

August / September 2014

ISSN 1175/2149

# NZSecurity



## Hills Acquisition

Creates NZ's Largest Security Sector Distributor

## NZ Security Conference 2014

Professionalising for Profit: Your Passport to Success

## Fewer Fires

Challenge Cost and Role of Fire Services

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



# EVERY HERO NEEDS A SUPERPOWER



## LS-SERIES

Compact Thermal Night Vision Monocular

Use your power of thermal imaging on duty.  
Catch suspects, find victims and recover  
evidence in total darkness.

**BE AWARE  
BE DECISIVE  
USE THERMAL**

For more information and to view the  
video go to: [www.flir.com.au/nzsecurity-le](http://www.flir.com.au/nzsecurity-le)

**Free Call: 0800 785 492**

The images displayed may not be representative of the actual  
resolution of the camera shown. Images for illustrative purpose only.



 **FLIR**



# Best imaging Smart solutions



## Smart solutions for every day IP video surveillance.

Are you looking to secure your business and take care of your system costs without compromising on image quality simultaneously? Benefit from IP 2000 and IP 5000 family cameras with the new DIVAR IP recording solutions from Bosch. By smartly combining these products you can tailor and scale your IP video solution to fit your needs. Guaranteeing best imaging, substantial reduction of storage costs and 24/7 access to your HD video images. The DIVAR IP recording solutions can handle up to 128 channels and storage devices can be added to meet growing storage requirements.

[www.boschsecurity.com.au](http://www.boschsecurity.com.au)



**BOSCH**  
Invented for life

**ZoneTechnology**  
Your Security Supply Partner

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

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

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

**Christchurch**  
225 High Street  
Christchurch  
Ph: 03 365 1050

## Contact Details

**Craig Flint**

Telephone: +64 07 868 2703  
Mobile: +64 (0) 274 597 621

Postal and delivery address:  
27 West Crescent  
Te Puru 3575  
RD5  
Thames  
New Zealand

All enquiries to  
[craig@newzealandsecurity.co.nz](mailto:craig@newzealandsecurity.co.nz)  
Editorial contributions welcome.

## October/November

- Professional & Business
- Accountants
- Lawyers
- Managers
- Consultants

## December/January

- 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.

# CONTENTS

- 6 Professionalism and a passion for future growth. We profile the new General Manager for all the Hills Building Technologies businesses in NZ, Kerry Heard
- 10 Hills Electronic Security's Acquisition
- 12 What is a Risk Management Consultant?
- 14 Risk = Chance x Effect
- 18 Western Digital launches expansion of NAS storage product ranges
- 21 Unlicensed Security Company Fined
- 22 BYOD Security
- 24 BYOD Threats
- 25 Allegion (New Zealand)
- 26 Connectivity and Convergence at GIL 2014 New Zealand
- 28 2014 Conference
- 30 Our focus is creating intelligent IP video solutions that fit your needs
- 32 NZ Security Training Association
- 33 The Countdown's On
- 34 Mandatory Training - What Have We Learnt?
- 36 The Convergence of IT Security and Physical Access Control
- 40 Thermal Imaging
- 43 Maeae Fires Reinforce Urgency
- 44 Fewer Fires Challenge
- 48 Kiwi Self Storage Arson
- 50 Code Changes Give More Options
- 54 Product Showcase

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

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

\*Standard terms & conditions of sale apply

**Loktronic**

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

## Associations







Anything. Anywhere. Anytime.

# We've got you covered.



With threats possible from any angle, the unexpected is pretty much a guarantee for critical infrastructure. That's why Axis focuses on securing you from perimeter to core. Our network video surveillance products help you secure your site in even the harshest conditions. Yet beyond that, we constantly work together with our partner network to bring you solutions that ensure safe, uninterrupted production that's also more efficient.

Visit [www.axis.com/critical\\_infrastructure](http://www.axis.com/critical_infrastructure) or send an email to [contact-sap@axis.com](mailto:contact-sap@axis.com)

Distributed by:



# Professionalism and a passion for future growth

We profile the new General Manager for all the Hills Building Technologies businesses in New Zealand, Kerry Heard

One of the key figures behind the biggest supply-side acquisition in the New Zealand security sector in recent years has only been in the industry for a short time but he is already making a lasting impact.

Kerry Heard has spent the last three and a half years leading the well known Intek importation and distribution business in New Zealand as General Manager. In this period, Kerry had been tasked with investigating and implementing a path for the future to achieve the revenue growth aims of the shareholders of the privately



*Kerry Heard leading New Zealand's major security industry supplier at a time of critical change.*

owned specialist importer and distributor.

The end result was the acquisition of Intek by Australian-based Hills Electronic Security.

Previous to his current role, Kerry was a Sales Manager (and for six months acting General Manager) for Monier Bricks and Roofing where he gained valuable experience in acquisitions and mergers, purchasing and integrating another private roofing business into Monier. Prior to this he was the Sales and Marketing Manager for B&D Doors and spent over five years at Carter Holt Harvey in sales, marketing and procurement roles.

Not one to crow about his achievements, Kerry also has significant tertiary qualifications with an MBA, Grad. Dip Bus, NZCS in Chemistry and a NZCE in Metallurgy.

Intek owners had wanted the management services of someone with fresh ideas and who understood channel management, selling processes and the particular vagaries of the New Zealand market. Since his appointment at Intek, Kerry has aimed to build a great culture with well recognised technical support and, for clients, ease of doing business.

While Kerry may have been involved in the security sector for a relatively short period of time, he is passionate about increasing the perception of professionalism of the industry in the eyes of the public. To this end he has been a board member of the New Zealand Security Association for the past three years. He says, "If you want to be the market leader you have

got to act like the market leader." He is very positive about the NZSA as the only organisation in the country solely focused on achieving the highest standards of ethical and professional conduct in the security industry. He says this is very important at a time of critical technological change and the elevation of high levels of professionalism in the industry.

Kerry says that he believes the consumer markets currently view security as a 'discretionary spend' and he would like to be part of changing that perception and having it viewed as 'essential.'

He says, "If consumers come into contact with any element of the security industry then it is incumbent on us to make sure that experience is a good one."

## **Ticket inspectors trial body worn cameras**

A recent coup for the newly merged Hills/Intek distribution company has been the equipping of a group of Transdev passenger rail service ticket inspectors in Auckland with body worn CCTV cameras for a three month operational trial.

The cameras capture high quality audio and video of interactions, and provide the opportunity to take a still photograph of a fare evader to support a Transdev network ban issued to non-compliant travellers. Additionally it is anticipated the cameras will provide a strong deterrent to anyone considering abusing or assaulting a staff member or other customers in the vicinity.



Fare evasion is an ongoing issue for public transport throughout the world and Auckland is no different. With fare evasion currently between four and five percent and revenue lost to fare evasion estimated at almost \$NZ1.5 million dollars per year, additional measures are required to make travel costs fairer for everyone.

Transdev has a team of around 50 ticket inspectors checking train customers at stations and on trains to ensure they are travelling with the correct ticket and, as part of their revenue protection efforts Transdev is committed to a programme of ongoing improvement.

The use of the cameras and network bans will be evaluated at the end of the trial period, for example:

- What did the public think of the use of the cameras and network bans?
- Were the cameras and network bans effective in reducing fare evasion rates?
- Did the cameras influence the behaviour of fare evaders, either positively or negatively?
- Did staff find the cameras a useful tool?

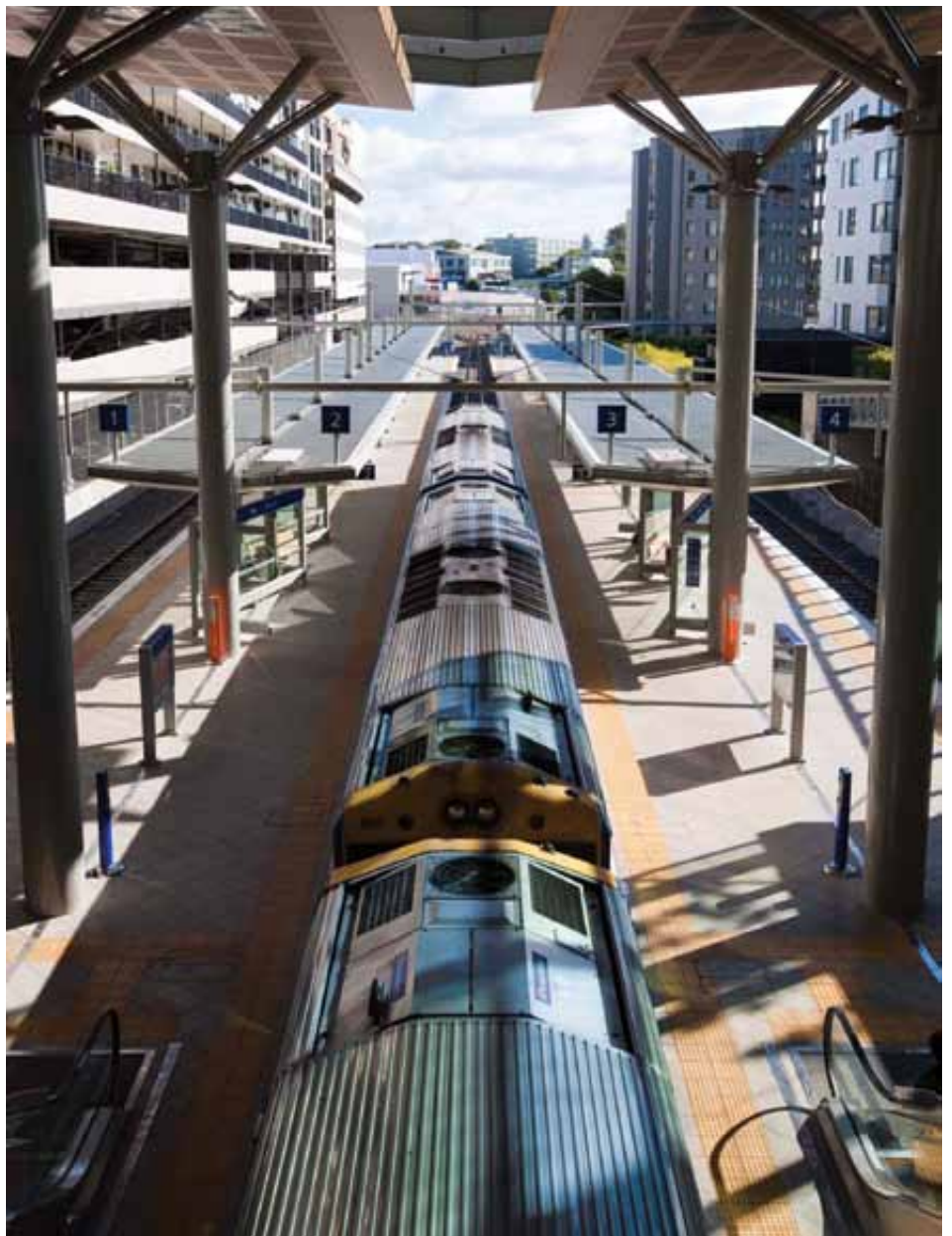
*The use of the cameras (and footage) will be in full compliance of the Privacy Act 1993 and best practice guidelines set out by the NZ Privacy Commission.*

### Top service and a long list of leading brands

The new organisation created by the merging of two of Australasia's leading security industry distributors will be marketing a veritable plethora of 'tier one' brands.

Here is a list of just some of the key names the new company will be distributing:

- Hills Reliance Series security system-ideal for residential and commercial installations
- Honeywell home automation systems
- Pelco thermography and camera analytics
- DSC neo-hybrid intrusion/access control
- Farfisa Zed and Hero intercom systems
- Tyco brands Kantech (large scale access control) and American Dynamics (cameras and free heat mapping)
- Axis IP camera manufacture
- Dvтел large enterprise CCTV cameras
- Tecom Challenger 10 access control
- Genetech IP video surveillance and access control systems
- Pacom integrated security systems



*The Newmarket train station; one of the locations for inspectors using new body-worn camera technology*

- Southwest Microwave outdoor perimeter security and microwave interconnect solutions
- Xandem tomographic motion sensing technology

In addition, the team will be there to assist system integrators and technicians in dealing with the increasing complexities and demands of current CCTV surveillance solutions. They will

be able to provide value added services including: system design, documentation assistance, setting up project hardware both off and on-site staging support, special programming and system customisation support, on-site service support, commissioning support, factory acceptance testing support, training, system acceptance testing support and maintenance support (i.e. systems check - software upgrades etc).

**HILLS<sup>TM</sup>**

For total security,  
one brand brings it  
all together

**HILLS**<sup>TM</sup>

All the components you need to  
offer a total security solution are  
now in one place.

APG

Electronic Security

Intek

OPS



## Tecom Challenger10

### Access control panel.

- Backwards compatible with Challenger V8 peripherals
- Challenger10 panel stores 10,000 events
- Programmable via LCD keypad arming stations or via Interlogix security management software
- Intelligent onboard power supply



## DSC Touchscreen Security Interface

### 7-inch PowerSeries touchscreen display.

- Easy and intuitive way to manage and control security systems
- Intuitive user interface and LED indication of security system status
- Output control
- Picture frame and clock feature
- Menu user programming
- Available in white and silver



## NEW: Xandem Tomographic Motion Detection

Xandem is a revolutionary motion detection technology which utilises nodes to create a wireless mesh to detect intruder movements through walls and obstructions.

- Invisible/hidden – can be installed behind walls
- Integrates with any security or automation panel
- Available in 6, 10 and 15 node kits



## Genetec Security Center

Leading security platform that seamlessly unifies security systems to help protect your organisation.

- Genetec IP security systems include: (Omnicast) video surveillance, (Synergis) access control, and (AutoVu) license plate recognition
- Unified security interface
- Security Center mobile and web apps
- Integration to your business systems



## Pelco Sarix™ Enhanced Mini Dome with SureVision™ 2.0

Delivers industry-leading image quality in the most difficult lighting conditions.

- Autofocus varifocal 3~9mm and 9~22mm MPX lenses
- IP66 rated
- H.264
- WDR
- Low-light performance
- Anti-bloom



For more information on these and other best-in-class solutions from Hills, visit [hills.com.au/branches](http://hills.com.au/branches) for your nearest location.

**HILLS**™

# Acquisition creates NZ's largest security sector distributor

Long established Australian listed corporation, Hills Ltd's subsidiary, Hills Electronic Security (HES) has acquired New Zealand-based Intek Security Group Ltd's security distribution business effective June 3, 2014

**T**he two complementary businesses have been joined in a merger process that was started only recently with a view to instituting some positive and forward thinking consolidation at the distribution end of the security sector in New Zealand. A further aim was to build a market leading importing and distributing business tailored to meet the particular challenges around building management and technologies for the future.

Intek's core competency has been in the area of intrusion control while CCTV has been one of Hill's biggest strength. The deal will allow the two companies to broaden their service solutions and product offerings to a growing customer base.

Bringing these businesses together will position the new entity as the leading provider in the security industry, building on Hills' stated goal of being the largest value added supplier of building technologies across Australia and New Zealand. The belief is that the deal also provides the best platform for further growth.

HES is New Zealand's largest supplier of security equipment, ranging from simple domestic alarm systems up to complex integrated access, surveillance and CCTV systems used in commercial and industrial applications.

Brad Newton, COO and director of Hills Technologies, said the Intek acquisition was a great fit for Hills and for the group's

ongoing strategy of building on its premier market position in the Australian and New Zealand security industries.

"It is very much in line with our strategy to focus on delivering integrated solutions into trusted environments, of which security and its managed solutions are prime components," Mr Newton said.

"Our specialist electronics and security division continues to emerge as a main revenue and profit winner for Hills and we are confident that this trend will continue with the inclusion of the Intek operations into our business."

Parent company of HES, Hills Limited is a trusted and iconic Australian company founded on the innovative Hills Hoist clothes line, created by Lance Hill in 1945.



## Cut through the clutter

*Xandem's TMD devices are immune to intruders avoiding sensors, adaptive to dynamic/ changing environments and can be hidden away (installed behind walls), as the sensing detection waves can see through walls and obstructions. The intelligent sensing technology can be adjusted to suit any application and will not deliver false alarms caused by temperature change or small animals, birds and insects. If you are in need of full coverage sensing, have a cluttered or changing environment, or want to completely hide your motion detectors, Xandem TMD is the best solution.*



Today it is an Australian ASX300 listed company recognised for its delivery of technology and innovation to government, enterprise, business and the home. Today its subsidiaries include DAS, Hills Antenna & TV Systems, Hills Sound Vision and Lighting, LAN 1, Pacific Communications, OPS, Step Electronics and Hills Health Solutions, including HTR, Merlon and Questek.

And just recently, Hills has also announced the acquisition of the Audio Products Group (APG), a long-established and successful Australasian value-added supplier of professional audio products.

Key products within the APG stable include Aiphone, which is the leading commercial and residential intercom brand. Other highly-recognised brands such as Tannoy (speakers), Lab.gruppen (amplifiers), Biamp and TOA are also strong APG performers.

On the Intek side, one of its biggest strengths has been a very strong technical support structure. The New Zealand-based company prides itself on the high standard of the technical expertise of its people and being an innovator and leader in the field. Intek was formed in 2004 and up until the merger was 100 percent New Zealand



*Honeywell is a leading international brand. Its Tuxedo brings touch screen technology to home automation*

owned. The business specialises in the importation and distribution of globally respected brands in the access control, intrusion, communication and surveillance segments, with tier one brands including Pelco, Honeywell, American Dynamics, Assa Abloy, CQR Fire & Security, Kantech, Onetop, ZK Teco, DSC, Optex and ACI Farfisa.

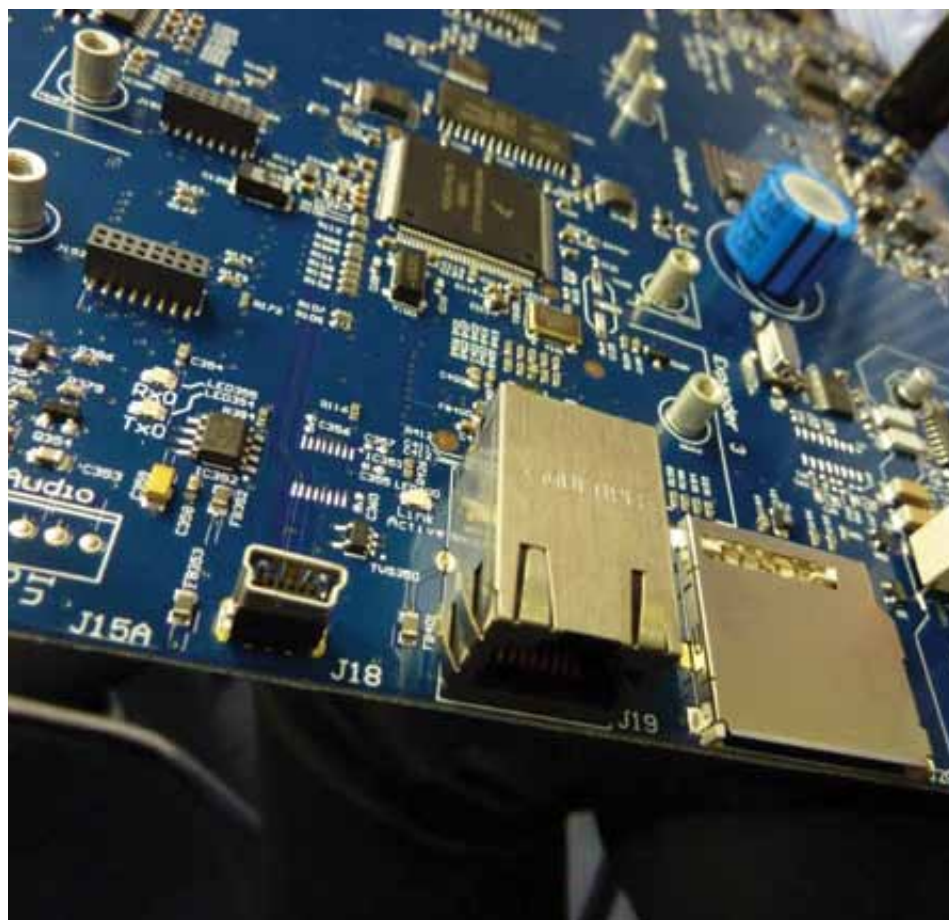
Based in Auckland with regional offices in Christchurch and Wellington, the Intek team comprises 23 staff, with the majority having extensive experience in the security industry in New Zealand. The team at Intek pride themselves on being innovators and leaders in the industry, always challenging the status quo to see if they can improve the level of service that they provide to their customers.

This approach means that it has constantly improved the business and in doing so, become the preferred supply partner for the security industry in New Zealand. The joining of forces with Hills will now allow it to offer even more products and an even better level of technical support.

As a result of the transaction key management personnel will be remaining with the business so it is business as usual for the new identity. While remaining committed to the branches in Auckland, they are seeking larger sites in Wellington and Christchurch for the merged entity to reside in.

Both of the merged companies are currently undergoing an integration of sales teams and back office operations as quickly as possible to ensure a continuation of delivery of services and solutions that customers want and expect. They say the transition will be extremely smooth and customers won't even notice the difference.

Both companies also say they are excited by the bringing together of the two businesses as it will allow them to grow the scale of the business through a bigger network of suppliers and product offerings and take it to the next level in its distribution, supply, design, development, training and maintenance of intercom, intrusion, CCTV and access control.



*The Tecom Challenger access control system has helped facilitate the move into networked environments while retaining existing infrastructure*

# What Is a Risk Management Consultant?

With today's precarious financial market many companies, no matter the size, are investing in the services of a risk management consultant. Because companies are looking for ways to gain business and financial success without making bad decisions and large financial loss, few organizations make major decisions about new projects without first assessing the associated risks.

Risk management is the identification, assessment and prioritization of risks, or the uncertainty of objectives, with coordinated and economical application of resources to minimize, monitor and control the probability and impact of unfortunate events.



*Ervin has more than 30 years of professional experience in the power industry, serving in multiple roles including engineering and finance. Erv has extensive experience in power generation, transmission, distribution, remote monitoring and control, and project management. Erv's primary responsibilities include resolution of technical issues associated with IEA and customer owned generating assets as well as engineering and project management associated with major upgrades and new installations. Erv holds a BS in Electrical Engineering from Iowa State University and is a licensed Professional Engineer*

In simpler terms, a risk management consultant researches ideas and plans that a company has come up with that involve spending large amounts of money and/or resources to find out if the return on that investment would be worth it, and if the project is liable to pan out in their favour or not. It involves a large amount of research, planning, analysis and informed predictions on how the future financial market will play out in accordance with the specific type of industry the company is involved with.

Risk managers coordinate loss control systems for companies and organizations. This includes disaster recovery plans; emergency evacuations; purchasing of insurance programs; managing claims and loss control activities; managing relationships with third-party service providers including brokers and insurers; preparing loss analyses and budgets; and identifying exposed areas, recommending solutions, implementing approved programs, promoting loss prevention, updating and monitoring compliance with insurance necessities and managing safety and risk management manuals.

This position is solely focused on strategizing and planning in order to protect the assets of companies and organizations.

In order to be a successful consultant, one must have the following skills: a good understanding of business administration, retail sales and marketing; technical knowledge of the insurance industry; excellent communication skills; attention to details; ability to pivot and multi-task; project management skills; be able to gather analytics then write reports summarizing the details; an ability to be outgoing and self-motivated.

Many times they may have a specialty field with specific knowledge of a certain industry that will help them match up with companies who fall into these industries. Some of these industries include, but are not limited to: chemical manufacturing, mechanical engineering, civil engineering, manufacturing, environmental science, medical devices, information technology, and the pharmaceutical sector.

Along with having a bachelor's or master's degree in accounting, auditing or compliance and finance, earning a Certified Risk Manager (CRM) designation is an important step in becoming recognized as a specialist in risk management. The CRM is a professional designation for those working in risk management and fields such as financial, insurance, legal, accounting, claims specialist, and loss control. The CRM is earned by completing five courses, each two-and-a-half days, followed by completion of a 2-hour exam required for each course to earn the designation.

After the CRM is earned, there is an annual two-and-a-half day course completion necessary to maintain the designation. Some higher-level risk managers also have earned a CPA, or certified public accountant, designation as well.

There is also a professional development group dedicated to this field.

SRMC, The Society of Risk Management Consultants, is an international organization of professionals who work in the fields of risk management, insurance and employee benefits consulting. The goal is to advance these fields to benefit the practitioners, their clients, and the general public. This type of organization dates back to the early 1960s, showing that this field has been a valid business entity for many decades.



# COMPACT WITHOUT COMPROMISE

When you need Full-HD performance but require a discrete, compact size, the Panasonic SW-158 and SF-138 mini-dome cameras are the perfect solution. Offering a versatile design without compromising Panasonic's renowned picture quality, these cameras will deliver in the most testing environments.



WV-SW158



WV-SF138

## COMPACT MINI-DOME CAMERAS

- Full-HD 1080p images up to 30 fps
- 3.1 Megapixels high sensitivity MOS sensor
- SDXC/SDHC/SD Memory card slot
- Built-in Microphone
- VIQS Technology

## VIQS TECHNOLOGY: VARIABLE IMAGE QUALITY ON SPECIFIED AREA

### VIQS Technology

VIQS technology delivers Full-HD performance, requiring less bandwidth and smaller data storage capacities than conventional cameras. VIQS cameras allow you to vary the compression rate and image quality, so you can record important areas in Full-HD and all other areas at a lower resolution.



Panasonic New Zealand Limited  
18 Sir Woolf Fisher Drive, Highbrook  
East Tamaki, Auckland 2013, New Zealand  
Telephone: 09 272 0100, Facsimile: 09 272 0134

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

**Panasonic**<sup>®</sup>

# Risk = Chance x Effect, but how to calculate this safely?

A definition of the kind of risks and how to value them.

In a next article the base and structure for a solid security plan for (or against) risks will be described.

by Tom Boot

## Introduction

Quite often during the process of creating a total security system there are clear signs of linguistic or conceptual confusions about the notion of risks. In the worst case this becomes only clear after an incident, with all the thinkable consequences.

In many cases the internal party (the organisation itself) and the external parties (the intervening teams like the police, ambulance services and the fire brigade), do not have the same perceptions about the relevant risks, resulting in not optimal, nor efficient actions during a crisis.

You must construct a clear framework about the conception of risks, including how the phenomena risk can be effected by human emotions, all of which will be discussed in this article.



*About the author: Tom Boot has been working for 30 years in the field of total security for organisations such as Governments, Insurance Companies, Nuclear Installations, Banking and Consultancy Bureaus in Europe. He is now a New Zealand resident and lives in Auckland*

## Risks as a starting point

The construction of each safety and security plan has as its first step a profound inventory of all thinkable risks. This is also called a risk analysis. The next chronological step is to realise and maintain the appropriate risk constraining measurements and procedures. In other words, risk analysis should be the foundation of each security systematic.

No matter for what kind of risk, 100% security will never exist. Therefore the following stage must be the set up of a good emergency plan as well as forming a trained emergency team, which has to be provided with all the necessary equipment. This in order to secure as much as possible all the personal safety aspects during an incident.

If you principally ask why it is necessary to take security measurements within an organisation, it always brings you back to the one and only answer, namely to secure the continuity of that organisation. So, the last consequential part of a total security system is a continuity plan. A discussion of this plan has been published in the June-July issue of this magazine.

Resuming, the steps for a setup of a security system are chronologically as follows:

- Risk analysis
- Security measurements and procedures
- Disaster planning
- Continuity planning

The impact and scale of risks need to be determined as exact as possible for the creation of a safe environment. But that is often not as easy as it seems. Because,



during this process there will be a mixture of or a struggle between the quantitative risks, based on analytical judgements, qualitative risks, based on sentimental judgements. This is valid for all kind of imaginable risks, both material (e.g. fire or flooding) and non-material (e.g. negative publication or consequential damages), that may occur.

## Damage causing elements

In order to really handle risks and define the appropriate damage preventing measurements and procedures, you have to analyse all the relevant damage causing elements of each kind of risk. Otherwise, it is probable that wrong choices for prevention will be made.

Only by permanent, absolute and distinct realising against what damage causing elements protection or prevention is necessary, the right security measurements can be taken. This is not as complicated as it may seem, if you break down all the kinds of risks to this level, you only have to deal with the following seven elements:



# iCLASS SE<sup>®</sup>

## The smartest access control platform



**Next generation access control. An evolution in security, adaptability and performance.**



HID Global's technology and media-independent iCLASS SE<sup>®</sup> Platform is a secure identity solution for physical access and the widest range of converged applications and environments. For maximum interoperability, iCLASS SE<sup>®</sup> supports legacy and nearly all card technologies for cost effective, seamless upgrades to higher security and enhanced performance.

**To find out more download the iCLASS SE<sup>®</sup> whitepaper [hidglobal.com/iclass-se-platform-nzsec](http://hidglobal.com/iclass-se-platform-nzsec) or contact us at +61 3 9809 2892 or email at [asiasales@hidglobal.com](mailto:asiasales@hidglobal.com)**

© 2014 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, and the Chain Design are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission.

- Damage caused by theft or manipulation of information, goods and machineries
- Damage caused by a too high or too low temperature
- Damage caused by smoke
- Damage caused by water or humidity
- Damage caused by toxic or radioactive substances
- Damage caused by violence
- Damage caused by a too high mechanical stress on persons, machineries, goods and buildings

As an example, you do not want to protect against fire, but against the damaging elements caused by fire, such as too high a temperature, smoke, humidity, water, toxic substances or too high a mechanical stress. Therefore, from that starting point effective prevention measurements can be worked out.

### Causes of damage

The possible causes of all imaginable unwanted situations (the effect of a damage causing element) can be defined to three main causes:

- Deliberate and accidental human action
- Technical failure
- Natural disaster

Both deliberate and accidental human action can cause the following unwanted situations:

- Theft or manipulation
- Destruction
- Injury

Technical failure can result in:

- Destruction
- Injury

Natural disaster can cause:

- Destruction
- Injury

Choosing for example for an access control system, a CCTV system or a burglar alarm is effective against unwanted human action, but has hardly anything at all to do with the other causes of damage. In other words, the damage causing elements are both dictating what you want to protect and giving the direction how to realise that in the best way. The causes of damage are more indicative of how things can happen.

### Measuring is knowing

The height or value of each kind of risk can be expressed as the result of multiplying the height of the chance by the height of the effect: Risk = Chance X Effect.

It is best to work here with the following two scales of four.

#### Value of Chance

- 1 = hardly ever happens
- 2 = small chance
- 3 = reasonable chance
- 4 = high chance

#### Value of Effect

- 1 = minor or small effect, negligible consequences for the organisation
- 2 = slight effect, some consequences for the organisation
- 3 = significant effect, huge consequences for the organisation
- 4 = extreme high effect, catastrophic consequences for the organisation

From a pure mathematical point of view, the risks with a value between 8 up to 16 are conspicuous, but this is a great mistake, due to the following two reasons.

Even when the level of prevention within a certain organisation is (far) too low, there will always be some sort of security measures, especially around the most vital parts, thus the business units that are of great importance for the continuity of that organisation.

This results in a reduction of the factor chance, even if this is far too low. In other words, using the scale of 1-4 in this systematic, the values between 12 and 16 will be extremely rare. The only way to get a reliable result here, is doing this measurement from the point of view of all the seven damage causing elements. So this is an important step back to the very elementary basis.

An essential next step is to have a serious thought about all the effects with a score of 3, resulting in significant consequences, and even more with 4, indicating that this will have catastrophic consequences for the organisation. For this last situation an extreme low chance (score of 1) is the only allowable value, but it most certainly does not indicate that there is no serious risk. For all these situations a separate and more profound examination is a must.

In other words, the method described above is a useful practical tool, but it does not mean that the extent of risks can be determined just and only by a method like this. Also because it has become quite clear over the past years that our perception about reality, and therefore also about the way risks might occur, can be quite limited. That is why for all the vital elements of an organisation the only starting point must be: "expect the unexpected!"

### Risk versus threat

Public Authorities often use the system Design-Basis Threat (DBT), thereto suggesting that this is the same as handling risks. Of course the level of certain threats can also be an important factor for a security system. But threat is something different than risk. Threats are less static and can be more or less temporary. DBT is for example very useful for upgrading or downgrading the level of awareness of governmental forces like police or army.

Risks are usually less temporary, although the level of risks can change due to a variation of internal and external factors.

Yes, threat does have some similarity with chance. These two terms both have something to do with probability, but it is certainly not the same. And threat is absolutely not the same as risk, where chance is only one of the two factors. So the threat or an unwanted occasion can be low, but the risk, due to unacceptable effects, very high.

### Qualitative and quantitative elements of risks

Here above are addressed the damage causing elements and the causes of damage in relation to the quantitative value of risks. But another important aspect for defining risks are the qualitative aspects, like the (assumed) manageability of the exposure to a certain risk, the familiarity with a certain risk or for example the social benefit.

Most certainly all the relevant qualitative risks must be considered during the construction of a security plan. Even if a reliable calculation that shows that a quantitative risk is very likely controllable, can the qualitative perception of that same risk result in such a tarnishing of the image, that the continuity of the organisation is in danger. Public opinion or political pressure can result that from a good controllable and explainable unwanted event, a new threatening situation arises and everything can get out of control.

Another example of qualitative effects is that in the first place reasonable security measures are not regarded as an issue. But often after an event, due to over reacting, security measures are often acted out as one big overkill. This is a well known area of tension between the qualitative and the quantitative judgment of risks.

The quantitative elements of risks will always be better controllable than the qualitative ones.



**Loktronic**

SECURITY • TECHNOLOGY • RELIABILITY

# *your* electromagnetic locking specialist!

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

**Standard features include:**

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

**Options include:**

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

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

**10**  
YEAR  
GUARANTEE



**Loktronic**

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



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

# WD launches expansion of NAS storage product ranges

WD (Western Digital), a world leader in storage solutions, invited a large number of guests to a special product launch at Sky City recently to announce the expansion of its award-winning WD Red and Red Pro lines of SATA hard drives

These NAS (network attached storage) systems featured the release of 5 TB and first-to-market 6 TB capacity for NAS-specific storage along with the introduction of WD Red Pro hard drives that address the medium to large business NAS market. Compatibility-tested with top NAS system manufacturers and optimised for power and performance, WD Red 3.5-inch hard drives are now shipping in 1 TB to 6 TB capacities; and the new WD Red Pro 3.5-inch hard drives are available in 2 TB to 4 TB capacities.

## WD Power of choice

One of the key points noted by the audience on the night was that WD has segmented its storage line-up into easy to recognise colours that give customers the



*Presenter Darrin Bulik explains how colours give you the power*

power to differentiate storage solutions and choose the right product for their needs. WD Blue is for everyday use; WD Green for capacity; WD Black for performance; WD Red (and Red Pro) specifically for network attached storage (NAS); and last but by no means least for those in the security sector, WD Purple for surveillance. Alongside the family of colours Western Digital has targeted its enterprise level market with the WD Se WD Re and the WD Xe. WD says it aims to offer more than a one-size-fits-all storage solution.

On hand from the USA to present the new products was Darrin Bulik, director of marketing at WD for NAS and digital

video products. He noted that, “With the expansion and evolution of the WD Red family, WD once again is providing loyal customers with increased capacity up to 6 TB; improved bay count support with up to eight bays; increased product breadth with WD Red Pro; and more features with the latest generation of NASware technology.

## WD Red

A storage industry innovation first introduced in 2012, WD Red hard drives address the unique environment of NAS and the growing demand for affordable, reliable and compatible storage that reduces customer total cost of ownership.





**Your security,  
our storage.  
The power of choice.**

## Marc Cisneros

Protector,  
Advocate,  
Guardian.

362,512 hours recorded,  
15,643 cameras strong,  
7,453 sequences stored,  
2,423 businesses secured,  
1,512 clients protected,  
**1** surveillance solution.



**WD Purple™**  
Surveillance Storage

See more of Marc's solutions at:  
[wd.com/choice](http://wd.com/choice)

**WD**  
absolutely™



Darrin said, "With the release of 5 and 6 TB models, the Red line has been further enriched with greater storage capacity and increased performance with NASware 3.0, an enhanced version of WD's original NASware technology, designed to improve reliability and system performance, reduce customer downtime and to simplify the integration process."

WD Red hard drives also feature 3D Active Balance Plus, an enhanced balance control technology, which significantly improves overall drive performance and reliability. Exclusive for WD Red customers, WD offers free premium 24x7 dedicated support.

By increasing NASware 3.0 capability, the WD Red 1 to 6 TB capacity drives are capable of supporting up to eight bay NAS systems with no negative impact to performance.

### WD Red Pro

Darrin said the new WD Red Pro line was ideal for medium to large business environments supporting 6 to 16 bay NAS systems. "The enhanced design offers reliable, high performance storage powered by NASware 3.0. By introducing the WD Red Pro, WD now has a full portfolio NAS storage solution with the WD Red family (WD Red and WD Red Pro) for both consumer and business NAS solutions."

### WD Purple

While not a highlight of the product launch on the night, the Purple range is the one most readers of this publication will be interested in. It offers exclusive AllFrame technology offering premium reliability and peace-of-mind when installing home or small to medium business security systems.

WD Purple's exclusive firmware upgrades work with ATA streaming to reduce error pixilation and video interruptions



*There was an excellent attendance at the event with people eager to learn more about WD's new releases*

that occur when desktop hard drives are incorrectly used as storage in security systems. The WD Purple surveillance storage range is built for 24/7, always-on, high-definition surveillance security systems that use up to eight hard drives and up to 32 cameras.

WD Purple surveillance-class storage has also been tested to be compatible in a wide-range of security systems. These drives are designed to replace standard desktop drives that were not designed for the harsh 24/7 always-on, high-definition surveillance environment. Desktop drives are built to run for only short intervals and are not engineered to withstand high-temperature fluctuations and equipment vibrations found in a typical surveillance application.

These hard drives reduce frame loss, improve playback and increase the number of drive bays supported.

AllFrame reduces video interruptions that commonly occur when desktop hard drives are incorrectly used as storage in security systems. Missed frames and lost footage is a serious problem when an event occurs and surveillance footage needs to be retrieved. WD Purple with AllFrame provides the confidence users expect when it's time to play back and review critical surveillance footage.

### Key benefits:

- Reduces video frame loss with surveillance-class storage.
- Specifically tuned for surveillance security systems.
- Caching algorithms are tuned for write-intensive, low bit rate, high stream count applications that are typical of surveillance applications.
- Priority change for write allocations and pre-emptive caching policies.
- TLER & ATA streaming support.
- Supports up to eight drives.

WD Purple surveillance hard drives are also built for compatibility with industry-leading chassis and chip set manufacturers for seamless integration into your new or existing video surveillance system.

Low power consumption is crucial in high-temperature always-on surveillance environments. With its exclusive IntelliSeek technology, WD Purple drives calculate the optimum seek speeds which lowers power consumption, noise and vibration that can damage and cause desktop drives to wear out more quickly.

WD Purple hard drives are optimised to support up to 32 high-definition surveillance cameras, giving you the flexibility to upgrade and expand your security system in the future. It has a three year limited warranty (worldwide).

For additional surveillance capacity, look at WD data-centre hard drives. Neither is WD Purple recommended for use in NAS environments, where users should consider using WD Red hard drives for desktop RAID and NAS environments or WD data-centre hard drives for rack-mount or large RAID configurations.

**For more information about WD products go to [www.wdc.com](http://www.wdc.com) or contact the New Zealand distributor: VST (NZ) Ltd on phone 09 444 8448 or email: [sales@vst.co.nz](mailto:sales@vst.co.nz) or visit: [www.vst.co.nz](http://www.vst.co.nz)**



*During the WD product launch paying attention really paid off for this participant with correct answers to a tricky question he won a significant prize. The winner was Clint Francis from Think Concepts Ltd (2nd from left.) The other people in the photo (L-R) Eric Chan WD, Ricky Leung VST, Darrin Bulik WD.*



# Unlicensed security company fined

A security company has to pay \$12,600 after it was convicted in the Auckland District Court today for operating without a licence.

Corporate Protection and Security International Limited (CPSI), of Sunnyvale, Auckland, pleaded not guilty to seven charges under the Private Security Personnel and Private Investigators Act. Judge David Wilson fined the company \$1,500 and costs of \$300 on each charge.

Sean Michaels, also known as Seu Illai Taleni, 51 of Massey, was acquitted on a charge of not holding a certificate of approval (COA). The court found that on the day he had allegedly breached the Act he had not received a letter informing him that his certificate had been suspended by the Private Security Personnel Licensing Authority.

Internal Affairs told the court that Mr Michaels was the face of CPSI which supplied security services to the public. The staff he employed were often non New Zealand residents, typically visitors to the country on short-term visas.



*Maarten Quivoo, General Manager,  
Internal Affairs Regulatory Services*

Mr Michaels did not obtain a licence for the company but held a COA until it was suspended on 2 May 2013. He maintained that he and his company were half owners of another licensed security company under whose umbrella he and his staff worked. An agreement to buy Stankovich Security and its licence was finalised in November 2013 – after CPSI's offending.

The company, which has the right to appeal the decision, provided security and crowd control for events and premises between April and August 2013, including Wellington Fashion Week, an Auckland Showgrounds' function, an Auckland hostel and a bar.

Internal Affairs General Manager Regulatory Services, Maarten Quivoo, said today's convictions are a warning that the security industry must take licensing seriously.

"Trained, licensed private security personnel help New Zealanders to be safer at work and in their homes, and to participate in social and recreational events safely. The requirement for a licence is there to reassure the public that people working in these industries can be trusted by those businesses and by the public who need to rely on them."

August - September 2014



## QUALITY DOOR SECURITY FOR EVERY APPLICATION



AIPHONE provides a wide range of reliable and easy to install intercom systems all with a three year warranty.

Talk to your local AIPHONE supplier about the best solution for your intercom application.

Available from...

**ZoneTechnology**  
Your Security Supply Partner

Auckland  
Unit 6, 25 Airborne Road, Albany  
Wellington  
35 Abel Smith Street, Te Aro  
Christchurch  
Office 13, Level 2, 225 High St

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

**NFS**  
NATIONAL FIRE & SECURITY

Auckland  
1/44 Greenpark Road,  
Penrose

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

# Rights and responsibilities: Good citizenship is needed in the struggle for BYOD security

Bring your own device, or BYOD, has come to define the post-work/life balance era of the early 21st century. For employers it promises higher productivity, agility and lower costs. For employees, it promises the freedom of being unchained from a desktop and to engage in the odd bit of social media on work time.

Essentially, BYOD is the use of personal equipment - usually phones, tablets and laptops - on a company network. It's a fantastic idea, and in years to come we'll wonder how we ever got by without it. But for some time now, the IT security world has been telling us that BYOD has left companies' security perimeters vulnerable to (i) an unprecedented array of attacks from the outside; and (ii) all manner of data loss from the inside.

For both employers and employees, BYOD seems to represent an uncomfortable blurring of the professional and personal. And with everyone focused on all the benefits of BYOD and mutually avoiding how to deal with the setting of professional/personal boundaries, nobody seems too bothered about the security threats.

## **Businesses free-riding the BYOD wave**

In terms of advantages to business, New Zealand ICT outfit Gen-i notes that BYOD creates a more flexible IT environment; supports recruitment and talent retention; streamlines operations and a more agile, sustainable business; increases productivity potential; reduces hardware costs; decreases mobile data charges with the use of Wi-Fi; saves on software as work moves to the cloud; and reduces property overheads as people move to remote working and hot-desking.

It's an impressive list of credits, but with the rewards come the risks. With all the vulnerabilities associated with BYOD, are businesses adequately investing in the security of their networks or have they been merely free-riding on the BYOD wave?

The Information Security Community on LinkedIn and Vectra Networks, a provider of real-time detection of in-progress cyber-attacks, recently announced the results of their second annual BYOD & Mobile Security Study. The study surveyed more than 1,100 IT security practitioners to provide insights into the state of BYOD and mobile security in 2014.

According to the study, about half of respondents agreed that users bringing downloaded apps or content with embedded security exploits into their organisation, and malware infections, were the top BYOD security concerns. 60% of respondents identified malware protection as a key requirement for mobile security. So far so good, but that seems to be where the good news ends.

Alarming, responses indicated that only 21% of businesses had fully implemented BYOD policies, processes and infrastructure, and 24% had no mobile device policy at all! 21% of respondents stated that privately owned devices were widely in use within their organisations but were not supported.



Businesses, it seems, are keen to derive the cost savings of having employees doing their work on their own devices rather than on employer-provided computers, but they're not willing to fork out for the cost of securing against the threats these personal devices may be playing host to.

With BYOD touted as a budget saver, too few have stopped to squint at the fine print. As a Blackberry report on the hidden costs of BYOD states, "while it's nearly impossible to put a price tag on the loss of IP, leakage of tightly-held secrets to a competitor could have catastrophic ramifications." And security breaches are not the only area of potential cost, with monthly voice and data, management complexity and potential legal expenses and reputational costs all suggesting the need for a more sober assessment of the savings to be made.

## **Employees: little care and no responsibility**

If businesses aren't taking BYOD threats seriously, it seems that employees are taking them even less seriously. In many cases employees are resistant to company BYOD policies and think nothing of ignoring them.

Despite the rise in the use of personal devices for business use, US consumers are showing scant concern for security when it comes to BYOD. According to a recent study by Gartner, a quarter of business users admitted to having had a security issue with their private device in 2013, but only 27% of them felt obliged to report it to their employer!

Interestingly it also noted that almost three quarters of respondents who regularly use their private devices for work had not yet signed a formal agreement with their employer.

According to Dell's Securing the enterprise workspace whitepaper, employee resistance to corporate security policies is part of the problem. "If employees feel that security policies impede productivity or could encroach on their personal data", states the report, "they might circumvent those policies." Users don't want their company IT people accessing their personal social media posts or accidentally deleting personal photos stored on a device.



And it seems that attitudes towards BYOD security haven't changed, with the results of Fortinet's 2012 still ringing true. 42% of this survey sample actually believed potential data loss and exposure to malicious IT threats to be the dominant risk, yet this didn't prevent many of them bypassing corporate policies. In fact, more than a third of respondents (36%) admitted they have - or would - contravene a corporate policy banning the use of personally-owned devices for work purposes.

Ultimately, people want to bring their personal devices to work and to use them for work, but they don't want work dictating how this is done. According to the Fortinet survey, the overwhelming majority of respondents consider themselves – not the company – to be responsible for the security of the personal devices they use for work purposes. And with employers tending to prefer a hands-off approach to BYOD security, everyone seems to have been kept happy. In this laissez-faire environment, it's been a free-for-all for malware, APTs and other nasties.

### Learning from the kids

The New Zealand school system has been at the forefront of BYOD uptake. Seeing obvious educational benefits to networked studies, many schools have been ahead of the curve. While inevitable controversy has surrounded the move, it appears that personal devices are fast becoming as ubiquitous as lunchboxes on school grounds.

What is striking about BYOD in schools is that schools have their own BYOD policies - without fail. Some of the policies are more comprehensive than others, but at the end of the day policies are in place that set behavioural requirements around how personal devices may be used in the school context.

As in the corporate world, schools place the responsibility for the security of personal devices on the user, but unlike employers, schools have strict parameters around how devices are used and when... and they enforce them!

At the Westlake school, for instance, "devices can only be used in the classroom for work as directed by the teacher: if a device is misused in any way, a teacher has the right to confiscate it." According to the Torbay School's mobile device user agreement, devices are "not to be used before and after school, morning tea and lunchtime" and are to be "locked in a cupboard" during these times. At Carmel College, inappropriate use of a device can result in "lunchtime detention".

Schools, it appears, are setting high standards when it comes to general behaviours around mobile devices, school versus personal use, and awareness in relation to online safety and security. They may not be complex, but clear boundaries dictate the use of personal devices and a culture of compliance and digital citizenship is nurtured from the start.

### Balancing risk and reward

There's still a generation before today's primary schoolers get jobs and infiltrate New Zealand's workplaces with a healthy respect for mobile security and the boundaries around appropriate use. In the meantime, employers will need to take a more active role in defining and enforcing BYOD rights and responsibilities, and all indicators are pointing to the need to take more of a 'headmaster' approach.

There are plenty of online resources and tools available for employers to learn more about BYOD security and how to develop policies. Auckland-based Optimus Systems provides a sample pdf BYOD policy template via its website, and there are many others.

Taking responsibility for the risks of BYOD will maximise the abundant rewards that mobile technology has to offer.

**FOR MOBILE  
CCTV SECURITY  
WHERE & WHEN  
YOU NEED IT**



# NZTRAILERCAMS



**Set-up in under 20 minutes**  
TrailerCam is a cost effective security surveillance solution with a complete record of incidents and real time alerts.

Giving you pinpoint CCTV coverage and recording with secure remote login and remote camera capability that can be monitored from anywhere in the world that has internet access.

This solar powered mobile surveillance unit is ideal for:

- Incident Management
- Disaster Recovery Monitoring
- Business Continuity Management
- Monitoring of Regulatory Enforcement
- Supplementing Static Guards and Patrols
- Traffic Monitoring
- Event and Crowd Security
- Monitoring Construction Sites

Equipped with motion detection, email and SMS intrusion notification this is a powerful, tailor-made mobile security solution.







**[nztrailercams.co.nz](http://nztrailercams.co.nz)**  
or call 0800 287 245

# Technology needed to neutralize BYOD threats

An interview with Bryce Boland, CTO Asia Pacific for FireEye, Inc.

Founded in 2004, cyber security company FireEye appears to have done a lot in a short time. In May, Forbes reported that shares in the company were up a staggering 379% from its September 2013 IPO price, making it the second-best performing company of all the firms to go public in the U.S. last year.

The company must certainly be doing something right, so we thought we'd approach them to seek their thoughts on BYOD security, and Bryce Boland, FireEye's CTO Asia Pacific, obliged.

Prior to joining FireEye, Bryce was the Security CTO for UBS, responsible for group-wide security strategy, architecture, and driving security requirements into technology development. Prior to this, he worked for ABN AMRO as a technology risk management consultant. Before embarking on his 16-year career as an information security professional, Bryce received his BSc. (Honors) and M.Sc. from Auckland University.

**NZSM:** A recent Webroot survey indicated that 34% of IT managers disagree that gains in employee productivity from using personal devices for work outweigh the risks associated with this activity. 95% of employees are also concerned about BYOD risks. Are these concerns justified?

**BB:** Both employers and employees should be concerned about the threats to their mobile device. Most mobile devices are inherently less secure than enterprise controlled PCs as they have fewer controls and are constantly connected to the Internet. Many users run out-of-date software with widely exploitable vulnerabilities on their mobile phones.

This is particularly true for Android devices, where they are dependent on their handset manufacturer to release updates.

Worse still, users have almost no way of knowing what any app they download



*Bryce Boland is the CTO Asia Pacific for FireEye, Inc.*

might do – and criminal attackers are increasingly targeting mobile devices for their money making schemes. For employers, there are real business risks in allowing devices outside of your control to access your sensitive corporate information – risks that can damage your business reputation, your operations, or even result in the theft of business secrets that reduce your profitability.

**NZSM:** It's not like BYOD arrived yesterday... has the industry been slow to provide adequate products to address BYOD risks?

**BB:** The challenge is that the market is largely driven by consumer forces that favour cost and convenience over security. As the drive for enterprise-suitable security features grows, we will see more development effort towards this. Recently Samsung and Apple have made moves to

provide more enterprise-grade software and security features, but this hasn't trickled down yet to the devices users buy today. The other area of concern is app security – and this is where companies like FireEye are leading the way with new technology to analyse the behaviour of apps to identify malicious behaviours, vulnerabilities, and data leakage.

**NZSM:** Are companies/employers doing enough to put firm BYOD protocols and policies in place?

**BB:** Policy is not enough to change users' behaviour; you need technology to enforce the policy through security controls. Most organisations don't have good controls in place today to stop data loss or insecure access to their networks via BYOD.

**NZSM:** What, in your opinion, are the major threats posed by/to BYOD?

**BB:** The primary threat is from the theft of corporate data that is stored on the mobile device. Secondary threats include stealing credentials (usernames, passwords, two-factor authentication token seeds, certificates), which are on the phone for use in attacking the corporate network directly, and loss of sensitive personal data which can be used in identity theft and impersonation attacks.

**NZSM:** What do you recommend in terms of addressing BYOD threats?

**BB:** Companies are best to limit the amount and types of data which can be stored on the BYOD device, put in place controls to limit the impact of a lost or stolen device, and implement technology which validates the behaviour of installed apps to prevent malicious apps from taking advantage of the data and access the mobile device provides.



# The right combination to simple access control – the new Briton 9360

Allegion, a global leader in security and safety technology, further pioneers with the new Briton 9360 Electronic Push Button Lock

The Briton 9360 pushes the boundaries of regular push button locks, with its electronic functionality. The battery powered lock allows up to 80 user codes of four to six digits. The unit doesn't require removal to change access combinations and codes can be added easily for increased security. In addition, the system allows up to ten 'one time' user codes and a key override as standard which ensures a prompt and non-invasive emergency opening.

Easy to install and retrofit to existing door preparations, the 9360 is a simple solution to upgrading an existing system and, due to its flexibility and adaptability, can be used in many applications such as retail stores and schools through to hospitals and commercial facilities.

Available in either tubular latch (Briton 9360) or mortice lock (Briton 9365), the locks can be fitted on timber or metal doors between 35mm and 65mm. Two remote connections can be wired to activate the lock from a reception desk, an intercom or remotely in an emergency.

The satin chrome finish is stylish, weather and dust resistant, and easy to maintain, making it suitable for internal and external use. The 10 year comprehensive warranty ensures confidence now and in the future.



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

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

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



**ALLEGION**

# Connectivity and Convergence at GIL 2014 New Zealand

With a market potential of USD\$731 billion in connected living by 2020

Massive technology-led disruption across all industries globally, driven by the rapid proliferation of connected devices and services is moving everyone and everything towards a state of 'connected everything'. Connected devices will continue to proliferate in every aspect of life with an average digital native of at least 10 personal connected devices at home and access to over 80 billion devices. It is expected that by the time we are into the 2020's, tens of millions of people will be connected by trillions of things and applications as a result of connected industries.

'Connected Living' is defined as a world in which consumers use many different devices to experience compelling new services that integrate video, voice, and data services to provide access and ubiquitous connectivity anytime and anywhere. In the future, smart and connected everyday objects and appliances will be able to monitor the environment, report statuses, receive instructions, and take action based on the information received from PCs, smartphones, and tablets.

This evolution has progressed since the 1970's, that had specialised activities driven by proprietary equipment and mainframes, then increased productivity in the 1990's propelled by the advent of PC's and the internet, followed by bursts of disruption and innovation in 2010 onwards through cloud and mobility.



*Mark Dougan, Managing Director,  
Australia & New Zealand, Frost & Sullivan*

Mark Dougan, Managing Director, Australia & New Zealand, Frost & Sullivan says, "Mobility and cloud computing have brought about significant changes in the ICT industry. Cloud computing, big data, mobility and low cost sensors are driving the internet of things and connected industries. The internet of things is forcing transformation and innovation across connectivity and convergence of people and industries, giving rise to the connected home, connected workplace and connected city. The consumerisation of the information and communication technologies (ICT) environment is forcing companies to converge and offer ICT-blended solutions. This is creating a whole new market of connected living solutions and services."

To understand the development and growth of the 'connected living' market Frost and Sullivan looks at the micro market level for the new products and services that are being taken up by consumers in the context of where we spend most of our time - at home, at work and out and about in the 'city'.

Frost & Sullivan forecasts the total connected living market to reach \$731.70 billion by 2020 as the importance of the internet and digital solutions grows in the overall economy. Connected city, comprising eGovernance, eCitizens, smart transportation cards, e-learning, mobile banking and digital classrooms, remote education services as well as digital libraries will contribute the largest percentage at 54%, equating to an estimated market potential of \$392.94 billion, with smart governance and education services making up 50% of growth in this segment.

Dougan says, "Connected cities will be driven by connected consumer services for mobility, governance, education, and banking and financial services. Data is the essential game changer and eServices such as ePayments, eExchange, eSharing, etc, will empower citizens with real-time access to personal data and related services. Smart governance and education services will transform access to information

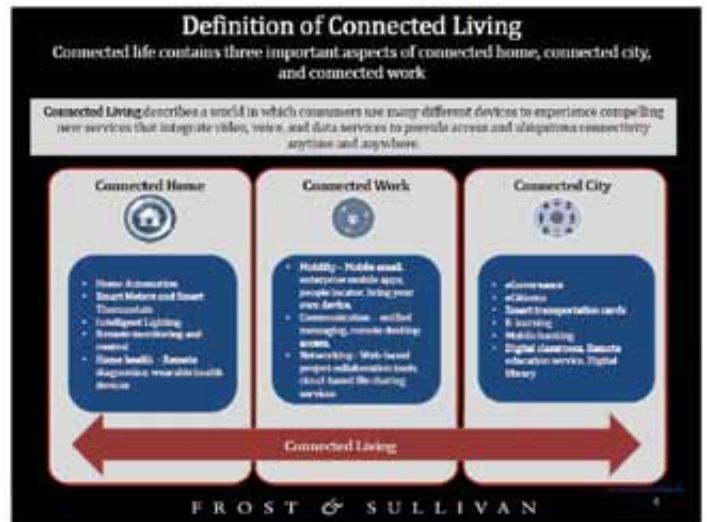
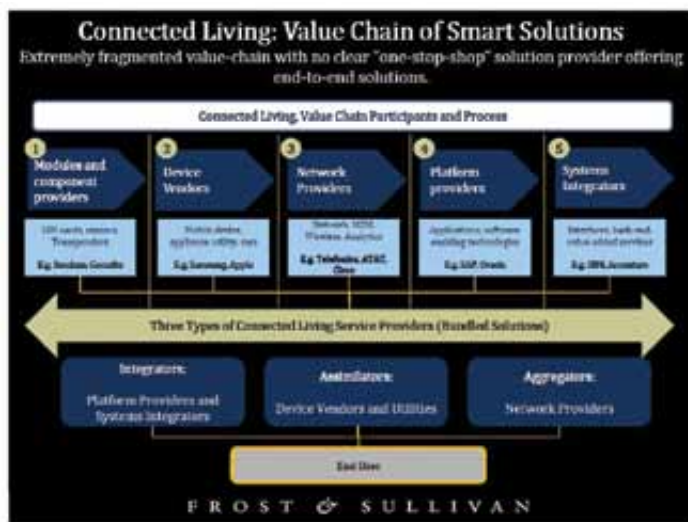
and learning. More than 60% of citizens of smart cities will have full access to eServices in the next 10 years."

Connected work comprises 31%, contributing \$228.44 billion. Connected work encompasses mobility (Mobile email, enterprise mobile apps, people locator, bring your own device), communication (unified messaging, remote desktop access) and networking (web-based project collaboration tools, cloud-based file sharing services). Connected work solutions (communication platforms, enterprise mobility applications, social media tools) will offer alternate working styles through fully integrated, software-focused architectures. More mobility solutions will eliminate the need for physical space through technologies such as augmented reality and virtual holograms. Instant language translation, virtual reality interaction and shared platforms will truly enable decentralised operations.

"Connected workplace technologies such as cloud computing, telepresence and simultaneous speech translation will flatten the structure of global companies and enable workers to connect with each other and share information in real time any place anytime. Already, IBM's SmartCloud is a virtual business with key processes taking place in the cloud. The leveling of the global playing field for talent will widen the traditional growths and these new connections will drive significant change. Productivity will rise as organisations become more global and collaborative, adopting a 'zero' approach to management, hierarchy, leave and working hours," states Dougan.

Connected home competes the remaining 15% at \$111 billion and incorporates home automation; smart meters and smart thermostats, intelligent lighting, remote monitoring and control as well as home health i.e., remote diagnostics and wearable health devices. Connected homes will be controlled through smartphones or wearable technology and monitored through a web of sensors, devices and intelligent infrastructure such as smart lighting, virtual touchscreen windows,





energy management systems and remote home health services. Power, heating and light will be automated and supplied based on movement and need. Security systems will be controlled through highly intelligent technologies such as voice, face or fingerprint recognition.

Frost & Sullivan predicts that by 2025, the rise of connected living will see 3.7 billion smartphones, 700 million tablets, 520 million wearable health-related devices and 410 million smart appliances in the connected person world. The connected worker world will see 90 million IP Telephones, 400 million laptops and over 60 million unified communication platforms. “Frost & Sullivan expects that nearly 80% of US enterprises will adopt BYOD, 30% of populations will access office networks remotely, and 90% of organisations will offer mobility to workers,” remarks Dougan.

Meanwhile, the connected citizen will have access to 15 million interactive kiosks enabled by 25 million cloud

servers servicing around 1 billion smart government and ID cards. Around 500 million smart transportation cards and 50 million contact-less payment cards will be issued and an estimated 35 billion subscribed location based services (LBS) devices by 2020.

Dougan elaborates, “The value chain of smart solutions to service all the components of connected living is extremely fragmented with no clear ‘one stop shop’ solution provider providing end-to-end solutions. There are many players, ranging from module/component providers to device vendors to network and platform providers to system integrators. Within these groups are big name players such as Sendum, Gemalto, Apple, Samsung, Telefonica, AT & T, Cisco, SAP, Oracle, IBM and Accenture. Early entrants are exploring ways to monetise opportunities in connected living. First movers in the market are taking one of three approaches, a single purpose solution, a partnership alliance or

a broad platform based offer. Partnership alliances are being formed between different providers.”

A key factor in the development of the connected living market is the ability to combine hardware and software so that new products and services can be offered. The current and future in the connected living market could be exploited by companies in two ways: by creating new opportunity or by capturing market share from others. A key dynamic is the wide opportunity this market represents to non-conventional companies.

“While the ecosystem of players is complex, there is no denying that collectively, the market potential is huge and presents immense opportunities. Manufacturers will drive value from smart factories, retailers will derive value from digital retailing and advertising, utilities will derive value from smart grids. This is truly a market where being successful means often transformative improvement and legacy means almost nothing; the number of new market entrants is expected to be significant,” finishes Dougan.

Mark Dougan presents these visionary insights showcasing the impact of these new Mega Trends as well as highlighting case studies of companies and a roadmap of global opportunities to 2020 in his GIL Exclusive session on Connected Living at GIL 2014 New Zealand (<http://gil-events.gilcommunity.com/events/new-zealand/agenda/>) at Villa Maria, Auckland on 28th August, 2014. To enquire or register, please email [djeremiah@frost.com](mailto:djeremiah@frost.com) directly with your full name, designation and company details.

Globally Frost & Sullivan conducts the Growth, Innovation & Leadership Congress (GIL) across more than 15 countries. More information about our global community is found here: <http://gil-events.gilcommunity.com>.

## Connectivity and Convergence Will Transform Visionary Innovation Perspective of New Zealand's Enterprises

Frost & Sullivan's Growth, Innovation and Leadership (GIL) Community of business leaders will convene at Villa Maria Estate, Auckland to be a part of Frost & Sullivan's Flagship Event - GIL 2014: New Zealand on August 28, 2014.

Top level executives from all over New Zealand will gather to share ideas and strategies to make their business choices successful.

Mark Dougan, Managing Director Australia & New Zealand, Frost & Sullivan; will present an Exclusive on Connected Living; a visionary session which will showcase the impact of New Mega Trends by highlighting case studies of companies and a roadmap of the global opportunities to 2020.

Other highlights of the summit include Visionary Innovation Think Tanks, Panel discussions, Cover Stories of News in 2020 driven by market and technology Mega Trends. The congress will also recognize New Zealand's best through Frost & Sullivan's 2014 New Zealand Excellence Awards & Networking Luncheon.

For more information on GIL New Zealand, please visit: <http://gil-events.gilcommunity.com/events/new-zealand/agenda/>

For further details, please contact: Donna Jeremiah, Director - Corporate Communications, Asia Pacific. Email: [djeremiah@frost.com](mailto:djeremiah@frost.com) Phone: +61 02 8247 8927





**Frankie Stevens**

Frankie Stevens performed in the club circuit in New Zealand and Australia and then went on to England where he performed at Talk of the Town, The Albert Hall and the Palladium. Frankie has represented New Zealand and England in several European Song Contests.

In 1998 he was invited to join the New Zealand Millennium Office (NZMO) as their events coordinator for the upcoming millennium celebrations. Frankie has also owned and operated his own entertainment venue in Wellington performing nightly shows. Frankie was awarded the New Zealand Order of Merit in the New Year Honours list of 2004/2005, for services to entertainment.



**Nick Tuffley**

Nick Tuffley was appointed as ASB's Chief Economist in January 2007, having previously worked at Westpac and the Reserve Bank of New Zealand. Nick studied at Canterbury University, graduating with a Master of Commerce in Economics.

He and the rest of the economics team provide regular analysis of economic developments and the outlook through written publications and media comments. Their key objective is to help the bank's clients make better-informed business and personal finance decisions.



**Suzanne Mosefield**

Suzanne is a body mind analyst AIBMA (body language specialist), micro-expressions trainer, clinical hypnotherapist, counsellor, writer, presenter, trainer and executive coach. With more than 18 years' experience as an empowerment facilitator, she inspires authentic leadership worldwide.

Suzanne is the Body Language Analyst for TVNZ, Close Up, Breakfast TV, SKY TV (UK) and The Herald on Sunday and a feature writer in several magazines and co-author of #No.1 best-selling books. Her body language and stress management expertise is employed by many of today's leading companies as a speaker, trainer and analyst consultant to assist businesses maximise engagement, increase personal impact and generate core level success to help them gain the edge.



**Gillian Stewart**

Gillian is a Principal Policy Analyst at Auckland Council. She is a social impact specialist & community development practitioner with over 10 years' experience in political and strategic analysis, social policy development and research in New Zealand, UK and Southern Africa. Gillian has a doctorate in International Development from the University of Bristol (UK), and a Masters in African politics from the University of Cape Town.

She has two young children and a commercial fig and feljoa orchard to keep her busy outside of work. Gillian will present the findings of the council-facilitated 'Safer Auckland CCTV Project'. Your input into the development of the draft strategic action plan will be sought at the conference. This strategic action plan will not only set the council's policy on public places CCTV, but also outline the changes required across all stakeholders to improve the approach to CCTV and deliver safer Auckland communities.



**Claire Turnbull**

Claire Turnbull is one of New Zealand's leading nutritionists and has been inspiring others through her work in the health and wellness industry for over 10 years. Claire is director of a successful private practice, Mission Nutrition, and is the nutritionist for the Healthy Food Guide Magazine, Newstalk ZB and AUT Millennium Sport. She also regularly features on current affairs programs, the news, and has taken part in several TV shows. She is also the author of Penguin's best-selling book, Lose Weight For Life, and is currently writing her second book. Claire's passion is to help you be your best - the happiest and healthiest you! She believes you have to live it to give it and is all about helping people 'make healthy happen' in the real world!



**Greg Mann**

Greg was appointed by the Local Organising Committee (LOC) of the ICC Cricket World Cup 2015 in June 2013 to lead the planning and quality assurance aspects of security delivery for the NZ based fixtures including host cities, match venues, training grounds, official functions and team and VIP hotel accommodations.

His current role requires significant government and trans-Tasman agency relationship management as well as coordination and planning document development with security industry providers. Previously Greg held a similar position for the RWC 2011 LOC after many years in senior management positions in national security companies across NZ. Greg's background also includes transport logistics, police, leadership, human resources and financial management and he holds a Master of Business Administration degree.

## 2014 Conference Structure

### WEDNESDAY 27 AUGUST

7:00am	Industry Breakfast	S
	An Insight into the Current Economic Conditions	N
9:00am	Conference & Exhibition Opening	
9:30am	Leadership and Communication	R
10:30am	Tea Break	
11:00am	Achieving success in a security mandate, whilst also delivering value.	T
12:30pm	Lunch Break	
1:30pm	'Are you Poised for Success.. Or Positioned for Failure?'	S
3:00pm	Tea Break	
3:30pm	Annual Police/CPPF Update	P
4:15pm	Qualifications and Training	S
5:00 - 5:30pm	NZSA AGM (Financial Members Only)	
5:30 - 7:00pm	Drinks & Nibbles	



**Tyson Johnson**

Tyson Johnson is a risk management executive who has worked in government, global banking and global manufacturing sectors. He has led investigations in Mexico, Thailand, China, India and Malaysia, as well as throughout North America and Europe. As a former intelligence

officer, Johnson understands the need for strong information collection and analysis to support proactive risk management.

Learning how to develop a business case to achieve success in a security mandate, while also delivering value to the business (profit, loss reduction & recovery). Understanding how new technology can assist with situational awareness, fraud identification and all-threats risk management as an effective way to drive value - directing resources in a more efficient manner.



to police and government detective, federal crime honours degree, four o with International and authored two books - Region and Security Risk and produced an online



## THURSDAY 28 AUGUST

### Speakers

Nick Tuffley, ASB Economist

Rob Redenbach

Lyson Johnson

Luizanne Masefield

Police

Skills Organisation and NZSA Training

### Speakers

9:00am Security Management in the Asia Pacific Chris Cubbage

10:30am Tea Break

11:00am The Auckland City Camera Surveillance Project Gillian Stewart

11:45am CCTV - from light to pixels Vlado Damjanovski

12:30pm Lunch Break

1:30pm Improved Performance through better Nutrition Claire Turnbull

3:00pm Tea Break

3:30pm Update from the NZ Intelligence Community CLASSIFIED (closed to media)

4:15pm Security and the 2015 Cricket World Cup Greg Mann

7:00pm Pre-Dinner Drinks

7:30pm Awards Dinner

### Chris Cubbage

Chris Cubbage is Director and Executive Editor of My Security Media, publishers of the Asia Pacific Security Magazine, Australian Security Magazine and a range of online channels dealing with current and emerging technologies.

Chris is a contracted security adviser to government agencies, is a former homicide commission investigator and holds an Australian Diplomas and is certified and registered in Regional Security Professions. Chris has been a speaker at Corporate Security in the Asia Pacific & Management in Corporate Governance documentary - 11 Years After 9/11.



### Vlado Damjanovski

Vlado Damjanovski is an author, inventor, lecturer and closed circuit television (CCTV) expert who is well known within the Australian and international CCTV industry. Through his company he provides consultancy, design & project management, system-commission, product testing, desk-top

publishing and training.

In 1995 Vlado published his first technical reference book - simply called 'CCTV'. This was, and still is, one of the first and complete reference manuals on the subject of CCTV. Now in its 4th edition, and translated into four languages, Vlado's book continues to have a 5-star rating. The 2013 edition is titled 'CCTV - from light to pixels'.



### Rob Redenbach

Rob Redenbach blends humour and hard facts to deliver powerful and memorable learning experiences. Rob holds postgraduate qualifications in (counter)terrorism, safety and security from the Australian Graduate School of Policing.

A former member of the Australian Defence Force, Rob's practical experience includes managing a security company in Papua New Guinea, working with the bodyguard team of Nelson Mandela, teaching his own system of self-defence to the American FBI and British special forces and providing security services to aid-workers in Iraq and Afghanistan. Rob draws from a wealth of real-life experience to captivate, motivate and educate.

# Our focus is creating intelligent IP video solutions that fit your needs

At Bosch, we believe that everyone deserves to live in a safe and secure environment. Through our dedication to superior quality and technical innovation we push ourselves to develop new products and solutions that put us at the forefront of our industry.

Our approach is based on three pillars. Firstly, we provide the highest quality of relevant IP video images anytime, anywhere. Secondly, we guarantee the most efficient bit rate and lowest storage requirements. And thirdly, we deliver superior intelligence and analytics at the edge.

This leads to products and technologies that are simpler to understand, easier to install, more precise and better connected.

We gladly introduce some of our latest in-camera technologies. Each of them specifically designed to meet your needs and demands, because our focus is on creating relevant IP video solutions. Discover how your surveillance situation can benefit from these innovations.

## Bosch In-Camera Technologies

### intelligent Dynamic Noise Reduction (iDNR)

Our focus is to reduce storage costs and network strain without compromising video quality. Quiet scenes with little or no movement require a lower bitrate. By intelligently distinguishing between noise and relevant information, such as movement, intelligent Dynamic Noise Reduction (iDNR) reduces bitrate by up to 50%. And because noise is reduced at the source during image capture, the lower bitrate does not compromise video quality. With iDNR, our focus is to significantly reduce storage costs, and lessen network strain by only using bandwidth when needed.

### intelligent Auto Exposure (iAE)

Our focus is to provide you with perfect exposure every time. Fluctuations in backlight and front light can ruin your images. To achieve the perfect picture in every situation, intelligent Auto Exposure (iAE) automatically adjusts the exposure of the camera. It offers superb front light compensation and incredible backlight compensation by automatically adapting to changing light conditions. With iAE, our focus is to provide you with perfect exposure every time.

### intelligent Tracking (iTracking)

Our focus is never to lose track of objects of interest.

In video surveillance, moving objects are usually the most significant objects of interest. Intelligent Tracking (iTracking) automatically tracks moving

objects based on predefined alarm rules or a simple click. By intelligently distinguishing between single and multiple reference points, iTracking will provide uninterrupted tracking.





Optimal capture of the object of interest is assured by dynamically adjusting the field of view. With iTracking, our focus is never to lose track of objects of interest.



### Intelligent Video Analysis (IVA)

Our focus is to alert you when needed and help you quickly retrieve the correct data.

After only 20 minutes you can miss 90% of the activity on a screen. Intelligent Video Analysis (IVA) assists by alerting you when predefined alarms are triggered. By smartly combining up to 8 IVA rules, complex tasks are made easy and false alarms are reduced to a minimum.

IVA also adds sense and structure to your video by adding metadata. This enables you to quickly retrieve the relevant images from hours of stored video. Metadata can also be used to deliver irrefutable forensic evidence or to optimize business processes based on, for example, people counting or crowd density information. With IVA,



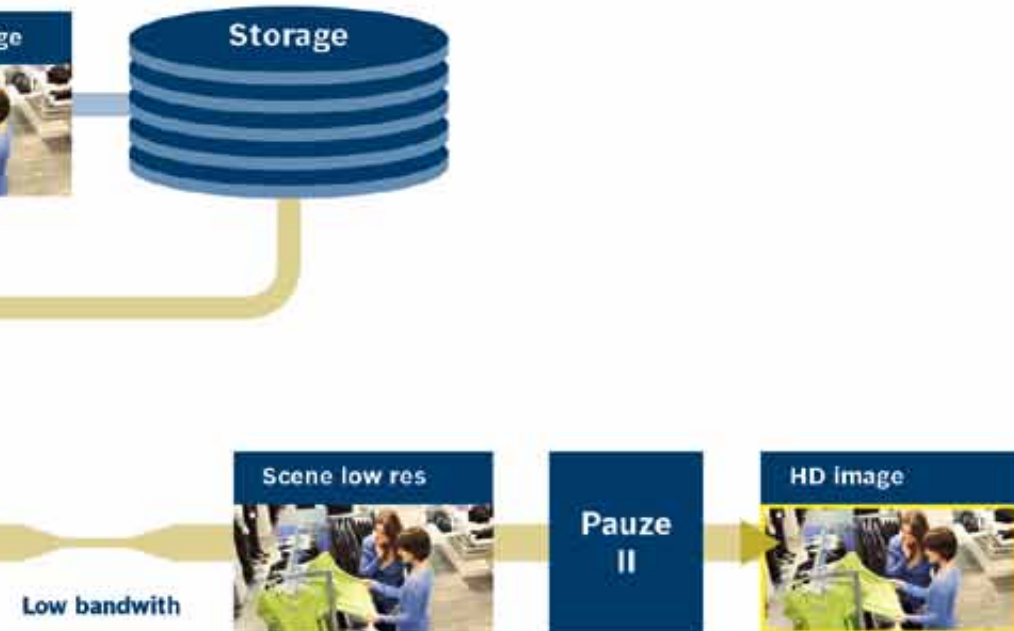
**BOSCH**  
Invented for life

our focus is to alert you when needed and help you quickly retrieve the correct data.

### Dynamic Transcoding

Our focus is on 24/7 remote access and camera control limited bandwidth makes it impossible to stream HD video on mobile devices.

Dynamic Transcoding delivers both smooth live video streaming and instant access to HD images when needed, regardless of available bandwidth. As you cannot be everywhere all the time, you can now use your mobile device to access camera controls, live video streams and HD images anytime from anywhere. Dynamic Transcoding also enables you to instantly retrieve the correct video data from hours of recorded material. With Dynamic Transcoding, our focus is to give you access to HD images anytime, anywhere.



**ZoneTechnology**  
Your Security Supply Partner

Auckland: (09) 415 1500

Wellington (04) 803 3110

Christchurch (03) 365 1050

Email: [sales@zonetechnology.co.nz](mailto:sales@zonetechnology.co.nz)

Website: [www.zonetechnology.co.nz](http://www.zonetechnology.co.nz)

# NZ Security Training Association

The introduction of mandatory training in October 2013 signalled a new era of professionalism across the security sector.

A focus on training highlighted a gap in the industry for an independent, apolitical organisation (not affiliated with NZSA) dedicated to supporting and informing training, training providers and training programmes. Out of this was born the New Zealand Security Training Association - NZSTA.

NZSTA is dedicated to supporting training within the security industry by providing a framework within which professional development flourishes. Its goal is to enrich security training and improve learning experiences and outcomes for trainees.

Membership is open to anyone from the wider security industry including:

- Private Training Establishments (NZQA).
- Security companies.
- Trainers & assessors within the security industry.
- External organisations who provide training to the security industry (e.g. Fire/First Aid).

## NZSTA functions

- Share information regarding the current NZQA Targeted Review of Qualification process.
- Share information regarding security training including national and international trends.
- Provide workshops and training events run by members to support industry training.
- Provide support to security companies regarding training and training processes.
- Provide a forum for security companies to give feedback regarding training and training delivery to ensure fit for purpose training.
- Support workplace assessors with training, assessment and moderation requirements.



- Liaise with relevant Industry Training Organisations (Skills, EMQUAL etc).

NZSTA has been endorsed by the Skills Organisation who see the benefit of working together to improve the quality of training and trainee outcomes. By providing support to workplace assessors NZSTA can assist with raising national programme completion rates within the sector. This also sits well with the Tertiary Education Commission, particularly as security has historically been one of the poorest performing industries with regards completion rates.

NZSTA members are excited about being able to address what has been missing for so long within the security sector and are committed to working together to raise the standards and professionalism of training. Our members

are already providing support to workplace assessors in Auckland and Christchurch as well as assisting companies to understand their options with regards formal training. Other members have embarked on a mutual collaboration which is providing trainer upskilling and workplace experience for trainees.

In the future there are plans for Train the Trainer and Adult Education courses for workplace assessors as well as OSH and Emergency Management qualifications provided by members and for members.

For further information please contact Kathy Wright – NZSTA Chairperson on [info@nzsta.co.nz](mailto:info@nzsta.co.nz)



**NZSTA**

Supporting Security Training



# The Countdown's On

Any security companies who have not yet started training their staff to meet the Private Security Personnel training requirements are running the risk of not meeting the deadline.

Lance Riesterer, General Manager Specialist Trades and Business for The Skills Organisation, says companies are now on the clock. "We've been saying the same thing for months – get going. If you're confused give us a call – if you know someone in the same boat give them our number. We want people to be ready and we can point them in the right direction."

## Who needs to undergo training?

The training requirements apply to License and Certificate of Approval (COA) holders including crowd controllers, property guards, personal guards and their employers.

The Security industry is a sector that has a relatively high staff turnover meaning that a lot of the 'new to industry' people have to complete this training. People who are employed in a holiday job over the Christmas and holiday season or

for events also need to complete the regulatory training.

If you're reading this and thinking "that's me and I've done nothing or don't have a plan" don't panic. People who are new to the security industry have a three month window of opportunity to get the minimum training completed otherwise they will not be able to operate within the security industry.

## What needs to be done

All staff that need to meet the training requirements need to gain the following three NZQA unit standards:

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

## Where can I go to get training?

There are a range of training providers who can provide training to meet the requirements. They are based throughout

the country and can advise your company how to go about getting your staff through the requirements. They can talk to you about how they deliver the training, when they can do it and about the cost.

The NZSA has a nationwide network of delivery - you can contact them on 09 486 0441 by email [info@security.org.nz](mailto:info@security.org.nz), or visit [www.security.org.nz](http://www.security.org.nz).

For the full list of training providers go to [skills.org.nz](http://skills.org.nz) and head into the security industry section.

## When do I need to complete the training requirements by?

There are two different deadlines – one for if you have a COA and one if you are new to the industry.

- 30 September 2014 (if you have an existing and current COA)
- 3 months from joining the industry (if you're new to the industry)

"This isn't the time to rely on skating by," says Riesterer. "The stand-by Kiwi attitude of it's going to be alright on the night will not do anyone any favours. Particularly your staff. So I'll say it one more time. Don't wait!"



# The clock is ticking

For more information about training options for the mandatory security training requirements visit [skills.org.nz](http://skills.org.nz)

**Time is running out!**

## skills.

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

# Mandatory Training - What Have We Learnt?

by Kathy Wright BHSc, PGDipHSc, MN (Hons), Managing Director C4 Group Ltd

---

It is now ten months since the Ministry of Justice announced mandatory training requirements for holders of Certificates of Approval or security licences. C4 has put over 3000 people from 70 different companies through the mandatory training and with a staff of 15 trainers are running between 13 and 15 courses a week nationally. As the largest provider of COA training in NZ, C4 has been well placed to review the sector and recognise trends and issues specifically related to security training.

One emerging trend is the heightened awareness of the importance of training to the industry and we receive calls regularly from companies wanting to know what their options are regarding the same. The majority of these companies have not previously seen the benefits of training or have found the process too difficult to manage. Initially many are only looking to fulfil the mandatory requirements but given comprehensive information regarding the national qualifications and the support available, their confidence in being able to manage training for their staff has increased significantly and they have been keen to commit to the full programme. Their main issue appears to have been a perceived lack of clarity and input from organisations whose role it is to provide support to the industry for training.

This process of growth has seen C4 increase its Level 2 training programme numbers by nearly 50% in an industry that has almost been in hibernation since the Rugby World Cup. It has been clear to

us that our companies who are currently undertaking national qualifications are getting serious about the importance of training with many appointing staff to positions dedicated to overseeing and supporting trainee performance. A closer liaison with C4 has contributed to an increase in trainee completion rates and improved learner outcomes. One major company has even included C4 in its formal presentation for a national contract tender demonstrating the importance of professional training to their organisation. Clients of security companies are also becoming more insistent that guards have at least the Level 2 qualification or are working towards it.

One issue that has been forced into the open is the low literacy levels within the industry. The Tertiary Education Commission has identified the security industry as having low literacy levels but until the advent of mandatory training we believe that the size of the problem was not truly understood. Historically training providers and the Skills Organisation have worked with trainees who are registered on training programmes and who required literacy support. However, the huge numbers of guards who have never engaged in formal training due to poor literacy has meant that the true picture has never been clear.

Now that they have been forced to undertake training they are out in the open, at times creating high stress levels within this group. This has presented C4 and other training providers with a great opportunity to support these trainees

and assist them to achieve the mandatory requirements and also to provide ongoing support for literacy improvement.

A concerning trend is the number of companies who have not engaged in the mandatory training process and who risk having uncertified guards come October 1st. There is a belief within some areas of the sector that the PSPLA will allow for extensions, exemptions and dispensations for companies that have not yet started or completed training their guards. PSPLA have stated clearly to C4 that any guard without the mandatory training at October 1st will have their COA cancelled at PSPLA level. Perhaps then compliance personnel will be able to check this in a fashion similar to Police checking driver licence status. Worst case scenario is that guards will be stood down from their posts during compliance visits if they haven't completed the required training.

This past ten months has been an amazing experience for C4 and our staff. We have met some wonderful people who are committed to the industry and wanting to make a difference. The achievement of the 3 COA mandatory unit standards has allowed many who have never succeeded educationally to believe that they can go on to completing the Level 2 national qualification. C4 has been proud to have assisted them with this and to be able to be part of the rest of their journey. The future of training within the security sector is exciting and C4 looks forward to being able to lead and support the industry along this pathway.



# Locked in... no compromise no comparison!

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

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

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

# 10 year\* guarantee

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

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



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

**Loktronic**

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



# The Convergence of IT Security and Physical Access Control

Using a Single Credential to Secure Access to IT and Physical Resources

A White Paper from HID®

## Executive Summary

Organizations are increasingly adopting a model in which multiple access control use cases and identities can be supported on one card or smartphone. This convergence of use cases and identities eliminates the need for users to remember and carry separate cards or other devices for opening doors, logging onto computers, and accessing cloud-based applications, and also enables the inclusion of other high-value applications including cashless vending, time and attendance, and secure print management.

There is growing demand for provisioning IT and physical access control system (PACS) credentials to a single card or smartphone, using a single set of processes. Beyond convenience, however, the convergence of credentials onto a single card or device can greatly improve security and reduce ongoing operational costs. It also centralizes identity and access management, consolidates tasks and enables organizations to quickly and effectively use strong authentication throughout their infrastructure to protect access to all key physical and IT resources.

The new, integrated credential management model moves organizations in four important directions: beyond cards to smartphones; beyond readers to “tap-in” access convenience; beyond Public Key Infrastructure (PKI) technology to simplified solutions for higher security; and beyond legacy PKI to true converged strong authentication access control.

This paper looks at the drivers, challenges, deployment options and results associated with a converged IT and physical access control solution, and also describes the value of a seamless user experience when using cloud-based

applications and services, accessing data, and opening doors. It also explains the benefits of unified enrolment processes and workflows spanning multiple identities across multiple IT security applications and the PACS.

## Understanding the Drivers for Convergence

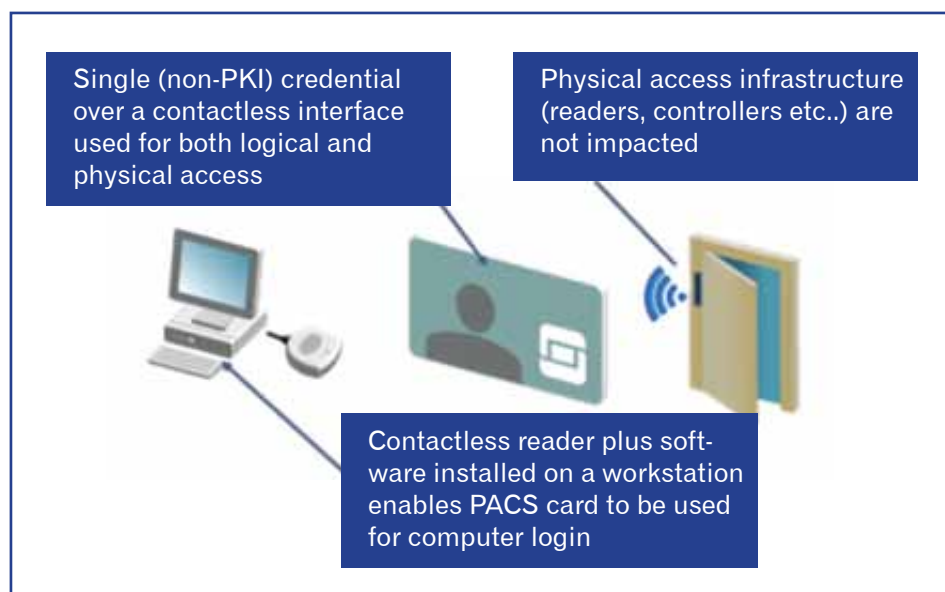
Historically, the focus for organizations has been on creating a strong perimeter to secure access to their physical and IT resources. Legacy access control approaches rely on a user presenting an ID badge to gain entry into a building, and then, once inside, using static passwords to authenticate to IT resources. Given the nature of today's Advanced Persistent

Threats (APTs) and all the internal risks associated with Bring Your Own Device (BYOD) adoption, however, these methods of securing access are insufficient.

Organizations require the ability to better control access and employ strong authentication throughout their infrastructure, as part of their multi-layered security strategy. Unfortunately, choosing an effective strong authentication solution for enterprise data protection has traditionally been difficult. Most available solutions are inadequate either in their security capabilities, the costs and complexities they introduce for the organization, or the user experience they deliver.







Employees want the convenience of being able to use a single card or mechanism to quickly and easily access the resources they need to conduct business. To accomplish this, organizations must deploy a solution that can be used to secure access to everything from the door to the corporate computers, data, applications and cloud. They must combine the traditionally separate domains of physical and IT security to coordinate the management of their users' identities and access.

### The Value of Converged Access Control

Truly converged access control consists of one security policy, one credential and one audit log. In some organizations, user management is already fully converged, with a single corporate policy that defines acceptable access and use of resources, a single master user repository, and a single logging tool for simplified reporting and auditing. This approach enables enterprises to:

- **Deliver Convenience** – replaces one-time password (OTP) tokens and key fobs, negating the need for users to carry multiple devices or re-key OTP to gain access to all the physical and IT resources they need.
- **Improve Security** – enables strong authentication throughout the IT infrastructure on key systems and applications (rather than just at the perimeter), and even at the door.
- **Reduce Costs** – eliminates the need to invest in multiple access solutions, centralizing management and consolidating tasks into a single set of administration and helpdesk processes around issuance, replacement and revocation.

### Exploring Multiple Deployment Options

With a converged access control model, the credential can be delivered in a variety of form factors, such as a smart card (e.g. ID badge) or even a smartphone. Depending on the enterprise's requirements and existing infrastructure, there are several ways to architect the solution. The following are the three most common models:

- **Legacy Contactless:** Enables an existing card-based physical access system utilizing technologies such as iCLASS®, iCLASS Seos®, MIFARE™ and MIFARE DESFire™ to be extended to authenticate to enterprise networks and applications. Software is deployed on the end user's workstation, with a contactless reader connected to or embedded in it. The card can be "read" without needing to be physically inserted into the reader device. This is convenient for users, who can take the same card they have been using with a door reader and tap it to a personal computer or laptop in order to gain access to their computer and to corporate and cloud applications.

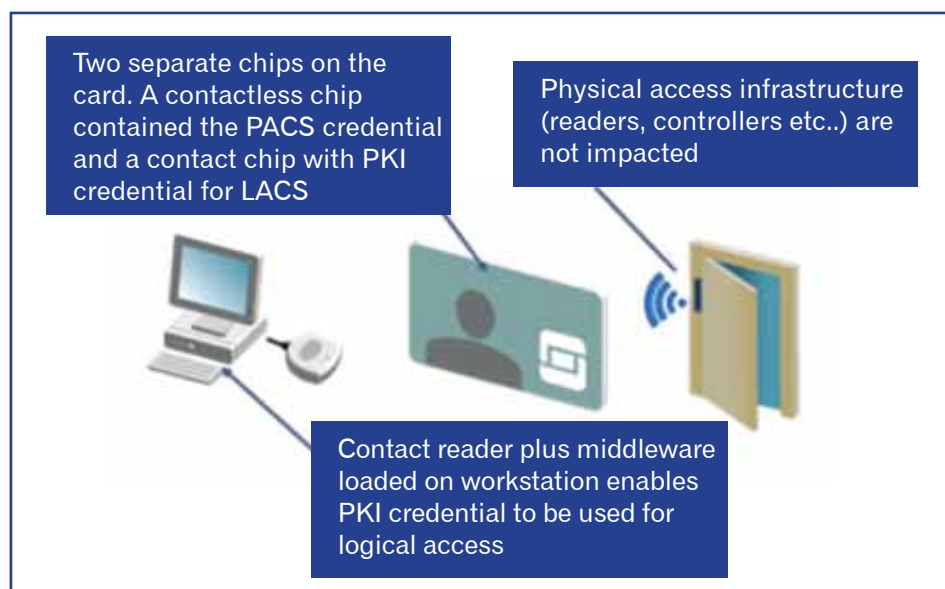
This approach doesn't employ PKI, which binds public keys with user identities through a certificate authority (CA). Used in the federal space, PKI strong authentication is a key element of logical access and digital document signing for agencies and their contractors. A digital certificate including the user's public key is placed on a Personal Identification Verification (PIV) card, which leverages smart card and biometric technology (a digitally signed fingerprint template), and also supports multifactor authentication methods. Rather than relying on a shared, secret key for authentication, a pair of public and private keys is used and these keys are linked such that information

processed with one key can only be decoded or validated using the other key. The Federal Bridge is used to establish trust between cross-certified agencies' PKIs (i.e., separate and independent infrastructures, each with its own root certificate authority), thus enabling secure information exchange of digital signatures and certificates sent from and between various other participating government organizations.

The legacy contactless approach eliminates many of PKI's key management challenges, but it also supports a more limited range of use cases and doesn't deliver the same security strength as PKI-based solutions. The contactless, non-PKI model is being deployed in hospitals, schools and other environments, where multiple users need access to the same workstation in quick succession. It is also being used as a bridging solution where mandates, such as those of the Criminal Justice Information Services (CJIS), require workstations and applications to be protected by strong authentication.

- **Dual Chip Card:** Embeds a contactless chip for physical access control and a contact chip for logical access control on a single smart card. Credentials, such as PKI certificates and OTP keys, can be managed on the contact chip using a card management system (CMS). The dual chip card model is popular with medium to large enterprises with sensitive intellectual property (IP) or customer data on their networks, because it delivers strong security. It also enables the enterprise to simplify management of their IT security infrastructure and leverage their existing PACS investments because, in many cases, the CMS can be integrated directly into the PACS management system (often referred to as the PACS head-end).

- **Dual Interface Chip Cards:** Leverages a single PKI-capable chip, with both a contact and contactless interface to support both physical and logical access control. The card can be used to support a contact card reader for logical access use cases, such as logging into a computer or signing an email, and PKI authentication for physical access. The dual interface card model is applicable primarily in U.S. Federal government organizations, where mandate OMB-11-11 requires that PIV credentials, specified by FIPS 201, be used for physical access. By default, PKI over a contactless interface can be slow for physical access usage. To address this challenge, FIPS 201-2 is expected to allow the use of the Open Protocol for Access Control Identification and Ticketing with privacY (OPACITY) suite of authentication and key agreement protocols that will add roughly four times the performance for critical tasks. It will also deliver secure wireless



communications, which will enable the use of PIN and biometrics on the contactless interface. This will further strengthen authentication for both physical and logical access control.

### Bringing Strong Authentication to the Door

An important benefit of convergence is that it enables organizations to leverage their existing credential investment to create a fully interoperable, multi-layered security solution across company networks, systems and doors. Strong authentication will increasingly be employed not just for remote access, but also for desktops, key applications, servers, cloud-based systems and facilities. This requires bringing strong authentication to the door.

One of the first places this will occur is in the federal space with users' existing PIV cards. To use a PIV card to enter a building, the PIV card's digital certificates are checked against a

Certificate Revocation List (CRL), which is provided by certificate authorities. PKI authentication is a highly efficient and interoperable method not only for logical access control to protect data, but also for physical access control to protect facilities, the latter referred to as "PKI at the door."

Agencies are taking a phased approach to implementing PKI at the door, as budget becomes available. To ensure that this is possible, they are configuring their infrastructure so that it can be quickly and easily upgraded to PKI strong authentication for physical access control when they are ready. For instance, they are first enrolling all of their PIV card holders into their head-end system, and then simply deploying Transitional Readers as defined by the General Services Administration (GSA), which read the unique identifier from the card and match it with the enrolled card holder without using any FIPS-201 authentication techniques. These Transitional readers can later

be reconfigured in the field to support multifactor authentication.

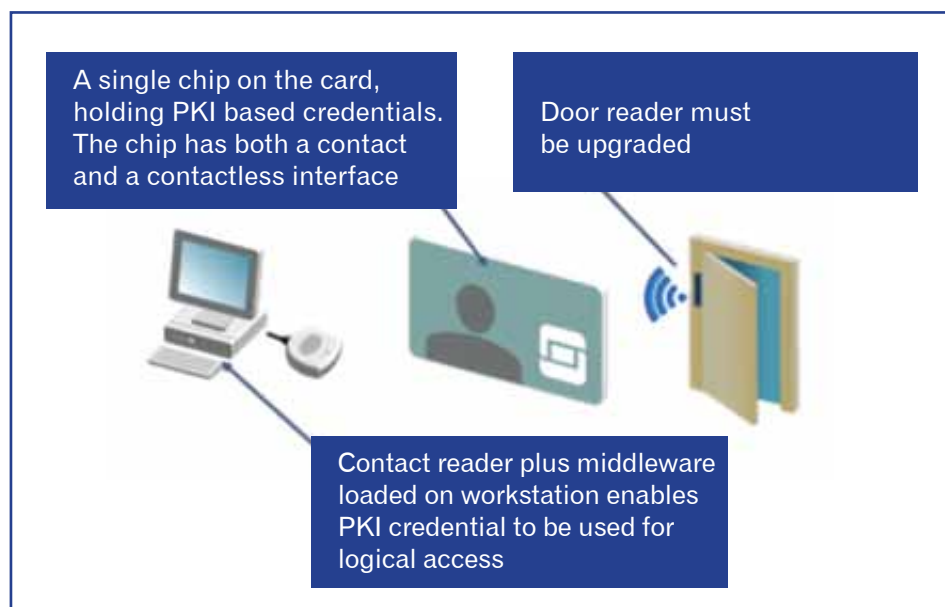
It is expected that PKI at the door will become more widely adopted as FIPS 201 evolves and there are more products available to support it. There also will be significant opportunities to deploy PKI at the door at lower cost with Commercial Identity Verification (CIV) cards, which are technically similar to PIV cards but don't carry the additional requirements associated with being trusted by the federal government. Unlike federal agencies, CIV card users will not have to purchase certificates from a trust anchor or pay annual maintenance fees, but can instead generate their own certificates. While the cards will be a little more expensive to accommodate the extra memory for certificate storage, this modest incremental cost will deliver the valuable additional benefits of stronger authentication at the door. Consider the example of a municipal airport, which will be able to use CIV cards alongside sibling PIV cards that are already being carried by federal Transportation Security Administration (TSA) employees there. Airport management will be able to create a single access control system that supports both airport employees and federal agencies that are also operating there, while ensuring higher security through strong authentication.

Extending strong authentication throughout the physical and logical access control infrastructure will also be important in the enterprise. Organizations need a range of authentication methods and the flexibility to easily support different users and protect different resources appropriately. With simple-to-use solutions, enterprises can secure access, from managed and unmanaged devices, to an enterprise's resources. Without having to build or maintain multiple authentication infrastructures, enterprises can use a single solution to secure access to all their resources, from a facility door or copier to a VPN, terminal service or cloud-based application.

### What About Mobile?

As we all know, users are increasingly mobile and bringing their own devices (BYOD) into the organization's environment, using smartphones, laptops and tablets to access the resources they need. According to ABI, there will be 7 billion new wireless devices on the network by 2015, which is close to one mobile device per person on the planet.

Organizations are trying to support all this mobile access, while looking at ways





to leverage their users' mobile devices as platforms for carrying credentials for physical and logical access control. There have already been pilots, such as one at Arizona State University, that have proved the concept of being able to use a mobile phone to carry a physical access credential. The federal government is also looking at mobile access control. FIPS-201-2 is expected to include extensions such as the concept of derived credentials that can be carried in the phone's secure element (SE) using the same cryptographic services as the card.

Mobile access control requires rethinking how to manage physical access credentials, and to make them portable to smartphones so that organizations have the option to use smart cards, mobile devices or both within their PACS. To do this, HID Global has created a new data model for its iCLASS SE® platform called the Secure Identity Object® (SIO®) that can represent many forms of identity information on any device that has been enabled to work within the secure boundary and central identity-management ecosystem of the company's Trusted Identity Platform® (TIP). TIP uses a secure communications channel for transferring identity information between validated phones, their SEs, and other secure media and devices. The combination of TIP and SIOs not only improves security, but delivers the flexibility to adapt to future requirements, such as adding new applications to an ID card. It is designed to deliver particularly robust security, and will be especially attractive in a BYOD environment.

With a mobile access control model, any piece of access control data can be supported on a smartphone, including data for access control, cashless payments, biometrics, PC logon and many other applications. The authentication credential will be stored on the mobile device's SE, and a cloud-based identity provisioning model will eliminate the risk of credential copying while making it easier to issue temporary credentials, cancel lost or stolen credentials, and monitor and modify security parameters when required. Users will be able to carry a variety of access control credentials as well as an OTP computer logon token on the phone that they can simply tap to a personal tablet for authenticating to a network. By combining mobile tokens on the phone with cloud app single-sign-on capabilities, it will be possible to blend classic two-factor authentication with streamlined access to multiple cloud apps on a single device that users rarely lose or forget. Plus, the same

phone can be used for opening doors and many other applications.

There will be challenges to solve since phones and other mobile devices being used for physical and logical access control applications will often not belong to the organization. For example, when a student graduates from a university, he/she doesn't hand their phone back in the same way that employees would hand their cards back when they stop working for a company. It will be critical to ensure the personal privacy of BYOD users, while protecting the integrity of enterprise data and resources. IT departments won't have the same level of control over BYODs or the potentially untrustworthy personal apps they may carry, and aren't likely to be loading a standard image onto BYODs with anti-virus and other protective software. We will need to find new and innovative ways to address these and other challenges. Notwithstanding the risks, the use of mobile phones equipped with SEs, or equivalent protected containers, opens opportunities for powerful new authentication models that leverage the phone for securely storing portable credentials, enabling use cases ranging from tap-in strong authentication for remote data access, to entering a building or apartment.

Mobility is driving ongoing convergence, as it forces the physical and IT security teams to work together to come up with a solution. The result can be a solution for easily managing PACS credentials and IT access credentials on phones in a cost-effective way, while delivering the same level of security they were used to with cards.

### Realizing The Benefits of True Convergence

The ability to combine access control for physical and IT resources on a single device that can be used for many applications improves user convenience while increasing security and reducing deployment and operational costs. It will eliminate the need for separate processes for separately provisioning and enrolling IT and PACS identities. Instead, it will be possible to apply a unified set of workflows to a single set of managed identities for organizational convergence. Organizations will be able to seamlessly secure access to physical buildings and IT resources, such as computers, networks, data and cloud applications. An effective solution will also scale to secure access to other resources, as needed, to support a fully interoperable, multi-layered security strategy that can protect the organization's buildings, networks, systems and applications, now and in the future.

# SUBSCRIBE NOW

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

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

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

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

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

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

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

Surname \_\_\_\_\_

Title \_\_\_\_\_

Company \_\_\_\_\_

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

Telephone \_\_\_\_\_

Email \_\_\_\_\_

Date \_\_\_\_\_

Signed \_\_\_\_\_

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

# Thermal imaging easy to use and hard to live without

## Clackamas Fire Department puts more FLIR Thermal Imaging Cameras in more hands

Clackamas Fire District #1 provides fire, rescue and emergency medical services to five cities in the state of Oregon, USA. With 17 fire stations strategically located throughout Clackamas County and a workforce of more than 200 employees & 100 volunteers, it's the second largest fire protection district in the state, serving over 179,000 citizens in an area covering nearly 200 square miles.

### Thermal imaging for firefighters

"The technology's really changed since the early days," says Captain Jason Ellison while between calls at the historic 1923 John Adams Fire Hall in Oregon City. "Thermal imaging cameras were very large, cumbersome units when we first started using them, and very expensive. In fact, we were only able to afford a couple of cameras for the entire district back then. But with the lower cost models that are available these days, now we have multiple cameras per rig and use them pretty much on a daily basis throughout the district."

"Thermal imagers have allowed us to see in situations where it's nearly impossible to with the naked eye. Obviously inside a fire environment it's incredibly smoky and dark, and we don't know the layout of the



*Captain Jason Ellison: "Thermal imagers have allowed us to see in situations where it's nearly impossible to with the naked eye."*



*FLIR K-Series allows seeing through smoke. It helps firefighters to find their way in a smoke filled building and to locate fire victims. It helps to save lives.*

building. TICs show us the way through so we can move swiftly, look for the seat of the fire, look for victims; basically they help provide a very effective roadmap."

In a technical nutshell, thermal cameras create images from heat instead of light by detecting temperature differences in a scene and transforming those values into a crisp thermal video image on the camera's LCD. On certain models, such as the FLIR K40 and K50, still frames can also be captured and stored to internal memory for later review and downloading for documentation and training.

### Seeing through smoke and in total darkness

"With the thermal imager, I can tell as I move down the hallway where bedrooms are, easily make out the location of beds, closets, windows, and see where others are around me," Ellison adds, "Windows, by the way, are a secondary egress for us so knowing where they are is crucial to our safety."



Ellison explains that firefighters manning the nozzle have their hands full and typically aren't the ones carrying a TIC. "There's thick black smoke, ventilation hasn't kicked in yet, and it's very hard for them to even see their hands in front of their face. But a company officer close behind with a thermal imager can be right there to hold the TIC in front of that firefighter so he can see the layout of the structure, press on, and direct the nozzle pattern where it needs to go."

That, Ellison says, really speeds up the effort. "In the old days, we'd have one hand feeling the way along a wall and another hand holding onto the leg of the firefighter in front of him. Try finding your way in your house with your eyes closed. That's what it was like. It really ate up precious time."

"With this (TIC) technology, we're able to get to the heart of the fire and knock it out much quicker and more safely. Even when the fire's essentially out, I'm still using the camera to look (through remaining smoke) for hotspots."



# Handheld Thermal Imaging Cameras for Firefighting Applications



Extremely affordable FLIR K50 cameras help you attack fires more strategically and find victims faster. Get the bright big picture and tactical advantage you need to see under the most challenging conditions.

Buy a K50 now through September 30th and we'll give you an Extech CO10 to help alert you to dangerous carbon monoxide levels.



**Get a **FREE** Carbon Monoxide Meter with Every K50 Purchase!**

Learn more at [www.flir.com.au/nzsecurity-k](http://www.flir.com.au/nzsecurity-k)



The World's **Sixth Sense**™



*The lightweight FLIR K50 camera provides clear and detail rich images of 320x240 pixels*

### Thermal imaging saves lives

Tracking down trapped, stranded and missing victims is another way TICs come to Clackamas Fire's aid. "In any fire situation," he says, "there's always a possibility someone's inside. So a thermal imager is very effective at helping us make sure everyone got out safely and the home gets the 'all clear'. We also use

them in our technical and water rescue efforts. For instance, we can search for people who may be stuck on a remote shore in the dark after falling in the river. Sometimes at night we have to deal with a car accident where someone got ejected from the vehicle and we need to locate the victim.

### FLIR K-Series: extremely affordable, compact and easy-to-use

"The cameras we originally started out with seemed like the size of computers... very bulky to carry. The new ones like the FLIR K50 are very light and much more compact. And that's important when you're already packing 50-plus pounds of gear. A smaller TIC on a lanyard like the FLIR K50 makes it a lot more practical to clip on your turnouts or self-contained breathing apparatus (SCBA) and be hands-free until you need the device. For me, it's very tactical to use without having to slip my hand through a handle... much easier to just grab, go, and then let go of."

He also likes the Search and Rescue (SAR) mode that narrows the temperature detection span more in line with body temperatures to alert him where victims are faster, especially in hotter environments. On the other hand, when he's working engine company and fire attack, he usually leaves it in "fire mode", which has a 300 to 1200 degree F range. "That gives me a really good colour alarm to show me where the super-heated gasses are and where there's fire around us."



*Like many fire departments in the USA, Clackamas Fire has depended on thermal imaging cameras (TICs) for well over a dozen years as a critical tool in helping protect lives and save property.*

The bigger, brighter LCDs of today's thermal imagers also make using thermal imagers more popular. "Having a nice 4" screen that the FLIR K50 has, makes it a lot easier to decipher what I'm looking at to guide my crew members to safety or to their objective."

More affordable pricing has also made a huge impact. According to Ellison, "We're looking for tools that can help keep us safe that are also the most cost-effective. FLIR's affordability will allow us and other departments to put more cameras on the rigs to help us do our job better and keep our guys safe."

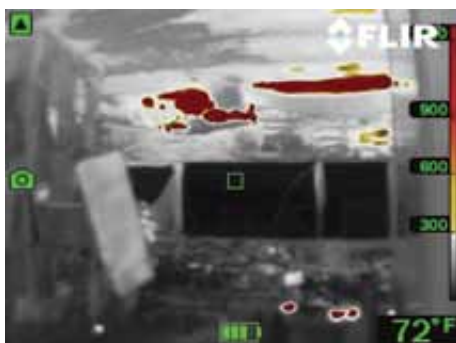
To sum it up, Ellison says it's a tool that, when used correctly, allows firefighters to move swiftly and safely and get the job done right. It's technology that would be very difficult to live without.



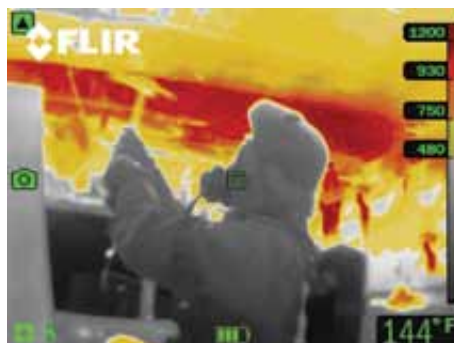
*Heat detection mode - Fire fighters searching in cold smoke*



*SAR mode - Rapid Intervention Team (RIT) Operations finding down fire fighter*



*NFPA mode - Hotspots during overhaul*



*Fire mode - Heavy heat in ceiling above fire fighter*

If you would like more information about this product or about FLIR Systems and its wide range of thermal imaging cameras for a wide range of applications, please contact:

FLIR SYSTEMS Australia Pty Ltd  
Toll Free: 1300 729 987  
New Zealand: 0800 785 492  
Email: [info@flir.com.au](mailto:info@flir.com.au)  
[www.flir.com](http://www.flir.com)





# Marae fires reinforce urgency for more affordable systems

The urgent need to revise restrictive Building Code conditions that make sprinkler systems too costly for many community groups was highlighted over a week in June when separate fires destroyed two North Island marae buildings.

In the early hours of 12 June five fire crews battled a blaze at the historic Mana Ariki marae in Taumarunui in the central North Island, established by Maori prophet Alex Phillips in 1961. Buildings were well alight when the first fire crews arrived at 5.10am and it took two hours to bring the blaze under control.

Then on 15 June the NZ Fire Service was called to a blaze at a meeting house being used for sleeping quarters at the Opotiki College marae on the East Coast.

Tables and chairs had been pushed across some emergency exits and mattresses laid out on the floor blocking other exits. Mattresses had also been placed over underfloor heating vents causing the fire. There were no sprinklers and a fire alarm was not working.

The 40 students who were planning to sleep in the building overnight were at kapa haka practice nearby when the fire broke out.

The NZ Fire Service says if the fire had occurred while they were in the building there would “almost certainly have been fatalities”.

The Opotiki fire chief said this should serve as a warning to other schools or marae to double check their fire safety systems and have a careful fire safety plan for overnight stays.

## Education ramping up

The fires occurred at a time when the NZ Fire Service Maori unit was ramping up its fire safety message and encouraging marae committees to ensure they had smoke alarms and fire alarms to protect those sleeping on premises, as well as tribal assets and treasures (taonga).

NZ Fire Service Chief Engineer Simon Davis says recent changes to commercial sprinkler system regulations which allow simpler, more affordable systems,



*Devastation after the Mana Ariki Marae fire in Taumarunui. Photos: Te Aorangi Harrington*

“without all the bells and whistles” has opened the way for more buildings to be better protected.

He says cost has been a major issue along with some cultural issues for example reluctance to have “red pipe and ugly sprinkler heads all over the place” or near tukutuku panels.

He’s hoping the NZ Fire Service report on the Mana Ariki marae fire will create greater awareness of the need to attend to such issues and get around what he calls “the Lotto mentality”.

Rather than gambling with fire safety, thinking it’s a million to one chance, he says people are beginning to wake up to the possibility that it could happen to them.

He says the NZ Fire Service has a very proactive group based in Gisborne including a fire engineer who’s senior station officer, running a project to educate Maori communities about the benefits of sprinklers and fire protection systems.

Generally he says there’s been a good uptake but the legislation is still a bit

loose around what is and isn’t required, including the size of the buildings and their age. “Some maraes have been around for many, many years, pre-dating modern legislation and in some cases even sprinklers.”

He says the losses of culturally significant buildings has turned the minds of communities to protection. “There are at least 140 in the East Cape and Bay of Plenty area that now have sprinkler systems.”

Davis sits on the New Zealand Standards group that recently ratified changes to the regulations allowing more affordable protection systems. “Ed Sawyer one of the fire engineers at BRANZ saw the gap and really pushed for these changes and got it across the line as an appendix to the standard.”

He says the changes apply to any community building up to 500 square metres whether it’s a marae, scout den, community hall, “and other properties that are usually run on the smell of an oily rag”.

– Keith Newman

# Fewer fires challenge cost and role of fire services

Keith Newman talks about the changing face of the fire industry with Neil Gibbins, the new international president of the Institution of Fire Engineers (IFE), fresh from touring WWI battle grounds on his BMW R1200RT motorcycle

---

Fire services around the world are under increasing pressure to downsize and diversify at the same time as building and business owners are using less fire resistant materials and looking at ways to reduce their fire protection costs.

Neil Gibbins, the UK-based International President of the Institution of Fire Engineers (IFE), says outdated operational models are being challenged as governments look at ways to reduce the size of fire services, repurpose their capabilities and in many cases slash budgets in the wake of the global financial meltdown.



Neil Gibbins QFSM,  
International President of the IFE

He says growing economic pressure, and the fact that better education and fire protection systems have resulted in less fires and deaths by fire, are challenging the traditional structure and function of fire services.

Although many are aligning with other emergency services such as search and rescue and ambulance they're still expected to ramp up their training to become skilled in a range of new areas.

Gibbins, with 30-years operational experience in the fire service, will be in Wellington in the first week in September as a keynote speaker for After Disaster Strikes – Learning from Adversity, the biggest emergency management conference in Australasia.

The conference will take an in-depth look at the impact of disasters, how emergency services can best support their people through adversity and how to build capability and resilience.

His message to New Zealand will be based around the need for greater knowledge sharing and lifting competence and interoperability between emergency services, “underpinned by validated examinations”.

## **Less spent on protection**

While less fires means fire services are under less pressure, Gibbins says there's no room for complacency as many businesses owners and property developers, are also cutting costs, often in ways that impact on traditional fire protection systems.

Gibbins says there's a greater focus on justifying investment in fire safety solutions, and for designers to achieve safety compliance at absolute minimum cost.

“Environmental and financial drivers are also leading to new designs that pose greater challenges should a fire occur, with concrete and bricks being replaced by renewable timber products.”

Another challenge is the development of taller buildings where traditional elements are replaced by timber frames and timber laminates. “While this may be due to environmental concerns or cost, the fire sector will need to provide building standards guidance, advice to occupiers and to maintenance and repair companies and emergency responders.”

The concept of cheaper but less durable buildings, alongside those designed to last 100-years and still remain standing after a fire, also raises issues that must be addressed, says Gibbins.

As designers learn more about fire precautions some traditional standards are being challenged and “engineered solutions” applied. Those decisions still need to be based on the best available information and the impacts considered through on all stages of a building's lifetime.

The generalisation that brackets similar types of buildings together for fire protection requirements is also changing. “Any significant building is likely to be designed for a specific use and against functional criteria but the questions always



# fire door holding electromagnets



Standard, floor mounted, wall to door distance 114mm



A)

B)

C)



## FDH40S

### unbreakable universal mounting

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

### 10 YEAR GUARANTEE\*

Designed, tested and produced in New Zealand to AS4178

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

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

C) Wall mounted, 355mm extn. tube (overall 431mm)



Flush mounted, wall to door distance from 50mm



Surface mounted, wall to door distance 70mm

## FDH40SS

### stainless steel surface and flush mounting

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

### 10 YEAR GUARANTEE\*

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



need to be asked about how quickly fires could develop, what the fire risk is to people, and how long would it take for them to leave safely?"

### Prevention imperative

While the fire protection industry often drives improvements in materials, technology and processes, in Gibbins view the main focus should be on preventative measures, "identifying where failures have occurred or are likely to occur and acting to stop them".

While fire protection decisions may be based on historic assumptions or on computer modelling from similar environments this raises issues for those who sign off the work, including the architect and regulator.

In fact, says Gibbins, the concept of "signing off" in relation to compliance issues is being challenged around the world. "Engineered solutions need engineered appraisals".

If a government body is responsible for a regulatory framework to ensure buildings are safe then that body needs the right skills and qualifications to make judgements and take appropriate action.

"If that's based on the simple application of codified solutions its reasonably straightforward but functional compliance means the person taking responsibility must understand the implications of the risk from first principles up."

## Encouraging younger volunteers

One of the challenges facing the NZ Fire Service and others around the world where there's a huge dependence on volunteers is the greying of the population.

"The forecast for the average age of the UK population over the next 50 years is mind boggling with a massive increase in the number of people living to 100-years, which clearly has an impact on support services."

To revitalise emergency services with younger people the UK has embarked on a long term training programmes or apprenticeships.

"Perhaps we should try to get all young people to be involved in community safety through their basic school curriculum and through membership of young person's organisations, fire and rescue youth association perhaps?"

*"For too long we had seen fire certificates issued by the fire service and little or no ownership taken by the building management, unless an inspection was scheduled."*

Neil Gibbins,  
IFE International President

### UK regulatory changes

Many of the changes in the UK, and indeed New Zealand, are being driven by an awareness that there have been considerably less fires in the past decade, with governments looking to refocus, repurpose and in some cases downsize fire services.

In the UK there's been a 40% fall in the number of dwelling fires in the last ten years and a massive fall in deaths from fire. Despite the fire and rescue service being in less demand Gibbins says, there's "a reticence to change" despite ongoing work to create greater regulatory and structural efficiencies.

The UK's "historic patchwork of stable door laws" was swept away in a 2005 overhaul of fire legislation which placed greater responsibility on the person creating the risk rather than the regulator.

"I was delighted. For too long we had seen fire certificates issued by the fire service and little or no ownership taken by the building management, unless an inspection was scheduled," says Gibbins.

Now fire risk assessment has to be undertaken and updated by the owner or employer, which he believes has contributed to a substantial fall in the number of fires. "My experience tells me most fires are easily prevented by a little forethought. That thinking is now happening in the way it does for other health and safety risks."

The new framework has resulted in partnerships between business and public services to find the most appropriate fire safety systems, and efforts to reduce the cost of compliance.

Gibbins says the spotlight is on reducing regulation to create the right conditions for economic recovery with "fire engineers, in the new 'self regulatory' environment, challenging traditional solutions to identify more cost effective approaches."

However, he says, there is still a requirement for "a highly competent body to check the whole process is working, and gathering data from audits and fires to help reassure the Government that the process is delivering what is needed."

### Review uncovers savings

Following a 2013 independent review by Sir Ken Knight, a former London Fire Commissioner with 40-years firefighting experience, the UK Fire and Rescue Service remains under close scrutiny, as it struggles to realign its reduced resources, including downsizing budgets and the number of volunteer and full time workers

Knight was asked to identify efficiencies and operational improvements without reducing the quality of front-line services. "Sir Ken Knight's review gives many pointers, especially about the potential savings from deploying retained crews in urban environments and changing practices that go back to WWII."

However, Gibbins says it's proving difficult to make some changes, largely because of the public's perception of trust built around what the fire services have traditionally done.

Sir Ken's independent report on UK Fire and Rescue services published in May, claimed millions could be saved without impacting emergency operations and public safety. He said fire fighter numbers and expenditure had remained the same for a decade despite the drastic reduction in call outs and incidents.

He highlighted huge variations between how the 46 UK fire authorities operated, saying most continued to spend according to their budgets rather than the risk they had to manage, opening up potential savings of £200 million (\$NZ395m) a year.

He concluded that eliminating duplication of resources and standardising



Sir Ken Knight, author of *the inquiry into the UK Fire and Rescue Service*





Neil Gibbins (right) being inducted as the IFE's International President by Roy Bishop OBE, Immediate Past President at the recent IFE AGM & International Conference

management structures and operational differences could lead to closer co-operation and reconfiguration of services.

### Less need for firefighters

As the fire safety process improves it will further reduce the demand for firefighting and be seen as "an opportunity to reduce provision or use 'spare' capacity in other ways," says Gibbins.

Better use of crews is often seen as the preferred solution with a number of models emerging to bring together 'blue light services' — fire and emergency medical — in the US and parts of Europe.

The challenge, says Gibbins, is how to train for all the various incidents and maintain competence in critical skills when the number of incidents is low and falling?

Governments will need to consider how to mitigate these risks and make difficult decisions about allocating constrained public money by accessing the best available data. "Do we spend on hospitals or research? Do we legislate to reduce risk or allow market forces to determine the outcomes?"

Driving down the real cost of fire is not just about stopping fires, it is about having the most efficient and effective fire safety system, preferably validated through international tests of knowledge through IFE exams.

"There must be a process to ensure that those placed at risk from emergencies or those commanding responders are properly qualified and competent to do so safely," says Gibbins.

### Funding fact finding

Gibbins says hard times have made people think harder. Fires and deaths have fallen, not by having faster response but through prevention and protecting people through education and fire safety and building and management standards.

He suggests this is a good time to evaluate the ways fire services are funded around the world, including insurance-

*"... the questions always need to be asked about how quickly fires could develop, what the fire risk is to people, and how long would it take for them to leave safely?"*

Neil Gibbins,  
IFE International President

based systems, and make that data available to help governments decide what's best for them.

"From an IFE perspective I would like to see more freely available information that helps identify real costs and real risks as decisions are made about allocation of meagre resources."

Big decisions such as whether to have sprinklers in all buildings, compulsory smoke alarms or banning smoking need to be fact-based.

"As we embrace diversity of task and of recruitment we must maintain knowledge, standards and competency to provide durable safe solutions."

This was particularly important as fire response equipment is adapted to meet the growing demand for non-fire emergencies, especially those brought on by natural phenomena.

A key to ensuring that different emergency services have each other's backs is mutual sharing of data and learning experiences and systems interoperability.

Gibbins believes the IFE should be at the heart of improving data sharing around simple agreed definitions. "This is a lifetime ambition of mine. The IFE is non-aligned, dependable and international, and learning from fire is our mission."

To achieve this there needs to be greater openness. "It's hard to say 'we got it wrong' but not too hard to say we could have done this better."

He wants to see cross service learning, including why things go wrong, so everyone can benefit from risk reduction. Ultimately he's hoping lessons learned and knowledge that would be valuable to other parties can be shared on the IFE website (<http://www.ife.org.uk/>).

"You'll soon be able to see information about many serious UK incidents that led to the deaths of fire fighters on the IFE website so everyone can learn from this."

NB: Neil Gibbins views are his own and not necessarily those of the IFE.

# SUBSCRIBE NOW

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

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

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

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

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

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

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

Surname \_\_\_\_\_

Title \_\_\_\_\_

Company \_\_\_\_\_

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

Telephone \_\_\_\_\_

Email \_\_\_\_\_

Date \_\_\_\_\_

Signed \_\_\_\_\_

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

# Kiwi Self Storage arson may spark Code rethink

The arson at Kiwi Self Storage in Kilbirnie in April may become the trigger point to challenge elements of the Building Code to ensure greater fire protection for commercial building premises despite the owners being cleared of compliance issues.

NZ Fire Service Chief Engineer, Simon Davis, says strong media interest in the fire has attracted sufficient Government agency attention to ensure changes to regulations or legislation is seriously considered.

In the early hours of 4 April this year around 370 units were destroyed when one of the large buildings in the Kiwi Self Storage premises in Lyall Bay, Kilbirnie, burned to the ground destroying



NZ Fire Service Chief Engineer, Simon Davis

the possessions of customers who had entrusted property, precious memories and prized goods to the company.

A representative group, stunned at their losses, sought an inquiry into how this could happen, was considering legal action, and raised questions about the lack of sprinklers and why alarms were not monitored.

Peter Fowler, spokesman for the group initially claimed the facility was built to minimum standards, making it possible for fire to spread quickly and alleged the company had failed in its care of duty to its customers.

He asked local MP Annette King and Internal Affairs Minister Peter Dunne to investigate.

Dunne declined to push for an inquiry.

## **No requirement in Act**

Simon Davis says currently the Building Act doesn't trigger the need for sprinkler and alarm systems for the protection of property unless it relates to occupancy or people sleeping overnight. "It's really up to the developer, the owner or insurer."

He says the question is often asked why those in a commercial environment, charged with looking after other people's goods and promising safety and security, aren't more geared for fire protection?

Despite the high likelihood of damage and loss of property once a fire gets hold of buildings including big warehouses, many do not have sprinkler protection or alarms systems.

"It all depends on the motivation, whether it's to build the cheapest building or just comply with the minimum requirements of the Building Act," says Davis.

The Kiwi Self Storage blaze, just across the road from the fire station and fire training facilities, took 24-hours to douse and within days investigators were asserting it was started by an accelerant which led to an explosion in one of the storage units.

A man was caught on surveillance video just after midnight carrying what appeared to be a large canister of petrol.

Lost in the fire were Oscar statuettes, priceless photographs, paintings, expensive cameras and video equipment and irreplaceable family heirlooms.

Shane Wood, of Miramar, was storing his goods while he was between flats and lost everything he owned including his collection of 71 skateboards and his building tools, suggesting the value was around \$400,000.

Wellington-based record collector and disc jockey Danny Lemon lost 8,500 rare vinyl records estimated to be worth around \$100,000.

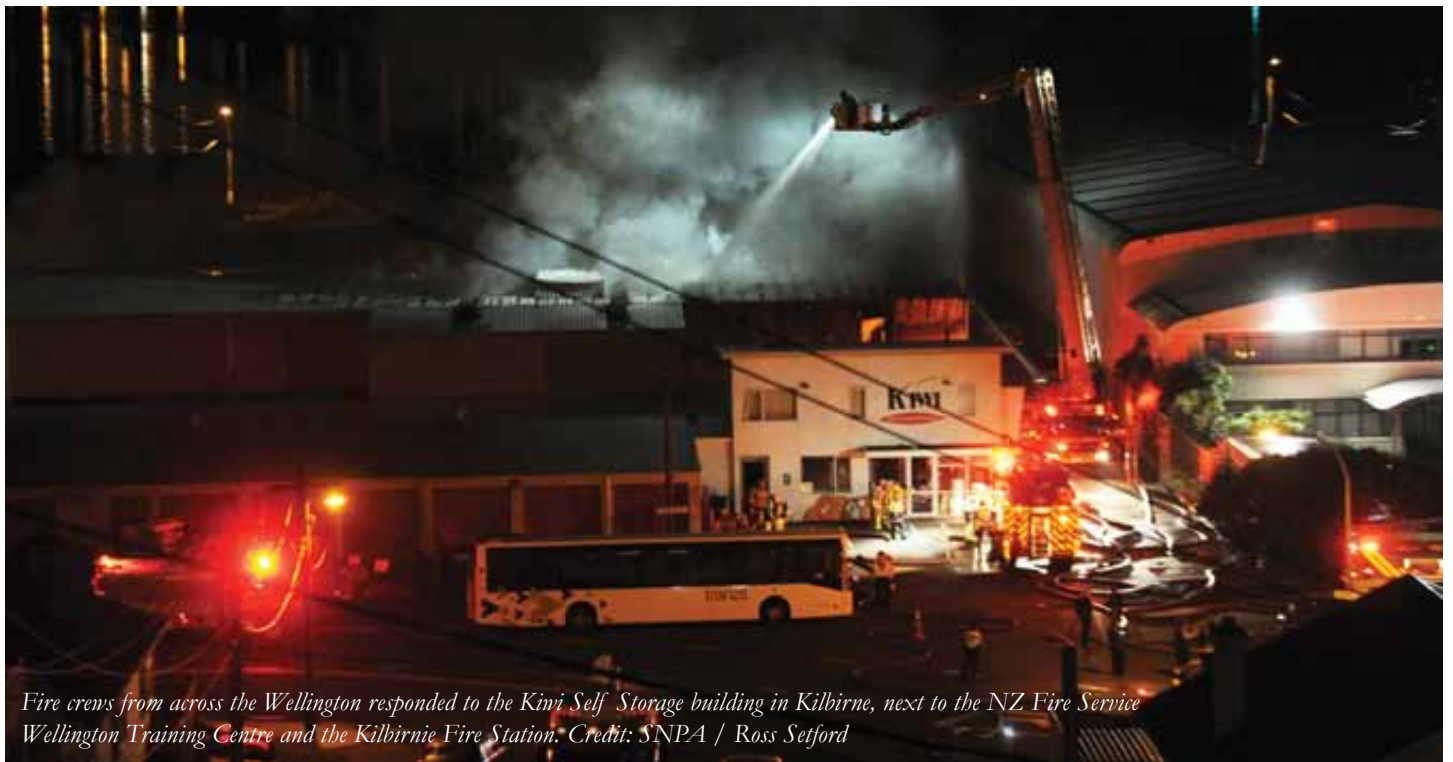
## **Un-named arsonist**

Within three weeks a 34-year old man appeared in the Wellington District Court charged with arson and was granted name suppression. He was remanded in custody to reappear for a jury trial in late July.

Kiwi Self Storage was cleared of any fault after it was confirmed in May that it met all Building Code requirements and compliance checks.

Although any likelihood of an imminent law change has been overshadowed by the upcoming elections, Simon Davis says the Ministry of Business, Innovation and Employment (MOBIE) is fielding inquiries about greater protection for storage facilities but waiting for all the reports before making a decision.





*Fire crews from across the Wellington responded to the Kiwi Self Storage building in Kilbirnie, next to the NZ Fire Service Wellington Training Centre and the Kilbirnie Fire Station. Credit: SNPA / Ross Setford*

He says the NZ Fire Service has regular meetings with MOBIE and the matter is effectively already on the agenda along with other concerns around the needs to clarify existing fire regulations.

The NZ Fire Service is conducting its own research into what could have been done better to prevent the Kiwi Self Storage blaze, looking at human behaviour, the performance of active and passive fire safety systems, the time it took fire trucks to arrive and get operating and the availability of water.

The research will determine if there's a theme or a pattern and result in a two page 'Heads Up' "executive summary" about the lessons that can be learned (<http://www.fire.org.nz/Research>) as part of its Fire Investigation Unit's "learning through loss" philosophy.

The focus will be on identifying any design process or material flaw that others can learn from to prevent this happening again.

As a result of similar investigations three heat transfer ventilation units from Weiss were removed from the market in June because of overheating and some Dyson AMO4/5 heaters were recalled because of a potential short circuit. "Those are the kinds of things we try to pick up," says Davis.

The NZ Fire Service and other investigations into the Kiwi Self Storage fire will be added to a list of concerns being raised with Government departments. Proposed changes will help clarify legislation, or the interpretation of it, where it has not been "as clear as it possibly could have been".

### **Buyer beware focus**

In the case of Kiwi Self Storage, Davis suggests end users need to be more educated about what they're getting for their money and learn to ask the right questions.

"They don't turn their mind to it, as the lawyers would say. It's got a key pad, locks and the property is secure from burglary but the question of fire safety probably doesn't occur. The more savvy person will say, "Oh hang on, I think I should go for a place that has a sprinkler rather than not".

While items were probably safe from a security perspective, he suggests business owners and their clients pay too little attention to fire risk. "In any business you are operating you have to look at what your risks are including security and fire."

Davis says the NZ Fire Service is caught between a rock and a hard place as the Government sets the target around life safety issues leaving it up to the owner to decide on building safety and optional levels of fire protection.

While many building owners and landlords recognise the benefits of installing sprinklers, others try and avoid this because of cost and ongoing compliance issues. "It's really up to the tenant or the operator of the building to either insist on or require that those are in there."

In some ways Davis says it's up to the insurance industry to determine the risk and require sprinklers or other types of suppression systems be installed.

He says insurance companies have risk assessors who look at individual premises

and the activities in those buildings. "I guess it's a commercial decision made around the premium... if fire safety features are required."

### **Too late when it happens**

Fire investigators are well aware of the typical response from building owners who didn't understand how fast a fire could spread or how black the smoke could be until it happened to them.

"People just don't expect the speed of fire and the dirtiness of the smoke because their everyday experience is with a controlled situation in a fireplace or barbecue."

He says the fire service is constantly battling perception problems. "We're far more likely to acknowledge the risk of riding a bike on the road, driving or swimming or silly things like getting attacked by a shark or being hit by lightning."

Davis muses that all fires are preventable, but it's the cost of preventing them that's the issue; "the cost benefit analysis that has to be robust".

A number of studies have been funded through the NZ Fire Service Contestable Research Fund, that show "with everything 'sprinklered' there would be very few fires at all but the cost to the country would be substantial".

Those costs are not just in the installation of systems but water supplies and all the other requirements to make them compliant and keep them maintained. "It would be uneconomic — market forces come into it as you weigh the sacrifices and benefits."

— Keith Newman

# Code changes give more options to protect community buildings

By Keith Newman

A critical adjustment enabling community halls, schools, marae and historic places to install sprinkler systems that are less likely to break the budget has been made to New Zealand Building Code Standards.

Currently New Zealand doesn't have a fire protection standard for community buildings or any requirement for them to have a sprinkler system. Even voluntarily installation raised compliance requirements so high that owners of

thousands of buildings regularly used by communities have opted for little or no protection.

Because these buildings are not considered domestic or residential, the standard activated in the New Zealand Building Code compliance document C/AS1 is the full sprinkler standard 4541:2007.

As a result of efforts by the Building Research Association (BRANZ) in conjunction with the NZ Fire Service and

the Fire Protection Association (NZFPA) an appendix to the Building Code was drawn up last year and adopted recently to permit alternative and previously non-complying methods of protection.

The resulting appendix to NZS 4541 allows for compromises that could save tens of thousands of dollars. The challenge was how to achieve a compliant system without compromising the correct operation and function of a sprinkler system?



*Less restrictive Building Code requirements make it more affordable to protect a school or community hall or historic buildings*

	<b>Marae - Manakau City</b>	<b>Baptist Church</b>	<b>Church</b>	<b>Remote Marae</b>	<b>Church</b>
Installations	\$39,100	\$33,500	\$17,000	\$62,600	\$30,000
Valves/gauges	\$6,500	\$10,800	\$7,600	\$55,200	\$8,400
Installations	\$39,100	\$33,500	\$17,000	\$62,600	\$30,000
Tank				\$95,000	\$60,000
Pumps				\$45,200	\$49,000
Town Main	\$13,300	\$4,800	\$18,000		
Design/certification	\$17,700	\$14,000	\$13,300	\$39,000	\$14,000
<b>Total</b>	<b>\$76,600</b>	<b>\$63,100</b>	<b>\$55,900</b>	<b>\$297,600</b>	<b>\$161,400</b>
Approximate area m <sup>2</sup>	1400	200	200	700	200

*Rounded budget for the cost of church and marae sprinkler systems based on figures from a sprinkler supplier. BRANZ*

### Lower cost options

Typically public assembly buildings capable of hosting 500 – 1000 occupants with floor heights from single floors to a maximum of 10 floors are not required to have sprinkler systems.

BRANZ proposed a framework allowing lower cost systems in buildings with a maximum of three floors, although at least two of those floors must have passive fire separations.

Until recently a sprinkler system to protect a small historic building of 61m<sup>2</sup> for example could cost \$13,000 and to protect a remote marae up to \$300,000. In many cases that required alarms and connections to the Fire Brigade.

It would also have meant complex valve systems rather than simple on-off or automatic release systems, concrete tanks, diesel pumps, compliant pipe systems, flow switches and jockey pumps to maintain pressure and detect leaks plus high tank capacity depending on the likely response time of the Fire Brigade.

BRANZ agreed some elements aren't up for negotiation including the number and type of sprinkler heads needed, the design, pipework and water demand alarms. However variations in water



*A 30,000 litre plastic storage tank may cost \$3,000-\$4,000 when compared to an equivalent concrete tank at \$60,000 - \$95,000*

supply, pumps, tanks and the control valve arrangement could result in significant savings.

For example using an electric pump rather than a diesel one can save \$20,000-\$30,000 in some cases although battery

back-up will cost extra (\$3,000-\$17,000). A 30,000 litre plastic tank alone can save between \$50,000-\$90,000 and a residential valve set rather than that previously stipulated for compliance can save up to \$6,000.



## All Risk on Owners

While welcomed by the NZ Fire Services, The Fire Protection Association (NZFPA) and many community groups, the appendix very clearly places all risk on building owners who are required to supply written acknowledgement that the solution is less reliable and less secure than that stipulated by the NZS451 Building Code requirement.

BRANZ Senior Engineer Ed Soja, who compiled the research for the original report, said “any compromise is negligible in that the sprinkler system will provide protection where none previously existed.”

BRANZ which led the charge for change as an incentive for building owners to protect their assets, collated information on fire risks and looked at fire incidents in marae, community halls, churches and other places of special interest over a 5-year period from 2005–2010.

Over this period there were 6,230 structure fires across all buildings. Of the 266 used in the BRANZ study 27 were destroyed. Although that was relatively low, less than one percent of all buildings structure fires in New Zealand, it was 24% of all assembly building fires.

In those fires, alarms were present in 25% of churches and community halls, and sprinklers were in approximately 2%. In marae-based premises 8% had alarms but none had sprinklers.

Although the relatively low number of fires suggested investing in sprinklers may not be cost effective, BRANZ suggested the cultural or historic value of buildings such as historic churches or wharehau, were of considerable value to the community and would benefit from sprinkler protection.

After seeking guidance from vested parties including designers, BRANZ put its research to the Standards New Zealand



*Rather than a diesel generated pump an electric pump can represent large cost savings*

Committee on sprinklers late in 2012 seeking a revision in the standard which was approved by mid-2014.



# AFAC14

## AFTER DISASTER STRIKES LEARNING FROM ADVERSITY

WELLINGTON 2-5 SEPTEMBER 2014



### The biggest emergency management conference in Australasia

## KEY ACTIVITIES

- 1-day all hazards Research Forum: 2 September
- 2-day conference: 3-4 September
- Gala Dinner: 3 September
- 4 Professional Development Workshops: 5 September
- 4 Field Study Tours: 5 September

The conference will explore the following major themes:

- Climate, Landscape and Environment
- Impact of Disasters
- Supporting our People Through Adversity
- Building Capability
- Involvement of Emergency Services in Recovery
- Resilience

**Early bird registrations close 27 June 2014**  
Full conference program and to register  
[www.afac.com.au/conference](http://www.afac.com.au/conference)

The New Zealand standards and Building Code are very clear about the requirements for automatic fire sprinkler systems in commercial buildings (NZS 4541:2007) and the kinds of sprinkler systems for apartments, motels, hotels and hospitals where people sleep overnight (NZS 4515:2009).

While there is a standard for domestic dwellings (NZS 4517:2010) there is no regulatory requirement to ensure sprinklers are installed in homes or smaller community buildings.

## NZFPA OK with Existing Sprinkler Laws

The New Zealand Fire Protection Association (NZFPA) has no plans to lobby Government to mandate the installation of fire sprinkler systems in buildings outside the provisions of existing building regulations.

NZFPA fire protection engineer, Ian Makgill, says many prominent fire protection engineers and selected NZFPA members engaged in intense debate with Building Industry Authority (BIA) representatives from the late 1980s who wanted selected provisions in NZS 4541 removed.

The challenges, leading up to the Building Act 1992 becoming law, were around what was deemed to be for property protection rather than life safety. “The stalemate was broken by the insertion of Appendix D in Section C/AS1 in the acceptable solutions section,” says Makgill.



The NZFPA is confident that the current suite of Fire Sprinkler System Standards provides a reliable, cost effective means to mitigate the risk of fire and are constantly being reviewed against international standards and evolving fire risks.

Makgill says the level of fire safety features in the majority of commercial buildings is “the minimum prescribed” in regulations, although others have exceeded this to protect property and mitigate other risks.

He says New Zealand’s life and fire safety record in buildings is “among the best in the world”.

Mandatory Building Regulations, largely geared to protecting occupants, require automatic fire detection systems, automatic fire alarms, automatic fire brigade signalling and fire resistant construction to ensure people have time to evacuate to a safe place.

Makgill says the majority of buildings used by the public contain some level of mandatory fire safety features subject of the Building Warrant of Fitness (BWOF) which the owner is responsible for maintaining under threat of significant penalties.

Over the past decade many community buildings have opted for sprinkler

protection to the accommodation-based NZS 4515 standard to mitigate the “increasing occurrence of arson.”

While this standard is less costly to comply with it is not appropriate for property safety in community buildings for a variety of reasons including water supply and the surface finishes and type of material used in construction.

NZS 4515 systems are designed for life safety and a 10 minute window for evacuation and “does not presume fire brigade attendance to assist with evacuation”.

FPANZ, however, endorses the inclusion of Appendix B into NZS 4541 2013 in relation to the protection of community buildings, enabling more affordable systems to be considered compliant.

“The addition of Appendix B provides guidance for an appropriate sprinkler system design and installation for community buildings, to protect property on a voluntary basis but still needs a Building Consent,” says Makgill.

### **Evolution of Standards**

The NZFPA says Fire Sprinkler Standards have evolved over the last 100 years to provide reliable and cost effective fire suppression.

Initially the development of these standards, initiated by building owner co-operatives and insurers, were to protect property, although they were not mandated by law, but “an act of prudent risk mitigation by owners and a condition of Insurance”.

At that time the safety of lives in buildings protected by sprinklers was a by-product of property safety. “Following the disastrous Seacliff fire in 1948 the Government, in a world first, decreed that all institutions containing incarcerated people, and all Crown-owned buildings be protected by a sprinkler system.”

As a result sprinkler systems became increasingly mandated by International Building Codes to mitigate the risk of fire in buildings and as a fire safety measure. By default, the ‘life safety features’ in a building may provide protection of the building and its contents from the effects of fire.

Makgill reiterates, that it is up to the individual to decide what additional fire safety precautions they wish to have to protect their property from fire. “It is strongly recommended that any decision on fire safety be taken in consultation with the Insurer of that property where appropriate.”

**– Keith Newman**





## Power supply cabinets

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

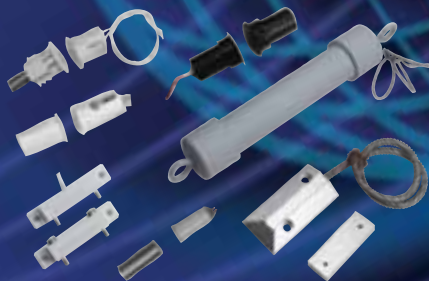
**Designed, tested and produced in New Zealand.**



**Loktronic**

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

20238\_PSC



## total reed switch solutions from Flair

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

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

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

**Loktronic**

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

20237\_FL



## Loktronic for power supplies

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

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

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

**Loktronic**

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

20757\_BP



**ASSA ABLOY**



**FUJINON**



**NETGEAR**

Auckland: (09) 415 1500 • Fax: (09) 415 1501 | Wellington: (04) 803 3110 | Christchurch: (03) 365 1050 | E



## Loktronic for gate locks

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

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

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

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



**Loktronic**

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

20756\_BP



## Key switches

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

Momentary contact (90°)

Turns 90° clockwise from vertical to turn on

Maintained contact (180°) locked on or locked off

Turns 90° clockwise from vertical to turn on

Turns 90° anticlockwise from vertical to turn off

SPDT switch 5amp rating

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

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

Supplied random keyed. Can be master keyed.

Client's own key cylinder can be converted.

Front or rear fixing.

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



**Loktronic**

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

20681\_KS

## Loktronic Power distribution module



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

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

**Comprises**

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

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



**Loktronic**

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

20239\_PDM





### Open Platform VMS

- Award-winning best open platform VMS
- Advanced built-in Video Analytics
- Micromodule crashproof software architecture
- ITPLUS are exclusive NZ distributor for Axxonsoft Solutions

RESELLER ENQUIRIES WELCOME



Ph: 09-950 4940 | E: info@itplus.co.nz  
www.itplus.co.nz



### Wireless IP Surveillance

- Cost-effective high-performance wireless access points for outdoor use
- Stockists of AirMax, AirFiber, AirVision, UniFi & mFi series products
- ITPLUS are a Ubiquiti certified and trained partner

RESELLER ENQUIRIES WELCOME



Ph: 09-950 4940 | E: info@itplus.co.nz  
www.itplus.co.nz



### IP Video Transmission

- Storage systems for video surveillance
- Ethernet over Coax devices
- Ethernet and PoE extension devices
- Networked video integration devices
- IP camera installation tools

RESELLER ENQUIRIES WELCOME



Ph: 09-950 4940 | E: info@itplus.co.nz  
www.itplus.co.nz

**AIPHONE**



**BOSCH ZoneTechnology**  
Your Security Supply Partner

mail: sales@zonetechnology.co.nz | www.zonetechnology.co.nz



### IP Video Intercom

- Wide range of single villa to multi-apartment stations options
- Wide range of control panels with / without phone handsets
- 1.3MP camera on station units
- Control panels also capable of communicating with Dahua IP CCTV cameras
- 2 years b2b warranty

RESELLER ENQUIRIES WELCOME



Ph: 09-950 4940 | E: info@itplus.co.nz  
www.itplus.co.nz



### HD-SDI CCTV

- Wide range of true-WDR full-HD (1080P) HD-SDI cameras
- Wide range of low to medium to high-end HD-SDI DVRs
- HD-SDI accessories
- Built-in DDNS client and user-friendly GUI on DVRs
- 3 years b2b warranty

RESELLER ENQUIRIES WELCOME



Ph: 09-950 4940 | E: info@itplus.co.nz  
www.itplus.co.nz



### Smart IP Access Control

- Wide range of standalone to fully scalable IP based access-control devices
- Reader/controller units also available on Weigand & RS485
- Fingerprint, Facial & IRIS based access control
- RFID & Keypad based access control
- 2 years b2b warranty

RESELLER ENQUIRIES WELCOME



Ph: 09-950 4940 | E: info@itplus.co.nz  
www.itplus.co.nz

**Loktronic**

SECURITY • TECHNOLOGY • RELIABILITY

# HOLD ON A MINUTE

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

**Not all products are created equal.**

Take Loktronic's premium quality Fire Door Holding Electromagnetic FDH40... they are simply the best in their field.



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



FDH40S: Standard, floor mounted



FDH40SS: Flush mounted



FDH40SS: Surface mounted



Designed, tested  
and **produced in NZ**  
to AS4178

**10 year guarantee\***

**Unbreakable**  
universal mounting

**Floor or wall**  
mounting options

**Superior quality**  
materials  
and fastenings

**Full and immediate**  
**on-shore support**

**Loktronic**

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

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

\*Standard terms & conditions of sale apply.