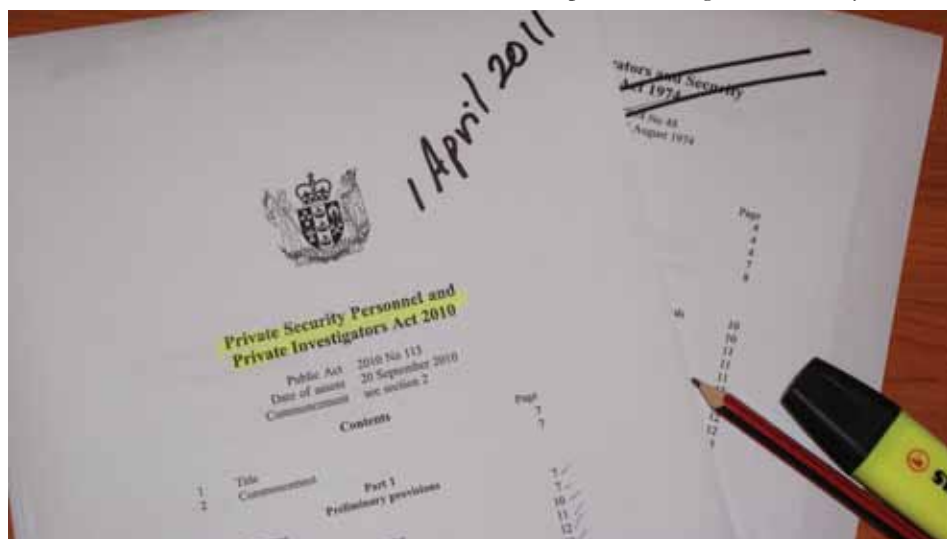
However each year licensees will have to submit an annual return to the Licensing Authority updating contact details and the details of any employees or contractors with certificates of approval.

Transition

The new Act has a section to help the transition of existing licences and certificates to the new regime.

If you currently hold a licence or a certificate of approval under the old Act it will still apply while your application for a new one is processed, provided you apply by 1 June 2011. If you do not submit your application in time, your old licence or certificate will expire the following day.

"You will be able to apply under the new regime from 1 April 2011," says the Associate Minister. "It is in your interest to beat the rush and apply early."





DDF - 4900HDV

The ideal entry into the world of HD!

The DDF4900HDV is a vandal-resistant Cam_inPIX® 5 megapixel high-definition colour network dome.

- 1/2,5" 5 megapixel CMOS sensor with Cam_inPIX® technology.
- Resolution: SD, HD (720p, 1080p, 3MP).
- Frame rate up to 30 fps.
- Video compression: H.264, MJPEG.
- Megapixel vari-focal lens: F1.8/ f=4-10mm
- Hybrid IP camera with an analogue preview output.
- Local video memory SDHC card slot.
- Power supply: 12V DC, PoE.
- Tri-axial adjustment.
- Also available in -ceiling mount and surface mount versions
- vandal-resistant housing with IP67 (surface mount variant).

We also have available the DDF4500HDV Dome (in 720p resolution) and the DF4900 Fixed Full Body Camera.

Please contact C. R. Kennedy for more Information or visit www.dallmeier.com.



VIDEO NET BOX

The VideoNetBox, VNB, is a compact hybrid audio and video recorder with up to 8 free allocatable video channels (HD , IP or analogue) designed for wall mounting. Using a release code the basic version with 2 video channels can be activated by blocks of another 6 free allocatable video channels at a time.

Its compact and robust design allows the recorder to be used ad-hoc.



DMX - 1600

Your ideal entry into the world of VideoIP solutions!

The Smatrix is ideally suited for applications requiring high-speed recording, expanded storage capacity, low power consumption, while ensuring maximum security.

The DMX 1600 is a hybrid audio and video recorder with integrated storage system for up to 16 free allocatable video channels. The DMX 1600 has a compact design (2HU) and is designed for mounting into a 19" rack.

- 16 free allocatable video channels (analogue/IP)
- Simultaneous real-time recording and streaming, live display, playback
- Hybrid recording: H.264, MPEG-4, MJPEG
- Bit rate up to 2 Mbps with analogue cameras, 6 Mbps with IP cameras
- Resolution: SD (up to D1) and HD (up to 1080p) and megapixel up to 8MP
- Evaluation with SeMSy® or PView 7 via Ethernet
- Integrated storage system: Up to 10 integrated 2.5" HDDs
- RAID functionality: RAID level 5
- Low power consumption: Max. 80W

NZ Security plain English guide to the Private Security Personnel and Private Investigators Act 2010 Part One

Licensing Authority

The Licensing Authority will issue both certificates of approval and licences. It will advise the police of applications. It may choose to make enquiries or it may ask the Complaints Investigation and Prosecution Unit for a report. The Licensing Authority replaces the Registrar of Private Investigators and Security Guards, but has more powers.

Licence

A security business, whether it is a sole trader individual, a partnership or a company, will need to apply for a licence for the class or classes of work it does.

Like the old Act a licensed security business must only employ people who have certificate of approval for security duties and must only appoint the directors and chief executive or manager approved in the licence. The exception is a business, for example a tavern, that directly employs crowd controllers for its own needs.

Individuals operating without a licence can be fined up to \$40,000 and companies \$60,000.

Certificate of Approval

A certificate of approval will allow you to work as a particular class of security employee in the security industry.

Although you will be asked to name your employers, you don't have to have a job to apply and the certificate will not be specific to a particular employer. You can

hold a certificate for more than one class of work. If you are a crowd controller your employer doesn't have to be licensed.

If you are an employee on contract you will still need a certificate, but if you are a contractor operating a business you will need a licence.

You and your employer may each be fined \$20,000 each if you work without a certificate of approval.

Validity of old licences and certificates

So long as you apply for a licence or certificate of approval under the new Act by 1 June 2011 your old licence or certificate will be valid until a decision is made about your new application. The opening date for applications is 1 April 2011.

Temporary Certificate of Approval

A temporary certificate allows you to work for up to three months while your main application for a certificate of approval is processed. This does not limit the period of transition from old licences and certificates explained above.

Temporary licence

There is no provision in the Act for a temporary licence.

Classes of security personnel

Volunteers and in-house personnel (except for crowd controllers) are not covered by the Act.

A business can be a person, partners or a company who carry on a class of work for money or reward.

Each class of business has a class of corresponding responsible employees who will need a certificate of approval.

Private investigator (licence):

A business that seeks information about people that is not on the public records.

Holding yourself as being ready to do this work is counted.

Like the old Act, you can't call yourself detectives. The Act makes sure journalists, historians and credit agencies are not covered.

Security technician (licence):

A business that installs or services alarms or surveillance cameras for others.

Includes locksmiths working on safes and strong rooms.

Installing and operating remote surveillance equipment is included in this class but monitoring using the same equipment falls under property guarding.

Security consultant (licence):

A business where people enter premises to sell or advise on alarms, surveillance or guarding.

Confidential document destruction agent (licence):

A business that collects and destroys confidential documents. Does not include confidential document management functions like archiving.

Property guard (licence):

A business that hires out property guards. Includes real time alarm and CCTV monitoring or response, delayed CCTV playback is not covered.

Personal guard (licence): A business that guards specific persons. Keeping order around that person can be part of the job. Personal guards only require one type of licence, even if there is some overlap between the work of a personal guard and crowd controller.

Crowd controller (licence):

A business that screens entry, or keeps order, or removes people. Ordinary ticket collectors at the door of a venue, or staff who may have to ask revellers to quieten down are not covered.

Crowd controller employee (certificate of approval):

If crowd control is just an incidental part of your main job, you do not need a certificate. Nor will you need a certificate if you only keep order, but don't screen admissions or eject people.

Disclaimer:

This guide is intended to be a plain English general outline only. Professional legal advice should be obtained if a legal interpretation is required. A copy of the Act may be downloaded from www.legislation.govt.nz.

See part two of this guide in the next issue of New Zealand Security to find out about important dates, applications, objections, hearings and complaints.

High Definition by Sony

A new benchmark in camera picture quality



The challenge has always been to design a camera with the dynamic range of **the human eye**. By using a newly developed High Definition EXMOR CMOS imager combined with Sony's image processing technologies Sony has developed a camera with an ultra wide dynamic range. Now at last there is a camera that can handle a wide range of difficult lighting conditions with high definition quality.

With a comprehensive array of advanced features Sony's new range of fixed and minidome IP Cameras will make installation easier. Just point and shoot...

IPELA

HD

For more information, please contact:

Anixter: James Gallon . 09 849 2801 . james.gallon@anixter.com
Channel Ten Security Imports Ltd: Hamish McKenzie . 09 262 0535 . hamish@channeltten.co.nz
Hills Electronic Security Auckland: Richard Hawker . 09 525 8007 . rhawker@hillsec.co.nz
Hills Electronic Security Wellington: Ray Foster . 04 939 9355 . rfoster@hillsec.co.nz
Hills Electronic Security Christchurch: Mike Clark . 03 374 6277 . mclark@hillsec.co.nz

pro.sony-asia.com/productcategory/prof-bc-video-security



SNC-CH140
Network HD Fixed Camera

Unhappy staff risk to company data

More than a third of people who took part in a survey on cyber security thought key company information had been stolen or deleted from their computer system.

Cyber-Ark's global survey, Trust, Security and Passwords, found that 35 percent of respondents believe their company's highly-sensitive information has been handed over to competitors.

Thirty-seven percent of the 400 IT professionals surveyed cited ex-employees as the most likely source of this abuse of trust. But top of the list was disgruntled workers.

Surprisingly, 28 percent suspected "human error" as the next most likely cause for lost data, followed by falling victim to an external hack or loss of a mobile device/laptop, each at 10 percent.

The most popular information employees shared with their firm's competitors was its customer database (26 percent) and R&D plans (13 percent).

The research also confirmed that snooping continues to rise within organizations. Forty-one percent of respondents confessed to abusing



administrative passwords to snoop on sensitive or confidential information – an increase from 33 percent in both 2008 and 2009.

Cyber-Ark's executive vice president Americas says while he understands human nature and the desire to snoop may never be something that can be totally controlled "we should take heart that fewer are finding it easy to do so, demonstrating that there are increasingly effective controls available to better manage and monitor privileged access rights within organisations."

He says with insider sabotage on the increase, the time to take action has already passed and companies need to heed the warnings.

New Zealand computer forensics expert Brian Eardley-Wilmot of Computer Forensics NZ says the surveys findings reflect what is happening in New Zealand. He says that while human error does play a part in data loss, by far and away the biggest culprits are disgruntled employees and ex-employees.

"Many companies are blissfully unaware of the risk they face when a disgruntled employee leaves the company," says Eardley-Wilmot.

"The risk is equally high across all departments and for large or small companies."

Management may never know that deletion or theft of data has taken place until it is too late.

"Companies are lax about protecting the lifeblood of their company. It's just far too easy in most companies for an employee to copy confidential data to a USB stick or email it off-site."

Eardley-Wilmot says if a company suspects an incident might have occurred it is important that computer forensic experts are called in and an investigation started, as over time vital evidence can be overwritten.

"In over 10 years of conducting computer investigations we have noted that if managers suspect data theft has occurred, 99 per cent of the time they're right," he says.

"If a company suspects an incident might have occurred it is important that computer forensic experts are called in and an investigation started, as over time vital evidence can be overwritten," says Eardley-Wilmot.

Check the Facts...



	PROX	iCLASS
Price	✓	✓
Installation	✓	✓
Power Req't	✓	✓
Security		✓++

iCLASS® is your secure migration solution.



HID Global offers a complete range of solutions for organizations migrating to high frequency smart card technology for increased levels of security.



Nearly identical to proximity in price, power requirements and installation footprint, HID's iCLASS® card- and reader-based technology migration solutions enhance your security while making it easy to add new applications or expand existing ones. Whether you are making the transition in a single building or across multiple facilities, the flexibility and convenience of iCLASS migration solutions enable you to cost-effectively upgrade your security to the power of smart cards.

For information on HID Global's innovative line of migration solutions, visit hidglobal.com/migration-NZSec

Concept Dealer Network (CDN) Update

The Concept Dealer Network (CDN) is a group of Inner Range trained and certified installers located throughout New Zealand who are knowledgeable in Concept 4000 Control Systems & Solutions.

Inner Range are world leaders in design and manufacture of state of the art security solutions. Since their inception in 1988, over 100,000 Inner Range systems have been installed in over thirty countries. Amidst impressive growth, Inner Range has remained focused on what it does best; the integration of intruder alarm and access control functionality.

Consumers are increasingly demanding integrated solutions in the implementation of building management technology. Inner Range equipment delivers an impressive mix of power and flexibility, which consistently out-performs its more expensive competitors.

In early November 2010, Atlas Gentech conducted three separate CDN Conferences in Wellington, Christchurch and Auckland respectively.

Inner Range has always played an important part in the New Zealand security industry and Atlas Gentech business is a key supply partner. This years' CDN Conferences were no exception with a large contingent of Aussies coming across including owners Vin Lopes & Doug Frazer, market specialists and engineers Paul Riordan, Adam Lopes & Nathan McGrath.

Attendees were treated to important information on the latest features and improvements to the Inner Range line up including Concept 5000, Insight Version 5 and the very powerful MultiPath IP product range.

The industries leading integrated security and access control management software is about to get a whole lot more powerful. Insight Version 5 has a host of exciting new features such as new user friendly/management screens, tagboard user location system, user credit system, qualification/certification management and updates to the schematic floor plan module.



Vin Lopes, Director of Inner Range presenting at the Christchurch CDN Conference (4 Nov).



Other highlights of the conferences were presentations by:

- Warren Eastwood on the ASSA ABLOY Hi-O and Aperio products;
- Leo Verstegen on the EkoTek integration to Concept 4000 for man-down and lone worker/guard products;
- Mike Allen of Atlas Gentech Distribution (Security) on the CCTV/IP Integration update; and
- Mike Riley of Atlas Gentech Communications on the 3M fibre revolution products.

The CDN as an entity has shown the capability to form powerful partnerships within its members, creating the ability for smaller players to perform at much higher levels of profile.

To become a member, the CDN has certain levels of expectations such as technical ability and performance is enhanced providing a better product package for the end-user.

If you are a CDN member and missed the CDN conferences or would like more information on becoming a member of the CDN or information on any of the products mentioned, please contact your local security representative at Atlas Gentech Distribution.

We are all sure that 2011 is going to be an exciting year for CDN members, Atlas Gentech and Inner Range.

Contact Atlas Gentech Distribution Ltd
Freephone 0800 732 637 • www.atlasgentech.co.nz



SECURE YOUR WORLD IN YOUR HAND

MOBILE PHONE SECURITY SOLUTIONS

Using a Android™ (🤖) or iPhone® (📱) Mobile Surveillance Software Application

A mobile surveillance software application turns mobile phones into a wireless surveillance station, which enables you to watch your home, office, retail store or any other place that is secured by IP surveillance products.



HIKVISION SOLUTION USING THE iVMS-4500 MOBILE SURVEILLANCE APPLICATION



HikVision iVMS-4500 is a mobile phone surveillance application based on iPhone OS 3.0, which supports the full line of HikVision products, including the DS-7000/8000 series DVRs (dual stream models), DS-7300/8100 series DVRs, DS-9000/9100 series DVRs, DS-6000/6100 series digital video servers, as well as network cameras and speed dome cameras that support standard H.264 video codec.



INDIGO SOLUTION USING THE iMON APPLICATION



The Indigo iMon mobile application allows you to access and live monitor your DVRs in real H.264 video streaming over the network with event check, alarm out control and local DVR set-up. Compatible with iPhone and requires iOS 4.0 or later.



ALNET SOLUTION USING THE CMS MOBILE APPLICATION



ALNET Systems CMS Mobile application is designed for mobile phones and PDAs and is currently one of the most advanced solutions on the market. CMS Mobile allows remote access to NetStation / NetHybrid servers from almost anywhere on the planet. Applications are available in versions for all mobile devices with Symbian OS, Windows Mobile, Blackberry or Android.



ONSSI SOLUTION USING THE NETPDA & NETCELL APPLICATIONS



NetPDA and NetCell allow you to create a quick, responsive surveillance system by allowing operators to monitor and control live cameras and even investigate incidents on the fly. With OnSSI's portable video clients, your guards no longer have to stay in the control room. Video from the entire system is now accessible while patrolling via the wireless or cellular network.



These innovative mobile phone security solutions are distributed throughout New Zealand and the Pacific Islands by:

Atlas Gentech Distribution Ltd | Freephone 0800 732 637 | Email orders@atlasgentech.co.nz | www.atlasgentech.co.nz

- Auckland: 8-10 Haultain Street, Eden Terrace
- Wellington: 25 Centennial Highway, Ngauranga Gorge
- Christchurch: 112 Wordsworth Street, Sydenham



ATLAS GENTECH
DATA | COMMUNICATIONS | SECURITY

New Door Station

combines access control with panoramic 170-degree field of view camera capability

Aiphone, a world leader in communication systems, has released a new door station with integrated access control keypad, complementing the range of popular JK-series products. The new JK-DVFAC door station is a flush mount, vandal-resistant unit that provides a 170-degree field of view as well as pan/tilt and zoom control for unprecedented visibility and security.

The new product allows installers to provide a complete solution that also looks great, thanks to its clean, flush mount design and brushed stainless steel fascia. Previously, two units (door station and Access Control Panel) were required to provide the same features, making installation more complicated and giving a less aesthetically pleasing result.

170-degree visibility with pan/tilt and zoom

The JK-DVFAC door station features a fish-eye lens that captures a panoramic 170-degree field of view. This allows users to easily see things that other systems would miss – a person in a wheelchair for example, or someone trying not to be seen.

Fortunately the distortion produced by conventional fish-eye lenses is a thing of the past; Aiphone has developed technology to compensate for lens distortion, resulting in a clear picture that allows perfect visibility.

Further enhancing visibility, the user can also control camera pan and tilt, and can zoom in to any area to precisely identify all visitors.

Fully featured access control

The access control panel offers important features such as lockout function to prevent attempted entry via random key presses, an anti-tailgate function, an output for triggering an alarm on forced entry, illuminated keys and a one-touch door release when used with an external timer.

Vandal resistant design

The JK-DVFAC door station is a flush-mounted, stainless steel design, making it extremely rugged and resistant to vandals.

For added security it is mounted to the wall using tamper-proof screws. Furthermore, the unit is weather resistant to IP54 for durability in all outdoor conditions.

Pricing and availability

The JK-DVFAC is available now and for more information on pricing please call the New Zealand distributor Audio Products Group on (04) 2320 030 or visit www.aiphone.co.nz.



Contact

For further product information please call:
Johnathan Meads (Product Manager) at Audio Products Group
on Telephone: 00612 9 578 0177 or
Email: jmeads@audioproducts.com.au

About Aiphone

Established in 1948, Aiphone has become the most respected and reliable intercom brand in the world. Aiphone's range extends from simple do-it-yourself door audio intercom kits to sophisticated multi-access apartment and commercial video systems. Every Aiphone system is engineered to last and 100% pre-tested for sustained trouble free operation.

Aiphone's family of video door intercoms

Aiphone, the world's leading manufacturer of security intercom systems, has recently introduced the innovative JKW-IP adaptor for its JK family of video door intercoms.



The JKW-IP adaptor allows the JK system to be extended to an IP-connected internal station, which can be located on premises or anywhere with an IP connection. The JKW-IP allows visitors to premises with JK intercom systems to be remotely identified, engaged in conversation and, if appropriate, admitted to the premises. The JK intercom with JKW-IP adaptor can be used in



residential or commercial applications: anywhere that requires remote or PC-based monitoring of the door intercom system.

For added flexibility, the JKW-IP system can be monitored by up to ten remote PCs. For large network applications, each remote PC can monitor up to twenty JKW-IP adaptors in up to twenty distinct locations.

For further information about the JK video door intercom or the JKW-IP adaptor, please contact a Aiphone Key Dealer.

To contact your nearest dealer:
Call 0800 111 450 or visit www.iphone.co.nz



Peace of mind
-without compromising style

Aiphone JK Series Video Intercoms



The Aiphone JK Series offers safety and security while stylishly complementing any home's exterior and interior decor.

The sophisticated JK Series is easy quick and easy to install, requiring a single-pair cable between the entrance station and the internal station.

The entrance station is available in several different configurations, optionally with an integrated access control keypad (shown). A high intensity LED illuminates the scene for clear pictures 24 hours a day.

Internal stations feature digital pan/tilt/zoom and a wide 170° view of visitors. The optional picture memory (shown) automatically records six images whenever the call button is pressed, providing enhanced security irrespective of whether there is any one at home.

Backed by a two year warranty, the Aiphone JK Series offers peace of mind without compromising style.

FOR YOUR NEAREST DEALER:

Call 0800 111 450 or visit www.iphone.co.nz

Proudly Distributed by

audioproducts
Group

One on One

with Ian Anderson

General Manager ADT Armourguard

What chain of events led you to a career in the security industry?

My first role on leaving university was as an assistant accountant for Armourguard – so my history with the company and the security industry goes back a long way.

I undertook some other significant roles as financial controller and director for some New Zealand and international companies over a nine year period, before returning to the Tyco Group.

In 2000, I became financial controller for Armourguard NZ, then moved to Sydney to take up a position with Wormald as director of planning and financial analysis. I later returned to New Zealand to take up my current position in 2007 as ADT Armourguard General Manager for NZ and Fiji.

What has been your biggest industry achievement so far?

It has been personally rewarding to get involved at a strategic level with shaping the security industry through my current role and while working as Wormald's director in Australia.

This strategic focus has given me a tremendous insight into the direction the industry is moving towards. It's also given me a great opportunity to influence levels of professionalism and services provided, all of which are becoming expected in our industry.

It has also been satisfying to build on ADT Armourguard's success over the years – to have a hand in empowering our managers and our front-line staff to serve New Zealand businesses, homeowners and communities with the best that the industry has to offer internationally.

I think the absolute non-negotiable in this industry is to be dependable. That means you need to have a strong work ethic, be consistent and always ready to face up to unexpected challenges.



The range of products and services available to the security industry is continually expanding, as we think of better and more innovative ways to protect people and property. It's exciting and rewarding to be part of this wave of change that allows us to make a significant contribution to the safety of New Zealanders.

What concerns you about the industry at the moment?

Our industry is being put under constant and growing pressure from rising crime. Today's environment is such that people now view robberies and violence as commonplace – something that affects families and communities as a whole. This is a real concern not only for our clients but also for our industry which is charged

with protecting people and property. As a result, our people are increasingly facing potentially dangerous situations.

We need to keep working to ensure the safety and wellbeing of our front-line security staff. Attracting responsible, professional and dedicated people to the industry and keeping on top of this growing crime wave is critical.

What are the most enjoyable parts of your job?

I get a huge sense of enjoyment out of interacting with our people at all levels. I'm proud of the professionalism they show through their work with our clients and the way that so many of them go the extra mile when dealing with our customers.

I receive stories almost daily about security officers somewhere in New

Zealand or Fiji who have done something exceptional and made a difference in someone's life.

For example, just recently a couple of our people working at Auckland Airport were able to use their CPR training to revive a man who had had a heart attack shortly after arriving in New Zealand – there can't be anything more rewarding than that.

We're a strong community and the contact I have with our staff and their families is also immensely rewarding.

What are the key attributes for someone working in your area of the industry?

I think the absolute non-negotiable in this industry is to be dependable. That means you need to have a strong work ethic, be consistent and always ready to face up to unexpected challenges.

I think you need to be 100 per cent committed to your community, and understand the importance of people feeling safe in terms of the implications for their health and wellbeing. It's also very important to treat each person you interact with, even those committing crimes, with respect and courtesy.

We live in a complex society, therefore, a person working in security needs to be able to understand and work around anti-social behaviour so that everyone's security is maintained.

In my role as general manager I also think it's important to be able to put things into perspective and have the foresight to see changes coming that could affect people and the working environment.

I believe that there are always ways that things can be done better. Together with my management team, we work hard to constantly improve the way that we work and to create better outcomes for our clients and staff. This is a crucial focus for our business and one that we nurture and encourage in all our people.

What technological advances in security are you most excited about?

The explosion of wireless applications for technology has huge implications for our industry's future.

On the one hand, there are a wide range of technologies which are emerging in wireless format which have the potential to transform our access to security information.

However, at the same time, we also need to be vigilant about the very real risks to the security of that information and protect it from hackers or electronic theft and vandalism.

I believe that over the next two to three years, we will see a major surge in applications of wireless technologies in the security industry. These advances will give us and our clients ready access to technological 'eyes' and 'ears' that we'll be able to use to counter all kinds of criminal activity. Our challenge is to remain at the forefront of utilising such cutting-edge technology and embrace advances as they become available – these are exciting times.

If you could change one thing about the industry, what would it be – and why?

It would be fantastic to be able to change some of the perceptions held in the community about the services we provide and the value we add.

Security is no longer just about having a mean looking thug outside your door, ready to deal to anyone who looks suspicious. It's about having the right security products and professional security personnel in place who really understand a client's diverse and constantly evolving needs.

I would love to be able to reinforce among clients that the services we provide are fundamentally important for their safety and wellbeing, and therefore, carry significant value.

How do you think the security industry is perceived by the public?

I'm concerned about the whole issue of public perception of our industry. As a market leader, I expect ADT Armourguard to lead by example. Because we are involved in so many aspects of everyday life in New Zealand, I think public perception of our services is pretty high. This is borne out by the many letters and positive comments we receive from the public and our customers.

However, I believe there are people in the community who have not had good experiences from some security companies; and whose criticisms unfortunately affect the industry as a whole.

It's important to me that our industry keeps its standards high, and works hard to build public confidence. Through our management structure and our intensive training programmes, we're certainly working towards those goals.

What do you do in your spare time?

In my spare time I'm a husband and father, and love spending time with my family.

Movers and Shakers at Ingersoll Rand Security Technologies

Ingersoll Rand Security Technologies is pleased to announce the appointment of Jeff Bennett as National Sales Manager for Residential Products. Jeff assumed this role on 1 October, taking over from Owen Thompson who is set to retire early next year.

Jeff has been with Ingersoll Rand for four years, starting as a Sales Consultant in the South Island before transferring to Auckland early this year to lead the marketing department.

Craig Patterson has recently joined Ingersoll Rand as the Marketing Coordinator, returning to New Zealand after four year overseas work experience in South Korea. Craig has over five years of marketing experience at Karcher Ltd in New Zealand and Germany, and a Bachelor of Business from the Auckland University of Technology.



Craig (left) and Jeff (right) are proud to be assuming their new roles, and look forward to working with Ingersoll Rand's channel partners to create demand for world leading brands including Schlegel, Legge, D&D Technologies and Henderson.



Securing the colourful world of small and medium sized retail

Contributed by Wai King Wong, Country Manager, Axis Communications

The world of small and medium sized retail is colourful. It's the diversity of ground-level retailers in the dense downtown areas that often defines a city's image. With the thousands of shops that have had to close across the globe because of the recession, this world is at a risk. But latest statistics from the US and Europe indicate that we have left the hard times behind and domestic demand is on the rise again almost everywhere. It's the right time for retailers to look forward and revise their strategies to secure the future of their businesses. Whereas IT technologies such as CRM or ERP play a central role for national retailers as they help retailers to improve their bottom line by giving them a better understanding of what their customers really want, many small shops can't afford those technologies. It might come as a surprise but video surveillance can be also a very cost efficient technology alternative that helps retailers to better understand their customers and improve their businesses.



A modern, state-of-the-art surveillance system goes way beyond mere surveillance and can even help retailers to enhance the customers' experience.

Traditionally, retailers have implemented surveillance systems to deter and catch shoplifters and violent criminals. But today's network video surveillance systems offer retailers much more than that. A modern, state-of-the-art surveillance system goes way beyond mere surveillance and can even help retailers to enhance the customers' experience. Equipped with people counting or heatmaps, such a system can detect the number of people entering a shop, waiting in a queue or if parts of the shop are overcrowded. It can send an alert directly to the store manager

who can immediately take measures. If the cameras are connected to the data generated by the POS system, retailers can analyse how conversion rates and sales amounts vary over time.

They can measure customer "dwell" times to evaluate the effectiveness of campaigns and in-store advertisements. They can also control items in stock, detect empty shelves and send out an alert that restocking is needed. The whole gamut of in-store processes can be streamlined efficiently with network video systems, resulting in higher profits.

Retailers' internal departments are starting to leverage each other's technology deployments. This cost-saving approach promotes cross-functional and organizational use of an existing investment in network and surveillance infrastructure. Operations and marketing people are now more and more aware of the fact that their surveillance system can be used for much more than spotting suspects.

Contrary to the popular belief, video surveillance systems are not only deployed by the big national retail chains but are also a useful tool for small and medium sized shops. However, the requirements of the small and medium sized retailers are very different. Whereas large retailers are much more willing to make short-term investments, smaller businesses are rather looking for future-proofed investments.

For retailers that are looking for future-proofed solutions, it would be especially prudent to consider network video surveillance systems over analog ones as they can operate over the existing internet already installed in the shop and be managed by the existing computers. What is even more important is the

compatibility with the existing store infrastructure, like e.g. POS and EAS systems. Another important detail that makes an investment future proof is open standards. As the EU Commissioner Erkki Liikanen formulated in 2003 "Open standards are important to help create interoperable and affordable solutions for everybody. They also promote competition by setting up a technical playing field that is level to all market players. This means lower costs for enterprises and, ultimately, the consumer."

Further, open standards give you maximum flexibility when choosing the peripheral equipment. The solutions are fully scalable and allow retailers to take advantage of the latest technologies and features. And these vary a lot among different retailers: highly specialized businesses that know their customers by heart might look more into security applications, shops in areas that face violence problems will be more concerned about staff safety, whereas small chains in a competitive landscape have a critical need to understand their customer to better stimulate their demand and therefore would need more video analytics features.

For retailers that are looking for future-proofed solutions, it would be especially prudent to consider network video surveillance systems over analog ones as they can operate over the existing internet already installed in the shop and be managed by the existing computers.



For those retail shops that need a video surveillance system for safety or security reasons, image quality is crucial. The better the image quality is, the easier the identification of incidents. Network cameras with HDTV standard are a leap forward in image quality by providing up to five times higher resolution than standard analog TV.

There are special video surveillance kits for small and medium sized retail stores. Axis Communications for example offers a complete, easy to install network video surveillance solution that includes network cameras and professional monitoring and recording software. The kits can be easily expanded if more cameras are needed. The company has a further intensive network of development partners, giving retailers access to all type of critical retail applications.

The world of retail is very diverse, and so are the needs of retailers. However, network video surveillance is an attractive technology that can help all types of retailers, from the smallest corner shop to the global retail chain, to cost efficiently secure their businesses, making sure the customer can also benefit in the future from a colourful range of offerings.



Mobile technology escalation outstrips forensic capabilities

Keith Newman discusses an out-of-control security dilemma with mobile forensics guru John “Zeke” Thackray

Businesses wanting to retrieve lost or erased data from mobile devices or create a chain of evidence for legal reasons should be wary of investigators and security companies who claim it's a simple matter, warns world respected computer forensics specialist John Thackray.

While there are tools that can extract layers of data from cellular devices to assist with cases of fraud, misuse and industrial espionage, their availability and the skills needed aren't typically available in New Zealand, says Thackray.

From a forensic and investigative perspective he insists New Zealand is way behind the rest of the world, and with the growing sophistication of mobile devices that gap is getting wider.

“Unfortunately there are no dedicated corporate mobile phone forensic professionals in New Zealand today and most organisations send mobile devices under suspicion to Australia or further afield.”

Thackray, who lives in the Far North and travels widely for various ‘agencies’, was first brought to New Zealand on secondment from the South Yorkshire Police early in 1998 to help NZ Police establish an electronic crime unit. Later that year he returned to the UK to receive the Churchill Fellowship Medallion from British Prime Minister John Major for his efforts in computer crime research, which included working with the FBI and British Secret Service on electronic evidence gathering.

He was instrumental in bringing together conventional and electronic forensic techniques, establishing standards and helping to create a global ‘family’ of computer crime investigators able to track cross-border fraud, so evidence gathered in one country was acceptable in another.

Thackray helped establish the New Zealand Electronic Crime Unit which improved the country's ability to investigate and present credible electronic evidence before the courts.

Before being recruited to work in private sector security he helped identify a group of university students who were crashing Unix businesses servers across New Zealand and assisted in the prosecution of ‘denial of service’ attackers, who were bombarding the mail servers of businesses and ISPs (Internet service providers) with data.

Difficulties of analysis

Thackray is now in demand across the world for his expertise in investigations that require deep analysis and extraction of hidden or deleted data from mobile devices that may have been used in corporate fraud, organised crime or terrorism.

In New Zealand however he says there are few local security companies with internal forensic or investigative personnel who can recover deleted documents or communications records. “If those capabilities are required in New Zealand they're most often outsourced.”

While the New Zealand Police claim to specialise in cell phone chip analysis he's not seen any case studies. “The only evidence is of them using point and click and ‘hook, suck and look’ tools that only take a logical impression of the device.”



Mobile forensics specialist, John Thackray

High Speed Gate Automation

From commercial gates to heavy prison gates, barrier arms to high speed swing gates, with a variety of high speed gate motors.



We installed a high speed automatic gate motor to a 15m gate in Palmerston North



This prison gate has a large capacity slide gate motor and moves at 600mm per second

We also manufacture, install and service

- ◆ Stainless gate drop bolt locks
- ◆ Remote controls and receivers
- ◆ Cantilever slide gate hardware
- ◆ Vehicle loop detectors
- ◆ PIR safety beams for automatic gates and doors
- ◆ Keypads wireless and stand alone fixed wired
- ◆ Light commercial 24v linear swing gate motors



A barrier arm for Peter Jackson's Wellington Headquarters



These swing gates are part of the Government House refurbishment



Swing gate motor for gates up to 15m

We design and manufacture all our automation products in Wellington, but pride ourselves on our installation and service anywhere in New Zealand.

For more information and trade enquiries contact:

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

This simply means they connect a suspect device to a so-called mobile forensic tool to extract visible data and then print a report. While tools such as Paraben, CelleBrite UFED, XRY and Access Data Mobile Forensic Tool might be used, Thackray says they miss vital information.

“These tools in their logical extraction function do not truly recover deleted data. They facilitate an investigation by quickly gathering on screen information so it can be reviewed and responded to but this is not forensics.”

And while these expensive devices can be helpful in an investigation, a combination of tools is required to extract information from the numerous devices now on the market. “Even then they do not recover truly deleted information,” says Thackray.

Mobile challenge escalating

He told NZ Security magazine that increasingly sophisticated mobile devices are presenting a real challenge from an investigative perspective and warns security issues will only increase as organisations move away from desktop and laptop computers.

“The criminal fraternity are now actively conducting counter surveillance when purchasing devices for use in organised crime such as drugs, money laundering and terrorism,” says Thackray.

“We have seen this in Mexico and the Middle East over recent years when the cartels and terrorists surf the mobile forensic forums to establish which phones can and cannot be examined.”

Once it is determined which phones are best suited for their purposes, the subsequent demand for this functionality results in manufacturers increasing their development which in turn making those types of devices more affordable, says Thackray

The use of stronger encryption on mobile devices, including cheaper brands, further adds to investigator frustration.

“Because there are now more cellular type devices in use than computer devices, law enforcement agencies, often using outdated detection and forensic tools, are becoming overloaded.”

And he says devices that can circumvent standard mobile communications with wireless, instant messaging (IM), Yahoo Chat, Skype and webmail are now commonplace.

“Unfortunately there are no dedicated corporate mobile phone forensic professionals in New Zealand today and most organisations send mobile devices under suspicion to Australia or further afield,” computer forensics guru John Thackray.

Thackray says it was predicted in the mid-1990s when he first came to New Zealand that users would eventually have access to their entire life information and communications needs from a handheld device. It was also determined that off-site storage of data in a cloud environment would also be a function of the future.



Organised crime syndicates conduct their own counter surveillance to ensure the mobile devices they purchase have high levels of encryption and are difficult for forensic investigators to recover data from

SAMSUNG TECHWIN

SCD-2080P

High Resolution Day & Night
Varifocal Dome Camera



- High resolution 600TV lines & 0.15Lux sensitivity
- 3.6x varifocal lens (2.8 ~ 10mm)
- Discreet and compact design
- 1/3" Super HAD Colour CCD
- SDDR (Samsung Super Dynamic Range) for better image clarity and detail Day & night with ICR (infrared Cutoff Removal)

SAMSUNG TECHWIN

SRD-1650D

Explore outstanding features of the new
DVR, H.264 Realtime series



- 4CIF Real-time Recording (SRD-1670/1670D/870/870D series)
- CIF Real-time recording (SRD-1650/1650D/850/850D series)
- 8Ch / 16Ch Audio Input & 1Ch Audio Output
- Main Display Capabilities: Composite, VGA, HDMI
- Programmable Spot Monitor Outputs
- Built-in Web Viewer
- SATA I/F HDD Support (Internal Max. HDD x 6HDD x 5)
- Smart Viewer Samsung Central Monitoring S/W Support
- Dual Codec to enhance recording and network transmission

SAMSUNG TECHWIN

SCB-3001P

Clear Image in the Dark
Super Hi-Resolution WDR camera



- Excellent high resolution 600/650TV lines color images
- Low light sensitivity of min. 0.3Lux
- 2D/3D filtering noise reduction technology, SSNR III
- 128x WDR (Wide Dynamic Range)
- ICR Day & Night function, 512x sens-up support
- PIP, coaxial control support



EOS New Zealand Ltd

Unit B, 156 Bush Rd, Albany, Auckland

Telephone: 09 448 2040 • Facsimile 09 448 1178

Email: sales@eosccv.co.nz • Website: www.eosccv.co.nz

SAMSUNG TECHWIN

SCP-3430HP/3430P

43x Zoom, Super High-Res, WDR PTZ



SCP-3430H/3430/2430H/2430 PTZ dome cameras are able to capture quality images over expansive areas thanks to the inclusion of a 43x optical zoom.

Embedded with Samsung Techwin's A1 chipset, these cameras offer clear and vivid images with 600TV lines color resolution and are able to perform perfectly at low light levels down to 0.7Lux/0.2Lux. SCP-3430H/2430H versions are pre-fitted into a housing for extra convenience.

43x Zoom High Resolution WDR PTZ Dome Camera

- Powerful 43x optical zoom (3.2 ~ 138.5mm)
- High resolution of 600TV lines (Color)
- Min. illumination of 0.7Lux (SCP-3430H/3430) 0.2Lux (SCP-2430H/2430)
- VPS (SCP-3430H/3430), coaxial control support
- Intelligent video analytics (Moved/Fixed)
- WDR backlight compensation (SCP-3430H/3430)

SANYO

VCC HD 5600P

Full HD High-speed Day/Night PTZ



- Built in x 10 megapixel - rated lens (6.3 to 63mm)
- 360-Degree Continuous PTZ
- 1080p Full HD, 25 ips Full Framerate with H.264
- Exclusive Xacti HD-Pro engine and Optimum IP-Pro engine
- Quad Stream
- Digital Image Stabilizer
- Video Analytics
- Bidirectional Audio
- Edge Recording on SD Memory Card
- External HDD

SANYO

VCD-HD3100P

Full HD Vandal-Resistant
Dome Camera Series



- Built-in megapixel-rated Vari-Focal Lens (3 - 9mm)
- IP66-rated Vandal-Resistant Discreet Low-Profile Design
- 1080p Full HD, 25 ips Full Framerate with H.264
- 4-megapixel (2288 x 1712) resolution with MJPEG
- Exclusive Xacti HD-Pro Engine (HD3500P) and Optimum IP-Pro Engine
- Quad-Stream (HD3500P), (HD3100P/HD3300P)
- Focus Assist Drive
- Video Analytics
- Edge Recording on SD Memory Card
- Bidirectional Audio
- Universal Power Input PoE, 24VAC and 12VDC

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 \$52.00 including 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
PO Box 4, Ahipara,
New Zealand 0449

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

Mr Mrs Ms _____

Surname _____

Title _____

Company _____

Postal Address _____

Telephone _____

Email _____

Date _____

Signed _____

nz Security Magazine
A trusted source of information for industry professionals

Mobile Security Assessment

- Undertake due diligence to select the best phone for your specific use
- Avoid clones or unknown brands devices
- Ensure you can get firmware and software updates on demand
- Make sure the phones can be encrypted to protect data
- Supply laptop and cell phones to key employees only
- Train all users how to securely and acceptably use laptops and cellphones
- Training should include way to identify if a device has been compromised
- Create acceptable use policies and strictly enforce them
- Unless a camera capability is required for the job, disable this function
- Turn off Bluetooth or enforce a policy on how and when it should be used
- Don't connect mobile devices to the corporate network using default security settings
- Never connect with unknown third parties or devices
- Management applications should include the ability to remotely wipe data from a mobile device if it is stolen or misplaced

"Clearly all of this is now well and truly with us. You have only to look at modern day activity to appreciate how hand held devices are taking over our every day lives."

Mobile as remote control

He says the advances are such that he can use his cell phone to open the main gate to his driveway as he approaches, remotely switch on the TV and record a favourite programme or open and close the curtains and turn the lights on and off to give the impression someone's at home.

He says future capabilities are only limited by the imagination of manufacturers and users. Mobile devices even present a challenge to credit and debit cards as they implement wallet functionality, something cell phone manufacturers have been gearing toward for years.

This is already available on several branded mobile phones, including Nokia, where the 'wallet' function is associated with a secure container on the device, designed to protect sensitive data, including passwords, banking information, account details and statements.

Initially cell phone wallets might be used to pay parking, tolls, movie tickets or bar tabs, with loyalty and other applications making this an increasingly preferred form of transaction once the major credit card companies and the banks formalise their agreements.

Meanwhile, Thackray says criminals are always one step ahead of the corporate world, enforcement agencies and security firms and that's unlikely to change.

"Manufacturers of handheld devices must ensure they not only develop the capabilities of devices but also keep pace with security requirements, particularly malware and virus protection."

And he says security companies need to make sure they have access to the right skills sets to advise their clients on safe practice and to help determine security risks and breaches.

This is where the security industry and information technology and telecommunications professionals need to find common ground. While there's clearly a convergence between telecommunications and computer networks, Thackray says ICT personnel need a broad range of skills in both disciplines and to develop and maintain new skills.

Do due diligence

He advises businesses looking to purchase mobile devices for their employees to go through a strict due diligence process and put in place acceptable use policies which should be strictly enforced.

This might include policies for the use of devices with cameras. "If that capability is inappropriate then a device without a camera should be selected to avoid the temptation of abuse by employees."

Training on how to safely and securely use this equipment should be an essential part of orientation when employees join a company or when the equipment is issued, says Thackray. And companies should insist employees read work related policies, agreements and conditions of use in their entirety before signing.

"I have seen many incidents occurring within a corporate world because the individuals did not know how to use the Blackberry or laptop. Training in their secure use would have avoided the subsequent leakage of information," says Thackray.



It is important businesses wanting to keep data secure have the ability to remotely delete sensitive information on a device if it is stolen or lost, a feature commonly available for RIM Blackberry devices and iPhones

Particular caution is urged when choosing a mobile smart phone that can connect back into the corporate network. These should be properly configured to suit the circumstances and made extremely secure rather than “simply clipping on devices with default settings”.

He says it is essential to secure sensitive data on a device if it is stolen or lost. “It is common knowledge that data on Blackberry devices and iPhones can be deleted remotely. Remote destruction and strong encryption are a must for any organisation.”

Security policies will vary between devices and how they are used internally and remotely. These policies should include the use of Bluetooth and infra red (wifi) communications for example and whether these should be switched on or off.

“Most spyware on mobile phones uses compromised Bluetooth functions so users must not accept pairing from unknown devices. Switch Bluetooth off, if you are not using it.”

Policies should also address whether employees are permitted to communicate via IM (Instant Messaging), Yahoo, Facebook or Skype and if they do, to ensure these are used correctly. “Users should not accept incoming calls or

requests from people they do not know.”

Compromised communications

While some organisations supply both a laptop computer and cell phone to employees as part of a wider incentive package, Thackray recommends this should be restricted to key personnel.

Determining whether a mobile device has been compromised, depends on understanding what a third party may be trying to attempt. He says understanding the tell tale signs should be part of the basic training and instruction to help users become aware of unusual functions and activity.

“Know what it can do and what it should be doing, switch off any functions that are not being used and restrict any applications that are loaded to the device such as games, music and video’s.” Before such applications are enabled they should be tested and approved by the security administrator.

And Thackray urges the major mobile carriers and manufacturers to lift their game in quality assurance of their products, making users aware of any security vulnerabilities and where necessary providing firmware updates if modification is required.

“This is common for iPhones where it is made simple for users when they

**For more information on
mobile security and computer
forensics contact
John Thackray:**

Email: services@thackray-forensics.co.nz
Web: www.thackray-forensics.co.nz

connect to iTunes and in the background all firmware updates and automatically notified.”

He says software and hardware vendors should not just keep producing new phones as a revenue process but keep pace with secure technology requirements.

“On average at least 50 new cell phone models are released each month and that’s not counting the counterfeit copies from China, Peru or Mexico which are widely available in New Zealand and Australia.” Keeping pace with technology is difficult enough but the growth of counterfeit devices, malware and viruses is creating a nightmare for Police and private and corporate investigators.

What makes the present situation worse says Thackray is that misuse and abuse of hand held devices is often outside the current knowledge and understanding of most organisations in New Zealand.

Gallagher once again celebrates success at the NZ International Business Awards

Gallagher Security Management Systems (GSMS) is celebrating success again as the winner of the 2010 New Zealand International Business Awards \$10-50 million category.

The annual event, held last month, commends companies who are succeeding in international markets and leading the way in international business. The award recognises success by net return to the New Zealand economy for businesses with total annual revenue between \$10 million to \$50 million.

GSMS designs and manufactures Cardax electronic access control and intruder alarm systems and PowerFence™ electric perimeter security systems and General Manager, Curtis Edgecombe, believes innovation is one of the key factors that sets Gallagher Security apart.

"We've had a number of world firsts and got a march on those competitors. There

"We've had a number of world firsts and got a march on those competitors. There are some products we developed up to nine years ago that our competitors are only managing to replicate now."

are some products we developed up to nine years ago that our competitors are only managing to replicate now," he says. "Using innovation and highly skilled people to come up with ideas for functionality and ease of use, differentiates us from our competitors.

We are the only company which manufactures a perimeter security system which integrates with an access control system."

The Gallagher Group employs a team of more than 90 Research and Development staff who have a thorough knowledge of the security sector including electric fence technology, radio frequency identification, IT and security requirements, data encryption, high security applications, systems integration and industrial design.

"R&D is a huge part of our business. Each department at Gallagher Group leverages off the other, and R&D supports all divisions," says Curtis Edgecombe.

Gallagher's security products are currently used around the world for a huge variety of purposes, ranging from protecting small businesses to controlling access points at international airports.

Judges of the category commended GSMS for its innovation, design and manufacturing which successfully markets its products to over 130 countries via the business unit's expansive network of channel partners worldwide. "Gallagher Security Management Systems is an innovative, well-run company. It has sophisticated and well thought out market entry strategies and spends significant time and effort listening to its customers. It approaches research and development in a sustainable way and with a clear understanding of future opportunities," commented the judges.



Bill Gallagher, CEO of Gallagher Group, accepts the NZIBA award for the company's security division.

The Gallagher Group has celebrated numerous successes across the globe this year with GSMS being a Security UK Finalist in 2010 IFSEC Security Industry Awards, two leading Gallagher animal management products scooping medals at the 2010 Plastics Industry Biennial Design Awards, and Bill Gallagher was also awarded the 2010 World Class Manufacturing Award.

The Gallagher Group is working in close partnership with New Zealand Trade and Enterprise (NZTE) to promote its business in key export markets around the world and expand its global reach. The latest push has been into Asia and South America with the help of NZTE, and the company has recently received co-funding support to research a vertical market in India.



Gallagher's access control product, Cardax, secures education facilities around the world include La tribe University, Australia.

"We want to be seen as New Zealand's largest global technology firm in time, and in order to do that, we want to have a single brand that's globally recognised across all divisions – agriculture, security or fuel systems," says Curtis Edgecombe.

In India, Ibex Gallagher has secured a contract with India's largest automobile manufacturer Tata Motors Limited while the first Trophy FT PowerFence system was installed in China to secure the 1.2 kilometre Governments Research and Development Centre for Fighter Aircraft site in Anhui Province. GSMS also recently won a major contract in the Middle East to provide an integrated security solution for the Etihad Towers in Abu Dhabi.

In North America GSMS is working on developments in correctional facilities, airports and utility sites. "There's a huge

growth potential; perimeter security is well established," says Curtis Edgecombe.

The vast differences in requirements of the customers means it's important to have a very clear understanding of what the customer wants, says Curtis Edgecombe.

"It's about creating technology that solves business problems, not creating technology for technology's sake," he adds.

"In our security division we have a very strong customer focus and it goes right through from the CEO Bill Gallagher, to the R&D staff, marketing teams, technical support people, and everyone else in the company. We travel to the markets and talk to the end users – it's particularly important when you're developing new products."

Because of Gallagher Security's strong customer focus and its ability to configure



Since installation of Gallagher's perimeter security system at Cadbury there have been no intrusions onto the St Kilda site.

the products to suit the customer's needs, GSMS is witnessing a movement away from pure security. Customers are able to adjust and adapt the system to their specific needs, including using real-time compliance for safety precautions, for example.

"Security is traditionally seen as a cost in an organisation, so we're trying to show businesses that we can deploy systems that will provide them with real business savings or benefits," says Curtis Edgecombe. "GSMS is now addressing competencies such as First Aid qualifications and risk management; is this person allowed to be on site, when do their competencies or qualifications run out?"

He says receiving the 2010 New Zealand International Business Award is great recognition that reinforces the hard work put in by the staff in all departments across the Gallagher Group and reaffirms GSMS's place in the security market.

On receiving the award CEO Bill Gallagher explained that while the security unit is very successful in its own right, what sets it apart is its ability to leverage the competencies and resources from other divisions within the whole Gallagher Group.

"Our in-house resources for tool making, plastics and electronics manufacturing, and logistics mean that production can be controlled end to end from concept design to manufacturing.

The benefits of this include quality control, rapid development and deployment to manufacture, and the ability to produce economic short runs as well as large production capability. All of this is centrally managed on our Hamilton site."



GSMS partners with various commercial developers including Sime Darby, Malaysia's leading multinational conglomerate.

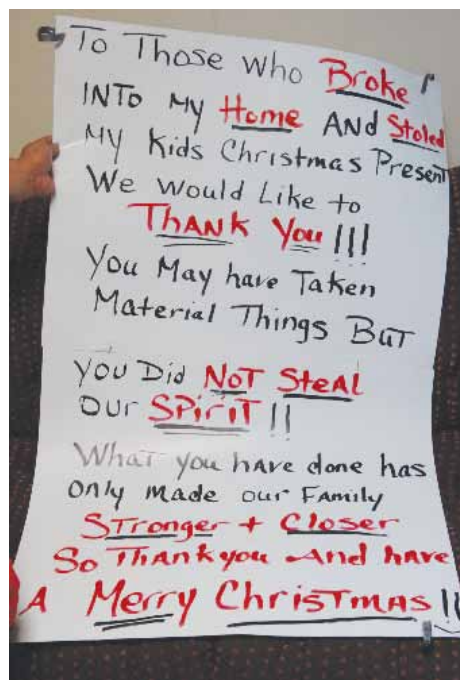
It's that season again!

By Fraser Burns

Have you taken the time to evaluate your current security preparations. Because this is the high risk season again.

Thieves and burglars know that you are more likely to have nice new things waiting for them. Whether it is the Christmas presents waiting under the tree, or the new plasma TV system that you are enjoying, they know that you will have things that are nicer than what they have. So they are going to target you!

Are you prepared to write a message to the burglars like this family did?



It is one thing to acknowledge that there is more to life than just things.

It is a different story when you have to face your family because their presents have been stolen, their home ransacked, horrible things sprayed all over the house, and they no longer feel safe. This is the reality that as Locksmiths we so often see. Too often people don't do something about their security until they have already been "done over" the first time. The cost of a typical burglary starts at \$1000 and rapidly goes up from there. These costs are much higher than the preventative locks.

While it is impossible to make your home or business absolutely impervious to attack, you can make an amazing difference with surprisingly little effort.

About 90% of burglaries can be stopped by implementing security measures that won't break the bank, although they may require you to plan how to implement them. The first step is to examine what you currently have. The second step is to determine what you need. When talking to a professional you need to make clear whether you only want to install minimum security or whether you want quality security fittings. Most devices come in standard models and heavy duty models. Obviously there is a cost difference.

What security do you currently have? Examine the locks you currently have installed.

1. What brand and model are they?
2. Are they the appropriate function for where they are installed?
3. Should they be operated by key from each side of the door? Should they be Fire Safe?
4. Should they automatically lock when you pull the door closed?
5. Are they strong enough?
6. Is the key mechanism secure enough?
7. Do you have one key to operate all your doors or do you have to search through a whole bunch of keys?

If you haven't yet graduated in the course of "What Locks Have I Got," then you can always contact a Master Locksmith to come and provide you with an evaluation. They have experience in what works and what merely looks good. For example: I was called out to a butcher's shop which had been burgled overnight. He had a Jemmy resistant deadlock on the front door which is exactly what was appropriate for that specific location. The problem was that this door had been jemmed open!

How could this be?

On closer examination it soon became clear. The owner had not liked the price of a quality lock offered to him by our locksmith. \$200 seemed to be a lot of money. So instead he had gone to an alternative hardware store and bought what looked like the same lock but in a different brand for about \$40.

Both locks mount in the same position. Both locks were key operated from each

side. Both locks had the same functional description. But the cheaper lock was made with less metal. Lots less metal!

So much less metal was used, that in the couple of years that it had been on the door, the casting has steadily broken open and the owner had kept sellotaping it together. So when the burglar had a go at the door, all he had to do was break the sellotape.

Guess what ... he was successful !!!

The savings from the cheaper lock was \$160. The cost of the burglary was over \$10,000. Wasn't that a great saving?

The range of locks available grows every year. There are locks for swing doors and sliding doors, roller doors and tilter doors, letter boxes and rubbish bins, motorboats and trailers, windows and sheds. The options become better matched each year to your application. Sometimes the price comes down. But that is only good if the quality has been maintained and only the manufacturing process has been made more economic. Otherwise you are installing a "pretty picture" and not actually improving your security.

Unless you are sure of your facts, call into a Master Locksmith, or get them to pop around to your place to find out whether what you have will provide effective deterrent for the 90% of burglaries that you **CAN STOP!**



Fraser Burns is the current President of the New Zealand Branch of the Master Locksmiths Association of Australasia Ltd.
Email: safe@safemasters.co.nz
or contact the Master Locksmiths Association of Australasia Ltd:
Web: www.masterlocksmiths.com.au
Email: national@masterlocksmiths.com.au
Ph: 0800 652 269



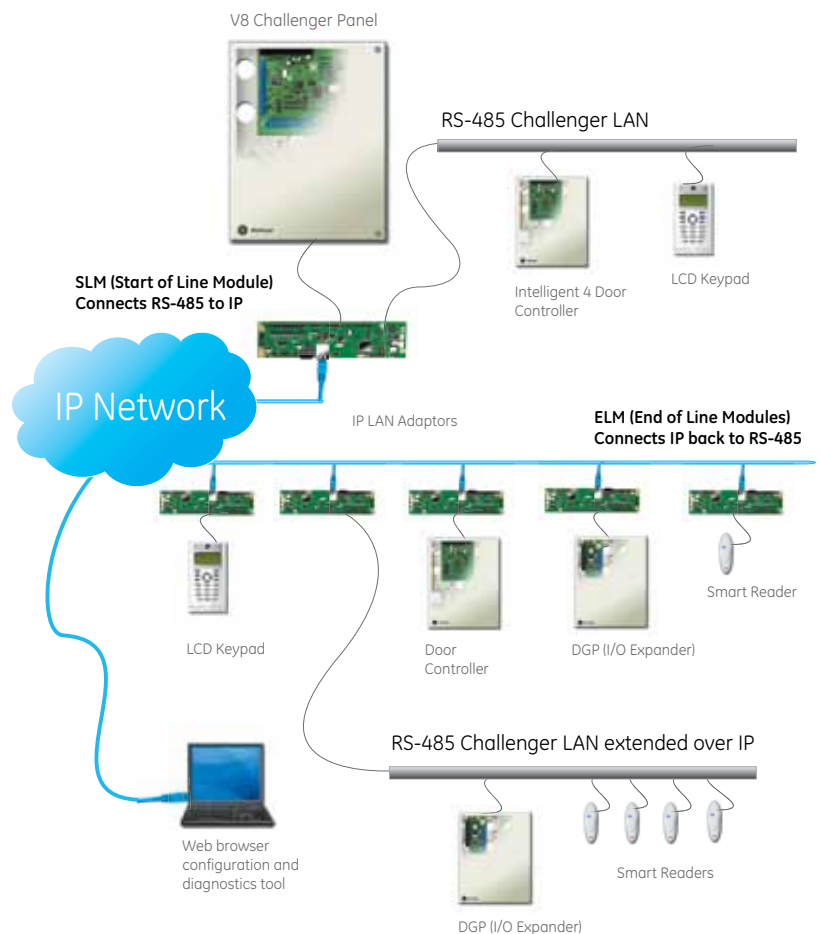


UTC Fire & Security

A United Technologies Company

Run Challenger™ LAN over existing IP networks

- Save time and money by connecting Challenger LAN devices over existing IT infrastructure
- Simultaneously IP enable all individual LAN modules, entire sections of LAN, or any combination of both
- 128-bit AES encrypted communications
- Device configuration over IP network via web browser — No need to connect directly to each device



NEW!!!

Introducing the TS0098
Challenger IP LAN Adaptor.

TS0098 modules enable
Challenger LAN data to be carried over an IP network

For more information contact your local Hillsec representative
or visit www.utcfs.com.au/IPLAN



www.hillsec.co.nz

AUCKLAND

Penrose

09 525 8007

Albany

09 525 8007

CHRISTCHURCH

Sydenham

03 374 6277

WELLINGTON

Petone, Lower Hutt

04 939 9355

NZIPI Update

We held our AGM on 8 October at the Crowne Plaza, Auckland with a great turnout. The comments resulting were that this was arguably the best meeting in years with everyone putting aside commercial opposition and without exception everyone engaging for the good of the industry.

New committee members this year are Rob Nicholl from Westland Investigations, Hokitika and Chris Lawton from C4 Risk Management Group in Auckland. We welcome them and value their expertise.

Resulting from the AGM, a working party was formed to look at the previously reported moves to restrict investigators from obtaining the owners of motor vehicles. NZIPI have since engaged a barrister to assist and we are hoping common sense will prevail.

We have also established a framework to monitor the response by Police to the files handed to them by our members and Police have welcomed this feedback, which only further proves their willingness to assist and their commitment to assist in fighting especially fraud offending.



Rob Nicholl from Westland Investigations



Chris Lawton from C4 Risk Management Group

Another working group has been tasked to liaise more closely with NZSA and ASIS as it was clear from the meeting that our industry (security and Investigation), just like the Policing community, is working more closely together with common goals and interests. In that respect there has been an increase in cases where just being an investigator is not enough, clients are also expecting a report on the “risk” associated with their premises, processes and systems, resulting from the investigation. This has in turn necessitated investigators to become more technologically advanced and current with the security measures available.

An example of technology, perhaps is that Section 228, Crimes Act, which replaced the old 229 (using a document) now includes that any recording, such as the claim lodgement call to an insurer, or the recorded interview with the investigator, is a “document” for the purposes of proving an offence of insurance fraud.

The feeling within our industry is positive and NZIPI members are certainly enjoying the benefits of being involved with a like minded group, dedicated to advancement and willing to support each others interests. www.nzipi.org.nz

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*

How good are your access controls

The client had noticed that a few times a week their computer keyboard and surrounding desk area was not quite how they had left it.

Nothing had been taken but things just didn't quite seem right. Also, the blinds were not quite as they had been left.

A covert CCTV camera was installed and it was noticed that late at night after all the workers had left, one of the computers was switched on for about 30 minutes, then switched off again.

A dark figure could just be seen in the light of the computer screen flickering. Surveillance was in place the next week and the workers were seen leaving. Then half an hour later, a dark hooded figure was seen approaching the building and entering using a key and obviously unsetting the alarm. No lights went on and the street side blinds were seen closing.

The Police were called and when they and the PI quietly entered, they caught a man watching porn on the client's computer with a hamburger in one hand, and you don't have to be a detective to work out what was in the other.

Whilst this is a horrendous story, it only demonstrates the need for all companies to have simple security measures such as proper access control, monitored alarm user codes and of course computer password protection.

Ten reasons to start now for training in 2011.

It has been another busy year in security training. Congratulations to the 392 trainees who finish the year having completed one or more qualifications. We've also seen 930 new trainees sign up for a National Certificate in Security qualification, bringing the total number of current trainees to more than 2000.

That's a great start to what we're all anticipating will be an even bigger year for security industry training in 2011. With that in mind, ETITO's security training team has come up with 10 reasons [there's more but we stuck with 10 for starters!] for security firms to consider before carving the Christmas turkey.

Don't leave subsidised training any longer – act now

Training is one of those things that are easy to leave for 'another day', but if you don't get sorted now you may not get back to it before the end of January. The Private Security Personnel and Private Investigators Act is due to come into effect on 1 April 2011 and the Rugby World Cup is here next August – the sooner security personnel are in the training the better placed you and they will be.

Real and tangible benefits

Customer satisfaction is just one of the benefits. Training is not only good for staff morale and retention, it fosters efficiency and productivity.

A building block for a true profession

It's not about what you have to do. It's about what you choose to do that makes you a professional. In 2011, in a new regulatory environment there is a great opportunity for the industry to advance the agenda of professionalism. It will reward those that meet expected standards and lift the poor performers.

New opportunities for a skilled workforce

There will continue to be demand for quality security services that offer value to a wide range of public and private sector customers. Add to that the Rugby World Cup and New Zealand's growing reputation for hosting major events. We should be ready to seize the opportunity.

Training gives a competitive advantage

A trained and qualified workforce provides a competitive advantage in a highly competitive marketplace where customer expectations for high quality cost-effective services continue to grow. How well trained your security personnel are will be under scrutiny in bidding for contracts.

Quality control is key in training too

Quality is central to ETITO's training and assessment. We are continuing to work with industry to improve a robust training and assessment system. This relies on our partnership with industry to ensure that the highest standards are met.

Literacy and numeracy – no barrier to success

Up to 42% of adults in New Zealand have literacy and numeracy issues. The security industry is not immune. We have run a pilot programme to assess the literacy and numeracy needs of security staff and we will continue to work with firms to identify issues and provide support. We've seen



Some of the most recent graduates, Mike Mould [left] and Jaco Keuler [right] of Opel Security, Auckland, with Opel co-owner Samantha Raymond and ETITO training manager Jay Hourani.

remarkable changes to benefit individuals and business through taking small steps.

Our training managers have the expertise to help

ETITO's training managers are skilled at working with trainees and employers to achieve completed qualifications within the required timeframe – while taking into account the needs of a busy and often casual workforce. We provide ongoing support for assessors, an essential part of a successful training system.

Working together

Achieving a skilled workforce and building a profession requires a partnership. ETITO, as the standards setting body for the security industry, works with trainees, firms, training providers and others, such as the New Zealand Security Association, to build a world-class training system for security professionals.

Contact ETITO

Pick up the phone now and speak with us about new training opportunities or how we can work with you to support or boost what you are already doing. Contact: Mike Hull [Northern, including Auckland] 09 583 1368, Kelly Walter [Central, including Wellington], 04 499 7678 and Ross Kennedy [South Island] 03 365 6391.

Best wishes from all at ETITO to our security industry current and future training partners for a safe and happy holiday season.

www.etito.co.nz

Auckland	Ph +64 09 525 2590
Wellington	Ph +64 04 499 7670
Christchurch	Ph +64 03 365 9819



ETITO

ASIS Update

As we approach the closing stages of 2010 and reflect upon another year of relatively tough and uncertain times globally and domestically, it would be easy to lose sight of a year of successes within New Zealand and specifically within our security industry. Certainly the New Zealand chapter of ASIS International has enjoyed continued support and growth in terms of quality membership and an ongoing engagement in industry participation at all levels, with representation on the Crime Prevention Partnership Forum, Security Industry Training Advisory Board, Australasian Council of Security Professionals, and effective working relationships with many other security associations locally. As a result, members through the designated chapter representatives have had significant opportunity to participate in development of policy and strategy in regards to a wide array of security related matters and fields, not least of which was the passing in September of the Private Security Personnel and Private Investigators Bill.

Clearly we are fortunate to include within our membership a large number of experts capable of participating in and leading initiatives to benefit our industry and society in general, who have credibility at the highest levels and are therefore able to influence change. More encouragingly is in the genuine depth of that expert knowledge within the membership, beyond the small group of very willing, committed,

passionate and capable people that are designated chapter representatives. This is critical for the long term success of the chapter and our industry, both in terms of refreshing of personalities, ideas and enthusiasm, and in regards to a moral responsibility to the people involved and the impact on their personal and professional time and energy.

At this time I would like to personally thank the following chapter representatives for their specific contributions during 2010 and respect their decisions to not seek reappointment for 2011:

- Craig Shepherd – CPPF Representative
- Charles O'Donnell – Chapter Secretary
- Ngaire Byrnes – Chapter Treasurer

At the time of writing, we are preparing for the ASIS NZ Chapter AGM to be held in Auckland on 2 December 2010 and suspect that by the time this issue goes to print the AGM will have been held and the new executive voted in. Certainly we are keen to maintain the great work carried out by the current and previous executive and look forward to a busy and promising 2011 calendar.

Both main branch centres of Auckland and Wellington are in good health with enthusiastic local volunteer leadership and participation at chapter breakfasts and other organised events. It is only right to express genuine thanks to those involved, particularly Michael Pepper, Bruce Couper, Ngaire Byrnes, Carlton Ruffell and Charles

O'Donnell. Beyond this, ASIS NZ chapter members have participated actively in a number of key industry events this year including the ASIS International Asia Pacific Conference held in Sydney in February. The combined ASIS NZ and NZSA Conference and Exhibition held in Auckland in September and most recently the annual ASIS International Seminar and Exhibits held in Dallas in October. Once again ASIS NZ members were well represented at all events, with a strong contingent attending in Dallas last month. For those of us returning, the event had lost little of its usual scale and grandeur and first time attendees were assured of a show of significant proportions and organisation. Irrespective, it was a fantastic opportunity for anyone with an interest in security to seek out information and/or technology as well as an unrivalled opportunity to network with security professionals from around the world in a professional but relaxed environment. There is no doubt that the scale of the security community within the United States and beyond allows for the staging of significant industry events beyond which we might otherwise be exposed. The point needs to be made that scale aside, the intellectual knowledge, ability, resourcefulness and professional standing of the industry in New Zealand is in itself significant, and we should never lose sight of that when making comparisons.

That said, and with Christmas fast approaching, may I take this opportunity to congratulate all ASIS NZ members and industry members generally on making some significant contributions and effecting positive change throughout the year while addressing the challenges and opportunities created by a changing world environment. I wish you and your families a very happy and safe Christmas and New Year, with genuine best wishes for 2011.



Alistair J Hogg, CPP, MSc

Alistair Hogg has been actively involved within the New Zealand Security Industry since 1987, in a variety of roles and across a broad range of activities with a strong background in electronic security, close protection and manned services.

Alistair is currently Chairman of both the New Zealand Security Association and the New Zealand Chapter of ASIS International.

An advocate of industry training in general, Alistair holds both the CPP designation from ASIS International and a Master's Degree in Security and Risk Management from the University of Leicester, U.K.

Alistair is a director of Dunedin based company, Aotea Security Ltd.

Email: alistairh@aotea-southern.co.nz

ASIS
INTERNATIONAL
Advancing Security Worldwide™

NZSA Update

Getting down to business has begun in earnest for the new board in a number of key areas for the NZSA's direction in 2010/2011. A review of the current strategic and operational plans is currently underway, with separately agreed targets on key elements in place and under action.

In particular these include:

- A focus on delivery of improved member benefits with the Board supporting the Association's Executive Officer, Greg Watts' interim proposal. This involves delivering tangible and improved member benefits, beyond the audit and accreditation process and other indirect commercial and reputational benefits. The Board awaits the final report and proposal for consideration at its next meeting
- Active engagement with the ETITO in relation to industry training and a focus on effective processes, consultation and participation by redefining lines of accountability and ensuring that the industry's best interests are maintained at all times. The development of a refreshed Memorandum of Understanding between the ETITO and NZSA is underway currently as is the formation of an effective consultation group with the ability to draw upon subject matter experts as required.
- The preparation of an effective marketing plan to promote the value of NZSA membership to all stakeholders and ensure that the genuine successes of the association are communicated effectively. The Board expects to review a report at its next meeting.

Separately, work continues with the general business of running the association with Greg, Paula and Lucy busy as always.

Support and engagement from the board as a whole has been pleasing, with all board members motivated and eager to lend their specific skills, making a difference and ensuring that the association, its members, and the wider stakeholder community, are well served. Certainly the workload for 2010/2011 is significant as are the expectations. It will be critical that the board delivers in respect of its role, as will the executive officer, staff and contractors generally.

It is perhaps not surprising that the passing of the Bill has stimulated an increased level of interest and activity in a number of areas although some of that activity may be late starting, it can only be a positive thing overall. The industry waits with interest more information from the Ministry of Justice in regards to time frames, processes, mandatory training requirements, etc. Clearly the NZSA seeks to be instrumental in ensuring that it has input where possible and in communicating effectively with its members. Certainly the NZSA office is endeavouring to establish lines of communication with the Ministry of Justice in order that the industry is informed and geared up to comply with requirements and timings. In fairness to all involved, the Ministry has itself been tasked with a significant challenge and a certain amount of patience at this stage is not unreasonable.

As the end of another year approaches with the traditional seasonal stresses and challenges, it is important to keep a realistic perspective overall and to ensure that as an industry we are all informed and prepared for changes, challenges and opportunities in 2011.



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 \$52.00 including 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
PO Box 4, Ahipara,
New Zealand 0449

or email your contact and postal details to:

craig@newzealandsecurity.co.nz

Mr Mrs Ms _____

Surname _____

Title _____

Company _____

Postal Address _____

Telephone _____

Email _____

Date _____

Signed _____

nz Security
A trusted source of information for industry professionals

TERRORISM

By Kim Hoskin



With 7th Gurkha Rifles on internal security duties in Hong Kong and on operations in Sarawak during Confrontation, Kim transferred to the Sarawak Constabulary as an assistant superintendent to form and lead a Border Scout group, meeting his first insurgents and terrorists.

In the New Zealand Army, Kim served as an intelligence officer in Malaysia and Vietnam, established the New Zealand Army Intelligence Centre, ending his military life as Honorary Commandant of the New Zealand Intelligence Corps.

Kim wrote the NZSA (then NZSIA) professional security officer training programme, then the first NZQA security qualifications. He is member of the Security Industry Training Advisory Board (SITAB) and the New Zealand Institute of Intelligence Professionals (NZIIP)..

Kim is responsible for an accredited National Diploma in Security programme which includes a terrorism risk module.

Hope is not a viable strategy

origin uncertain

New Zealand has no experience of terrorism or terrorist activities at a level common in other countries. The Rainbow Warrior and Trades Hall bombings are exceptions that give weight to the general rule that New Zealand remains isolated from this particular form of violence.

Yet the circumstances in which terrorist organisations may develop, migrate, or operate here, undoubtedly exist. In view of this, the risk presented by terrorism in New Zealand may best be viewed as a matter of time rather than hope.

Security practitioners need to have a sufficiency of knowledge about terrorism and about the practical and sensible steps that may be taken in the current New Zealand environment to reduce the risk of terrorist attack and to respond adequately to a terrorist incident should it occur. To borrow Baden-Powell's well-worn adage, be prepared, rather than be surprised.

This article seeks to provide security practitioners with a brief overview of terrorism and the risks it presents: to explain the nature of modern terrorism in terms of its key elements and its effects, and to identify trends relevant to New Zealand. It does not discuss the risk management options that might be considered by security practitioners. That is the subject of a separate article.

Content is based on publicly available sources and references tempered by some personal exposure and training.



Loktronic ● Innovationz

Security with innovative technology

fire door holding electromagnets

FDH40S

unbreakable universal mounting

Low power consumption - low operating temperature •
One product suits floor and wall mounting • Universal armature - offsets to 55° to suit doors opening past 90° • Additional flexible mounting in both planes to speed alignment • Wall mount extensions available • Wall mounted, overall 429mm, is also available finished switch end only, and can be cut to any length • 12 VDC models and 24 VDC models • Push off button - no residual magnetism • Oversize armature for easy alignment • Emergency release button • Electroless nickel plated armature and electromagnet • Stainless fastenings • Blackened stainless screws • Full local support and back up • **PLUS NEW 10 YEAR GUARANTEE***

Designed, tested and produced in New Zealand to AS4178



Standard, floor mounted, wall to door distance 114mm



Wall mounted, 126mm extn. tube (overall 202mm)



Wall mounted, 156mm extn. tube (overall 232mm)



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 or 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 now utilise one device for surface mounting, which is ideal for solid walls of concrete, stone and the like, or for flush mounting into plaster board lined walls, because both options are packaged in the same box. **PLUS NEW 10 YEAR GUARANTEE***

Designed, tested and produced in New Zealand to AS4178



Both options are packaged in the same box.

Loktronic ● Innovationz
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

Continuing to set new standards for strength, flexibility, quality and value Loktronic Innovationz has developed the strongest, most reliable fire door holding electromagnet in New Zealand.

*Standard terms & conditions of sale apply.

16898

Introduction

Terrorism is not a new phenomenon. In one form or another it has been used by dissident organisations throughout history in attempts to achieve political and other objectives that were not practicable by other means.

Events over the past decade have bought the risk of terrorist activity closer to home. The Bali bombings in 2002 and further attacks in 2005 in Djakarta and elsewhere which deliberately targeted venues used by tourists, and more recently the planned attack on the Holsworthy Army base outside Sydney in 2009, are perhaps the most significant.

There are other examples: the possible targeting of Lucas Heights nuclear research facility near Sydney in 2000 by a group reportedly operating from New Zealand, and interest in the Sydney Olympics by an international terrorist organisation.

Security practitioners employed in the public and private sectors need to consider the risk presented by terrorist attack, ways to reduce the risk, and their responsibilities should an attack occur.

This is not fanciful scaremongering but a rational response to an evident risk. It reflects a professional duty of care.

From the perspective of security practitioners, the events of 9/11 at the World Trade Centre and the role of one of the security executives working there, Rick Rescorla, provide the best argument for this.

Rick Rescorla, in our terms the security manager of one of the principal occupants of the Centre, recognised the risk of terrorist attack and did his best to reduce it and its likely consequences. He warned of the risk presented by truck bombs but failed to get trucks banned from entering the basement car park of the Twin Towers.

The explosion of a truck bomb in the car park in 1993 encouraged him to recommend that the company move out of the building, a recommendation that was rejected. He predicted an attack by aircraft and introduced extensive emergency evacuation procedures and had them practised. As a result, there were very few casualties amongst the staff for which he was responsible when aircraft hit the Twin Towers.

Terrorism in Action

Terrorism is not generally restricted to a single act. It is more likely to be a continuing campaign of escalating violence and fear intended to create circumstances in which governments that fail to contain or defeat it are forced to treat with the organisation that employs it. Some – indeed most – governments may negotiate with terrorist organisations in order to reach a compromise that limits the risk of continuing damage and destruction or buys time in which to secure a viable solution, often in exchange for concessions to terrorist demands.

A terrorist act may appear to be isolated but is instead part of a regional or global strategy conducted to support broad political, ideological, or religious aims – in Islamic terms a jihad or holy war against non-believers, in radical Irish republican terms to defeat British and protestant domination. In domestic terms, terrorist acts in kind may also be committed by activists in the furtherance of such causes as animal rights and, perversely, humanitarian objectives.



While terrorism may be associated with an organisation or group that is apparently lawful and open in its aims, like the Irish Republican Army (IRA) and its association with Sinn Fein, it is more often associated with clandestine organisations that are illegal or proscribed.

Terrorism is characterised by attacks that are designed to achieve maximum shock and horror – ‘the more awful, the better’ – in order to create terror. Terror however is the means, not the end. Terrorist attacks are generally but not always directed against vulnerable rather than protected targets. Modern terrorism aims to obtain maximum effect for minimum but generally carefully crafted effort, and to destroy the security that people regard as necessary for a normal existence.

Two examples, ‘9/11’ – the attack on the World Trade Centre in New York, and ‘7/7’ – the London Underground bombings, both illustrate the immediate tactical and broader strategic objectives of terrorism and, in their execution, the underpinning terrorist maxim of giving tactical events strategic significance.

Terrorist attacks may involve improvised explosive devices or explosives delivered by what would previously be considered unconventional means – car and truck bombs, or human beings with ‘suicide waistcoats’ for example – but may also involve the threat or use of chemical or biological agents such as anthrax.

The sarin poison gas attacks in Tokyo’s underground rail system in 1995 are an example of this.

Terrorism practiced by Islamic extremists and their cohorts introduced the relatively new dimension of martyrdom as the ultimate reward for actions that are to others, simply appalling acts of mass murder.



Terrorism is not a legal and acceptable means of war or armed conflict. It is prohibited by a broad range of international law. In New Zealand, acts of terrorism as defined in the Terrorism Suppression Act 2002 are illegal.

Terrorism is a tool that has been used or instigated by governments, state agencies and independence movements. However this should not cloud the definition of terrorism and does not change its purpose or methods.

While terrorism and terrorists may be seen from different viewpoints characterised by the catchphrase: ‘one man’s terrorist is another’s freedom fighter’ this gross over-simplification ignores the literally dreadful means terrorism uses to achieve its aims: the use of extreme violence and fear, most often against the most vulnerable of targets, to create maximum psychological and social effect.

Terrorism should not be confused with insurgency or guerrilla warfare although insurgents may use acts of terrorism, one somewhat amateur effort much to the surprise of the writer.

The Taliban in Afghanistan are accurately described as insurgents while Al Qaeda is clearly a terrorist organisation. There is another significant difference between the two organisations: while Al Qaeda is structured to operate across international boundaries and presents a global threat, the Afghani Taliban are restricted in their objectives and operations to Afghanistan and neighbouring states, including Pakistan, reflecting Pushtun tribal affiliations.

However, as the international boundary between Afghanistan and Pakistan (the now ill-famed Durand Line) divides



traditional Pushtun tribal territories, it is hardly surprising that the border provides sanctuary to the Taliban rather than a boundary.

Pakistan has its own indigenous Taliban, the Tehrik-e-Taleban, (TPP) which the United States Justice Department has recently designated as a terrorist organisation as it is thought to have organised a suicide bomb attack on an American intelligence facility in Afghanistan.

While the immediate impact of an effective terrorist attack creates casualties, damage, shock, and perhaps chaos; by attacking a critical or iconic asset or a specific section of a community it also demonstrates its broader purpose of discrediting governments and public security, and gaining credibility. Terrorism attacks the fabric of society by magnifying fear, distrust and disunity: establishing by implication that nowhere and no one is safe.

Terrorist acts are not always designed to inflict casualties although generally they are. The bomb attack in the financial centre of the City of London in 1993 towards the end of the IRA campaign was made to demonstrate continuing IRA capability and to force negotiations with the British government to a conclusion that might not otherwise have been so readily obtained. Despite the size of the bomb, and the location, only one person was killed.

The attack was designed to expedite negotiations by making a point. Executed on a Sunday to minimise casualties and thus restrict public outrage while at the same time putting pressure on the British government. An IRA ceasefire agreed after the attack lasted until 1996 when another bomb was exploded in Canary Wharf, again a London focal point.



Defining terrorism in plain terms ...

Terrorism may be defined by describing its three principle characteristics or elements: the *what*, *why*, and *how* of terrorism:

the *what* of terrorism – *what* is terrorism?

the planning, instigation, threat, use, or attempted use of extreme violence and fear to create terror

the *why* of terrorism – *why* terrorism?

to achieve ideological, political, religious and other social objectives other than those associated with common criminal intent and personal gain, or protest and industrial actions that are accepted parts of the democratic process

the *how* of terrorism – *how* does terrorism work?

through the threat or use of weapons, methods, and the selection of targets that result in terror, including for example:

- bombs and explosives
- chemical and biological substances
- kidnap and extortion
- execution, assassination, torture, and mutilation
- hijacking and hostage-taking

The where and when of terrorism are elements that the terrorists generally do their best to conceal unless, like the Irish Republican Army (IRA), they use a warning system as a component of their operational strategy.

The 1993 attack also illustrated the huge direct and indirect cost of terrorism in financial terms: a property damage bill estimated at the time to be one billion pounds and the disruption of the insurance industry.

Contrast this with recent terrorist attacks in Pakistan in which a target is attacked by a car or truck bomb, another is detonated when the emergency services arrive, followed by yet another in the medical facility to which the casualties are taken.

The response of governments to terrorism and terrorist activities may itself be counter-productive as it 'uses sledgehammers to crack nuts', proving perhaps one of the points that terrorist organisations usually make – that the government it opposes is repressive. In a perverse way, the events of 'Bloody Sunday' in Northern Ireland in 1969 illustrate this phenomenon, 'creating' terrorists by measures intended to contain them.

Ultimately the general aim of terrorism is to force a government into making decisions and concessions that it would not otherwise make. In one sense, terrorism is blackmail on an horrific scale.

Changing Faces

Terrorism in its application 'morphs' or it would not survive: it changes to reflect the environment in which it operates, the measures used to contain or defeat it, and the objectives it seeks to achieve.

It also changes the weapons it employs. In technical terms, Guy Fawkes had to make do with gunpowder in barrels – some of it of questionable service – and bundles of firewood in the attempt to destroy the English Parliament in 1605. In more recent times, efficient plastic explosives like semtex are widely used, while 'agfo' a mixture of commonly available agricultural fertilizer and diesel oil is used for truck bombs.



Cell phones now provide a convenient remote control triggering device while 'shoe-bombs' – explosives concealed in the soles or heels of shoes – have been used in attacks on passenger aircraft.

The ground and bomb attacks on selected targets in Mumbai, India, in 2008 by the Pakistan-based Lashkar-e-Taiba illustrate another dimension of terrorism; their ability to execute quasi 'special force' operations on foreign soil.

A United States citizen, David Headley, was subsequently convicted of supporting the attack by collecting information used in planning it.

While bombs may remain the terrorist's weapon of choice, perhaps for the foreseeable future, recent attacks have demonstrated a wide range of methods terrorists may use.

What next? is a valid question.

Cyber-terrorism, in which the electronic information systems on which the modern world is increasingly dependent are targeted or used to achieve the attacker's aims, is a development that reflects the ability of terrorism to adapt to and use different methods.

Globalisation has many faces: trade, people, drugs, money, ideas, information, weapons, and enables terrorism to travel more easily.

Terrorist organisations differ widely in terms of their structure, size, composition, objectives, capabilities, membership, and methods of operation, but even if small and relatively new, they present significant risk.

While some terrorist organisations have a hierarchical structure through which operational direction and targeting

instructions flow, others may have a more fragmented organisation in which each small group has a degree of operational autonomy. In all terrorist organisations however, closed operational cell structures are used while a few key personalities generally have critical roles.

Closer to Home

The Bali bombings of 2002 and the subsequent series of bomb attacks in Bali and Djakarta in 2005 directed at Australian and other foreign nationals point to more of the same but, so far at least, without export potential.

However, last year's (2009) planned attack on the army barracks at Holsworthy near Sydney by Australian nationals living in Melbourne brings the issue of terrorism much closer to home and demonstrates that it is not confined to exotic locations.

New Zealand remains isolated in geographic terms. Its once relatively homogenous population would not have provided suitable ground for the development or support of terrorist organisations.

However that is no longer the case: a very small segment of the community may provide the nucleus of an operational terrorist cell or local support for an international terrorist organisation that chose to operate here. There are appropriate targets with international significance: shipping, aircraft, and sports events perhaps being some of them. A cruise ship in port while the Rugby World Cup is in progress would be tempting.

Without good intelligence it is of course impossible to predict if, when, where, how, and by whom the next terrorist attack may be made in New Zealand.

Given this background, and with no better insight than anyone else, it is suggested that a future terrorist incident might be the responsibility of either:

- an off-shore terrorist group exploiting a vulnerability and attacking a suitable target, perhaps with a local support group seeking the opportunity to create world-wide headlines, or
- a small, presently less visible but developing group already in New Zealand, perhaps less competent than its international counterparts, but with outside connections, allegiance, or agenda.

We may hope not, but as someone remarked, 'Hope is not a viable strategy'.

To contact Kim Hoskin email:
kim@crms.co.nz



The fine line between feeling safe and unsafe

There is a fine line between selling security to make people safe and making them feel unsafe from the way the system is sold says Mike Tolhurst, the Registrar of Private Investigators and Security Guards.

Speaking at the New Zealand Security conference, Tolhurst says that after only a few months in the job he has fielded two complaints about security companies selling home security systems.

As a result of his experiences Tolhurst would like to see a code of conduct adopted.

“Not only for the actual services that are provided to clients but also for the way in which the industry markets and promotes those services,” he says.

Enforceable codes of conduct will be possible under the new legislation due to replace the current legislation on 1 April 2011. *(See story page 10)*

Tolhurst says regulatory codes of conduct are his principle interest in the new legislation.

“I find it astounding that your industry has not had such a code,” he says.

Tolhurst gives the example of selling CCTV camera systems door to door at 7 or 8 o'clock in the evening.

“It may be a totally inappropriate way to behave where the people to whom the systems are being sold feel quite unsafe in having a stranger visit them at that time of the night,” he says.



Mike Tolhurst, the Registrar of Private Investigators and Security Guards

“It may make people unsafe to be visited by a stranger in the middle of the day without an appointment when the stranger identifies themselves as a security consultant. To be discussing something as personal as security with somebody who has just arrived on the doorstep could be daunting to some people.”

He says he has asked that Justice Department consult him about the new code.

“A clause in the code could require security guards and private investigators to first make an appointment with a person with whom they wish to meet at a time that is convenient to both. This may overcome the issues which currently exist where there is no guideline whatsoever to what sort of behaviour may make people feel unsafe.”

Despite Tolhurst's views, the government says at this stage it only intends to introduce a code of conduct for private investigators.

Alcohol

Tolhurst says he has also dealt with cases that involve alcohol and drug taking.

“Most would agree that any sort of consumption of these substances within a reasonable period of a guard going on duty should be prohibited. The code could stipulate a period so that everybody is clear as to what is acceptable and unacceptable in this regard.”

He says alcohol plays a large part in the failings of industry members, as it does in every other industry.

“In most cases, but for a more responsible approach to alcohol use, the issues which are either complained of, or objected to, are able to be addressed. I have on more than one occasion imposed a requirement that the applicant undergo some sort of alcohol treatment course as part of their licensing requirement. This condition seems to have been accepted positively by the applicants as well as the police,” he says.

Tolhurst says he would like to hear about other activities which should be dealt with under the code.

“I think that as an industry you need to deal with this now so that you get a code

which is both encompassing of all activities which might cause problems and which is able to manageable,” he explains.

Reality

Although it is his job to deal with complaints, Tolhurst says in reality he mainly deals with objections by the police to licence applications. Most of the objections are as a result of the applicant having a conviction over the past five years prior to the application being made.

Tolhurst was a policeman himself for eight years before setting up his own law firm.

He says the legal issues around the granting of licences are not complex but the personal and factual situations generally are. Each case requires a careful analysis of the background and personal circumstances of each applicant as well as the facts regarding any incident in which they may have been involved.

“I have not had a case yet which has panned out exactly the way that I thought it would when I was preparing for it,” he says.

“Some of the cases have had totally different results from what I envisaged at first. This has brought home to me the very real need to hear from and see the parties in person as opposed to dealing with matters in any other way. I think to deal with matters which impact upon people's livelihoods without giving them the benefit of a hearing would be a breach of the basic principles of natural justice.

“My philosophy in regards to how I deal with complaints and opposition to licences is to try to get a solution which if at all possible keeps the applicant in the industry,” he says. “This will normally come with conditions regarding things like training and alcohol counselling.”

Tolhurst expects little change to the registrar's job under the new legislation – apart from being renamed as the Licensing Authority.

He says overall responsibility will still be dealing with objections and complaints but they might increase when the licensing regime covers crowd controllers because of the numbers that will apply.

Collaboration gathers pace

The top level Crime Prevention Partnership Forum between police and private industry is gathering pace, but a policing researcher warns that changing front-line police attitudes to private security will be a challenge.

"The question is whether they can replicate the higher level strategic stuff on the ground," says Dr Trevor Bradley, a lecturer at the Victoria University Institute of Criminology who has researched the relationship between the private security industry and the police.

Bradley spoke to NZ Security after giving a presentation at the New Zealand Security Conference.

"The police see some advantages for themselves in terms of the resources potentially available but they are not putting a great deal back into that relationship, but that is changing and the change is coming down from the top," he says.

According to Bradley there are thinkers at the higher echelons of the police who appreciate the broader context and the value of exchange with other groups. "But most front line general duties cops are relatively dismissive of private security and private security guards in particular, and I think that is what needs to change."

Bradley told the conference that working relationships between police and private security do exist at the front line - particularly in rural and semi rural areas. However they are based on personal contacts and networks and have to be re-established as police personnel move.

"You've got to get away from that and draw on a system where there are mail lists and messenger services and where the information is swapped on a much more routine and organised basis," Bradley says.

"I don't think the industry is looking to take over activities from the police. They are just looking for a more effective way of providing assistance, and of course if they can do that then they are providing their clients with better service too, because a better informed local police is better for everybody in the community."

Combining resources

It's a theme that resonates with Police Inspector Rob Duindam who is - among other duties - the secretariat for the Crime Prevention Partnership Forum (CPPF). The group was formed to improve collaboration between industry groups and police.

"Its purpose is to combining resources and goodwill to improve community safety and public reassurance," he says.

"With the advent of the policing act it is quite obvious policing is going to involve an awful lot of different people in the future."

He is referring to the relatively new Policing Act 2008, a statute that in section 10 specifically acknowledges the role of the private security industry as important and valuable in the performance of the functions of the police.

"The Policing Act really broadened out the modern approach to policing," he says. Among the private sector groups represented on the CPPF are the NZ Security Association (NZSA), the NZ Institute of Professional Investigators (NZIPI), American Society for Industrial Security International (ASIS). Other bodies like the New Zealand Retailers Association are also members.

Since the end of last year we've been meeting quarterly. We share information and we try and work up actions to follow," says Duindam.

"When you start from nothing you have got to build a process and a structure and the functionality around this so we invested quite bit of time in writing a charter and getting some information and intelligence sharing protocols together."

Initiatives

The CPPF has undertaken a number of initiatives already including analysis of crimes such as bank robbery, sharing of information on fraud offenders, consultation with members on insurance investigation standards; and discussions on crimes such as retail theft, stolen vehicles, and assaults on taxi drivers.

"We've done some briefings around Rugby World Cup - as you can imagine everybody across the country was pulling

things together. It worked out really well because it established some common issues and established a network of people," add Duindam.

Like Bradley, Duindam sees the U.K.'s Project Griffin as good illustration of how technology can be used to enable better information sharing between police and private security.

Described at the New Zealand Security Conference by U.K. Counter Terrorism Security Advisor, Ian Mansfield, the project provides an official and direct channel through which the police can share and update information relating to security and crime prevention. Using regular conference calls, SMS, pager and emails police keep individuals and groups aware of current information and intelligence, as well as issues or incidents affecting their particular area.

Duindam says the presentation about Project Griffin at the Security conference has stimulated discussion on that approach here but it is early days and how it actually would function in New Zealand and the work that is necessary to pull it together, are unknown.

"There is definitely an opportunity," he says. "The police have got a finite amount of resources and obviously the security industry has an increasing broad base and they are becoming more and more professional over time with training and standards improving"

"If we can harness technology and share information, then it is going to produce a far stronger base to reduce crime."



Dr Trevor Bradley, a lecturer at the Victoria University Institute of Criminology

Next Step to Trusted Identity

Access control systems (ACS) are migrating well beyond cards and readers into a whole new world of configurable credentials, contactless technologies and a world in which mobile phone and other devices can carry “digital keys” that they receive over the air or via the Internet. As people become more mobile, there are new demands on secure identification and trust, paving the way for virtual identification rather than access with a key card. To meet the challenge of the explosion of fully-distributed, always-connected, smart devices, it is necessary to develop an infrastructure initiative to support the evolving ACS domain and which drives all new product development efforts. Near Field Communications (NFC) is one promising technology that makes this possible, but the only way to make it secure is if the industry can establish an identity methodology based on a comprehensive chain of custody, in which all end points in a system or network can be validated so that identity transactions between them can be trusted at any time, on demand.

Trusted Identity Platform (TIP), a recent development of HID Global, is a trusted and secure network that provides the framework for identity transactions which will enable the delivery of secure products and services. It is comprehensive framework for creating, delivering and managing secure identities. Simply put, the architecture is a central secure vault that serves known endpoints, such as credentials, readers and printers, on a secure network connection, within a published cryptographic key management security policy. HID Global refers to this as a bounded-type system, where all the devices attached to it are known and therefore trusted to exchange

information securely. The TIP architecture is fully scalable, its transmission protocol and encryption models are standards-based, and can support multiple applications. TIP systems also can be virtualized, cloud-based and therefore can provide services across the internet without compromising security.

How does TIP work?

TIP provides a protected identity transaction network that enables validation of all its endpoints, or nodes, in the network so that transactions between the nodes are trusted.

The TIP model consists of 3 central elements:

1. The Secure Vault, which provides a secure storage capability for encryption keys, available to known and trusted endpoints;
2. A Secure Messaging methodology using industry standard symmetric key methods for transmitting messages to the endpoints; and finally
3. A Key Management Policy and Practices (KMPP) governance which sets the rules by which the Secure Vault is accessed, and keys distributed to endpoints.

So let's take a closer look at how we establish these endpoints and trusted transactions:

Endpoints are enabled by implementing a TIP node protocol so that they can be recognized and registered by the Secure Vault as a trusted member of the network; this means that they are allowed to communicate with the Secure Vault.

Endpoints, such as credentials, readers and printers, communicate to the Secure Vault via a software workflow process, whose access and processing rules are strictly governed by HID Global's Key Management Policy and Practices. Only trusted devices are permitted to participate in this network - unlike the internet where any computer can access any website - deriving an implicit strong authentication.

Using industry standard cryptography, TIP messages between endpoints are encrypted to form secure transactions that follow published security policy (KMPP). These TIP message packets are secured by two nested symmetric keys which hold Secure Identity Object messages, or SIOs. Several SIO's can be nested in a TIP

message to deliver multiple instructions to various devices such as access cards, smart phones and computers, each with different access control characteristics, if required. For example, the simplest SIO is the emulation of the credential program data on an iCLASS card.

Once a “handshake” is accomplished between the Secure Vault and an endpoint device, then the device is deemed to be “Trusted” in the network. Trusted devices no longer need to communicate with the Vault and operate independently. In this way the transaction between endpoints, such as a credential and a reader is trusted and the resulting transaction, such as opening a door, or logging onto a computer, can be deemed trusted.

Using Near Field Communications (NFC), phones with this technology can be supported as TIP endpoints and therefore can be programmed with different SIO's to allow card emulation, or more complex applications, to not only grant access to doors, but to implement complex access control rules interpreted by the NFC phone itself.

HID Global will begin deploying TIP later this year, and has already taken a first, big step toward realizing its vision of a trusted, virtual and on-demand identification network with the announcement of its first partnership, with NFC chip leader INSIDE Contactless. INSIDE Contactless is one of a handful of companies driving the NFC trials currently underway around the globe. This first partnership will allow NFC-enabled phones to hold the same market-leading iCLASS® access control and credentials information as our physical smart card. This credentials information will be delivered via HID Global's TIP system, and it will be possible to merge these credentials with other web services and real-time communication. HID Global plans to announce other similar partnerships that will combine contactless solutions, NFC and other widely deployed technologies from HID Global and other suppliers to create a wide variety of platforms, from mobile phones to laptops, for applications ranging from user authentication to cashless vending and PC log-on security. These platforms and applications will significantly extend the value proposition for contactless smart card credentials.





Dialock DFT Furniture Locking System

The key to Customer Comfort and Store Security



Dialock DFT is used by leading retailers and department stores as well as the world's leading luxury brands to protect valuable store display stock, as it is an electronic furniture locking system that meets the highest requirements of store security, functionality and aesthetic appeal.

With its cleverly concealed locking components, Dialock DFT lets you lock and unlock cupboards, drawers and even glass sliding doors, quickly and easily with just a swipe of an electronic key in front of either a visible or concealed reader.

If a door or drawer is left open too long an alarm can be set to remind staff. Lost keys can be quickly and easily replaced at low cost and without compromising security.

To request your copy of the Dialock DFT Furniture Locking System brochure email dialock@hafele.co.nz or phone (09) 274 2533. The brochure can also be viewed at www.hafele.com



Auckland Head Office • 16 Accent Drive, East Tamaki, Auckland • P: (09) 274 2040, F: (09) 274 2041
 Beaumont Street Design Centre • 20 Beaumont Street, St Mary's Bay, Auckland • P: (09) 274 2530, F: (09) 274 2531
 Wellington Design Centre • The Wool Store Level 1, 262 Thorndon Quay, Wellington • P: (04) 472 0294, F: (04) 472 0295
 Christchurch Design Centre • 5 Wigram Close, Sockburn, Christchurch • P: (03) 343 8200, F: (03) 343 8201

HÄFELE
 FINDING BETTER WAYS

The PowerFence™ Solution for Perimeter Security at Hamilton Zoo

Ensuring animals at New Zealand's Hamilton Zoo are housed in a safe and secure environment is of the utmost importance and a Gallagher Security PowerFence™ provides the required perimeter solution.

The project brief from Hamilton Zoo's Director Stephen Standley, was to design and construct an alarm monitored PowerFence perimeter system which would deter possible intruders, with a secondary function to provide back-up against animal egress. The final solution combines small aperture chainlink mesh in the lower area to prevent the flow of rabbits and livestock between the Zoo and neighbouring farms which were also an issue.

Manufactured by Gallagher Security Management Systems and installed by an authorized PowerFence Dealer, Barakat Contractors, the system uses a safe, non-lethal electric shock to deter and detect attempts to breach the perimeter. System components are manufactured and installed to international standards (IEC 60335-2-76 standard) and the Gallagher Code of Practice which exceeds installation codes of practice currently existing around the world.

The appearance of the system was a priority to the Zoo with special consideration given to the public car park and site frontage areas. Accordingly a green colorsteel panel fence was constructed to meet these requirements. The topper PowerFence utilized green anticlimb insulators and powder coated posts to blend with the bush environment and match the fenceline.

The system has been constructed using Alloy PowerFence wires which have three times the conductivity of steel and will never rust. Security anti-climb insulators that break-away on an intruder climb, chance response. A Rooftop PowerFence™



protects against climbing over the entrance buildings and the remaining area is secured with galvanised Chainmesh-PowerFence™ combination.

The Zoo perimeter runs for a distance of 3km around the site. This is divided into 17 separately alarmed Zones for immediate response to the place of attack. Upon attack, an alarm is sent to the monitoring centre to despatch a security guard, ensuring the site is secure day and night. Any of these Zones can be separately turned 'On' and 'Off' from either roaming keypads around the site or from a licenced computer on the zoos local PC network. During standard work hours the perimeter security system is monitored by key administration staff, after hours it switches over to the zoos usual security company.

The same networked system can be upgraded at any time in the future to bring information onto the zoo network of electrified animal enclosure fences. It will show them on the PC screen; their operating state, voltages on the fenceline and allow control of these.



For information on Gallagher Security products including Cardax and PowerFence™ contact:
Michael Collins on
Mobile: +64 21 221 7482

AWARD WINNING FULLY INTEGRATED ACCESS CONTROL AND PERIMETER SECURITY SOLUTIONS FROM **GALLAGHER**



Need to know more?

Contact Gallagher Security Management Systems

Phone 07 838 9800

Email salesnz@cardax.com

www.cardax.com



SECURITY
MANAGEMENT
SYSTEMS

Security Guards in New Zealand

By Lucy Mullinger

Employing a security officer:

When employing a security officer or signing a deal with a security company, it is important that the employer gets all the facts right to ensure they are doing business with a reputable security company that they can trust to do the right job.

Employing security guards who hold a license is vitally important. The Ministry of Justice is currently responsible for administering the licensing of private investigators and security guards. This function is carried out at Auckland District Court for the whole of New Zealand.

Security officers need to apply to the Registrar of Private Investigators and Security guards at the Ministry of Justice. According to the Ministry of Justice website "If you hold a license and have people working for you, they will need a certificate of approval."

Licenses and certificates do not last forever and need to be renewed by 31

March each year and no matter what time of year they are applied for; they will still expire on that date.

Employers can be assured that all license holders are given a police check. The registrar will forward a copy of the application for security clearance before the license is granted and wait for the police to consider the application before they go any further.

If the police don't object to the issuing of the license or certificate the applicant will be granted the application immediately which gives all employers the peace of mind that they are employing staff they can trust.

On top of this, all applications for licenses are advertised in the newspaper, this allows members of the public to lodge any concerns about the applicant before the license goes through.

An application can take a few days or weeks for approval depending on when it is applied for (January to March is a busy time of the year to apply, so it makes sense to send the application through, outside of this peak time). Therefore it is important an employee checks that the security guard and the company's paper work is up to date and valid when discussing employment with the security company.

The money invested in a company makes it a precious commodity to all business owners. This is why it is important to get the right security guard with the experience and integrity essential for keeping a business safe from criminals including intruders, employee theft and product damage



According to ADT Armourguard General Manager, Ian Anderson, "Anyone who is looking to employ security personnel should ensure that the security firm's staff have certificates of approval issued by the Ministry of Justice to work as a licensed Security Guard. Other than that, companies should look at the security firm's history and experience, ability to meet all contingencies in terms of power and communications failures, reputation in the market place and assess cost against investment - cheap doesn't always mean effective. At ADT Armourguard, we also carry out reference checks and, where appropriate, credit checks of staff."

There are currently no compulsory training or qualifications needed prior to entry into the security industry. "However, NZQA Security Levels two and three would be viewed favourably by employers (including ADT Armourguard)," says Anderson.

In New Zealand, a security officer must obtain a Certificate of Approval issued by the Ministry of Justice, before they can act in the capacity of a Security Officer.

Becoming a security officer:

Technology plays such a big role in the fight against crime, including alarm systems, Closed Circuit Television (CCTV)

cameras and computer run monitoring systems, so it might be surprising to hear that security roles are generally easy to find around New Zealand.

In fact the demand for security personnel has significantly increased by a whopping 33% from 1996 where there were 4,521 officers employed nationwide to 2006 with 6,015. This is despite the fact that crime rates have been decreasing during the same time period.

A security officer's role is variable and depending on the employees experience and interest, it is not hard to find a role that suits them, jobs can range from security work at a banking facility or financial institution through to security for weddings and birthday parties.

The criteria for a security officer can vary depending on the employer, however the NZSOF don't have any requirements and effectively anyone can apply to be a security guard.

Contrary to popular belief, security guards are being employed in all shapes, sizes, cultures and genders. Even though a security guard has historically been pictured as a stocky male with tattoos up his arms and piercings all over his face, these days, all types of cultures and people of all statures are being employed, including many female officers.

Anderson says that most duties require a good level of health and wellbeing to minimise personal harm.

Some businesses may choose to employ female officers to deal with female offenders and issues that are sensitive where only a female can do the job, however it is not a prerequisite to have a female officer available at all times, "a male officer confronted with a female offender cannot materialise a female officer out of thin air," says Bryce Winstone from the New Zealand Security Officers Association.

In Bryce's opinion female security guards are being employed more in some sectors of the industry than others, alarm monitoring for example, have always employed high numbers of women, whereas patrol services are more likely to employ male security guards, solely because male security guards are more likely to apply for those types of roles.

According to Statistics New Zealand, the highest rate of employment for security officers is in Auckland with 38% of staff employed whereas the Bay of Plenty employs the lowest at 5%, however depending on what part of the industry a security guard is interested in working, they should be able to find work in most cities, however it is important to



RED EYE

Reseller Partners WANTED NOW




Standalone and Portable Outdoor Surveillance

Unrivalled Battery Life *delivers* Continuous Operation
5 month battery is trickle charged by an integrated solar panel

Flexible add-ons: **Night Vision, REMOTE Triggers,
GSM Modem** for immediate viewing of events

Latest PSIS technology for High Quality
Security-grade Images

RedEye from Mi5
at last; a security
solution for covert remote
surveillance *anywhere*

www.mi5security.com
call now: 0800 111 309



Mi5

SECURITY

remember that like most jobs, the bigger the city, the more likely it is for people to find work and the more qualified the employee is, the more likely they might be to get a better role (once again this is not a prerequisite, however some organisations will choose a staff member with NZQA qualifications in a certain area over those who have no qualifications at all).

Problems faced by Security officers:

One issue that security guards are increasingly facing is the lack of authority they have to deal with criminals. A security officer has the same powers to detain arrest and use force as any member of the public however “in my opinion these are insufficient, but that’s what we have,” says Bryce.

Security officers are employed to “detect, deter, observe and report,” however they don’t have the authority to hold an intruder down or physically stop someone from breaking into a building or damaging a building.

If a dangerous situation occurs, police are not always available to call on if anything gets out of hand and are only notified once it has been confirmed that a criminal offence has been committed. “Attempting to notify them before then is usually met with a refusal to enter an event as ‘no offence has been committed,’” Bryce says.

“Determining whether an offence has been committed usually requires an officer investigation which is where it all goes pear shaped,” he says.

Problems that can arise from this is that if the offender is still present they may attack the officer, alternatively they will leave the scene quickly before the police arrive “despite assurances from on high, they are not deterred by traffic laws and



ADT Armourguard General Manager Ian Anderson, at ADT's Auckland office

do not tend to drive their stolen cars at 50 km per hour,” says Bryce.

However in different situations, a security officer may be required to use force, according to Anderson, “a guard working for the courts may be required to escort an offender out of a courtroom where some contact with the offender may be required.”

Although they may not have as much authority as the police, security guards are still a good deterrent for a business, with most criminals choosing to hit a business that is not being guarded as opposed to one that is. Most criminals will watch a business and possibly enter the building a few times to check out the monitoring systems before they actually break in. Statistics on how much more effective security guards are for any business is highly confidential yet Bryce says that

from his experience, most crime has been known to reduce once a security officer is employed.

The role of a security guard can be dangerous, with two officers being murdered in the last eleven years and many in a critical condition after a break-in has gone wrong. The statistics of how many security guards are injured per year are not available but depending on the nature of the business, being a security officer can be a very rewarding although often dangerous job.

Alarm monitoring security

Some businesses choose to employ a monitoring system that doesn’t have a security guard on site but will notify a security company if an alarm is set off. This can be used in both the employees home and at a business address or sporting arena.

A security officer has the same powers to detain, arrest and use force as any member of the public however “in my opinion these are insufficient, but that’s what we have,” says New Zealand Security Officers Association Bryce Winstone.



Security officers are about more than checking locks and NZSOA believe they should have more powers than they currently are allowed by law

The monitoring system usually works over a standard telephone line and will connect to the security centre within seconds if an alarm is triggered.

Once the security system receives an alert they will carry out the instructions they have been given by the employer. This may include calling the premises or a set amount of key people in the organisation to check that everything is ok then calling emergency services or sending out a security guard straight away.

If the alarm has been set off by mistake, staff can be given a code to enter into the keypad which will bypass the security company. If the alarm is tripped by an intruder, it can be a matter of minutes before the emergency services or a security officer is sent to check out the problem.

This isn't always as effective as having a set of security guards standing at the door or circling the premises; however there is the option to install a silent alarm which will not alert the intruder but allow security to get to the scene before the intruder runs away.

Gate Security officers

For high profile businesses, large homes or organisations where highly confidential information is held, many companies will choose to employ security guards at the gate; their roles will usually involve keeping an eye on who is coming in and out of gate and whether they have authorisation to be in the area. Although many companies choose to use electronic gates and swipe cards, the security guard is still a great tool because they can keep an eye on the perimeter of the area and ensure that no one tries to break in.

Depending on the nature of the business, this can be a rather dangerous and tedious job, aimed towards people with a lot of patience, the ability to deal with confrontation and think on their feet if any problems arise, such as intruders, disturbances, unauthorised people trying to enter the building and threatening behaviour.

Conclusion

No matter how big an organisation is, it is always important to remember to get a

Employing security personnel as part of the business, on a contractual basis or through a security company may cost a little extra but the investment is worth the money that you could lose after a break in or through theft.

good security system installed. This may include alarms, CCTV cameras, swipe card machines and computer monitoring devices. Most importantly it is vital to remember that no matter how effective an alarm system is, there is always the danger of a power surge or damage from an intruder who could close down an alarm system if there are no back-up systems.

Alarm back-up systems include silent alarms that will go off if wires are cut or there is a power surge and of course, the trusty security officer. A clued up security officer is always more effective than an electronic system which could break down so it is important to invest in both an alarm system and a security officer to monitor the system. With both a monitoring system alongside a reliable security firm, organisations are more likely to save money in the long run by avoiding the high costs of repairing windows, replacing products and reclaiming product loss from employee theft and criminals.

The average security guard is one of New Zealand's unsung heroes, without them, businesses can be highly vulnerable to observant criminals. Although they might not have the abilities police do, if trained well and employed by a reputable security company they will arrive at a break-in faster, they usually know the business better than the police system do and they usually have the experience to deal with dangerous situations in a calm and sensible way.

Employing security personnel as part of the business, on a contractual basis or through a security company may cost a little extra but the investment is worth the money that you could lose after a break-in or through theft.



Segway Personal Transporters are currently being used in New Zealand by the security industry in both government departments and private enterprise

NEW - Bosch Recording Station

Building on DiBos technology the Recording Station uses Bosch's proven video management, recording and communications technology and takes IP based video surveillance to a new level. It forms an integral part of overall security solutions for many applications – including banks, large retailers, railway stations, city centers, industrial facilities and office buildings.

With Recording Station you can retrieve live and recorded video from anywhere in the network. Whether they are on site or at a remote network location, authorized personnel have quick, convenient access to all information making Recording Station the perfect solution for surveillance over distributed networks.

Recording Station supports live viewing and recording at any resolution up to 2048 x 1536 pixels (3 Megapixel) including HD widescreen resolutions. It manages up to 32 IP video sources (Bosch and 3rd party) that are compatible to the following video compression standards:

- ◆ Bosch H.264
- ◆ Bosch MPEG-4
- ◆ Axis MPEG-4
- ◆ MJPEG via HTTP and TFTP

The unique, scalable GUI allows live and recorded images from multiple remote stations to be viewed from a single PC (receiver station). With this powerful function, security managers can monitor and supervise multiple locations simultaneously even if remote stations are connected through a WAN.

Each camera offers in-window pan/tilt/zoom functionality from local or remote facilities. Images are displayed with date/time, location, camera name and the status of connected devices such as detectors and sensors. Recording Station can be programmed to respond to specific situations and events automatically. In response to alarms, the system can be programmed to record at a higher quality and to transmit images or messages to security personnel.

Playback is easy thanks to familiar search and navigation functions using a graphical timeline control. Users can playback recordings from multiple stations simultaneously and synchronously on one interface. Fast, powerful image search functions like the Smart Motion Search eliminate time consuming manual searches.

Bosch Recording Station



Key Features:

- ◆ Recording and Management Software for IP video
- ◆ Connect up to 32 video sources per station
- ◆ Supports Bosch H.264/MPEG-4, third-party MPEG-4 and JPEG devices
- ◆ HD / Megapixel camera support
- ◆ Connect to and from any station
- ◆ Unlimited remote receiver stations
- ◆ Web browser remote access and viewing
- ◆ Low bandwidth (WAN) support
- ◆ Interfaces with Bosch intrusion, fire and access solutions

Security Systems

1 ST-VS/PRM4 | 6/21/2010 | © Robert Bosch GmbH 2010. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

**BOSCH**



Export the video to an archive with the push of a single button - all digitally watermarked to ensure the credibility of your recordings. You can even export multiple cameras from different recorders.

Use the scheduled export to recurrently backup your recordings on various storage devices, such as external disk arrays and NAS (network attached storage).

To ensure the highest security, all system access is controlled by multiple user authorization levels which determine individual permissions for each user to a very high level of detail. These authorization levels determine what a user can do in the system.

Elements such as camera viewing and control, playback and export of recordings, as well the types of system

configuration settings that are allowed can be individually configured. Events, such as login, log-off, status changes, image transmission, video export, and system shutdown are logged in a database and can be easily imported to spreadsheet programs like MS Excel. Video authentication is built-in to detect any attempt to alter the recorded Images.

Recording Station provides various interfaces to other systems such as Bosch access solutions and alarm panels, as well as external systems like ATM and POS terminals, fire alarm systems, number plate capture equipment and video content analysis solutions.

Integration with other security and building management systems is accomplished using OPC (OLE for Process Control). When even tighter integration is required, our VideoSDK

ZoneTechnology
Your Security Supply Partner

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

provides you with a complete toolbox of modules for playback, searching, viewing and much, much more.

Use Recording Station in a LAN environment with Bosch Video Management System to advance to a true enterprise solution which provides a comprehensive feature set such as centralized user, event and alarm management, multimonitor workstations with zoom able sitemaps and CCTV keyboard control.

Bosch Recording Station

Compatible Cameras

Bosch H.264 cameras / encoders



new
NBC-225/255-P
NDC-225/255-P
NBC-265 (HD)
VIP-X1XF
VIP-X1600XFM4
Dinion 2X IP
FlexiDome IP
...and compatible

Bosch MPEG-4 cameras / encoders



Dinion IP
AutoDome IP
FlexiDome IP
Extreme IP
VIP X1/X2
VIP X1600
VideoJet X10/20/40
...and compatible

Axis MPEG-4 cameras



new
AXIS 211/211A/211M
AXIS 214
AXIS 221
AXIS 223M
...and compatible

max. 32 cameras
per station

MJPEG cameras / Megapixel

Bosch Megapixel
(NWC 700/800/900)
...and compatible to
HTTP/TFTP



Security Systems



Chemical Facility Anti-Terrorism Standards (CFATS)

By Richard Allardice

In 2006, the United States Congress authorised the Department of Homeland Security (DHS) to develop and implement security regulations for chemical facilities that handled high-risk chemicals. These would take into account risks to the general populace should a terrorist attack take place. A set of standards called the Chemical Facility Anti-Terrorism Standards (CFATS) were released on April 9th, 2007, which outlined security standards for facilities from a range of sectors, including: chemical manufacturing, storage and distribution, energy and utilities, agriculture and food, paints and coatings, explosives, mining, electronics, plastics, and healthcare.

Compliance with CFATS follows four stages. Stage I is classification; facilities which house, produce, use, or handle 'Chemicals of Interest' (COI) above a threshold set by the DHS must complete a CFATS Top Screen, which gathers information on the quantity and type of COIs involved at a particular facility. This is completed via a DHS secure website called the Chemical Security Assessment Tool (CSAT). Facilities are then divided into tiers based on potential risk (Tier 1 represents the highest risk and Tier 4 the lowest) and then notified of their Tier level. According to Ryan Loughlin, Director of Petrochemical and Energy Solutions for the Advanced Integration Division of ADT (writing for SecurityInfoWatch.com), 'Characteristics obviously change from site to site, but tier ratings appear to be based on a combination of COI type and amount, proximity to a population centre and the recognition of the COI by the general public'.

If facilities receive a Tier level in writing from the DHS they must complete a Security Vulnerability Assessment (SVA).



Fuel storage tank on Auckland's waterfront could have been a major security threat

This Stage II step requires facilities to catalogue critical assets related to their COIs, and to outline their security procedures and equipment. In addition, facilities must evaluate their own vulnerability and emergency response procedures to a series of DHS-prescribed attack scenarios.

Stage III is a Site Security Plan (SSP), which requires facilities to create a security plan based on their Tier level, and any particular issues identified by their DHS notification letter. A document called the 'Risk-Based Performance Standards'

(RBPS) outlines 18 parameters along which facilities have a degree of discretion to create their plan. The parameters are adjusted according to the Tier level of the facility. For example, 'RBPS1: Restrict Area Parameter' for a Tier 1 facility requires 'an extremely vigorous, high-integrity system to secure the perimeter that severely restricts or delays any attempts by unauthorised persons to gain access to the facility.' In contrast, a Tier 4 facility requires 'a system to secure the perimeter that reduces the possibility of access to the facility by unauthorised persons.'



Loktronic ● Innovationz

Security with innovative technology

LOKTRONIC slimline electromagnetic locking solutions

now with all
stainless fittings

Whether your need is for unmonitored, part or fully monitored locks, aluminium or stainless, indoor or outdoor locks, we have all your needs covered. A complete range of accessories allows a simpler and more professional installation. **PLUS! New 10 year guarantee!***

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 locks
- Stainless outdoor and gate locks

*Indoor models only.

Loktronic ● Innovationz
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



The implementation of the SSP is Stage IV. Facilities are afforded a fixed amount of time before a series of DHS inspections to ensure the SSP is being appropriately implemented. There are hefty fines for noncompliance: \$25,000 a day or even closure of the facility by the DHS. Facilities are required to monitor their COI levels; exceeding a minimum threshold for COIs requires facilities (whether currently tiered or not) to submit or resubmit a CFATS Top Screen.

Given the degree of judgement and discretion involved, and the amount of documentation and signing-off required, compliance may seem a daunting undertaking. Facility safety officers may require the services of a security integrator to assist with compliance procedures for CFATS. Security firms such as ADT Security have a dedicated ADT Advanced Integration Division to serve facilities in need of integration assistance. They have considerable experience and knowledge in chemical security predating CFATS.

The following is a condensed summary of the current ADT Advanced Integration Division featured White Paper (available on their website) outlining '10 Tips for Completing a CFATS Site Security Plan':

1. Develop your plan before you begin the SSP

The CFATS SSP is designed to allow the DHS to ascertain whether current security measures are adequate. Important considerations are COIs, Tier level, and types of potential security threats. The SSP should be the end result of identifying 'the combination of security technology and policy and procedures that, when combined and integrated, provide a security strategy it believes appropriate for the requirements of CFATS'.

2. Know what your Tier level means

Tier level dictates the performance level a given facility needs to have in order to adhere to the 18 RBPS. Tier level differences can equate to considerable differences in the intensity of the RBPS (as illustrated earlier by Tier 1 and Tier 4 RBPS for restricting the area perimeter). A facility should also tailor its approach to each RBPS based on the kinds of DHS-prescribed attack it may potentially face. The White Paper gives the example that 'the Tier 1 with release issues will need to consider such things as standoff distances, crash-rated barriers and line-of-sight between critical assets (targets of attack) and attack positions inside and outside the parameter.'

3. Understand the ramifications of 'Release' security issues and 'Theft & Diversion' security issues

'Release' security issues revolve around the consequences of an attack on a facility close to 'population centres and other critical assets.' This could result in explosions or the spread of toxic vapour. The DHS has set out a number of attack scenarios which leave little chance of preventing the attack, so in planning for these eventualities emphasis should be given what the response will be. Strategies should 'provide adequate time from the point of detecting an attack to the point that the planned response is effective.'

'Theft & Diversion' security issues involve undetected access to COIs, which may in turn be used as 'weapons of mass effect,' or components of these weapons later on. Emphasis here should be controlling who has access to both COIs, and the manner in which COIs are transported. Recommended steps include 'training, written procedure and cyber security.'

4. Include all of your critical assets in your plan

It is important that the critical assets reported in the SVA match what is later reported in the SSP. Changes should be justifiable to the DHS and evident upon inspection. The DHS outlines that non-critical assets could be considered critical 'based on the ability of an adversary to use the assets as weapons against a critical asset,' for example, fuel in a vehicle fuel tank could be used as a weapon. 'The physical security of cyber assets' is also important in preventing unwarranted control and release of COIs.

5. Apply the concepts of control, deter, detect, and delay

These four simple principles encompass most security plan requirements. 'Control' is a facility's ability to manage activities and assets; this refers to both access to information and physical space/assets. 'Deter' requires that the effort an attacker requires to attack a facility is greater than that required elsewhere. This might mean having layered security, with a number of steps required to gain access to sensitive areas. 'Detect' is the ability to recognise an attack is occurring. Faster attack recognition means a faster response time. 'Delay' is the means to hinder an attack long enough to respond appropriately. This could be a combination of layered access, limiting vehicle mobility and reducing visibility.

6. Record your answers and rationale

Both answers, and rationale for the answers, should be recorded to pave the way for a smooth DHS inspection. Having this information in a separate document also allows greater ease of management and legal review.

7. Consider using industry standards and best practices

There may be 'decisions that have significant cost and operational consequences' to consider. Using industry standards and best practices guidelines allow facilities to show justification for their rationale, based on the recognised practices of other reputable groups.

8. Generate a list of security procedures

Since personnel will be the driving force behind enacting revised security procedures, individuals should: have copies of their responsibilities; they should be trained; and there should be a policy for the periodic review of these procedures. The DHS will require evidence of this upon inspection.

9. Generate a list of responsible personnel

There needs to be a management plan for effective communication and security. It is a requirement under 'RBPS 17: Officials and Organisation' that facilities have a demonstrable and efficient chain of command.

10. Seek help with your plan

There is no need for facilities to feel isolated, or that they need to reinvent the wheel. There is a growing body of knowledge around compliance with CFATS that can be accessed through the DHS itself, industry trade groups, consultants, and security integrators.

A note on CVI

The Chemical-Terrorism Vulnerability Information (CVI) program sets restrictions on who has access to sensitive information. Since information submitted to the DHS comes under the CVI requirements, individuals who handle this information must be CVI trained and certified. Compliance with CVI is taken very seriously.

CFATS and the requirements detailed here are United States regulations, but watertight security and management of potentially dangerous chemicals are naturally also considerations for New Zealand facilities. The implementation of any new regulation such as CFATS requires considerable cooperation between industry and governing bodies; the ongoing work between the DHS and facilities in the United States will continue to be of interest in terms of how to make this kind of process proceed as smoothly as possible.



LEAWELD

Total Perimeter Security

Risk Assessed

THE TRUSTED ARMOUR SOLUTION...
for all your perimeter security requirements



TRUCK STOPPER



INDUSTRIAL CANTILEVER



LOUVERED GATE



SWING GATE



WIRE MESH SLIDER



HANDIFENCE FLAT TOP FENCING



HANDI FENCE SPIKE TOP FENCING



PALISADE



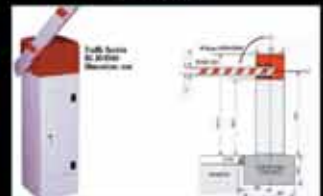
MILD STEEL MANUAL
RETRACTABLE BOLLARD



BURGLAR BAR GRILL



SECURITY TURNSTILE

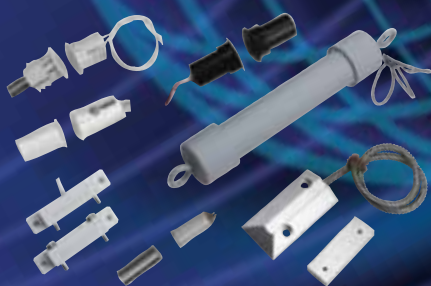


100% DUTY CYCLE
TRAFFIC BARRIERS



Leaweld Manufacturing Ltd. Telephone: 09 827 1904. Fax: 09 827 1804
Unit 4, 31a Veronica Court, Veronica Street, New Lynn, Auckland.
Email: sales@leaweld.co.nz www.leaweld.co.nz





total reed switch solutions from Flair

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

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

Flair reeds from Loktronic Innovationz: an unbeatable combination.

Loktronic Innovationz
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

15387_FL



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 Innovationz
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

15388_PSC

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 Innovationz
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

15389_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 New Pacom EVO Series Cameras Have Arrived.

The series comprises of full-bodied cameras, dome cameras and infrared vandal proof domes. All these cameras feature high quality resolution of 540 TV Lines with a 1/3" Sony Super HAD CCD image sensor.



The Pacom EVO-540 (S74391) camera is a High Resolution camera that provides sharp image quality utilising a high-tech Digital Signal Process combined with the 1/3" Sony Super HAD CCD Image Sensor.

The Pacom EVO-540DN is a High Resolution camera that provides excellent picture quality in both Day and Night operation utilising a high tech Digital Signal Process combined with the 1/3" Sony Super HAD CCD.

The Pacom EVO dome cameras provide sharp high-resolution images with excellent colour reproduction and incredible noise reduction. These day/night dome cameras also have 3-Axis capabilities for added installation flexibility..

The Pacom EVO IR Dome cameras come with in built IR LED's providing sharp high-resolution images during day and night operation. This is achieved by combining the image conversion from Colour to B&W and the precise operation of the removable day night IR cut filter.

The Pacom EVO is now available from your nearest Hillsec branch.



PENROSE, AUCKLAND

Unit 1/ 30 Greenpark Road, Penrose

Ph:(09) 525 8007 • Fax: (09) 525 8009

Pacom H.264 DVR's



Hills Electronic Security is excited to introduce the latest Pacom DVRs - the PDRH-8-RT and the PDRH-16-RT H.264 standalone DVR's, which utilises the all-new ClearView ISP1000 multi function chipset, designed specifically for Pacom DVR's.

These digital recorders provide real time recording at CIF and have 4 CIF recording capabilities, offering high performance features that make them ideal for advanced digital surveillance applications.

The ClearView ISP1000 has a number of features specific to the security industry, such as integration of multiplexer, multi channel audio codec, multi-resolution compression, motion detection, blind detection, de-blocking filters, to name a few.

The PDRH-8-RT (S76408) and the PDRH-16-RT (S76409) features include:

- Embedded Linux operating system
- H.264 Compression
- 8 or 16 Channel Looping inputs
- Recording and Playback rate - (Real-time @ CIF)
- Built-in DVD-RW
- Two-way audio communication
- Digital zoom (x4) in playback mode
- Multi channel data export with audio
- Remote monitoring, search, backup, setup, upgrade

The PDRH-8-RT and the PDRH-16-RT are now available from your nearest Hillsec branch.



PENROSE, AUCKLAND

Unit 1/ 30 Greenpark Road, Penrose

Ph:(09) 525 8007 • Fax: (09) 525 8009

DX8100 Digital Video Recorder



The DX8100 Series digital video recorders (DVRs) bring to market a new and innovative hardware platform that is powered by unparalleled and unique highperformance software. The DX8100 is expandable to meet your future security requirements.

The DX8100 is interoperable with your existing DX8000 DVRs, allowing you to build upon your existing DX8000 security system. A DX8100 client can operate and administer DX8100 and DX8000 servers in the same network.

When you need to quickly and easily add more security cameras, the DX8100-EXP 16-channel expansion unit extends the 8- or 16-channel DX8100 to 24 or 32 channels. With or without the channel expansion unit, all of the cameras can now take advantage of the increased frame rate of 2CIF and 4CIF recording. The DX8100 records video up to 280 images per second (ips) at a maximum CIF image size.



PENROSE, AUCKLAND

Unit 1/ 30 Greenpark Road, Penrose

Ph:(09) 525 8007 • Fax: (09) 525 8009



Key switches

This versatile product range is produced with two functions

Momentary contact (30°)

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 sampling rate

Accessories are: Key switch mounting bracket (suitable for mounting bracket)

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

Supplied random keyed. Can be master keyed.

Client's own key cylinder can be converted.

Front or rear fixing.

Designed, tested and produced in New Zealand by Loktronic.



Loktronic Innovations
LIMITED

Unit 7, 19 Eden Street, M.E. Eden, Auckland
P.O. Box 2229, Wynndene Street, Auckland 1150 New Zealand
Ph: 61 9 622 2919 Fax: 61 9 622 2921 0800 PDR LOCK
www.loktronic.co.nz mail@loktronic.co.nz



Loktronic Innovationz control buttons and plates

The Touch to Exit unit and each push button 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.



Loktronic Innovations
LIMITED

Unit 7, 19 Eden Street, M.E. Eden, Auckland
P.O. Box 2229, Wynndene Street, Auckland 1150 New Zealand
Ph: 61 9 622 2919 Fax: 61 9 622 2921 0800 PDR LOCK
www.loktronic.co.nz mail@loktronic.co.nz



CyberLock

access control conversions

CyberLock is an innovative lock system that easily converts existing mechanical locks into fully functional access control systems.

CyberLock electronic cylinders replace standard mechanical cylinders. No wiring or battery is required at the lock.

The keys cannot be duplicated and each key contains a list of locks it can open, at specific times and dates. Keys can be assigned start and expiry times. The audit trail is recorded in both the locks and the keys, and can be downloaded to CyberAudit software for viewing.

Loktronic Innovations
LIMITED

Unit 7, 19 Eden Street, M.E. Eden, Auckland
P.O. Box 2229, Wynndene Street, Auckland 1150 New Zealand
Ph: 61 9 622 2919 Fax: 61 9 622 2921 0800 PDR LOCK
www.loktronic.co.nz mail@loktronic.co.nz

Extreme CCTV
SURVEILLANCE SYSTEMS
A member of the Bosch Group



BOSCH Zone Technology
Your Security Supply Partner

The latest Pacom PDR



The PDR-4LXH is the latest PDR from Hills Electronic Security and is accompanied with new features which allow record and playback speeds of up to 100ips @ CIF. The DVR comes with 4 CIF record capabilities that make it ideal for advanced digital surveillance applications requiring triplex functionality, such as real-time recording, real-time playback and monitoring with superb video quality. It comes with built-in Web-server and two-way audio when connected to the RASplus monitoring software. Recorded video can be exported via an Internal CD±RW Drive and also to external USB devices.

Features include:

- 4 Channel Loop-Through Video Connectors
- Playback and Recording rate: 100ips @ CIF
- 4CIF recording capabilities
- Embedded Linux Operating System
- Live or Recorded Video Access via Internet Explorer Web Browser
- Search on:- Date/Time, Record Table, Calendar, Event, Motion, Museum, Text-In
- New Case Design
- New Advanced GUI

Hills
Electronic Security
New Zealand

**Excellence in
Security**

PENROSE, AUCKLAND

Unit 1/ 30 Greenpark Road, Penrose
Ph: (09) 525 8007 • Fax: (09) 525 8009



Dialock DT Lite

is an electronic identification and locking system for secure and simple access control solutions for your project.

Dialock DT Lite can be used to flexibly allocate and block access for your guests and staff in hotel office and residential applications. DT Lite is also easy to install or retrofit. The fact that identification is touchless makes the system water-resistant and extremely low maintenance.



- Consists of an inside module / outside module
- Access integration
- TAG-IT ISO™ 15693 technology
- Fast opening process
- DND function (do not disturb) via thumbturn
- For door thicknesses 38-80 mm
- Alarm function

www.hafele.com
Freephone 0800 4 hafele

HAFELE
FINDING BETTER WAYS



Dialock Door Terminal DT400

Design

- Appealing and unobtrusive design, matches modern interior architecture.
- Six door handles and three different finishes are available: Matt and polished stainless steel and polished brass (other finishes on request).



Innovation

- The solution for the hotel room door or office only requires standard rosettes on the outside and the extremely flat reader behind the escutcheon.
- No other components except for the locking cylinder for emergency opening.
- The terminal electronics, the battery compartment and the DND module are accommodated in the internal fitting.
- The DT 400 is easy to operate.

www.hafele.com
Freephone 0800 4 hafele

HAFELE
FINDING BETTER WAYS

always lok in new zealand made!



always specify and buy with
confidence and quality in mind.

Seal in the brand of security that is uniquely...

Loktronic ● **Innovationz**

Security with innovative technology

Unit 7 19 Edwin Street Mt Eden Auckland
PO 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 mail@loktronic.co.nz