

NZSecurity^{Magazine}

A trusted source of information for industry professionals

August - September 2011

www.NewZealandSecurity.co.nz



Changing the shape of security

Inner Range

How to deliver in a crisis

Risk management

Christchurch

Five months on

One on One

Interview with Chris Mangan

FREE online subscription to NZ Security - see inside for details

Total HD surveillance

Uncompromising vision from Bosch

125 Years **Bosch**
1886-2011



Bosch HD takes image resolution to the next level

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

Ask about our Bosch HD product solutions today.



BOSCH
Invented for life

ZoneTechnology
Your Security Supply Partner

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

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

Wellington
35 Abel Smith Street
Wellington
Ph: 04 803 3110

Christchurch
Ph: 03 365 1050

Turn night into day!



NEW FLIR F-Series

NEW FLIR PT-Series

Total Darkness

Thermal Image

Fog or Smoke

Thermal Image

Network-ready thermal imaging cameras for security applications

Thermal imaging cameras are becoming more and more popular for security and surveillance applications. Many users are asking for thermal imaging cameras that can seamlessly be integrated in new or existing TCP/IP networks. The new FLIR F- and PT thermal imaging cameras are an answer to their demands. The F-Series are fixed mount thermal imaging cameras. Once installed they always look in the same direction. The PT-Series are mounted on a precision Pan/Tilt. This drastically increases

situational awareness. They also contain a daylight/low light camera that can be used when conditions permit. All cameras can be installed in a TCP/IP configuration or an analog configuration.

According to your needs, you can choose from a wide variety of lenses. You also have the choice of image quality: 640 x 480, 320 x 240 and 160 x 120 pixel detectors are available.

Available at:

Contact

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

All enquiries to

craig@newzealandsecurity.co.nz
Editorial contributions welcome.

Deadline for all copy

October / November 2011
issue is the 15th September 2011

Features

Oct - Nov 2011
Professional & Business Accountants,
Lawyers, Managers and Consultants

Dec 2011 - Jan 2012

Retailers

The largest retails in the country by
number of employees.

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.

ISSN 1175/2149

CONTENTS

- 6 Changing the shape of Security & Building Automation
- 8 Time to lift our game
- 12 Christchurch update
- 18 Spy ring shaken
- 20 Can you deliver in a crisis?
- 28 Changes challenge storage and back-up
- 30 Sensitive data grows faster than protection efforts
- 32 Gallagher hosts Technical Account Managers Conference
- 33 The Falcon 8200 Series Automatic Operator
- 34 Gate automation is all torque
- 36 NZ Conference 2011
- 38 Learning to get the most out of smart cards
- 44 Intelligence where you need it
- 46 Association News ASIS
- 48 Association News NZSA
- 50 Wintec shuts security course
- 52 NFC Mobile Phones
- 54 Bosch Video Recording Manager
- 56 Taming internet usage with real proof
- 58 Building Automation
- 60 Accounting
- 62 Entrada Data Centre opens
- 64 Cloud computing
- 66 Product showcase

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

NOW a 10 year
guarantee

on Loktronic Indoor
Electromagnetic Locks!

Loktronic • Innovationz

0800 367 565 www.loktronic.co.nz

16462_ELS

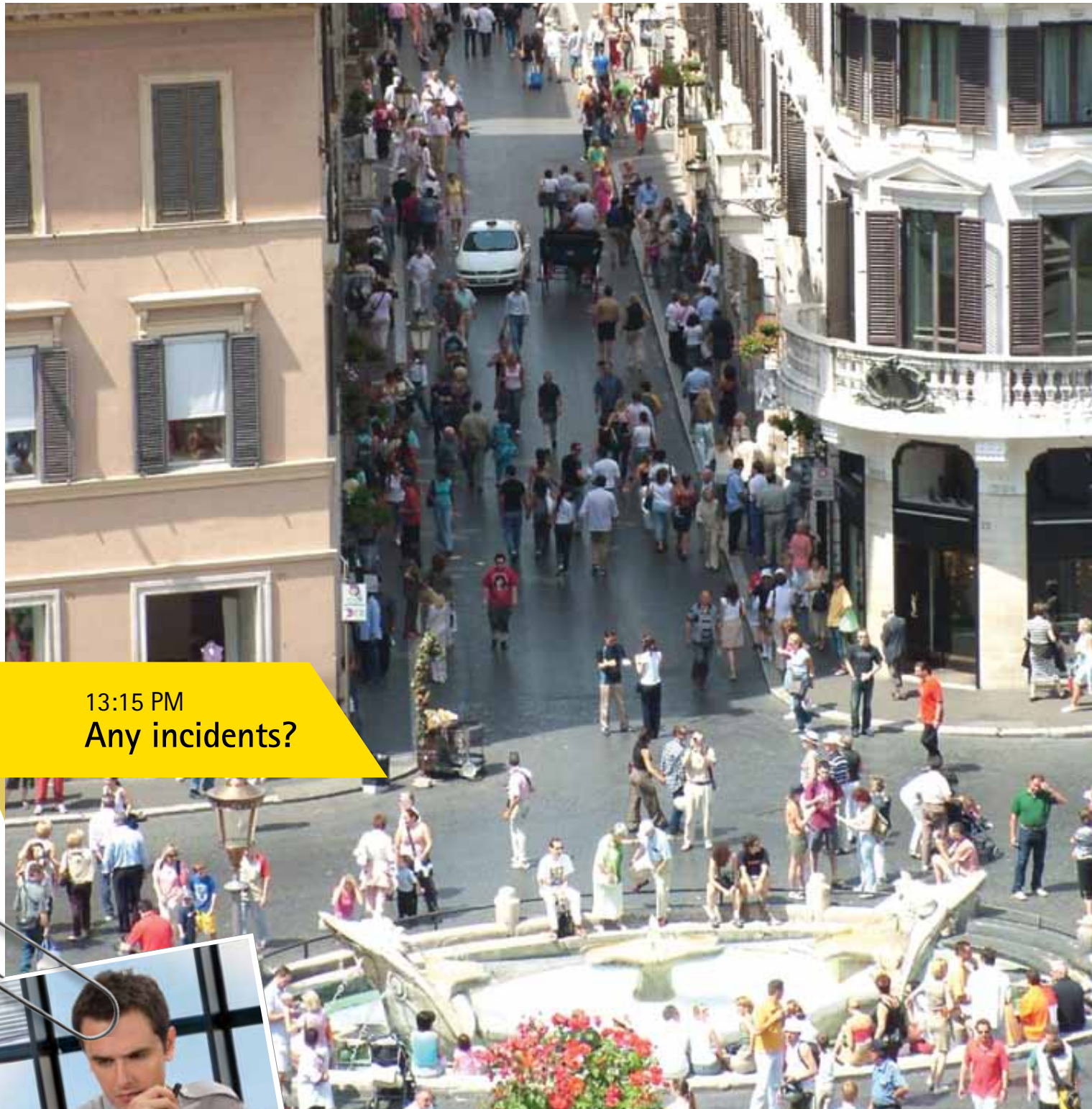
Associations

ASIS
INTERNATIONAL
Advancing Security Worldwide™
www.asis.org.nz

MASTER LOCKSMITHS
www.masterlocksmiths.com.au


NEW ZEALAND INSTITUTE OF
PROFESSIONAL INVESTIGATORS INC.
www.nzipi.org.nz

NZSA
SECURITY
NEW ZEALAND SECURITY ASSOCIATION
www.security.org.nz



13:15 PM
Any incidents?



13:15 PM
NOTHING TO REPORT

Effective outdoor video surveillance protects what you value most, alerts you to unexpected events and can even trigger appropriate response. But the cameras that achieve it must endure intense sunshine, heavy rain and strong winds – and still deliver usable results.

Axis outdoor cameras are exceptionally easy to install, which saves valuable time and minimizes maintenance.

They withstand extreme weather conditions, and offer superb image quality. Because your surveillance system needs to deliver indisputable evidence in the form of clear, crisp video images – even in the toughest environments.

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



www.axis.com/outdoor

AXIS Q6034-E PTZ Dome Network Camera: IP66 and NEMA 4X-rated casing, 18x optical zoom, HDTV 720p with 16:9 field of view, day/night, H.264, Power over Ethernet, Arctic Temperature Control, and much more.

AXIS[®]
COMMUNICATIONS

Inner Range - Changing the shape of Security and Building Automation Systems



Case Study: Jetts Gym

Situation

Jetts gyms is a rapidly growing network of nationwide 24/7 fitness centres. Running ahead of the game, within the last 4 years over 100 gyms have opened around Australia and New Zealand so far. Beating at the heart of their operation Jetts boast of convenience, freedom and value, with members being offered access to all Jetts gyms around Australia and NZ via their single access card. And it shows, over 100,000 members have warmed up to the idea already. This dynamic company is stretching the boundaries of the fitness industry faster than we can say 'whey protein'.

Action

The Inner Range system was chosen by Jetts as a perfectly balanced solution to meet their immediate and future requirements. With a tick next to each goal, all of the versatility and advanced controls called for were met without breaking a sweat. All Jetts sites are connected permanently to a central Insight System Management server via the internet. The Dynamic User Import Module within Insight enables outside platforms, such as the gym membership software, to export their user database into Insight including adding new and deleting expired members.

The monitoring station can see and communicate with the member via the camera system which includes built in microphones and speakers. The PA system is also interfaced with Concept for automated announcements. For example, if the front door is left open too long, or if a duress button is pressed, Concept provides the logic control to stop the music, continually play the associated announcement, and then return to playing music when the alarm has been acknowledged (e.g. closing the door). The Inner Range solution is a healthy fit for the job.

Task

As a 24/7 fitness centre, many hours of operation are unstaffed. Jetts required a highly sophisticated security and access control system to ensure the safety and confidence of their members. This system needed to offer advanced integration options, a flexible modular design, building automation control and support for hundreds of thousands of members across hundreds of sites internationally.

Also essential to the exercise was the ability for the access control system to interface to the gym membership software. This interface would enable members' details and card numbers to be entered into the gym membership software, with this information automatically populating to the master Control Module on each site, providing the member access.

Virtual Panel within Insight provides a mechanism whereby a user needs only to be programmed once and that user will be automatically propagated down to each Concept 4000 Control Module, granting access for that user. Virtual Panel effortlessly enables members to access all Jetts gyms through their single access card. The Active User Rotation Module within Insight allows expansion to hundreds of thousands of users through a rolling cache method, far exceeding the 50,000 user limit per Concept 4000 Control Module.

In terms of hardware integration, each Control Module on site provides intruder detection, building automation, duress alarm and access control. Mobile and fixed duress buttons are used to notify the monitoring station of an issue.

Results

The Inner Range product is much more than simply a security and access control system. Running successfully for over four years now, Jetts' implementation of this advanced platform has highlighted the many advantages the Inner Range system can offer. Delivering a complete but flexible package, Inner Range is changing the shape of security and building automation solutions. Jetts members can workout assured knowing they are protected by one of the world's most advanced and proven security systems.



Insight

Core package providing site management, panel programming, event review, floor plan functionality, basic reporting, operator and user administration.

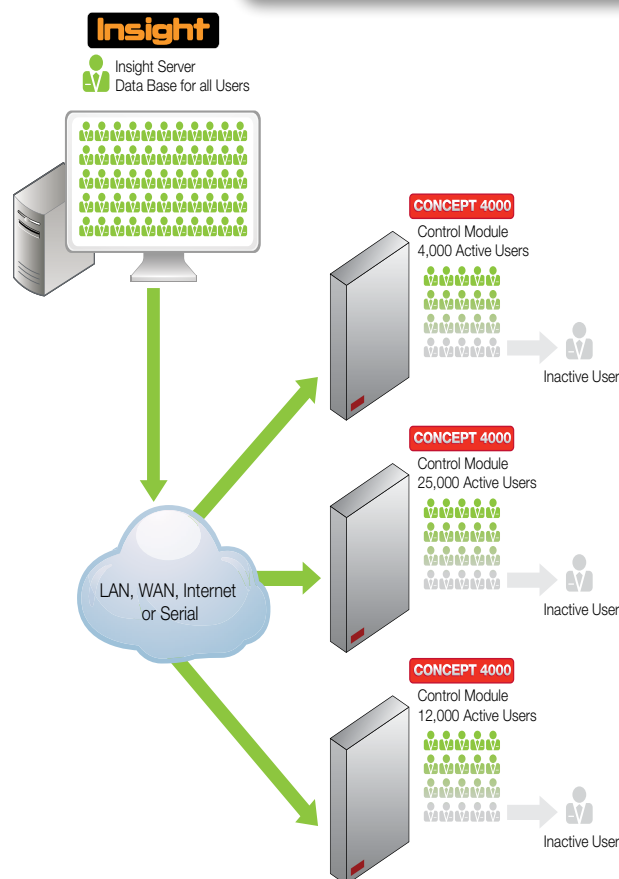
Optional Modules:

- CCTV Integration Module
- Advanced Reporting Module
- Photo-ID Module: Adds card design/print support
- COM Interface
- Dynamic User Import Module
- Card Pool
- Insight Communicator
- 3PGateway for Communicator
- Active User Rotation Module
- Insight Qualification Module
- Tag Board



Active User Rotation Module (AURM)

AURM has been designed to accommodate configurations consisting of one or many Concept control modules that require more users than the maximum allowable memory configuration. Panels with a permanent connection to the Insight server using the Active User Rotation Module can utilise this feature to extend the number of users much larger than the actual capacity of the Concept control module. (i.e Hundreds of thousands) If a user presents their card to a reader but is not found in the control modules` database, the control module will send a request to the Insight server. Within three seconds the Insight server will search for this user within its own database and if found, download the user`s record to the control module, granting the user access. If no free user records exist within the control module, then the user record that has been inactive the longest will be replaced. Without deleting user records AURM creates a rolling cache of users allowing for far greater numbers of cards than can be stored locally.



Inner Range`s Insight software solutions are distributed exclusively in New Zealand by Atlas Gentech (NZ) Ltd . Freephone 0800 732 637

- Auckland: 76 Carbine Road, Mt Wellington
- Wellington: 25 Centennial Highway, Ngauranga Gorge
- Christchurch: 112 Wordsworth Street, Sydenham

ATLAS GENTECH
DATA | COMMUNICATIONS | SECURITY

Insight

MANAGEMENT SOFTWARE For
CONCEPT SECURITY / ACCESS SYSTEMS

Time to lift our game

Steve Hart reports what former NZSA Chairman and CEO of Waikato Security Services, Chris Mangan thinks needs to be done to improve the lot of guarding companies and static guards

Waikato security firm owner Chris Mangan tells Steve Hart that it may be time to clear out the old guard at the NZSA and put some fresh blood in.

Security guards need to organise themselves, industry pay rates should rise and the NZSA needs to lift its game when it comes to promoting the organization. These are the thoughts of Chris Mangan, a former NZSA Chairman and CEO of Waikato Security Services.

Mangan has been a part of the industry for more than 25 years, starting out as a part-time static guard. Facing the threat of redundancy from his full time motor mechanic job in 1985, he jumped ship and started his own security firm that today employs 84 people.

"It was a big undertaking when we started the business, we went in blind and have learned from experience – there have been some hard knocks," says Mangan. "But I have had a lot of help from people, especially my family. I went through a very steep learning curve, but

equally I have had some great people working for me."

The firm focuses squarely on the Waikato region and, having just bought two smaller companies – an alarm supplier and Cambridge Security – is in a period of growth.

"We are moving down the technology road now," says Mangan. "But technology will never replace manpower – technology and people are both needed, they should work together.

You can't get better than a person walking around a site or office, even if it is just to check a tap hasn't been left on in the kitchen or being there to help a member of staff who may have collapsed around the corner."

He says a lack of respect for the work of security staff has led to lower wages, which causes problems for firms such as his when it comes to attracting good quality people. In short, he says, as long as firms continue to pitch in with lower rates to secure contracts, pay rates will remain at the lower end.

"Security guards today are being paid the same hourly rate that I used to get a quarter of a century ago," says Mangan. "Guards should be on a higher wage, in line with their qualifications and responsibilities.

Ultimately this comes back to clients who say they want the best service for the cheapest price. Many companies that hire security firms know they are paying a low price. Then halfway through a contract they will often change what they want by making some quite significant demands – a lot of companies buckle to that or risk going out of business."

Mangan says pressure from industry customers up and down the country is suppressing wages and believes a lot more can be done to improve the image of the industry. His rationale is that if the industry is valued higher, then everyone wins.

"We should be in a position to charge more and pay our staff more, but the reality is that security is right up there with insurance, in many cases it is a necessity and the price is driven down by the end user.

However that is not indicative of all customers; there are opportunities to have a value based relationship with clients. We actually had one firm increase their contract price because they wanted a higher level of service.

We are not here to rip people off, but to deliver the best service we can. But it is the end user that really dictates what we can pay our staff."

Apart from inflation and training costs (leading to better skilled staff), Mangan says there is a big difference between what a security officer does today compared with 20 years ago. But that extra responsibly, greater risks they face and technical expertise, doesn't appear to be recognised by the vast majority of customers.

"The level of respect for law and order has slipped," he says. "Some people think nothing of swearing at a police officer or lashing out at them. Security staff are lower down the pecking order, so people are less inclined to take any notice of them, and in some physical situations, the public will take a crack at you.

Security guards are not policemen, they don't want to be policemen, yet they can find themselves in serious confrontational situations. You have to respect the risks they face for minimum wage.

I don't think guards are appreciated or held with the regard they should be for what they do. Just try standing outside a bank for a day as a static guard – it takes a very special person to do that job."

However, Mangan recognises there has been some encouraging changes in recent years, notably the industry having closer relationships with the police "we are now



Chris Mangan is the CEO of Waikato Security Services and a former Chairman of the NZSA

DS-2CD853F-E

2MP Network Camera

- H.264/MJPEG video compression with high compression ratio for higher quality images
- Progressive scan CMOS
- Up to 32 GB SD/SDHC card local storage
- Electronic Pan/Tilt/Zoom
- Power over Ethernet support
- Conforms to ONVIF and PSIA



DS-2CD7153-E

2MP Mini Dome Network Camera

- H.264/MJPEG video compression with high compression ratio for higher quality images
- Progressive scan CMOS, capture motion video without sawtooth
- Electronic Pan/Tilt/Zoom
- Power over Ethernet support
- Conforms to ONVIF and PSIA



DS-2CD752MF-FBIR

2MP Outdoor IR IP Dome Camera

- Linux OS embedded
- TI DaVinci hardware compression
- High resolution video preview 1600×1200 pixels
- H.264/MPEG-4 video compression with high compression ratio for higher quality images
- Up to 32 GB SD/SDHC card local storage
- Support IE and client software for network preview



DS-2DF1-572

1.3MP Network Speed Dome Camera

- H.264 video compression with high compression ratio for higher quality images
- 1/3" Sony progressive scan CCD
- 3D intelligent positioning
- 216X zooming capability (18x optical, 12x digital)



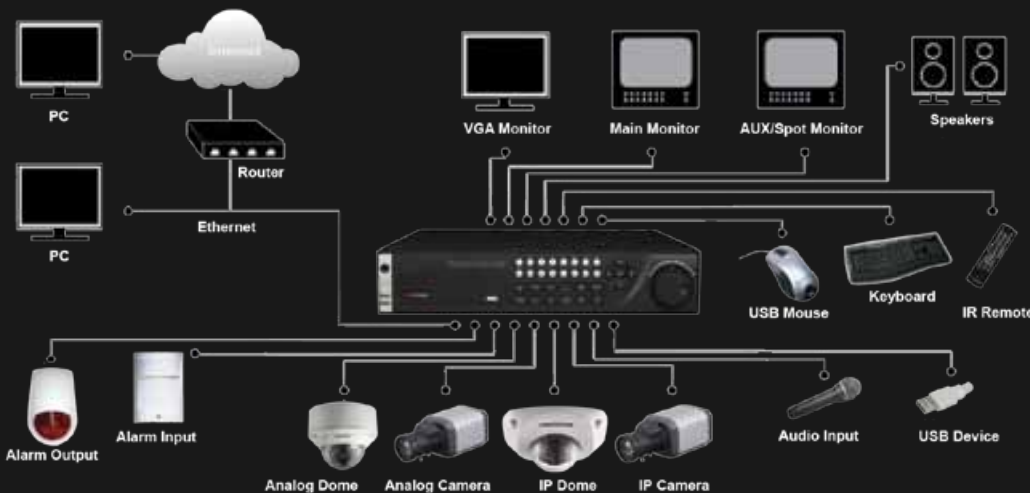
REVOLUTIONARY HYBRID DVR PLATFORM

DS-9016HFI-S Intelligent Hybrid DVR



By adopting the most advanced DSP platform and technologies the DS-9016HFI-S Intelligent Hybrid DVR not only integrates analog and IP seamlessly it also delivers powerful features, such as high-definition display in preview and playback and optional video analytics. Advanced motion detection, easy back-up to USB and CD/DVD-RW and supports up to 8 SATA hard disk drives.

Hybrid DVR Application:



ALSO AVAILABLE (non hybrid)

DS-9516NI-S

Network only NVR -

16 Channel with 1 TB Hard Drive

DS-9616NI-SH BNC

IP DVR with 2TB Hard Drive.

BNC outputs x2, VGA or HDMI outputs

HikVision is distributed exclusively throughout New Zealand and the Pacific Islands by:

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

- Auckland: 76 Carbine Road, Mt Wellington
- Wellington: 25 Centennial Highway, Ngauranga Gorge
- Christchurch: 112 Wordsworth Street, Sydenham



ATLAS GENTECH
DATA | COMMUNICATIONS | SECURITY

widely accepted by the police, which is better than it used to be.”

He says while the professionalism of the industry is higher than it was, there is still room for improvement. He hopes the new licensing laws will lead to positive change.

“It has been easier to get a security licence than to lose it,” he says. “But with the new Act that should tidy things up. It will introduce a lot more professionalism, and ultimately I would like to see that reflected in the guards’ pay packets.”

Mangan says when he first started working in the security industry he was paid \$15 an hour plus double time or time-and-a-half at weekends.

“I never thought I would hear myself saying this, but I think it would be good to have a practical representative body for security guards, which would lead to a more level playing field when we are quoting [for a job],” he says.

“I wonder if the guards need a union of some kind. There are some great people working in the security industry and the great majority want to go to work and do the best they can. But they have to do long hours every week to make it worth their while.

Any guard may be looking after millions of dollars worth of property and often being paid little more than \$14.50 an hour.

There are some people who’ll say ‘if you don’t like the heat get out of the kitchen’, but I love what I do, my staff achieve great things.”

In 2004 Mangan joined the board of the NZSA and stepped up to the plate to be its chairman. He says the association should take a leaf out of the Master Builders’ book.

“We only have to look at builders, for example. You see adverts for Master Builders on TV and hear them on the radio, so this and other associations – such as plumbers and gas fitters – are

building credibility for themselves with a higher profile and public recognition. We need more tools like that, they afford us that additional level of credibility when we go out to the market.

We need strong organization backing. Someone said a long time ago at a security conference that we are not an industry; we are a bunch of companies trying to be an industry. He was right then, and I believe nothing has changed much since.”

Mangan says the NZSA is not spending enough on marketing the organization. He may have a point. According to the NZSA’s accounts for the year ending March 2010 (latest accounts available) it spent \$2,346 on marketing and promotion in addition to \$20,383 on ‘industry lobbying’.

“Marketing does take money, but a campaign doesn’t have to be that expensive,” says Mangan. “Even a radio advert would be good. It doesn’t cost a whole lot. But I suppose it is a chicken and egg thing and members continue to ask why they should pay into it and what will they get out of it.

Nonetheless, the association has to establish itself and it needs money to do that – which can only come from the membership.”

Mangan says that while the NZSA has come some way, it hasn’t quite brought itself up to what he expects of a modern organization, whose members handle some of the most sophisticated technology available, carry a significant amount of responsibility and risk.

“I’d say that if you went up and down the country you’d get the same complaints about the NZSA as you would have got 20 years ago,” he says.

“I think the NZSA is run by well-meaning people, they are genuine, but we really need to step up our focus... there has been some good work done with the licensing and other areas, but I think maybe it is time to look at the NZSA as a whole.

What is really important is that we must have a strong and capable CEO – that is critical. The association is doing its best but I think we could do better. Ask the hard questions. Are board members there for their benefit, their organization’s benefit or the membership? Perhaps it is time for a really good sort out and fresh start.

The NZSA also needs to communicate more with its members and more with the end users. The association needs to be the membership champion in the public eye.

To me one of the most important things is communication. If the association is not communicating to the right people, in the right way, we are going to get nowhere.”

Mangan says distrust between industry firms isn’t helping the cause.

“There is still that suspicion of other companies, mistrust between us,” he says. “The industry is driven by big players in the market – there are some multinationals, and that’s fine. But there doesn’t seem to be that camaraderie among us that is reflected in other industries.

It is a great industry we work in and it has tremendous potential. As an industry we just need to get our house in order.”

Mangan says while security firms may get information from the association and others, they in turn need to work harder to share it with their staff – no matter where they are or what they do. “Better communication is a large part of the answer for people working at every level of the industry,” he says.

For his part, Mangan ensures all employees get news as it is passed down the chain from managers to supervisors – right through to front line staff.

“We have an internal system that means all news goes out by electronic and hard copy and to our all our guards. Communication is a big thing and I do think that is where some companies continue to fall down,” he says. “They don’t communicate with their staff enough. I think it is a culture thing we need to work on within the industry. It really is just good employment practises.

We need to communicate with everyone, to make staff feel engaged and valued and many business owners need to put their best foot forward, move on from the ‘sell & forget mindset’ and really sell the benefits of our industry (and the NZSA) to the customer.”

All opinions expressed in One on One interviews are the views of the person interviewed not necessarily those of New Zealand Security Magazine.

What the NZSA has spent on marketing

Marketing

2008: \$15,505

2009: \$12,079

2010: \$2,346

2011: not available

Income from membership fees

2008: \$266,331

2009: \$278,162

2010: \$298,498

2011: not available

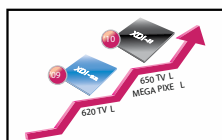
Source: NZSA audited accounts

EXPERIENCE THE SHARPNESS OF 650 TV LINES!



High Resolution Image of
650 TV Lines

LG new camera is equipped with new ISP (Image Signal Processor) Platform XDI-II and the largest 520K/610K (N/P) pixel CCD so as to deliver clear images of 650TV Lines.



XDI History

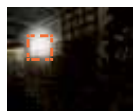


XDI-II

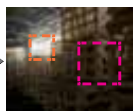


Enhanced Back-Light
Compensation with
68dB WDR & ACE

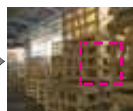
The world's widest 68dB WDR and Adaptive Contrast Enhancement (ACE) clearly distinguish objects in backlight conditions.



Original Scene



WDR on



WDR / ACE on



Improved Clarity in
low light conditions

With supersensitive CCD and improved 3D-DNR & Sens-up technology, the new analog series offers clear images in low light conditions.



Others



LG

L5323



L6323



L332



LG
Life's Good

Five months on: a note of optimism

Five months from the February earthquake in Christchurch and the rest of New Zealand has still has difficulty comprehending what it is like to live in a city where the plan to demolish or partly demolish over 650 buildings is well under way and whole suburbs will be abandoned.

All the same, even as the winter cold snaps roll through, there is a note of optimism among security companies in the city.

Back in February residential and small business alarm servicing and installation company Garden City Security was hit with a double whammy as large numbers

of customers sought urgent help even as the company was knocked out of its own premises.

Managing director James Seaward set up desks in his lounge and ran the operation from there, counting himself lucky to have power and water.

His business has now been back in his original premises for about four weeks.

“It is good to have a divide between work and business again,” says Seaward.

“Of course as soon as we moved in again we had a couple of good shake ups to keep us on our toes.”

After the February quake struck Seaward was concerned that after the initial response there would be a lull in

business, but these concerns have so far proved unfounded.

“There are still system faults, and there is a lot of system removal, relocation and re-installs. Once they have managed to find a new area they can go to, then people are shifting so they can get their businesses up and running again,” he says.

“We did lose a lot of money after the September earthquake with the uncertainty of the future and the money not flowing initially. It is nice to know that we have made up for that loss, and we do have a good forecast going forward.

“It seems that here in Christchurch there is no middle ground. Lots of





All the pieces you need to win.

Grow your
business with the
fastest growing
global brands.

IFS™



- ✓ Network Switches
- ✓ IP to Fibre
- ✓ Coax to Fibre
- ✓ IP to Coax
- ✓ Media Converters
- ✓ UTP Products

TruVision™



- ✓ Cameras
- ✓ DVRs
- ✓ Monitors
- ✓ Software

UltraView™



- ✓ IP Cameras
- ✓ Encoders
- ✓ Hybrid DVRs
- ✓ NVRs
- ✓ Extendable Storage
- ✓ VMS

For ideal security that protects your business and budget.



businesses can't trade properly, but other businesses are doing very well. There is a lot of demand for certain industries, especially in the trade services."

Overnight changes

Another locally owned company, Sub 5 Private Security, is also finding increased business even though central business district fixed contract patrolling disappeared overnight as the area was cordoned off immediately after the February quake.

Managing director Ike Houghton says while he now has reduced staff on patrols but static guarding, alarm installation and upgrades are more than making up for the downturn in that sector.

He says piecemeal guarding work as a result of the quakes also goes some way to making up for the cut backs in regular patrolling of buildings in the CBD.

"We're doing a property at the moment where all the floors are cracked and we put guards in at night. We have a lot of that one-off stuff that might go for about three weeks," he says.

According to Houghton things are still a long way from going back to normal, but like Seaward he has noticed many CBD customers are quietly relocating, and staying loyal to their security supplier.

He thinks strong companies that cover multiple security sectors will be in a good position as the city rebuilds, but for the moment at least, there is still major disruption to daily operations.

"You adapt and get used to it, but you learn not to go a certain way because the roads are in bad shape, or it is no entry. As bad as it looks on television - it is actually worse in real life," he says.

The experience has given him a renewed appreciation of things the rest of New Zealand takes for granted.

"My house is damaged but I've got a sewer, I've got power, water and I can watch television, put the heater on and cook myself a meal – and compared to a what lot of people in Christchurch have been through, that is pretty good," he says.

Fenced off for safety

For other security companies the focus has been on helping the authorities establish security in damaged areas, some of which are now open to the public again.

For Leaweld Perimeter Solutions Ltd this meant one-off contracts for massive amounts of temporary security fencing.

In a normal civil defence emergency a few phone calls would see temporary fencing quickly delivered and installed, but the sheer scale of the destruction in February called for another approach.

According to Leaweld managing director Steve Evans, the solution being considered by the authorities in February was to call on Australian help and urgently freight 19 containers of security fencing across the Tasman, although as it turned out, that would have been just the beginning of what was required.

Following the first earthquake in September, Auckland-based Evans had been in Christchurch to present the case for high-tech automated turnstiles to handle the Rugby World Games at AMI stadium, a project now sidelined by the disaster.

Thanks to that trip, when the second bigger quake struck in February he realised it would be possible to put together a New Zealand bid that would keep the work on this side of the Tasman, and would help put sorely needed business back into the battered Christchurch economy.

"First up, we won an order to supply 17 km of security fencing panels for the perimeter cordons to be installed around the Christchurch central business district," Evans says.

This initial order alone dwarfed any previous New Zealand orders for security fencing but the orders kept growing until a total of 31 km was supplied.





LEAWELD

Total Perimeter Security



Risk Assessed

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



TRUCK STOPPER



INDUSTRIAL CANTILEVER



LOUVERED GATE



SWING GATE



WIRE MESH SLIDER



HANDIFENCE FLAT TOP FENCING



HANDI FENCE SPIKE TOP FENCING



PALISADE



MILD STEEL MANUAL
RETRACTABLE BOLLARD



BURGLAR BAR GRILL



SECURITY TURNSTILE



100% DUTY CYCLE
TRAFFIC BARRIERS



LEAWELD
Total Perimeter Security

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



“We broke it down into six manufacturing packages for local Christchurch firms, so as to keep the work where it can help the local community,” says Evans.

“We knew there were the skilled people down there to do the work and at the peak of production we had about 75 people producing 1.3 km of fence per day.”

Only one local firm had too much damage to participate and Evans says they all worked well together – sharing ideas and machinery as needed.

At the same time companies from other areas of New Zealand also got behind the project as a way of contributing to the recovery effort and at the beginning meetings were held around the clock to co-ordinate the first raw materials supply and set up the project management.

In South Auckland, steel recycler and building materials supplier Pacific Steel supplied millions linear meters of galvanised steel wire for the Hurricane Wire division of Steel & Tube to weave into mesh for fencing.

Evans is quick to praise all those who contributed.

“Normally it would have been impossible to get such a large project organised so quickly, but there had been an extraordinary amount of co-operation from everyone involved, including the authorities in Christchurch,” he says.

“Everyone worked their guts out to make it happen, and it shows what we in New Zealand are capable of when we put our minds to it.”

“I have nothing but praise for the Civil Defence,” says Evans. “It was a \$2.2 million project but they quickly got on board and we arranged with them to pay invoices immediately to help the local business’s cash flow.



Evans says the 12 week fencing project is now behind them, but Leaweld is busy on other projects.

“Our manufacturing operation builds fencing products and automated gates, and that is going from strength to strength. We have had to advertise for new staff to help fill orders,” he says.

New staff

ADT Armourguard has also been recruiting staff in Christchurch to replace extra staff from around New Zealand brought in to help with the immediate aftermath of the February quake.

The company reports that today it is still busy with guarding and customer focused roles for organisations like the NZ Police and the Department of Building and Housing.

General Manager Ian Anderson says staff seconded from the North Island have now returned to their home areas but the company has recruited an additional 50 new staff in Christchurch to replace them.

“This brings our total new staffing since the earthquake on 22 February to 150,” he says.

But it has been a rocky road for Christchurch since the biggest quake.

“The two new significant aftershocks on 13 June resulted in additional building collapses,” says Anderson.

“We are continuing to provide guarding services at these sites. We are also working closely with the Ministry of Justice at their satellite District Court located in a marae in the eastern suburbs and continuing to provide services for private clients throughout the city.”

He says that since the first days after the quake the big challenges of transporting all the temporary staff have subsided now they have return to the North Island. At the same time the company has developed new systems and processes to manage any new events as and when they occur.

“These include our web based rostering system which is able to broadcast a text message to all staff members should an event occur,” he says.

Anderson says that given the challenging employment situation in Christchurch, ADT Armourguard is pleased to be able to recruit high quality staff from a variety of backgrounds.

“It has given us opportunities to promote team members into operational and supervisory roles,” he says. “It is a win-win situation for everyone.”

intek

first by far™

THE POWER OF SPEED



A NEW AGE OF FREEDOM AND VIRTUAL CONNECTIVITY HAS DAWNED

ALEXOR

WIRELESS SECURITY PANEL

The finest 2-way Wireless Security System
The World has ever known... ALEXOR



DSC

Distributed exclusively in New Zealand by:

intek

www.Intek.co.nz
Freephone 0508 4 INTEK

Auckland Head Office:
51 Normanby Rd, Mt Eden, Auckland.
Wellington Regional Office:
Unit 4, 57 Marsden St, Lower Hutt, Wellington.
Christchurch Regional Office:
40 Buchan St, Sydenham, Christchurch.

Spy ring shaken

Spies from Israel, police computers, fleeing backpackers, international intrigue and a political hot potato. Steve Hart reports on allegation Mossad helpers were active in Christchurch.

What exactly was going on in Christchurch on 22 February when an Israeli tourist was killed during the quake, and how many passports did the dead person have? More importantly, was he one of a team of Mossad 'helpers' trying to nab sought-after Kiwi passports?

It's all unfolding as NZSM goes to press. The drama revolves around Ofer Benyamin Mizrahi, who died in the quake, Michal Fraidman, Liron Sade and Guy Jordan as well as an unaccredited Israeli search and rescue team.

"The allegations over suspicious activities by Israelis during and immediately after the February earthquake in Christchurch are serious and deserve a response (from John Key)," says Labour's Foreign Affairs spokesperson Maryan Street.

"If there has been any breach of this country's security and sovereignty that John Key knows about, then he needs to tell us. Were these young people really just backpackers?

Or had an innocent group of tourists been infiltrated by Mossad 'helpers' whose mission it was to take Kiwi identities? One of them was carrying five passports?"

It almost looks to be a repeat of what took place in 2004 when Mossad agents were convicted for passport fraud and breaching New Zealand's sovereignty. Has Mossad been caught out again?

In an attempt to put the matter to rest, Prime Minister John Key said the unusual circumstances surrounding a group of Israeli nationals were "fully investigated" and no evidence found of a link between the group and Israeli intelligence.

"The unusual circumstances which triggered the investigation was the rapid departure from the country of the three surviving members of the group of Israelis in question," said Key, speaking at a press conference in LA.

"Security agencies conducted the investigation and found no evidence that the people were anything other than backpackers."

Strange then that the backpackers were seen taking photos of the crushed van

they had been sitting in when the quake happened and fled the country leaving their dead friend in the driving seat.

Key says the dead Israeli man, killed by building rubble falling onto the cab, was found with a European passport. The other three people who had been in the van took their passports when they left the country – within 12 hours of the quake – and apparently handed over the dead man's Israeli passport to Israeli representatives before flying out.

The story took another twist when it was alleged that an Israeli search and rescue squad turned up unexpectedly within hours of the 22 February quake. They were apparently escorted out of Christchurch's red zone – an area they should not have been in.

There were fears they had, during the confusion of rescuing people, slotted a USB drive into a police computer to load software that would give hackers a back door into the police national computer. Police say a subsequent check of their computers found nothing untoward.

Investigative journalist and Security Intelligence Service expert Nicky Hager was reported on the Stuff website saying that having access to the country's police database would provide a "fantastic resource".

"You've got potential names you could steal and use, you've got all their backgrounds. You've got this fantastic resource on another country," he said. "If you're an intelligence agency that would be a very high-value thing to seize."

Speaking on National Radio, Mossad expert Gordon Thomas, author of the book *Gideon's Spy – The Secret History of the Mossad*, said events surrounding the four Israelis featured all the hallmarks of an intelligence operation. He says Israel has a reputation of using students as agents.

He made his own inquiries in Israel and says 23-year-old Ofer Benyamin Mizrahi was the group's leader.

"The Israelis specialise in this type of operation," he said. "They put together a team with false passports."

"Urgent enquiries are going on around Europe because the passports the team held were French, Irish and UK."



Two couples, man and woman partners, is a standard Mossad operation because it is easier to pass unnoticed and unchallenged. The fact that three of them fled New Zealand within 12 hours of the quake is suspicious.

I know that contacts are now being made between the SIS, Mi6 in London and other European intelligence organizations to try and track down these passports.

I am told on good authority that there were eight passports altogether, which makes sense because they normally carry more than one passport (each). They never travel on Israeli passports.

The question that is puzzling to me is why did the Israeli Prime Minister Benjamin Netanyahu have to make four phone calls to John Key...to enquire about what? I am told by intelligence source that I trust that Netanyahu rang to make quite sure that the story of the Mossad operation would remain quiet."

Thomas says Mossad's agents are expanding across the Pacific searching for al Qaeda cells.

Israel's ambassador to the South Pacific region, Shemi Tzur said reports of Mossad spies in New Zealand were "science fiction".

SONY

So small and sleek that they can fit anywhere X Series

The X series HD network cameras are not only affordable; they also offer high definition clarity, making them ideal for commercial spaces, offices, retail shops and outdoor areas. Certain models even sport rugged and vandal-proof features, which make tampering more difficult. What's more, they are so small and sleek that they can fit into the tiniest of spaces, making them perfect for covert use.

Key Features

- Incorporated with "Exmor" CMOS sensor to ensure high image quality and low noise
- Excellent 1080p HD picture quality, supporting H.264 at 15 fps
- Three codecs (H.264, MPEG-4, JPEG) and a dual streaming capability
- Electrical Day/Night function for switching to Day or Night mode, depending on the light level
- Stream Squared function to send two 4:3 aspect ratio videos in user-selectable resolutions up to SD simultaneously (Low-cost solution to replace two SD cameras located in a line)
- DEPA Intelligent Video Analytics system can be set up with a DEPA-enabled recorder
- Bundled with recording software (RealShot Manager Lite)
- ONVIF (Open Network Video Interface Forum) compliance that ensures greater interoperability and flexibility in building multiple-vendor systems

SNC-DH210



SNC-DH210T



SNC-CH210

Actual size

IPELA

Exmor



www.sony.co.nz

Sony New Zealand Limited
Akoranga Business Park, Northcote, Auckland
Tel: +64 9 488 6188 Facsimile: +64 9 488 0503
Email: sonybusiness.snzpf@ap.sony.com

SONY and *make.believe* are trademarks of Sony Corporation.

Can you deliver in a crisis?

Preparing for the worst

By Keith Newman

After the earth shakes, the lightning strikes, the water recedes, the embers have died down or burglars have fled with the computers, the only saving grace for many businesses is knowing their core systems are backed up off-site, so they can pick up where they left off.

The events in Christchurch have bought emergency management and disaster recovery plans of councils, businesses, individuals and service providers, including security companies, under the spotlight. The questions remain: how prepared are we; and if the answers are uncertain, what are we doing about it?

Even a short interruption can result in serious revenue losses but with IT systems out of action for a week or even months,

reputation, goodwill and relationships with partners and customers can be irreparably damaged.

A new Government report on the readiness of Wellington saw response groups confident they could respond to localised events but concerned that capacity and capability would be overwhelmed in a larger event.

The Civil Defence and Emergency Management Ministry raised the spectre of lack of leadership, rivalry between councils and general uncertainty about who would be in charge, ultimately diminishing the ability of Wellington to respond to a large earthquake.

Other cities and towns around the country are reviewing their policies and procedures for response in the aftermath



*National Channel Manager for ADT-Signature,
Peter Freeman*

Challenges ahead of a crisis

- Do you have a business continuity plan?
- Is everyone aware of it?
- Who's responsible for the welfare of staff?
- Do you have an emergency number?
- Is a list of essential contacts kept off-site?
- Are key IT and security systems backed-up off-site?
- How long ago was the back-up done?
- When did you last test your back-up systems?
- What happens if your technology fails?
- What happens if you lose access to your site?
- What do you do if you lose staff members?
- Do you have a crisis management plan?
- Have you rehearsed it?
- Do you have an off-site location to go to?
- Who will make quick business decisions?
- Who will operate the phones and how?
- Who will restore and access the information systems?
- Who will co-ordinate with police and emergency services?
- Who will talk to the media?
- Who will communicate with stakeholders and customers?
- Who will pay staff?

of a disaster, asking how co-ordinated regional and local council plans are, and whether emergency services are sufficiently equipped.

While power, telephone coverage, water and sewerage infrastructure were restored relatively quickly to Canterbury, Peter Freeman, the National Channel Manager for ADT-Signature, was amazed how few companies had planned for a disaster or even done a risk analysis.

He says that planning should include how they will handle staff welfare, security and business continuity issues such as answering phones and how to respond if isolated from their core technology.

"There are still companies in Christchurch in that situation today; they hadn't thought through what might happen if their head office or one of their main offices was taken out of action for a month or two," Freeman told NZSM.

Surveillance cameras run 24x7. Capture it all with
WD reliability.



WD AV storage. The ultimate in reliability for surveillance applications.



Don't depend on anything less than WD's AV-class hard drives — built to thrive in the always-on demanding world of digital video surveillance. These drives are designed to support HD video from up to 12 simultaneous streams. They also minimize frame loss, which can pose a real problem when you use standard desktop drives for surveillance storage. For a solution that's a safe bet 24x7, you can count on WD reliability.

WD AV-Class Hard Drives



PUT YOUR LIFE ON IT®



“A number of companies weren’t able to switch phones over to other offices and didn’t know which phones were being answered or how to get their emails diverted because they couldn’t access the servers inside their buildings.”

One firm with offices across the country couldn’t access their payroll system, was unable to pay its staff for two months and ended up estimating wages. “That will create ongoing problems with tax and a host of other things,” says Freeman.

Following the Christchurch disaster, many insurance companies have indicated conditions for coverage are likely to be tightened and personal, business and property premiums increased.

Internationally concessions are made if companies can show they have taken every measure possible to raise security levels, which may include business continuity and crisis management plans.

Freeman suggests a good crisis management plan would ask what critical pieces of work are carried out in specific locations that cannot be easily replicated, and what would happen if that function is taken out. He reckons a good place to start is with Standards New Zealand, Risk Management Handbook HB 436:2004 guidelines (www.standards.co.nz).

She won’t ‘be alright’

Ian Tuke, Operations Director for business continuity firm Plan-b, believes New Zealand businesses often have a “very slack ... she’ll be right attitude” and have literally been given a shake-up.

He says the best way forward is to have a crisis management team rehearse how they will respond in the worst possible scenarios including how to get things back up and running.

That would require the CEO, heads of departments and senior support people getting around the table to figure out how to run the business following a crisis and ensuring everyone understands their roles and responsibilities.



Ian Tuke, Operations Manager for business continuity firm Plan-b

Tuke says they need to agree on a maximum acceptable outage ‘they can stomach’ without key functions. “Then you work out what systems support those functions and tailor a recovery strategy around timeframe and recovery point objectives.”

And he says, you don’t need a different crisis management plan for every potential event such as earthquake, fire and flood. “You focus on general high level impact which we see in three buckets: technology failure, loss of access to your site and loss of key people.”

You can throw any scenario into those buckets and if a company has done its homework they should be able to recover their generic systems, know where responsibilities for various tasks lie and have a business continuity plan that will work.

Even then, there’s a lot to take on board. The crisis management team needs to consider all the possibilities from evacuation and safety and welfare of personnel to ensuring core IT and security systems — including CCTV and card access — are backed up and can be recovered.

They need to ask who’s going to make the quick fire decisions to keep the business running, who will man the phones, access the information systems, co-ordinate with police and emergency services, contact the media, communicate with stakeholders and customers and pay suppliers and staff?

“Rather than producing a kilo of paper in a documented plan that no-one will ever read, rehearsals help determine what the recovery strategies are and figure out agreed priorities of who should be doing what within a safe setting.”

Tuke says it’s a lot less painful if you can figure out what can realistically be achieved through a simulation exercise than trying to pick up the pieces afterwards.

ADT-Signature’s Peter Freeman says the Civil Defence website makes it clear businesses should have an emergency phone number for people to call to check on colleagues and get updates on what’s happening.

“If someone’s travelling and can’t get in touch with the main office they need to know other numbers to call.”

Freeman suggests there should be a key contact book kept offsite with the phone numbers of key personnel and procedures and instructions about who to contact for security monitoring, physical security and boarding up doors and windows, for example.

Letting people know

The crisis management challenge not only relates to businesses but public organisations including government department, schools and academic institutions. The more people involved the greater the responsibility to have a well thought through plan.

Those responsible for co-ordinating emergency and recovery procedures should be well versed in their responsibilities, attending refresher courses so they remain familiar with the procedures. There should also be a required number of people within any organisation who know basic first aid.

And while it’s essential to have procedures for orderly evacuation, including a head count to ensure everyone is safe, technology can play an important part in an early warning system.

An identifiable alarm and voice message over security or communications networks; alert messages via cellphone or email, and even concise but stern pop-up notifications on computer screens advising staff to leave the building, may ensure everyone is aware of what is required in an emergency.

Specific messages could be generated to key staff reminding them they should now step into their allocated emergency procedure roles. Such notification systems may be incorporated as part of the existing IT or security infrastructure. For university campuses or public places this may include digital signage.

These options could be worked through with technology partners or systems integrators with consultants suggesting they need to be tailored to the need and culture of each organisation. Staff must be also aware of the system and have seen it tested, as part of a fire or other emergency drill.

While there’s a tendency to come up against budgetary constraints, the question must be asked whether ‘return on investment’ arguments are at all valid when weighed against saving human lives.

Vulnerability check

While there’s a legal obligation to have a clear evacuation strategy, including a mustering area for staff to meet in an emergency, Greg Watts Chief Executive of the NZ Security Association, says it likely many businesses haven’t included a security check in the process.

In his view, someone should be given responsibility to check for vulnerabilities during and after evacuation and this should fall to the person or team in charge of evacuation.



Dialock DFT Furniture Locking System

The key to Customer Comfort and Store Security



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

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

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

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



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

HÄFELE
 FINDING BETTER WAYS



Greg Watts, CEO of the NZSA

After an earthquake, he says there should be a policy to ensure electronic security alarms are still operational and whether sliding gates, standard doorways, grills and window fastenings are still intact and secure.

"A lot of security grills and barriers on shop fronts are well designed but some are not. Standard cage doors with mesh and bars are less successful than the ones that slide back and forth because they don't fit into a physical size," says Watts.

While most building access systems have a battery back-up, if the power goes out, the question needs to be asked whether the magnetic door locks still operate or go into a free state. "That's an important aspect to consider.

You wouldn't want a system that hinders evacuation or one that creates unnecessary vulnerability."

A rethink of security policies should also take into account what process there is for re-entry into the building. If the doors are no longer secured how do you check people without security clearance don't sneak in with returning employees?

Off-site workspace

Plan-b's Ian Tuke, a former detective and Senior Manager with KPMG's Australasian forensic practice, says it is important for teams to come together face to face after an event, as 'unusual decisions' have to be made quickly.

He says it's imperative to designate an alternative workspace where there's access to the tools and processes needed for a business to continue functioning.

After the initial earthquake in Christchurch, one of Plan-b's customers allowed employees to operate from home for the first two weeks, something they decided never to do again.

"It was the school holidays and when customers called there were lawnmowers going in the background and kids running around — it was not a productive time."

To prepare for the worst, Tuke suggests a crisis management drill once a year, where call centre and office personnel move to a stand-by site for a day or two. "We do this about 50 times a year for our various clients so they can confidently rehearse their recovery in a bubble."

Tuke says one of his Christchurch customers with 20 or so branches nationwide had its data centre completely demolished.

"We restored their entire environment from our back-up in Albany, including servers and connectivity to all their branches and had them operating as if it was their own office; they just happened to be at our place where the wallpaper was a different colour."

Plan-b has helped more than a dozen Christchurch organisations maintain their businesses following both major quakes. "We still have people in our premises now because their buildings are toast, while a number of their competitors are still working in garages or have gone down the tubes."

Crisis questions raised

NZSA Chief Executive Greg Watts says the Christchurch crisis has raised a lot of questions for both the security industry and businesses, including how things might be done better in the future.

Pressure is on security companies to provide a wider range of services, in some cases including an assurance that customer security data is backed up at more than one location, possibly in another city.

That alone narrows down the field to a handful of Kiwi security firms with monitoring centres in multiple cities, raising the bar for competition as many clients re-evaluate their security needs and providers.

Businesses want a security partner that protects premises and assets with the same level of reassurance expected from a technology service provider, charged with backing up and protecting essential data.

"When designing or upgrading security, businesses should be asking providers what their own plan is and how they will continue operating in the event of a crisis," says Watts.



Backing up systems locally and off-site is becoming a 'no brainer'

NEW

AIPHONE®

GT SERIES

3year
warranty

Hands-Free Colour Video Apartment System with
Picture Recording, Pan/Tilt and Zoom Features



The stylish new GT Series boasts industry-first technology such as a door station with digital pan/tilt and zoom, icon and voice announcement at entrance station and optional hearing loop internal stations for hearing impaired residents.

Featuring simple wiring and DIP switch programming, the system is a breeze to commission. Best of all, Aiphone's legendary reliability is backed by a three year warranty on all the GT Series products.

- Wide angle door station with digital pan/tilt and zoom
- Picture memory internal stations (option)
- Up to four internal stations per residence with internal communication
- Icon and voice announcement at entrance station to guide caller
- Hearing loop internal stations for T-coil hearing aids (option)
- DIP switch programming for fast commissioning
- Choose from hands-free or handset internal stations
- Individual door station per apartment (option)

Proudly distributed by

audioproducts
Group

Address:
1/44 Greenpark Rd,
Penrose, Auckland

W: www.nfs.co.nz
P: (+64) 9 580 1576
E: sales@nfs.co.nz

NFS
NATIONAL FIRE & SECURITY
LOW VOLTAGE ELECTRONIC SUPPLIER

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
PO Box 4, Ahipara,
New Zealand 0449

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

Mr Mrs Ms _____

Surname _____

Title _____

Company _____

Postal Address _____

Telephone _____

Email _____

Date _____

Signed _____

nzSecurity Magazine
A trusted source of information for industry professionals

Since Christchurch, that question is being asked a lot more. "People not only want to know about the level of service you can provide but about back-up systems for their data, wired and wireless sensors and cameras, maintenance, what support you can expect in a crisis and your manpower availability."

Watts says no-one can be a credited monitoring centre unless they have uninterruptible power systems (UPS) and can continue monitoring in a power outage, "unless of course the building falls down".

He says Christchurch placed a big pressure on security personnel and some companies are clearly in a better position to bring in manpower from other regions than others. "People want to know how well geared up you are."

Back-up and storage

While larger organisations such as banks are required by regulation to manage their own back-up and recovery systems, most other businesses are increasingly relying on third party service providers to do this.

Ian Tuke strongly advises against relying on the company secretary, for example, to remember to take back-up tapes off-site each night. "That's ridiculous. You create those back-ups every day for a reason, that's to recover your business if the worst happens."

A big part of having an outsourcing partner, he says, is to have someone else recovering systems and data so even the IT staff can go home and attend to family matters.

"It's far more cost effective these days to outsource business continuity needs than expecting your IT manager to try and sort everything out. The ability to be able to recover through an alternative infrastructure off-site is a no brainer," says Tuke.

However, he warns that too many people don't test and prove their ability to recover business systems from those back-ups and recommends disaster recovery systems be fully tested at least once a year.

"More often than not, unknown hindrances occur when you try to recover your average Kiwi company's back-up. Often things are excluded that turn out to be critical."

Protecting the boundaries

While much of the Christchurch red zone was secured fairly quickly, NZSA's Watts says the initial contract for fencing and barricades went to Australia until a member of his organisation stepped up and challenged that decision.

Ultimately the business was co-ordinated by an Auckland-based

company who ensured much of the fencing was supplied directly from Christchurch. The question remains whether co-ordinators knew of local security resources and capabilities; and if they didn't, what can be done to improve communication?

The fact that some buildings were no longer alarmed or secure after being physically damaged also raised questions. Watts asks, what happens if personnel charged with guarding those buildings can't gain access because the cordons are up?

"You have to hope the security aspect falls back on to the authorities tasked with securing the area but in some cases that hasn't worked and there's been looting and people gaining access to areas where they shouldn't be."

The NZSA and its members are continuing to look at these issues.

Peter Freeman believes an increasingly useful tool for the future will be the CCTV registration database, being championed by the NZSA in conjunction with NZ Police, which may help identify who was in or near an impacted area during a crisis.

Accredited NZSA members are asked to register their camera coverage area and enable access so Police can quickly view footage.

While banks and several other institutions have registered, Freeman says uptake among other businesses has generally been slow.

Another way to protect, monitor and police boundaries in a crisis, is to deploy the growing number of mobile or temporary electronic security solutions available, including battery or solar powered intruder alarms and CCTV cameras that transmit over cellular or radio networks.

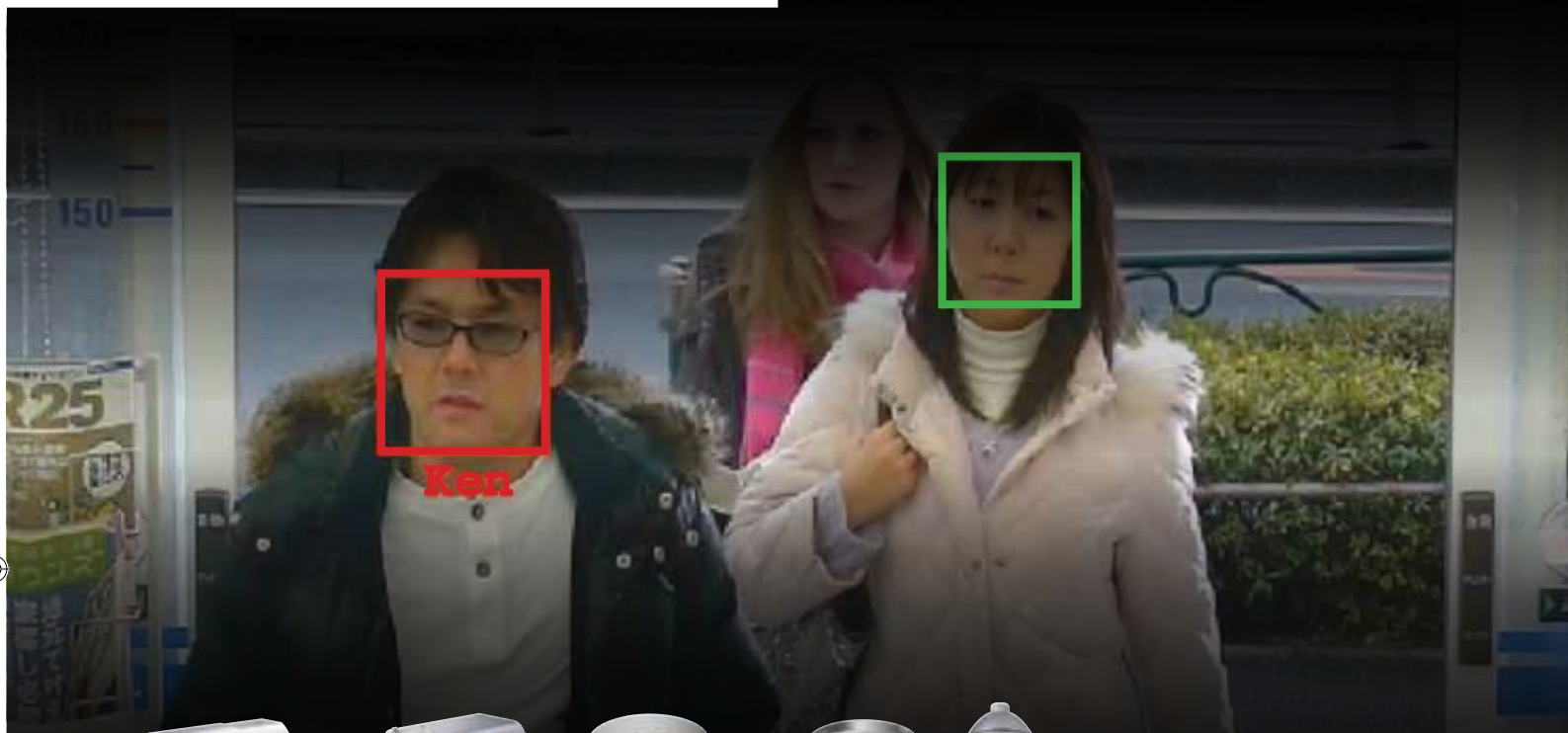
They're typically put in place to secure building, construction or roading sites, but after the events in Christchurch, Freeman believes they'll find a broader range of uses.

There's nothing like a civil emergency or crisis event to sharpen awareness about where our vulnerabilities lie. Hoping someone else, whether its local or central government, emergency services, security firms or IT back-up providers, will cover for you is no longer an acceptable excuse.

A major event, whether it involves acts of God: fire, water, wind or quakes; or God forbid, bombs or acts of terrorism, is the ultimate test of crisis management and disaster recovery planning. Failing to prepare, as the old adage goes, may indeed simply add insult to injury.

SMILE

PANASONIC REAL-TIME FACE RECOGNITION



WV-SP105

VGA/1.3MP
Simple day/night
PoE



WV-SP306

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



WV-SF336

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



WV-SC385 / WV-SW395

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



WJ-NV200

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

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

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



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

Panasonic

ideas for life

panasonic.co.nz

Changes challenge storage and back-up

By Keith Newman

Any business or organisation that does not regularly back-up its essential business data may be complicit in bringing about its own end in the event of a computer systems crisis.

Most companies today are information technology dependent; without a customer database, email access, inventory, supply chain connections, accounts and payroll systems, there is no business.

Increasingly there are legal, business and compliance requirements to store everything in a digital format in-house and off-site at a secure facility. And, it's not only server hard drives that should be backed up and replicated but the data held on PCs and laptop hard drives.

For small to medium businesses most security, antivirus and network management suites can automatically back-up designated files on removable or even remote drives at scheduled times, most often when the system is not in use.

With the right kind of network redundancy and replication, even if one server crashes or principal systems are damaged, you can often be up and running in minutes rather than hours.

Having critical information stored off-site implies a recovery system that should enable you to rebuild data on a remote system after a more severe crash or if the main building is inaccessible.

Keeping track of versions of documents and knowing exactly where specific files are, especially when restoring from a

back-up, is the bane of many organisations, particularly if they're working with multiple file types and storage devices.

As the amount of business data increases incrementally so does the cost of adding disk space on older proprietary systems, particularly as legacy management software becomes less efficient and estranged from industry trends.

Tradition perdition

Traditionally data was stored on magnetic tape but increasingly that's being relegated to archive use as newer disk arrays move to the fore, including storage area networks (SANs) or network attached storage (NAS).

Even then it's recommended regular checks be undertaken to ensure the back-up software recovers data efficiently. And while disk space on modern systems is increasingly cost effective, there remain serious concerns about long term use.

"You can't really afford to do long term archival of 5-50 years on disk; the technology changes rapidly, disks fail and they do not have the longevity of tape," says Gartner Group's VP of data centre infrastructure research, Phil Sargeant.

What's more, he says, those who don't stay on a continual migration path, risk becoming stranded over the next five years as new approaches for storage and back-up are adopted. For example high speed flash is expected to become 'a pervasive new tier of storage in the near future.'

Sargeant suggests prioritising critical data and storing or archiving secondary data on less expensive disks or tape storage, while planning to migrate to more energy efficient solutions that cost less to run.



*Phil Sargeant, Gartner Group's
VP of data centre infrastructure research*



*Rasika Versleijen-Pradhan ,
IDC's New Zealand senior services analyst*

While compression has long been a standard space saver, de-duplication takes things a step further, stripping out multiple versions of files and only updating what has changed so data occupies less space and moves more quickly over networks.

The trouble is, the older your system is, the less likely it is to support these new tools. As an interim solution you might be able to add an 'appliance' to 'thin' out or optimise data. Virtualisation can help standardise access to data across different vendor's equipment.

Did the back-up back up?

Since Christchurch, there's renewed focus on auditing and testing back-up and recovery systems to determine how long it might take to get businesses back on track, says IDC's New Zealand senior services analyst Rasika Versleijen-Pradhan.

Companies need to determine what the acceptable time lag is, then establish best practice to ensure minimal disruption with vendor service level agreements (SLAs) around those capabilities.

A recent IDC survey of 100 organisations in New Zealand revealed that disaster recovery was among the top priorities when improving or designing a data centre. One of the keys was spreading the risk across more than one data centre or region to increase client confidence.

"The Government for example is adamant it wants to have local data centres spread across geographic areas in New Zealand with certain distances between them to make sure it can continue business as usual, regardless of outages or disasters," says Versleijen-Pradhan.

She says data centre providers are realising that it is critical to offer vendor independent services and a relationship that is as close as other partners in the supply chain.

Another challenge is the move to 'the cloud' or on-line services, which demands more flexible and integrated storage media to better handle intense traffic loads.

So far there's been little deployment of cloud services for storing mission critical data; it's more for back up and archiving of low performance data. However that's all about to change.

Ovum's 2011 Trends to Watch report, says the volume of data stored remotely in 'the cloud' continues to soar; in some cases by as much as 50 percent a year, with a growing demand for higher level access.

It says storage will continue to be challenged by the public cloud, with recent breakthroughs suggesting it could become a major competitor for off-site back-up and storage.

As the data deluge continues, customers will want to deal with vendors and resellers who cannot only provide storage capacity and management systems, but outsource, manage and host storage in the private, hybrid (a mixture), and increasingly the public cloud.

Complexity challenges

In its sixth annual 'Disaster Recovery Study', Symantec suggests the growing complexity of business IT infrastructure presents major challenges for managing, protecting and recovering mission critical applications and data.

It suggests that providing a confident level of security across an array of physical, virtual and cloud resources is increasingly difficult, with virtual systems are often poorly protected.

The study says only a half of the data on virtual systems in New Zealand is regularly backed up, and only a quarter of respondents used replication and failover technologies to protect virtual environments.

Symantec indicated that 47 percent of virtualised servers weren't included in current disaster recovery plans. It warned that using multiple tools to manage and protect applications in virtual environments creates major difficulties for data centre managers.

Symantec said 93 percent of back-ups only occurred weekly or less than daily. The survey blames resource constraints, lack of storage capacity and incomplete adoption of advanced and more efficient protection methods in virtual environments.

And 94-96 percent of respondents claimed lack of primary storage and back-up storage made protecting mission critical data more difficult.

Keeping it simple

The survey also showed recovery from outages took twice as long as expected. If a major disaster were to occur that destroyed their main data centre, respondents expected to be up and running within two hours.

While that was an improvement of two hours on the previous year's survey, the reality was the average downtime per outage, over the previous 12 months, was six hours. There was an average of six downtime incidents in that period, as opposed to a global average of four incidents.

When asked the cause of outages over the past five years, 93 percent of Kiwi companies cited system upgrades, power outages and failures (63%), cyber attacks (53%) and natural disasters.

While introducing new technologies such as virtualisation and cloud computing bought costs savings and improved disaster recovery, Symantec said it was clear many businesses had not yet mastered the art of managing across these environments.

It recommended data centre managers simplify by adopting tools that provided a comprehensive solution with a consistent set of policies across all environments.

The fewer tools required to manage virtual, cloud and physical environments, the more organisations would save in time and training costs while having a better shot at successfully automating processes.

As networks get faster and storage capacity grows from terabytes into petabytes, there's clearly a growing need for smarter more dynamic technology to futureproof an organisation's needs through lower cost media and more intuitive management software. Many Kiwi businesses however cling to their old back-up systems, fail to regularly test them, or realise that without a planned upgrade path they may be heading into an information limbo.

Securing The World One Door At A Time

Grow your system from one location and one PC to 32,000 locations and up to 999 PCs on a Wide Area Network.

Intelligent Controllers give DSX enormous flexibility and diversity.



New Zealand's Exclusive
distributor for DSX



Contact:
Ph: 0800 377 379
0800 ESS DSX
Sales@eSecuritySales.com

Sensitive data grows faster than protection efforts

By Keith Newman

We're drowning in data, running out of places to store it and failing to secure much of the sensitive stuff, according to the latest EMC Corporation/IDC Digital Universe study.

The 2011 'State of the Universe' report shows the curve continuing to advance skyward with expectations of surpassing 1.8 zettabytes (1.8 trillion gigabytes) this year.

In 2009 the digital information we created and copied grew 62 percent, up from 800 billion gigabytes the previous year. In 2010 the 'digital universe' cracked the zettabyte barrier for the first time — a zettabyte is a trillion gigabytes, the equivalent of 75 billion fully loaded 16Gb Apple iPads.

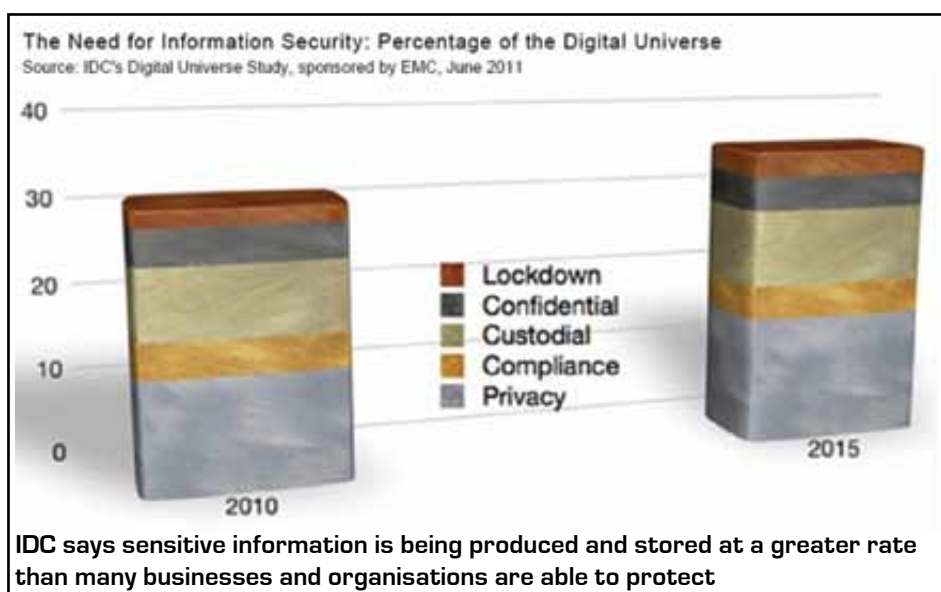
The data deluge will continue over the next decade as voice, TV, radio and print continue to complete the journey from analogue to digital; and new streams of digital information and ways to process and repurpose it, are added to the mix.

In effect the world's information is doubling every two years. And while 75 percent of the information in the digital universe is generated by individuals, 80 percent of it will pass through or be stored by some trusted third party or enterprise.

The report concludes that we need better data storage and management tools and techniques, but also drops the bombshell that sensitive information is growing faster than our ability to secure it.

It suggests less than a third of the information we generate has minimal security or protection and only half of what should be protected is protected.

The growing amount of insecure information is largely compounded by government regulations, and company policies and processes that insist records be kept.



The pressure to ensure data doesn't get lost or fall into the wrong hands is further complicated by employees leveraging more mobile devices, consumers sharing more personal data and companies finding new ways to mine this data.

Different degrees of security are required for personal privacy, compliance or custodial reasons, so account information, for example, isn't leaked or used for identity theft.

Trade secrets, customer lists and internal memos need to remain confidential and 'lockdown' data such as medical records, financial transactions, personnel files and military intelligence require the highest security.

In order for organisations to maintain trust with clients, business partners and customers, the integrity of information needs to be assured at all times. Its origin has to be verified, along with the processes and computing systems that generate, capture and manage it.

Even the credentials and identities of individuals and business entities that have access to the information need to be part of the secure loop.

The EMC/IDC report says organisations are under increasing pressure to adopt policies to manage security and compliance obligations even across the laptops, tablets and smartphones used to conduct business and personal affairs.

In fact an entire industry has grown up around laws, regulations and customs pertaining to information in the enterprise, often resulting in regulatory compliance systems being built into storage management systems.

The EMC/IDC report says new security practices and tools can help enterprises identify the information that needs to be secured and at what level, using specific threat protection devices and software, fraud management systems and reputation protection services.

The report suggests that by 2020 the world will generate 50 times the current amount of information while IT staff managing this will grow less than 1.5 times. Clearly then smarter more secure storage and management tools will need to continue evolving to keep pace.

Endless specifications.

One solution.



HID 13.56 MHz migration solutions:



- Enhanced security with 13.56 MHz technology
- Multi Applications with only one system
- Seamless migration from HID Prox® or MIFARE® to HID iCLASS® or DESFire® EV1.

Whatever future requirements are – new HID migration solutions enable seamless migration to future proof smart card technologies while supporting common legacy systems at the lowest total cost of ownership.

To find out when and how to migrate and what solutions are available please visit hidglobal.com/onesolution-NZSec and download our latest migration whitepaper. For more information please call **852-31609831** or email to asiasales@hidglobal.com

Gallagher Hosts Technical Account Managers Conference

Hamilton-based Gallagher Group was a hive of activity recently as they hosted technical account managers from around the world. The week-long TAM conference was a future focused event for the staff in the market to gather at the head office and discuss upcoming products and plans for the direction of business for Gallagher.

The technical account managers got valuable face to face time with product managers as the company prepares for the launch of their latest product, Gallagher Command Centre v7.00. Gallagher will have a major product launch later this year for Command Centre v7.00 which has already received much positive feedback from channel partners and users around the globe.

Gallagher's new Command Centre Premier in v7.00 ensures the security team sees exactly what they need to see, sized and placed on screen exactly where they want it. From alarm management, to general monitoring and control; from challenge to cardholder administration, the information the security team needs is provided seamlessly and in context, exactly as they have designed.

With an in-built and intuitive user interface design tool, high resolution multi-monitor workstations have never had so much power. Operators can create or adjust screen layouts in minutes with previews updating as they work. No specialist skills are needed, and the job is done in minutes not hours. They are



able to mix and match information from different sources and filter the content to provide operators with real situational awareness. Everything they need and nothing they don't, Command Centre Premier is customisable right down to an individual's role, providing targeted information at the operator's fingertips.

The conference took a hands-on approach with two full days of workshops for the technical account managers. The interactive workshops provided opportunities to discuss what had been going well and have input into future roadmapping for upcoming Gallagher products.

"There has been very positive reaction to v7.00, but the associated workshops also gave us an opportunity to prioritise and work out 'where to next'," said Gallagher Product Manager, Trish Thompson.

"Workshops and demos give people a chance to give immediate and direct

feedback, something which can be missed when TAMs are in their markets and focussed on other areas. It also gives us at head office an opportunity to highlight specific areas of the product, to pass on detailed technical information and future visions for our products which may not be immediately obvious at first glance," she added.

"The TAM conference is incredibly useful for being able to gauge the main pain-points and new product requests from our different geographic markets. It helps direct decision making on where to focus development effort next."

The practical element of the conference was well received by those present, as well as the regional update session, where representatives from each region – New Zealand, Australia, USA, South Africa, UK, Asia and the Middle East – got to present the successes and challenges of the past year.

Head office staff found the conference to be a great opportunity to hear from the staff members who deal directly with the market and to understand what the challenges and issues were in their individual settings.

Gallagher's security division provides premium integrated security solutions encompassing both systems and professional services. They deliver electronic access control, intruder alarms management, perimeter security and compliance management through a single integration platform.



The Falcon 8200 Series Automatic Operator

Tough enough for high use areas while elegant enough for interior spaces, the new commercial grade Falcon 8200 Series Automatic Operator by Ingersoll Rand Security Technologies is the smart choice for industries where a reliable and tough door operator is critical.

This new addition to the Falcon range is one of the most cost effective solutions available for assisted living environments, retail, hospitality and any application where interior doors require added assistance.

Everything you need to install the Falcon 8200 is in the box, making installation as quick and easy as possible. All necessary features are built-in making configuring simple and you can make more openings accessible than ever before.



Falcon 8200

This intelligent system has many user friendly features such as sensing and overcoming external pressure conditions through graduated energy assistance for secure latching, open position learning to prevent wall and door damage and obstruction detection preventing damage to doors and users.

The Falcon Automatic Operator is not only user friendly, but installer friendly

For more information on the new Falcon 8200 Series from Ingersoll Rand Security Technologies, visit www.ingersollrand.co.nz or Phone 0800 477 869

with an on-board power supply, one-piece mounting bracket, non-handed motor gearbox and fastening notches for faster installation.

Ingersoll Rand Security Technologies is pleased to announce that Gary Crump will assume responsibility for our commercial electronic security business effective 1 August 2011.

In his role of Business Development Manager, Gary will be responsible for demand creation, channel development and establishing strategic alliances to grow Ingersoll Rand's commercial electronic security business in New Zealand and the Pacific Islands.

Gary has several years experience in electronic security and has been successful in winning a number of major projects, while utilising his strong relationship skills and product knowledge.



CO Series Stand Alone Electronic Locks

Modern, Secure, Robust.

- Keypad, proximity cards and magnetic stripe card options available.
- Convenient and secure.
- User friendly.
- Open platform.



CO-100 pictured

0800 477 869 www.ingersollrand.co.nz

IR Ingersoll Rand
Security Technologies

Gate automation is all torque

When the people at Government House wanted a system to open its gates weighing three quarters of a tonne, the engineers at Withington Electrical got their calculator out

Engineers at Withington Electrical have just completed a \$50,000 installation of automatic gate equipment at Government House in Wellington. The work is part of the government's \$43 million renovation project of the heritage building.

The bespoke job meant the Withington Electrical had to upscale its range of motors, gears and gate arms to design a pair of units that could handle opening gates weighing 750kilos (1653lbs) each.

Not only that, the opening and closing time had to happen in less than 12 seconds.

"Our system came in just under the specified time limit at 11 seconds," says the firm's Managing Director, Simon Withington.

Withington started his automated gate firm 15 years ago following a career as an electrical contractor.

The firm's motors normally handle gates weighing up to 350 kilos, so finding a pair to open Government House's gates was a challenge.

"We don't normally supply gear for gates weighing this much, it is a big ask," says Withington. "We found a company in Australia that could supply the motors and gears we wanted, but then we sat back and thought 'all we have to do is build on what we already make here' – it was just a case of getting the maths right in the end."

Withington's team designed, built and installed the larger motors and gearing mechanisms in less than five weeks.





One issue the team had to overcome was the distance of the gate from the corner of the heritage-listed columns.

"Normally a gate will be on the corner, so a short arm will often be enough to connect the motor to the gate, but these gates were well away from the corner of the column and they couldn't be moved to the optimum position."

A new design of arm was made and – says Withington – it all worked perfectly from the moment the installation was completed.

"Having made a smaller version it was easy to go bigger as most of the design work had been done," says Withington.



"The reach of each arm is 1.7m and in a normal situation these would be good for gates up to 6m in length."

With gates weighing three quarters of a tonne being opened, some nifty computer programming is needed to ensure they have a soft opening and closing.

"Again we just used what we know to work well and altered the programming slightly to compensate for the heavier gates," says Withington.

Another installation issue was that, because the property is listed, the weatherproof boxes containing all the electronics could not be physically attached to the two columns – as is normally the case.



"The motors are mounted on pedestal frames, the specification called for nothing to be attached to the heritage columns which is why a separate foundation for the motors was made," says Withington.

Making the motors has, says Withington, created some interest in the gate automation industry with installers now calling for more details.

"Because of the interest we will be adding these new larger models to our range," says Withington. "It just shows that a bit of flexibility can go a long way."

www.withingtonelectrical.co.nz

High Speed Gate Automation

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



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



A barrier arm for Peter Jackson's Wellington Head Quarters

We also manufacture, install and service

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



Swing gate motor for gates up to 15m



These swing gates are part of the Government House refurbishment

We design and manufacture all our automation products in Wellington, but pride ourselves on our installation and service anywhere in New Zealand. For more information and trade enquires contact:

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

The New Zealand Security Conference And Exhibition

Rendezvous Hotel, 71 Mayoral Drive, Corner Vincent Street, Auckland
17 - 18 August 2011

This year's New Zealand Security Conference and Exhibition will be held at the Rendezvous Hotel, Auckland on 17-18 August 2011.

Prices for the two day conference and exhibition are:

Member	\$495 + GST
Non Member	\$595 + GST
Industry Breakfast	\$35 + GST
Awards Dinner	\$95 + GST

**to qualify for membership rates you must be an NZSA, ASIS, NZISF, ASIAL, NZIPI, ICA member.*

Registration

Registration is open to members of NZSA as well as any person involved or interested in the security industry.

All enquiries regarding the Conference should be directed to the NZSA office on (09) 486-0441 or info@security.org.nz

Team Discounts

Discounted rates are available when multiple people from the same organisation register at the same time:

- ◆ 5% discount for 3-5 registrations
- ◆ 10% discount for 6 -10 registrations
- ◆ 15% discount for 11 or more

Early Bird Discounts

A 5% discount of the full conference rate (prior to team discounts) will be given if registration, bookings and payments are received by 22 July.

Cancellations

If you must cancel for any reason please notify NZSA in writing at least 10 business days prior to the start of the programme and a full refund will be given. Cancellations received within 10 business days of the conference will be subject to a \$95 fee.

No refunds will be made for cancellations received on or after Wednesday 10 August 2011

Delegates

If you wish to register more than one delegate (such as your spouse/partner or colleague), please use a separate form for each registration.

Forms can be photocopied or downloaded from www.security.org.nz.

Please refer to the full Conference brochure for more information.

CPP Credit

Attendance to the conference by current CPPs can be reported for credit towards recertification.

Accommodation

Accommodation has been arranged at The Rendezvous Hotel at special conference rates. Deluxe Room Only \$160 (incl. GST), Deluxe Room Breakfast included \$180 (incl. GST). Bookings can be made via the home page of the NZSA website.

3 Easy Ways To Register

Email
info@security.org.nz

Facsimile
+64 9 486 0442

Post
PO Box 33 936, Takapuna,
North Shore City 0740, NZ

Industry Breakfast

Wednesday 17 August. A special guest speaker will be present. Cost of \$35 +GST per person.

Awards Dinner

Thursday 18 August. The Awards Dinner and presentations will be preceded by a cocktail hour and followed by entertainment. Cost of \$95 +GST per person.

Awards

These will be presented at the Awards Dinner by a special guest.

Any nominations for awards, should be forwarded to either Josephine Gallagher of the ETITO at Josephine@etito.co.nz or the NZSA office by email info@security.org.nz

intek

ASIS
INTERNATIONAL
Advancing Security Worldwide™

NEW ZEALAND SECURITY ASSOCIATION
NZSA
SECURITY

NZSecurity
Magazine
A trusted source of information for industry professionals

Conference Agenda 2011

Wednesday 17 August

Speakers

7.30am	Industry Breakfast An Insight into the Current Economic Conditions	Chris Tennant-Brown, ASB Bank
9.00am	Conference Opening	
9.30am	National Crime and Security Update	Speaker details withheld for Security Purposes
10.30am	Tea Break	
11.00am	Keynote One	Adam Montella, The Disaster Guy
12.30pm	Lunch Break	
1.30pm	Providing Clarity in Crisis	Nick Thompson, Director, Thompson & Clark
2.15pm	Keeping the Lines of Communication Open in Christchurch	David Nielsen, Security and Facilities Risk Manager, Chorus
3.00pm	Tea Break	
3.30pm	Managing Staff Welfare in a Crisis	Michael Moriarty, Training Manager, First Security
4.15pm	IT Disaster Recovery	Ian Funnell, Code Blue
5.00pm	Close of Day One	
5.00–7.00pm	Cocktails	

Thursday 18 August

9.00am	Conference Main Sponsor Presentation	
9.15am	Security Training Update	Michael Frampton, Manager of Strategy and Corporate Relations at ETITO
9.45am	Overview of Microsoft Global Security and it's Operations Centres	Speaker Shayne P. Bates, CCSK, CPP, CHS-V, DABCHS
10.30am	Tea Break	
11.00am	Keynote Two	Dr. Marc Siegel, International Security Standards and Auditing
12.30pm	Lunch Break	
1.30pm	Keep Your Recipe Secret: Ingredients To Safe-Guard Your Confidential Information	Jason Weir and Barry Foster, Deloitte
2.15pm	Security Licensing Authority and Compliance Unit Update	
3.00pm	Afternoon Tea	
3.30pm	Update On Legal Developments	Turner & Hopkins
4.00pm	NZSA Procurement Update	Peter Royle, CEO, GSB
4.30pm	NZSA Auditing Update	
4.45pm	Closing Remarks	
5.00pm	NZSA AGM	

intek

ASIS
INTERNATIONAL
Advancing Security Worldwide™

NEW ZEALAND SECURITY ASSOCIATION
NZSA
SECURITY

nzSecurity Magazine
A trusted source of information for industry professionals

Learning to get the most out of smart cards

It is when you lose your wallet that you realise just what a card-dependant society we are. With the cash in your wallet gone along with the cards, you are in limbo until the banks open again and you can convince them that you are the person you claim to be without producing any cards or a licence photo.

But even though cards are essential to modern life, the insecure mid-1970s magnetic stripe cards have proved surprisingly resistant to takeover by the far more secure smart cards.

It was only in March this year that New Zealand's EFTPOS terminal network became fully ready for smart cards. But even then, some retailers had to be dropped from the system because their terminals were no longer compliant.



Peter Neil, Red Crater Software Solutions

They weren't exactly caught in a whirlwind of change.

"New Zealand retailers are being forced to replace EFTPOS terminals as networks ramp up capacity and performance for a new era of services based around smart cards," complained The Telecommunications Review when smart cards seemed imminent – right back in August 2004.

In fact, smart card technology has been around for some 15 years or so, but the security industry is only gradually learning how to get the most out of the technology.

Smart card expert Peter Neil of Red Crater Software Solutions says multifunction smart cards provide a way of leveraging extra business value from ordinary stand alone access control systems.

Added value

Neil was the solution architect on a recent smart card project for Waiariki Institute of Technology in Rotorua. The tertiary education institute had security needs - identity and access control - and combined them with the added value services of public transport, printing and photocopying.

"Incentivising students to use public transport was important because they do not have a lot of space for parking," says Neil.

"They really want to entice students to go to Waiariki as opposed to one of the many other institutions around the country and a student card that works on public transport is a good value proposition."

But one of the challenges of the project was integrating with the bus ticketing system in the city, a task which was not just about card reader compatibility but also about the willingness of outside parties to share information on system administration and back office functions.

You have to be comfortable with a collaborative style for that approach to work.

"It is quite understandable other tertiary institutions might have security managers that want to look after their own cards and not want anything else on them," says Neil.

"From a technology point of view it is possible to come up with good solutions but from a process perspective some people prefer to stick with what they know."

Spin off

But that approach misses the spin off from adding more functions to an access control smart card – better access control security as a result of the extra value placed on the card as users grow dependant on them for other functions.

"The most common security smart card applications today are access control and printing/photocopying," says Neil.

"But let's say you are in an organisation with fairly slack access processes whereby you can turn up and wave at the receptionist and she will let you in. In this environment it is not a big deal if you leave your card at home.

"But if you have to badge your card at the copier or printer before it will release your job then the probability of remembering your card for work every day rises dramatically.

YOU HAVE MADE THE RIGHT CHOICE

The right choice is choosing DVTel's Latitude NVMS!

Award Winning

DVTel's award winning Latitude NVMS® is an open standards, IP-based software platform with features including Scenetracker, Casebuilder and Mentor, turning the application into a surveillance management system.

Technology

The on going road map provides you with a sense of satisfaction for your investment choice, protecting you well into the future.

Design

Latitude was designed for the end user in mind - Open platform, extremely easy to use, with a dynamic visually enhanced user interface.

Reliable

With installation sites nearing **400** throughout Australia and New Zealand, and ranging from discreet sites to major installations (one of which has over 4300 cameras), DVTel's Smart Security Solutions are the most end-to-end IP based security surveillance systems deployed today.

Professional

Exclusive suppliers of DVTel, Hillsec, offer an unmatched sales and product support of the DVTel system with:

- Regular scheduled Certified Training
- National sales branch coverage in Australia and New Zealand
- Dedicated national IT team of over 20 staff
- Professional Services



AUCKLAND

Penrose 09 525 8007
Albany 09 525 8007

CHRISTCHURCH

Sydenham 03 374 6277

WELLINGTON

Petone, Lower Hutt 04 939 9355

“I think that is where a lot of people have not really cottoned on to the true value of smart cards.”

Biometrics

Smart cards can also provide quick two factor identification – card and fingerprint – for biometric access control in high security environments.

Neil says this is only practical with smart cards because accessing server based biometric data is slower.

“It is about performance. When you start talking thousands of users, physically it is quite time consuming for those devices to resolve biometric data whereas with the data stored on your smart card, it is a local look up.

It is easy to forget that wired connections back to a server aren't viable all of the time – as we've seen in Christchurch. So having the data stored on a card is beneficial in situations like that.”

Access control proximity smart cards, also known as contact-less cards, do not require actual contact with the reader, which makes for quick and easy access control. A common design of smart card of this type used in New Zealand is Mifare (my fare), a name that reflects its overseas public transport origins.

Neil says unlike conventional proximity cards which store a single number, even the lowest capacity Mifare smart card can store 15 different numbers.

“Let's say your access control system is a Cardax system and one of your leased premises is an HID site with HID smart card readers. You can have completely separate numbers on that card that will work on both systems. From an access control perspective that is one of the big advantages of using smart cards over simple proximity cards.”

However proximity smart cards like Mifare do not have the processing power, capacity and higher security of contact smart cards, often called chip cards, which draw power from the card reader as a physical connection is made – for instance in an EFTPOS terminal.

According to Neil there is a lot of diversity and range of contact smart cards types, from low-tech, low storage cards, to bank issued cards that look almost identical but have strong security and large amounts of storage on the card.

“We quote projects for high security applications such as computer logons where the price might be \$40 and the clients says a mate of a mate can get a chip card for 30 cents. But even though they look the same they are actually quite



different and the cost depends on what functions you are using them for.”

Single sign-on

Higher security contact cards are preferred for single sign-on computer systems where a smart card grants access to multiple computer systems without requiring repeated logins.

According to Neil large organisations like Shell, Robobank and Microsoft use this type of system around the world not only for office computer logons but also for people who access the networks remotely via virtual private networks. Some of these cards are a combination of contact smart cards and proximity smart cards for access control.

“That becomes a really good security tool for organisations because it provides better security for your physical assets as well as your computer assets,” says Neil. Contact cards are more secure because to log onto a computer you need to put the card in the reader and enter a PIN.

“If you need to go out of the office to go to a meeting and you have to go through an access control door then you will have to take the card with you.

Normally the readers and computers are configured so that when a card is taken out of the reader it will lock the workstation immediately instead of waiting ten minutes for a screensaver.

Again, if you are an organisation that has got a bit of a slack attitude to physical security and you leave your card at home, it's no big deal.

But if you are in an organisation that is using those cards for computer login as well, you know you are going to have a pretty unproductive day if you leave your card at home, so you make sure you always have it.”

Health and safety

Another add-on for security smart cards is in workplace safety, says Neil.

“There are mine sites in Australia that store your health and safety information on the smart card as well as your training details.

For example, if you haven't had the right training, you can't drive a forklift. If you have had the training, the expiry date is on the card and when your current training lapses your ability to operate the forklift also lapses.”

But the more sophisticated a project is, the more the system set up and card management comes into play, especially across different division or third party organisations.

“The issue around card management is one of the major stumbling blocks to amalgamating smart cards,” says Neil.

Issuing smart cards for access control is quite easy – they purchase the cards which might be pre-programmed, learn the card into the system, if it is an ID card they print it, hand it to the person and away they go.

As soon as you add another application, say photocopying and printing, then you have another step. I might program, print and issue a card, but the cardholder may have to go off somewhere else to get that card programmed into their printing system. If they have got cash on the card it has got to be on another system. If the card comes from a bus company it has got to go through a whole lot of other steps.

And if the person loses the card the whole process of removing everything they had and re-allocating it becomes logistically challenging for some sites.

So one of the key things for a successful implementation of multiple application smart cards is that organisations need

PANOMERA EFFECT

The Panomera effect: highest detail resolution at every distance

Panomera can be adapted to every customer's needs and the resolution can be scaled nearly limitlessly – up to 51 megapixels in real time.

Panomera's resolution at 160 m distance would correspond to that of a 215-megapixel camera! Because the Panomera effect begins where conventional HD and megapixel cameras reach their limits.

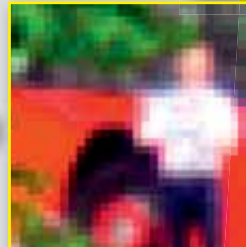


Dallmeier Panomera DP6000 Long Distance camera compared to Nikon D7000

Standard
16 Megapixel Camera

PANOMERA

525 ft / 160 m



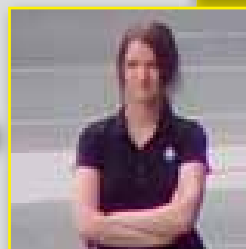
5

328 ft / 100 m



4

197 ft / 60 m



3

131 ft / 40 m



2

66 ft / 20 m



1

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
PO Box 4, Ahipara,
New Zealand 0449

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

Mr Mrs Ms _____

Surname _____

Title _____

Company _____

Postal Address _____

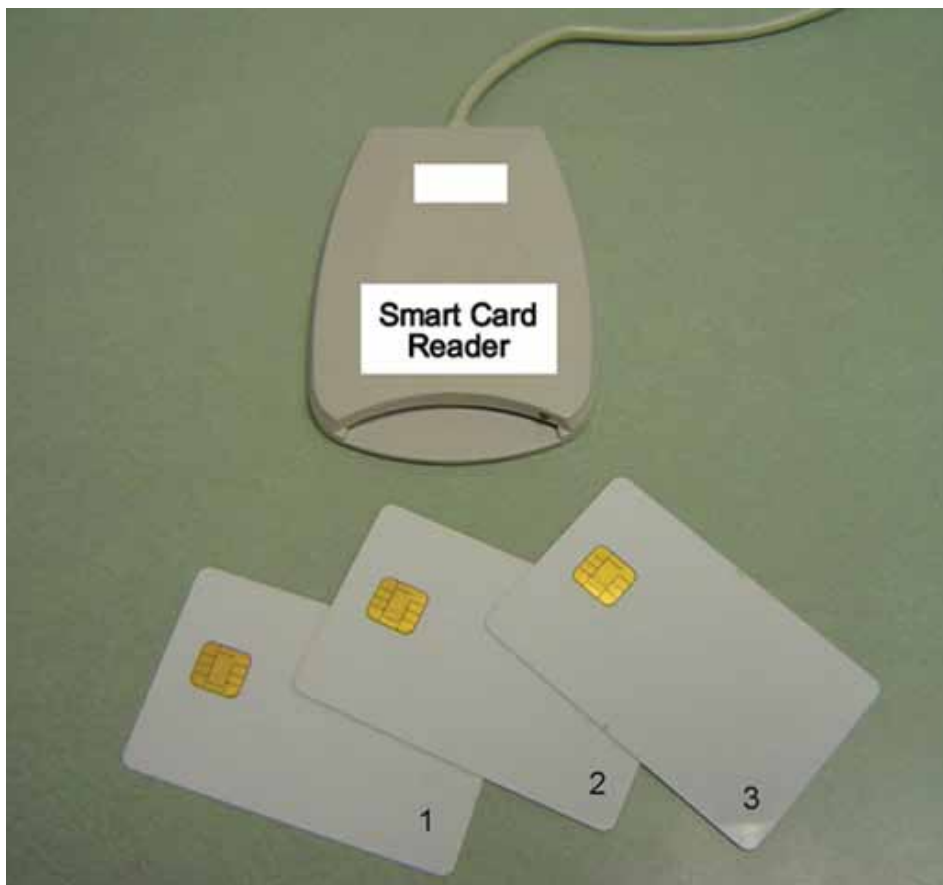
Telephone _____

Email _____

Date _____

Signed _____

nzSecurity Magazine
A trusted source of information for industry professionals



to think through the card issuing and programming process. If it is a manual process they need to have prompts in the workflow or they may want to automate it using software.”

NFC mobiles

But just as our EFTPOS system and the security industry get to grips with implementing smart cards, NFC (near field capable) mobile phones are being announced.

“It is like having a smart card reader and a smart card chip built into your phone,” says Neil.

“Most of the times they emulate a Mifare smart card, so potentially you can have a mobile phone programmed for access control.

In theory – I don’t know if anybody has done this – if you wanted to assign new temporary access you could send an MMS (multimedia version of a text message). The message could load security data on to your phone then you could use your phone on the card readers. To revoke the security access you could send another message to cancel it.”

Neil says this would be good for access control of contractors visiting a site but the main driver is ticketing for major events for stadiums in Europe.

“A lot of stadiums are set up for using low cost smart card based tickets for entry to major events, but the new idea would be to order a ticket online, have it

sent to your mobile which you badge at the entrance to the venue using the NFC feature like a proximity card.

“But the concept is that it also acts like a reader as well so if I wanted to send my ticket to you because I no longer want to go to the event, I just send it on to you and it transfers from my phone to yours.”

Business context

But here in New Zealand NFC mobiles are still a long way off and we haven’t even seen the back of magnetic stripe credit cards yet.

The challenge right now for Neil and his colleagues at Red Crater is to implement smart card solutions that extend what can be done in an ordinary New Zealand security and business context.

“The cards and the technology are relatively simple – it is more around the process,” says Neil.

He says with the Waiariki project they were able to elicit cooperation from vendors of third party systems because they don’t sell those systems themselves and don’t provide any threat to incumbent providers.

According to Neil that is where a technology agnostic and independent solution provider like Red Crater finds its niche.

“It is not about doing really weird things, but things that are quite practical and relevant,” he says.

Unlocking the potential – what we must do now

Most people in the security industry would have come across mention of literacy and numeracy in recent times. In fact it's a subject that has and will continue to get plenty of attention – and for good reason. In this article we outline five key things you need to know about literacy and numeracy and the role each of us needs to play to make a difference to security firms, staff and the broader New Zealand community.

1. It's a priority for New Zealand

More than one million New Zealanders have literacy and numeracy skills below those needed to participate fully at work, home and in their communities. That's 43% of all adults aged between 16 and 65. A whopping 80% of these people are in work, which means they are not achieving their personal potential or ability to contribute in their work and careers. A workforce with high levels of literacy and numeracy skills will be better able to contribute to New Zealand's economy – importantly there are also key social benefits for parents, families and communities.

2. Keeping pace with change

Changes have occurred throughout workplaces that mean a greater demand for higher levels of literacy and numeracy. Modern workplaces are increasingly complex. There are new technologies evolving all the time, growing competitiveness and demand from customers and clients for higher quality services to be delivered cost-effectively. Strengthening literacy and numeracy skills is needed to keep pace and support the ongoing transformation of workplaces into ones that are highly productive and in which staff do more valuable work – for their firms and themselves. More skills mean better communication with customers and colleagues, improved recording of information, use of technology and handling of all kinds of data and tasks.

3. It makes sense – at work and while learning

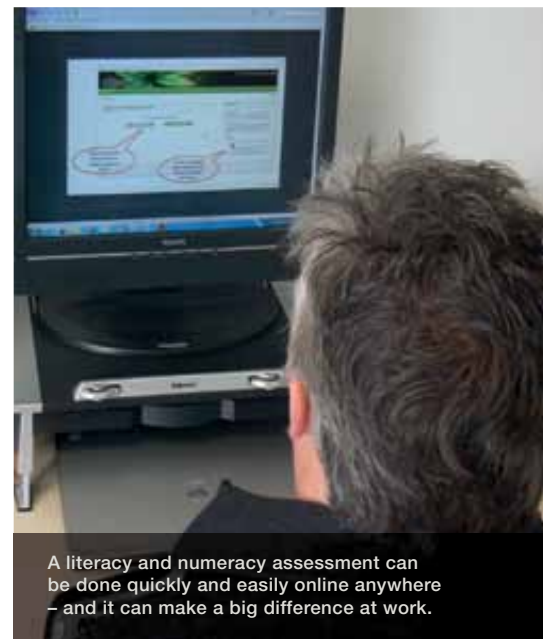
The security sector is one of many in New Zealand

identified as having great potential to be unlocked through improved literacy and numeracy skills. Security firms and trainees are already on the road to working on literacy and numeracy – and realising the benefits from small and bigger wins. They're not alone though – companies across the country are taking the same journey and like security, a number of others are doing so with the help of ETITO. For example, ETITO is working with electrical apprentices to give them the help they need to improve their literacy and numeracy so as to be able to successfully complete their training and make an even greater contribution in their work. Some adults left school with limited skills and qualifications. For others, English is their second language. The fear of maths or reading can be a powerful barrier to people being able to take up new challenges or learning – but it doesn't need to be.

It makes sense to focus on literacy and numeracy at work and particularly while people are gaining qualifications. Better literacy and numeracy means a better chance at success in completing qualifications and then applying the knowledge to the job.

4. What we need to do together

All security trainees working towards a Level 2 or Level 3 National Certificate in Security should complete a literacy and numeracy assessment before beginning their qualification. There is a specially developed online assessment available to do this. It takes just 20-30 minutes to do and people can complete it from a computer at work,



at home, or at a local library. Some firms have found making a computer available to trainees and booking them in for assessments works. The assessment will identify literacy and numeracy abilities and where they might need to improve to help a person meet the demands and needs of their job. ETITO will receive the results and our team can then work with firms and trainees to tailor the kind of things that will work for them to make a difference. This could involve changing some practices or tasks or reviewing resources and materials to ensure they are going to be able to support improved results.

5. Just start now

No matter how or where the assessment is done the important thing is to do it as soon as possible. We can help you get set up with the log in for assessment and other information you need.

Contact your ETITO Training Manager for help on getting started or our vocational literacy manager Lee Agnew at leea@etito.co.nz or phone [09] 583 1347.

www.etito.co.nz

email: info@etito.co.nz

Auckland 09 525 2590

Wellington 04 499 7670

Christchurch 03 365 9819



ETITO

Intelligence where you need it

Improve your bank's safety and security processes with video analytics

Banks face diverse threats every minute of every day — from minor verbal customer altercations to serious robberies. And with multiple sensitive areas, including ATMs, entrance doors, teller lines and vaults, the amount of video information to analyze is tremendous. That's where intelligent network video innovations make all the difference.

To help monitoring personnel focus on the right incidents and respond in the best way, security vendors have developed intelligent video (IV) applications for better analytics — some of which have been proven to increase safety and security in banks.

Audio detection provides sound security

Often, the first hint of trouble is sound, not sight. This application uses noise — such as loud, threatening voices — as a trigger to transmit and record video, or to alert operators of suspicious activities. Axis offers audio detection in all network video products featuring audio support.

Tampering alarm keeps you focused

As part of your front-line defense, cameras are obvious targets for would-be criminals. Active Tampering Alarm is an application available in select Axis network cameras that alerts security staff of disrupted camera operation caused by vandalism or accident — such as redirection, blocking, or defocusing.

Intrusion detection helps you act faster

Catching a security breach as it happens is invaluable. Video analytics from Axis partners allow you to define a virtual zone, line or perimeter and receive a real-time alert for fast response any time someone crosses a line.

Item recognition protects lives and property

This application allows you to receive alerts if any objects are left unattended in a defined area longer than a set time, — offering heightened protection from critical situations such as explosive packages left in the bank or ATM area. You can also take advantage of such applications to detect the removal of pre-identified objects in an image — offering instant theft alerts.

Loitering alerts help you prevent crime

Loitering can be a simple case of passing time or the first sign of a threat. Subjects that remain within a defined virtual area longer than a specified time trigger an alert — allowing you to catch suspects planning an offense before they do any harm.

Make more efficient use of resources

Instead of assigning personnel to watch monitors for hours to spot suspicious activity, you can put video analytics to work for you and make better use of your staff's time. Since the system alerts operators to important information — such



as people in restricted areas, abandoned bags, or attempts to tamper with the surveillance cameras — you need fewer operators even for very large installations.

Respond to real-time alerts

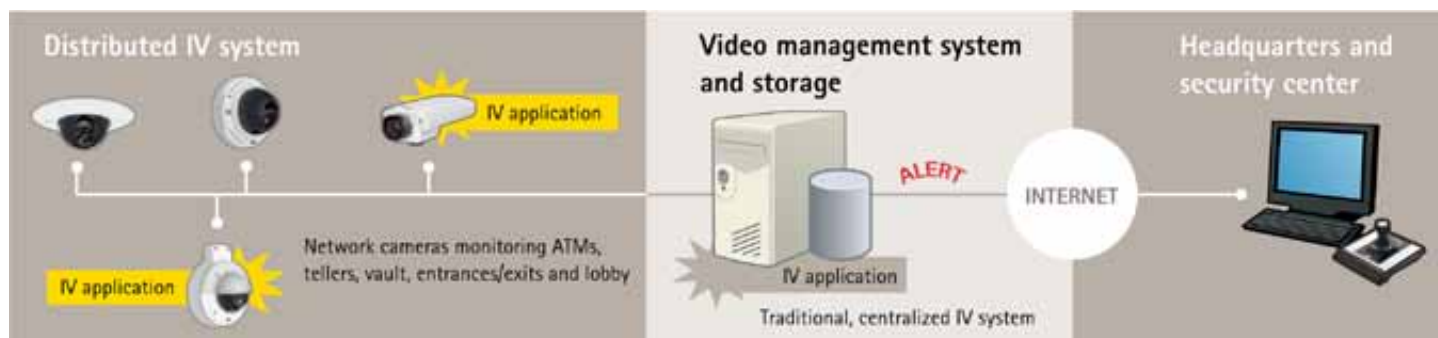
Intelligent video directs monitoring personnel's attention to relevant activities in real time. This means staff can respond to events in a quick and efficient way — providing significantly improved safety and security.

Retrieve stored video faster

You can be sure your system only stores relevant video footage — so when the need arises to search through old recordings, you'll only retrieve video that could potentially include the event in question.

Optimize your operations

Video analytics also provides in-depth reports, charts and graphs to help your organization make better decisions. You can use the information to optimize the network video security system as well as increase efficiency in terms of staffing requirements, customer satisfaction, employee training, and more.



always lok in new zealand made!



always specify and buy with
confidence and quality in mind.

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

Loktronic ● **Innovationz**

Security with innovative technology

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

The design of security organisations

I have just finished reading, 'The Design of Business', by Roger Martin, the Dean of Business at Rotman University, Canada. (\$47, available through Unity Books, Wellington). Martin states that business exist to solve a mystery for their clients. To solve a mystery, Martin says, that businesses create an heuristic. An heuristic is a definition of what the business does. Selling alarms, for example. Efficient businesses should then have ambiguity stripped away from the heuristic to produce an algorithm; or set process for completing the job. The company then seeks more and more economies from the same algorithm to make the most profit from the idea.

An example of a 'mystery' might be, how do business prevent loss through theft and damage? The heuristic that the company comes up with might be, a manned guard force. The resulting manned guard force 'runs' that heuristic and makes money from it. In an effort to

make more money from the business, the management strips away extra services, negotiates good deals on contracts for staff and vehicles and writes a comprehensive manual that allows it to employ unskilled labour at a low cost.

If you are reading this and think that you cannot create algorithms for what you do, you may be correct. Purely heuristically based businesses normally handle what are described as 'wicked problems'. These are complex problems that have 'one of a kind' answers. They weigh perfectly correct solutions against each other to discover the best one. True security consultancy falls into this realm.

For most other businesses the process works in a funnel, with the mystery at the top, the heuristic in the middle and the algorithm at the bottom. Companies have grown huge running their ever more efficient algorithms but, and here is the crux of the book, they will eventually be overtaken by their competition if they fail to look at what the next mystery is or to

re-examine the first mystery. The secret to longevity in a company and therefore long-term, sustainable profit is, using the existing algorithm, to create profit and then channeling that profit back to the 'validity thinkers' in the organisation who are constantly looking to solve the next mystery.

The problem is that current business education teaches people to seek reliability - that which is provable based on past events - over validity, or ideas that could solve a customers problem. The last part of the book is taken up with lessons of how each type, reliability thinkers and validity thinkers, can work with each other and, what kind of support is needed to create what Martin calls, 'Design Businesses'. Simply put; the right balance of money making algorithm with mystery solving heuristics.

Martin's focus is business but, I can see this model working in many areas of intelligence and security where, reliability thinking butts up against validity thinking and competes for available budget.

Mentioning this theory to a Detective friend caused him to say that he saw this in many voluntary organisations; a lot of whom are slowly going extinct due to their inability to tackle the next mystery. He stated that many clubs that he belonged to were populated by the same people, who turned up because it was a social occasion.

'The activity at the club was secondary to the tea', as he put it. When members moved away or died, the organisation shrank and was unable to recruit new members because it did not seek to solve the new mystery of what new members of the club might want.



Carlton Ruffell is a former New Zealand Infantry Soldier and member of the Police Diplomatic Protection Service.

He has worked for a British Risk Consultancy in the Middle East and as the Security Information Officer for Parliamentary service, where he conducted targeted violence threat assessment for MP's and staff.

His consultancy, Ruffell & Associates, provides understanding for individuals faced with threats of violence and offers solutions to reduce any quantified risk.

Carlton holds a Bachelors Degree in Defence Studies from Massey University and is a Certified Protection Professional (CPP) and Physical Security Professional (PSP) with ASIS International.

He is the deputy Chairman for ASIS New Zealand.

Remote Surveillance from anywhere



See us at the
NZ Security Exhibition & Conference

**Surveillance and
Monitoring has never
been so easy &
affordable**

Standalone and
Portable Cameras

Unmatched Battery Life

Flexible add-ons

Online viewing with MyMi5



**Reseller Partners
WANTED NOW**



www.mi5security.com

call now: (0800) 111 309

This caused me to look at ASIS New Zealand, an organisation dedicated to improving security through education and aimed at security management, for which I am the Deputy Chairman. Thankfully I can say that recruiting is going on at a steady rate so we must be doing something right. However, the test is in retaining members and unfortunately they move away from the organisation at a steady rate too.

I have to ask myself, is this the result of our running a comfortable algorithm of meetings and conferences over and over and failing to address what the new mystery might be? Once the mystery is defined then often an answer can be postulated so, I thought the question might be, "Who are security managers in modern New Zealand?" ASIS has traditionally recruited from private detectives, guard force managers and security managers from large companies but, particularly with the convergence of Information Technology, these people may no longer be the 'typical' security manager. Another mystery that I often ask myself is, "Why don't security professionals want to learn more about security?" I mean, don't they enjoy it? Do they

know everything already? Another mystery might be, "What format for security organisations best meets a security managers needs?" I like monthly, face to face interaction but, in the age of Myfacebo (social networking) is there a better or more relevant way? All of the proposed answers must be balanced with the time, money and ability constraints of a voluntary executive.

While on the topic of networking; a major draw card for ASIS is the networking prospects that allow members to market their services and see a return on their membership fees but, the strength of networking lies not in making ties within established groups but, in making new ties with different groups. As Malcolm Gladwell points out in his excellent book, 'The Tipping Point, How little things can make a big difference,' (viewing ideas as epidemics), people in the same social group know each other and rarely introduce new ideas or requirements. Networking power comes from 'connectors' (Mark Nicholas of Protect Security, Wellington, comes to mind here) or people who span several different social groups and who can

introduce us to people with new ideas and new needs. In the days when a business must weigh every dollar to seek maximum return, security organisations should attempt to create cross group networking opportunities. Is this the new heuristic for New Zealand security organisations?

Finally I might ask, have security organisations gone far enough in pushing the algorithm to its possible final form? What does the organisation seek to do and does it accomplish this in the most effective way? I think that we have this right in ASIS New Zealand with our focus on top quality educational speakers at our monthly meetings and our consistent drive to get professionals to prove their ability by becoming internationally certified in the areas of security management, physical security and investigations.

We currently meet the goal of advancing security through education but, this does not mean that we can sit back and relax. There is competition for the 'discretionary dollar' in more than just security organisations and ASIS New Zealand must keep an eye to the next mystery and free up its 'validity thinkers' to address these.

Recognising an Industry stalwart

As I opened my June/July copy of NZ Security for the first time and was greeted by the smiling (well almost!) picture of my long time friend and mentor Ian Dick, with the suggestion that he 'speaks out' alongside, I have to admit to some concerns as I flipped to the pages containing his article wondering what he may be 'speaking out' about this time and how.

Many of us I'm sure have enjoyed the challenges of a verbal sparring match with this grand old gentleman of the security industry and marveled at the sharpness of his thinking, equaled only by the sharpness of his tongue at times, and inwardly smiled when the most politically inappropriate comments escape his mouth in open meetings, whilst shaking our heads disapprovingly for appearances sake.

Ian Dick has made long term and significant contributions during his very long career within the industry and I am very pleased to call him my friend. Like many within the industry and NZSA membership specifically, I hold the utmost respect for what Ian has done, the experiences gained and the advice that he is well placed to give.

As I read through the article I couldn't help but smile in the realization that for the most part, Ian's seemingly provocative comments were as usual, reasonably well considered and delivered for effect and as he will well know, in line with the current strategic plan and discussions around the board table.

In considering some of the specifics within the article I considered it a good trigger to pass some comment as an update for NZSA members generally albeit I will be inviting Greg Watts, the NZSA Executive Officer, to expand on this in detail in the near future, and certainly during the forthcoming NZSA and ASIS annual conference and exhibition.

Like Ian, I too consider myself to be a relative digital dinosaur in that I prefer face to face, or at least telephone based interaction with my peers, and although comfortable with the 'modern' options for communication and information sharing, struggle with the potential for lack of direct engagement that those options can present.

For this reason, a key element of the NZSA's marketing and communication plan has been to develop strategies for

re-engaging with members directly whilst at the same time continuing to improve the web based and back of house functions necessary as part of a modern organisation.

We have been very pleased with the refreshed monthly meetings reintroduced in Auckland successfully as a trial and that these have enjoyed good uptake and participation. The challenge of course is to maintain interest going forward through diversity of presenters and creating genuine opportunities for networking and education by default.

Based on that success and the enthusiasm and ability of the organizers, it is our intention to facilitate similar events at other key locations around the country as interest, opportunity and funds permit.

Certainly I invite expressions of interest from members in Hamilton, Wellington, Christchurch and Dunedin as a minimum, to be made via the NZSA office as we are looking for willing volunteers to work with us in pursuing this initiative.

Having considered that the first line of customers of the NZSA to be served are our members and that there is a need to find better options to engage with them directly, our next focus is on our 'customers' customers, and indeed the public in general.

A broader campaign for promoting a professional industry in general and the benefits of using accredited NZSA members specifically has been a topic long debated and called for and is perhaps more relevant now than ever.

Indeed this was a key requirement in the recruitment of the Executive Officer in 2010 in terms of desired skill sets around marketing and we have been pleased to see an increasingly solid platform established from which to promote NZSA membership to the



Alistair J Hogg, CPP, MSc

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

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

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

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

Email: alistairh@aotea-southern.co.nz

Atlas Gentech is a value added Technology Distribution Company specializing in 3 core sectors of the market; Data, Communications and Security.

Atlas Gentech values and understands the importance of technical and customer/sales support to our varied customer base and places strategic emphasis on this core ingredient in business.

The Atlas Gentech Training Academy is responsible for identifying what training is required to promote and support the vast product range the company distributes, courses offered to Atlas Gentech customers include:

- Paradox Digiplex EVO Technician Course
- Paradox SP/MG Technician Course
- Inner Range Certified (Basic) Technician Course
- Inner Range Advanced Technician Course
- Internet Protocol and Computer Networking Concepts

A range of online training is also available. Atlas Gentech is also working on commercial end-user training courses that teach commercial end-users how to use the equipment, whether it is an alarm, access control, CCTV, building management or telephone system.

For further information and current training schedules, visit the Atlas Gentech Training Academy website:

www.atlasgentech.co.nz/trainingacademy



broadier public as part of an effective marketing campaign.

Of course any form of active marketing comes at a cost and we have considered that significant works have been required within the organisation prior to any significant spend promoting the merits of the organisation or its members. We look forward to the progressive roll out of a promotional and awareness strategy in the months ahead and the board awaits with interest, options to be considered in line with that strategy.

The key to many marketing campaigns of course is promoting a point of difference and in many cases assuring confidence in the product or service being marketed. In regards to the NZSA, perhaps the most tangible and marketable point of difference to those customers of our customers, is the association's audit and accreditation programme which has been a labour of love for many and an essential element of the NZSA's core functions.

The whole point of course is to provide users of security products or services with some confidence that the providers of these products or services meet minimum standards of quality, training and ethical behavior, particularly in an industry

which has attracted a variety of operators of varying quality and behaviour over time.

The audit and accreditation programme has taken some time to establish fully, however we are pleased that it has reached a point where it can be taken to the next step and this is also reflected in Ian's comments around the introduction of new and additional auditors and the manner in which audits are arranged and conducted.

An absolutely critical strategy within the first stage of auditing was in regards to mentoring of members towards achieving a satisfactory audit meeting the minimum standards required.

Clearly as part of our stated desire to lift standards generally alongside the perception by the public of the security industry, it is our aim to continue to lift the bar and to use the audit process as a means of helping members continue to work towards this and in doing so adding value to their business generally.

In order to do this, the audits themselves must be conducted in a more formal manner and focus on ensuring that compliance and excellence is the norm within an operation, not the exception.

We are confident that this next stage of auditing will add significant value to members and support our marketing initiatives in giving us a genuine story to tell to the wider public. Again Ian has been critical to the evolution of the audit and accreditation programme and we cannot thank him enough for having assisted in getting it to the stage that it is today.

All of that said and in closing, it is not without some sadness and a significant amount of respect that I acknowledge Ian's imminent retirement from active involvement with the NZSA board and auditing due to continuing declining health and mobility and a desire to enjoy the remainder of his retirement.

I am looking forward to accompanying him on a final audit visit later in the year and once again enjoying a number of stories (not all politically correct I'm sure), and taking on board his views on the industry and the association, of which he is not slow to share.

I will be pleased to continue to look to him for advice often even during his retirement and enjoy a friendship based on respect for this grand old gentleman of the New Zealand Security Industry.

Wintec shuts security course

While the security industry awaits an announcement from the government on what training will be compulsory under new regulations, Waikato Institute of Technology (Wintec) is closing its National Certificate in Security Level 2 course.

The closure has come at a time when the government has said it intends to introduce compulsory training for some 8,000 property guards and an estimated 9,000 crowd controllers.

According to NZQA almost 3,750 people have so far earned a National Certificate in Security Level 2 qualification – an average of 250 per year since 1996. Some of those people will have left the industry by now, but whatever the exact number, and whatever the exact requirements turn out to be, a sizable training challenge is looming. But any training boom will be short lived,



because once the minimum standards are reached by current Certificate of Approval holders, the need for mandatory training in the industry will tail off to match the number of new entrants to the industry every year.

But at Wintec the Level 2 certificate is no longer on offer, with a spokesperson citing low domestic completion rates as the reason behind the closure.

“Despite efforts to improve the programmes’ outcomes they remained unsatisfactory. More recently the number of domestic enrolments has also decreased, leading to a review of the programme,” says the spokesperson.

A feature of the course was that it offered an option where candidates employed in the security industry were nominated for training by employers who had a training agreement with ETITO.

According to Wintec, despite the drop in total numbers, twenty four equivalent

full time students were enrolled under the ETITO programme this year, up from ten last year.

The spokesperson says Wintec is committed to ensuring that currently enrolled students have an opportunity to complete the programme even though the majority of the staff have gone.

“Five staff have been made redundant, leaving one staff member so that existing domestic students can continue in the programme and international opportunities can continue to be pursued,” she says.

Proposals to make the security programme staff redundant began to circulate in May, when shortly before, at the end of April, Wintec announced a partnership with the Open University of Malaysia to develop a Certificate in Security Management, an agreement that would see Wintec provide subject matter experts, its ‘train the trainer’ programme, and quality assurance.

“Tailored training and experiential training – where we assess people as they work or assess work experience – is an area in which Wintec excels,” said the announcement.

“Wintec’s subject matter experts will be sent to Malaysia for up to three weeks in late May to work alongside the Open University of Malaysia facilitators and support them with the new security programmes,” it said.

The quick change of heart by Wintec saw the Tertiary Education Union EU National President Sandra Grey issue a terse statement accusing Wintec of a failure to plan strategically and invest in staff.

“Our Malaysian colleagues may find they have an agreement with an outside agency and new staff they do not know. It hurts Wintec’s reputation and New Zealand’s tertiary education reputation overseas,” she said.



Late comers should take a holiday

So far over 11,000 companies and individuals have applied for a certificate of approval or licence under the Private Security Personnel and Private Investigators Act 2010 which came into force on 1 April this year.

According to Wayne Newall, Ministry of Justice National Manager Tribunals, the majority of people and firms in the industry made their applications well before the 1 June deadline.

“Over 9,600 licences and certificates have been issued to date,” he says.

Wide-spread publicity – including stories in *NZ Security Magazine* – have encouraged security personnel and companies to apply in time.

Companies and individuals that applied for new licences by 1 June had their old licences extended until the new ones are issued.

But in spite of the risk of incurring hefty fines under the new legislation well over 100 companies and individual licences holders failed to get their applications in by the 1 June.

“Anyone who did not get around to it will not be able to operate lawfully in the sector until the licensing process is completed,” says Newall.

The Ministry of Justice says applications to the Licensing Authority take about seven to eight weeks to be processed, providing there are no issues, no disqualification criteria apply, and no objections are lodged.

Although it is possible some applicants could be new comers to the industry or personnel who are not working in the industry at the moment, around 700 security personnel also didn't get their applications in by 1 June and did not pay the extra \$20 for a temporary licence to tide them over legally while their application for a new certificate is processed.

They too, should not work be working in the industry.

Newall says an employee working in the security industry without a certificate of approval faces a fine, on conviction, of up to \$20,000. An individual conducting business without a licence faces a fine, on conviction, of up to \$40,000, and a company conducting business without a license faces a fine, on conviction, of up to \$60,000.

However Newall will not be drawn on whether the Licensing Authority intends to allow a grace period for enforcement while the new Act beds in.

Free complaints

Whether the Authority intends to implement an easy going or a tough enforcement policy in future remains to be seen. However action may be initiated by any member of the public or the industry who lays a complaint – a process that costs nothing.

“Whilst enforcement can be initiated by the Authority, most matters will be dealt with in response to complaints, which can be made directly to the Authority or the Police,” says Newall. That process is underway.

“A number of complaints are being investigated and only once that process is completed will the Authority make a determination,” he says.

With the majority of security guards and companies getting their paperwork done and operating legally, the next stage in the Act is to bring the new classes of security personnel into the fold.

“The new licensing scheme means some security personnel, such as crowd controllers, security staff employed by licensed premises and personal guards will require a licence or certificate of approval for the first time, although this

won't kick in for most people until after the World Cup,” says Newall.

“One of the primary challenges this year will be to make those people aware of the need to get licensed. For most people in the industry, licensing has been around for almost 40 years and this new scheme should make things easier for them in the long run, with initiatives such as moving from an annual to a five-year licensing cycle and allowing online applications.”

New applications

Back in March the Ministry of Justice estimated around 12,500 applications would come from current licensees and certificate holders and 9,000 new applications for crowd controllers.

Some 4700 or so crowd controllers have already applied but almost 95 percent of those are property guards in any case.

The new Act goes to great lengths to define seven distinct classes of security work but individuals applying for a certificate of approval as, say a property guard, may as well tick all the boxes because it doesn't cost any more to do so.

So far around a quarter of individual applicants have applied to be five or more of the seven classes of security individual while around 250 ticked all the possible boxes on the form.

Once mandatory training requirements kick in, it will apply to property guards, personal guards and crowd controllers. There will be a disincentive for, say a private investigator (PI) or security consultant to apply to be a crowd controller because they would have to sign up for a training course.

However the reverse will not apply. A crowd controller can happily tick the private investigator box on the form just because, well, one day they might want to work as a licensed PI.

Creating a Secure Infrastructure for NFC Mobile Phones

Trusted Identity Platform (TIP) Enables NFC Phones To Be Used for Access Control and Other Transactions
By Dr. Tam Hulusi, Senior Vice President, HID Global

Today's mobile phones do much more than make and receive calls. They now serve as calendars, cameras and even game consoles. Thanks to Near Field Communications (NFC) technology, another valuable tool can also be loaded onto your phone – your keys.

NFC is a short-range wireless communication technology standard that enables the exchange of data between devices over a distance of several centimeters. This data can include credentials previously stored on contactless smartcards used for opening doors. Today, contactless credentials are available as fobs and plastic access cards that can be programmed to provide various levels of facility access. Now, the same contactless credentials can be loaded on a mobile handset, eliminating the need to carry any other access credentials while making it easier for security managers to track who is entering and exiting monitored access points. NFC provides a platform for many types of contactless applications and transactions including payment and transit ticketing, keys, data transfers including electronic business

cards, and access to online digital content.

NFC enables these capabilities, but the only way to make them secure is if there is a comprehensive chain of custody in which all system end points can be validated. Only in this way can identity transactions between the end points be trusted at any time.

An example of this type of trusted system is HID's Trusted Identity Platform (TIP), which turns access control readers, laptops, NFC-equipped mobile phones and other products into trusted identity nodes that can be securely provisioned regardless of where they are or how they're connected.

Trust is the Key

The basis for modern transactional systems has been the ability to trust the identification of a person, computer, website, check, or a credit card. Unfortunately, the effort required to authenticate them has grown exponentially. There are three basic building blocks for constructing and using trusted identities: un-forgable signatures; shared secrets; and tamper-resistant hardware. There are a variety of

commercial offerings for each of these basic blocks, but it is not a trivial matter to simply pick the correct, basic building blocks for a particular situation.

There is, however, an aspect of secure identity systems that simplifies the problem: like mobile networks, secure identity systems are closed systems. To use them, you often must complete a background check and sign a legal document to construct the basic blocks describing your identity. It's this strong authentication and binding that endows a secure identity system's basic blocks with inherent trust.

To even have a current and valid set of identity blocks means that one has passed this bar and is a member in good standing of the closed system. It also means that the blocks and the systems supporting them can be simpler and constructed so that they can be implemented using industry standards. This is the approach taken with TIP, which enables the validation of all endpoints, or nodes (such as credentials, printers, readers and NFC phones) in the network so that transactions between the nodes can be trusted.



TIP Secure
Vault



Key
Management



Lifecycle
Management



TIP Device
Management

TIP is designed to enable the provisioning of virtual products, including security credentials, and NFC is one vehicle for doing this. TIP delivers three critical capabilities: plug-and-play secure channels between hardware and software; best-in-class key management and secure provisioning processes; and seamless integration with information technology infrastructures.

At the heart of the TIP framework is the Secure Vault that serves known nodes within the published security policy. Data security, privacy and reliability are ensured using symmetric-key cryptography, so that all nodes can execute trustworthy transactions.

Deploying NFC Mobile Phones

One of the first steps toward widespread deployment of TIP-enabled mobile phones was the July 2010 partnership announced between HID Global and INSIDE Contactless, one of a handful of companies driving the NFC trials currently underway around the globe.

This first partnership will allow NFC-enabled phones to hold the same market-leading iCLASS® access control and credentials information as traditional physical smart cards. This credentials information will be delivered via HID Global's TIP system. Similar capabilities can be extended to other mobile devices including laptops, for applications ranging from user authentication to cashless vending and PC log-on security.

These platforms and applications will significantly extend the value proposition for contactless smart card credentials.

Another example of early NFC mobile

phone deployments is the first hotel pilot of NFC technology at Clarion Hotel Stockholm in Sweden. The hotel worked with HID Global parent ASSA ABLOY, Choice Hotels Scandinavia, TeliaSonera,

VingCard Elsafe and VEnyon, a fully owned subsidiary of Giesecke & Devrient, to replace the hotel's room keys with NFC-enabled mobile phones. As part of the pilot program, the selected Clarion hotel guests receive a Samsung mobile phone with NFC and relevant software. They can check in on the mobile phone before arrival, which prompts a digital hotel room key to be delivered to the mobile phone. On arrival, the guests skip the check-in line, go directly to their room and open the door by holding the mobile phone close to the door lock. When leaving the room, the doors lock automatically and guests check out using their mobile phones.

NFC-based access systems will enable a new era of more convenient and secure transactions. Delivering on this promise will require a simple but protected, fully scalable and standards-based identity delivery system that can support a wide variety of identity nodes – ranging from readers and cards to NFC-equipped mobile phones – that each can be registered as a “trusted node” so that it can be securely provisioned anywhere in the world.





Bosch Video Recording Manager (VRM) provides a Distributed Network Video Recorder solution, eliminating the need for dedicated NVRs and signaling the second generation of IP network video recording. VRM supports iSCSI-based storage systems and Bosch Video-over-IP devices (IP cameras and IP video encoders).

VRM introduces the concept of a storage virtualization layer. This abstraction layer enables VRM to manage all of the individual disk arrays in the entire system as a single “virtual” common pool of storage, which is intelligently allocated as needed.

VRM eliminates the need for Network Video Recorders (NVRs) and their associated server hardware, operating systems, and anti-virus software, as well as the ongoing software patches and updates these systems require. This new technology makes installation, operation and maintenance much easier while reducing the total cost of ownership.

The central Recording Management Service runs as a service on Microsoft Windows platforms. Bosch recommends running VRM Server on a dedicated server/hardware platform. VRM offers system-wide recording, monitoring and management of Bosch iSCSI storage, video encoders and cameras.

VRM 2.12 software supports Bosch H.264 and MPEG-4 IP video devices including all encoders, Dinion and FlexiDome IP cameras, as well as AutoDome and Extreme IP cameras and the Bosch HD cameras.

Supported storage subsystems include the Bosch iSCSI-based DVA, DSA and DLA Series disk array systems. The iSCSI disk arrays can be attached anywhere on a standard IP network.

VRM 2.12 offers additional redundancy and data availability by supporting Automatic Network Replenishment (ANR) with Bosch Video-over-IP devices (BVIP Firmware 4.0 or later required).

Optimal Performance

The Video Recording Manager offers a high-performance, flexible, scalable and a highly reliable iSCSI storage management solution.

Optimized performance is obtained by the use of intelligent addressing on a block level, which also allows for load balancing of the video recording to all available storage blocks located on any storage array in the system.

Load balancing is provided with respect to the bandwidth and the number of iSCSI connections and is configurable per IP address (iSCSI target).

Logical Virtualization

The VRM virtualization layer allows the scalability of storage beyond the physical limits of a single storage subsystem.

This logical abstraction layer means that each camera can use any storage space it actually needs, rather than an allocated, arbitrary, discrete chunk ahead of time. Adjust retention times of video data as required.

Fast Recording and Retrieval

VRM provides fast and flexible retrieval via a search database of recordings and metadata. Metadata is a form of data that describes other data such as events, ATM/ POS information, and video content analysis data. The metadata is recorded with the video data and provides a fast and efficient way for the search engine, in the playback client, to quickly locate specified video clips. The database also keeps track of the location of recording blocks. If this database is lost, VRM can recreate the database by reading the stored metadata, thus providing a self-healing capability.

Distributed Storage

VRM not only provides for redundant management of metadata, it also introduces a significant enhancement of overall reliability and availability. By providing redundancy for storage



VRM Server Configuration Client

The configuration client allows for central configuration of the network storage subsystems, recordings (including schedules), data rate, frame rate, stream and privileges, as well as for managing user accounts.

provisioning and a failover design for the central recording management service, there is no single point of failure. In addition, unlike NVR systems, VRM scales without requiring additional PCs. This greatly reduces the risk of system failures.

Functions

VRM Server

VRM Server, with the central Recording Management Service, maintains a database containing the recording source information and a list of associated iSCSI drives. The central monitoring includes a Web-based user interface for status monitoring. This provides system status overview, recording status information, as well as for live view and recording preview for single cameras.

For more information about Bosch Video Client BVC, see the product specific documentation.

Automatic Network

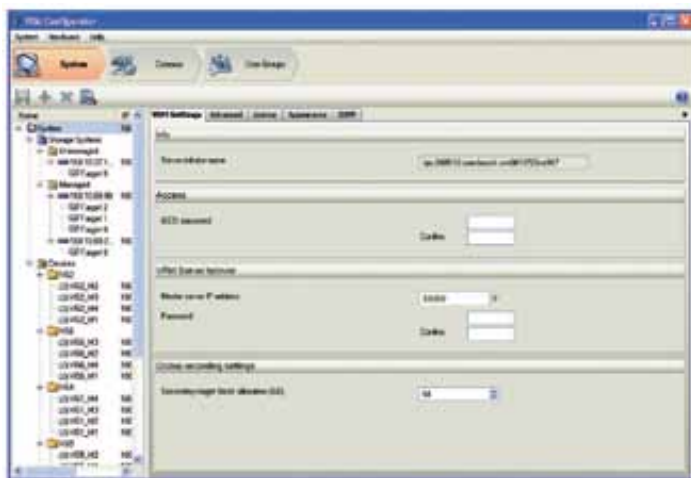
Replenishment ANR

A VRM server can perform maximum 3 ANR jobs simultaneously. If you configure multiple ANR jobs for 1 device (for example with 4 channels), these jobs are performed one after the other. This avoids overload of the device.

The number of ANR jobs cannot be increased by a secondary VRM server. The maximum performance is 24-times of replay, the actual performance may be limited by the capabilities of the encoder/camera. ANR is only effective for data within the minimum retention time of the system. Recording gaps outside the minimum retention time will not be considered.

Backup of data through VRM

A VRM server can execute maximum 5 backup jobs in parallel. The number of backup jobs cannot be increased by a secondary VRM server. The maximum performance is 24-times of replay. Consider this for bandwidth estimation of the iSCSI targets. The backup functionality is not supported by the BVC replay client.



Configuration Client

Playback Client

For replay use Bosch Video Client BVC Version 1.1.
The BVC is available on the Bosch ST web site
www.boschsecurity.com.

- ◆ Distributed storage and configurable load balancing
- ◆ iSCSI disk array failover for extra reliability
- ◆ Used with all Bosch Video-over-IP cameras and encoders
- ◆ Configuration support for all Bosch disk arrays (DVA, DSA and DLA series)

Design Recommendations

Load Balancing (if VRM is configured in “All Mode”). When calculating the number of storage arrays for VRM environments we strongly recommend adding an additional iSCSI target (n+1 calculation) or to use the “Failover Mode”. This recommendation is especially important when using the DLA Series because these storage systems provide a lower reliability and availability than the DSA Series.

ANR

The first implementation of ANR in VRM is suited to protect against single short network outages. One network outage must be longer than 10 seconds to be detected by the ANR mechanism. If the outages are shorter potential gaps are not detected and recording is not refilled.

ANR is not suited to be used for:

- Wireless applications because of frequent network outages.
- Mobile applications because of long outages with large recording gaps which takes very long to be filled.

Licensing

Existing VRM 2.0 licenses can be used for VRM 2.12.

Installation/Configuration Notes VRM Components

The Video Recording Manager consists of the following components which may be installed on separate systems.

- VRM Server (central Recording Management Service). with Web interface for VRM Monitor.
- VRM Configurator.

VRM Monitor

- Displays overall system status information, including uptime, bit rate and retention times.
- Provides status information on recordings and storage.
- Displays live view and recording previews for a single camera.

VRM Configurator

- Allows configuration of the iSCSI storage subsystems.
 - Bosch DVA Series (Bosch OEM Disk Arrays)
 - Bosch DSA Series (NetApp Storage Systems)
 - Bosch DLA Series (Bosch OEM Disk Arrays)
- Allows configuration of recording parameters, including schedules, data rates, frame rates, streams, and privileges.
- Allows management of users and groups with privileges and roles.
- Allows configuration of load balancing parameters (bandwidth and iSCSI connections) per disk array (IP address).

Taming Internet Usage with Real Proof

Internet access for any business has become a necessary survival tool and enables companies to connect with their customers regardless of where they are located. But, an unmanaged internet connection can cause all sorts of issues within a working environment.

Those risks include potentially infecting machines or a company network with viruses or malware. This often results in a degradation of network service and probable time lost in cleaning the infection, plus the time taken with restoring systems from backups. Additionally, when a staff member appears to be internet surfing for pleasure rather than company business, the amount of time and money in lost productivity is surmountable.



Dean Stewart has over 25 years experience in the IT industry, has worked 14 years overseas and has almost 10 years in IT Security.

He has two teenage children and is passionate about cyber safety and all aspects of internet security. He is based in Christchurch, has survived 4 major earthquakes and is looking forward to the new rebuild of the city.

He is a keen tramp and enjoys getting away regularly for a weekend in the mountains.

Contact Details:

Email: info@websafety.co.nz

Web: www.websafety.co.nz



Statistically, research shows that 70% of staff will spend at least 1.5hrs on non-work related internet surfing per day, during work hours. Take an average hourly wage of \$20 per hour, that amount escalates to about \$7,000 per annum for 1 staff member alone!

Team moral often takes a hit when one staff member is seen to be outside the bounds of acceptable use relating to internet usage. This not only leads to poor performance of that individual, but also affects the rest of the team members. Companies cannot afford to have unhappy staff as it ultimately has a direct impact on their bottom line.

Managing internet usage in the workplace can be difficult unless the business is prepared to invest in expensive software and have the expertise either in-house to run it, or employ contractors whenever they require changes to be made.

Add the pressure of profit margins to reach and one soon finds that productivity becomes the key driver to success.

Managers who identify staff within a team as an under-performer have the task of either identifying any personal issues or even more difficult, proving a history of internet surfing.

Apart from the occasional glance at the computer screen, it is difficult to quantify what is actually taking place.

Welcome WebSafety NZ Limited. This business provides an internet forensic service known as a 'WebSafety Audit'. It targets any Microsoft computer and extends to the top 5 internet browsers used today.

"The customer sends the laptop or computer box to us by courier. We then take a copy of certain hidden internet files and upload them to our machine for analysis", says Dean Stewart, Owner & Director of the company.

He goes on to say "after running the files through our security software, we analyse the data and produce reports for the customer."

Included in the WebSafety Audit is a written report of the findings, analysis of



Setting the **NEW** benchmark in Electronic Security Sales

- ✓ The **BEST** in customer service
- ✓ The **MOST** proactive support
- ✓ The **RIGHT** business partner



Farpointe Data
Readers • Credentials

Call Michael Danger directly on
0412 948 161

	Index	URL_ID	Type	Visits	Action Date [Local]	User	Web Page Title	Universal Resource Locator (URL)
<input type="checkbox"/>	0000001	5		3	29-01-0123:00:11 [+1200 DST]			http://www.google.com
<input type="checkbox"/>	0000002	25		1	29-01-0123:00:15 [+1200 DST]			http://go.microsoft.com/fwlink/?linkid=121792
<input type="checkbox"/>	0000003	13		5	29-01-0123:00:15 [+1200 DST]			http://www.microsoft.com/windows/internet-explorer/welcome.aspx
<input type="checkbox"/>	0000004	27		13	29-01-0123:00:18 [+1200 DST]			http://www.google.com
<input type="checkbox"/>								

Sample report screenshot

any concerns and detailed reports based on any of the concerns.

The examining software is used by law enforcement agencies around the globe and has the ability to search through millions of images in minutes.

The software also has the ability to:

- Produce detailed reporting
- Custom reporting on any request
- Rebuild web pages
- Produce reporting on internet search terms used
- Recreate Facebook chat
- Create an image report containing the image, original site opened with time and date
- Report on all internet activity including times and dates

Stewart explains that by default, internet history is kept for about 30 days. There are several log files that are not only hidden, but also in a format that cannot be read without security software. The files are also not accessible by the user logged into the machine at that particular time.

Staff trying to cover their tracks sometimes will manually delete internet

history within the browser. However, other hidden folders hold copies of images viewed within the browser. At times this has proven to be the key to evidence, as the images also record a time and date stamp, as well as the internet site it was viewed from.

Where files exist, the service also includes producing chat, phone and file transfer records of messenger programs such as MSN and Yahoo Messenger, as well as Skype. Conversations could be important to a company investigation where sensitive information may have thought to have been leaked. Likewise, file transfer records and call logs may identify a bigger picture than already understood.

Skype also pulls down the entire set of log files attached to the user name, onto the computer being used for Skype. This results in the log file containing activity not only on the computer being examined, but any other computer where Skype has been installed for that username!

Since offering the service 12 months ago, WebSafety NZ receives work from all over New Zealand. The service has proven popular with both smaller

businesses as well as larger ones. It is cost effective and customers are able to identify all activity taking place and have the proof at hand to address the behaviour quickly.

It has also proved to be useful in schools, where they examine internet usage on laptops of teachers suspected of viewing objectionable material.

In most cases, the investigation finds that the pattern of internet surfing has taken place for 3 months or more.

Most commonly, they find sites relating to social networking, shopping, online games and videos to be among the top categories discovered and often for the majority of the day. However, the WebSafety Audit has also uncovered staff surfing pornographic material, either during working hours or at home. In these cases, the culprits often head down the path of dismissal.

A pattern of viruses being triggered from a machine over a period of days becomes an ideal target for an internet audit.

A computer is infected with a virus from one of two methods, the first being via an external device being plugged in, or from the internet and too often the latter has been a source of infection.

Since writers of viruses always look to infect as many computers as possible, sites containing objectionable material, games or rogue software often infect machines of those who visit such sites.

Auditing internet access provides businesses with a clear picture of internet activity occurring on any given machine.

Whether singular, targeted or a random selection of machines are analysed, be assured that all activity will be uncovered.

**“A wealth of information creates a poverty of attention.”
Herbert Simon, Economist, 1971**

and miss out on opportunities to create meaningful metrics and key performance indicators. Consider coordinating the use of the naming convention or a portion of the naming convention across systems (i.e. BMS, asset management, purchasing, work orders, etc.) so that other departments and applications can understand and share the data.

The format of a naming convention for data and equipment is less important than strict adherence to and enforcement of one standard naming convention.

Lack of Data Mining

Facility managers are missing opportunities if they don't have the analytic tools to mine, predict and correlate building data. How many building owners are "harvesting" and analyzing data for the purpose of gaining insight into their building's performance? Very few. However, when you look at other organizations and businesses they "mine" data from their users and customers and analyze the data in order to predict and guide their business and business processes. Data mining has been around for a while and is used extensively in websites, retail purchases, financing, smartphones, to name a few. Look at a retailer like Wal-Mart which knows how many rolls of paper towels are sold daily at each store location, data that is part of a process to optimize their just-in-time supply chain process. Yet, how many large building owners can even tell you how many people entered their building on a daily basis or which building space is the least energy efficient? Which is the most used space? Which is the most and least secure?

Data mining related to energy usage would seem to be a wide open field. Energy consumption metrics related to space usage, operations processes and business aspects can provide new insights. As Frank Rotman, a former head of analytics at Capital One has said, "If I examine a new data set, the chances are I can find something in that data that has predictive value". Predictive value means the organization can be proactive rather than reactive.



No Validation of Data

There's no point in collecting inaccurate data. To get the most accurate

information you'll need to 'tune-up' the building systems and check the calibration of sensors and meters. The building systems themselves should be regularly re-commissioned or better yet continuously commissioned using a real time building system analytic tool. Traditional commissioning uses the design documents and design intent for the foundation of commissioning. Over time however, building spaces or uses may change; the effect is that while you can confirm or validate the design parameters, for example 54° air being delivered by an air handler, the space may have changed and have a different cooling load and may not need 54° air from the air handler. There the systems may need to be adjusted in order to reflect current conditions.

Sensors and meters should be regularly calibrated, both the device itself as well as the communication between the device and its controller. Inaccurate sensors may provide a false sense of complacency and more importantly waste energy and money. For example, assume you have a temperature sensor that is 2° off, showing a discharge air temperature of 55° when its actually 53°; this two degrees may trigger extra cooling and additional power consumption by the chiller and air handler or reheating of overcooled discharge air which obviously wastes energy.

Haphazard Document Management

How much time do we spend trying to find as-built drawings or some similar dated documents? While the building systems' data points can be part of a typical database, a significant portion of relevant FM information is likely to be in other formats; primarily paper, including hard-copy drawings, submittals, O&M manuals, photographs, contracts, faxes, forms, etc, but also electronic files in Word, PDF, Excel and Autodesk, all of which need to be managed. A document management system should be implemented to scan the paper documents into an electronic format and store all of the electronic files.

The system typically has an index with a format that may be similar to that of the building database, which either stores the document or directs users to another system where the document resides. Systems typically have a 'search' capability allowing users to retrieve documents based upon different criteria. These systems compliment the data management plan previously referred to and in order to truly fit they need intuitive indexing and firm adherence to the administrative

processes of indexing and document conversion.

With the flood of data and information that's potentially generated in a building it's not unusual or unexpected to feel overwhelmed. With the right administrative processes the technology that is generating the deluge of data can be put to work to deal with all that data and find the valuable information we need to effectively manage our buildings.

For more information, write us at info@smart-buildings.com.



For over 25 years, Mr. Sinopoli has worked extensively on projects involving the design, construction and operation of buildings and building systems. This has involved the configuration and optimization of building technology systems, facility management and operations. Mr. Sinopoli is the Managing Principal of Smart Buildings, which provides engineering and consulting services for the design and operation of integrated building technology systems. His background is in construction practices, design, procurement, project management, account management, and building systems and operation, with a particular focus on monitoring and managing a building's performance.

Mr. Sinopoli has experience in the healthcare, corporate, education, manufacturing, finance, construction and government industry sectors. His clients have included Fortune 100 corporations, major school districts, university systems, airports and ports, national government agencies, large private and public hospitals, technology companies, and major developers. His international experience includes projects in Asia, Europe, the Middle East, South America and Africa. United States federal clients have included the Internal Revenue Service, the General Services Administration and the US Postal Service.

Mr. Sinopoli's educational credits include a B.S. in Engineering from Purdue University and a M.A. in Applied Science and Environmental Management from Governor's State University. He is a licensed Professional Engineer, an Accredited LEED Professional and a Registered Communications Distribution Designer. Mr. Sinopoli is Chairman of the Continental Automation Buildings Association's Task Force on Industry Training and Education. He has spoken on numerous occasions at conferences and seminars focusing on building management and technology systems including ALA, BOMA, Builconn, Realcomm, BICSI and CEFPI conferences. He is a contributing editor for the web site AutomatedBuildings.com, and has written for many industry publications worldwide. He has received the international "Harry J. Pfister" award from the Building Industry Consulting Service International (BICSI). His most recent publication is a book titled "Smart Buildings Systems for Architects, Owners and Builders".

How to be sure you're making money and keep some for yourself

A simple way to ensure business profitability and healthy cash flow is to focus on what drives both.

- What drives revenue needs to be understood.
- How saleable is the product or service and what's the market?
- What marketing is working and how much is it costing to acquire a customer?
- Is it profitable revenue?
- How does the true cost of delivering the product or service compare with the price?
- Are customers returning and if not why not?

One of the biggest missed opportunities we see in business reports is lumping all revenue into one account and not breaking it down into categories. Breaking down, not only the revenue, but the costs associated with each revenue source, enables you to see clearly where you're making and losing money.

Pricing of products and services is vital to profit. To ensure profit it's vital to know the true cost of the product or service and keep an eye on it, to avoid 'margin squeeze' i.e. allowing costs to rise without increasing prices and absorbing extra cost.

Market forces have an impact on pricing but it's not viable to continually absorb cost increases without price increases. It's not always necessary to increase everything.

Example:

One client recently told us they hadn't increased prices for years. We did some analysis to find out what were their best selling products. On each of these we agreed to a small increase with no resistance from customers. A small regular price increase is much easier to achieve than irregular big ones. Most customers expect a CPI increase and if it's written into contracts, it's much easier to achieve.

Costing of products and services is vital knowledge to work out gross profit. Gross profit is the difference between revenue and costs and is an important benchmark. Cost of products may include: the product, importing, freight, packaging, labour, warehouse, raw materials etc.

Cost of jobs may include: labour, materials, out of pocket expenses etc. If gross profit is below expectations it may be necessary to assess how products and services are costed and acquired.

Example:

We had one client in a wholesale business whose packaging was a large portion of costs. When we questioned their ability to negotiate a better price with the supplier, they said it wasn't possible. We did some shopping around and found a supplier who offered a 10% reduction. The regular supplier soon agreed to a similar reduction.



Sue Hirst is the director of CAD Partners (CFO on Call), Financial Controllers, who provide small/medium businesses with the opportunity to use the on-site skills of ex-corporate finance managers on an on-call basis, without the normal high cost of hiring one full time.

The idea for CAD Partners (CFO on Call) was born when Sue was a practice manager for a Chartered Accounting firm. Here she saw first hand how clients usually got their management accounts once a year, often eighteen months after the financial year-end. She asked, "How can they manage a business on historical accounts that are a financial year or more old?"

As a result Sue began offering mobile management accounting and financial control services to SMEs for a fixed monthly fee. The company started in 1991

and within two years had built up a substantial base of clients who liked the fact they got regular monthly reports, that were easy to read and they "knew where they stood".

Due to the success and the demand in the market for good financial control help, Sue franchised the business in 1993. The current client base today exceeds 15,000 and CAD Partners is the only large-scale provider of on-demand financial control services in Australia and New Zealand with over 70 advisors.

Sue remains passionate about educating business owners on important issues such as good cashflow management and financial control. As such, she features regular advice in SME and industry publications.

Labour is another example of cost management on jobs. It's often the case where chargeable labour spends time doing non chargeable work such as admin. If you take the number of people, and calculate the total hours spent on admin multiplied by their hourly charge out rate, it's often the case that the cost of employing someone else to do it, is less than the missed income.

Overheads can get out of hand where there is no budgetary control. Owners don't always have time to keep an eye on what everyone is spending, or shop around for the best deal. A budget can be a saver as well as keeping your banker happy.

One overhead that can get out of hand is wages. Often in a growing business, staff are employed to meet demand, without proper job descriptions. An organisational chart can be useful for a growing business. Begin by listing all tasks in the business, then list who currently does them. Any overlaps and gaps should become obvious and job descriptions can be realigned to suit. Giving someone the task of shopping around for better deals can be a saver.

Debt collection is an area that has blown out recently. Dunn & Bradstreet

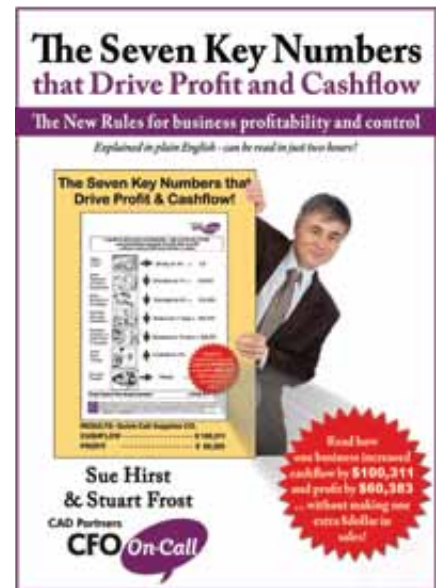
recently reported that average collection days were 55.6 days. Compare this to your 7 day terms to see what impact this is having on cash flow. Start with Terms of Trade so your customers understand the expectation. Invoice as soon as the product/service has been delivered or get a deposit or progress payments. Then follow up smartly. Email follow ups for small amounts and phone calls for large amounts. Keep good records of reasons/ excuses for late payment and agree to outstanding amounts being paid off in instalments over a period.

Stock and Jobs can be a huge drain on cash flow. Think of stock as dollars piled up on the stock room floor and jobs in progress as dollars on the work room floor. It really pays to reduce the time stock sits in store and jobs wait to be finished and invoiced. Good records and planning are vital to management of both.

There are some cost effective online systems available that can save thousands of dollars in working capital requirement to fund stock and jobs. Examples are Unleashed Inventory Software and WorkflowMax Job Management Software, both of which link to Xero Online Accounting Software.

Slowing down payment to suppliers is often the last resort where there's cash flow problems.

Often we see suppliers being paid too quickly or worse being overpaid. A close eye on this area can provide much needed cash.



CFO On-Call would like to offer a FREE book 'The Seven Key Numbers that Drive Profit and Cash Flow' to readers of this article. Call us for your copy on: 0800 180 400 or visit www.CFOonCall.co.nz (NZ).

'Workplace violence in half of organisations surveyed'

By Massey University

A Massey University survey of 96 organisations found more than half had experienced workplace violence.

Nearly a fifth of the 2,466 cases reported involved physical injury and 175 cases led to lost time and/or hospitalisation.

This accounts for a total of 572 lost working days directly attributable to workplace violence.

The health sector had the highest rate of workplace violence with 42 of the 175 most serious cases of physical assault. The rate is five times the magnitude of the next highest sector, agriculture.

The 2011 New Zealand Workplace Violence Survey aimed to find out the incidence and nature of workplace violence and identify sectors affected.

Study co-author Dr Bevan Catley, of the Healthy Work Group in the School of Management, says the incidence rate for all violence cases (32.3 per 1,000 employees) was very high compared to rates reported by researchers in North America and Europe.

"In dollar terms, the 572 lost days represents a significant cost to industry,

especially when extrapolated across the entire New Zealand workforce and indirect costs such as training, litigation and compensation are taken into account," he says. "Clearly workplace bullying is a multi-million dollar problem and deserves further attention."

The survey covered a range of sectors including manufacturing, health, public administration, scientific and technical services, education, construction, agriculture and utility services.

Violence reported ranged from attempted assault on people and damage to property to serious physical assault. The health sector, which covers health care and social assistance, included nearly a quarter of the more serious physical assault cases.

Dr Catley says while the survey respondents, who were mostly health and safety managers, identified an impressive array of interventions, it was concerning that just 50 per cent formally recognised violence as a hazard in the workplace.

"Interestingly, workloads and time pressure also received relatively high ratings, suggesting work-related stress

increases the perceived risk of violence in the workplace," Dr Catley says.

The online study – which represents over 76,000 New Zealand employees, approximately four per cent of the workforce – is the biggest yet and was based on workplace data from 2009. It shows a higher incidence of physical violence than observed for the 2007 workplace violence survey, which reported 143 cases of physical assault from the 62 organisations responding.

Participating organisations were mainly located in the main New Zealand cities and population centres, including Auckland (24 per cent of organisations), Waikato (8.3 per cent), Bay of Plenty (10.4 per cent), Wellington (10 per cent) and Canterbury (8.3 per cent).

The research was carried out by Professor Tim Bentley, Dr Bevan Catley, Dr Darryl Forsyth and Dr David Tappin.

Read the full study here:

<http://www.massey.ac.nz/massey/learning/departments/school-of-management/research/healthy-work-group.cfm>

Softsource opens first Converged Infrastructure data centre

Ultra-sustainable new Entrada Data Centre opens, entirely supported by latest HP technology

Overview

IT solutions specialist Softsource has opened its state-of-the-art Entrada Data Centre in Albany, Auckland, built entirely on the latest HP technology.

It will be the first operational data centre in New Zealand to offer end-to-end HP Converged Infrastructure, incorporating ISS (Industry Standard Servers), storage and HP Networking. It is also the first time HP's latest 3PAR technology has been implemented in the Asia Pacific region, since HP completed its acquisition of 3PAR.

The Entrada Data Centre will provide New Zealand business customers with flexible and fully orchestrated IT solutions to enable individuals and organisations to scale their needs to meet market demands.

By providing companies with the opportunity to utilise Softsource's Infrastructure as a Service capabilities through the Entrada Data Centre, New Zealand organisations will be able to

dynamically provision virtual resources from a remote location within minutes and be operational immediately.

Attractive entry-level costs coupled with the ability to scale up rapidly as needed, mean that customers are able to remotely specify their hardware requirements and will have access to their custom-designed solution within 15 - 30 minutes.

The Infrastructure as a Service (IaaS) model provides businesses with added security and storage benefits. In addition to this, co-location, email & web security, email archiving, online backups, disaster recovery and continuity to businesses are also available.

The new facility also has strong green credentials and has been built with a focus on sustainability and efficiency. The Tier Three facility offers carrier neutral, 24/7, ultra high-density racking and there are plans for the data centre to become self-sustainable in the future. Clients are then able to enjoy reduced operational

costs through lower power consumption and simplified systems structure.

The data centre is now open and has been operational since early June 2011.

Product and service features

Softsource's Entrada Data Centre uses HP Converged Infrastructure, an integrated solution involving ISS, 3PAR and HP Networking. The design of the data centre is based on HP's Converged Infrastructure architecture that integrates server, storage, networking and management resources into a modular and adaptable design. This flexible architecture enables easy management of clients' existing, as well as future, business and technology requirements.

Features include

ISS (Industry Standard Servers):

HP ProLiant DL360 G7 and DL380 G6 servers are housed within the Softsource data centre, providing the centre with the most energy efficient servers in the industry. The inclusion of new HP high efficiency Power Supplies, which meet 80 PLUS Platinum 94% power efficiency specifications and are part of Thermal Logic technology, help reclaim wasted energy and save money.

StorageWorks Division (SWD):

The 3PAR F400 Storage System brings the utility storage revolution to fruition for Softsource. The 3PAR F400 quad-controller architecture is built to deliver a multi-tiered, multi-tenant storage platform, which provides the agility to align application requirements with data Quality of Service (QOS) levels flexibly, precisely,



Pablo Garcia-Curtis, General Manager, Softsource

and on demand as required by the Softsource services offerings.

ESN/ProCurve Networking:

The Softsource data centre architecture is built on modular and resilient HP Networking E5412 fabrics. This allows a secure, scalable and customer partitionable network layer capable of incorporating embedded services. With 10Gbps connectivity and a dual IPV4/6 base operating system, the fabrics provide a platform that ensures Softsource customers experience a flexible and adaptable service roadmap.

Environmental features

The Entrada Data Centre will be a platform for green, energy-efficient business services and has been designed with the environment in mind.

Features include

Heat sensors:

Heat sensors provide maps of the areas that require more or less cooling, allowing tailored cooling solutions and preventing excessive use of cooling systems.

APC InRow Cooling Solutions:

State of the art hot aisle APC InRow Cooling pods maximise the cooling effectiveness in the new high-density data centre. These water cooled InRow cooling units increase the efficiency, capacity, and predictability of the cooling systems. The hot water produced by the cooling units is sent through an in-ground heat disbursement system before being chilled by energy efficient chillers.

Renewable sources:

There is potential to insert wind turbines and solar arrays at the data centre, enabling it to develop energy generation capabilities and potentially become self-sustainable.

Softsource has also expressed an intention for the data centre to reach a Power Usage Effectiveness (PUE) rating of 1.2, significantly lower than the New Zealand average of 1.6 – 1.9 and in line with leading international organisations, such as Google and Yahoo.

Based on initial pilot tests, it is estimated that the Entrada Data Centre will deliver a 20- 30% reduction in power consumption compared to other facilities, with capacity to increase this energy saving to 35-40% in the future. This will provide cost benefits for customers.

Onsite design features

Specific onsite design features include:

- Racks have been optimised to work more efficiently in a high-density environment and can sustain up to 30 kilowatts per rack. Each rack is designed with two power supplies to provide N+1 power redundancy.
- The data centre is currently designed for up to 40 racks, although there is room for future expansion.
- The above ground level building floor has been strengthened to accommodate up to 850Kg per sq metre.
- The power, cooling and network elements of the Softsource Data Centre have been designed with N+1 redundancy to ensure availability.
- Colocation racks have been designed to deliver secure half racks through to full height high density racks.
- In addition to the UPS device an onsite auto-start generator with a 24 hour fuel supply ensures power supply to the data centre.
- All cabling is Cat 6a and supports the 10Gb network core. Dual VESDA detection systems protect the data centre along with a FM200 gas suppression system.
- Round the clock environmental monitoring for heat, water, humidity, power and fire.

Customer benefits

The Entrada Data Centre will provide the latest technology, infrastructure and services that organisations need for cloud computing application modernisation and data centre operation.

It will enable customers to fully scale their IT requirements as required to suit their business needs, meaning customers will be able to improve operational efficiency, drive down costs and increase competitiveness.

The cost reduction enjoyed as a result of the centre's significant energy efficient capabilities will improve customers' business and environmental outcomes, with up to 40% savings over costs associated with legacy data centres.

Customers will also be able to enjoy the benefits of having 24/7 support from the Softsource team and the significant product and technical knowledge they offer.

The Entrada Data Centre has the capability to service both New Zealand and international customers.

For more information visit:

www.softsource.co.nz or
www.entrada.co.nz

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
PO Box 4, Ahipara,
New Zealand 0449

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

Mr Mrs Ms _____

Surname _____

Title _____

Company _____

Postal Address _____

Telephone _____

Email _____

Date _____

Signed _____

nzSecurity Magazine
A trusted source of information for industry professionals

New Challenges Emerging as Virtualisation and Private Clouds Go Mainstream

By Symantec

Symantec Corp has announced the findings of its 2011 Virtualisation and Evolution to the Cloud Survey which examined how organisations plan to move business-critical initiatives to virtual and hybrid cloud computing environments. The survey highlighted topics including server, client and storage virtualisation, storage-as-a-service, and hybrid/private cloud technologies; and the results uncover disparities between expectations and reality as enterprises deploy these solutions. CEOs and CFOs are concerned with moving business-critical applications into virtual or cloud environments due to challenges including reliability, security, availability and performance. The survey is based on more than 3,700 respondents from 35 countries worldwide.

“Cloud computing represents a major shift within IT – changing from a traditional IT delivery to a service-provider model. Moving to the cloud is a complex evolution for many companies and it’s essential that IT and executives are aligned on initiatives,” said John Magee, vice president of virtualisation and cloud solutions, Symantec. “Virtualisation is an enabler for private and hybrid clouds and our survey shows that planning a seamless move is critical to achieving all the simplicity, affordability and efficiency that these environments have to offer.”

Gaps Between Expectations and Reality Reveal Market Evolution

Adoption of server virtualisation is widespread and more than 75 percent of organisations are discussing private and hybrid cloud deployments. Of the technologies evaluated in the survey,



server and storage virtualisation are the most mature with 45 and 43 percent of enterprises implementing. Private storage-as-a-service is the least mature with 36 percent adopting.

Early investments have revealed gaps between expectations and reality which indicate that organisations are still learning what these technologies are capable of and how to overcome the new challenges they bring with them. We asked respondents about initial goals in server, storage and endpoint virtualisation; private storage-as-a-service; and hybrid/private cloud. We then asked those who have already implemented which goals they actually achieved. The difference between the two answers revealed an expectation gap.

Server virtualisation projects were most successful, with only a 4 percent average gap between expected and realised goals. The biggest gaps occurred in scalability, reducing capital expenditures and reducing operating expenditures.

The average shortfall in storage virtualisation was 33 percent, with disappointments coming in agility, scalability and reducing operating expenditures.

Respondents reported an average gap between expected and realised goals of 26 percent with endpoint/desktop virtualisation. They cited disappointments in new endpoint deployment, application delivery and application compatibility.

Seventy-seven percent of organisations are considering private storage-

as-a-service, but these projects are challenging to implement and fall short of expectations by 37 percent. For example, complexity reduction was a goal for 84 percent of respondents, but reached by only 44 percent.

These gaps are a hallmark of early stage markets where expectations are out of step with reality. As the virtualisation and cloud markets continue to mature, we expect to see those gaps close.

Increasing Focus on Business-Critical Applications

Organisations investing in virtualisation and hybrid/private cloud technologies tend to follow a similar path, starting by virtualising less critical applications such as test and development environments and progressing to more important applications such as email and collaboration; line of business; eCommerce and supply chain; and ERP/CRM.

The survey shows that organisations are leveraging virtualisation for business-critical applications. Of enterprises who are implementing virtualisation, more than half (59 percent) plan to virtualise database applications in the next 12 months. Fifty-five percent plan to virtualise web applications, and 47 percent plan to virtualise email and calendar applications. Forty-one percent plan to virtualise ERP applications.

We found that organisations are more slowly leveraging hybrid/private cloud technologies for business-critical applications. An average of just 33 percent of business-critical applications such as ERP, accounting and CRM are in hybrid/private cloud environments. Respondents stated concerns over account, service, or traffic hijacking; authentication vulnerabilities; access vulnerabilities; disaster recovery; and encryption.

Quality of Service Challenges Emerge as Top Priorities

As virtualisation and private cloud technologies become more widely adopted, the cost and performance of storage is becoming increasingly top of mind. More than half of respondents (56 percent) said storage costs somewhat or significantly increased with server virtualisation. Of those in the process of virtualising storage, the top three reasons for deployment include reducing operating expenses (55 percent), improving storage performance (54 percent), and improving disaster recovery readiness (53 percent).

Seventy-six percent of enterprises who have implemented server virtualisation

indicated that security was a somewhat/extremely large factor in keeping various constituents from being more confident about placing business-critical applications on virtualised servers. Sixty-three percent listed security as a significant/extreme challenge to implementing server virtualisation.

Performance issues are a factor for the majority of organisations. Seventy-six percent of those who have implemented server virtualisation stated that performance was a somewhat/extremely large factor in keeping various constituents from being more confident about placing business-critical applications on virtualised servers. Seventy-two percent of organisations that have implemented hybrid/private clouds cited performance as a significant/extreme challenge.

Among enterprises that have implemented server virtualisation, reliability was the number one concern. Seventy-eight percent said it was a somewhat/extremely large factor in keeping various constituents from being more confident about placing mission-critical applications on virtualised servers. Of those who have implemented storage virtualisation, 83 percent stated uptime and availability as an important goal.

IT and Business Executives Out of Synch on the Potential

According to the survey findings, 46 percent of CFOs who are implementing hybrid/private clouds are less than “somewhat open” to moving business-critical applications into those environments. Forty-four percent of CEOs are cautious about moving these applications.

Main concerns cited about virtualisation and hybrid cloud deployments are reliability (78 percent), security (76 percent), and performance (76 percent). In practice, many C-level concerns are unfounded based on responses from IT. For example, concerns about performance are a top reason cited for caution, yet 78 to 85 percent of those who deployed server virtualisation achieved their goals related to performance.

Recommendations

Enterprise IT’s evolution to the cloud has a fair share of challenges, but also compelling rewards. Despite concerns, most enterprises are implementing virtualisation and moving to a cloud computing future. For these enterprises, Symantec offers recommendations to help make the journey as smooth as possible.

Ensure alignment between IT and executives in virtualisation and cloud initiatives: It is important to show that you can address C-level concerns such as security and availability. Show that their concerns, while important, can be successfully overcome by leveraging existing best practices and robust solutions that ensure valuable information and critical applications are protected and highly available.

Don’t operate in a silo when it comes to cloud computing: Virtualisation and cloud initiatives are most successful when implemented as mainstream, comprehensive IT initiatives. Because they involve all aspects of IT (servers, storage, network, applications, etc.) they can fail when managed as siloed “special projects.” Rather, treat cloud as an IT-wide initiative with all departments included in planning and implementation.

Leverage and modernise your existing infrastructure: Before you’re ready to implement hybrid/private cloud, make sure you are leveraging the existing infrastructure to achieve the same efficiencies and then modernising it as needed. Convert static servers, storage and networking into a virtualised pool of resources. Replace static provisioning with self-service provisioning, and make sure to implement monitoring and metering to demonstrate value to the business.

Set realistic expectations and track your results: Remember that despite the hype, cloud is a new and still maturing market. Do your homework to set expectations that are realistic, then follow up and track results to identify ways to improve project efficiency going forward.

Symantec’s Virtualisation and Evolution to the Cloud Survey

Symantec’s Virtualisation and Evolution to the Cloud Survey is the result of research conducted in April 2011 by Applied Research, which surveyed IT and C-level professionals responsible for computers, networks and technology resources at small, medium, and large enterprises (defined as 1,000-2,400, 2,500-4,999, and 5,000+ employees). The report was designed to gauge how organisations plan to move mission-critical initiatives to virtual and hybrid cloud computing environments. The survey included more than 3,700 respondents from 35 countries in North America, EMEA (Europe, Middle East and Africa), Asia Pacific and Latin America.

HD PELCO DVR from **intek**

PELCO DX4700 & DX4800 Hybrid Video Recorders



Users can now enjoy the benefits of megapixel image detail to watch registers, cash counting operations, high-value merchandise areas or lobbies and entrances, while still utilising existing analog cameras and cabling. An intuitive interface makes custom installation easy and decreases learning time for end-users.

Product Features:

- H.264 compression
- Megapixel hybrid performance
DX4700-30/25 IPS @ CIF
DX4800-30/25 IPS @ 4CIF
- Connectivity to DX and DS clients
- Internal storage up to 8TB
- DVD standard
- PTZ, Coaxitron
- Supports KBD 300A
- Bi-directional audio



intek

www.Intek.co.nz
Freephone 0508 4 INTEK

Honeywell Mid Segment Cameras from **intek**

Honeywell Vista Range of Fixed and PTZ Cameras



Honeywell Vista Series Cameras are designed for cost-effective and quality surveillance applications. With Day/Night switching, WDR, BMB and DNR functions, the Vista Series Cameras are perfect for a wide range of both indoor and outdoor environments.

Fixed Camera Features:

- 1/3" Sony Super HAD CCD >540TV
- Minimum Illumination of 0.001lx (DSS On)
- Day/Night, WDR, DNR, Privacy Zone Masking

PTZ Features:

- 1/4" Sony Super HAD CCD
- 10x Optical Zoom, 16x Digital Zoom
- 240 preset, 8 pattern, 8 Tour, 8 Scan
- Vandal-proof roof and IP67 on VSD-101P



intek

www.Intek.co.nz
Freephone 0508 4 INTEK

DSC MAXSYS by **intek**

Proven Fully Integrated Access & Security System

*New starter kits now
available at extra low prices*



The new number one value proposition for integrated intrusion and building access control systems in New Zealand.

An unbeatable single-system solution particularly suited to New Zealand's typical small to medium retail, commercial, industrial and institutional facilities, as well as large or multi-level residential units.

The new range of Maxsys all inclusive starter kits from INTEK are now even easier to specify and cheaper to install.



intek

www.Intek.co.nz
Freephone 0508 4 INTEK

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



ASSA ABLOY

SNC-CH210

Network HD Camera - X Series



Full HD
1080

Compact Affordable 1080p HD
Security Camera

- Excellent 1080p HD picture quality supporting H.264 at 15fps
- 3 Megapixel (2048 x 1526) maximum resolution
- Three codecs (h.264, MPEG-4, JPEG) and a dual streaming capability
- The Exmor CMOS sensor incorporated to deliver high quality and low noise

SONY
make.believe

SNC-DH210

Network HD Camera - X Series



Full HD
1080

Compact Affordable 1080p HD
Security Camera

- Excellent 1080p HD picture quality supporting H.264 at 15fps
- 3 Megapixel (2048 x 1526) maximum resolution
- Three codecs (h.264, MPEG-4, JPEG) and a dual streaming capability
- The Exmor CMOS sensor incorporated to deliver high quality and low noise

SONY
make.believe

SNC-CH160

Network HD Bullet Camera



HD

Integrated IR Day Night Camera
Weatherproof IP66

- Excellent 720p HD picture quality, supporting H.264 at 30 fps
- 1.3 Megapixel (1280 x 1024) maximum resolution
- Three codecs (H.264, MPEG-4, JPEG) and a dual streaming capability
- The "Exmor" CMOS sensor incorporated to realise high image quality and low noise

SONY
make.believe



Dallmeier DMX 1600 S Matrix

Your ideal entry into the world of Video IP solutions!

The Smatrix is ideally suited for applications requiring high-speed recording, expanded storage capacity and low power consumption, while ensuring maximum security. The DMX 1600 is a hybrid audio and video recorder with integrated storage system for up to 16 free allocatable video channels. Using a release code the basic version with 8 free allocatable video channels can be expanded by up to 8 further free allocatable video channels (maximum 16 channels in total).

The DMX 1600 has a compact design (2HU) and is designed for mounting into a 19" rack!



Dallmeier DMS80

The DMS 80 is a stand-alone hybrid audio and video recorder with support for up to 24 channels including High Definition.

- Up to 8 free allocatable and 16 IP based video channels (SD-IP/HD-IP)
- PentaplexPlus functionality: Simultaneous real-time recording, streaming, live display, playback and remote access
- Hybrid recording: H.264, MPEG-4, MJPEG
- Bit rate up to 1.5 Mbps with analogue cameras, up to 6 Mbps with IP cameras
- Resolution with analogue cameras: up to 4CIF
- Resolution with IP cameras: SD, HD (720p, 1080i, 1080p), up to 8 MP
- Frame rate per channel up to 12 fps at CIF with analogue cameras, up to 25 fps at 1080p with IP cameras



Dallmeier DDZ4010HD-SM PTZ

The high-resolution full high-definition Cam_inPIX® colour dome camera DDZ4010-YY/HS/HD with 10x optical zoom is available in different mounting variants (in-ceiling, surface, weather-proof).

- 1/3" high-definition sensor with Cam_inPIX®
- Pure Digital Signal Processing
- High-speed PTZ dome
- 10x optical zoom, 12x digital zoom
- AWB, AGC, BLC and extended slow shutter
- Auto-focus with manual override
- Resolution: SD, HD (720p, 1080i, 1080p)
- Frame rate up to 60 fps2)
- Video compression: MJPEG, H.264
- Simultaneous multi-streaming with independently adjustable resolutions, frame and bit
- Motion detection with selectable sensitivity
- Weather-proof variant



PARADOX®
SECURITY SYSTEMS

TM40 Touch Interface Module - NEW PRODUCT RELEASE



A Touch of Paradox

- 4.3-inch (10.9 cm) brilliant and vivid widescreen color display
- Compatible with EVO V2.16 or higher and MG/SP V4.72 or higher
- Supports up to 32 floor plans
- Controls up to 8 PGM outputs
- Supports WinLoad, not NWare
- In-field firmware upgradable via micro SD card
- Powerful FPGA processor
- Indoor temperature sensor
- Faceplate available in 3 finishes: brushed aluminum, brushed black anodized, brushed white anodized

Distributed exclusively through Atlas
Gentech - Freephone 0800 732 637

PARADOX®
SECURITY SYSTEMS

REM101 Emergency/Panic Remote - NEW PRODUCT RELEASE



A Touch of Paradox

By pressing the action button for two seconds, the recently released Paradox REM101 remote, can be used to activate emergency/panic signals.

The REM101 is compatible with all firmware versions of MG panels and MG Consoles, as well as any firmware version of RTX3 and RX1 for use with SP and EVO panels.

The REM101 is also suitable for use in clinics, restaurants and other similar entities due to its applications. The battery is designed to last at least 1,800 transmissions or 5 years.

Distributed exclusively through Atlas
Gentech - Freephone 0800 732 637

IQeye Alliance-mx HD Vandal Dome Camera



IQinvision
smart camera systems

Introducing the Alliance-mx, IP camera combining sleek design with some of the most innovative HD/megapixel technology in the industry.

Alliance-mx uses MAIN Profile H.264 to deliver exceptional high-definition clarity at up to 30 frames-per-second. A high-quality, ultra-strong polycarbonate bubble and powder-coated aluminum body make Alliance-mx vandal resistant yet esthetically pleasing in any scenario.

- H.264 and MJPEG
- Varifocal Megapixel Lens (3-13mm)
- All-Weather IP66 Housing
- Day / Night High Definition Camera
- 480p / 720p / 1080p

Distributed exclusively through Atlas
Gentech - Freephone 0800 732 637

FSH FES10 Electric Strike



Features

- 5 Year Warranty
- Stainless steel faceplate and keeper
- Easy installation
- Low power consumption
- Weather resistant
- Superior holding strength
- Dual Voltage
- Field Changeable

Specifications

Holding Force: Over 1300kg. Dual Voltage:
12V DC 200mA or 24V DC 100mA. 4 Hour
Fire Rated. Power to Lock or Power to release
– Field Changeable. ANSI Footprint.

Ph: 09 580 1576

Email: sales@nfs.co.nz • Web: www.nfs.co.nz



LOW VOLTAGE ELECTRONIC SUPPLIER

Securing The World One Door At A Time

Grow your system from one location and one PC to 32,000 locations and up to 999 PCs on a Wide Area Network.

Intelligent Controllers give DSX enormous flexibility and diversity.



**New Zealand's Exclusive
distributor for DSX**



Contact:

Ph: 0800 377 379

ESS DSX

Sales@eSecuritySales.com

Long Range 4 Button Transmitters

- ◆ Wiegand Output
- ◆ Farpointe / Keri, HID, Indala, Tecom, iClass & Mifare combos available
- ◆ Custom Formats available
- ◆ Up to 30 meter read range
- ◆ Robust weather resistant casing



Farpointe Data
Readers • Cards • Tags

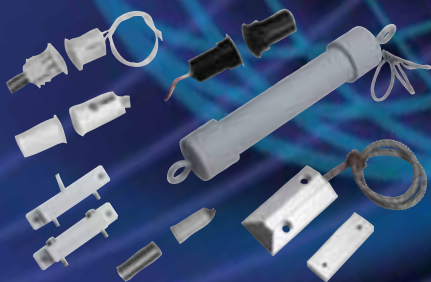


Contact:

Ph: 0800 377 379

Sales@eSecuritySales.com

To advertise your new products here contact Craig



total reed switch solutions from Flair

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

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

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



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 Power distribution module



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

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

Comprises

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

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



**Loktronic Innovationz
LIMITED**

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

15387_FL

**Loktronic Innovationz
LIMITED**

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

15388_PSC

**Loktronic Innovationz
LIMITED**

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

15389_PDM

Powerful Yet Cost Effective Flexible, Expandable



Features

- 16 Reader access control system
- Built in Elevator Control, for up to 32 levels
- 16 Fully supervised inputs
- 16 Open Collector outputs
- Communications: 1 x RS-232 + 1 x RS-485
- Dial up modem or optional TCP/IP interface
- 2,000 users
- 2,000 events

ISCS New Zealand Ltd

5 Arawa Street,
Grafton, Auckland
Ph: 09 3666 150
Fax: 09 3666 151
Email: salesnz@iscs.co.nz • Web: www.iscs.co.nz



The definitive LONG RANGE SOLUTION that opens it all!



Connects to an Access Control System just like a prox / smart card Reader!

Just one product and with the touch of a button, the i-Key 4 is the smart and simple way to control access to your secure areas such as boom gates, rising barriers, roller shutters and doors. Cutting edge technology allows the i-Key 4 to enter multiple facilities with just one key. Use the i-Key 4 and your secure access couldn't be simpler!

Features

- Multiple frequencies available
- Easily Interfaced
- Long Range
- 4 Wiegand Outputs
- Flexible
- High Security



ikey4 supports technologies such as, HID, Indala, Farpointe Data/Keri proximity, along with iClass, Mifare, Tecom/GE smartcard technologies.

ISCS New Zealand Ltd

5 Arawa Street,
Grafton, Auckland
Ph: 09 3666 150
Fax: 09 3666 151
Email: salesnz@iscs.co.nz • Web: www.iscs.co.nz



Are You Looking For A Smarter Card Solution?

ISCS is pleased to introduce the iCLASS GOLD CLASS Program, offering users the highest level of card-to-reader security available today!

Gold Class

When using iCLASS contactless smart card technology, The GOLD CLASS program offers users the choice of their own secure 26,33,34,37 or 38 bit format. This format includes a company ID Code that is unique to each user. For added security ISCS tracks all card numbers to ensure that no duplications occur.

Security is further enhanced through the use of an encrypted authentication (security) key. This authenticates the card and reader.



GOLD CLASS is the security professionals first choice for ultimate security of your facilities.

ISCS New Zealand Ltd

5 Arawa Street,
Grafton, Auckland
Ph: 09 3666 150
Fax: 09 3666 151
Email: salesnz@iscs.co.nz • Web: www.iscs.co.nz



on 09 409 2018 or craig@newzealandsecurity.co.nz

Panasonic NVR WJ-NV200K



The WJ-NV200K provides the first real alternative to analog DVRs – at an analog price point!

Ideal for retail, hospitality and Education markets, the WJ-NV200 is driven via mouse and keyboard to eliminate PC costs and desk space.

Installation is simplified by quick setup automatic camera detection and simple setup wizard – all without requiring a PC.

Real time Face Matching is also achieved using the Face Detection feature of the Panasonic Smart HD range of IP cameras. This provides fast detection and matching VS a stored database of known faces to alert the operator / store owner of unwanted guests.

Features Include:

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

Panasonic New Zealand Ltd

350 Te Irirangi Drive, East Tamaki, Auckland
Ph (09) 272 0100 • sales@nz.panasonic.com

Panasonic

Panasonic Video Doorphone VL-SW250BX



The VL-SW250BX is the latest video door phone from Panasonic. Monitor and even open the door remotely via the wireless handset. The main station stores up to 400 images to see who has been knocking while you were out!

Ease of installation as a single twisted pair is all that's required from the gate station to the main monitor.

Features Include:

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

Panasonic New Zealand Ltd

350 Te Irirangi Drive, East Tamaki, Auckland
Ph (09) 272 0100 • sales@nz.panasonic.com

Panasonic

Panasonic SD5 Dome WV-CF504E



Panasonic have released an internal dome variant of their class leading Super Dynamic 5 analog camera. The WV-CF504E has the same functionality as the popular full body camera in an attractive compact dome.

SD5 is still recognized as the best performing camera in severe backlight situations! perfect for retail, corporate and industrial applications.

Features Include:

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

Panasonic New Zealand Ltd

350 Te Irirangi Drive, East Tamaki, Auckland
Ph (09) 272 0100 • sales@nz.panasonic.com

Panasonic

Challenger™ IP LAN Adaptor

Save time and money installing Challenger™ with the new TS0098 Challenger IP LAN Adaptor.

TS0098 modules allow Challenger RS-485 LAN data to be carried over an IP network. This provides an IP connection between a Challenger panel and its LAN devices such as Remote Arming Stations (RAS) and

Data Gathering Panels (including Intelligent Access Controllers) reducing the need for dedicated wiring of expensive two-pair twisted, shielded data cable (Belden 8723).

The TS0098 also enables physically separate segments of the Challenger RS-485 LAN to be linked together over an IP network, either to extend distance or inexpensively utilise existing IT infrastructure. TS0098 modules provide securely-encrypted IP communications via a unique 128-bit encryption key.

The TS0098 can be configured easily and conveniently over the IP network via a web browser. The new TS0098 is available via your local Hills branch.



For more information please visit www.utcfs.com.au/IPLAN

Monitor the LED “ECO Savings”



The new Pacom range of “ECO Saving” security specific LED Monitors from Hillsec consists of 2 series: E-series and the P-series.

The ‘E-series’ monitors consist of 2 sizes and are ideal for office type environments, requiring monitors for PC’s and workstations etc. These new models are available in 18.5” and 21.5” LED screen sizes with the 21.5” offering Full HD Resolution (1920 x 1080).

Meanwhile, the ‘P-series’ features 18.5”, 21.5” and 23” LED screen sizes, with the latter two offering Full HD Resolution (1920 x 1080). They also feature a trigger input which switches between inputs on activation providing a number of viewing options.

The E-series and P-series monitors provide substantial savings in running costs when compared to LCD monitors and result in lower CO2 emissions, providing greater environmental benefits for us all today and for future generations.

The E-series and the P-series LED Monitors are available from your Hillsec branch.

AXIS Q1755/-E Network Cameras



AXIS Q1755/-E Network Cameras deliver HDTV 1080i or 720p in compliance with the SMPTE 274M and 296M standards regarding resolution, colour fidelity, 16:9 format and full frame rate.

The cameras enable multiple, individually configurable streams in H.264 and Motion JPEG. H.264 greatly optimizes bandwidth and storage without compromising image quality. AXIS Q1755/-E cameras have 10x optical zoom, 12x digital zoom and auto focus.

Installation is made easy with Power over Ethernet (PoE, IEEE 802.3af), which eliminates the need for power cables. The cameras also have an SD/SDHC memory card slot for storing recordings locally. AXIS Q1755/-E cameras offer video motion detection, audio detection, active tampering alarm and the Gatekeeper functionality, which enables the cameras to automatically zoom in when there is activity in the scene, and then zoom out after a preset time interval.

The AXIS Q1755/-E Network Cameras and the AXIS range is available from your Hillsec branch.



For more information on their great product range visit your local Hills branch or go to www.hillsec.co.nz



KCV-D374 - Kocom's ultimate intercom



Kocom have definitively expanded their innovative range of intercoms with the new KCV-D374 intercom, now available at Hills Electronic Security. The KCV-D374 comes encased with a large 7” colour LCD screen - renowned for displaying bright and refined imagery through its widescreen design.

The KCV-D374 features hands-free functionality, on screen display (OSD) and touch keys, which all link seamlessly together to help keep in line with Kocom’s vision to simplify communicating with visitors.

For added security, the KCV-D374 enables users to conveniently connect to an additional monitor, 2 door strikes and 2 door cameras. Users are able to intercommunicate between an additional monitor, whilst at the same time, monitor their premises through the connected door camera(s).

With its 4 wire capabilities, the KCV-D374 can integrate flawlessly with the new Hills ComNav, allowing users to communicate with visitors whilst away from home through their Hills alarm system.

Kocom’s ultimate intercom KCV-D374.

Security Commander™ has arrived



The most powerful Windows management software for Challenger™ is now available from Hills Electronic Security.

Security Commander™ is a highly-scalable multi-site application that can support up to 128 Challenger panels, over 6,000 intelligent doors and 32,000 alarm points.

Security Commander™ is compatible with Windows 7 and is intelligently based on a SQL database, ideal for easy access to raw data for powerful database replication, information exchange and custom reporting.

One of the Security Commander™ standout features is its client-server architecture, capable of allowing up to 10 operator workstations to manage the system simultaneously.

Even more exciting news is the Security Commander™ video integration capabilities with supported GE/UTC DVR’s, allowing Challenger alarms and other events to be linked to video footage for improved operator response and easier post-event investigation.

Eager to find out more? Then contact your local Hills Electronic Security branch today for a demo and information about training dates.

Hillsec heats up with Flir Systems



The new and exciting Flir Systems product range of Thermal Cameras is now available at Hillsec!

Thermal cameras compliment and complete your security camera network by giving you the power to see threats invisible to the naked eye, turning night into day (as seen in the image below).

Thermal security cameras make images from the heat energy that is around us all the time, not from reflected visible light, giving you true 24/7 imaging capability without lights or illuminators.

The cameras are enhanced further by FSM (Flir sensor manger) software which offers complete management of connected thermal cameras. Analytics and radar integration are just some of the benefits of FSM.

For information on the hot FLIR range visit your local Hillsec branch.



UTC Fire & Security
A United Technologies Company

Hills
Electronic Security
New Zealand

Security CommanderTM

NEW Management Software for ChallengerTM

Windows 7 Compatible

Client Server Architecture

SQL Database

CCTV Video Integration

Multi-site Partitioning



Available
now at
Hills

Hurry and book your training dates and demo with Hills Electronic Security today!



Training & Support with Hills Electronic Security

Together with UTC Fire & Security, Hills Electronic Security have developed a specialised training course to assist you to take full advantage of Security Commander's advanced features and capabilities.

Don't leave it to the last minute to book your training. Be quick to secure your spot!

For more information, be sure to contact your local Hills Electronic Security branch or visit our website at www.hillsec.co.nz

Available from:

Hills
Electronic Security
New Zealand
www.hillsec.co.nz

AUCKLAND
Penrose
Albany

09 525 8007
09 525 8007

CHRISTCHURCH
Sydenham

03 374 6277

WELLINGTON
Petone, Lower Hutt

04 939 9355

An ID Change for Cardax

cardax a recognised leader in security management systems and a key part of the Gallagher Group for more than 10 years.

To further support our success, Cardax will now move to the world-wide brand name of Gallagher.

The name is changing and with our people designing even better products, it's going to get even better.

For further information visit: gallaghersms.com/renaming

