

ISSN 1175/2149

# NzSecurity Magazine

June/July 2013



PERIMETER SECURITY  
SECURITY CONFERENCE  
PASSWORD HACKING  
**FIRE INQUIRY**

[www.NewZealandSecurity.co.nz](http://www.NewZealandSecurity.co.nz) • [www.FireandSecurityNews.co.nz](http://www.FireandSecurityNews.co.nz)  
Trusted sources of information for industry professionals

# Total HD surveillance

Uncompromising vision from Bosch

**125** Years **Bosch**  
1886-2011



## Bosch HD takes image resolution to the next level

The level of detail in Bosch HD images captures extensive information throughout the whole scene. Our HD portfolio offers you a complete solution across the entire surveillance chain - from scene to screen. Every component is designed specifically for HD technology, so you can be sure that 'HD in' equals 'HD out'.

Ask about our Bosch HD product solutions today.



**BOSCH**  
Invented for life

**ZoneTechnology**  
Your Security Supply Partner

Email: [sales@zonetechnology.co.nz](mailto:sales@zonetechnology.co.nz)  
Web: [www.zonetechnology.co.nz](http://www.zonetechnology.co.nz)

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

**Wellington**  
35 Abel Smith Street  
Wellington  
Ph: 04 803 3110

**Christchurch**  
Ph: 03 365 1050



# IP SMART & EASY

## Network Video Recorder

# NVR



### Direct Connect PoE

Built-in PoE switch.

### Quick Configuration

Install up to 8 cameras in minutes.

### Auto Discovery

Just plug the cameras in  
and it will do the rest.

### Easy Set up Wizard

Easy to follow instructions. Set up  
complete in 8 easy steps.

## All in one smart, easy, and simple solution.

### Available at:

## Contact Details

Craig Flint

Telephone: (64) 07 868 2703

Mobile: +64 (0) 274 597 621

Postal and delivery address:

27 West Crescent

Te Puru 3575

RD5

Thames

New Zealand

## All enquiries to

[craig@newzealandsecurity.co.nz](mailto:craig@newzealandsecurity.co.nz)

Editorial contributions welcome.

## Deadline for all copy

August - September 2013 issue

is the 15th July 2013

## August/September

Banking, Insurance, Finance,

Loss Prevention, Industry Training

## October/November

Professional & Business

Accountants, Lawyers, Managers

and Consultants

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

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

# CONTENTS

## Security

- 6 Night Vision & Thermal Imaging
- 8 Fencing industry sees the light
- 12 Future Fibre Technologies
- 14 CCTV Network Cameras
- 16 FLIR launches new D-Series
- 18 Synology releases latest Surveillance Station
- 19 aptiQ™ Multi-Technology Readers
- 20 Wireless system solves automatic gate dilemma
- 21 Thermal perimeter security system cuts power bills
- 22 Axis Communications
- 24 HID Global
- 28 NZSA Conference & Exhibition 2013
- 30 Zone Technology
- 32 Case Study - Tru-Test Group
- 34 MLAA Association News
- 35 NZSA Association News
- 36 NZIPI Association News
- 37 Investigating Fraud
- 38 Kiwi invention prevents password hacking
- 40 Data breaches costing firms dear
- 41 Small businesses targeted by cybercriminals
- 54 Product Showcase

## Fire

- 42 Kiwi helps expose errors in London blaze
- 46 BROOKS Alarms
- 48 Contract law change essential
- 51 Every crash reverberates
- 53 Kiwi high rises safer than London

For a FREE online subscription go to  
[www.newzealandsecurity.co.nz](http://www.newzealandsecurity.co.nz)

ENJOY a **10** year  
guarantee

on Loktronic Indoor  
Electromagnetic Locks!

**Loktronic**

0800 367 565  
[www.loktronic.co.nz](http://www.loktronic.co.nz)

## Associations

**ASIS**  
INTERNATIONAL  
Advancing Security Worldwide™  
[www.asis.org.nz](http://www.asis.org.nz)

**MASTER LOCKSMITHS**  
[www.masterlocksmiths.com.au](http://www.masterlocksmiths.com.au)

  
NEW ZEALAND INSTITUTE OF  
PROFESSIONAL INVESTIGATORS INC.  
[www.nzipi.org.nz](http://www.nzipi.org.nz)

  
NEW ZEALAND SECURITY ASSOCIATION  
**NZSA**  
SECURITY  
[www.security.org.nz](http://www.security.org.nz)



Visit Axis at Security  
Exhibition 2013:  
July 24-26  
Sydney  
Booth E22

What are you looking for?  
See it – and every detail of it.

All images are conceptual. For product information and actual footage from Axis cameras, visit [www.axis.com](http://www.axis.com)



Image quality is always important, but the benefits are really determined by how you will use the images. We make your job easier, by focusing on **image usability** first. Utilize our competence and our comprehensive range of image features such as HDTV, Wide Dynamic Range and Lightfinder.

As the world leader in network video, we ensure you always get video you can use – no matter what the conditions are.

**Get the Axis picture. Stay one step ahead.**

Visit [www.axis.com/imageusability](http://www.axis.com/imageusability) or email [contact-sap@axis.com](mailto:contact-sap@axis.com)

Axis network cameras with HDTV performance deliver true color representation and high quality images. An appealing solution when every detail matters.

**AXIS**<sup>®</sup>  
COMMUNICATIONS

Distributed by:

**CHANNELTEN**  
SURVEILLANCE SOLUTIONS

**Hills**  
Electronic Security  
New Zealand

# Revolutionary new Night Vision and Thermal Imaging systems for public safety and security

**T**he ability to see at night, whilst remaining unseen, is critically important for security, law enforcement and military personnel. Dangerous situations can be identified and observed whilst awaiting back-up. Night vision systems are also important for Search and Rescue, navigation and crowd control.

Nelson based **Archetype Precision Systems Limited** are New Zealand's leading supplier of night vision systems, with a highly developed range of products designed for civil and government applications. These products include image intensifier tube night vision systems, digital night vision systems and thermal imaging equipment for mobile and fixed applications.

These technologies are suitable for a variety of situations and budgets and are classified by detector type:

### Image intensifier tube night vision

These systems amplify light using a compact cathode ray tube that converts ambient light into a highly amplified electron stream, which is focused onto a phosphor screen that emits light many times brighter than the original image.

These devices are available as monoculars, binoculars, goggles and rifle sights. The cost of these items varies with the performance of the image intensifier tube. The tubes that are available include CF-Super tubes, Generation 2+ tubes, and auto-gated Milspec Generation 3 tubes.

### Digital night vision

This exciting new technology is at the forefront of night vision development. A low-light sensitive, infrared-biased CCD array captures and amplifies the image. A SumLight algorithm may be employed to further enhance the image, a technology that was first developed by the US Airforce to identify spy planes during the Cold War. SumLight performs this enhancement in real-time, enabling the user to see and record in extreme darkness.

Digital night vision systems vary in price according to their resolution, light amplification factor and ability to record. In-built digital recorders feature motion sensor recording and date and time stamping. Prices start from \$600 through

### The Pulsar Edge



*The Pulsar Edge GS 2.7x50 night vision binocular is a fine example of a CF-Super tube system. With a very attractive price and performance mix, this product is currently in use by Ministry for Primary Industries Fisheries officers for anti-poaching surveillance.*

### The Guardian Thermal Imager



*The Guardian Thermal Imager is built to modern military standards. It forms an infrared image with a motorised 61mm germanium lens and a high speed ULIS SAS Amorphous Silicon (a-Si) detector. This unit can detect a person at 2000 meters in complete darkness, which is ideal for surveillance, search and rescue, coastal patrols, and policing dangerous situations.*



to \$2500. These systems are available as monoculars and rifle sights.

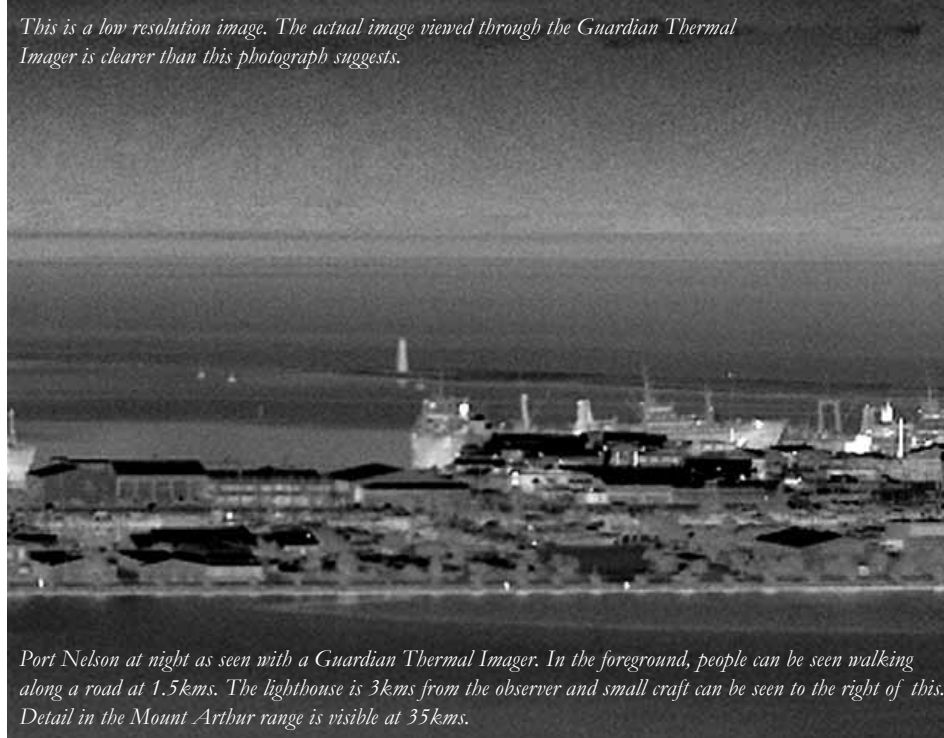
### Infrared thermal imaging systems

Thermal imaging cameras are effective at night and in daylight, even in poor weather conditions. The infrared sensor forms an image in the near infrared spectrum of between 700µ through to 1400µ. Red light has a wavelength of 650µ.

People can be rapidly detected at long range, even when obscured by foliage and light fog.

The **Archetype Precision** range of thermal imaging cameras are built with leading edge European Amorphous Silicon (a-Si) infrared detectors. These detectors are more sensitive, durable, and cost less to manufacture than Vanadium Oxide (V-Ox) detectors, that have until now, been the only previous option. Because a-Si technology is sourced from Europe, it is not subject to the performance restrictions imposed by the US Department of State on US made models.

The product range includes thermal monoculars, bi-oculars, riflesights, gyro-stabilised marine systems, and fixed cameras that integrate into existing



security networks. These uncooled systems start from \$5,000. High-end cryogenically cooled Thermal Image systems are available for applications such as defence, policing, and naval patrolling.

All of these technologies are available to civilian companies and

government departments, who are now able to source the very best equipment from a New Zealand Supplier.

As well as supplying equipment, **Archetype Precision Systems** offer training, advice, and servicing and can be contacted on 03 9700 570.

# Advanced Safety and Security Systems



**Pulsar Edge GS Night Vision Binocular**



**Pulsar Recon Digital Night Vision Video Recorder**



**ANV Generation 3 Night Vision Goggle**



**Pulsar Quantum HD38 30Hz Thermal Imager**



**Guardian IR516F Bi-Ocular 50Hz Thermal Imager**



**ARCHETYPE**  
PRECISION SYSTEMS LIMITED



**PTZ 50Hz Thermal - Digital Fusion  
Fixed Security Cameras**



**PTZ Gyro-Stabilised 50Hz Thermal  
- Digital Fusion Cameras**

**For more information and prices phone 03 9700 570  
www.nightvision-nz.co.nz Email: sales@acad.co.nz**

# Fencing industry sees the light

**Firms operating in the perimeter fence arena are starting to turn their back on copper systems in favour of fibre optic cables, writes Steve Hart**

**C**ompanies in the perimeter fence industry are in for a boom time according to one industry professional.

Alec Owen of Future Fibre Technologies believes global revenue forecasts for 2013 are in the vicinity of \$400 million for PIDS systems, with fence-mounted sensors accounting for more than 65 percent of the total.

According to his report "The Boundaries of Security 2013", expectations are that revenue will continue to grow steadily at around five percent a year.

"The market split for fence-mounted sensors is around 25 percent for Asia-Pacific and the remaining 75 percent is evenly split between the Americas and EMEA."

Owen, who is international client manager for the fibre optic based intrusion detection firm, says sales of fibre optic fence-mounted sensors continue to outstrip sales of copper sensors.

"Recent announcements of fibre-based intrusion detection solutions by some previously copper-only manufacturers further reinforce this market shift," he says.

In his report, Owen says global social and political instability with the ongoing threat of terrorism will continue to drive the need to both fund and enforce regulation and legislation regarding perimeter security at critical national infrastructure sites such as water reservoirs, data centres, transportation hubs, and historic landmarks.

He says an increase in organized protest movements – environmental, political, climate and economic – is also heightening the need for advanced perimeter security.

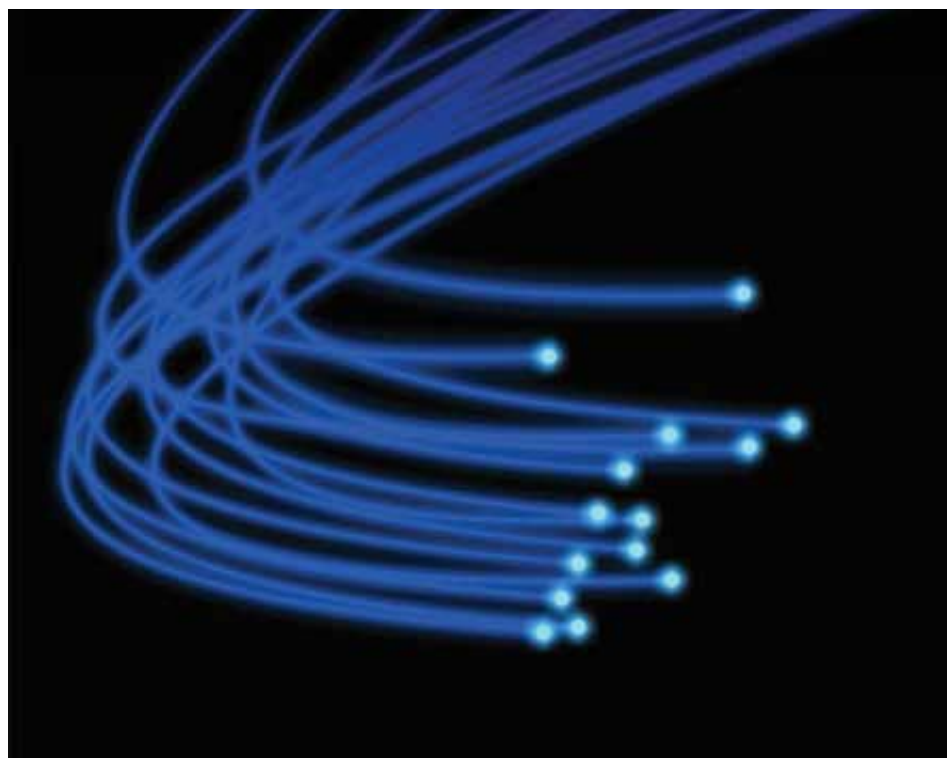
"Legislation will continue to play a major role in the growth of perimeter security equipment along with stimulus monies and other regulation," he says. "Chemical, petrochemical and liquefied natural gas (LNG) facilities are subject to increasing government legislation and regulation in many countries.

While the potential growth for perimeter security is large, typical government bureaucracy and delays in rolling out any project means the actual market growth will be at a more moderate and steady pace."

He predicts there will be increased demand for newer perimeter intrusion detection systems that require limited or no power in the field, especially for those remote locations and long distance applications where power is not readily available, making these installations more viable than in the past.

"Innovation has been driven by numerous smaller developers and manufacturers of niche technologies," he says. "The plethora of intrusion detection sensor systems now on offer and under development includes electromagnetic point sensors, geophone point sensors, fibre optic fence sensors, infrared beams, buried magnetic lines, fibre optic mesh, buried seismic lines, vibration sensors and video event detection.

Globally, sales of fence-mounted fibre optic intrusion detection systems are estimated to be almost twice those of the traditional copper based microphonic and vibration based systems."





# HIGH - DEFINITION IMAGE EXACT & CLEAR VISION

VIVID IMAGE DAY & NIGHT



## LVN7300

3 Megapixel High Resolution  
Vandal Proof Dome Camera

3MP @ 20fps, ICR Day & Night, Wide Dynamic



### FEATURES

- 6.49 mm (1/2.8 Type) CMOS
- 3 ~ 9 mm Vari-focal Lens, F1.2
- 20 fps @ 2040 x 1536 - 30 fps @ 1920 x 1080
- Min. Illumination
  - Color : 0.5 Lux @ F1.2 - B/W : 0.07 Lux @ F1.2
- Auto Back Focus
- 80dB of Wide Dynamic Range
- ICR Day & Night, 2D + 3D DNR
- Video Analytics Embedded
- LG Ipsolute VMS, Mobile App
- Micro SD Slot
- Vandal Proof (LVN7300)
- Onvif Compliant

## Design

Owen says designing an effective and reliable outdoor perimeter security system is rarely a simple exercise. Determining the specific site risks, customer expectations, monitoring and intruder response mechanisms available, and more importantly the customers' security budget, must all be taken into account.

"While each individual installation will have its own unique characteristics and requirements for outdoor perimeter protection, they still follow the fundamental protection rules known as the Five Ds – define, deter, detect, delay and detain.

An effective perimeter security system will consistently prevent intruders from reaching their target within the site undetected.

The key to securing perimeters is to use a multi-layered approach. The more layers or obstacles an intruder needs to get through to reach his target, the more determined he will need to be, the more likely the chance he will be detected, and therefore the more secure the site ultimately is.

By taking a holistic approach to site security, each of the individual components or layers that make up the final intrusion detection solution should complement each other, working together to protect against both known and perceived threats.

At a number of points in the design phase there will be trade-offs made, usually associated with price and performance."



## Global growth areas for perimeter fencing

- Government and military prisons, border protection, military bases and camps.
- New airports and airport expansion programmes.
- Petrochemical sites.
- Increased seaport security for illegal people movements and to address the International Ship and Port Facility Code (ISPS Code).
- Water treatment facilities have been identified as potential risk sites.
- As demand for power increases, so does the drive to build more nuclear power plants and LNG facilities.
- Conventional coal or fossil fuel power plants face the risk from activists.
- Solar power generation is subject to the theft of expensive solar panels.

*Source/Alec Owen, Future Fibre Technologies*

## Basics

Owen says the first step in planning perimeter protection is risk profiling the site – defining the facility and considering things such as buildings on or near the perimeter (which are potential hiding spots) and looking at the land, is the area open and flat, or undulating?

He also says attention should be given to likely extreme weather conditions and to profile the type of intruder who may want to gain illegal access. Are they likely to be vandals, petty thieves, trespassers, or professional highly skilled intruders?

"Even the very best sensors available today will deliver less than optimum performance if not correctly tailored to meet the specific requirements of the site – for example, microwave sensors used on undulating ground," he says.

"The role of any perimeter security system is to act as the first level of protection – defining the boundary of the site, providing both an early warning of intrusion attempts as well as deterring, detecting, documenting and delaying any incursion," says Owen.

"The other layers that make up the solution are then used for the verification and tracking of intruders once they have breached the perimeter."

He says completing a site survey and creating a holistic plan for security, despite pressure from a customer to skip over this step, is essential.

## Upkeep

"A fence should be in a good state of repair, have adequate lighting and have vegetation cleared from both sides for clear observation," says Owen. "Always remove large trees and overhanging branches that may provide climb points.

In addition to defining the boundary of the site, the fence should also provide a sufficient delay to an intruder climbing it to give the intrusion detection system enough time to activate and position a CCTV camera to visually verify the intrusion activity.

Regardless of the fence type selected, it must be regularly inspected and maintained if it is to retain its deterrent value, and the cost of this maintenance must be taken into account.

In its simplest form, CCTV linked to motion triggered lighting can be a useful low-cost deterrent to opportunistic thieves by providing improved surveillance and observation of suspect activities.

But the more determined criminal will not be frightened off at all. Hence the need for multi-layer security systems where lighting forms an integral part."

*On the web, [www.jfftsecurity.com](http://www.jfftsecurity.com)*



## TruVision®. The new generation of HD.

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



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

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

# On guard

**Alec Owen of Future Fibre Technologies comes out fighting as he explains to Steve Hart why customer expectations need to be managed and how the perimeter fence industry can lift its game**

**A**lec Owen, international client manager at Future Fibre Technologies (FFT) in Australia, says there is no single technology on the market that will deliver full perimeter security on its own – he says there is no ‘one size fits all’ when it comes to protecting property at the boundary.

His report ‘The Boundaries of Security 2013’ says security firms need to match boundary system design to each site’s profile, and says every site will be unique.

He wrote the 114-page report, which features numerous white papers, after seeing too many companies buy inappropriate boundary protection systems from ‘box shifting’ sales staff who were ‘probably selling cars the week before they began selling security systems’.

“I wrote the report as a bit of a brain dump to educate our own people, but have made it available to everyone because the knowledge needs to be shared for the good of the industry and its customers,” says Owen.

“Too many customers are being sold absolute crap, they are being sold stuff off a brochure and what they are being told by sales people has no relationship to reality.”

Owen says staff at Future Fibre Technologies have lost out on tenders to cut-price competitors only to see that the subsequent installation of the boundary protection system fall well short of what was promised or needed.



*Alec Owen, international client manager at Future Fibre Technologies (FFT) in Australia*

“One of them was Sydney Airport which wanted boundary protection at the end of one of its runways, which is right next to a motorway,” says Owen.

“What they chose to buy is totally unsuitable technology for the location as the sensors are constantly being triggered by passing motorway traffic. Three years on and the system is delivering too many nuisance alarms and is still not working.

When companies buy a cheap system then they need to understand they won’t work as expected. They will be promised everything, but we have seen people being let down at places such as four airports in New York which feature a cheap and nasty rattler system – a system we advised them not to use.

We let the airports know it wouldn’t work and six years later it is still not running. The airports management have been sold a pup and they just have to live with it.”

Owen says in some cases it is the customer who should take responsibility for buying cheap products, rather than the best and most suitable system.

“They just buy what’s cheapest and like everything in this world – you get what you pay for,” he says. “A system that is going to have the intelligence to handle things such as large scale nuisance alarms is not going to be cheap – but it will work.”

As an advocate of the security industry, and in a bid to share best practice and offer independent advice to potential clients, Owen has tried to alert them to some of the things they should watch out for when specifying and buying boundary systems.

“I just cringe sometimes when I see some of the decision customers make. I have suggested to some people that what they are buying is really not the right product for their needs, I’m not selling them anything – just trying to help.”

It’s a communications issue that the security industry needs to work on, he says.

“Often the customers – the end user – don’t understand what they are being told,” he says. “One thing I have been pushing for is a common testing procedure so all the systems can be measured against each other on a level playing field. Then people can compare each system.

That’s the problem they face right now, they can’t compare one against another. All they can do is trust what the sales person tells them when they are told they won’t get nuisance alarms with the system they are being offered.

But we know the reality is that every system will give you nuisance alarms. Make no mistake about it, no system is perfect.

Customers also sit there wanting a ‘below cost solution’. They may opt for a perimeter system when in reality they need a perimeter system and cameras.”

Owen says his firm has seen some major installations that don’t feature cameras and the cost in sending out a contracted security guard to check on every false alarm has rocketed.

“Security guards get an alert that an alarm has gone off and some wonder if they should bother going to have a look,” says Owen.

“In some cases these will be contracted security guards and the client gets billed for every time a guard goes out and in some cases the police are called out as well.

“It is a false economy not to have cameras watching a perimeter. If you buy cheap then don’t expect it to be ‘prison grade’.

Too many customers have an unrealistic expectation and to win the business a lot of vendors are over promising on the products they sell.”

And it’s here where Owen says industry sales people need to take a leading hand and ensure that customer expectations are not higher than reasonably achievable.

“As an industry we need to help people understand what is possible,” he says. “We need to set realistic expectations for the customer because they can have unrealistic expectations.

And sometimes it is based on what they see on TV with shows such as CSI where a video camera zooms in from a mile away on someone’s tattoo – it just can’t be done with a \$150 camera. Even some of the brochures promoting these cameras are incredibly misleading.

What I hope to do is educate the market. Too many people are being bamboozled by what’s out there.”



# The path to interoperability.

**HID iCLASS SE**



**Open, adaptable and powerfully secure, iCLASS SE® is the platform that simplifies everything.**



iCLASS SE® is HID Global's next generation access control platform that enables authentication of a wide variety of commercial credential technologies. A highly flexible reader family along with an array of multi-technology credentials ensure interoperability in a variety of technology environments. iCLASS SE is also enabled for (NFC) mobile phones and other smart devices. Now, you can use multiple form factors to create your ideal access control solution today. **For more information on HID's iCLASS SE access control solution, visit [hidglobal.com/path-nzsec](http://hidglobal.com/path-nzsec) or contact us at +613 9809 2892 or email at [asiasales@hidglobal.com](mailto:asiasales@hidglobal.com).**

© 2012 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, iCLASS SE, Secure Identity Object, SIO and Seos are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

# Flexible CCTV management works with virtually any camera

The days of having to carefully pick and choose, and then configure cameras for a CCTV network, are over with the introduction of exacqVision

**Exacq Technologies** is a leading manufacturer of video management system (VMS) software and servers for firms serving the top end of the video surveillance industry.

The company's products are exclusively marketed in New Zealand by iTron CCTV and Automation, an Auckland-based operation with offices in Albany on the city's North Shore.

A point of difference of the ExacqVision program – which went on sale in New Zealand late last year through an officially appointed local supplier – is that virtually any popular IP camera is recognised by the software, which is available for Windows, Linux and Apple Mac systems.

The exacqVision program is among the top 10 of the VMS systems on the market globally. "Not only is it a good choice for a first installation of security cameras, but anyone who needs to change their CCTV management software can install exacqVision and obtain instant benefits with their existing cameras," says a company spokesperson.

iTron is a wholesale company and so only supplies trade customers who are offered free training by the company's staff.

"We provide free training to installers if required, and one of the team would be pleased to assist with an installation of the exacqVision system if an installer was unsure – but the system is so intuitive and easy to use that anyone who has installed an IP based CCTV set-up should have no problems," says the spokesperson.

"As a company we do support all our customers with solid backup, so no one should have any concerns with selecting an exacqVision system, installing it, or upgrading and extending it later.



"This is designed to suit medium to large installations. It is a system that wouldn't be out of place in high security places such as a bank – in fact, it is used in some banks and financial institutions to provide uncompromising security."

There are three versions of the software aimed at different markets, exacqVision Start, which runs up to 16 IP and 16 analogue cameras. ExacqVision Professional, which caters for up to 64 analogue and 128 IP cameras per server.

The exacqVision Enterprise adds multi-layer map functionality and the Enterprise Health Monitor option, which EHM manages, monitors and logs all aspects of the video surveillance server's health, including: Video loss on any analogue or IP camera, hard drive failure, system temperature alerts, loss of server connection and more.

System logs record all events. EHM is compatible with customer-supplied MySQL or MS SQL databases, or will

generate its own SQ Lite database.

"The exciting part of these Exacq software systems is that they can be infinitely scaled up, so there is no limit to the number of cameras that can be managed by it," says the spokesperson.

"It means that if a building is expanded, perhaps with an extension, or if cameras are subsequently required elsewhere on the property, then there are no headaches for the security and IT department to worry about."

As the device licences are generic, if you buy licences for 16 devices you can connect 16 devices. If a camera fails you just replace it with another. The licences are not locked to a device.

"Not only that, virtually any type of camera will be recognised by the system. That means the security manager is not tied to a particular make or model of camera – they have an almost completely free choice on what cameras they want to install," says the spokesperson.

“This is an excellent option should a camera fail – you don’t have to buy a particular camera and then work to have it recognised by the software – you just plug it in and set it up – job done.

Generally, we find in the local market people have either gone with Cardax (Gallagher) or Concept (Inner Range) for their access control solution and Exacq works with both those systems, so it is pretty flexible.”

Exacq Technologies has just released version 5.4 of its ExacqVision software, this latest version adds simplified archive drive search, a new direct driver for Samsung IP cameras, enhanced client control for panoramic/fisheye cameras and ONVIF Profile S support.

Nearly 200 new IP cameras from many of the industry’s leading manufacturers will be supported thanks to the release of version 5.4.

The release introduces a new search archive drive – that can retrieve video from both the local video server and the archive drive location seamlessly, with the results displayed as if all the video was from the same server.

Version 5.4 also adds support for nearly the entire line of Samsung IP cameras and encoders with the addition of a new Samsung IP camera direct driver.

Panoramic and fisheye cameras now have more enhanced control from within the exacqVision client. Users can now choose from three different views from most panoramic/fisheye cameras in live or recorded view in order to obtain better video evidence. The latest version of exacqVision also adds support for the new M3007 panoramic camera from Axis Communications. This camera features multi-streaming capabilities and allows users to create several live views of the camera in different view modes and resolutions simultaneously. The new release also makes it easier for customers to update their software subscription.

“With internet access enabled, exacqVision will check for available server software updates and will download the latest version based on the subscription end date,” says the spokesperson.

“Every system comes with three years of free software and firmware upgrades, and if you choose not to pay for the



license subscription at the end of the agreed term, then the system will carry on running as normal.

“It will slowly go out of date as upgrades are missed, but it will continue working. Installers and end users get total peace of mind.”

Naturally the exacqVision system can be accessed from anywhere in the world where there is internet access and user restrictions can be predefined to levels such as watching live footage only to full control of the cameras and video archive.

There’s also a range of apps for smartphones for people who need access to the system on the move.

“Users are set up in the system by the licensed owner and given a user name and password,” says the spokesperson. “Access can be managed to the nth degree – it’s a control freaks paradise.” When it comes down to the bottom line, the cost of an exacqVision installation is favourably comparable with similar systems.

“Ultimately we are selling a software license, and while we can supply all the servers and hardware required, people who already have this in place – or who want to build their own servers – then that’s fine. That is how flexible exacqVision is.

“We are not selling boxes, we are selling software that’s easy to use, flexible and reliable. The only requirement – as with any software – is that the hardware be compatible. The required hardware specifications are available for those wishing to build their own servers or buy off the shelf units.

## Three exacqVision options to choose from

### ExacqVision Start

ExacqVision Start VMS combines the ease-of-use of exacqVision with the essential features necessary for low-cost video surveillance.

It is ideal for stand-alone IP and analogue video surveillance needs. Up to 32 cameras (16 IP + 16 analogue) can be connected. Multiple users can be connected simultaneously.

The exacqVision client enables multiple-monitor and video wall operation, and is available in Windows, Mac and Linux versions.

Easy graphical search enables fast retrieval of desired video. Multi-camera playback lets you see the whole event.

POS & ATM connectivity included for easy searching and retrieval of transactional-based video.

ExacqVision is web service compatible. Users can view, search and playback video using a web browser or the exacq mobile apps for iPhone, iPad and Android.

### ExacqVision Pro

ExacqVision Pro comes pre-installed on all exacqVision A-series hybrid and IP servers, the enterprise-level Z-series hybrid and IP servers and is available on the EL-S/EL-SR hybrid and the EL-Series IP embedded appliance servers.

ExacqVision Pro VMS can also be purchased separately for installation on commercial off-the-shelf (COTS) servers running Windows or Linux.

The pro version creates an advanced security solution, providing recording of the latest, state-of-the-art IP video surveillance cameras.

### ExacqVision Enterprise Server

The Enterprise Server option, introduced with exacqVision Version 4, adds server and user administration functionality ideal for an enterprise deployment of exacqVision Pro VMS.

The option can be enabled on any exacqVision Pro-based server, whether hybrid or IP. When enabled, the following functionality is available through the exacqVision client on that server:

- Active Directory / LDAP integration
- Enterprise User Setup
- Enterprise Camera Administration
- Multi-Level Mapping
- Able to connect to optional Enterprise Health Manager module, a stand-alone client-server monitoring system for exacqVision video surveillance deployments. It monitors all exacqVision Enterprise-enabled servers and is designed for enterprise deployments where central monitoring of the status of all exacqVision servers is needed.

### Contact details:

On the web: [www.itron.co.nz](http://www.itron.co.nz)

Phone: 09 414 5101





# FLIR launches new D-Series

Multi-sensor thermal security cameras in ultra-compact networked, outdoor dome enclosures

The D-Series outdoor dome enclosure provides precision pan/tilt control while providing fully programmable scan patterns, radar slew-to-cue, and slew-to-alarm functionality. Fully enabled for control and operation over IP and serial networks, the D-series combine a thermal imaging camera with a colour CCD camera. This makes them the perfect replacement for day/night dome cameras, providing clear 24/7 imaging capability in an attractive, discrete dome-style enclosure.

The new FLIR D-Series are a lot more compact. TCP/IP compatible electronics are integrated in the camera and no longer in a separate box. This also means that the FLIR D-Series can now be mounted in ball up and ball down position, giving you more flexibility

### Choice of image quality

D-Series systems deploy a 640 x 480 or 320 x 240 pixel thermal imaging camera. To make sure that there is a D-Series for every security application FLIR Systems offers a wide variety of lenses. Longer lenses have a narrower field of view and allow you to spot intruders from further away.

Continuous E-zoom provides enhanced alarm assessment and optimization of camera field of view. Optionally available on all 640 x 480 pixel models.



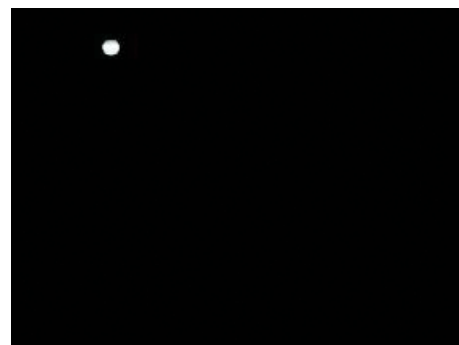
All versions are equipped with a long range daylight/low light camera. The daylight camera offers an 36x optical zoom.

### Wide dynamic range

WDR delivers high contrast thermal images in the most diverse conditions, even when the sun is in the field of view. But also in cold and low contrast thermal scenes. Ideal for working together with video analytics that need properly contrasted images in order not to generate false alarms.

### Precise Pan/Tilt mechanism

All D-Series thermal imaging cameras come with a precision pan/tilt mechanism. It allows the user to rotate the camera 360° continuously and to tilt it +20° to -90°. This drastically increases situational awareness. The Pan/Tilt has 128 pre-set positions. Ideal if you want to scan an area continuously.



*All images are used for illustration purposes only*



### IP control and ONVIF compliance

The D-Series can be integrated in any existing TCP/IP network and controlled over a PC. No additional cables are required. Using this configuration, you can monitor all activity over the network, even when you are thousands of kilometres away. The D-Series are fully ONVIF compliant.

Multiple channels of streaming digital video are available in H.264, MPEG-4, or M-JPEG formats. Simultaneous digital and composite video output is standard.

### Radar Connection – “Slew to cue”

The D-Series can be connected by the integrator to a radar system. If the radar detects an object, the D-Series will automatically turn in the right direction and give you a visual image so that you can instantly see what the blip on the radar screen really means.

### FLIR Sensors Manager

Each D-Series camera comes with a single sensor copy of FLIR Sensors Manager. This intuitive software allows users to manage and control a D-Series camera in a TCP/IP network.

## About Thermal Imaging

Thermal imaging is the use of cameras constructed with specialty sensors that “see” thermal energy emitted from an object. Thermal, or infrared energy, is light that is not visible to the human eye because its wave-length is too long to be detected. It’s the part of the electromagnetic spectrum that we perceive as heat. Infrared allows us to see what our eyes cannot.

Thermal imaging cameras produce images of invisible infrared or “heat” radiation. Based on temperature differences between objects, thermal imaging produces a clear image. In contrast with other technologies, such as light amplification, thermal imaging needs no light whatsoever to produce an image on which the smallest of details can be seen. Thermal imaging provides full visibility irrespective of the prevailing light level and weather conditions.

It can see in total darkness, in the darkest of nights, through light fog, in the far distance, through smoke and is able to detect anyone hiding in the shadows.



NEW FC-Series S



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



Compact D-Series

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

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

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

Here's how:



High contrast scene with standard AGC algorithm applied.



DDE applied – all targets can be observed simultaneously.



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



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



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



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

Your vision

Thermal image without Wide Dynamic Range (WDR).



Thermal image with Wide Dynamic Range (WDR).

[www.flir.com](http://www.flir.com)

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

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

Email: [info@flir.com.au](mailto:info@flir.com.au)

ISO No. FLIR20873 Disclaimer: Images for illustrative purposes only. Specifications subject to change without notice.

# Synology officially releases the latest Surveillance Station

More flexibility and interoperability

In May 2013 Synology® released the latest edition of their surveillance package Surveillance Station. The **Central Management System** (CMS) will be deployed to provide scalable and convenient administration for massive projects.

“This version has been released after 50 days of beta period. It has generated a lot of enthusiasm from our users. Almost 20,000 downloads were recorded which has helped us to fine-tune our Surveillance Station in order to meet users’ high standards”, declared Vic Hsu, CEO of Synology Inc.

Watching over a building, a mall, a train station, requires a tremendous amount of cameras and recording servers. It’s critical for IT managers to have a reliable, scalable and unified point of control for their architecture. CMS has been designed to specifically answer those needs.

Watching live feeds and playback recordings, intelligent video analysis, users’ privileges, cameras settings and licenses, notifications, e-maps: everything is centralized within the CMS host for efficient management. This unified administration brings many benefits.

For instance, cameras can be filtered out by different criteria, offering a quick search experience. They can also be moved seamlessly from server to server.

This latest version of Surveillance Station will be compatible with cloud cameras and more technical standards. Thanks to the newly acquired ONVIF Profile S certification, a broader range of devices can interoperate with Surveillance Station.

The Mobotix MxPEG codec, which enables high quality recording while using less computing power, is also now supported.



The compatibility list of Surveillance Station has been extended and now includes over 1,400 IP cameras from 58 brands.

Please check <http://www.synology.com/surveillance/index.php?lang=enu> for more details.

### Synology at a Glance

Synology is dedicated to providing a professional IP-based video surveillance solution, combining the functionality of advanced NVR and NAS (network attached storage). The company aims to deliver a scalable, future proof, user-friendly NVR solutions and solid customer service to satisfy the demands of businesses, individual users and our partners.

**Contact:** [marketing@synology.com](mailto:marketing@synology.com)

### Availability

**Surveillance Station is free to download. It is now available in the Package Center for DiskStation Manager.**

**Supported models are:**

- |            |  |
|------------|--|
| 13-series: | DS213j, DS213+, DS413, DS213, DS413j, DS213air, DS2413+, DS713+, DS1513+, RS10613xs+, RS3413xs+  |
| 12-series: | DS712+, DS212, DS212+, DS212j, RS212, RS812, DS1512+, DS1812+, DS3612xs, RS3412xs, RS3412RPxs, DS112j, DS112, DS412+, RS812+, RS812RP+, RS2212+, RS2212RP+, DS112+ |
| 11-series: | RS3411xs, RS3411RPxs, RS2211+, RS2211RP+, RS411, DS3611xs, DS2411+, DS1511+, DS411+II, DS411+, DS411, DS411j, DS411slim, DS211+, DS211, DS211j, DS111              |
| 10-series: | RS810+, RS810RP+, DS1010+, DS410, DS410j, DS710+, DS210+, DS210j, DS110+, DS110j   |
| 9-series:  | RS409+, RS409RP+, RS409, DS509+, DS409+, DS409, DS209+II, DS209+, DS209, DS209j, DS109+, DS109, DS409slim  |
| 8-series:  | RS408, RS408RP, DS508, DS408   |



# aptiQ™ Multi-Technology Readers

The new aptiQ™ multi-technology readers, from Ingersoll Rand, read both proximity and smart credentials, providing users with a simple migration path to increased credential security levels, including various forms of proximity, MIFARE® Classic and MIFARE DESFire™ EV1. The readers are also NFC compliant, allowing users the ability to easily migrate to mobile credentials in the future as needed.

Their eye-pleasing, wall-hugging design suits a larger variety of architectural styles and the four new colour choices complement any building's décor. These readers provide the high security of aptiQ™ technology with read range comparable to other readers on today's market.

The new aptiQ™ readers are versatile, supporting a variety of contactless credentials: 125kHz Proximity, 13.56 MHz MIFARE® Classic, Ingersoll Rand's aptiQ™ MIFARE DESFire™ EV1 smart card. The aptiQ™ readers can also read the card serial number (CSN) of most 13.56 MHz smart credentials and are able to communicate with the growing population of NFC enabled mobile phones.

The new line of aptiQ™ readers are designed to provide both integrators and end-users unique advantages over other



leaders on the market today. This is a simplified offering of readers that will meet the access control needs of virtually every application. The readers also allow end-users the ability to expand and/or upgrade credential technologies.

aptiQ™ readers are extremely easy to install, using a quick-connect wiring harness and a familiar standard wiring colour scheme. Providing a streamlined offering of fewer readers with multi-technology capability, Ingersoll Rand meets the large variety of access control product needs without a confusing number of complex choices.



## Monita joins the Customer Services Team

Customer Service team is excited to welcome Monita Dilsook on board as Customer Services Representative.

Monita's experience in Ingersoll Rand's purchasing department together with her Bachelor of Commerce majoring in Marketing and Information Systems, will be a valuable contribution to the Customer Services department.

Monita's vibrant personality and can-do attitude complements the industry leading service already given by Jo, Fati and Willie.

For more information on aptiQ or Ingersoll Rand, visit [www.ingersollrand.co.nz](http://www.ingersollrand.co.nz) or phone 0800 477 869



## Privacy Plus Lock System

Easily manage multiple access to one room with the Legge Privacy Plus Lock System

- Four functions in one controller; Standard, Secure, Air Lock and Man Trap
- Complete system in one packset
- **New** nurse call function



0800 477 869 | [www.legge.co.nz](http://www.legge.co.nz)

**IR Ingersoll Rand**  
Security Technologies

# Wireless system solves automatic gate dilemma

As it has been a while since we last heard from Simon of High Speed Gate Automation he has said he has not had time to develop any new products apart from tweaking a few existing gate automation products. But a wireless intercom which he has been working on for the last couple of years came to our attention.

One of the problems some people find with a remotely operated gate on their property is finding an intercom system that's cost-effective and will work over longer distances.

"It's something many people overlook," says Simon Withington of High Speed Gate Automation.

"When the owner arrives at their property with a buzzer they can quickly open the gate and enter, but when buying an automated gate system, many people forget their visitors will not have a buzzer and will need to let the homeowner know they are there. I have heard stories of visitors having to call the owner from their mobile to let them in."

Retro fitting a communication and gate activation system can be expensive, but Simon has been working on a wireless system that should help anyone with a remotely operated gate.

There are few systems that allow homeowners to communicate with people at the gate and open it remotely. These include a hard-wired system that may involve groundworks and the risk of the cable being damaged by future earthworks, earthquakes and water penetration.

Another option is a cellphone arrangement, but this has ongoing charges with the mobile phone provider and is not suitable for areas plagued by poor cellphone coverage. And there are short-range (50 to 100 metres) video entry systems that are not ideal for people whose gate is too far away from their home.

"Digging up a drive to lay cable can be expensive, particularly for rural properties where a drive could be hundreds of metres long," says Simon. "Also, not everyone enjoys good cellphone coverage – even some suburban areas can't rely on the mobile network for calls, so you don't want that for your security gate."

Simon, whose firm has installed hundreds of powered gate systems, says every now and then he has struggled to recommend a reliable way for the homeowner to talk with visitors waiting at the gate and open it remotely.

However, he came up with an idea while working on a recent installation that draws on old technology – namely, five watt, 99 channel, CB radios. It's low cost, has a range of 3k – up to 5k in open areas – and with some extra electronics, encryption technology and a robust custom-designed housing, can be adapted to solve one of the automatic gate industry's biggest headaches.

"There's not really a lot on the market when it comes to long range intercom systems," says Simon. "So we are adapting current technology to suit our needs by importing handheld transceivers from China. The technology is proven on the UHF long-range network, so there is no need to reinvent the wheel."

This new system fills the gap between running a long distance cable from the gate and using the cellphone network. My whole goal has been to create a long-range option that has zero ongoing costs and is cheaper to install than a cable."



Apart from allowing users to talk with each other over the wireless system, Simon has configured it to also allow the homeowner to remotely open a gate with an encrypted wireless signal (so as not to risk opening another gate within range of the 99 channel system).

"Just like any similar system, there will be a key pad in the home for people to talk with the person at the gate, and a separate button to open the gate – which uses an encrypted signal," says Simon.

Re-engineering the two-way radios hasn't been as easy as Simon assumed though. "We had radio frequency interference issues that involved sorting out some of the electronics, so we had to isolate that issue," he says. "We had to establish and configure a robust and reliable charging system for the radios' batteries, then there was the electronics for the encrypted code we needed."

We are at the advanced working prototype stage and looking for feedback from others in the industry, to take on any ideas readers may have so we can refine the product further."

On the gate-based unit Simon has adopted an externally mounted aerial that can be placed higher if required, and is using the radio's supplied aerial for the in-home transceiver unit.

He is using 316 marine grade stainless steel for the exterior housing so it can handle all weathers, and keeping the units' lithium batteries charged up is either available power or a solar panel at the gate.

Simon says potential customers simply need to weigh up the price and ongoing costs of other systems and then look at his new UHF offering to decide which one works out the best value.

His system, which is as yet un-named, is likely to be around \$1500 plus the cost of installation. It will be available by the end of the year, once the modified transceivers have been certified for use by a New Zealand EMF testing laboratory.

"Although the UHF units are shipped with a certificate of compliance, because I have added technology to them they need to be checked again," says Simon. "I have spoken with the guys at the EMF lab and they say there shouldn't be too much of a problem because the units are made to a high standard."

To find out more about this new UHF gate operation and comms system,  
email Simon at [SimonW@xtra.co.nz](mailto:SimonW@xtra.co.nz)  
or visit his website at  
[www.withingtonelectrical.co.nz](http://www.withingtonelectrical.co.nz)



# Thermal perimeter security system cuts power bills

With power prices unlikely to get any cheaper, virtual perimeter alert systems appear to be an easy way to save owners of commercial property millions of dollars in construction and annual lighting costs.

Virtual perimeter alert systems – which require much less artificial light – are increasingly being used to reduce ongoing costs without compromising safety and security.

The systems work with cameras instead of physical fences. Quick to install and maintain, they require no planning permission and stop complaints about eyesores going up around buildings and building sites.

These systems typically feature a fully integrated virtual perimeter alert system using thermal cameras for threat detection and assessment.

Systems can feature a combination of thermal security cameras, video analytics software and other intrusion detection sensors for integrating and displaying the status and feedback from all the deployed perimeter security sensors on one display.

One such system comes from Flir. Its thermal security cameras and Sensors Manager software provides automated perimeter approach surveillance, intrusion detection and alert capabilities for every perimeter security application including critical infrastructure, petro-chemical facilities, ports, prisons, commercial campuses and residential installations.

Thermal security cameras make images from heat – they can see clearly in total darkness, through smoke, dust and light fog. They allow operators to see more and see farther than any other night vision technology on the market today and even see clearly in blinding sunlight.

In its simplest form, a ‘thermal fence’ could be a single thermal security camera managed by the software application.

A Flir spokesperson says: “With these simple components, you can establish a virtual perimeter, create customized alarms and tripwires to alert you instantly to potential intrusions.

Or it can be as complex as it needs to be for a seamless, layered perimeter defence system integrating multiple thermal imaging cameras, CCTV cameras and non-video alarm sensors such as shaker fences and RFIDs on your existing IP network.”

Less expensive than installing a new physical barrier and less intrusive than expensive lighting infrastructure, thermal fences allow security professionals to boost their alarm detection and assessment capabilities along existing physical fence lines.

They can also be used to establish a virtual perimeter in areas that cannot be fenced due to economic, environmental, or logistical restrictions, and improve the security of critical zones within existing secured perimeters by creating exclusion zones and establishing concentric rings of increasingly stringent security coverage.

Flir has also introduced Raven – a free web-based tool using Google Maps that allows you to design your security application and camera layout using an online planning tool.

It can handle up to 50 cameras at a time and displays both range and location for each camera specified. Using Raven, you can choose from a complete list of all thermal imaging cameras.

It will show you the area of detection coverage, allowing you to plan which cameras you need to have installed and where.

A Raven user’s guide is available online at [www.raven.flir.com](http://www.raven.flir.com).

---

## It’s a simple equation

---

### Your team + our team = workplace success

The Skills Organisation supports New Zealand security companies to achieve industry-specific national qualifications.

Find out how we can equip your staff for workplace success by contacting us today.

**0508 SKILLS** (0508 754 557)  
or [info@skills.org.nz](mailto:info@skills.org.nz).

**skills.**

The Skills Organisation  
[skills.org.nz](http://skills.org.nz)



# Bergermeer Gas Storage Terrain monitored by Axis cameras

## Thermal cameras for management and security purposes

### Mission

TAQA Energy B.V. has been extracting gas from the North Holland Bergermeer terrain ever since the 1970s. The Bergermeer gas field is now nearly empty, but is certainly not useless as the field can now be used to store gas. The field has a porous layer of sandstone at a depth of approximately 2,500 meters. The tiny holes in the sandstone which contained gas for millions of years can be used to safely store gas once more. In order to monitor the terrain, TAQA Energy B.V. hired Spyke Security B.V. to secure the area and also make it possible for the terrain to be managed remotely. Spyke Security chose a nature-friendly solution for the area, namely camera protection - more specifically, thermal camera protection. This camera makes it possible to detect and image objects in perfect darkness as well as mist and other forms of precipitation.

### Solution

The company chose a complete Axis camera installation, including four thermal cameras and one HD camera with infrared capabilities.

This allows the company to create images of any objects detected at any time of day and under any weather conditions. The HD camera with infrared capabilities is on a swivel mount meaning it can scan in every direction using the pan and tilt functions. This camera complements the thermal cameras on site. Every camera contains intelligent software by Agent VI, which enables video content analysis (VCA).

### Result

The company is pleased with the camera security, initiated in June of 2010, on the gas storage terrain in the Bergermeer. The gas storage terrain is located in a remote section which means a continuous

stream of information using live camera images is very useful. The cameras are intended to both protect and manage the area. This means that TAQA Energy B.V. can also view the terrain where the engineers or subcontractors are currently working by entering a secure log-in code on the Internet. Spyke Security only views the area with the cameras for security purposes.

TAQA Energy B.V. is part of the Abu Dhabi National Energy Company PJSC (TAQA), an energy company that operates on a global level. TAQA's activities include detecting and producing oil and gas, generating energy and desalinating sea water. In the Netherlands, TAQA B.V. works on exploration, production and the transportation of oil and gas.

TAQA Energy B.V. additionally manages the Piek Gas Installation in Alkmaar. In the 1960s, the Netherlands



### Organization:

TAQA Energy B.V.

### Location:

Bergermeer, North  
Holland, Netherlands

### Industry segment:

Utilities

### Application:

Safety and security

### Axis partners:

Spyke Security,  
Agent VI

found gas not only in Slochteren, Groningen but also in Bergermeer. TAQA Energy is one of the parties to have extracted gas from this location and from other locations in the region. At the end of the 1990s, TAQA began storing gas in the gas field under Alkmaar. The new gas storage capability under Bergermeer will become one of Europe's largest gas storage facilities and has an initial working volume of approximately four billion meters cubed of gas.

The company chose camera security to manage this remote terrain from a distance. "This way we can monitor the terrain where needed from a distance and keep an eye on the presence of maintenance mechanics, for example. We can additionally react swiftly to unrecognized visitors. If the cameras perceive an abnormal situation, they send a signal to the Spyke Security communications center. Someone is then sent to check the situation out," says Peter van der Sman, TAQA Public Relations Manager, Energy B.V. Alkmaar Region.

The gas storage terrain is located in the middle of the polder in a pasture, which means that, due to environmental guidelines, no one may place light towers in the area. This is connected to preventing the destruction of the skyline. The company were also not allowed to fence the terrain off due to the wading birds that so often frequent this area. Fences approximately 2 meters in length could disturb the waders.

Moreover, the gas storage area is underground, whereby nothing of the gas



AXIS Q1910-E

storage area can be seen above ground level. These are the chief reasons for choosing camera security. Because Spyke Security makes frequent use of Axis cameras, they knew they could trust Axis for this project as well.

#### AXIS Q1910-E and AXIS Q1755

The company installed a total of 5 Axis network cameras. René den Dekker, director of Spyke Security, the company that manages and mans the Surveillance Headquarters and is also responsible for the system:

"This installation uses four AXIS Q1910-E Thermal Network Cameras.

They are thermal network cameras that can deliver images even in perfect darkness and over a large distance through detection based on temperature sensitivity. In addition to the thermal cameras we have supplemented with one HD camera with infrared capabilities - the AXIS Q1755 Network Camera." The thermal cameras work both during the day and at night and send a signal so the HD camera can see details of objects that occur in a certain range by using the joystick controls. These cameras are fitted with intelligent software by Agent VI, which enables video content analysis."

#### Viewing the images

The images, as well as the TAQA Energy B.V. terrain that Spyke Security B.V. monitors, are viewed in full screen format in the Boekelermeer Surveillance Headquarters. The software raises the alarm where necessary and includes an image of what provoked the alarm. Users can also call up other images using the intelligent software. The images are analyzed and suspect images are sent through to mobile surveillance, who respond in a physical sense. The images are stored for seven days so they are safely stored to act as legal evidence if needed.

*"Because the cameras provide images of the entire terrain, we do not need to physically patrol it at set times for security purposes. The same applies with regard to TAQA Energy B.V.'s management aims. We would like to offer this system to other TAQA Energy B.V. terrains, too."*

René den Dekker, Director of Spyke Security



# HID Global's EasyLobby®

## Solution Scales Enterprise-Wide Secure Visitor Management for Manufacturing Company

**N**avistar International Corporation, a \$12+ billion manufacturer of heavy-duty trucks, midsize trucks, school buses, diesel engines and replacement parts, first implemented HID Global's EasyLobby Secure Visitor Management (SVM™) software in 2001 – initially via a single EasyLobby SVM™ implementation in their Chicago corporate headquarters.

After approximately 3 years of successful deployment, Navistar's security department decided to deploy visitor management on an enterprise basis in late 2004.

### Challenges

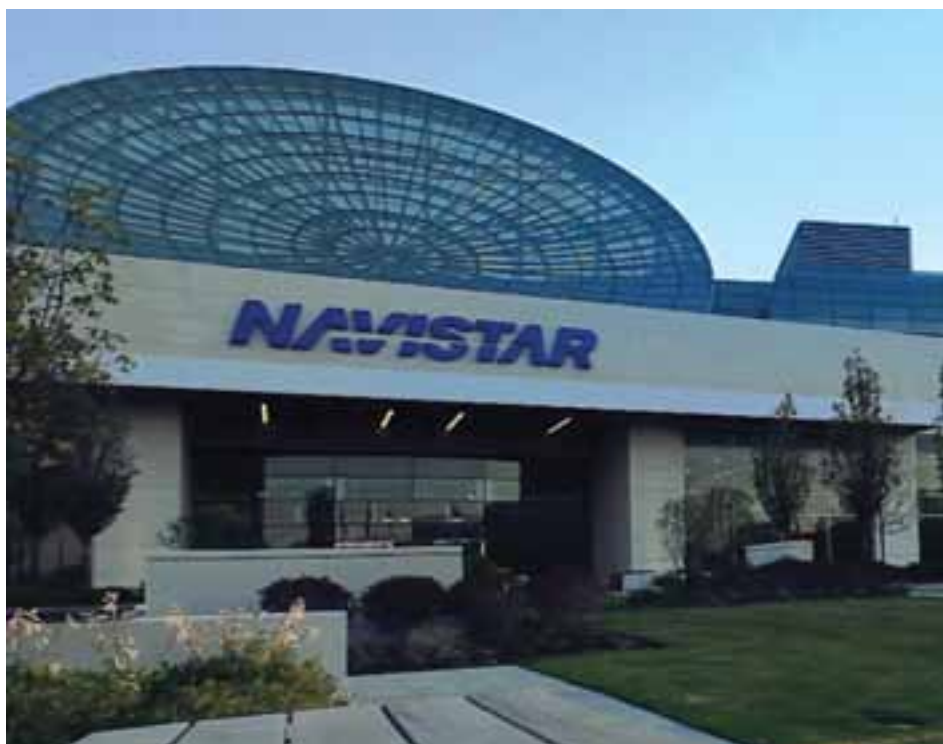
Processing an average of 12,000 visitors per month, the manufacturing facilities were particularly in need of enterprise visitor management since they lacked a standard for visitor management beyond having guards inconsistently collect drivers' licenses.

"We were using an early version of EasyLobby and decided to upgrade to the latest version and 'go enterprise' at the same time," said Michael Scribner, Security Executive with Navistar International Corporation.

### Solution

HID's EasyLobby solution helped scale enterprise-wide secure visitor management across many facilities.

"We went from being a corporate headquarters-only customer to 12 sites and manufacturing facilities in one upgrade cycle," said Scribner.



*Image courtesy of Navistar.com, used by permission*

"We went through a full competitive evaluation and chose EasyLobby because it was the easiest product to use and the company was willing to work and grow with us."

### Results

Navistar's EasyLobby implementation currently consists of 31 workstations across 20 different sites – all running off of a single EasyLobby database.

Most of the sites using EasyLobby currently have a single EasyLobby SVM license in place, although some have multiple systems in place - including a

self-service deployment at corporate headquarters. Each of Navistar's EasyLobby SVM licenses are linked to a single enterprise-wide database so that so that visitor information can be tracked and managed across the entire enterprise.

"Because we use a SQL database it's very easy for us to set up a new site," said Scribner. "We can quickly get updates enterprise-wide. We track and report on daily and monthly visitors, check-in and check-out times and other information our enterprise needs to more effectively manage our visitors and our security."



# What is in your security platform's DNA?



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

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

**See what you need at [genetec.com/SecurityCenter](http://genetec.com/SecurityCenter)**

Video Surveillance | Access Control | Automatic Number-Plate Recognition

For more information

**Panasonic ideas for life**

[www.panasonic.co.nz](http://www.panasonic.co.nz)

Innovative Solutions

**Genetec**

# SUBSCRIBE NOW

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

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

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

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

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

or email your contact and postal details to:  
[craig@newzealandsecurity.co.nz](mailto:craig@newzealandsecurity.co.nz)

First Name \_\_\_\_\_

Surname \_\_\_\_\_

Title \_\_\_\_\_

Company \_\_\_\_\_

Postal Address \_\_\_\_\_

\_\_\_\_\_ Post Code \_\_\_\_\_

Telephone \_\_\_\_\_

Email \_\_\_\_\_

Date \_\_\_\_\_

Signed \_\_\_\_\_

**nzSecurity** Magazine  
A trusted source of information for industry professionals

*“We went from being a corporate headquarters only customer to 12 sites and manufacturing facilities in one upgrade cycle.”*

*Michael Scribner Security Executive Navistar International Corporation*

For the company's field locations, it is critical to know who is in what building and at what time.

“We knew which employees were where and when, but we didn't have much information about visitors and couldn't go back in time to figure it out,” said Scribner. “When we finished our EasyLobby enterprise-wide deployment our upper management was shocked to learn that we have more than 140,000 visitors per year – and are approaching visitor number 500,000 to be badged by EasyLobby.”

Navistar uses EasyLobby SVM's watch list feature extensively to flag former employees and vendors, a feature which has been particularly useful for managing visits by former employees with sensitive jobs. EasyLobby has also been used for investigative projects due to its ability to track and manage visitor data across the enterprise.

EasyLobby's solution has provided straightforward ROI to the company's visitor management process. The company processes 12,000+ visitors per month and knows who and where the visitors are at any given time.

“Our premises are safer and because our people feel safer, they are more productive,” said Scribner. “We actually set up a contest for our security guards to see who could become most proficient at checking visitors in via EasyLobby – it was a great way to get our people proficient, and resulted in some true productivity gains, not to mention enhancing our security.”

## Future Plans

As Navistar continues to expand their presence worldwide, they have committed to using EasyLobby in their future visitor management deployments.

“We are planning to roll out our deployment to our international facilities – we are already using EasyLobby in Canada as well as the Spanish version of EasyLobby in Mexico,” said Scribner. “We plan to expand our use of EasyLobby in South America, Europe, Asia and other regions in the near future.”

Over time, Navistar plans on utilizing new features of EasyLobby SVM including web-based capabilities, such as eAdvance™ pre-registration.

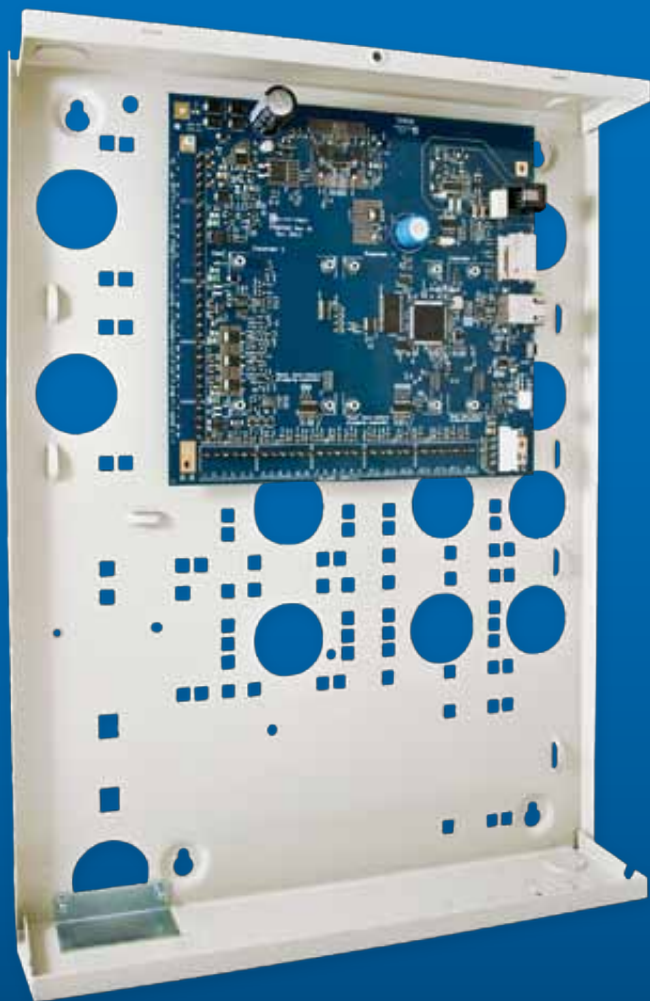


For more information on HID's products and services within New Zealand, please contact Stephen Blakey on 09 537 0279 or 0210 824 6096 email: [sblakey@hidglobal.com](mailto:sblakey@hidglobal.com)

## Challenger10™. Now available.

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

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



**Fully compatible** with Challenger V8 peripheral hardware

**Superior scale** to meet the ever-increasing security demands of modern systems

**Industry-leading connectivity options** with IP, USB, RS-232 and dialler as standard. Simultaneously communicate with up to 10 monitoring stations and software packages

**Multiple holiday types** can be configured to span multiple days and repeat on an annual basis

**Efficient switch-mode power supply** with advanced diagnostic capability and resettable fuses

**Link multiple internal areas to a perimeter area** to control your site's entry/exit procedures

**Flash upgradable firmware**

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



## New Zealand Security Conference & Exhibition 2013

**T**he New Zealand Security Conference 2013 is to be held at the Rendezvous Hotel, Auckland on 28th & 29th of August. A two day security exhibition will be held alongside the conference. The event is staged by the New Zealand Security Association in association with ASIS.

The conference is the single largest gathering of security professionals in New Zealand, attracting around 200 delegates from over 140 security organisations and hundreds of visitors to the exhibition.

In addition to this the NZSA will be advertising the event on national radio with thousands of commercials airing



*A great time was had by all at last year's Conference Awards Dinner*

### Key Note Speakers



**Bob Forsyth MloD MSyl**  
**Managing Director**  
**MITIE Total Security Management (TSM)**

Bob will discuss his vision of the future of the industry; the way it will evolve in the coming years; and the way regulation and training needs to be upgraded to recognise the emergence of new technologies. Bob wants to see the security sector become a career of choice, one that people choose rather than is a last resort. He will highlight the way the UK Security market has evolved, to show ways in which the market in NZ may change in areas such as, the emergence of Facilities Management companies and the way the market has changed in its buying from longer silo selling to basing everything on a Risk agenda.



**Jim Della-Giacoma**  
**Giacoma (Australia/Indonesia)**  
**International Crisis Group**

What might appear to be obscure conflicts in a distant country often can have the potential to have a dramatic impact way beyond their borders. New Zealand is not only linked to the countries of the region by trade but also terror.

It citizens were killed by the Bali bombers, business disrupted by the Red vs. Yellow conflicts on the streets of Bangkok and investments in places like regional Indonesia are often vulnerable to the violent dynamics of local politics. If war were to take place on the Korean Peninsula or clashes result in the South China Sea, the impact would be amplified as old alliances invoked and New Zealand not spared any adverse consequences.



**Mark Piper**  
**Senior Security Consultant**  
**Insomnia Security**

Advanced Persistent Threats are a focused form of cybercrime, particularly aimed at business and political targets. There is definite intent behind the actions of APTs and the crime typically occurs over a prolonged period of time.

- What is an APT and how might it breach your organisation?
- Mitigating and safeguarding against APT.
- Responding to an APT incident.

Mr Piper is a Senior Security Consultant for Insomnia Security where he specialises in enterprise web application security, having worked in the New Zealand security consulting for over ten years.

to a total audience of over 1.4 million listeners, which is expected to increase visitor numbers significantly, providing companies with an excellent platform to promote their products and services.

The conference & exhibition will provide information on the latest trends relevant to the security industry and a forum to build networks of security practitioners by interaction with hundreds of executives and decision makers from general industry.

The conference and exhibition will appeal to a wide range of security industry and associated organisations. These include, but are not limited to:

- Security Managers
- Government Security Advisors
- Security Consultants
- Security Trainers
- Risk Managers
- Facility Managers
- Private Investigators
- Security Systems Providers and Installers
- Police
- Insurance Companies
- IT and Intelligence Professionals
- Emergency Managers
- Business Continuity Consultants
- Fire Protection
- Senior Managers from General Industry

### Exhibition Opportunities

A wide range of stands are available to the industry and interested parties, (see graph opposite).

### Sponsorship Opportunities

Sponsorship opportunities, for the Security Conference 2013, offer a unique and highly valuable opportunity to target security professionals from business and government, they include:

#### Cocktail Reception Sponsor

The Cocktail evening will commence immediately after the last session of the first day. It will run for two hours and will be held inside the exhibition where guests will be able to view the exhibits.

#### Lunch Sponsors

This is an opportunity for sponsors to participate in one of the two lunches.

#### Awards Dinner Sponsor

The Security Industry Awards Dinner is a special and popular event, with many of the industry's leaders attending.

**For more information, please contact:**

**Greg:** greg@security.org.nz  
**Lucy:** lucy@security.org.nz  
[www.security.org.nz](http://www.security.org.nz)

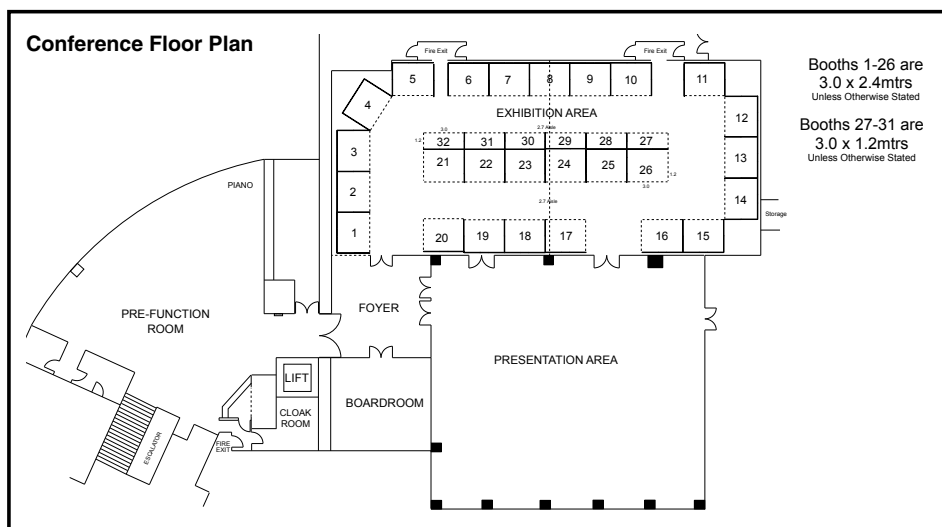
**Phone:** 09 486 0441  
**PO Box 33 936, Takapuna, North Shore City 0740**

#### Session Sponsor

This is an opportunity for sponsors to participate in the proceedings of one of the sessions. If you wish you can introduce the speaker.

#### Keynote Speaker Sponsor

This is an opportunity for sponsors to participate in the proceedings by sponsoring one of the Keynote speakers. If you wish you can introduce the speaker.



**Steve Dixon**  
**VP, Customer Experience & Operations**  
**Vivint (US)**

If a trusted friend or associate asks you, 'In the last year, what company has provided you with the level of service and positive customer experience that makes you want to tell all your friends?' does any particular name come to mind?

It is (or should be) the goal...even aspiration...of every company to be the one that customers recognize as providing outstanding service.

In this session, Steve Dixon, VP of Customer Experience and Operations with Vivint, one of the world's largest home automation and home security companies, will share his insights on what it takes to provide customers with such a high level of service that it will make them want to tell all their friends and associates.



**Victor A Vella**  
**FEDERAL Business Development Manager**  
**Panasonic Systems Communications Company of North America**  
**Director, Antiterrorism Services Program (RET)**  
**US Dept of Defense (NAVFAC ESC)**

How do you kill an ideology? With the increase in terrorist activities targeting innocent citizens it is imperative that governing agencies and private companies provide effective security protection for facilities and their people against terrorist threats. This session explains the ideologies, modus operandi, and tactics used by transnational and domestic terrorists. Attendees will develop an understanding of why and how terrorism continues to occur and what indicators to look for that may illustrate an imminent attack.



**Dr Warren Tucker**  
**Director of the New Zealand Security Intelligence Service NZSIS**

Warren is a founding member and Patron of the New Zealand Institute of Intelligence Professionals (NZIIP) and is Chair of the Strategic Advisory Board, Centre for Defence and Security Studies, Massey University.

On 1 July 1996 he was appointed Intelligence Coordinator in the Department of the Prime Minister and Cabinet. Warren was appointed Director of the GCSB with effect 13 December 1999. From November 2000 until December 2010 he was Colonel Commandant of the Royal New Zealand Corps of Signals (with the rank of Honorary Colonel). He took up the position as Director of Security, New Zealand Security Intelligence Service on 1 November 2006.

# Bosch Video Management System v.4

The Bosch Video Management System is a unique enterprise IP video security solution that provides seamless management of digital video, audio, and data across any IP network. It is designed to work with Bosch CCTV products as part of a total video security management system. You can integrate your existing components into one easy-to-manage system, or use our full-line capabilities and benefit from a complete security solution based on cutting-edge technology and years of experience.

The Bosch Video Management System allows a very flexible system design:

- Compact: Single Site System 1 to 2000 cameras out of the box. Only this system supports BIS-BVMS connectivity.
- Enterprise: Multi Site-Single Customer. Up to 10,000 cameras. Supporting multi-site requirements for Metro, Airport and other large industrial facilities. Consisting of individually configured servers Combined monitoring in Operator Client.
- Enterprise: Multi Site-Multi Customer. Up to 10,000 cameras. Up to 10 individually configured subsystems. Enabled for legally different companies

- ◆ **Enterprise-class Client/Server based video management system.**
- ◆ **Superior alarm handling with alarm priorities and selectable user group distribution.**
- ◆ **Mobile video client for live and playback.**
- ◆ **Edge based intelligent Video Analytics (IVA) and forensic search.**
- ◆ **Support of 3rd party cameras that are compliant to ONVIF Profile S.**



The Bosch Video Management System is installed on a Microsoft Windows

## Operating System.

We recommend using Bosch Workstations and Servers. They are fully tested and optimized for Bosch Video Management System. In addition to the Bosch ST standard terms and conditions of sale, the Bosch Video Management System Software is a great option to benefit from the Bosch maintenance service, keeping your VMS always up-to-date. It can be found in your online CCTV product catalog.

## System overview

The Bosch Video Management System contains the following software components:

- Management Server software provides management, monitoring, and control of the entire system.
- Enterprise Management Server provides access to multiple Management Server computers.
- Video Recording Manager (VRM) provides recording and playback management of video, audio and data.
- Configuration Client software provides the user interface for system configuration and management.
- Operator Client software provides the user interface for system monitoring and operation.

- Mobile Video Service, Mobile Client.
- Video Streaming Gateway.

These software components can be run together on a single PC for small systems or on separate PCs and servers for large systems.

Bosch Video Recording Manager (VRM) provides a Distributed Network Video Recorder solution, eliminating the need for dedicated NVRs. The VRM provides load balancing and failover for the iSCSI storage and makes it easy to add additional iSCSI storage later on. VRM introduces the concept of a storage virtualization layer. This abstraction layer enables VRM to manage all of the individual disk arrays in the entire system as a single “virtual” common pool of storage, which is intelligently allocated as needed. The usage of multiple client workstations offers great scalability.

The Bosch VMS manages 2000 IP cameras / encoders per Management Server (up to 10,000 in Enterprise Systems). A Bosch VMS supports 100 workstations.



**BOSCH**  
Invented for life



## Deployment

- Updates of Operator Client and Configuration Client automatically deployed from Management Server.
- Supports all Bosch MPEG4 & H.264 encoders, MPEG4 & H.264 IP cameras and IP AutoDome cameras in SD & HD format, decoders, Allegiant, DiBos, Bosch POS/ATM Bridge, and DiBos-compatible ATM Bridge.
- Supported HD resolutions: 720p and 1080p.

## Configuration

- Enterprise System: Operator Client can access up to 10 Management Servers simultaneously.
- Support of 3rd party cameras that are compliant to ONVIF Profile S.
- Intelligent Video Analysis (IVA) and Forensic Search without servers.
- Connectivity to mobile clients (iPad and iPhone, App available in AppStore).
- Automatic scan of IP devices
- Automatic IP address assignment of IP devices.
- Batch firmware updates of IP devices.
- Configurable Logical Tree.
- Pre-configured camera sequences with 25 cameras with each up to 100 steps with individual dwell times.
- "Automatic Sequences" created by multiple selection and drag and drop to Image panes.
- 4 configurable user-events (can be triggered via menu command).

## User Interface

- Zoomable sitemaps with links, devices, sequences, and Command Scripts.
- Automatic map positioning of a camera in a map when this camera is selected.
- Sitemaps in DWF format are used. DWF format version 5.0 and 6.0 are supported.
- Up to 4 PC monitors supported per Workstation.
- CCTV keyboard support, connected to either Workstation or IP decoder CCTV keyboard support the Enterprise System (select the desired Management Server).
- Flexible Image panes allow any combination of video window sizes and layouts.
- Any live Image pane can be switched to instant playback.
- Multiple instant playback Image panes.
- Image windows can display live video, instant playback video, text documents, maps, or web pages.
- Device states shown by icons, including networkconnection loss, video loss and camera deadadjustment.
- Favorites tree can be individually configured per user.
- Favorites tree can include complete views with Image pane layouts and camera assignments.
- Bookmarks in Live and Playback Mode for easy investigation and export of recordings. Selected clips can be exported to DVD, network drives, or USB sticks with a few mouse clicks.
- Camera selection by double-click or drag and drop from site maps, Logical Tree, or Favorites Tree.

- Decoders can be organized in Monitor Walls from within Operator Client.
- Monitor Walls can be controlled without connection to Management Server.
- Control of analog monitors connected to decoders via drag and drop.
- Sophisticated multi-camera timeline allows easy, graphical searching of stored video.
- Timeline colors indicate recording status – normal recording, alarm recording, motion recording, protected recording, and audio recording (not for cameras managed by a VRM).
- Easy clip selection by dragging hairlines in the timeline.
- Flexible search works across all DVRs connected to the system.
- Post-recording motion search allows easy locating of changes in selected areas.
- Forensic Search allows the usage of Intelligent Video Analysis (IVA) algorithms on the recorded video.
- Two audio listening options – selected channel only, or multiple simultaneous channels.
- Audio Intercom functionality.
- 4:3 and 16:9 Image panes.
- Continuous Operation for live, playback and export while Management Server disconnected.
- Live and Playback of the following recording engines: Video Recording Manager, Local Storage, DirectiSCSI-Recording, Bosch Recording Station, Video Streaming Gateway. For legacy purposes the following recording engines are supported: NVR, DiBos, Vidos NVR.

## Scheduling

- Up to 10 Recording schedules with Holidays and Exception Days.
- Task Schedules with Holidays, Exception Days, and recurring schedule support.
- Per camera settings for minimum and maximum recording times.
- Per camera, per recording schedule frame rate and quality settings for live, normal recording, motion recording, and alarm recording.

## Event Handling

- Compound events (combining events with Boolean logic).
- Event duplication allowing separate handling.
- Event allocation to user groups.
- Schedule dependent event logging.
- Schedule dependent event-generated Command Script invocation.

## Alarm Handling

- Schedule dependent alarm generation.
- Alarms can trigger alarm-mode recording for any cameras.
- 100 alarm priorities.
- Selective auto-popup on alarm.
- Alarms displayed in separate alarm window.
- Up to 5 Image panes per alarm with live or playback video, sitemaps, documents, or web pages displayed in an 'alarm row', with highest priority alarms on top.
- Audio file per alarm.

- Workflow with user instructions and user comments, optionally forced before clearing.
- Email or SMS notification on alarm.
- Alarm display on Monitor Wall.
- Alarm auto clear options either time or state dependent.

## User Management

- LDAP compatible for integration with user management systems such as Microsoft Active Directory.
- Access to system resources individually controlled per user group.
- Logical Tree customized per user group – users only see devices for which they have access.
- User group rights for protecting, deleting, exporting and printing video.
- User group rights for Logbook access.
- User group priority assignment for PTZ control and Allegiant camera access.
- Individual per-camera privileges assignable per user group for live access, playback, audio, meta data display, dome control.
- Dual-authorization logon – special privileges and priorities granted when two users log on together System Monitoring.
- System-wide health monitoring, including Bosch cameras, computers, software and network equipment.
- Network equipment and other third-party devices monitored with SNMP.

## Customization and Interfacing

- CameoSDK for easy integration into 3rd party Physical Security Information Management (PSIM) and other Management Systems.
- RemoteClient Enterprise SDK for system integrators wanting to interface a running Bosch VMS Operator Client.
- Custom Command Scripts can control all system functionality.
- Built in Command Script editor supporting C# and Visual Basic .Net.
- External software can trigger events and send metadata via 'Virtual Inputs'.
- Any .Net programming language (C#, JScript, etc.) or COM programming language (C++, Visual Basic, etc.) can be used to interface Bosch VMS functionalities.
- Other systems can control a virtual matrix with Allegiant CCL commands that can be sent via RS232.
- Compatible with Bosch Building Integration System.
- Compatible with Advantech.

**ZoneTechnology**  
Your Security Supply Partner

**Auckland:** (09) 415 1500  
**Wellington:** (04) 803 3110  
**Christchurch:** (03) 365 1050

**Email:**  
sales@zonetechnology.co.nz

**Website:**  
www.zonetechnology.co.nz

# Quietly Securing Futures

**A**ndrew Dalton, Security Business Development Manager at Tru-Test Group tells Craig Flint about a New Zealand manufacturer who has spent the last 20 years quietly building a world class reputation for their security electric fence systems.

Since acquiring iconic electric fencing brands Speedrite and Stafix in the 90's, New Zealand owned and based manufacturer Tru-Test Group has been solidly working at growing its footprint and reputation in the security industry globally.

In New Zealand the core demand for security electric fence systems is still largely driven by ensuring the safety and security of people, protection of assets and the meeting of health and safety requirements. The physical fence barrier combined with the psychological and actual deterrent of a safe yet short, sharp electric shock remains highly effective. While wall-top and roof-top electric fence installations are common in international markets, in New Zealand security electric fencing is usually implemented through full height fences.

### The principle behind security electric fencing

In a security electric fence system, an energiser unit sends out pulses of energy to an electric fence every 1.5 seconds. The fence voltage drops if anything or anyone touches or breaks the electric fence wires. It is this drop in voltage which is used to raise a fence alarm.

### Solid, reliable performance

Tru-Test Group's Stafix and Speedrite security products are designed and manufactured at their New Zealand plant to deliver consistent product quality and performance. The energisers are certified to global IEC standards. Their electric security fence accessories are UV resistant and highly durable.

Configuration through a keypad makes the system easy to use and maintain. User roles and privileges managed via Personal Identification Numbers (PINs) helps to maintain the integrity of the system set-up and operation.







A range of definable and optional features provide the ability for installers to fine tune the system according to the customer's needs. For example, Low Voltage Monitoring enables the system to raise an alarm without the high voltage shock – a desirable feature for applications and times where the public may legitimately visit the site. Further examples are Configurable Entry and Exit Delays. These enable authorised people to enter/exit the site through monitored gates without raising an alarm.

#### **Park 'n' Ride**

In New Zealand, Tru-Test Group has established a network of experienced installers. Flexible in their approach, they are able to work with installers to provide the best solution for customers. An example is the security electric fence system installed at the Park 'n' Ride facility at Auckland International Airport.



Stafix Installer Colin Trafford of Livewire Security was commissioned by Ross Reid Construction to supply an electric security fencing solution for client Auckland Airport who was building a substantial Park 'n' Ride facility located on Verissimo Drive. The facility required approximately 1.3 km of fence to be installed and because the public had access to the inside of the facility, needed to be easily switched between high and low voltage to protect the public's safety. Tru-Test Group's Security Business Development Manager, Andrew Dalton worked closely with Colin to review the specification and develop a secure solution to meet the specific requirements of the site.

The site is divided into camera monitored zones which enables Kiosk and Airport security staff to immediately assess and respond to any changes in voltage on the fence. Central control via a keypad also enables the quick change from high to low voltage when required. The Stafix energisers were strategically located with other site infrastructure and contained within watertight stainless steel enclosures.

#### **Observations**

Colin has been in the electric security fencing industry for many years and has seen a number of developments. Most notable is the ongoing drive to make electric security fences stronger in order to keep pace with development in 'criminal smarts'. Changes have included increasing numbers of security electric intermediate fence posts and earth wires for increased strength and faster detection of attempts to breach fences. The addition of springs to fence construction has increased fence longevity through maintaining tension on the fence and for more rapid detection of fence climbing. Eliminating barbed wire fence tops has also proven to reduce fence shorts and eliminate a potential weak point at the perimeter.

#### **More Information**

Security electric fence requirements can vary significantly. If you would like to know more about Tru-Test Group's security electric fence capabilities, or to enquire about joining Tru-Test Group's installer network, contact Andrew on 021 966 148 or email him at [andrew.dalton@trutest.co.nz](mailto:andrew.dalton@trutest.co.nz). Andrew has more than 21 years experience in electric fencing through Stafix and Tru-Test Group.

#### **About Tru-Test Group**

Tru-Test Group has been able to leverage its expertise in electric fencing in both the agricultural and security markets. While applications may be different, the same core values of strength, straight-talking and reliability apply. Tru-Test Group is considered a leader of electric fence systems globally.

Tru-Test Group's security electric fence systems have been installed to manage wall top, roof top and full height electric fences in residential, commercial, industrial and infrastructure markets. The systems are sold through an established network of regional distribution partners and installers and are successfully securing thousands of sites. Key markets currently include Africa, Asia, Australia, Latin America and New Zealand.

The Group has invested heavily in Lean manufacturing principles and systems whilst developing its R&D capabilities to continue to deliver world class solutions. In 2012, the company was recognised as one of New Zealand's 'Top 10 companies to watch' (as rated by the TIN Network, a Technology Investment Network that aims to help facilitate the growth of the technology sector in New Zealand). In 2013, the company featured again, at number two on the list, reflecting its strong growth.



# Security is an Art

For a number of years now Locksmiths have had to cope with pressure from electronic security techs, computer nerds, security consultants and the like about locks being insecure. Therefore locksmiths should tell all the secrets of locks and make them available to the public.

The reality is that while they have many plausible arguments they really are just desperate to show off. They want some of the Locksmiths mystique where we do the impossible now, while the difficult takes a little longer. They want to show off how weak the locks must be because they can break in . . . "See, I can do it too !" But of course it is all done in the name of security. Interesting that although the locks are supposedly weak, these "professionals" can't bypass them without further training – formal or otherwise.

Now you have the introduction of the new generation of credit cards such as Pay Pass where you only have to wave the card at the reader to complete the financial transaction. It is SO SECURE that the banks have limited the transactions to a

whole \$80. Obviously their boffins know better than their salesmen that this system is inherently insecure. One of the claims is how short the range is between a reader and a card. Therefore they cannot possibly read the other cards in your pocket. Clearly they are totally forgetting the effects of multiple radio signals from different sources. Access control specialists quickly have to learn about these issues or face the consequences.

Or maybe you are thinking about all the modern cars that are suddenly being stolen. BMW owners are currently in an uproar because of the ease with which the modern generation of cars are being stolen. They are promoting the argument that the information about the security system should not be made available to anyone else. It should be kept secret.

Vehicle manufacturers are arguing that they should not have to make the information about their cars available to others. Carefully forgetting that if the information was limited to this extent then there would be more burglaries of OEM programming equipment. But it would at least assist the profitability of the automotive industry in these times of financial crisis.

Computer nerds are busily claiming that this just proves the systems are inherently insecure. You need to add security steps like "3 strikes and you are out". It must be fun to live in the land of fantasy. They clearly have never had to get out of the world of cyberspace into the real world where you and I live. For instance imagine parking your car in one of these giant shopping malls which can have anything up to 5000 cars. Nearly all of these vehicles will have some kind of proximity or remote control device. Probably in the course of a day the client turnover will be close on once per hour so in the course of a single day it would be real easy to get over 50,000 signals of which only ONE is correct for your car. So if we have 3 wrong tries before you are locked out . . . where do you think you are going? NOWHERE FAST! We already have many instances of people having to push their car down the street to

get it to a position that they can use their electronic key to start the vehicle.

Or alternatively imagine the number of clients New Zealand locksmiths see EVERY day who have either lost their keys, cards or fobs or alternatively had them stolen.

Already there are many instances where going to the dealer will cost you over \$5000 because the manufacturer says it has to be done by replacing the vehicle's computer. Whereas our boffins may tell us to spend \$5000 on this XYZ equipment and service this model of vehicle for \$500 per time. In most cases this will also enable same day or following day solutions rather than importing expensive gear from the other side of the world.

For those of you who haven't learnt it yet... *Security is the art of ignorance* because once you know, it is no longer secure.

Computer nerds are inclined to talk about adding another layer of security. They are assuming the level of ignorance of those who will attempt to crack their system. In most cases this is a realistic interpretation. But when the demand rises, those of us doing it legally, or the "boys on the night shift" just step up to a new level of abilities. Each step of difficulty is only secure because those attempting to bypass it are still in a state of ignorance.

Electronic systems are extremely convenient but don't be fooled into thinking that they are necessarily more secure, because often they are not. A security system needs to be comprised of multiple different technologies and systems to get the best because the more different skills a criminal needs to apply, the greater will be his likelihood of ignorance.

Consult a Master locksmith as to what may be the best locks for your situation. Don't try to survive by just reading the salesman's latest literature, because then YOU are operating out of a position of ignorance. The choice needs to match the risks that apply to your situation. It is unlikely that we need to provide you with the same grade of locks that may be required by the SIS or CIA.



Fraser Burns is a member of the New Zealand Branch of the Master Locksmiths Association of Australasia Ltd  
Email [safe@safemasters.co.nz](mailto:safe@safemasters.co.nz)

Contact:  
Master Locksmiths Association of Australasia Ltd  
Web: [www.masterlocksmiths.com.au](http://www.masterlocksmiths.com.au)  
Email: [national@masterlocksmiths.com.au](mailto:national@masterlocksmiths.com.au)  
Ph: 0800 652 269

# Is a career choice in security 'Just the Job?'

**I**s a career choice in security 'Just the Job?' Yes it is, if the recent filming of a TV programme named Just the Job led by The Skills Organisation is anything to go by. Just the Job, featuring Edward Tataurangi, a senior student from Wanganui City College was captured by the film crew as he got to experience a day and night in the life of a security guard.

Edward was given an introduction to the role of a security guard by Mark Simmonds, owner of Wanganui Security.

The introduction included the legal requirement of a security guard to be licensed, the training requirements, code of conduct, responsibilities and keeping safe on the job.

Edward got to observe guard work first hand as the guard team at Wanganui Security carried out a normal 'day at the office'. The first job was alongside the guards checking and kennelling greyhounds prior to racing, escorting dogs to the track and starting the race. Not the usual security job but one that Wanganui Security has expertly carried out for Wanganui and Manawatu Greyhound Racing for several years. Edward found out greyhounds are one of the easiest clients to satisfy with a kind word and a pat on the head.



NZSA Chairperson Bronwyn Paul



Edward then headed to the Mall where security is employed to assist keeping shoppers safe, lead fire drills, manage unruly behaviour and minimise shop lifting. Here Edward had orientation by security guard Alister who has been with Wanganui Security since 2006. Alister believes his role as a security guard fits perfectly with his long involvement in the NZ Army Reserves Territorial Force, where Wanganui Security has supported him to attend training. In return the Army training equips Alister to bring valuable and unique skills to his security position believing security is equally good grounding for guards gaining experience towards other careers such as the Defence, Fire or Police services.

Security is a 24/7 job and Edward quickly learnt this by riding with the night patrol guard, Mike. Mike explained premises, car yards and gates needed lock downs early in the evening to ensure client premises are secure. The rest of the night the film crew filmed Mike and Edward as they performed security checks at premises and attend alarm response dispatch. Mike trained to Level 3, reinforced to Edward the value of good and ongoing training that has helped him to better understand the law, his

responsibilities, how to manage shift work and how to communicate with people from all walks of life.

Bronwyn Paul, Chair for New Zealand Security Association applauded the initiative by The Skills Organisation to highlight security as a career path for young people. Bronwyn says "the security industry involves more than guarding. There is a whole range of roles within the industry for young people to consider. For instance training as a security technician or monitoring control room operator. Within the guard sector there is a variety of work to keep young people interested." With an industry and Government mandate to encourage more young people into trades and training the time is right for entry into the industry.

NZSA and The Skills Organisation are working closely together to ensure entrants to the industry have the appropriate training available. As the Ministry of Justice legislation comes into effect later this year, training will become a mandatory requirement not only for new entrants to security but also to those who are currently licensed and working within the industry to attain a minimum level of formal training.

The security segment of Just the Job goes to air on June 22nd on TV2.

## Case referrals to Police from Private Investigators

**P**private investigators are often required to submit complaints to Police on behalf of their clients and it makes sense that the better the referral the more likely the Police will take action.

In this role the private investigator is a third party and not the complainant proper and more often than not the complaint to Police is made after the fact.

In some cases though the investigation is live and the private investigator is seeking to work with Police to obtain a search warrant such as following stolen funds in a fraud or internal theft matter.

In the past there have been a few cases where a search warrant obtained resulting from a private investigators complaint have been challenged and other cases where the evidence provided to Police in the private investigators complaint just did not stack up.

As a result, in 2008 NZIPI were part of a panel with interested stakeholders that resulted in a Local Police Order for the Auckland District which set

guidelines and policy where complaints had to be submitted to a set format, meet certain criteria and be of acceptable evidential standards.

In return the Police undertook to keep the investigator updated and to assist as soon as possible, resources accepted.

Now five years on the Police are finalising revised Policy and Guideline Notes that will see the previous trial spread nationwide.

This new policy and guidelines cover not just private investigators but other similar groups who might wish to lay a complaint in their capacity as third parties as opposed to a complainant fronting at a Police Office.

Again, NZIPI were invited to provide input into the content and format that these referrals might take and we are currently working with Police on the final draft. Since the 2008 trial, members of NZIPI have enjoyed sharing the template and guidelines ensuring our members produce a consistent high quality file to Police.

In my six years as Chairman I have yet to be formally advised of an inferior complaint to Police by a member of NZIPI, a true reflection on the NZIPI high standards and our member's commitment to our Code of Ethics.

Clients who instruct members of NZIPI can be assured they are dealing with a true professional, vetted by and who is able to draw on the combined strength of their peers, individuals who put the fight against commercial crime before their own egos.

When this system was first raised, a few quarters claimed it might be seen as a form of queue jumping by a select few.

The reality is the opposite. Virtually all our members are former Police and appreciate the demands on an officer's time and the value of receiving a well-documented file supported by facts and not supposition.

We also appreciate and accept that every complaint is handled in accordance with available police resources and without favour.



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](mailto:Ron.McQuilter@paragonnz.com)

### Not all fraudsters are rocket scientists

#### Two quick stories that I found amusing

1. *A scam email received 21 May from a person claiming to be a Caribbean bank "Investment Advisor" offering the usual cash 50% of US\$76m. The advisor said he had worked as a discretionary advisor with "Ernest and Young" prior to joining the bank.*
2. *A man about to be sentenced in the USA for \$1.8m social welfare scam told the judge he did it because he needed the money to feed his kids. The Judge replied "What did you think when you were driving your new Bentley?"*



# Crime & Punishment

(Title borrowed from the Russian author Fyodor Dostoyevsky)

**F**or four decades now I have been dealing with crime and punishment, mainly in the area of detecting, investigating and seeking some form of punishment or determination for criminal acts. I have watched the justice system deal with the results of my investigations and witnessed first-hand the effects the various crimes have had on their victims.

Having hopefully qualified myself to speak, or at least contextualised my perspective, I want to say that I do not believe that the way we deal with crime and punishment is the best way forward. I don't think I will get much of an argument from anyone by saying that our current methodology is not very successful from a deterrent and recidivism perspective. However, criticising without suggesting alternatives is not very constructive, so here is my viewpoint.

To begin we need to examine the fundamental elements of crime and punishment. Crime equates to a breach of rules or laws and punishment is an authoritative imposition of something negative on a person in response to behaviour deemed unacceptable. The reason we have rules or laws is for human guidance, to help shape society positively and as a social mediator. Why do we do that; because we need a stable platform or environment within which each member of our society can grow and develop as an individual and ultimately make a positive contribution towards humanity.

Accepting for a moment that these simplistic definitions are fundamentally correct, then crime and punishment is about modelling human behaviour towards its more acceptable and positive forms.

So if it is all about encouraging positive behaviour then we need to examine the best process for achieving that. That brings forward the argument of the carrot or the stick, and I think that we have proven

over the last few hundred years that the stick methodology isn't working so well. How do you encourage positivity by using negativity? (Rhetorical question).

Our processes should be designed to achieve our aims. If our aim is to shape and encourage positive human behaviour and development, our processes should be focussed heavily on that outcome. I suspect that currently we have become so focussed on satisfying a broader societal demand for retribution that we have lost sight of our fundamental goals.

If one breaks each crime down into its basic elements, there is an offender and a victim, both human beings, both suffering as a consequence. Our priority should be in addressing both forms of human suffering, that of the victim and the offender, in that order. We need to assist the victim in all ways possible to recover from his or her loss at the hands of the offender, so that he or she can recover and move on with their lives in a positive way. We also need to address the behavioural shortcomings of the offender in an attempt to rehabilitate him or her in order to prevent or minimise reoffending. Dealing with the human consequences of each crime and focussing on those outcomes, takes care of the punishment. The process of achieving that is the punishment. Whatever, and how ever long that takes, but clearly it is focussed more on behavioural science than ritualistic imprisonment, although practically it may involve both.

Our systems and resources should be heavily weighted towards these objectives, and we should reverse the trend of just treating the symptoms and focus on the causes. It's a more holistic view, but one that is becoming obvious in a wider range of topics, not only crime and punishment.

Now before you all think that I have lost the plot and gone soft on crime; that is not the case. Facing and resolving personal issues of and by the offender are a lot more complex and difficult to deal with than

simple incarceration. More importantly, if achieved, they will ultimately result in less crime and less strain on the judicial system and contribute towards a more harmonious and positive society.

It reminds me of a Chinese proverb, *(which by chance I have hanging on my wall)*.

"If there is light in the soul, there is beauty in the person.

If there is beauty in the person there will be harmony in the house.

If there is harmony in the house there will be order in the nation.

If there is order in the nation there will be peace in the world."

These thoughts are simply a high level overview, a concept that requires considerably more detail and is intended only as a discussion document. However, in my humble view, an interesting starting point.



**Philip Roigard CPP**

*Phil Roigard is a Licensed Private Investigator and Director of RISQ New Zealand Limited. [www.risq.co.nz](http://www.risq.co.nz). He is also an Executive Committee Member of the New Zealand Institute of Professional Investigators (NZIPI)*

# Kiwi Invention Prevents Password Hacking

**A** New Zealand company has developed a new way of protecting Kiwi consumers from password hackers.

The average Kiwi is a 'sitting duck' when it comes to data security – and it is only a question of time before hackers exploit security loopholes that will see thousands of logins and passwords stolen – according to a prominent IT expert.

The CEO of leading NZ technology firm Optimizer HQ Manas Kumar says most Kiwis need to urgently review their data security practices, as stolen personal information is often used for cybercrime.

"We all have about 10 to 12 logins and passwords that we use for daily activities at work and home, for example, internet banking, email systems, Facebook, Twitter, LinkedIn, the Wi-Fi router at home, the

shared drive at work. What happens is that as humans, we have limited capacity for memory, so often these passwords are variations of the same combination of dates and numbers, your birthday, for example, or the name of a favourite pet!"

"It makes sense, of course, to create passwords that are easy to remember, but guess what? If a password is easy to remember, it's also easy to hack, and you run the risk of losing your entire life if a hacker gets their hands on your most personal information," says Kumar.

Kumar points out that most of us access social media sites, our email, a public or personal wifi network connection, chat with friends online, share photos and use internet banking to move our money around every day – all of which require us to use



*Manas Kumar is the CEO of technology firm Optimizer HQ*



passwords. This means our passwords are fundamentally prone to security breaches, he says.

"The problematic truth is that most of us don't have a clue of how incredibly vulnerable we are to identity theft and other potentially deadly security violations," says Kumar.

There is rising concern globally about the safety of personal information following major breaches of security on websites such as LinkedIn, which was hacked in June resulting in the loss of 6.5m user passwords, he says.

"What happened with the LinkedIn security breach was that within a very short amount of time, people started finding that their Gmail, Facebook and Twitter accounts were also hacked, because they use the same password across all these sites," Kumar says.

# PANOMERA®

## Multifocal sensor system



### Latest technology for stadium security

Panomera® is a completely novel camera technology, which was specially developed for the all-encompassing video surveillance of expansive areas. With Panomera®, huge widths, as well as areas with large distances can be displayed with a completely new resolution quality, in real time and at high frame rates of up to 30 fps.

With Panomera®, a huge area can be surveyed from a single location, and depending on the customer's needs, the resolution can be scaled nearly limitlessly.





It was with those cautionary tales in mind that Optimizer HQ developed Locker, a cross-platform password management system that can be used across Windows, Mac and Linux. The application uses military-grade encryption to store passwords, and requires a secure key as well as the app, which is free to download upon purchase of the key, to access user passwords.

Kumar says many New Zealanders create passwords and list them all on one spreadsheet on a shared drive. All a hacker has to do is get their hands on that spreadsheet and suddenly there's a major security breach that can cost thousands to clean up.

With Locker HQ, Kumar has created a simple two-step system that he says buys his customers peace of mind.

"People can purchase a secure key that plugs into the USB slot, where they can store all their passwords, then plug the key into their computer to access them. You need both the key and the app for the system to work – and here's my favourite part, we've created a special 'enterprise' version which has the added functionality of allowing you to remotely erase or reset all passwords, and even instruct the app to shut down if your laptop is stolen."

Kumar says the offering is available at low cost, because he wants to make data security affordable for all Kiwis both at work and home.

He's also made the application easy for anyone to use. Once a user has stored

all their passwords in the app, accessing them is just a matter of plugging in the Secure Key, launching the app, then simply clicking on the app link, and dragging and dropping the relevant password into the login form of the website.

Kumar's invention aims to counteract the danger that New Zealanders could become complacent about security attacks, as previously we have not been subject to them.

"But if you take Australia as an example, about three years ago, Australia was not even in the top 20 'most phished' countries in the world. Today, Australia is the no 3 target globally for password hacking and email scams and that's all due to a major boom in e-commerce sites that started seeing more people and businesses making transactions online."

"The exact same thing is happening in NZ, so in a few short years, we are going to be a target for those online scammers, so we need to start taking precautions now to protect our personal safety and private data," says Kumar.

Furthermore, safeguarding ourselves against others gaining access to our private information is not just limited to our passwords, he says. Other information can be harmful to us if it ends up in the wrong hands, and that's why there is no limit or restrictions to the type of data that can be stored inside Locker HQ.

"Locker HQ has been designed to protect any key-value pair. In other words, you can use Locker HQ to safely store

other sensitive information such as your credit card numbers, your social security number, or even your bank account number," Kumar says.

For those who think that firewall and anti-virus software will provide them with security, they are sadly mistaken, he says. "While these services do a good job of protecting your computer against scams and viruses, their capacities seldom extend to password protection," Kumar says.

"We're talking about password security and your firewall or anti-virus software was never designed to protect you in that area because the onus was always put back onto the user to choose strong passwords that couldn't be easily broken."

"The problem we're trying to solve goes beyond the capabilities of your firewall. It addresses the single biggest point of vulnerability as far as an interaction between a person and the internet is concerned – the password," he says.

In his aim to encourage others to recognise the massive security hole that our passwords are creating in our lives until now, Kumar suggests a few ideas for formulating the perfect password.

"Passwords need to be long, strong and not made up of common words, dates or numbers. They also need to be accessed securely and in a way that leaves no room for any nasty creepers inside your computer to sniff them out."

**For more information on Locker HQ visit [www.lockerhq.com](http://www.lockerhq.com)**

---

# Data breaches costing firms dear

A global survey of IT security professionals finds many do not have the tools or the time to prevent or detect hackers and malicious software crippling their systems

**S**olera Networks, a provider of security intelligence and analytics, has polled more than 3000 IT security professionals in eight countries to understand the steps they are taking to thwart data breaches.

The Ponemon Institute carried out the survey, speaking with 3529 security practitioners in Australia, US, Canada, UK, Brazil, Japan, Singapore and UAE. All those who took part in the study represent organizations that had one or more data security breaches in the past 24 months. The survey found that data breaches are on the rise and that many organizations are unprepared to detect them or resolve them.

According to the majority of respondents, data breaches have increased in both severity (54 percent) and frequency (52 percent) in the past 24 months. While 63 percent say that knowing the root causes of breaches strengthens their organization's security posture, only 40 percent say they have the tools, personnel and funding to pinpoint the root causes.

The institute's report says breaches typically remain undiscovered and unresolved for months, and that on average, it is taking companies nearly three months (80 days) to discover a malicious breach and then more than four months (123 days) to fix it.

Surprisingly, security systems are not preventing a large portion of breaches with one third of malicious breaches not being caught by any of the companies' defences – they are instead discovered when companies are notified by a third party, either law enforcement, a partner, customer or other party – or discovered by accident.

Meanwhile, more than one third of non-malicious breaches (34 percent) are discovered accidentally.

The report says malicious breaches are targeting key information assets within organizations with nearly half of malicious breaches (42 percent) targeted applications and more than one third (36 percent) targeted user accounts.

According to the survey's findings, on average, malicious breaches (US\$840,000) are significantly more costly than non-malicious data breaches (US\$470,000). For non-malicious breaches, lost reputation, brand value and image were reported as the most serious consequences by participants.

For malicious breaches, organizations suffered lost time and productivity followed by loss of reputation.

"Security breaches continue to occupy the headlines on a daily basis, making

it clear that there is still much work to be done before companies are prepared for the inevitability of today's advanced targeted attacks," says John Vecchi, vice president of marketing, Solera Networks.

"In a post-prevention world, organizations must shift their focus toward attaining the real-time visibility, context and big data security analytics needed to see, detect, eradicate and respond to advanced malware (malicious software) and zero-day attacks."

Larry Ponemon, chairman and founder,

Ponemon Institute, says: "Our study confirms that organizations are facing a growing flood of increasingly malicious data breaches and they don't have the tools, staff or resources to discover and resolve them.

"Meanwhile, months are passing as their key information assets are left exposed. The results demonstrate a clear need for greater and faster visibility – as well as a need to know the root cause of the breaches themselves – in order to close this persistent window of exposure."

---

## Small businesses targeted by cybercriminals

**S**oftware security firm Symantec's latest Internet Security Threat Report (ISTR) shows a 42 percent surge during 2012 in targeted attacks compared to 2011.

The April 2013 report shows that criminals are setting out to steal intellectual property using targeted cyberespionage attacks that are increasingly hitting the manufacturing sector as well as small businesses. Stephen Trilling, Chief Technology Officer, Symantec says small businesses are attractive targets and a way in to ultimately reach larger companies via 'watering hole' techniques. In addition, consumers remain vulnerable to ransomware and mobile threats, particularly on the Android platform.

"This year's ISTR shows that cybercriminals aren't slowing down and they continue to devise new ways to steal information from organizations of all sizes," says Trilling. "The sophistication of attacks coupled with today's IT complexities, such as virtualisation, mobility and cloud, require organizations to remain proactive and use 'defence in depth' security measures to stay ahead of attacks."

Targeted attacks are growing the most among businesses that employ fewer than 250 employees. Small businesses are now the target of 31 percent of all attacks, a threefold increase from 2011.

While small businesses may feel they are immune to targeted attacks, cybercriminals are enticed by these organizations' bank account information, customer data and intellectual property. Attackers hone in on small businesses that may often lack adequate security practices and infrastructure.

Web-based attacks increased by 30 percent in 2012, many of which originated from the compromised websites of small businesses. These websites were then used in massive cyberattacks as well as 'watering hole' attacks. In a watering hole attack, the attacker compromises a website, such as a blog or small business website, which is known to be frequently visited by the victim of interest.

When the victim later visits the compromised website, a targeted attack payload is silently installed on their computer. The Elderwood Gang pioneered this class of attack; and, in 2012, successfully infected 500 organizations in a single day. In these scenarios, the attacker leverages the weak security of one business to circumvent the potentially stronger security of another business.

Shifting from governments, manufacturing has moved to the top of the list of industries targeted for attacks in 2012.

Trilling believes this is attributed to an increase in attacks targeting the supply chain – cybercriminals find these contractors and subcontractors susceptible to attacks and they are often in possession of valuable intellectual property.

Often by going after manufacturing companies in the supply chain, attackers gain access to sensitive information of a larger company. In addition, executives are no longer the leading targets of choice.

In 2012, the most commonly targeted victims of these types of attacks across all industries were knowledge workers (27 percent) with access to intellectual property as well as those in sales (24 percent).

Last year, mobile malware increased by 58 percent and 32 percent of all mobile threats attempted to steal information, such as e-mail addresses and phone numbers.

"Surprisingly, these increases cannot necessarily be attributed to the 30 percent increase in mobile vulnerabilities," says Trilling. "While Apple's iOS had the most documented vulnerabilities, it only had one threat discovered during the same period. Android, by contrast, had fewer vulnerabilities but more threats than any other mobile operating system."

Android's market share, its open platform and the multiple distribution methods available to distribute malicious apps, make it the go-to platform for attackers.

In addition, 61 percent of malicious websites are actually legitimate websites that have been compromised and infected with malicious code. Business, technology and shopping websites were among the top five types of websites hosting infections. Trilling attributes this to unpatched vulnerabilities on legitimate websites.

"In years passed, these websites were often targeted to sell fake antivirus to unsuspecting consumers," he says. "However, ransomware, a particularly vicious attack method, is now emerging as the malware of choice because of its high profitability for attackers.

In this scenario, attackers use poisoned websites to infect unsuspecting users and lock their machines, demanding a ransom in order to regain access.

Another growing source of infections on websites is malvertisements – this is when criminals buy advertising space on legitimate websites and use it to hide their attack code."

# Kiwi helps expose litany of errors in 'preventable' London blaze

By Keith Newman

**A** 10-week public inquiry into London's worst residential tower block fire in which six people lost their lives should be a wake-up call for landlords, the New Zealand Fire Service and the fire protection industry about how quickly things can go wrong if all the checks and balances aren't covered off.

Former NZ Fire Service Operations Manager, Brian Davey was called on by the London Coroner as an independent expert witness to help investigate why the 3 July 2009 blaze at Lakanal House, Camberwell in south London, got so badly out of control in such a short time.

At the centre of the inquiry was the Southwark Borough Council, owner of the 14-storey, 98 apartment block built in 1958, and its failure to comply with fire safety checks. The London Fire Brigade was also proven to be ill-prepared for the disaster which showed up a range of operational and communications issues.

Complex legislation around the British equivalent of the New Zealand Building Code, which allowed for different interpretations of compliance, was also raised as a result of the fire which saw 150 people rescued or evacuated and nine people treated by emergency services.

In reporting on the final outcome of the inquiry at a jury trial just after Easter this year, the London Guardian newspaper, described "botched and unsafe renovation work... the council's failure to inspect the building, as well as confusion and chaos during the fire fighting operation."

The main messages bought home by Davey relate to the need for good decision making even in unexpected circumstances and how decisions made by different agencies, including the government, can align to cause tragedy.



*Brian Davey, former NZ Fire Service Operations Manager and expert witness in the Lakanal House inquest*

### No room for complacency

"It's about not being complacent and learning lessons from all around the world," he says. The Doha Mall fire in Qatar where Kiwi twins died last year and which caught fire again in April this year, is another example we need to learn from, "to ensure our legislation covers off all the things that led to these tragedies".

Davey was called in to examine the causes of the London tragedy because of his operational experience, his independence and his role as a director and trustee of the New Zealand Institute of Fire Engineers.



*The west side of Lakanal House showing from the bottom up flats, 37, 53 and 79. Fatalities occurred in flats 79 and 81. Photo Courtesy London Fire Brigade*



# fire door holding electromagnets

Standard, floor mounted, wall to door distance 114mm



## FDH40S

### unbreakable universal mounting

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

**Designed, tested and produced in New Zealand to AS4178**

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



Flush mounted, wall to door distance from 50mm



Surface mounted, wall to door distance 70mm



## FDH40SS

### stainless steel surface and flush mounting

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

**10 YEAR GUARANTEE\***

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



**BOTH  
options are  
packaged  
in the  
same box**



*There were serious command and control issues, particularly around the London Fire Brigade hand-over process which resulted in an inadequate number of appliances turning out.*

His work began in April 2012 but escalated in October on his retirement from the NZ Fire Service, when he was asked among other things to look at the effectiveness of London's building legislation in relation to fire protection.

As part of a public inquiry, Davey was asked to help investigate the cause of the deaths, the factors leading up to the fire including the responsibilities of the Southwark Borough Council and the operations of the London Fire Brigade.

The cause, an electrical fault in a television set on the ninth floor, ended up exposing a lineage of culpability and confusion and while there have been apologies all round, none of the parties is accepting legal liability.

Davey says this was largely because Police had been through the law prior to the

inquest and determined no individual could be found criminally liable, although relatives of the deceased are now bringing civil cases against the council, the London Fire Brigade and the renovation contractor.

#### **Approach too informal**

Davey says the London Fire Brigade did not know enough about Lakanal House before they arrived and had a "pretty informal approach" to pre-incident planning, not having previously seen the building as a major risk.

Having recently completed a two year programme developing pre-incident planning for the NZ Fire Service national headquarters he could see where a lot of the faults had occurred. "Although I know the London Fire Service has since made a lot of changes, my assessment had to be based on what they were doing at the time."

For a start, Davey says bad advice was given to tenants, who were told their apartments were fire-proofed and they should remain inside. "This had worked in 1997 when one apartment was gutted and tenants above and on either side were quite safe but the exterior panels had been changed since then."

Council and government officials gave conflicting evidence about the required fire rating of the wall cladding which was a big contributor to the fire spreading.

Did the panels need to be completely fire resistant; like the old asbestos panels they replaced, or zero fire spread rating — flammable but with a surface that doesn't spread the flame?

As part of a 3.5 million pound maintenance and renovation programme, allegedly to make the 98 unit building



*The external, supposedly fire proof panels buckled and exposed flammable material in the Lakanal House blaze. The floor below the fire is actually the roof of the flat below. Courtesy London Fire Brigade*

compliant with fire standards, the contractor had used composite cladding panels with zero flame spread.

#### **Too much ambiguity**

The inquiry found the panels twisted, exposing non-fire resistant panels behind them, causing the flames to spread to apartments above. The deputy coroner, Judge Frances Kirkham with a background in building law, was concerned at the confusion and recommended all ambiguity in regulation be avoided.

Because it was the middle of summer, Davey says, people had their windows open and debris fell down and entered the apartments below resulting in the fire going "vertically up and down" rapidly accelerating the fire, something emergency operators at first refused to believe.

The findings also determined there was a general lack of knowledge by tenants about escape routes and they were given wrong advice by the London Fire Department's control room. Unaware of the severity of the situation, they told callers to stay put when they should have been evacuated.

In one example, an operator kept a woman on the phone for 45 minutes and despite her yelling that the flames were at the door and that something had fallen on her from the ceiling, she obeyed instructions and died as a result.

In a neighbouring apartment four people got out but five took refuge in a bathroom and suffocated when smoke entered the room through a steam venting system which had been exposed when panels buckled.



*The seared and buckled remnant of burnt panels on the lower (bedroom area) and upper floor (lounge, kitchen) of two flats, in the Lakanal House apartment building in south London*



*Smoke billows from the ventilation grille at the north end of the 11th floor internal corridor as a consequence of a severe internal fire*

Davey says incident commanders didn't understand their control room was advising occupants to stay put — he blames lack of training and poor communications procedure.

“Even those control room operators who had been there for some time could only recall one training session a decade earlier. There was no regular training programme to keep them up to speed with the sort of questions they should ask and how to respond.”

#### **Command and no control**

And Davey says there were some serious command and control issues, particularly around the London Fire Brigade hand-over process which resulted in an inadequate number of appliances turning out.

The arriving officer made “pumps four” when four engines were already on the way, then when queried only ordered another two, thereafter pumps were ordered in increments of two, three times over the next 20 minutes.

Davey says the first officer should have got at least six more pumps on the road then ramped it up. In the end 18 pumps turned up but it was too late to have the necessary impact. “They failed

to assess the extent of the situation quickly enough.”

When a “type 5, aerial appliance” with 18 metre extension ladder and platform arrived in the first five minutes the operator refused to deploy, saying there was too much flaming debris. Half an hour later another unit went to work successfully in the same circumstances.

“There was an issue around familiarity with the area of operation; if the first appliance operator could have found a way to deploy they could have improved access or at least put up a water curtain to extinguish the burning debris,” says Davey.

The inquest was also critical of the hand over process. Procedures require a more senior officer to take command as an incident escalates and to be briefed on an action plan based on how the fire is developing.

In this situation, says Davey, the hand-over occurred three times in five minutes and no-one got a full briefing period until things had settled down.

#### **Serious failures outlined**

As a consequence there were insufficient personnel available. Although a forward

*“There was no regular training programme to keep them (the control room operators) up to speed with the sort of questions they should ask and how to respond,”*

*said expert New Zealand witness, Brian Davey*

command post was established on the 7th floor, two floors below where the fire started, it quickly spread to floors 3 and 11. With only 30 minutes of air in their breathing apparatuses, running between floors meant each person had only about seven minutes actual fire fighting time.

All the while fire fighters were required to engage in search and rescue. “They were overwhelmed, under a lot of pressure and unable to formulate a proper plan which would normally have happened in a fairly structured way.”

Davey was required to be in court for the 10-week inquest which concluded in February and then after returning home to his farm near Oamaru was back in London giving final evidence and being cross examined before a jury. The verdict was delivered in April.

The jury highlighted numerous ways in which the three women and three young children from Brazil, Nigeria and Hampshire, could have been saved, saying the fire was ‘preventable’.

The jury heard Southwark Council, responsible for fire safety checks at its flats since 2006, had not completed these on the Lakanal Block or other similar residential blocks by 2009, resulting in “a serious failure” by the council and its contractors.

The court was told that a proper inspection would have picked up work that had been ongoing from the 1980s where vital fire-stopping material between flats and communal corridors was removed. The replacement of asbestos window panels with composite equivalents that burned in less than five minutes was also an issue.

Deputy coroner Kirkham, recommended fire services visit high-rise blocks to learn their layout, landlords consider fitting sprinkler systems and residents also get better fire safety information.



# SUBSCRIBE NOW

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

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

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

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

or email your contact and  
postal details to:  
[craig@newzealandsecurity.co.nz](mailto:craig@newzealandsecurity.co.nz)

First Name \_\_\_\_\_

Surname \_\_\_\_\_

Title \_\_\_\_\_

Company \_\_\_\_\_

Postal Address \_\_\_\_\_

\_\_\_\_\_ Post Code \_\_\_\_\_

Telephone \_\_\_\_\_

Email \_\_\_\_\_

Date \_\_\_\_\_

Signed \_\_\_\_\_

**nzSecurity** Magazine  
A trusted source of information for industry professionals

## Stop The Silent Killer

**Carbon Monoxide Kills. You can't smell it, see it or taste it.  
But you can hear it. Fit BROOKS Alarms now!**

**C**arbon Monoxide (CO) is an invisible, odourless, tasteless and extremely toxic gas. It is absorbed by red blood cells in the lungs in preference to Oxygen - this results in rapid damage to the heart and brain from Oxygen starvation.

**It is known as the Silent Killer because Carbon Monoxide is:**

- A poisonous gas that is a by-product of an incomplete combustion process
- Odourless, tasteless and invisible
- Symptoms are often mistaken and misdiagnosed
- A tragedy that could be avoided
- Detection is the only sure way of knowing it's present

**Accidents/Events That Can Lead to CO poisoning:**

- Faulty or damaged heating appliances
- Heating appliance not maintained or serviced
- Rooms not properly ventilated
- Blocked chimneys or flues
- Indoor use of a barbecue grill or outdoor heater
- Poor installation of heating appliances



- Improper operation of heating appliances
- Property alterations or home improvements, which reduce ventilation
- Running engines such as vehicles or lawnmowers in garages
- Using cooking appliances for heating purposes

CO Awareness and Prevention is the key, especially now that **WINTER** is here and the use of GAS heaters is far greater and CO alarms are also good for boats and caravans



**Fit BROOKS Carbon  
Monoxide Alarms now!**

**For more information phone  
0800 220 007 or visit  
[www.brooks.co.nz](http://www.brooks.co.nz)**



**NEW**

# STOP THE KILLER

**Carbon Monoxide kills.**

You can't smell it, see it or taste it.  
But you can hear it - **Fit BROOKS Alarms Now!**



The dangers are  
all around you



Protect **Your** Family

For more information regarding safety in the home please contact:

BROOKS New Zealand: Ph 0800 200 007 - [www.brooks.co.nz](http://www.brooks.co.nz)

BROOKS Australia: Ph 1300 78 3473 - [www.brooks.com.au](http://www.brooks.com.au)

# Contract law change essential to stop 'subbies' being fall guys

Keith Newman does the rounds with lobbyists, specialist sub-contractors, a contract law expert and the Minister of Building and Construction over the growing pressure to address 'subbies' retentions, the elephant in the room, as the Government takes another look at the Construction Contracts Act

Specialist trades sub-contractors want an urgent law change to put an end to 'retention abuse' by the building and construction industry and tidy up unfinished business left over from the decade old Construction Contracts Act.

The loss of around \$20 million held on behalf of sub-contractors through the collapse of Mainzeal Construction in February was the last straw for many involved in the scaffolding, roofing, plumbing, glass, gas fitting, electrical, security, fire protection and other building-related trades.

They're fed up with being forced to give up a portion of their income as interest free cashflow for builders and main contractors with no guarantee they'll ever get it back.

In effect 'subbies' carry huge risk, having to pay for materials and wages and typically working on a 10 percent margin which can be tied up in retentions for up to 18 months. If the main contractor goes belly up and they don't get paid the domino effects ripples right through the supply chain.

Holding on to retentions has become standard industry practice and when the liquidator steps in specialist trades have to wait in line behind the banks, employees, the IRD and everyone else with a slim chance of a payout.

Housing and Construction Minister, Maurice Williamson agrees there's a problem and while some parties are lobbying for change, he says others think things are fine just the way they are.

*"If you listen to one side you'll get black and white justification for what they want and the exact opposite argument from the other side which seems to have just as much merit," Housing and Construction Minister Maurice Williamson*

And while there's "no moral justification" for builders using sub-contractors money as cashflow, developers say if retentions are taken out, cashflow will dry up and there'll be no new projects. "If that was the case subbies would soon be screaming, 'there's no work'."

Williamson says the issue is full of fish hooks. "If you listen to one side you'll get black and white justification for what they want and the exact opposite argument from the other side which seems to have just as much merit."

He says it's the murky bits inbetween that concern him, when you realise "whatever you do may cause as much damage as it provides benefits." There's a need for balance and he's mindful that the greatest explosions in Parliament come from "the law of unintended consequences."

The Specialist Trade Contractors Federations (STCF), the umbrella group for the main sub-contractors, believes the retentions issue should be included in amendments to the Construction Contracts Act 2002 (CCA) put before the House just before the Mainzeal collapse.

Prior to the original Act, the common industry practice was that sub-contractors only got paid when the lead contractor got their money from the developer — if the receivers were called in it was the tradespeople who often missed out altogether.

The CCA set out an agreed schedule of payments and dispute resolution and put an end to the practices of that dark era after several years of hard lobbying.



Building and Construction Minister, Maurice Williamson





Construction law expert, Peter Degerholm of Calderglen Associates

Peter Degerholm, Chief Executive of Lower Hutt-based Calderglen, who worked from the late 1990s to overturn the entrenched ‘pay when paid’ approach, says the building industry only conceded to changes after forcing sub-contractor retentions off the table.

“Giving up pay when paid was a big enough step, giving up retentions was a step too far at the time,” says Degerholm. Now, however, with the fall out from the Mainzeal collapse fresh in people’s mind, he thinks it’s the right time to finish the job.

He says subbies need to present an evidence-based case for statutory protection and to be aware the original Act only got traction because contractors were united, came up with a solid solution

and the issues were given a high profile. He’ll be making personal submissions on the CCA Amendment Bill and supporting the STCF and others.

### Minister softens stance

STCF executive member Neville Simpson who’s leading the charge on behalf of specialist contractors has found Building and Housing Minister Maurice Williamson less dismissive of contractor concerns than he was when the Bill was first tabled.

After several meetings, the STCF was asked to come back with a simple, low cost option that might be considered as a supplementary order paper (SOP) to the Bill.

As it stands, the Construction Contracts Act 2002 Amendment Bill simply removes the distinction between residential and commercial work, broadens the definition of ‘construction work’ to include design, engineering and quantity surveying and expands options for resolving non-monetary disputes.

The STCF proposal wants statutory protection for existing bond provisions in the Act as the default position for all sub-contractors, putting them back in charge of their own cashflow.

Rather than being forced to leave 10 percent of the cost of each contract unsecured and in the hands of the main contractor or builder until ‘practical completion’ and ‘a defect period’ of another 12 months, subbies would put up their own bank-secured bond for example.

A copy of the proposal has been circulated to all STCF members and Simpson, who’s also head of the Electrical

Contractors Association (ECANZ), is urging member groups to give strong and vocal support including writing submissions to Williamson.

### NSW inquiry sets tone

Peter Degerholm says a debate around the issue is long overdue and he’s encouraged by the recommendations of a New South Wales State Government Inquiry, triggered by a \$45 million construction company failure, that revealed ‘massive retention abuse’ across the State.

The term ‘retention abuse’ is not used in New Zealand, although if Degerholm has his way it may soon become part of our vocabulary. He says a sliding scale that caps builder’s liabilities to a developer at two percent for example and withholds two or three times that amount from their sub-contractors has become a game of “holding on”.

The NSW report recommends all retentions be held in a trust account or project bank account to ensure the receivers don’t get it and to prevent it being used as part of a company’s cashflow structure.

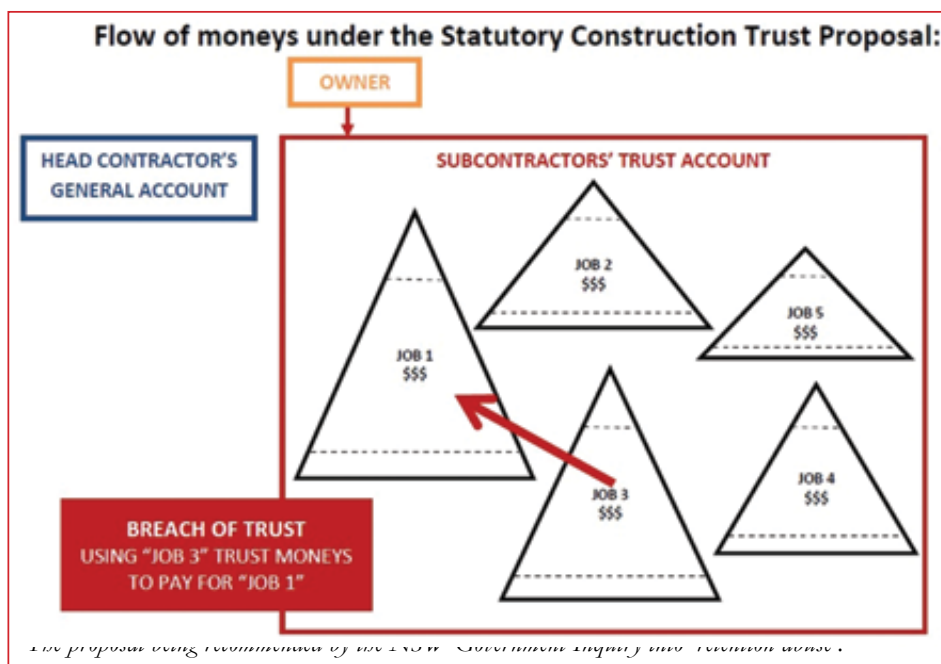
To kick start the debate, he’s invited the chairman of the NSW inquiry Bruce Collins QC to come to New Zealand in June to address among others, the Construction Law Society and the Quantity Surveyors Institute.

Building and Construction Minister Williamson insists he’s not sitting on his hands. “If I can get anyone to persuade me there’s a solution where the benefits outweigh the detriments then we’ll move quite quickly and the Amendment Bill before the House would be the right vehicle for it.”

His officials are looking into the STCF proposal and those from other parties and “working across the sector” to get advice and looking at other jurisdictions, particularly Australia and the UK to see if there’s a regime with enough benefits and a downside that’s “not too scary”. The NSW Government Inquiry recommendations are also being considered.

While the SCTF claims to have a workable idea that doesn’t go to the extremes of earlier attempts to address the retentions issue, Williamson says he has to look at the wider impacts on the economy.

He told NZ Security he’s not ruling anything in or out until all the reports are completed. “I’ll be waiting and reading around the history of what’s happened in the past because its always been fraught with problems that’s why a lot of the



earlier provisions got taken out.” His intention is to have the matter resolved by the end of the year.

Meanwhile Degerholm is planning to make his own independent submissions on the CCA Amendment Bill urging that retentions be held in trust as a kind of bond, secured in the contractor’s name until the contracts are all signed off and then released in a timely fashion.

He’ll also support others in their submissions, including the STCF, but doesn’t believe changes should be rushed through by simply tweaking the existing Bill.

### Who holds the gold?

So why have subbies put up with this situation for so long? One suggestion is that it’s because of the lobbying power of the main contractors who are hugely influential at a government level.

STCF head lobbyist Neville Simpson agrees: “The power resides with those who hold the gold.”

The builders who finance projects through a developer “hold the purse strings and dictate what’s going on”.

Some in the fire industry want to see retentions in their present form done away with entirely and replaced with bonds or retentions in a trust account managed by an independent solicitor and released at sign off by an independent engineer or specialist.

Currently retentions are there to protect clients and the head contractor from sub-contractors falling behind schedule, defective work, failing to complete remedial work or being incompetent or insufficiently resourced to complete what they started. However, there’s a strong view that normal credit terms would take care of most of those concerns.

Meantime some wonder whether there’s sufficient time to raise a strong enough voice so sub-contractors are heard above the potential opposition from the building and construction industry. It may be the industry has to raise its concerns in another Bill if it can’t get a strong enough case together in time for the current amendment.

Degerholm says the case will cost a lot of money but agrees contractors need to make as much noise as possible otherwise no-one’s going to listen. “The industry needs to decide how to make that noise and choose a forum and make every word count.”

However Minister Williamson says additional lobbying won’t help as the STCF and other groups are doing the right thing by presenting a united approach. “I know it’s difficult but you have to find a solution that takes care of all the risks, giving certainty and guarantee of payment... without killing the goose that lays the golden egg.”

*“Why are you holding on to our retentions and not accepting bonds?”*

*“...If you were in business and someone gave you 12 months interest free access to money, you wouldn’t have to be a rocket scientist to figure that out. It’s really an ethical matter.” STCF’s Neville Simpson with a rhetorical question.*

### Got to get it right

STCF’s Neville Simpson is in no hurry, as the industry will need to make adjustments in the way it does business, including an attitude change from the building industry if its to restore confidence among the contractors it so heavily relies on.

Like others, he wants to know why the existing provision in the Act, allowing sub-contractors to put up a bond ‘in lieu of retentions’, is so often rejected by builders who indicate they’ll find someone else to do the job if retentions aren’t agreed to?

The message to the building and construction industry is simple, he says, “why are you holding on to our retentions and not accepting bonds?” That is more of a rhetorical question. “If you were in business and someone gave you 12 months interest free access to money, you wouldn’t have to be a rocket scientist to figure that out. It’s really an ethical matter.”

Under the bond system, subbies would go to the bank to secure an overdraft facility; using their house or business as collateral if necessary, and make this available to the lead contractor. “Instead of the payer determining the bond it’s now the payee,” says Simpson.

The bond protects against the contractor going out of business and guarantees the specialist tradesperson will come back and correct any defects or problems found within the standard 12 month period. “You’d be crazy not to go back and fix any outstanding issues to keep your bond.”

With full monthly progress payments and funds freed up at the practical completion and the end of the defect period, Simpson says, it’s more likely sub-contractors would use their own cashflow to “improve their IT systems, take on more apprentices, upskill the workforce or go out and buy a boat”.

## Slapped twice for being insecure

Sub-contractors can get slapped twice when a company such as Mainzeal goes under, particularly if liquidators take the insolvency provisions of the NZ Company’s Act too literally.

On top of losing retentions that are supposed to be put aside for work completed, there’s a potential for liquidators to go trawling through payments already made to sub-contractors.

Mike Connelly, Executive Director of the Fire Protection Association (FPANZ) says it’s not exactly equitable that the liquidator is a secured creditor when it comes to getting their accounts settled while sub-contractors are pretty much last in line.

And when a company such as Mainzeal goes under, there’s a provision in the law for the liquidators to claw back money paid out legitimately up to two years previously.

Construction law expert Peter Degerholm says there’s evidence some liquidators are even looking to ‘claw back’ subbies’ provisional monthly payments.

And Mark Bishop, Managing Director, First Fire Systems says the receiver or liquidators should never be able to touch the retention money. “I’ve heard companies who’ve lost \$90,000 and \$450,000. The reality is if we don’t pay our debts then we’re in trouble.”

He says the big contracts put out to tender by Hawkins, Mainzeal and other large firms have relatively low overheads because the sub-contractors carry most of the risk by providing materials and labour.

“They’ve already screwed the sub-contractors down so there’s little margin in these jobs and the retentions can be the difference between whether a job is profitable or not,” says Bishop.

And at the end of the contract he says most construction companies are not good at paying up the retentions “unless you chase them down”.

### Payment claims underplayed

However, Peter Degerholm says subbies must be aware of what's already available to them under the law. Currently even simple provisions aren't used as widely as they should be to enforce earlier payments.

"We're ten years down the track and a large proportion of people are not putting in payment claims... even this basic protection can be hugely helpful."

Degerholm says rather than sending invoices, a 'payment claim' is a demand made under the Act which requires the contractor to give a schedule of payment. If payments aren't made within 20 days, it can be enforced as a debt straight away.

While it's not going to help if a construction firm goes belly up, he says it's a "very effective way" to get paid on time "and prevent issues from festering so sub-contractors are less exposed".

And while there are complaints the builders don't let subbies know when their retentions are due. Simpson says any good sub-contractor should be keeping

track of this through their business systems and processes.

If the STCF proposal becomes part of the amended Act, he says it will put responsibility on sub-contractors to be more informed about who they're working for and whether they're good payers and for builders to check out the subbies and not just go for the cheaper price.

For subbies, knowing money is coming into the business at the appropriate time will create a sense of security and allow them to plan ahead with more certainty.

"It will also mean builders will have to restructure and actually have the appropriate capital or get money from the usual sources rather than relying on sub contractor's money to tide them over if things get tough."

When it's all weighed up, he says, it could be a win-win situation. "Builders can use this system of bonds with the developer who holds retentions over them."

As Williamson says, a balance needs to be found, but if subbies who end up

doing all the work are essentially being held to ransom, with their profit margin gambled with by speculators, then they are disproportionately on the losing side. It sounds like the building and construction industry needs to work on their relationship with the banks.



*Neville Simpson head of the Electrical Contractors Association (ECANZ) and chief lobbyist for Specialist Trades Contractors Federation (STCF)*

## Every crash reverberates - subbies take it on the chin

Sub-contractors across the country cringe every time another large building contractor bites the dust, only too aware of the risks to their trade when the liquidator takes control of funds, supposedly held on their behalf.

A string of collapses over the past two decades have robbed them and their associates of up to 10 percent of overall earnings from jobs mostly completed to the highest standards. Concerns were heightened through last year's failure of Auckland's Alliance Construction and

February's Mainzeal Construction crash which left hundreds of 'subbies' out of pocket.

Construction law expert, Peter Degerholm, says contractors need to leverage the Mainzeal crash as evidence of their vulnerability and pressure the Government to change the retentions regime.

While \$10 million was withheld from Mainzeal by its clients, it held around \$20 million over its sub-contractors and that was before January and February receipts

were accounted for.

"That gives the impression that the sub-contractors money was in fact providing Mainzeal with interest-free unsecured lending of around \$10 million," says Degerholm.

And that's just the tip of an iceberg says Specialist Trade Contractors Federations (STCF) Executive Member, Neville Simpson. "There are bigger guys than Mainzeal who are operating like this, for example the bulk builders who operate huge groups — one of their franchisees goes under every couple of months."

The industry is full of excuses about why retentions are withheld or aren't paid on time but to many subbies, it's a reminder of the bad old days when no-one got paid until the developer and then the head contractor got their share.

### Trail of shame

Even if you start the trail of shame 13-years ago in Auckland, the America's Cup building boom and bust tells its own story of a volatile overblown economy where subbies carried the can for the speculators.





Goodall ABL hit the wall in March 2000 owing around \$20.4 million for work on Auckland apartment buildings with the retentions owing to dozens of sub-contractors wiped out.

In January 2001 there was a double whammy when GFF Ltd (formerly Equinox Construction) and Tauran Construction; both with few workers and only director shareholders at the helm, crashed with 1250 creditors owed \$5.2 million.

Then a month later Hartner Construction took a dive in the middle of completing the \$50 million Hilton complex at Auckland's Princess Wharf, locking out 250 subbies, ultimately owing \$30.2 million to 1105 unsecured creditors. As one commentator stated at the time, it sent a 'cascade' of subcontractors out of business.

Ironically the receivers moved in on Hartner, the day associate Minister of Economic Development Laila Harre announced the Government's intention to introduce the long lobbied for Construction Contracts Act.

Peter Degerholm, who championed the new law on behalf of the Building Subcontractors Federation (now the

STCF), says the TV cameras on the evening news panned across to the Tamaki Yacht Club where creditors were meeting with Hartner's receivers. "It was very convenient and from a public perspective it was seen as responsible and in tune with the issue."

### Immediate impact

Fire Protection Association (FPANZ) Executive Director Mike Connolly says there were 32 responses from their members to a survey they conducted over a 24-hour period, which is indicative of the level of concern. Those who responded claimed direct exposure to Mainzeal of around \$1.25 million in current claims and for completed work, but indirect exposure including suppliers and installers was more likely to be \$8 million, he says.

About 130 or 60 percent of FPANZ members are sub-contractors, and the impact was not only on contractors to Mainzeal but sub-contractors further downstream. The main contractors stand to lose everything that was retained and millions of dollars in work they were relying on, which puts them "in a precarious position," says Connolly,

He adds that if the 32 respondents is merely a representative sample from one collapse, even though Mainzeal was one of the five largest construction companies, then it is reasonable to assume the total exposure across the whole construction industry is in the tens of millions of dollars, even before considering the wider business and social impact.

It is not good enough for the politicians to say that they have no evidence that there is an issue, or that the impact in terms of jobs and business will be minimised because someone else will pick up the business and jobs will be maintained.

He says retentions are a major issue and something his organisation has been trying to address for some time. "Dealing with these issues through changes in the law is long overdue."

The FPA will join with other industry bodies in the belief that "broad sector, collective representation" has a better chance of being heard. It will be making its views known as soon as the new bill passes its first reading. "You can bet your bottom dollar there will be some strong submissions," says Connolly.

## Unsecured risk not worth it



*Mark Bishop, Managing Director,  
First Fire Systems*

As a result of the Mainzeal collapse, Auckland fire protection sub-contractor First Fire Systems has pulled away from installation work on major contracts unless there is a strong existing relationship with the head contractor or developer.

Managing Director Mark Bishop, says his company will stick with service work to reduce the risk. "All of the bad debts we have provisioned for have come from developers, construction companies and the building industry where the potential risk is dramatically worse than anything else we do in our business."

Bishop considers himself one of the lucky ones having forfeited less than \$1000 in retentions through the Mainzeal collapse but admits he's lost much more through previous construction company failures.

He says it is unacceptable that subbies labour and materials is unsecured. "I think the whole retention thing is a racket and subbies are getting screwed left right and centre — that needs to change."

Bishop says it can be 15-18 months before you get full payment. "We're not happy with that. We've done the job and been paid progressively and the retention money should at the very least be placed in a trust exactly the same way you deal with tenancy bonds."

And he says the receiver or liquidators should never be able to touch the retention money. "I've heard companies who've lost \$90,000 and \$450,000. The reality is if we don't pay our debts then we're in trouble."

He says the big contracts put out to tender by Hawkins, Mainzeal and other large firms have relatively low overheads because the sub-contractors carry most of the risk by providing materials and labour.

"They've already screwed the sub-contractors down so there's little margin in these jobs and the retentions can be the difference between whether a job is profitable or not," says Bishop.

And at the end of the contract he says most construction companies are not good at paying up the retentions "unless you chase them down".

# Kiwi high rises safer than London but no excuse for bad information

Firefighters need to have accurate information about buildings, including anything unusual about layout and construction, to avoid the chaos that caught the London Fire Brigade off-guard four years ago.

While the New Zealand Fire Service (NZFS) has good policy and procedure around pre-incident planning, unless its applied properly on the front line there's a risk of missing valuable evidence, says former NZ Fire Service Operations Manager, Brian Davey.

Davey, who helped develop the NZFS pre-incident planning strategy was called as an expert witness in an inquiry into the fire which ripped through the 14-storey Lakanal House apartment block in South London, claiming six lives.

"People need to know what to look for and what is different about each building." If there had been more process around operational staff visits to Lakanal House and even basic information recorded, things might have been very different, he says.

While staff had previously checked riser systems, fire fighting lifts and exits they had little understanding of the layout and design, including the fact all the apartments were maisonettes occupying two floors.

A simple note stating the bottom floor covered only half the width of the building with an exit into the main corridor and the top floor was the full width with an exit on either side, would have been very useful, says Davey.

The blaze got out of hand for a complexity of reasons including the use of non-compliant building materials, lack of sprinklers, no evacuation procedure and botched London Fire Brigade communication both on the ground and at its control centre.



The London fire brigade was unaware of the unusual layout of the maisonette flats in the Lakanal House blaze and the fact those on the east side of the corridor mirrored those on the west. Photo courtesy London Fire Brigade.

## Housing boom backfires

Davey says the issue with London started after the Second World War and the big housing boom that replaced old slum areas with high density housing, which created the problem now manifesting 60-years later "in this sort of disaster".

However, the recently revised and strenuously applied New Zealand Building Code, the requirement for sprinkler systems, stringent evacuation regulations and the fact most of our high density buildings are fairly recent, make such a event unlikely here.

Any concern would be limited to Christchurch, Dunedin, Wellington and Auckland, although Davey suggests those planning higher density developments in Auckland need to keep these issues in mind.

He says our Building Code mandates sprinkler systems in all high rise apartments, and even in smaller blocks, flame spread would be unlikely because each apartment is a cell designed to contain a fire for two to four hours.

He believes the NZFS is well resourced but warns you can never resource for exceptions, "you can only cover for those occasions with good decision making".

Mobile communications, particularly around differences in building design will help, although New Zealand doesn't as yet have data terminals in all its appliances. "The more information available to engines as they head off to fires the better."

While the London Fire Brigade has mobile units in its engines, Davey says our command units are better set up.

Issues including confusion over the interpretation of the British equivalent of our Building Act, no sprinklers or evacuation regulations, and the lack of pre-incident planning and fire training are all being investigated as a result of the London inquiry.

*The recently revised and strenuously applied New Zealand Building Code, the requirement for sprinkler systems, stringent evacuation regulations and the fact most of our high density buildings are fairly recent, make such a event unlikely here.*

**Pacific GSM**  
Jablocom Presents new:

**CLOUD SERVICE ANDROMEDA**

**EYE-02**




**JABLOCOM**

- Access, Control, Configure and see live your Jablocom devices from the web and phone
- Free connection
- Free Cloud Storage for 3 hours for EYE-02 Camera and CU-07 Vehicle Tracker
- EYE-02 GSM Security Monitoring Camera complete remote security system in one housing
- CU-07 GPS Tracker Plug and play device with on-line map tracking, only data charges apply

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

**09 948 4762**

**Pacific GSM**  
Presents

**Jablotron 100**

Revolutionary Alarm System  
Easy –Smart –Flexible



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

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

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

**09 948 4762**

**KOCOM®**  
SEE IT. TOUCH IT. RECORD IT.



KVR-D510 - INTEGRATED INTERCOM, CCTV & DVR SOLUTION

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

Now available at your local Hillsec branch.

**H ES**  
Hills Electronic Security

For all product information visit  
[www.hillsec.co.nz](http://www.hillsec.co.nz)

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




**FUJINON**

**GSP**  
DIGITAL VIDEO SECURITY SYSTEMS



**Panasonic NVR  
WJ-NV200K**



The WJ-NV200K provides the first real alternative to analog DVRs – at an analog price point!  
Ideal for retail, hospitality and Education markets, the WJ-NV200 is driven via mouse and keyboard to eliminate PC costs and desk space.  
Installation is simplified by quick setup automatic camera detection and simple setup wizard – all without requiring a PC.  
Real time Face Matching is also achieved using the Face Detection feature of the Panasonic Smart HD range of IP cameras. This provides fast detection and matching VS a stored database of known faces to alert the operator / store owner of unwanted guests.

**Features Include:**

- 16 Camera NVR
- H.264, MPEG-4 and JPEG multi format
- Simple mouse / monitor operation with intuitive GUI
- Quick search with calendar / timeline
- Full HD HDMI monitor output
- WV-ASM100 management software compatible
- Real time Face Matching with Smart HD cameras
- DVR price point!

**Panasonic New Zealand Ltd**  
350 Te Irirangi Drive, East Tamaki, Auckland  
Ph (09) 272 0100 • [sales@nz.panasonic.com](mailto:sales@nz.panasonic.com)

**Panasonic**

**Panasonic Video  
Doorphone  
VL-SW250BX**



Main Monitor      Wireless Monitor      Door Station

The VL-SW250BX is the latest video door phone from Panasonic. Monitor and even open the door remotely via the wireless handset. The main station stores up to 400 images to see who has been knocking while you were out!  
Ease of installation as a single twisted pair is all that's required from the gate station to the main monitor.

**Features Include:**

- Video Intercom unit with wireless remote handset
- Recording up to 400 images
- Voice changer function
- Simple installation
- Door release function
- 20 apartment Lobby unit available for expansion

**Panasonic New Zealand Ltd**  
350 Te Irirangi Drive, East Tamaki, Auckland  
Ph (09) 272 0100 • [sales@nz.panasonic.com](mailto:sales@nz.panasonic.com)

**Panasonic**

**Panasonic SD5 Dome  
WV-CF504E**



Panasonic have released an internal dome variant of their class leading Super Dynamic 5 analog camera. The WV-CF504E has the same functionality as the popular full body camera in an attractive compact dome.  
SD5 is still recognized as the best performing camera in severe backlight situations! perfect for retail, corporate and industrial applications.

**Features Include:**

- Super Dynamic 5
- 650TVL resolution
- i-VMD including object detection (removal and abandonment) and scene change
- Auto back Focus
- True day / night (IR cut filter)
- 3.8mm to 8mm AI lens
- 3 way axis for ceiling or wall mount

**Panasonic New Zealand Ltd**  
350 Te Irirangi Drive, East Tamaki, Auckland  
Ph (09) 272 0100 • [sales@nz.panasonic.com](mailto:sales@nz.panasonic.com)

**Panasonic**





## Challenger10™ Now available



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

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

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

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

Now available at your local Hillsec branch.



For all product information visit  
[www.hillsec.co.nz](http://www.hillsec.co.nz)

## Massive storage cost savings\*

That's the Quasar advantage!



dv<sup>tel</sup>

The Quasar HD IP camera series delivers high quality video at massively reduced storage requirements.

Save on costs, not quality! It's **WINNING JOBS** now!

\*Contact our branch to find out how.



For all product information visit  
[www.hillsec.co.nz](http://www.hillsec.co.nz)



## VSW8041

Industrial PoE+ Gigabit Ethernet Switch  
4-port PoE+ 10/100/1000BaseT + 1-port  
Gigabit SFP open slot



The Vidipac VSW 8041 Industrial PoE Gigabit Ethernet Switch (4-port PoE+ 10/100/1000BaseT + 1-port Gigabit SFP open slot) is designed for harsh and demanding network environments.

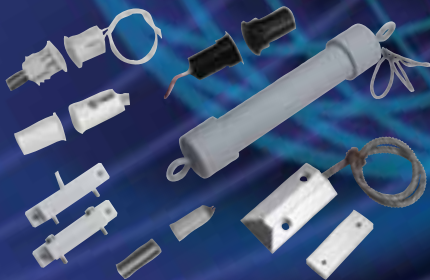
### KEY FEATURES

- Rigid Aluminum Case
- Broadcast Storm Control
- -20 to 70°C Operating Temperature
- DIN-Rail Kit
- Link Loss Forwarding Technology
- Redundant Power Inputs
- Power Reverse and Over Current Protection
- High degree of vibration

Now available at your local Hillsec branch.



For all product information visit  
[www.hillsec.co.nz](http://www.hillsec.co.nz)



## total reed switch solutions from Flair

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

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

Flair reeds from Loktronic:  
an unbeatable combination.



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



## Power supply cabinets

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

Designed, tested and  
produced in New Zealand.



Loktronic 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](http://www.loktronic.co.nz)

## Loktronic Power distribution module



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

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

### Comprises

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

Designed, tested and  
produced in New Zealand.



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

# fired up protection

**ViTECH**

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



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

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



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

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



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

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



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

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

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



**STI-RP-WS-11/CN** Ref. 720-052W  
Resettable call point surface mount and flush, DPDT. Positive activation mimics the feel of breaking glass. Visible warning flag confirms activation. Simple key to reset operating element - no broken glass.

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

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



**STI-RP-RS-02/CN** Ref. 720-058  
Resettable call point surface mount and flush, SPDT. Positive activation mimics the feel of breaking glass. Visible warning flag confirms activation. Simple key to reset operating element - no broken glass.

**STI-6255** Ref. 720-042

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



**STI-6720** Ref. 720-047  
Break Glass Stopper. Keys under plexiglas. Protects emergency keys from inappropriate use. Keys remain visible. Fast, easy installation. Simple, inexpensive plexiglas. 3 year guarantee against breakage of the ABS housing within normal use.



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



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



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



ViTech products are designed and produced in New Zealand.

**Loktronic**

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

