

February/March 2014

ISSN 1175/2149

# NZSecurity

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

## Hikvision & Atlas Gentec

making big moves in the New Zealand security market!

## Technology, Privacy

raise the bar on public safety surveillance project

## Seamless standards

enable plug-in surveillance network

## Zone Technology

appointed Aiphone "Key reseller"

## Reputation Management

defending against cyber threats and negative online content

## Smoke Detectors

trigger compliance overkill claim

**Loktronic**

SECURITY • TECHNOLOGY • RELIABILITY

# HOLD ON A MINUTE

## ...OR AN UNRIVALLED 10+ YEARS!

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



**PLAY IT SAFE AND LOCK IN**  
Loktronic quality, every time



FDH40S: Standard, floor mounted



FDH40SS: Flush mounted



FDH40SS: Surface mounted



**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)

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

\*Standard terms & conditions of sale apply.



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

## Introducing Bosch Starlight HD cameras.



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

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



**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

## 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.

## April/May 2014

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

## June-July

Wholesalers and Manufacturers  
Perimeter Protection, Alarms, ID  
Management

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

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

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

**Loktronic**

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

# CONTENTS

## Security

- 6 Hikvision\Atlas Gentech making big moves in the New Zealand security market!
- 8 Hikvision's Smart IP Cameras
- 10 Safety and welfare at the heart of security in fun central
- 14 New surveillance cameras have eyes on everything
- 16 Technology, privacy, raise bar on public safety surveillance project
- 22 Seamless standards enable plug-in surveillance network
- 26 Reputation Management:  
defending against cyber threats and negative online content
- 28 Zone Technology appointed Aiphone "Key Reseller"
- 30 Mining your surveillance video for real-time business intelligence
- 32 Embracing and Leading Change In the Access Control Infrastructure
- 36 Can an employer be held accountable for the unforeseeable?
- 38 Africa by night
- 40 Good days and Bad days are a fact of life
- 41 New Zealand security qualifications review gets underway
- 42 Office building security: A complete approach
- 46 Open but invisibly secure
- 54 Product Showcase

## Fire

- 48 Smoke detectors trigger compliance overkill claim
- 52 Offshore interest in emergency messaging system

## Associations



**[www.NewZealandSecurity.co.nz](http://www.NewZealandSecurity.co.nz)**



**Make sure the bad doesn't happen  
so the good can. Anywhere. Anytime.**



When you're responsible for the safety, security and everyday function of a big city, you have your hands full making sure the bad doesn't happen so the good can. At Axis, our deep experience in city surveillance gives us invaluable insight into the complexity of what you're facing every minute of every day.

That's why you can rely on Axis city surveillance solutions for dependable, crystal-clear HDTV video in real time anywhere you need it.

It's easy to coordinate your whole surveillance system centrally — and even share live video. Plus, as the world leader in network video, rest assured Axis brings you a future-proof solution that's ready for today's smart technology as well as tomorrow's.

Axis city surveillance solutions — securing everyday life.

Visit [www.axis.com/citysurveillance](http://www.axis.com/citysurveillance) or send an email to [contact-sap@axis.com](mailto:contact-sap@axis.com) for more info.



HDTV quality • Excellent zooming capabilities • Rugged outdoor cameras  
• Vandal-resistant • Sharable live video • Future-proof

**AXIS**  
COMMUNICATIONS

Distributed by:

**CHANNELTEN**  
SURVEILLANCE SOLUTIONS

**Hills**  
Electronic Security  
New Zealand

# HikVision & Atlas Gentech making big moves in the New Zealand security market!

---

With an annual turnover in excess of US\$1.16 Billion and a combined staff of 8000 people (3000 of which are dedicated to R & D), HIKVISION can afford to choose its partners carefully and with some expectation.

This is why they chose to run with Atlas Gentech in New Zealand as their exclusive distributor. Both companies share common values built primarily on trust, support, innovation and commitment.

There is no doubt if you talk to anyone associated with the world CCTV market that the big mover in the industry over the past few years is HIKVISION.

Already recognised as the largest manufacturer of cameras and DVRs, HIKVISION have invested heavily into IP Solutions and are really pushing their name to the top of some very big trees.

More and more HIK product is being accepted and in fact specified into Commercial and Industrial applications, which may not have been the fact 2 years ago.

This is completely attributable to HIK's dedicated commitment to produce quality, feature rich product at very competitive pricing.

No longer can European and Japanese manufacturers expect to take the cream projects due to past reputations. HIK VISION happily put their product forward to compare and compete with anyone with a quiet confidence.

With more and more of the local market moving towards IP CCTV Solutions with full 1080P HD quality images and recording a prerequisite. HIKVISION and Atlas Gentech are poised to aggressively compete in and dominate this market.



*Hikvision DS-2DF7286-A series  
IR High Resolution Smart Speed Dome*

The introduction of IP Plug'n'Play Network Video Recorders and associated IP 720P and 1080P cameras have made the transition from the older analogue products to full IP much more bearable as it takes a lot of the heartache out of the set up. With self enrolling cameras and PoE ports built into the recorders and an on-board wizard making programming a 5 step mouse click operation.

Recognised as an area with huge growth potential, HIKVISION have recently set up an office in Sydney equipped with 4 local staff including 2 engineers to help foster the fast growing name of HIKVISION in both the New Zealand and Australian markets.

This factory representation will be invaluable working alongside Atlas Gentech in the New Zealand market to help foster and grow this impressive company and their amazing products.



*Blue Penguins arriving in Friendly Bay at night  
Photo supplied by the Oamaru Blue Penguin Colony*



# Hikvision protects the Oamaru Blue Penguin Colony



## Oamaru Blue Penguin Colony

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

### Situation

To create a "viewing experience" for the public by updating existing analogue system.

### Hikvision CCTV Solution

Hikvision is the world's largest supplier of video surveillance products and solutions. The company specializes in video surveillance technology, as well as designing and manufacturing a full-line of innovative CCTV and video surveillance products. Since its inception in 2001, Hikvision has quickly achieved a leading worldwide market position in the security industry.

### Hikvision Products

- Hikvision DS-9016HFI-ST 16 Channel Hybrid DVR
- Hikvision DS-2CD752MF-FBIR 2MP Outdoor Vandal Proof IR Domes
- Hikvision DS-2CD7153-E 2MP Outdoor Vandal Proof Domes
- Hikvision DS-2DF1-783 2MP Outdoor PTZ Camera with 80m IR LED arrays

### MorComm Systems Limited (Installer)

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

MorComm Systems Limited is a locally owned company operating in Oamaru since 1997.

Owners Ian and Shirley Morris lead an expert team of sales people and technicians, ensuring you receive the correct advice and technical assistance to meet your requirements.



Hikvision CCTV is distributed through NZ by:

**Atlas Gentech (NZ) Limited**  
Freephone 0800 732 637  
[marketing@atlasgentech.co.nz](mailto:marketing@atlasgentech.co.nz)  
[www.atlasgentech.co.nz](http://www.atlasgentech.co.nz)

Enhancing the viewing experience has taken on a new meaning at Friendly Bay, in Oamaru, with the installation of the Hikvision CCTV solution—installed by Mike Balcombe of Morcomm Systems.

The colony began when a small number of blue penguins started nesting in a rock quarry area at the edge of Oamaru Harbour in the early 1990s. Today, it is Oamaru's largest tourist attraction, with over 75,000 visitors per year.

There is a boardwalk where the public can wander past nest boxes to a building where they can view the 'nest cams' on a 50" plasma screen as well as on iPads using the IVMS-4500 application. They also have viewing shots next to the nest boxes under the building.

The old analogue cameras have been added onto the new Hikvision 16 Channel Hybrid DVR and had also upgraded to the Hikvision Outdoor Vandal Domes and PTZ as soon as they saw the improved image quality.

Free Wi-Fi has also been installed, with time and data limits, covering the Friendly Bay and Steampunk playground area.

Harbour Project manager Rex Stringer said the security cameras had been installed by the penguin colony to monitor the Holmes Wharf blue penguin reserve, but was also providing coverage for the Friendly Bay and new playground/Marine Parade area, with police already using it to help them investigate two incidents.

The Hikvision cameras can provide night time infrared footage as well as conventional daytime footage (as featured below).



# Hikvision's Smart IP Cameras

As video surveillance continues to incorporate IP technology into their products, security manufacturers are now considering how “SMART” technology can enrich their own product lines and strengthen product competitiveness. Hikvision is prepared to meet this latest trend with the introduction of a professional 4-line IP camera range, which aims to revolutionize the surveillance market by offering a kit of “SMART” features.

“Smart is the latest concept which aims to bring video surveillance into every aspect of professional, intelligent, efficient, and convenient surveillance. Enriched with Smart technologies - such as Smart Codec, Smart Detection and Smart Control - Hikvision Smart IP cameras are specifically designed to deliver this concept to the market and convey the idea of smart security,” noted Keen Yao, International Marketing Director at Hikvision.

## Smart on Bandwidth and Storage Utilization

Incorporated with an advanced codec algorithm, Hikvision's 4-line smart IP cameras deliver images at a very low bit rate without compromising on image quality. Compared to traditional cameras, these Hikvision 4-line cameras can boost image quality up-to 30% when under a 2Mbps bit rate / 720p resolution mode. This significantly minimizes the system's load and storage requirements.

4-line smart IP cameras also support ROI (Region of Interest) codec. This allows the cameras to decrease non-ROI's image quality to save on maximum bandwidth and storage. Additionally, these ROI's will be transmitted with better detail and image quality under identical bit rate streaming conditions.

In vertically-shaped areas (such as corridors or hallways), the camera's horizontal-shaped image may result in pixel waste. However, Hikvision 4-line smart IP cameras address this problem by utilizing a “Rotate Mode,” which creates a vertically-oriented video feed from the



*Hikvision 4 Line Smart IP Camera series*

camera. This further maximizes image quality while concurrently eliminating bandwidth and storage waste. As well, triple streaming is supported to perform live monitoring with up to three independent streams.

## Smart on Image Quality Delivery

Hikvision 4-line smart IP cameras bring imaging to a new level with the help of defogging technology, high frame rate, smart IR, WDR technology, starlight-level low-light capability, and much more.

Through an image correction algorithm, defogging noticeably improves image clarity in poor weather conditions, such as rain or fog.

## In order to meet various applications

where image detail is critically important, Hikvision's 4-line smart IP cameras offer an ultra-high frame rate of 60fps in HD or Full HD resolution. This results in detailed and excellent image quality. Meanwhile, the improved Smart IR function allows IR strength adjustment and better visibility for the specific requirements of an application.

## Smart on User Convenience

Hikvision 4-line smart IP cameras are equipped with various industry-leading technologies for user convenience. Of

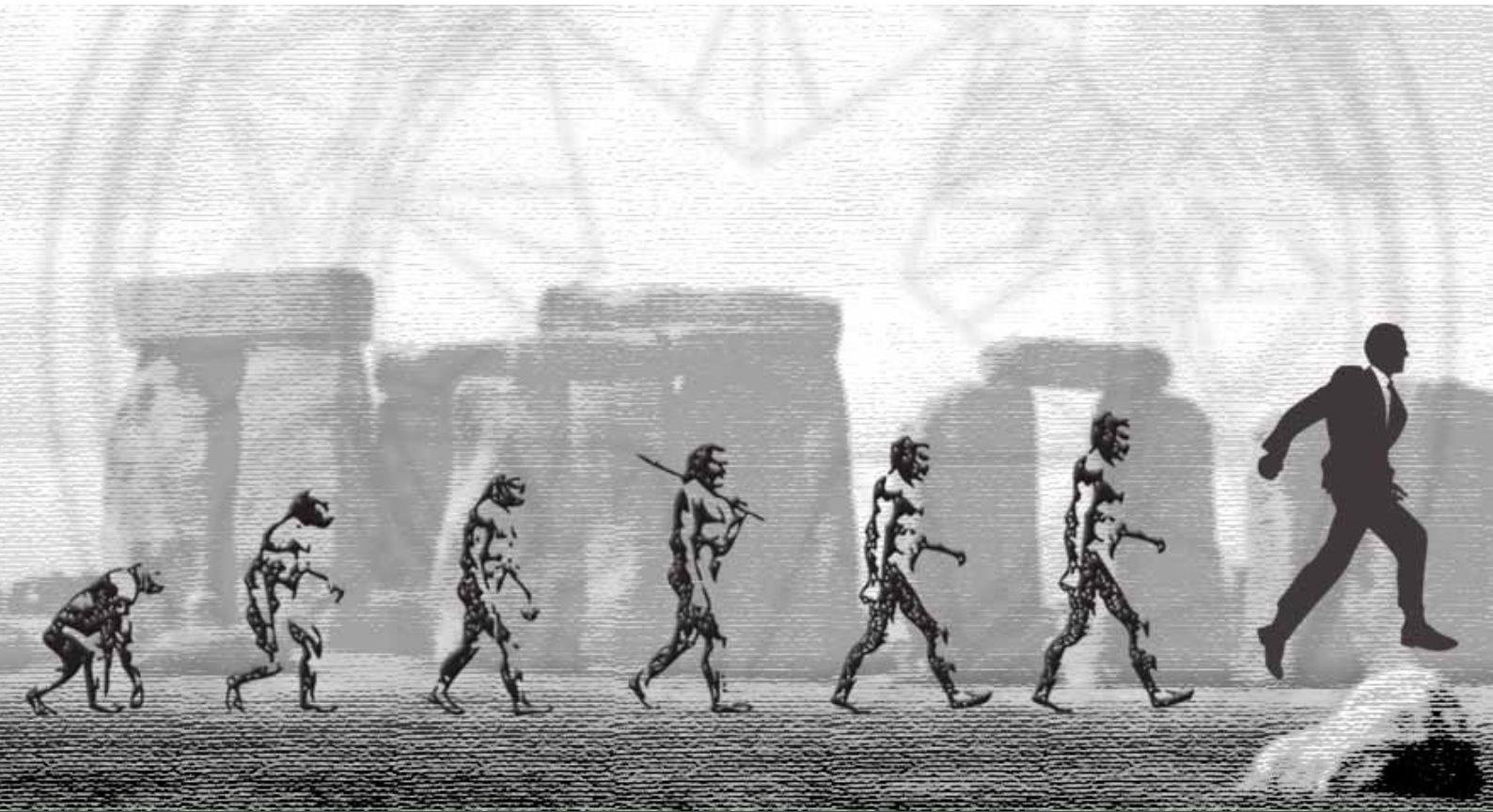
particular note is the Auto Focus feature which allows cameras to focus the image automatically when there are changes within the field of view.

These models come with Intelligent Video Analytics to detect activity by various means such as Facial Detection which enables the camera to accurately detect human faces, while Intrusion Detection helps the camera to detect moving objects within a predefined area of interest. However, both features make it possible to automatically trigger an alarm and event recording simultaneously. Audio Detection gives users another tool to analyse local sound and trigger an alarm based on these parameters. Additionally, this tool can filter out background noise interference to help avoid false alarms.

In the event of an issue relating to storage, network connection, lens redirection, defocus, or tampering, built-in VQD (Video Quality Detection) technology allows 4-line cameras to automatically self-diagnose and trigger an alarm accordingly.

Hikvision's 4-line Smart IP cameras can be coupled with existing Hikvision Smart PTZ domes, storage devices, and video management software to deliver a truly vivid Smart solution for professional applications.





## THE HIKVISION (R)EVOLUTION



Since its inception in 2001, Hikvision has evolved at an extraordinary rate and has been recognized as the world's largest supplier of video surveillance products and solutions since 2012 (IHS Report).

Hikvision today has the world's largest R&D team, with over 2800 engineers, and state-of-art manufacturing facilities; both allow Hikvision's customers the benefit of world-class products designed with cutting-edge technology. As a further commitment to its customers, Hikvision annually reinvests 7% of its revenue into R&D for continued product innovation and improvement. That equates to over \$80million dollars spent on R&D in 2013.

With sales in over 100 countries and offices around the world, Hikvision is opening a new office in Sydney in February 2014, providing support and service across the Oceania region.

If you want to be part of the (r)evolution and find out why the world is turning to Hikvision for its CCTV solutions, please contact Atlas Gentech, our official New Zealand distributor.



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

#### Headquarters

Tel: +86-571-8807-5998  
Email: [overseasbusiness@hikvision.com](mailto:overseasbusiness@hikvision.com)

#### Hikvision Australia Pty Ltd

Unit 14a, 2 Eden Park Dr  
Macquarie Park NSW 2113  
Email: [salesau@hikvision.com](mailto:salesau@hikvision.com)



**ATLAS GENTECH**  
DATA COMMUNICATIONS SECURITY

**Atlas Gentech (NZ) Limited**  
Freephone 0800 732 637  
[www.atlasgentech.co.nz](http://www.atlasgentech.co.nz)  
[orders@atlasgentech.co.nz](mailto:orders@atlasgentech.co.nz)

**Auckland**  
76 Carbine Road,  
Mt Wellington  
Tel 09 574 2700

**Wellington**  
Unit 5, 25 Centennial Highway,  
Ngauranga Gorge  
Tel 04 477 9142

**Christchurch**  
112 Wordsworth Street,  
Sydenham  
Tel 03 379 7926

#### Stay connected with us

LinkedIn: <http://www.linkedin.com/company/atlas-gentech-nz-ltd>  
Twitter: <https://twitter.com/Atlasgentech>

# Safety and welfare at the heart of security in fun central

The big city can be a cold, unfeeling and downright dangerous place. But within that, places for fun and entertainment can be a beacon of light. Keeping that beacon bright is a big job.

Welfare is a word you don't often see associated with the world of professional security services. In our series on high profile security industry people, it is doubtful we will find an individual with a role as wide and varied; as all-encompassing yet as strictly bound by regulation as our subject this month.

As well as being responsible for the security of one of the country's most high profile businesses, he has the added responsibility for a daily influx of some 16,000 people. And that is a different 16,000 from yesterday... and from tomorrow. These visitors won't know it, but their welfare and safety is of vital importance to one man and to the team he manages.



Junior Toleafoa is the personable but highly professional security and host responsibility manager at Sky City Auckland, the massive gaming, entertainment, dining, accommodation and conference precinct that includes the iconic Sky Tower. Visitors to the complex are looked after by 3,500 Sky City employees. As Junior tells us, "We are bigger than a small town like Tokoroa. Broadly speaking security here is tasked with keeping the people and the place safe."

The fact that Junior reports directly to Sky City general counsel and company secretary, Peter Treacy is an indicator as to where security services and issues sit in company structure and philosophy. Sky City Entertainment Group Limited operates monopoly casinos in New Zealand (Auckland, Hamilton and Queenstown) and Australia (Adelaide and Darwin), alongside a variety of industry-leading restaurants and bars, luxury hotels and convention centres.

The Auckland operation is the flagship of the business. That means a 24 hour casino with 1,600 gaming machines and over 100 gaming tables, including various VIP gaming areas and services. Added to this core are two hotels, 14 restaurants, eight bars, a convention centre with 21 function rooms, a 700 seat theatre and, of course, the Sky Tower, at 328 metres high, the tallest structure in New Zealand.

The company's philosophy states; "We aim to provide the best possible gaming and entertainment experiences for our customers, and deliver healthy long-term returns to our shareholders."

Junior's job is to make sure they can deliver on that statement. "We operate in a highly regulated and compliance focussed environment with daily, monthly and annual reporting requirements to the Department of Internal Affairs who regulate us," says Junior. "The Gambling Act and Sale of Liquor Act are the two key pieces of legislation that have helped influence the way our security operation is constructed."

The other regional properties at Hamilton and Queenstown and the two in Australia operate their own on-site security teams based on a company-wide model. But Auckland is the biggest. In total there is a 100 staff in the Auckland security team under Junior's management. From time to time they utilise external security providers to assist with events outside of the core gaming areas such as New Years Eve celebrations, Rugby World Cup and other major activities.

Junior's security personnel break down into four teams of security officers with 16 individuals per team. Each team has a manager and two assistant managers. Within each team, the manager plus at least two officers are trained in advanced first aid. Feedback from customers has been extremely positive about the Sky City security team's reactions to medical situations of all varieties. Their abilities and response times are second to none and something Junior is justifiably proud of.

The teams work seven-to-seven 12 hour shifts with 24 hour breaks in between. Their duties vary widely. In addition to the welfare of their daily influx of visitors,



# What is in your security platform's DNA?



**Security  
Center**

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

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

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

Video Surveillance | Access Control | Automatic Number-Plate Recognition

For more information



**Open  
Platform  
Systems**

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

Telephone: +64 9 927 7614  
Mobile: +64 21 970962  
Email: [jason@opsystems.co.nz](mailto:jason@opsystems.co.nz)  
Website: [opsystems.com.au](http://opsystems.com.au)

Innovative Solutions

**Genetec**



these duties can include cash escorts, the so-called 'chip runs,' and a range of frequent 'static patrols,' rovers in the car parking facilities and other environs, and sometimes through the gaming halls.

A surveillance team, which is separate to the security operation, provides comprehensive CCTV support.

As well as the teams, Junior is also responsible for a separate security adviser and projects manager, an investigator, a security manager, a security analyst and other administrative personnel managing the lost and found, access and key management.

Trend analysis is very important for Junior and his team. It helps them to identify patterns and pre-empt undesirable activities by turning intelligence into a picture that helps build better strategies.

The host responsibility part of Junior's job designation is also something Sky City takes very seriously. Its Host Responsibility Programme, which is required by law, is described as representing 'a new New Zealand, and international, standard in harm prevention and minimisation for New Zealand and internationally.' The casino is responsible to the Gambling Commission for adherence to the terms of the licence and to the Department of Internal Affairs as regulator for its enforcement.

Junior is responsible for implementing his part of Sky City's programme which contains a wide range of initiatives designed to ensure guests enjoy a safe and responsible gaming environment. There is training for all staff in the responsible service of alcohol and in problem

gambling awareness and the responsible provision of gambling, including taking all practicable steps to ensure that anyone under 20 years of age is not allowed in the gaming areas.

When employing new staff, Junior looks for people with experience in the casino industry but is also welcoming to newcomers. A Certificate of Approval issued under the Gambling Act is required. Internal training is extensive and newcomers work under six to eight weeks of guidance from an experienced officer. All officers are encouraged to complete the NZQA certification in casino security. The 12 month course is not compulsory but officers are incentivised to complete it. There is also refresher training, usually on an annual basis.

Some of the casino's security staff finds their future in pursuing a career with the Police, benefiting from the encouragement to widen skills. In saying that, a number of the team have been with the company since day one, some 18 years ago.

It is obvious that in an industry all about people and with such a huge influx of visitors each day, the corresponding protection and security is also largely about people too. But technology today is vital in any large security situation. Junior says, "In regards to technology we use access systems, information reporting and retrieval systems which are standard issue across the casino industry. In other words, we don't have all the 'magical' technology TV cop shows have invented."

But you can bet that they get the job done.

Particularly valuable has been a software programme known as

i-Track.Net. This simple-to-use online application enables organisations to track and manage activities, tasks, projects and contacts. It is an adaptable tool that can be used in a wide variety of situations involving planning, tracking or managing information or workflows. Junior is using it largely for incident reporting, pass tracking and managing a large lost-and-found service. Its success has garnered interest from other large organisations around New Zealand.

Junior has a proud Samoan heritage, his parents coming to New Zealand in the early 1950's. He served for some 20 years with the NZ Police, starting as a cadet in 1977 and leaving as the sergeant in charge at the Mt Roskill station. He has been at Sky City for 16 years now in various leadership roles; in his current role since early 2008.

His is an ever-changing environment. With Sky City's impending development of the \$402 million International Convention Centre his role looks certain to change even further. Recent changes to legislation will extend Sky City's Auckland casino licence to 2048 and provides for an increase in gaming product and other gaming concessions; 230 gaming machines, 40 gaming tables, a further 12 gaming tables that can be substituted for 20 automated table game terminals, the introduction of cashless card-based gaming, the extension of 'Ticket In/Ticket Out' technology and at least 780 new car parks.

As the agreement also includes introducing further and additional host responsibility measures, it is probably a safe bet that Junior will have plenty on his plate for some time to come.

## 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.



# New surveillance cameras have eyes on everything

Dallmeier's leading edge multi-focal Panomera surveillance cameras were put through their paces at a number of demonstration sites around the country over the past year, including during the March 2013 Blues and Crusaders game at Eden Park, Auckland.

Eden Park has many CCTV cameras which provide full coverage of the stands, car parks and other areas.

Management were shown that a Panomera installation could replace many of those cameras. Through the demonstration management saw the potential for this technology to enhance existing security systems.

The Panomera camera range, from German manufacturer Dallmeier, distributed by Mt Wellington-based C.R. Kennedy New Zealand Ltd, can record constantly in real-time up to 25 frames per second (fps) and is capable of 68 Megapixels resolution, enabling the operator to zoom in on individual or a group of potential troublemakers while still recording the entire crowd.

The three Panomera cameras currently on the market are not limited to a standard 16:9 or 4:3 aspect ratio view, they can have any combination of sensors to cover an area including wide horizontal strip monitoring for airports and stadiums for example, or vertical strip monitoring of tall buildings, elevators or open lift shafts and other irregular areas.

A Panomera system can combine the overall view with simultaneous top detail resolution so that distant objects can be

displayed in the same resolution as those in the foreground. If an issue is spotted in the crowd for example, images can be captured and sent to the mobile device of a security guard on the ground.

Many towns and cities around the world are using tailor made CCTV/IP video surveillance solutions from Dallmeier to

protect and safeguard their citizens and deter crime and vandalism.

The greatest demand is for compatible and flexible system architecture to enable easy integration into existing security management systems and to ensure a high picture quality output with ease of operation.





Open Platform VMS by AxxonSoft



SolidStore



Micro-Module architecture



MomentQuest2



Interactive 3D Map



Time Compressor



Video Analytics



Information boards



User comments



Map with embedded live video thumbnails



Saving and quick access to queries for MomentQuest2 forensic search



OpenStreetMap integration



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

axxon  
Experience The Next®

# Technology, privacy, raise bar on public safety surveillance project

Keith Newman asks who's watching who and why, and who's watching the watchers?

Privacy concerns, the fear of government agencies spying on people and the growing sophistication of technology once considered the domain of science fiction, may be among the greatest obstacles facing plans for a seamless nationwide approach to CCTV surveillance.

The Auckland's Video Surveillance (AVS) project, currently the subject of a series of audits, inventories and the creation of technical, security and privacy guidelines, is being viewed as a template for integrating public and private CCTV systems.

However, in the wake of the Dotcom debacle, the Tuhoe terrorism claims, Copyright and Government Communications and Security Bureau (GSCB) law changes and allegations the US National Security Agency (NSA) is spying on us, Kiwis are on high alert about who's watching who and their rights in the digital age.

Auckland City Council policy analyst and AVS project leader Dr Gillian Stewart says the global atmosphere of suspicion over spying and privacy means that "ethical leadership" is essential and public perception needs to be informed, with

the right debates and surveys to measure people's attitudes to CCTV as a safety tool.

The group, working closely with the privacy commissioner and 21 Auckland community boards since November 2012, is completing guidelines on how CCTV footage is to be stored and used and who can view it. The Crime Prevention Partnership Forum led by the NZ Police is also engaging in conversations with "the right people".

Dr Stewart says it's imperative all the security and privacy issues are covered off and all sectors are continually informed so there's little chance of anyone "scuppering the works".

While there are strong security industry codes of practice in place and technical standards are now being peer reviewed, the battle for public perception may be just beginning.

Thomas Beagle, spokesperson with the Tech Liberty group has a range of concerns about expanded video surveillance, including whether it can actually create safer communities.

Tech Liberty kicked off in 2000, lobbying to ensure our laws kept pace with civil liberties in the digital age, and wants to be involved in future discussions with the AVS group.

An early cause was protesting Section 92a of the Copyright Act which essentially said you were assumed to be guilty if someone accused you of copyright infringement. "We asked, what happened to due process and the right



*Surveillance technology is moving so rapidly that the potential for seamless camera connectivity is starting to look like a scene from the TV series Person of Interest*



# SEEING IS BELIEVING

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



## WV-SW598 NETWORK CAMERA

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



i-PRO  
SmartHD

MEGA SuperDynamic



IP66  
standard

ONVIF

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

### Droplet formation prevention

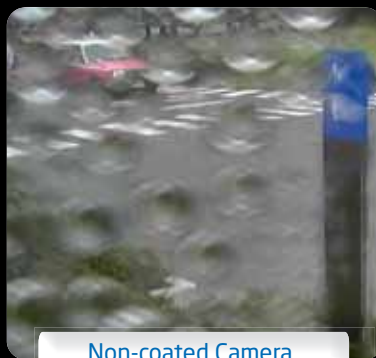
Visibility is maintained due to droplet prevention coating.

### Advanced coating technology

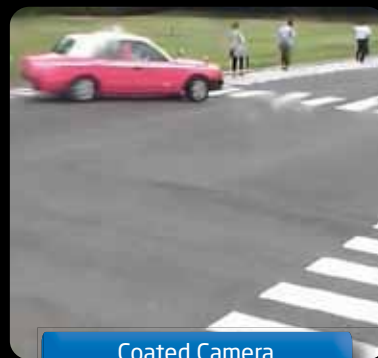
Long-term performance due to advanced coating technology.

### Reduced Dirt

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



Non-coated Camera



Coated Camera

to a trial. Guilt on accusation is not how our system works and of course that got changed.”

Beagle says the potential to integrate camera footage with cellphone tracking and “other bits of information people leave around when using eftpos machines or bus cards,” complicates matters.

If you are managing or monitoring a large number of cameras and start adding facial recognition, gait recognition; a biometric technology that can help identify people by the way they walk, and begin following an individual, when does that come under the Search and Surveillance Act 2012?

Basically he asks, if you are following someone from camera to camera, “is that an electronic tracking system and do I need a warrant?”

Greg Watts CEO of the New Zealand Security Association (NZSA) who’s chairing the AVS technical workgroup agrees the technical side, including the creation of standards for interconnectivity, impacts on the discussion of privacy.

He insists this is not a prelude to Big Brother but specific to creating safer communities. “This is not something we are forcing on people, there are options all the way.”

### Technology game changers

However, the issues do become more complex with growing innovation in surveillance technology that enables smarter and more rapid management of footage collected from interconnected networks of digital and analogue cameras.



Thomas Beagle, Tech Liberty spokesperson

---

*“This goes beyond privacy to civil liberty. New Zealanders are not famous for standing up and opposing things so the idea that the government can watch your every move is quite a worry in the medium to long term.”*

---

Thomas Beagle, Tech Liberty spokesperson

High definition cameras (16 Megapixel) in the United Kingdom, for example, can isolate a face from a crowd at 800m distance, and using facial recognition can map that against someone sought by the police.

Worldwide video surveillance equipment is expected to grow 80% over the next five years with network video gear making up 57% of that growth despite the market being described as fragmented with many vendors continually offering network video products for security purposes.

According to market research firm HIS in its June 2013 report, the industry, currently valued at over \$US13 billion, is poised to rocket ahead to \$23.2 billion by 2017.

Locally there appears to be strong interest from a number of organisations and venues looking at deploying the latest IP-based digital surveillance technology and management systems.

An industry insider told *NZ Security* this year will see incredible advances, particularly through the data management or data mining capabilities of computer-based video management systems.

He says the smart drill down technology now hitting the market is taking us closer to the scenario offered on the TV series *Person of Interest* where people of interest can be followed through a series of public and private cameras and camera networks.

These can follow specific images through a security system to track a person, a vehicle or determine for example when a bag went missing.

This technology enables you to track a person from the time they enter a

building and follow them wherever they go. “You can grab images from several cameras and make a 3D image, isolate a square area and ask it to look for a blue van of a particular size then have all relevant images from the past 24-hours come up on screen without any processing or having to go through hours of footage.”

For example the Axon Next VMS launched here in January uses advanced video analytics, time compression and metadata search, licence plate and facial recognition and ‘tag and track’ features across an unlimited number of cameras, servers, workstations and remote clients.

### Paranoia mentality growing

Thomas Beagle of Tech Liberty, says it’s sad that society has already changed to the degree that people no longer expect privacy in a mall or on the street, and in the interests of safer communities will be asked to give up even more.

As we get more power to track people and the expectation of being watched increases, the tendency is that people modify their behaviour to avoid even the appearance of doing something wrong.

“This goes beyond privacy to civil liberty. New Zealanders are not famous for standing up and opposing things so the idea that the government can watch your every move is quite a worry in the medium to long term.”

For example, he says, since police began turning up at public protests taking photos of everyone, Government employees and people in respectable positions have become more reluctant to get involved.

“Political protests in New Zealand are seen as a highly protected form of freedom of speech or expression. It’s a core civil liberty and if you feel intimidated then people may limit even legal activities.”

And he says, you have to ask how much impact CCTV surveillance is actually having in reducing crime? “A big issue overseas is that they have so many cameras no-one can watch them all, and even when people do illegal things often no-one responds or there’s no manpower to follow it up.”

If it doesn’t make people feel safer or actually achieve anything, he wonders whether expanding surveillance may in some cases simply be a waste of time.

Beagle says close attention needs to be paid to who is monitoring and why. “What sort of checks are being done on those who monitor the cameras and what’s to stop them taking advantage

# ultimate reliability

for video surveillance storage.



**WD AV-GP**  
Video Storage

WD AV-GP hard drives with exclusive SilkStream™ technology deliver smooth, continuous digital video recording and playback in high-temperature, always-on video surveillance environments. With 24x7 reliability and ultra-cool operation, WD AV-GP gives you a clear advantage. Learn more at [wd.com](http://wd.com).

**absolutely™**



Western Digital, WD and the WD logo are registered trademarks of Western Digital Technologies, Inc. in the U.S. and other countries; Absolutely and SilkStream are trademarks of Western Digital Technologies, Inc. in the U.S. and other countries. Other marks may be mentioned herein that belong to other companies. Product specifications subject to change without notice. Picture shown may vary from actual product. © 2013 Western Digital Technologies, Inc. All rights reserved. 4178-705825-A00 April 2013



of that information, particularly if you have a number of cameras and can start following people around.”

### Wandering eyes an issue

Beagle asks who will have oversight of the operators to ensure they don't concentrate on the wrong thing? Checks on the British surveillance system for example showed, “a strange tendency for the cameras to follow big breasted women.”

A high profile local example of misuse of CCTV footage had its sequel in June 2012 when a bouncer at Queenstown's Base Bar found himself in court for downloading surveillance footage for his own personal use.

Bouncer Jonathan Dixon was charged with accessing a computer and deliberately obtaining property after he posted YouTube footage of England rugby team's captain Mike Tindall, husband of the Queen's granddaughter Zara Phillips, flirting with an old flame during the Rugby World Cup in 2011.

He took the footage from his place of employment with the intention of selling it to an English newspaper but the court was told, when that fell through he seemed satisfied with the notoriety of posting it on social media.

In April 2013, Dixon was found guilty by an Invercargill District Court jury of dishonestly accessing a computer and in September sentenced to four months' community detention and 300 hours' community service. He said he would appeal.

His defence lawyer made much of the culture around staff access to the bar's security system and computers, and Dixon's alleged belief that he was allowed to do what he did.

While staff viewed the footage of patron's antics for their entertainment, security guards were only allowed access



for security or liquor licensing reasons. There had been no written agreement or training on the use of the CCTV footage.

---

*“There's more accountability now than ever before with protocols and codes of practice in place. In the old days anyone could sit in a monitoring station, you can't legally do that today.”*

NZSA Chief Executive, Greg Watts

---

### Improving CCTV skills

The security industry will have an ongoing role in supporting end users, suppliers and manufacturers as part of the AVS project and the new minimum standards document will include advice on physical installation, quality, back-up, scheduled maintenance and training for those who monitor surveillance.

NZSA Chief Executive Greg Watts says there is clearly a need to ensure the right people monitor and access footage.

Recent legislation changes covering security guards, mean anyone at a CCTV monitoring station has to be fit for purpose and licensed with a certificate of approval (COA).

He says there's more accountability now than ever before with protocols and codes of practice in place. “In the old days anyone could sit in a monitoring station, you can't legally do that today.”

Currently a lot of premises have cameras that are inappropriately placed and not maintained. “We went into one office building for a meeting about technical standards and I noticed two cameras videoing panels on the ceiling.”

If people aren't adequately trained, Watts asks, “how can they set the parameters for what they're recording.”

AVS project leader Dr Gillian Stewart says the whole area is highly political and the value argument needs to be strong enough so the discussion doesn't become more complex than it needs to be.

Ultimately she says Auckland Council needs to ensure the public is informed, knows what their rights are and how to go about complaining. “The council are interested in the economic as well as the social and community safety aspects and public opinion matters so they need to have the right evidence-based information.”

She says the right balance needs to be struck between meeting the safety concerns and needs of the public and stakeholders in the Auckland project and “the big brother idea and the view that everyone's got CCTV and we should have more.”

Stewart says the whole issue of scoping and rolling out the project and taking on board privacy and related concerns is huge. “My problem is to document what we're actually doing and to make sure we're clear about the messages and what we need to be talking about.”

### Milestones:

**February 2014:** Minimum technical standards defined.

**February-May:** Stocktaking, testing, pilot programmes, guidelines defined.

**End of May:** Report on the state of Auckland public access CCTV due August: Research from pilot projects consolidated.

**August-November:** Agreement on strategic vision and partnerships.

**Oct 2014 - June 2015:** Auckland Council formal Long Term Plan (LTP) policy decision.

**Loktronic**

SECURITY • TECHNOLOGY • RELIABILITY

# *your* electromagnetic locking specialist!

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

**Standard features include:**

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

**Options include:**

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

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

**10**  
YEAR  
GUARANTEE



**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)



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

# Seamless standards enable plug-in surveillance network

By Keith Newman

A plan to seamlessly link Auckland's disparate CCTV cameras and networks as part of a safer communities project is currently being put through a series of pilot programmes to ensure core technical, security and management specifications are robust enough for a proposed regional roll out.

If the public can be convinced the benefits outweigh privacy concerns, thousands of traffic management cameras, those used in public places, council buildings, malls and businesses may be linked into a cohesive network, setting the tone for the rest of the country.

A stocktake is currently underway of all public places CCTV cameras and networks owned by Auckland Council,

---

*"If police were looking at criminal activity somewhere in the city it would be great if there was an opportunity to use surveillance to prevent that or catch those responsible."*

---

Greg Watts, Chief Executive of the NZSA who's chairing the AVS technical workstream.

---

being re-evaluated as various parties seek clarity on the way forward. At the heart of the debate is the ownership of cameras, the scope of the project, who pays who and the level of interconnection proposed.

Regardless the Auckland Council facilitated AVS team remains determined to develop a regional network whether it ends up being owned by AT or is a more collaborative effort to enable CCTV sharing.

"We've still got to work through all the legal and privacy aspects of sharing information but technically this work will make that possible," says Dr Stewart. Ultimately, she says, the proposed system would enable the various networks to "plug in like you would to the internet".



Dr Gillian Stewart, Auckland Video Surveillance (AVS) Project Leader

council controlled organisations (CCOs), Auckland Transport (AT) and those owned by business associations and communities to determine what's there, how the technology is working, who it connects to and how well it's functioning.

Auckland Video Surveillance (AVS) project leader Dr Gillian Stewart says the inventory data will be added to a secure interactive geographic information systems (GIS) register to ultimately allow police to have electronic access.

The register is being developed by the Auckland Safer City (ASC) network based around Auckland Transport (AT) efforts to converge CCTV cameras from seven previous local authorities into a single infrastructure.

The original goal was to use Auckland Transport's network as the basis for further development, although that's

## Strategic overview

AT is currently ramping up the capabilities of its own restricted access network, including investing in more robust infrastructure with telecommunications carriers to determine the best way to integrate copper, wireless and microwave links across the wider Auckland region.

After the stocktake exercise the AVS group will know the state of the various technologies, how interoperable the multiple VMS (video management systems) and networks are, and be in a position to be "more strategic about what needs to be upgraded and which systems to bring on".

The AVS project is underpinned by the New Zealand Security Association's (NZSA) Code of Practice and best practice security industry operational requirements (SOR) with legal, regulatory and privacy





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

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



frameworks being worked on concurrently.

A common technology standard for interconnection by all participating networks and cameras including those owned by shopping malls and small businesses is being firmed up ahead of a final peer review.

Greg Watts, the Chief Executive of the NZSA who's chairing the AVS technical workstream, says the objective is to create a futureproof system so industry, retail, NZ Police, councils and transport agencies in Auckland "and hopefully around country" can sign up.

He says the whole project is being driven by the desire for safer communities. "If police were looking at criminal activity somewhere in the city it would be great if there was an

*"We've still got to work through all the legal and privacy aspects of sharing information but technically this work will make that possible...it will enable the various networks to plug in like you would to the internet."*

Auckland Video Surveillance project leader, Dr Gillian Stewart

opportunity to use surveillance to prevent that or catch those responsible."

If surveillance from a retailer or a mall couldn't be accessed or downloaded or the data wasn't compatible with NZ Police systems for example, "it would seem to me that we're missing the point," says Watts.

Rather than having to download footage to a disc and courier it across town, he asks, why wouldn't the owners of premises use this new standard to connect to the grid and share information?

#### Best team and standards

Watts' team looked at Australian, British and Australian standards and those currently used by the NZ Police and has settled on what best suits the New Zealand environment.



# ITPLUS

YOUR TECHNOLOGY PARTNER

**Surveillance specialists with a complete range of CCTV products for distribution**

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

Telephone: 09 950 4940 • Unit 9A, 9-11, Laidlaw Way, East Tamaki, Auckland • Email: [info@itplus.co.nz](mailto:info@itplus.co.nz)

Included in the technical team are representative of Auckland Transport, Auckland City Council, NZ Police, systems integrators, and consultants from the NZSA and security professional group ASIS, technology distributors and manufacturers from across the country.

"I feel comfortable that we have a good representation of the best minds at the table to ensure we're not being draconian. They're all doing this because they believe in it and are not charging for their time and even paying for their own travel."

The Crime Prevention and Partnership Forum led by the NZ Police, including heads of the banks and private sector businesses, has also been working with the group on establishing minimum standards.

Once these have been adequately tested and determined to be "fit for purpose" a final document will be available for download for anyone wanting to use it as a guideline for what to install and how to configure systems to plug in to the wider network.

Watts says it's not a Ferrari specification with all the bells and whistles or something everyone will be forced to be part of. "That would defeat the purpose. We want this to be accessible to everyone from a single shopkeeper with a camera outside his store to local authorities."

In most cases it will work with existing technology, although "some cameras may require tweaking", and for others it may also provide an opportunity to upgrade from obsolete technology.

A number of lower cost technologies and cheaper brands can still deliver on the requirements. "We're not defining brands



Greg Watts, CEO of the  
NZ Security Association



so no one is influencing that benchmark."

Watts says he usually consults friends first when buying whiteware, for example, to see what product they recommend and how well it has worked for them. "Why recreate the wheel when some of the best minds in New Zealand have put together a standard."

Watts says the standard is to ensure that the technology delivers on the needs of stakeholders more effectively. "Central London surveillance has had an amazing impact on crime prevention and the same goes for New York. It's been said some of those technologies are too draconian and certainly they're too expensive unless you are the City of London."

### Not a Big Brother thing

He reiterates, "this is not a Big Brother thing"; there will be no central monitoring station. Police won't automatically have the right to access the various networks to monitor criminal activity. It will be based on discussion and agreement with each industry, retailer and sector to determine the level of connectivity.

A shopping mall for example might be happy for police to have access online in real time, only providing data to police if there is an incident or using their own people or an alarm company to monitor their systems, says Watts.

Dr Stewart says during the year a number of pilot programmes will test assumptions for users and owner-operators about what is possible and what the broader network will look like technologically.

Her group will define guidelines and test these on key projects; for example determining if the Parnell Business Association will go with CCTV coverage and whether there's any synergy with Newmarket where the contract for the existing system is up for renewal. "We want people to think outside their own silos."

The review will include council controlled cameras at the Auckland waterfront and at regional facilities such as event centres, the Zoo, Mt Eden and Mt Smart stadiums, art galleries and Auckland Council's eight public place cameras to see how those might be "integrated or rationalised".

It's planned that research from pilot projects will be consolidated and shared with other projects by August so decisions can be made about how the parties can work together. "It's a great opportunity that could easily be deployed elsewhere but first we've got to get the basics right," says Stewart.

A memorandum of understanding (MOU) has been signed with the NZ Police. "They have a very clear view. They're not going to start purchasing cameras but will probably purchase the supporting technology that allows them to gain access to live footage for staff on the street or in cars."

She says NZ Police are already reviewing most of their internal policies in relation to what we're doing with the view to this becoming national. "We've also got a huge piece of work with Local Government New Zealand (LGNZ) and government agencies which is a longer term strategy discussion."

Dr Stewart says the Auckland Council will also have to decide whether it should be investing in the CCTV game or whether it has a role in managing relationships between stakeholders and users or providing public information.

She says Auckland may end up gifting its public cameras to another party. "We could outsource this to Auckland Transport... We might not need an operational technician on staff."

The challenge now is balancing interests and responsibilities and defining roles. "There's a great amount of common consensus and goodwill about what the future could look like."



NEW FC-Series S



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



Compact D-Series

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

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

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

**Here's how:**



High contrast scene with standard AGC algorithm applied.



DDE applied – all targets can be observed simultaneously.



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



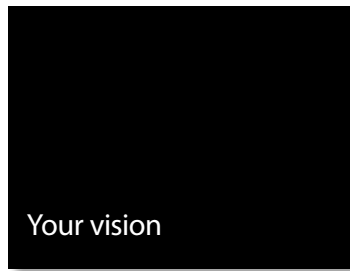
**Excellent Range** - FLIR thermal imaging cameras can detect targets several kilometres away.



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



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



Your vision

Thermal image without Wide Dynamic Range (WDR).



Thermal image

Thermal image with Wide Dynamic Range (WDR).

[www.flir.com](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)



# Reputation Management: defending against cyber threats and negative online content

The field of reputation management tells us that cyber threats facing businesses come in all shapes and sizes, including some you may not have thought of, from malicious attacks to poor customer reviews.

---

‘Reputation management’ is the practice of influencing the perceptions held by stakeholders of an organisation’s credibility and brand. It is a term that conjures up thoughts of spin-doctors, image consultants and style coaches - those anonymous PR folk who are paid to make public figures look good. But it is also something that business is increasingly taking very seriously - and particularly when it comes to data security and online presence.

Following major public sector data breaches in 2012, including the ACC spreadsheet breach and MSD kiosk breach, a TV One Colmar Brunton poll showed that 60% of New Zealanders didn’t trust government departments to protect their personal details. Similarly, the Ponemon Institute’s 2012 Consumer Study on Data Breach Notification found that 83% of respondents believed organizations that fail to protect their personal information are untrustworthy. Trust is critical for reputation. Customer distrust resulting from a major cyber attack or data breach can - and does - have a damaging impact on a business’ bottom-line.

But it’s not just cyber crime and data security failures that can be reputationally damaging to a business. Reputations are also be made or broken online in often less menacing yet just as powerful ways. Online competitor misrepresentation, slander campaigns, defamatory reviews, negative search

content and even a substandard online presence can damage customer confidence in a business’ brand and products.

The now critical role of the internet as a vehicle for virtual ‘word of mouth’ has fuelled the rapid rise of specialised online reputation management, or ORM. Managing reputations online involves various monitoring, social media and search engine optimisation (SEO) techniques to maximise positive perceptions of an organisation and its products and minimise negative perceptions. It’s about preventing fires and fighting them when they happen.

## Fire Fighting

According to the 2012 annual PwC, CIO and CSO survey of more than 9,600 global executives, respondents ranked the compromising of brand/reputation as the third biggest impact to business of security incidents. This placed reputation behind financial loss and intellectual property theft in terms of impact, but ahead of legal expose and loss of shareholder value.

A lot is at stake, but the faster a business can respond to an attack, the more they know about the issues being raised by their attackers, and their ability to respond credibly, the more likely they are to contain the impact. And the opposite also rings true. Revelations that members of the public could access confidential documents

from kiosks installed at Work and Income offices blew into a national scandal in 2012, resulting in major egg on face. What didn’t help was that the agency chose not to act after an informant had come forward seeking a cash reward prior to the issue becoming public.

According to the Ponemon data breach notification survey, 72% of consumers were disappointed in the way in which they were notified of the breach. Respondents felt that most notifications missed key facts, such as how the breach could affect them and their families, and protections that would be provided to minimize the harm. A significant proportion was sceptical of the notification, believing that key facts about the data breach were being hidden and that the message was being ‘sugar-coated’. Most alarming was the statistic that 54% of respondents dismissed the notification as junk mail, spam or a telemarketing call.

The solution? Timely, clear and accurate notification, even if all the facts or the full extent of the breach are not yet known. Regular updates can follow. Much reputational cudos may be salvaged by explaining the risks or harms likely resulting from the breach, disclosing all facts, not “sugar coating” the message, personalising the communication so it’s not mistaken for junk or spam, and minimising the use of technical or legal terms.

Quick and decisive action is also the mantra of ORM consultants when

it comes to reacting to reputational attacks online, such as competitor misrepresentation or a proliferation of negative search content. Reactive reputation management involves the relegation of harmful information in search engines as soon as possible after it appears, as well as publishing information refuting negative, inaccurate or malicious information in such a way that reputational damage is minimised.

### Fire Prevention

Although fire fighting is crucial when incidents occur, the key to managing reputation is preventing fires from igniting in the first place. It's about proactive management of one's name or brand. Managing a good reputation is far more cost-effective than trying to salvage a damaged reputation.

According to Ernst & Young's annual Global Information Security Survey 2013, only 17% of respondents indicated that their Information Security function fully meets the needs of their company. Competing priorities stretching limited investment capacity mean that many companies are spending less than they'd like to on information security. But as

EY New Zealand Information Security Leader, Ken Wallace, comments, the key question for Boards and executive teams for 2014 is, "do you want to address information security as a risk today or reactively address it as a major operational or brand issue tomorrow?"

Clearly, many businesses are baulking at the idea of directing limited funds into adequate cyber threat and data theft prevention, but in doing so they run the risk of incurring the far greater cost of cleaning up their reputations after an attack.

The 'act now, save later' principle advocated by IT security professionals also holds true for businesses protecting their reputations online. According to New Zealand reputation management company Fifteenminutes, "the skill is to be aware of what is being said about your organisation and to act quickly to head off potential issues before they pose a threat to your business."

Being on the front foot involves the regular monitoring of news, social networks, customer feedback, and online forums and review sites. Often, damage to a business' reputation may be happening without the knowledge of its management and staff.

Then there is also traditional consumer behaviour to consider. Negative customer experiences, for example, tend to result in negative reviews more often than positive experiences result in positive reviews. According to Auckland-based firm Statigik, "Even though a firm may deliver high quality customer service, clients must be invited to share positive stories."

It's also about quality controlling one's own content to ensure that it's not sending out the wrong messages to prospective customers. Lionel Stanbrook of Clement Reputation notes that, "whether it's fair or not, and whether we admit it or not, we judge companies and their managers by the words they use and the clarity they show." Many businesses out there are undermining their own reputations by maintaining an amateurish online presence and failing to use spell-check before publishing content.

There are many measures a business can implement to safeguard their reputation in cyberspace - some simple and inexpensive, some more complex and highly priced. Whatever the suite of measures one chooses, a truth of doing business today is that what happens in cyberspace does not stay in cyberspace.

# A Page out of the Reputation Management Textbook?

Reputation management companies claim to be the experts in advising clients on what they need to do to maximise the reputation of their brands and to minimise the damage when things go wrong. They advertise that they can prevent an embarrassing data breach from turning into a full-blown public relations nightmare.

So, how would a reputation management company respond if it became the unwitting victim of a cyber attack?

On Tuesday 30th April 2013, online reputation management service, Reputation.com, notified its customers that its website had suffered a security breach, exposing client data to an unknown attacker.

To have fallen victim to a hacking attack must have come as a worse-case scenario to a company whose own reputation is built on being the world leader in making businesses look their

best on the internet. With millions of users in more than 100 countries, there was much to lose.

The company reacted quickly, having detected the attack while it was still in progress. All customers were then notified by email, which advised that:

1. An attack had been detected and then stopped, and that hackers had gained access to customers' basic information.
2. The company had quickly begun investigating the attack while working with independent security experts.
3. Names, emails, addresses, and in some cases phone numbers, dates of birth and occupational information, had been accessed.
4. Other personal information had not been accessed.
5. The passwords had been effectively encrypted making it unlikely the hackers could decrypt it, but that

despite this the company had immediately changed the password of every user.

6. The company was offering a full year of free credit monitoring to customers who wished to monitor their financial info, and had established a confidential assistance line.

Industry experts lauded Reputation.com's response for its 'above and beyond' transparency, the detail with which it had alerted customers of the breach and - importantly - its solid security practices. A lack of these things could have produced an entirely different result.

Although Reputation.com's 'fire prevention' measures had failed to prevent the attack, they minimised its impact and allowed the company to react in a way that kept their reputation intact.

# Zone Technology appointed Aiphone “Key Reseller”



Audio Products Group Pty Ltd, the Australian and New Zealand distributor of the premium Aiphone range of intercom systems, is pleased to announce the appointment of Zone Technology Limited as a “Key Reseller” in New Zealand commencing in February 2014.

The appointment of Zone Technology will serve to strengthen Aiphone’s already strong market position in New Zealand and market leadership position both in Australia and internationally.

Zone Technology is a 100% New Zealand owned company with over 15 years experience in the security industry. With branches in Auckland, Wellington and Christchurch, Zone Technology is well placed to design, provide technical support and supply product for your residential and commercial intercom requirements nationwide.

Aiphone have earned a position of leadership by focusing on quality every step of the way. Through Aiphone’s 65 year commitment to Total Quality Management they are constantly seeking ways to improve products and processes. The result is a worldwide reputation for

technological advancements, a broad range of high quality products and most important, customer satisfaction.

Established in 1948 Aiphone has become the most respected and reliable brand of intercom systems in the world. Aiphone’s comprehensive range extends from entry level audio only systems, through high quality colour video residential systems, to multi-tenant apartment video and IP based commercial systems.

The Team at Zone Technology are pleased to have the reputation of the Aiphone brand as part of their quality portfolio of security products to support their growing customer base in the New Zealand market.

**ZoneTechnology**  
Your Security Supply Partner

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

**Email:** [sales@zonetechology.co.nz](mailto:sales@zonetechology.co.nz)  
**Website:** [www.zonetechology.co.nz](http://www.zonetechology.co.nz)



# Video and audio intercoms



Aiphone is the world's leading manufacturer of security intercom systems.

Aiphone's intercom range covers simple audio-only systems for single dwellings through to sophisticated video + audio systems for large commercial and apartment buildings.



## Apartments

- 16 entrances
- 500 apartments
- video or audio



## Single Homes

- stylish design
- easy to use
- video or audio



## Commercial

- IP or hard-wired
- video or audio
- remote door release

## Aiphone intercoms are ideal for...



Now available from



**Auckland**  
6/25 Airborne Rd  
Albany, Auckland  
Ph: 09 415 1500

**Wellington**  
35 Abel Smith St  
Te Aro, Wellington  
Ph: 04 803 3110

**Christchurch**  
Office 13, Level 2/ 225 High St  
Christchurch  
Ph: 03 365 1050



[sales@zonetechology.co.nz](mailto:sales@zonetechology.co.nz)

# Mining your surveillance video for real-time business intelligence

With the embedded analytics in network video cameras, you can garner real-time statistics to help you improve store layout and product placements and identify bottlenecks and dead areas on the floor.

By Dr. Jumbi Edulbehram

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

With the embedded analytics in network video cameras, you cannot only observe customer behaviour in-store, you can garner real-time statistics to help you improve store layout and product and display placements, and identify bottlenecks and dead areas on the floor. Unlike the hit-or-miss approach of customer surveys and mystery shoppers, network video gives you an accurate and unbiased report of the immediate situation and of changes over an extended period of time. You get a clear view of how customers move along the aisles, making it possible to optimise floor plans and merchandising strategies to drive your sales and profitability.

### Sharing Intelligence Across Channels

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

### Optimizing Floor Plan

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

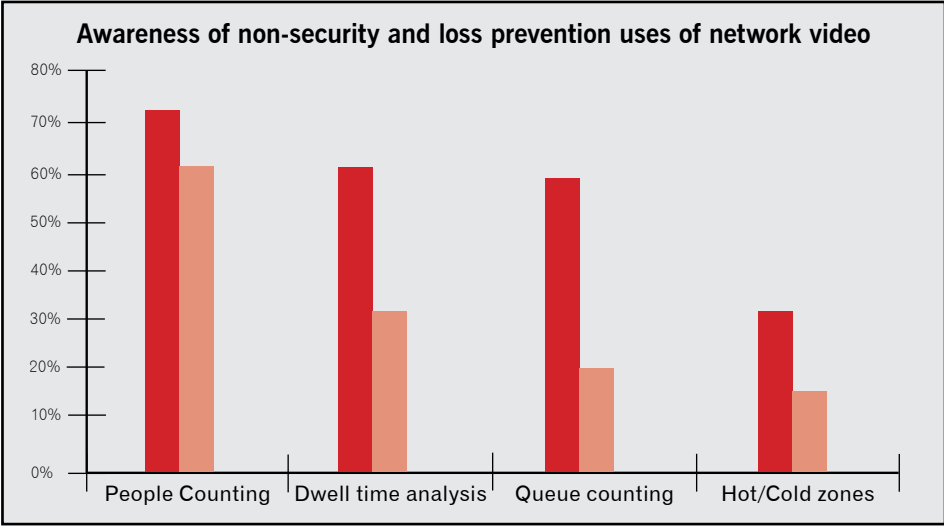
### Improving End Caps And Displays

Another way to leverage video intelligence in your retail operation is in the area of product placement and display strategies. Store managers can

record video of customer interactions with different displays and can then review the heat maps to see how effective those displays are at attracting shoppers to purchase the featured merchandise. You can also use video surveillance to compare traffic flow and sales figures between stores with or without a particular end cap or display.

### Evaluating Advertising And Signage

Similarly you can test the effectiveness of promotional campaigns, in-store advertising and signage by studying the customer flow captured on surveillance video. With the addition of analytic tools to the surveillance system, you can even measure the dwell time customers spend in front of a sign or display. These analysis applications provide a number of key performance statistics, including



average viewing time, distribution of viewing time, and a number of shoppers viewing during a selected time period.

### Placing Surveillance Intelligence Where It Does The Most Good

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

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

#### 1. Minimise bandwidth usage –

Cameras and encoders can be programmed to only transmit video when they detect motion in a defined area of a scene. This dramatically reduces bandwidth consumption and

the number of operators needed to review transmissions. For instances, they can extract a head count from a frame and send just the essential data with a few snapshots instead of consuming bandwidth with several hours of unfiltered video.

#### 2. Reduce Server costs –

In centralized surveillance architecture, servers typically process four to sixteen video streams. When cameras do the processing, servers can handle more than 100 video streams. For people counting applications, for example, the resulting data (rather than the video stream) can be sent into the database, further reducing the load on servers.

#### 3. Improve surveillance analysis –

When network cameras provide raw video data before it is degraded by a compression format, the quality of analysis greatly increases. This configuration also reduces the number of servers required to process the transmission because fewer video packets are actually sent along the network for uncompressing or transcoding prior to processing.

#### 4. Lower operating costs –

With fewer servers needed power consumption and maintenance costs drop. This also removes the burden from environments without server rooms to build special facilities to support their surveillance networks.

#### 5. Lower equipment investment costs –

Reducing network bandwidth usage by streaming only essential information (metadata and snapshots) gives retailers the option to deploy more moderately priced network components that can easily support reduced data rates.

### Combining Video Intelligence And POS

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

### Impacting The Bottom Line

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

## What You Can Learn From Video Surveillance

**Question:** Is my shelf display attracting customers?

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

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

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

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

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



*Dr. Jumbi Edulbrbram is the director of strategic channels for Axis Communications, a provider of IP-based network video solutions that include network cameras and video encoders for remote monitoring and security surveillance. He has spent more than a decade providing thought leadership in the area of retail surveillance technology and has extensive experience with intelligent video application for the retail market.*





# Embracing and Leading Change In the Access Control Infrastructure

---

Organizations often avoid or delay change due to concerns about budget and the impact on productivity and workflow. This can be especially dangerous, however, in the access control infrastructure, where a combination of technology obsolescence and escalating security threats can quickly cripple an

organization's ability to protect its people, facilities and data assets. It is far more effective to be proactive, rather than reactive, about change. This requires building an infrastructure that presumes and prepares for ongoing change to support evolving access control needs, and enables the organization to preserve

investments in its current infrastructure as it moves to new technologies and capabilities.

There are many reasons to embark on this path, including upgrading inadequate security, and enhancing investment value and user convenience with a platform that supports multiple applications on smartcards or, in the future, Near Field Communications (NFC)-enabled mobile phones. The ability to embrace the positive aspects of change requires an access control platform that can meet today's requirements with the highest levels of security, convenience and interoperability, while enabling organizations to adopt future capabilities without disrupting the ongoing business operations.

Legacy security solutions can't deliver this future, because they often use proprietary technology that is static. This makes them easy targets for attack, and precludes their evolution beyond current abilities and security levels. Organizations should pursue solutions that are dynamic and adaptable to the changing needs of their organization and the best practices in the industry.

## Benefits of High-Frequency Contactless Smart Cards

In contrast with legacy solutions, the latest high-frequency contactless smart card solutions are built for interoperability, as part of a larger identity ecosystem that is significantly



# Intelligence EVOLved.



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



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

**For more information on VertX EVO, visit [hidglobal.com/evolved-nzsec](http://hidglobal.com/evolved-nzsec) or contact us at +64 9537 0279 or email at [asiasales@hidglobal.com](mailto:asiasales@hidglobal.com).**

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

more dynamic. These solutions also ensure that security is independent of hardware and media, making it much easier for organizations to evolve their infrastructure to support tomorrow's needs. Today's solutions also enable smart cards to be portable to smartphones so that organizations will have the option to use smart cards, mobile devices, or both within their PACS.

For instance, HID Global's iCLASS SE platform and iCLASS Seos card technology use a new Secure Identity Object (SIO) data model that represents many forms of identity information on any device that has been enabled to work within the secure boundary and central identity-management ecosystem of the company's Trusted Identity Platform (TIP). Any piece of data can be supported, including data for access control, cashless payments, biometrics, PC logon and many other applications. The combination of TIP and SIOs not only improves security, but delivers the flexibility to adapt to future requirements, such as adding new applications to an ID card. Additionally, iCLASS Seos credentials can be carried inside smartphones in a managed access environment, delivering a more hassle-free experience for users, who can carry the credentials for many access control applications on a device they rarely lose or forget.

The latest solutions minimize disruption during migration through the use of multi-technology smart cards and readers that leverage these extensible and adaptable platforms. Another advance is the availability of encoders that enable organizations to encode and instantly issue cards using a single device. Multi-technology encoders make it easier for organizations to migrate from current technologies to the security, adaptability and portability of new high-frequency contactless smart card platforms.

In the case of HID Global's iCLASS SE platform, an encoder is available that provides an entirely open solution for encoding multiple credential technologies, including both Genuine HID® and

third-party credentials, so that users can upgrade their existing card populations for use with iCLASS SE platform readers. For maximum interoperability, the encoder solution supports Seos, iCLASS SE, standard iCLASS®, MIFARE® Classic and MIFARE DESFire® EV1, as well as 125 MHz HID Prox® for encoding Prox credentials, and for migrating from HID Prox to high frequency technologies. Users can seamlessly and easily migrate from one technology to another by simply extracting access control data from an existing card and writing it to the new credential, without having to manually input data or being encumbered by encoding details. For even higher security, users can "wrap" their access control data within an SIO and then write it back to the same card. Based on open architecture, the encoder enables SIOs to be added to the full range of supported cards, including MIFARE and DESFire credentials.

With this type of forward-looking solution in place, organizations can achieve the highest possible security now, along with the flexibility to adapt to future requirements.

### Future-Proofing Secure Issuance

In addition to an organization's foundational access control card-and-reader platform, it is also important to consider current secure issuance requirements with an eye to tomorrow. Today's printers, card materials and software incorporate critical visual and logical technologies so that organizations can implement multi-layered validation. There are a number of available hardware choices, including monochrome direct-to-card (DTC) solutions and high definition printing (HDP) retransfer technology for contactless or contact smart cards. There are also high-throughput solutions that optimize performance and productivity. Today's desktop card printer/encoder products also give organizations a single solution that can deliver the high-volume reliability and advanced credentialing features of large centralized printers, as well as the lower cost and smaller footprint required for the distributed printing model.

Secure validation is another important consideration. Most ID card issuance systems simply compare the person presenting credentials with identifying data that is displayed on the card. This two-dimensional identifying data may be a simple photo ID or sophisticated elements such as higher-resolution images, or it might be a laser-engraved



permanent personalization attribute that makes forgery and alteration virtually impossible. Smart card chips, magnetic stripes and other digital components add an important third dimension of security. With expanded data storage, cards also can include biometric and other attributes to further enhance validation.

Another element to consider is speed and convenience. Printers with built-in programmers/encoders combine what previously were multiple processes into a single in-line card personalization step, significantly boosting issuance speed, convenience and efficiency. Users simply submit a card into a desktop printer equipped with an internal smart card encoder to personalize the card. This not only speeds issuance but also eliminates the risk of waste as a result of human error during manual entry. Opting for field-upgradable units enables organizations that already own a card printer to add an encoder in the field so they can leverage smart card benefits well into the future.

### Transition to a New Platform

When is a good time to start the transition? There are many possible entry points from which to begin the migration process, including:







- **Merger or acquisition:** Mergers and acquisitions often involve rebranding and/or the merging of disparate administrative and other systems, technologies and processes. Usually at some point in the process, the organization will need to issue new credentials. With the cost of new technology being competitive with legacy systems, this would be a perfect time to migrate to a more secure, sophisticated and capable system.
- **Standardize on a single card:** Due to rapid growth, decentralized administration systems and/or multiple physical locations, an organization may end up with several different access control systems. Since new technology offers the ability to issue or change credentials remotely, it's now possible to integrate access control into one system that is centrally managed. Standardizing all locations and employees on one system can increase security and improve resource management. Going a step further to mobile access control delivers the benefits of over-the-air remote provisioning and management of secure identity credentials.

- **Facility consolidation:** If a company is moving or adding a building, new credentials will have to be issued for that location. This is an ideal time to look at access control for the entire organization. It may be time to standardize all locations into one system.
- **Re-issuance process:** As new employees join, many organizations manage costs by purchasing additional cards that work with their old technology. Some organizations may also need to change their cards due to a new brand image or logo, at which point they can upgrade to newer technology.
- **New card applications:** Organizations that want to add new applications such as time and attendance, secure print management systems, or cashless vending functions will need to issue some type of associated card to users. They can migrate to a contactless smart card that combines access control with these other functions, enabling employees to carry a single card for many functions. Administration of these functions is centralized into one efficient and cost-effective system. Organizations also can seamlessly add logical access control for network log-on to create a fully interoperable, multi-layered security solution across company networks, systems and facilities. In the future, they can migrate to the convenience, flexibility and security of carrying digital keys and credentials on smartphones and other devices.
- **Risk management improvement:** Either due to insurance requirements or to improve risk-management costs by reducing liabilities, moving from an outdated system to a current one can dramatically improve the security in an organization.

- **Changes in security requirements:** As a result of new legislation or regulatory requirements, an organization may be required to increase its security. Similarly, if a company acquires a new client that requires a high level of security, it may need improved access control. A new building tenant may also trigger the need for greater building or campus security, either to protect the parent organization or to comply with the tenant's requirements. They also might want to add new visual security technologies to prevent counterfeiting.
- **Security event:** The reality is that sometimes it takes an unexpected event or security breach to move an organization to make the investment in a new access control system. Ideally, an organization should migrate before there is a problem, especially if the system is still low frequency, which can be easily cloned.

There is significant value that can be derived from shifting the traditional way of thinking about change, and looking at it as a leadership opportunity rather than something initiated in response to an adverse event. With the right approach, users can easily and inexpensively expand and upgrade their systems to meet changing needs while taking advantage of new technologies. By using dynamic rather than static technologies, security becomes independent of hardware and media, and the infrastructure can evolve beyond current abilities with the adaptability to combat continuously changing threats. Making the right technology decisions today will also help organizations meet new requirements with the confidence that they will be able to preserve investments in their existing infrastructure.



# Can an employer be held accountable for the unforeseeable?

Mark Lawlor, an employment law partner at Duncan Cotterill in Auckland, discusses the recent ruling involving the death of a security guard and whether his employer should be held accountable. He looks at the role the foreseeability of the risk of harm plays in the assessment of whether an employer has taken all reasonably practicable steps to ensure the safety of its employees.

---

Employers face prosecution if they fail to take all reasonably practicable steps to ensure the safety of their employees while at work.

But the employer is unlikely to be held liable when it can be shown that, even if all such steps were taken, this is unlikely to have prevented the serious and unanticipated harm.

Recently, a court ruled that the company that employed Auckland security guard Charanpreet Dhaliwal could not be held accountable for his death.

CNE Security was charged with failing to adequately ensure Mr Dhaliwal's safety, but in a judgment released by the Waitakere District Court, the company was found not guilty.

Mr Dhaliwal was killed in November 2011 on his first night on the job as a static security officer at a base campsite for workers engaged on an interchange development. The case, brought by the Ministry of Business Innovation, looked at the extent to which CNE was responsible for the death.

The site where Mr Dhaliwal died was regarded by both CNE and site controllers Fulton Hogan as low risk. CNE had not been fully informed about previous incidents on-site and although it was his first day, Mr Dhaliwal was an experienced guard who had previously done work that was more difficult compared to the basic work of a static guard.

It is possible the result might be different if an employee had little or no previous experience - especially if the employer was aware of previous serious incidents on the site as the risk of harm could be much greater.

## The facts

CNE was engaged by Fulton Hogan Ltd to provide security at the site, which contained port-a-coms, a few containers and various construction equipment. The site had experienced several break-ins at night. The static security guard was to perform hourly checks of the buildings and gates, with a log to be completed in one of the port-a-coms.

Mr Dhaliwal called the owner of CNE to seek work and was told he would be contacted if there was any work available. A few weeks later, CNE called Mr Dhaliwal and asked him to work that night, as another employee needed the night off. He accepted and agreed to meet the CNE's owner on-site at 10.30pm.

When Mr Dhaliwal arrived he was provided with the site keys, a high-visibility vest and a business card containing the owner's 0800 number so he could be contacted throughout the night. He was then walked around the premises by another employee, showing him the keys for the gate and port-a-coms, how to set and unset the alarm, the boundaries and how to complete the log book. The employee then took Mr Dhaliwal's mobile number to pass on to the owner and left.

That was last anyone heard from Mr Dhaliwal. He was found dead at approximately 3.30am by a Fulton Hogan employee.

## The decision

The MBIE informant inspector suggested two practicable steps CNE could have taken to ensure the safety of its staff. First, ensuring its security officers received appropriate induction and site training and second, having an effective procedure to monitor CNE's staff.

Judge Tremewan accepted that, given that there were no potentially hazardous construction or building issues and no restricted areas on-site, it could be properly regarded as a low risk site. She also held that the comparatively minor incidents did not indicate that a physical confrontation was a likely risk.

The Judge acknowledged that texting as a means of checking on staff was an appropriate step that CNE should have taken. She believed that such monitoring would still not prevent an attack occurring, but it would allow CNE to respond faster to any potential problems, and possibly reduce the resulting harm.

Ultimately, the Judge decided that even if CNE had taken the steps suggested by the MBIE informant, these would not have made any difference to what occurred.

The Council of Trade Unions is seeking to appeal the decision.  
mark.lawlor@DuncanCotterill.com  
<http://www.duncancotterill.com>

# Locked in... no compromise no comparison!

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

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

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

# 10 year\* guarantee

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

**20 + years service and experience.**  
A future of secure growth and development.



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

**Loktronic**

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



\*Standard terms & conditions of sale apply.





# Africa by night

## On safari with a FLIR thermal imaging camera

Many years ago the word 'safari' was associated with big-game hunting, but today 'safari' is understood to be a trip for observing and photographing wildlife, most commonly in Africa. In fact 'safari' was originally a Swahili word meaning 'long journey'.

Most safaris take place during the day, as in many African national parks it is not allowed to drive after dark and, in any event, it is extremely difficult to spot or photograph wildlife in total darkness unless you have a thermal imaging camera.

Powell Ettinger, founding editor of [www.wildlifeextra.com](http://www.wildlifeextra.com), travels around the world to explore the local wildlife. Prior work includes working in the adventure travel industry. He shares his stories and educates over 130,000 website visitors a month from all over the world. On one of his last travels he found a way to enjoy the African wildlife at night as well as by day: a thermal imaging camera.

"Whilst talking to some friends about a forthcoming safari to Botswana and Swaziland, I explained to them that I get up at 5:30 in the morning. It sounded odd to them getting up this early in the morning whilst on vacation. However in Africa the nights are long. It gets dark at

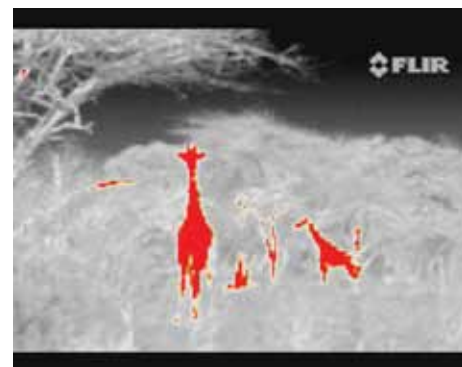
18.00, so there is only a limited amount of time to go out on safari," said Powell. "When someone asked about the wildlife after dark, I made various comments about not being allowed to drive after dark in many national parks, not being able to see the wildlife and not being able to photograph it. Firing off a camera with a flash usually provides dreadful results and quite often scares them away or enrages them."

Powell learned about thermal imaging cameras and how they produce a crisp image in the darkest of nights. They do not need any light whatsoever to produce a crisp image. He took both a FLIR PS24

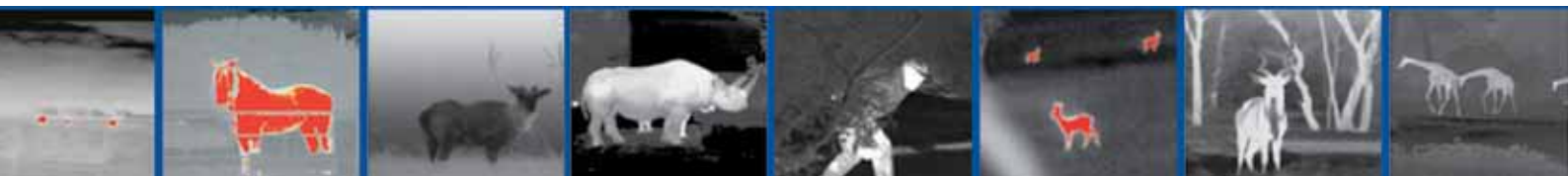
*The FLIR PS24 (left) is the smallest thermal camera available. With the TS24-Pro (right) it is also possible to record images and video.*



*"Black hot" thermal image of a warthog*



*The InstAlert™ image, shows the giraffes very clearly*





*"Much to my surprise, despite not having heard the faintest whisper, there were several impala grazing on the lawn just 40 yards from where I was sitting."*



*"White hot" image of the PS24 being used*

and a TS24 Pro thermal imaging camera with him on his next safari and used it to search for wildlife at night as well as during daytime.

Both cameras produce thermal images of 240x180 pixels. The TS24 Pro is able to store still and video images on a removable SD card. The FLIR PS24 cannot.

## Swaziland

It is forbidden to drive around Botswana game reserves during the night. Given this difficulty, Powell and his group also went to Swaziland's Mbuluzi Reserve, a neighbour to Hlane Royal National Park. Mbuluzi is 2,500 hectares of dry bush dissected by the Mbuluzi River and contains plenty of common game such as giraffe, zebra, kudu, blue wildebeest, nyala, bushbuck, impala and warthog. As a predator free reserve, it is allowed to drive, and even walk at night.

"Using the FLIR PS24 thermal imaging camera, we drove around the reserve in the dark. Although the camera gives a remarkably clear image, it is not always practical to use it whilst on the move, so we stopped every few hundred yards and tried our luck," Powell explained.

The PS24 thermal imaging camera has different image settings giving you the choice of seeing the images "white hot" or "black hot". It is also equipped with the InstAlert™ mode that colours the



*"FLIR PS24 revealed a few elephants feeding within 100 yards of the campsite."*



*Vervet monkeys are commonly seen around the campsites*

hottest parts in the image red. "InstAlert is extremely useful when searching wildlife but the problem is that at the end of an African day, when the earth has warmed up during an entire day, practically everything turns red."

I therefore preferred the "white hot" image mode just after sunset. Using the "white hot" image mode we did find some antelope, kudu or nyala, just off the track. The InstAlert mode is very effective after the earth has cooled down so we used this mode just before dawn."

At 05:00 the next morning the group set out on foot in an area where giraffe are often seen. "Using the InstAlert function it didn't take us long to pick up the red glow of a very long neck. A giraffe stood out very clearly in the darkness," Powell elaborated.

Powell continued: "Later that evening, as the embers from the braai glowed in the pit on the lawn in front of our lodge, I found the PS24 thermal imaging camera in my pocket, so I turned it on and swept the grass around the lodge. Much to my surprise, despite not having heard the faintest whisper, I noticed several impala grazing on the lush lawn just 40 yards from where I was sitting. Similar sweeps at regular intervals revealed a fine nyala bull, who lingered a long time, as well as what appeared to be an immature bushbuck, or perhaps a duiker of some sort."

## Botswana: see without being seen

Botswana is very different to Swaziland. There are vastly greater numbers and variety of wildlife, but sometimes less accessible at night. However, some species are drawn to a campsite, where perhaps a piece of fruit might be left lying around, or a few scraps of leftovers might be available near the dishwashing area.

As is often the case with campsites in and around African national parks, vervet monkeys hang around looking for the chance to nab a biscuit or even just some orange peel. Occasionally a hyena may wonder through looking for scraps and sometimes a shy genet may come down from the trees. However the tell-tale crash of a branch being ripped off is the easiest of noises to identify.

"FLIR PS24 revealed a few elephants feeding within 100 yards of the campsite. They were very relaxed and, in this case, not the slightest bit disturbed by our presence. The FLIR Systems thermal imaging camera helped us to see without being seen ourselves," said Powell.

## Enhanced wildlife watching

Powell continues; "Using thermal imaging enhanced our wildlife observations in two main ways. Without the thermal imaging cameras, we would not have known if there was anything around us in the dark at all. Much of the wildlife that is around at night keeps extremely quiet, as you would expect from animals that are constantly under threat of being killed and eaten by predators. We were amazed by just how much wildlife we found in close proximity to our lodge in Swaziland. Having a thermal imaging camera enabled us to record and identify what was there."

"On other occasions, we knew from the noise around us that there was something out there, in the dark, but we had no idea what." Powell concludes: "Another use for the equipment was to enhance our safety. If you need to go out of the tent or lodge during the night, it can be reassuring to check the neighbourhood for hyena before you leave."



To find out more about  
FLIR Systems and our  
product range go to:  
[www.flir.com](http://www.flir.com) or  
Phone: 0800 785 492  
Email: [info@flir.com.au](mailto:info@flir.com.au)





# Good days and Bad days are a fact of life!

By Fraser Burns - Master Locksmiths Association Ltd

But what was going through the head of this key cutter? In the photo it shows a set of keys that were duplicated. The key cutter has managed to reverse the profile, change the length and dream up a method of how to duplicate this monster. Was it a matter of mooning about the new girlfriend? Was it a repudiation that alcohol makes you think better? Was it lack of training? Needless to say that with "that much care" none of the keys worked at all. Three failures out of three attempts. Maybe he should take up betting instead.

Obviously only the person concerned can do anything about the first two likely causes. But if lack of training is the issue, then maybe they should join the Locksmith Apprenticeship scheme. During this last year we have had our first block course held in New Zealand rather than at Melbourne TAFE. This has been a major step for us and has been worked on for several years and required the support of many different people in the industry to pull it together. Getting it up and running is expensive in terms of dollars as well as effort from a number of people. But ultimately it will provide



*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)*

*or contact the 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*



New Zealand with better training as it is optimised for the conditions that we find in New Zealand. So both apprentices and employers, take the opportunity to make use of this training. It is only as we use it, that the course providers can keep making the improvements that we would all love to see. Already the training material has improved significantly over what was being provided a few years ago.

Never assume that you know what is important for your client. Other people have an amazing way of looking at things differently. Recently I had an emergency callout at 7am. The bathroom/toilet would not open! The door had just stopped working. And the lady needed to get away to an important event 6 hours drive away. So knowing what it is like to be unable to go to the toilet when you need to, I made haste. However by the time I made it to site, it was nearly an hour later. I was surprised to discover that in fact the owner had already left on her trip just leaving her mother behind. Puzzled, I tried to make sense of the situation, and immediately got filled in with how her daughter had been forced to go down to the supermarket and buy new cosmetics and how expensive these were. Now utterly confused, I muttered, "But didn't she need to go to the toilet?" "Oh", came the reply, "She just used mine!"

So obviously I should have asked more questions. Because she was assuming that I could arrive on site and fix the problem in less than 15 minutes. Instead my other customers for the next few hours had

their timetables disorganised too. So it is our responsibility when talking to a customer to interview them rather than just take instructions from them. We need to understand what they mean, as opposed to what they are asking (or telling) us. Remember those helpers? Who and Where, and What and Why and When. It is then up to us to provide the "How".

Currently we see increasing pressure to sell locks based on price. This is bad for New Zealanders. If you buy a cheap drill from China, you will probably get one with a designed life of 8 working hours. For many home handmen this is fine because they use it infrequently, that may give them effectively 10 years use. But when you buy a cheap lock, you are buying into one of two situations.

**Option 1:** The lock is going to collapse when you shut the door one too many times. The door will no longer open. Now you will need to call a professional out. You may be wise and call a Master Locksmith and they can fix the job fairly quickly. Or you may choose to call the cheaper builder out. Then you might have the fun of watching him get out his saw and cut the section of the door out that contains the lock and then take that down to the locksmith for repair. Then when he comes back, he can try to glue the door together again. It's truly amazing what glue can do these days.

**Option 2:** The lock buckles when the "fella in the night" (or even in the day) comes along and tries a few quick tricks to see if he can "borrow" (long term of course) your precious possessions.

Either way, you will regret that saving of perhaps \$100 when you face the greater bill or loss caused by the failure of that product.

And I say this not as a means to a sale, but because week after week I see the waste of dollars being spent that I now need to try and put right. As Locksmiths we need to help our customers understand why some products may be more expensive. There is a reason. We need to sell/teach each of our customers.



# New Zealand security qualifications review gets underway

Starting in February, The Skills Organisation will be leading a review of qualifications for the security industry on behalf of industry and other qualification owners.

To kickstart the review, near the end of 2013 The Skills Organisation asked for nominations for a Sector Review Group (SRG). The purpose of this group is to draft qualifications that are fit-for-purpose and will meet the future needs of the security sector as well as supporting a logical and accessible career pathway for trainees.

This group will include representation from all parts of the sector including industry, industry bodies/associations, Institutes of Technology and Polytechnics (ITPs), Private Training Establishments (PTEs) and Universities.

The SRG will be looking at the sector from a strategic perspective. The results of their work will include graduate

profiles (what a trainee will know, understand and be able to do when they achieve the qualification) and strategic purpose statements (these identify why the qualifications should be on the NZQF) for the proposed qualifications. The group will also produce draft qualification pathways that support logical career pathways.

The first SRG meeting is planned for early February. Following this will be approximately one meeting per month for six months. There will be consultation workshops in-between these meetings, as needed to support the review process.

Once the sector review is complete The Skills Organisation will submit to NZQA proposed qualifications for development. If this approval is given The Skills Organisation will then lead the next phase of the process which is the development of the individual qualifications.

For anybody interested about the detail of the review of qualifications, additional information is available on the NZQA website. To be kept up-to-date about the progress of the SRG or to join the wider sector review group mailing list, email [teohor@skills.org.nz](mailto:teohor@skills.org.nz) – people can be added to this list throughout the project.

Leading the review forms part of the role The Skills Organisation has as the Industry Training Organisation for the security industry. The review is required by the New Zealand Qualifications Authority to ensure the qualifications on the national framework support productive and skilled staff and they are recognised and valued by employers, providers and trainees.

**The Skills Organisation will be updating [skills.org.nz](http://skills.org.nz) throughout the process.**

## On your way to a COA?

### We can point you in the right direction.

Find out who is providing training sessions and workshops for the Private Security Personnel requirements at [skills.org.nz](http://skills.org.nz)

# skills.

The Skills Organisation  
0508 SKILLS (0508 754 557)  
[skills.org.nz](http://skills.org.nz)



# Office building security: A complete approach

---

Providing security in commercial offices involves more than a choice of products and features. A well engineered and maintained building automation system provides a solid return on investment over many years and delivers the highest level of security.

The best security in office buildings involves more than just good choices of alarm systems, cameras, and other security devices. A security system integrated into a flexible and scalable building automation system allows the building owner to use multiple security systems at once, expand applications of security for least cost and protect the security system capital investment from becoming obsolete.

Owners of these buildings today face security issues that concern owners and occupants alike. Whether a property is owner-occupied or tenant-occupied, providing the best security to ensure the safety of people and protection of intellectual and physical property is essential.

Companies invest millions of dollars in security technology with the intention of increasing security, protecting people, and solving security issues. This technology includes burglar alarms, fire protection systems, video surveillance, access control systems, and intrusion detection devices. Technology, in the hands of competent and capable security officers, can reduce property liability, cut material losses and keep people safe. But keeping security staff trained on separate, stand-alone systems can be challenging and must be addressed as part of broader security objectives.

## **Integration: more powerful, lower cost**

The key systems of security are intrusion detection, access control and video surveillance. By integrating these

under a flexible building automation system (BAS), owners can realise a lower up-front investment for a considerably more powerful security solution. Installation and training occur on a single system. Operational costs like administration and maintenance are also reduced. Component devices are used in multiple ways to trigger lighting, video capture, pan-tilt-zoom, higher video resolution or frame rate, door locks and other aspects of building control. A single system enables greater flexibility to add security components that can be easily integrated into the overall system, keeping the cost of capital expenditures low and requiring little additional training.

## **Security concerns today**

Employee theft, property crime and information security are the major security concerns according to a survey reported by the American Society of Industrial Security (ASIS). Burglary and vandalism ranked high as additional concerns. For owners, these findings translate to two priorities: keeping occupants safe and protecting buildings and contents.

The importance of security can also be measured by the amount of money major companies have committed to it. Computer and network security equipment lead the list, representing nearly 40 percent of all security purchases. An estimated one out of four surveyed companies also said they had purchased burglar alarms, fire protection systems, digital video recorder (DVR) surveillance and video cameras. Security lighting, access control, sensors, detectors and identification card printers were commonly purchased items as well.

These separate systems each address

a different security need and require training and familiarity to be most effective. A system that integrates the functions of many security devices into a single system significantly reduces capital expenditures and lowers facility operating costs because component devices are used in multiple ways and security officers can be trained on one system rather than many.

## **Protecting property and information**

Protecting data is also an expensive issue. Another ASIS survey suggests these losses amount to as much as \$59 billion annually in the USA. Companies also reported that former employees and on-site contractors were among the greatest risk factors for proprietary information and intellectual property losses, almost equal to the threat from foreign and domestic competitors. The most commonly lost information pertained to customer data, strategic plans, financial data and research and development.

Loss of information and intellectual property are not the only security concerns though. Violent crime near office buildings or in parking lots is another issue. In this environment, security will remain an important concern.

Manufacturers, mindful of this now offer an array of solutions, ranging from simple locks to complex biometric systems. Technological advances also provide even more innovative products to keep buildings and occupants safe.

Increasingly, new security products are offering integration with other building systems bringing many advantages to owners who understand that coordinating various security measures makes sense.

# fired up protection

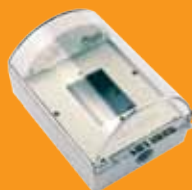
**ViTECH**

**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)





Purchasing a system with the most flexibility for integration lets management easily add components to increase security. Integration helps take full advantage of previously deployed sensors, cameras and other devices. As a result, higher security can be achieved with the same budget year after year. Integration is the key enabler.

### Moving beyond basic security technology

Regardless of the size of the office building or office park, its location or the level of risk to be addressed, there are essential components to an electronic security system, including intrusion detection, access control and video surveillance. These three systems, in the hands of competent staff, apply technology effectively to reduce crime and protect people and property. Integration will examine each system individually and in combinations to demonstrate how integrating security into the building automation system leverages these systems in multiple ways, increasing security and reducing operating and training costs.

### Intrusion detection

Intrusion detection involves the use of door or window contacts, glass contacts, or motion sensors, in combination with an audible alarm that sounds when a person has forced entry. An alert is sent to notify authorities of the time and location of the incident. Security officers respond in person to evaluate the situation.

But the effectiveness of the response at the scene and any subsequent prosecution is dependent on several things; the proximity of security personnel to the incident; whether witnesses were present; the number of people involved; the seriousness of the incident etc. Furthermore, with simple intrusion detection, there is little in place that would deter people from committing a crime in the first place.

More information would be helpful, such as captured details of the situation that could lead to proper response and identification of perpetrators, reducing the likelihood that similar incidents would occur again. Door and window contacts, motion sensors and other devices already in use for alarming can be put to better use to help gather this information by triggering other parts of the security system.

### Access control

Varying degrees of access are required depending on use and administration of access control can be distributed amongst several individuals. With different needs for owner-occupied and tenant-occupied buildings, how does management evaluate the various types of access control systems available and the best to meet future needs?

A flexible form of access control uses cards with magnetic card readers, proximity readers, barcodes, or smart cards with embedded microprocessors. Card access control at many large office buildings is common today, and there is a variety of systems with different levels of sophistication.

Employees can be coded with access to specific areas depending on need, company affiliation, or other factors. Individual privileges can expire on a given date if desired and in areas where tighter security is required management can install keypads, keypad/card combinations, or biometric devices that can scan fingerprints or handprints.

When used as a stand-alone system, card readers and other electronic access devices offer a cost-effective and flexible way for owners of office buildings to control who has access to the various areas, with the system recording who has gone where,

and when. But if a device can trigger the lock, why not use this inherent ability to trigger other security devices as well? As a stand-alone system, access control does its job, but does not fully leverage the connected sensors for broader security objectives.

### Video surveillance technologies

Video surveillance has evolved significantly in the last decade. Digital video recorders have made significant advances in features and functions, taking advantage of fast computer processors and high density storage media to digitize, compress and record video from analogue cameras. Newer cameras have embedded processors that enable video to be compressed within the device and transmitted real-time to Network Video Recorders (NVRs) that centrally manage video feeds from many IP cameras.

Streaming video can be continuously recorded and discarded in cycles of days, weeks, or months if no security incidents occur. If an incident does occur, disk indexing and time-stamping make it simple to find video from a given date and time. In addition, because the video is digitized, it can be exported and distributed via email or backed up on CD, DVD, or other digital media using common computer backup programs.

If purchased as a separate system to meet the needs of a security plan or upgrade, a DVR or NVR may be adequate. But if this is integrated with an organisation's access control and intrusion detection system, the user improves surveillance and reduces the need for additional security personnel.

Integrated with access control, video verification, for example, allows a user to see live video as well as the cardholder's picture when a given access card is presented at a reader. The security staff can verify that the person presenting the badge is the actual cardholder. Another example of video verification effectiveness occurs in identifying individuals who are "tailgating" or when one person swipes their badge and gains access to the facility and another person follows them in without presenting their badge.

### Video analytics help spot incidents

Video analytics enables examination of a camera's field of view for patterns of movement that match real-life events, such as falling, fence climbing, lurking and trip-lines. A DVR or NVR can be configured to only display a camera's video if a specific event or alarm occurs. At an office for example, foot traffic on a sidewalk near a back entrance may be deemed normal and not trip an alarm according to video analytics assessment. However, stepping off the sidewalk and crossing left-to-right across the field of view to a window or restricted-access door may trigger an alarm.



*HID Access control systems*

## Integrating intrusion protection, access control and video surveillance

Today's access control and video surveillance systems can work together in an integrated BAS to provide a holistic solution at commercial office buildings.

More and more offices rely on CCTV as part of overall security. Using an integrated system, staff at a central monitoring station can view live images from surveillance cameras, control pan-tilt-zoom cameras, or search for video clips stored on DVR's. When an alarm is triggered by another part of the BAS, it can command the DVR to begin recording, display live video from a linked camera at the location, map the alarm location and send alerts to administrators all at the same moment.

With an integrated approach, when an employee contacts security, lights and surveillance cameras can be activated to monitor the scene to observe the emergency and officers can pinpoint where to intervene.

## Integrated security and lighting control

Consider the benefits of simply installing a lighting control system versus integrating it with security. In an office building, the lighting controls will enable the operator to maintain comfortable lighting levels and use preset schedules to control on/off periods. This ensures the lights are only on when and where they are needed, saving energy and maintenance costs. If, however, there is a security breach late at night, without integration, personnel will need to locate switches or issue commands to the control system to switch on lights in the affected area. If the lighting controls are integrated, the scenario after the security breach is much different. The lights are automatically switched on in the area where the breach is reported and cameras are activated to record movements. The operator has a single console to assess the situation and to ensure the appropriate reaction from building security or police.

With an integrated security and BAS, it is possible for building operators to control entire facilities from one workstation via a networked computer. From this single browser interface, operators can manage diverse building functions, such as environmental control, access control, video surveillance and alarm and event monitoring. Building staff can view live or recorded video, open or lock a door, grant access to service technicians for emergency situations and handle visitor management. These tasks can be accomplished onsite or remotely at any time.

## Convergence: the future is here

Changes in how and where companies do business, along with rapid technological advances, are driving innovations in the security and BAS industries that impact commercial office buildings as well. Important trends driving change are the convergence of the enterprise network and the building's IT network.

This is created by the need to share corporate information, such as human resource data, with the security staff and other groups within an organisation. In addition, owners of multiple commercial properties want to interconnect facilities spread over different geographical locations to access real-time data over the internet. This information can be used for remote monitoring, facility management, analysis and control.

Using one, integrated system reduces overall hardware and software requirements, including the number of workstations needed on the operator's desktop. It also causes fewer training issues, lowers training costs and reduces the number of staff required to effectively and efficiently manage many buildings.

## Inside Sales - IP Security Products.

Open Platform Systems is Australasia's fastest growing IP CCTV distribution company, with a focus on providing IP based CCTV, software based video analytics and network hardware to allow our system integrators to provide complete turn-key solutions.

Due to recent expansion into the New Zealand market, OPS are looking for a competent Inside Sales person to join our Auckland based team.

As part of your initial responsibilities you will receive sales by various means (phone, email and over the counter), manage inventory of inwards and outwards goods, and be hands on in unloading, unpacking, and storage. Plus you will take full responsibility for the generation of consignment notes, the shipping of goods and meeting of deadlines.

Previous experience in the Security market will be an advantage.

### Preferred Competencies:

- Experience in warehousing/logistics industry.
- Liaising with NZ dealer base to secure sales.
- Receiving & Dispatching Goods.
- Picking and packing of orders.
- Knowledge of CRM type software for sales, logistics management and invoicing.
- Excellent customer service skills.
- Stock Control & Stock Take.
- Working closely with team members to deliver the highest standard of customer service.
- General Warehouse duties including some lifting.

This is a challenging role requiring a varied skill-set and a can-do attitude. The successful applicant will need to display excellent communication skills, occasionally think outside the square and will be able to work unsupervised or with a team.

To apply, please send your CV and covering letter to [jason@opsystems.co.nz](mailto:jason@opsystems.co.nz)



## Technical Support Engineer – IP Security Products.

Open Platform Systems is Australasia's fastest growing IP CCTV distribution company, with a focus on providing IP based CCTV, software based video analytics and network hardware to allow our system integrators to provide complete turn-key solutions.

Due to recent expansion into the New Zealand market, OPS are looking for a competent support engineer to join our Auckland based team.

Your responsibilities include identifying the solutions to any ICT related problems, assist the team in the customisation and adaption of existing products and services to meet customers' requirements if necessary. Providing telephone, online or face-to-face support to customers are also expected.

Previous experience in the Security market will be an advantage.

### Preferred Competencies:

- IT Qualification (e.g. Diploma in IT/ICT, MCTS, MCSA or MCSE).
- 3-4 years IP CCTV & access control experience.
- Good knowledge of MS Windows and Linux OS.
- Solid experience with Microsoft exchange, Active Directory, Windows Server, Terminal services, VMware or Hyper-V.
- Exceptional trouble shooting skills.
- Customer service skills with a genuine desire to help people.

This is a challenging role requiring a varied skill-set and a can-do attitude. The successful applicant will need to display excellent communication skills and will be able to work unsupervised or with a team.

To apply, please send your CV and covering letter to [jason@opsystems.co.nz](mailto:jason@opsystems.co.nz)



# Open but invisibly secure

By John Lazo-Ron

Today, when you think about building security, the first things that come to mind are security cameras, alarm systems, electronic swipe cards, secured doors, and maybe security guards standing at those doors but basically, electronic security.

Most buildings within the western world are fitted with the latest security technology on hand, as access to this type of technology is fairly widespread.

With technology advancing at a rapid pace and security threats also rising on a daily basis, electronic security plays a huge role in keeping people safe in the building areas they have access to, and keeping those who don't have access to those areas, out.

## But it hasn't always been that way.

Building security has changed significantly over the past half century as most would expect with advancing technology.

Security cameras started proliferating in buildings in the 1970's with footage quality improving immensely overtime, while electronic swipe cards were mainly used by military departments around the world before being used in public building security just a few years later.

But the major changes to building security have not just solely come from technology, but also due to factors such as public appearance.

With building security technology mainly at a foundation stage approximately 60 years ago, most people and organisations relied on having their 'wealth' confined within a solid building or 'fortress'.

Having that wealth locked up securely as possible was considered a necessity as consumer/retail products, personal belongings, assets and other important documents were treated like gold back then. But the only way people thought this could be done was by having their buildings built, whether it was a commercial, residential, or state owned building, with solid concrete walls with limited windows and doors.

As a result, most buildings had that fortress look many were after, which kept their wealth secure, but it also gave the

buildings a very defensive look, which ended up giving most of them a negative demeanour.

The lack of transparency from these fortress buildings became very off-putting to the public and discouraged many from entering.

As businesses searched for ways to become more consumer-friendly, the demand for the 'fortress look' dropped significantly and eventually led to a major change in building design called 'openness'.

Wellington based architect and director of Building Science at Victoria University, Guy Marriage, described openness as a term architect's used when it came to designing modern day buildings for businesses and companies that wanted to appear more open to the public.

He says a solid wall building was now seen as being very negative in terms of building design, with the western world now keen on transparency and open space in buildings today.

"The desire for openness when it comes to building design is quite high," says Marriage.

"Many years ago you would have a business like a bank that would have big stone walls around it to show it was like a fortress. However, it brought about a negative effect and banks don't want that type of building anymore. Banks want to encourage people to come in, so what they require is bigger glass windows with more open counters. They want their buildings to look friendly and that you can just wander in."

One building Marriage gave as an example is the Logan Brown restaurant building in Wellington City that was formerly a Bank of New Zealand (BNZ) office.

The BNZ left the building, which is stone fronted and set high up with very small windows, many years ago due to its lack of transparency, moving its main office to a building on the Wellington waterfront which has a glass ground floor.

"The BNZ left that building [Logan Brown] because it was perceived as being ominous or threatening and not

perceived as being open and welcoming," says Marriage.

"They've now moved to a building that has that perception of openness and I think it's probably true that you won't find a single bank in the country that's within its original building that was initially designed to make them feel secure."

Despite many businesses throwing out the welcome mat everyday to encourage people to walk into their buildings as well as trying to maintain that 'we are very friendly' look through openness, Marriage says many are still wanting that high level of security that a concrete walled building would bring.

He says this has become a tricky issue for architects over the years when it comes to open building design, as he says a fully glassed building, which can still be extremely strong, cannot give the same level of security as a solid concrete wall.

"Because people want openness when it comes to their buildings, it has caused a bit of a clash between what the security industry has available, what the public wants, and what architects are trying to design, which is the same security but without the appearance of it," says Marriage.

"To me that is the biggest issue. The clash between having that openness that we're trying to design into buildings and having the perceived need of having a place that feels secure without bars. You can't have a concrete wall and have openness at the same time."

Because of these clashes, Marriage says what openness has attained, which has helped architects in their design plans, is the birth of a new effective element of security that he personally likes to call 'invisible security'.



*Guy Marriage is a Wellington based architect and Director of Building Science at Victoria University*



When you see water fountains out in front of a building, big sculptures, park benches or even trees; to the naked eye these items look like beautiful objects that have been put where they are to look aesthetically pleasing.

But Marriage says because of the majority buildings that are now glass fronted, landscape objects have a much different purpose than just being placed to look pretty, but are actually there for security reasons.

“Many buildings today will use a lot of hard landscaping in front of their entrances,” says Marriage.

“You might have a nice concrete seat with a wooden back which people can use to sit down, but the real purpose of that concrete seat is to stop a vehicle from driving into the building.

“Then you’ll have soft landscaping as well which are things like trees, plants and water fountains. So if you are walking towards a building and see all this, you perceive it as being a comfortable place to sit with a bit of shade, but it’s actually a nice secure environment without overtly looking like that – invisible security.”

Marriage says invisible security is becoming more and more common today due to open building design.

He added again although toughened glass can be “incredibly strong”, so strong that you cannot just break it with a sledgehammer, a truck driving through it will clearly bring it down, which is why invisible security is required more often these days.

Marriage spoke of some Apple stores around the world that have been openly designed, where criminals have gone to extreme measures to break in as

electronic security stops most in their tracks attempting to break in any other way.

“Apple stores around the world now often have their main facades built entirely from glass,” says Marriage.

“Apple, who have some of the most expensive consumer products around, are specialising in these buildings where the whole building appears to be glass and very open and transparent. They obviously want people to go in but at the same time they need to lock their merchandise away at night. Recently there have been a couple of cases where people have ram raiding Apple stores by driving trucks through the glass. You may not be able to break the glass with your fist or a hammer, but a truck will definitely do the job so having invisible security certainly can help.”

Marriage also stated many United States embassies and government buildings around the world, have been using invisible security for quite some time to deter any possible terrorist attacks.

He says although they are very aware of the possibility of such attacks, they still don’t want to have big iron bars and gates to shut people out, so have begun using bollards or very big sculptures to keep suicide bombers from gaining access.

“Outside Wall Street [in New York] they’ve got bollards that are shaped like bronze sculptures on the street, so you walk down the street and you think what a great array of bronze sculptures until you realise that they’ve been designed and placed to make it harder for terrorists and criminals from gaining access. You don’t really see it but invisible security is there,” says Marriage.

Australian based New Zealand architect Stephen Matthews has been working on building design projects, including projects involving invisible security, for close to 10 years. He believes invisible security can be great for a building because it has the potential to work hand in hand with your normal electronic security systems when trying to stop someone from breaking and entering.

Time is always a factor in burglary, which is where he believes invisible security can play a major role.

“When someone is trying to break into a building with an unlimited amount of time, they’re always going to be able to succeed,” says Matthews.

“But having invisible security around is going to significantly remove that unlimited time factor. The idea of using

invisible security is usually to delay a criminal act long enough so your other security measures such as alarms can come into play, making it harder criminals.”

Another form of invisible security that Matthews says he has worked on through building design is passive surveillance. He described passive surveillance more as a location security factor that made it easier for people in surrounding buildings to see what was going on in a specific building.

“The required level of security will always determine the construction,” says Matthews.

“There’s different security for every type of building, but for smaller buildings, the main threats are burglary or arson at night, so it’s all about passive surveillance when it comes to design. That means designing a building where the building itself along with its entrances can be seen by surrounding buildings giving it better protection.”

Matthews says passive surveillance was especially helpful for smaller buildings that don’t have the budget or room to have public space objects in front of their buildings.

Matthews admits invisible security is definitely a good tool in the box to have, but despite invisible security measures in place due to the openness of a building, Matthews says it doesn’t always provide restrictions, which means it can’t always discourage potential offenders.

Sometimes it is just as well to have obvious security measures such as electronic security in place as well.

### **Cost can be another major issue.**

Matthews says architects can design anything to look great and make their clients feel secure, but that it ultimately comes down to a cost analysis by the client.

“Basically if you have the space and money then you can do anything to make security for a building look a lot more subtle,” says Matthews.

“But if you don’t have the space and money you’re not going to have everything on the menu in every building. Different security measures should be used in conjunction with each other, which is why cost can be an issue.”

So when you’re walking down a street and see a water fountain in front of a building, along with some nice bronzed sculptures with park benches that look like a great spot to sit down and have lunch, it’s really just another form of security – invisible security.



# Smoke detectors trigger compliance overkill claim

The long accepted practice of adding smoke detectors to security alarm systems to help protect properties could end up costing small businesses hundreds of dollars in annual compliance costs if the MBIE (Ministry Business Innovation and Employment) has its way.

A number of local authorities are now acting on by a five year old MBIE declaration which classifies detectors configured in this way as emergency warning systems, raising concerns that schools, churches, fish-n-chip shops and corner dairies may have to pay a minimum of \$500 annually to comply.

Ron Green, Chairman of the Association of Building Compliance (ABC), believes MBIE's ruling goes too far and plans to challenge the way the regulation is being enforced. "It's bureaucratic overkill, it penalises people for being proactive in looking after their property."



Brooks EIB2110 Multi Sensor

In an article in its Codewords (Issue #34) publication in February 2009, MBIE said smoke detectors needed to be on a compliance schedule as part of a building warrant of fitness (BWOFF) and possibly require a building consent.

Prior to this Green, like many others, recommended smaller commercial premises add smoke detectors to an existing security system as an affordable property protection measure. "The majority of these systems are not designed for warning people of a fire, it's for property protection."

He says the ABC is building a relationships with a number of councils, and meeting regularly with Auckland City Council which has taken a more pragmatic approach, saying systems will only be required to be on a compliance schedule if they're clearly for life protection or part of an evacuation scheme.

## Auckland holds line

While in Auckland having a detector as part of a security system would continue to be exempt, not all councils have the same view.

Others insist that because smoke detectors warn people of danger, they should be on a compliance schedule.

Green says this means many more buildings will require a BWOFF and that will start a chain of compliance



Ron Green, Chairman of the Association of Building Compliance

costs. "We're looking to test some of these things to get a legal point of view, particularly as this is happening at a time when the Government says it's trying to reduce costs to building owners."

Typically, Green says, those who don't require a full fire alarm system have been asking their security company to add smoke detectors so the monitoring service is aware of any problem.



# **BROOKS Provide Complete Fire Solutions...**

**Starting from the ground up!**



## **...for Residential, Commercial and Industrial Applications**

**BROOKS New Zealand**  
Ph: 0800 220 007  
Unit 106 "The Zone"  
23 Edwin Street Mt Eden  
Auckland 1024  
Web: [www.brooks.co.nz](http://www.brooks.co.nz)

**BROOKS Australia**  
Ph: 1300 78 FIRE  
4 Pike Street  
Rydalmere NSW 2116  
Web: [www.brooks.com.au](http://www.brooks.com.au)





# 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)

Mr Mrs Ms \_\_\_\_\_

Surname \_\_\_\_\_

Title \_\_\_\_\_

Company \_\_\_\_\_

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

Telephone \_\_\_\_\_

Email \_\_\_\_\_

Date \_\_\_\_\_

Signed \_\_\_\_\_

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

*“We’re looking to test some of these things to get a legal point of view, particularly as this is happening at a time when the Government says it’s trying to reduce costs to building owners.”*

Ron Green Chairman of the Association of Building Compliance

He says this approach is not about life safety as the fire service is likely to take longer to get there but it is another means of enhancing property protection. One logical option, he says, would be to only turn on the smoke detectors at night.

MBIE suggests when people see a smoke detector they assume it’s part of a full fire protection system. However Green asks “who looks at smoke detectors in a building apart from those in the industry”.

He says MBIE’s interpretation of the law raises a few issues; if they insist smoke detectors linked to a security system need a consent, questions are raised about standards, placement, testing and who is responsible for that?

## So who’s responsible?

Green says the ABC is trying to work with councils to get some answers. “In the fire alarm standard you test a minimum 20% of smoke detectors every year and during monthly tests a range of panel inspections are performed.”

However, he says, to undertake this work as part of the BWOFF regime you need to be an Independently Qualified Person (IQP) approved by a local council but most security companies are not approved to do this work.

Different companies check the fire alarms, air conditioning, lifts and security and each produce 12A forms which need to be approved for a BWOFF. “If the security industry isn’t approved to do this, does it go back to a fire alarm company?” asks Green.

“We’re going to look at addressing this issue, maybe through a determination or other means. The risk of course is that the outcome might not go in our favour and more councils could start enforcing the regulations.”

Mike Connolly, Executive Director of the Fire Protection Association (FPA) says MBIE’s notice to Building Control Authorities was nothing new, it was simply a reiteration of existing code requirements.

He says smoke detectors are an element of a building safety warning system and are specified under clause F7 of the Building Code. “As such they must be listed in the compliance schedule and installed and maintained to the relevant standard (NZS 4512:2010) regardless of whether they are connected to a security system.”

And he says, where smoke detectors are connected to a security system, then the security system itself must comply with the installation and maintenance requirements of that standard.

## Conflict over standards

Green insists a security system cannot comply with the NZS4512 as the security panel does not meet its requirements and neither do detectors attached to security panels. “There is no spacing, testing or maintenance requirements for smoke detectors connected to a security system under any security standards.”

Green agrees the issue has been a longstanding one and has caused some clients to remove detectors from security systems to avoid compliance costs. However, he agrees that smoke detectors will need to comply if fire protection systems are being monitored by a security system monitoring company.

In the meantime he’s advising security companies to warn their clients who have smoke detectors as part of their security systems that they could be required to add this to a compliance schedule for a BWOFF thereby incurring additional inspections and costs.



# fire door holding electromagnets



Standard, floor mounted, wall to door distance 114mm



A)

B)

C)



## 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

# Offshore interest in emergency messaging system

After 17-years of being tried and proven in the line of duty the unified messaging platform developed by Unisys to support the NZ Fire Service is attracting some serious interest from the Asia Pacific region.

Its proven capabilities and the lessons learned through the Christchurch earthquakes where the locally developed system continued to operate without any major failures have caught the attention of at least two interested parties.

“The level of inquiry we’re dealing with is certainly very serious and is being considered on a national basis,” says Kate Giles, Sales Manager with Unisys New Zealand technology consulting integration services.

“Unisys has strong credentials in the work we do with emergency services and Police departments worldwide so it certainly fits within our core stream.”

Giles wouldn’t be drawn on what the potential worldwide market other than to say, “we’re definitely excited about this,” and it’s likely the first deal would be signed this year.

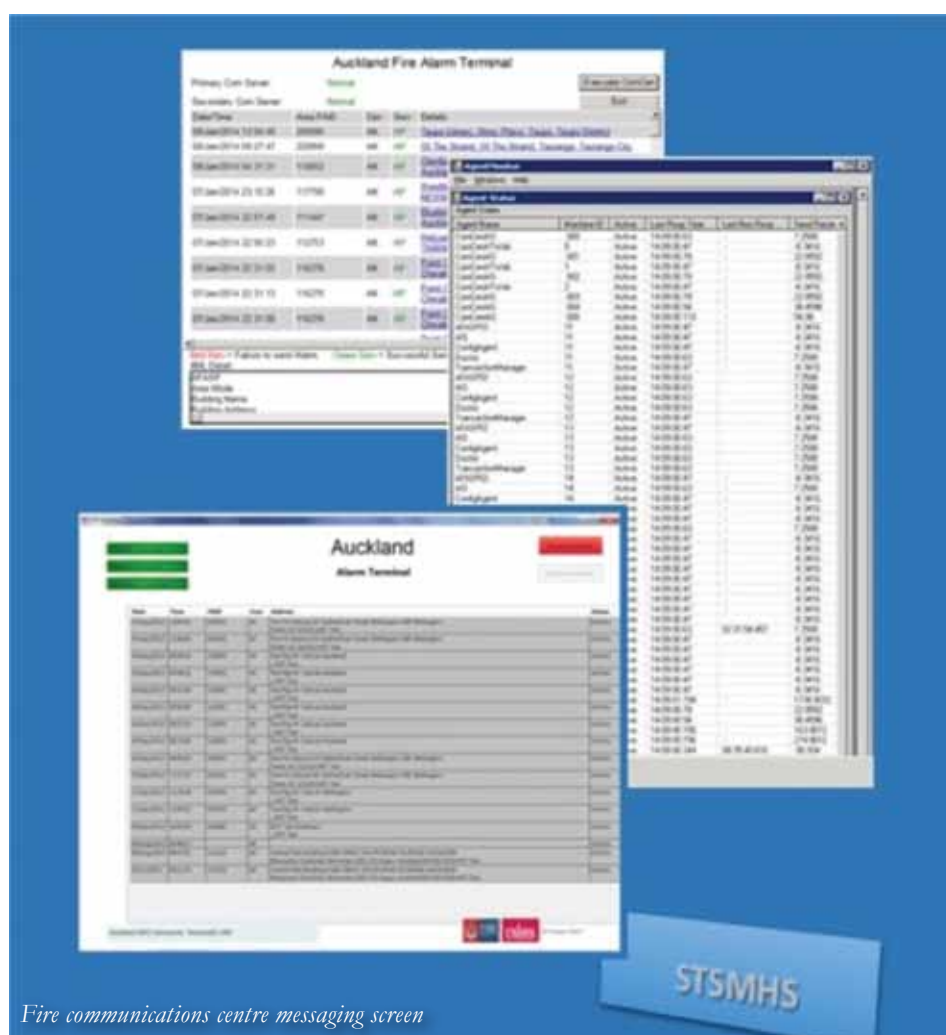
One of the reasons the Unisys system is seen as a frontrunner is because it works across the emergency services including the NZ Fire Service and the NZ Police. “Across the Asia Pacific region a number of countries and cities haven’t yet put in a single co-ordinated messaging platform,” says Giles.

The national automatic fire alarm system (NAFAS) monitors over 20,000 fire alarms in more than 6000 commercial

and industrial buildings across New Zealand triggering messages to the appropriate Fire Service Communications centre to deploy first responders.

The messaging system is the brainchild of software developers, architects

and members of the Unisys Global Telecommunications Team and Centre of Excellence in Wellington. If major offshore contracts are secured, Giles says it’s likely much of the skill and expertise would remain in New Zealand.





---

*Unisys software architect Paul Carter, believes the NZ Fire Service leads the world with technological standards and the Unisys messaging system could provide many countries with a single platform for communications.*

---

### Unshakeable in quakes

Unisys software architect Paul Carter, says there are no universal standards for fire alarms around the world which has created problems for the fire and alarm industry and believes what the NZ Fire Service and Unisys have achieved is world leading.

He believes the partnership has resulting in something that could easily be emulated by other countries because the proven robustness of the messaging architecture, enables the software to work with most off-the-shelf hardware.

A real test of the NAFAS came with the 2010 and 2011 Christchurch earthquakes. The 2010 quake generated 522 fire-related messages and 2044 alarm error messages. In the aftershocks of the larger earthquake in 2011 there were 5226 fire-related messages and 34,642 alarm error messages.

“The fire alarm system is not a standard business system but aspects are

very important to the NZ Fire Service’s life-critical business, including high reliability, 24x7 operation, redundancy and the ability to produce operational reports,” says Carter.

Unisys began supporting the NAFAS in 1996 when the NZ Fire Service wanted to move to a multiple service provider model. To achieve this it needed a high performing, scalable back-end system to handle alarm transactions.

It developed the IP-based alarm monitoring and messaging solution known as the Signal Transport System Message Handling System (STSMHS) which became the back-end architecture.

The new automated system was installed at the Unisys Kapiti data centre, going live in 2006. The system hardware was refreshed in 2011 and implemented in a second data centre in Auckland using a scalable distributed operations environment to increase resilience and business continuity.

The servers at both data centres receive and process every alarm message; if a server fails to respond within three seconds it automatically defaults to another.

### Messaging prioritised

When a fire alarm is triggered, it sends an instant message to the STSMHS, alerting the NZ Fire Service whether this is a fire or a fault, then routing it to the appropriate communications centre in Auckland, Wellington or Christchurch.

An average of 60 incidences of fire and about 40,000 message transactions including scheduled inspections, tests and reports are recorded each day and automatically categorised by order of importance.

Fire notifications are then displayed on alarm terminals and the Fire Service and NZ Police computer-aided dispatch system so the appropriate services can be directed to the exact location.

The STSMHS enables the Fire Service to receive and analyse a wide variety of alarm and sensor information and quickly identify the status of the buildings and the stage of fire involvement.

Polling and reports from the alarms continually prioritise events to gain a clearer understanding whether buildings have collapsed, are able to be occupied and whether the fire alarm is still online.

Stuart Waring, NZ Fire Service ICT Manager for Data and Intelligence, says the Unisys system is highly available and resilient and has significantly reduced the costs of maintaining and managing alarm responses enabling the NZ Fire Service to continue exceeding its response requirements.

He says the NAFAS is mission critical. “A fire can double in size every 30 seconds which is why it’s essential that our fire alarm system is always on and doesn’t fail.”

Unisys continues to work with the NZ Fire Service to enhance and make specific changes, most of which are confidential.

“Part of the reason this system has survived for 17-years is the need to continually evolving based on what the fire service and the public require. Development is continuing on a consistent basis to ensure it stays modern and flexible,” says Kate Giles.

Many of those changes align with the digital strategy that are aimed at ensuring a better flow of critical information gets to fire trucks and emergency vehicles at the time of a call out.



*The Unisys messaging system for fire alarms has attracted offshore interest*



### Real Time IP Kit Plug & Play!

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

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

iPhone, Android and Windows compatible.

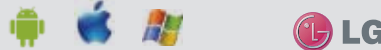


### LG LNV7300 3 Megapixel Camera

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

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

iPhone, Android and Windows compatible.



## 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**

Auckland: (09) 415 1500 • Fax: (09) 415 1501

Wellington: (04) 803 3110

Christchurch: (03) 365 1050

Email: sales@zonetechnology.co.nz

www.zonetechnology.co.nz



**FUJINON**

**GSP**  
DIGITAL VIDEO SECURITY SYSTEMS

**IR LAB**  
SURVEILLANCE TECH



**ASSA ABLOY**



## 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**

## Go DirectIP to Faster Setup



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

#### SmartIP Features:

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

Now available at your local Hillsec branch.



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

## HTS Group Ltd



## BARRIER GATES

Performance Guaranteed

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

We are looking for distributors!

0800 487 476

**www.htsgroup.co.nz**





## Loktronic for gate locks

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

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

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

**Gate locks from Loktronic – a wise choice.**



**Loktronic**



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

20756\_BP



## Key switches

**This versatile product range is produced with two functions**

Momentary contact (90°)

Turns 90° clockwise from vertical to turn on

Maintained contact (180°) locked on or locked off

Turns 90° clockwise from vertical to turn on

Turns 90° anticlockwise from vertical to turn off

SPDT switch 5amp rating

**Accessories are:** Key switch mounting bracket  
escutcheon for mounting bracket

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

Supplied random keyed. Can be master keyed.

Client's own key cylinder can be converted.

Front or rear fixing.

**Designed, tested and produced  
in New Zealand by Loktronic.**



**Loktronic**



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

20681\_KS

## Loktronic Power distribution module



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

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

**Comprises**

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

**Designed, tested and  
produced in New Zealand.**



**Loktronic**



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

20238\_PDM

# NETGEAR®



# BOSCH ZoneTechnology

Your Security Supply Partner



## Power supply cabinets

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

**Designed, tested and  
produced in New Zealand.**

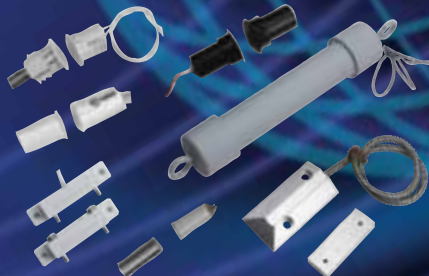


**Loktronic**



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

20238\_PSC



## total reed switch solutions from Flair

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

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

**Flair reeds from Loktronic:  
an unbeatable combination.**

**Loktronic**



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

20237\_F-L



## Loktronic for power supplies

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

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

**Power supplies from Loktronic – a great deal.**

**Loktronic**



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

20757\_BP





# ITPLUS

---

YOUR TECHNOLOGY PARTNER

**Phone: 09 950 4940 • Email: [info@itplus.co.nz](mailto:info@itplus.co.nz) • Web: [www.itplus.co.nz](http://www.itplus.co.nz)**