NZSM

New Zealand Security Magazine

June 2026

How to write a (very good) NZ Security Awards nomination

Race to the Bottom: Europe's security industry just like us

John Wick and the art of physical security risk management

www.defsec.net.nz

Loktronic

Loktronic Limited 36 years servicing NZ's Security Industry
SINCE LNZ 1989

Three great brands that stand for QUALITY and VALUE

Loktronic

LOKTRENZ

ViTECH

from Loktronic Limited

SERVICE and SUPPORT drive us.

Loktronic

Loktronic Limited Unit 7 19 Edwin Street Mt Eden Auckland 1024
Ph 64 9 623 3919 • Fax 64 9 623 3881 • 0800 FOR LOK
mail@loktronic.co.nz • **www.loktronic.co.nz**

ventia

Keeping essential infrastructure **working for our communities.**

At Ventia we work around the clock to deliver essential services that keep Aotearoa moving. We deliver catering and hospitality services and integrated asset management to critical infrastructure including defence bases, hospitals, roads, telecommunications networks, and community facilities.

Visit **ventia.co.nz** to find out more.

Call 0508-**VENTIA (836 842)**

ventia.co.nz

CONTENTS

DEFSEC
NEW ZEALAND - PACIFIC
DEFENCE - SECURITY - SAFETY

Contact Details:

Chief Editor, Nick Dynon
Phone: + 64 (0) 223 663 691
Email: nick@defsec.net.nz

Publisher, Craig Flint
Phone: + 64 (0)274 597 621
Email: craig@defsec.net.nz

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

Upcoming Issue

July 2026
Outstanding Security Performance Awards, Advanced Analytics and Artificial Intelligence, Security of Critical Infrastructure

Social Media

linkedin.com/company/defsec-media-limited

ISSN Online 2537-8937

NZSM
New Zealand Security Magazine

Nick Dynon
Chief Editor

Nick has written for NZSM since 2013. He writes on all things security, but is particularly fascinated with the fault lines between security and privacy, and between individual, enterprise and national security.

Prior to NZSM he clocked up over 20 years experience in various border security and military roles.

Kia ora and welcome to the June-July 2026 issue of New Zealand Security Magazine. With this issue, we hit the Winter months with the first in a series of changes designed to get your NZ security sector news and analysis to you quicker than ever.

NZSM has typically been published on a bi-monthly (every two months) basis, but from this issue onwards the magazine will now be published monthly!

That's right! We've made the move from six magazines per year to twelve.

This means that each issue of the magazine will be shorter than the previous benchmark length of 48 pages, but they will be more frequent so that you don't have to wait a whole two months between issues.

Another change you'll notice with this issue is that each of its articles will be available to read simultaneously in the magazine as well as on the Defsec website as individual article posts. You choose how you wish to engage with our content.

Consequentially, you can also expect the frequency of our e-newsletters to increase. If you don't subscribe to **THE BRIEF** already, I recommend that you visit www.defsec.net.nz to sign up!

Leading this latest edition of NZSM is an update to an article we publish each year on how to write a good nomination for the **New Zealand Security Awards**. As a former awards judge, I've seen the good, the bad, and the ugly of nominations, so this article serves as a guide to submitting a compliant and competitive nomination that does justice to your nominee.

In the latest editorial offering from the good folk at **ICARAS Security Consultants**, we're provided a master class on what John Wick and the New Zealand Government's Protective Security Requirements (PSR) have in common. It's funny stuff, but it makes good sense too – and that's the beauty of it. You won't look at the PSR the same way again!

Also in this issue, recent **International Security Ligue** research out of Europe analyses the raw data of 40,000+ bid announcements and contract awards for security personnel services, finding that tender processes continue to prioritise lowest-cost bids over quality, capability, and long-term value. A race to the bottom. Sounds familiar?

If New Zealand wants to meaningfully address image-based sexual abuse in the age of generative AI, we have to go further than criminalising it. That's what **Dr Cassandra Mudgway** from the University of Canterbury, argues in her piece that explores the Deepfake Digital Harm and Exploitation Bill currently before Parliament.

Plenty more commentary and news in this issue of NZSM, including some significant career milestones, OSPAs finalists, a birthday for Inception, a win for Nextro, SecTech, and Brazilian Jiu-Jitsu.

Keep safe.
Nicholas Dynon,
Lincoln.

Make it Count: Nominating for the 2026 New Zealand Security Awards

If you're thinking you have a colleague who might be worthy of a New Zealand Security Award, nominate them, writes chief editor Nicholas Dynon, but make sure your nomination is a compliant and competitive one.

Nicholas Dynon is chief editor of NZSM, and a widely published commentator on New Zealand's defence, national security and private security sectors.

Nominations for the 2026 New Zealand Security Industry Awards open on Monday 29 June. This year will culminate in a gala awards dinner at the Parliament Buildings, Wellington, on Friday 11 September.

For the past few years now I've published an article in the August issues of NZSM to provide advice – from my perspective – on how to make your nomination count, and with this year's nomination deadline looming it makes sense to again reiterate the tips and tricks. If you're planning to nominate, you should continue reading!

When I sat on the judging panel some years ago, I tended to find myself on the one-hand inspired by the many impressive nominations I saw, yet frustrated by the abundance of pretty ordinary ones.

In the vast majority of cases it wasn't that the nominee wasn't up to scratch, but rather that the nomination itself was either non-compliant, poorly put together, or inadequately evidenced.

Nominating a colleague for an award is a good thing – for two reasons. Firstly, excellence should be recognised, and outstanding individuals within the industry should be celebrated. Secondly, quite simply, the more nominations submitted in a particular category the more competitive the pool

and the more worthy the winner. That's a good thing for the industry.

In this article, I offer my perspectives on what makes a competitive nomination, including some tips on how to ensure you've given your nominee an even chance of being among the finalists.

Ensure your nomination is compliant

If you've taken the effort to identify a colleague for nomination, then it's important that you make that nomination count. A good place to start is to ensure that your nomination is fully compliant with the Conditions of Entry (Terms and Conditions). If you don't know what these are, it's worthwhile acquainting yourself with them.

Golden rule. Make sure your nomination is prepared and submitted well in advance of the close off date (5.00pm on Friday 14 August 2026). Late entries are not accepted, and you don't want to take the time to prepare a nomination only for it to be disqualified at the starting blocks.

The other key dates to keep in mind are April 2025 to June 2026. Nominations must relate to work, employment or activity carried out within this 15-month period. By all means mention relevant pre-April 2025 milestones for backstory and context, but avoid going too far down that rabbit hole. The judges are required to assess work and achievements that fall specifically within the past 15 months.

Each nomination must contain a fully completed nomination form in the format provided, including a testimonial not exceeding 1,200 characters describing why "the nominee has the attributes and professional experience that would make them a deserving recipient of the award". Supporting information may be uploaded with each nomination but limited to two files per nomination with a maximum file size of 2MB per file.

I've seen too many nominations that failed to follow the required format. Worse still, I've seen too many where the nomination was nothing more than a short paragraph two or three sentences in length. Something like this gives the judges nothing to assess. It's an immediate fail.

The most disappointing example of this I've seen was in relation to a nominee who I believe would likely have won their category if their nominator had gone to the effort of writing more than just a sentence or two. In the interests of fairness, the judges can only consider information in the papers before them even if they are otherwise aware of the exploits of the nominee.

Put in the effort; aim for excellence

The New Zealand Security Awards are all about recognising and celebrating excellence. If you don't aim for and achieve excellence in your preparation of a nomination, then it logically follows that the judges will struggle to see excellence in your nominee.

I recommend that you read the tips on the NZSA website's Nomination Information and Conditions of Entry pages. They contain useful tips.

One of these is to directly address each of the 'recognition requirements' specified in the category criteria in a clear and concise manner. For example, in the Guarding Sector Trainee of the Year category, the category criteria require the individual to demonstrate that:

This award recognises an individual who has made outstanding progress in professional development and training for their role in the guarding sector of the security industry. They will have displayed commitment towards training and achieving results though the NZQA national qualification framework. The recipient will be a person who is self-motivated, sets goals and aspires to progress their security career.

The NZSA recommends that responses to each of the recognition requirements be addressed individually, in the order listed within the Category Criteria (with the use of headings or bullet points to ensure they are easy to follow), and as clearly and concisely as possible.

If we were to split the above example into its individual recognition requirements, I'd suggest that this results in:

- Outstanding progress in professional development and training,
- Achieving results through the NZQA framework, and
- Self-motivated, and career goal oriented.

Read the category criteria carefully. The two trainee categories, for example, require that the nominee has "displayed commitment towards training and achieving results through the NZQA national qualification framework." If you're thinking of nominating someone for this category, confirm that they are indeed displaying commitment towards NZQA training rather than forms of training not relevant to that framework.

In order to systematically and fairly assess nominations, the judges award points in relation to each of the specified recognition requirements. It is therefore very important that each one is responded to.

It's also important to demonstrate exactly how a nominee meets each of the recognition requirements by way of specific examples, stories and references. These can be supported by attachments to the nomination. Note that the online nomination form allows for a maximum of only 5,000 characters, so make the most of the attachments (two documents with a maximum file size of 2MB – these are for customer references/testimonials and/or metrics only).

If this sounds like a whole lot of effort, that's because it is! The judges do not want to be reading War and Peace, but putting a nomination together does require you to get a reasonable amount of information across in a convincing way. Don't underestimate the task.

Be prepared to write, but stay on message. Take care to avoid getting side-tracked with superfluous or unnecessary information and detail. None of the categories require the nominee to enjoy footy or boating in their spare time.

Don't undersell your nominee, but be careful to avoid making hyperbolic statements about them without associated evidence. Overuse of superlatives and hyperbole cheapens a nomination and calls into question its credibility.

For example, if your customer champion nominee is indeed "viewed as providing a substantial and quantifiable benefit to the customers business operations", then how so? What are some specific examples of the quantifiable benefits your nominee has provided?

Think about the type of evidence you should be submitting to back up your claims. The evidence should be as objective as possible. Relevant metrics/statistics and external stakeholder testimonials can constitute compelling evidence, but they can take time to collect – so don't leave your nomination to the last minute.

I concur with the NZSA's recommendation that you get your nomination proof read by a third party prior to it being submitted, ensuring that it reads well, addresses all of the category criteria and effectively 'sells' the merits of the nominee. This is critically important – a second pair of eyes can make all the difference.

Also, be aware that there may have been some slight changes to the assessment descriptors in some of the categories since the last time you put together a nomination. Make sure you're nominating your nominee against the current criteria!

A word about categories

There are 18 categories to choose from, which seems like a lot. But given the diversity of sectors and roles within the industry, it's not a long list. Take care to select the most appropriate category for your nominee.

That being said, sometimes a nominee might – in your opinion – be a potential contender across more than one category. There's no harm in submitting separate nominations for the one individual across multiple

categories, but if you do just make sure that each of the nominations are tailored to the specific category criteria.

For the NZSA, getting the categories right is a perennial challenge, and in recent years there's been plenty of tweaking in this regard. Categories such as 'Cash Services Professional of the Year' and 'Visionary Leadership', for example, were jettisoned a couple of years back in favour of the newer categories of 'Customer Champion of the Year' and 'Security Specialist of the Year'.

2024's "Outstanding MSD Placement Candidate of the Year" category, which had replaced 2023's "Outstanding Skills for Industry Employee of the Year" category, was axed last year. This resulted in there being one less category in 2025 compared to the previous year.

Such changes occur for any number of reasons, including changes to industry programmes, evolutionary changes in practices, feedback from the industry and whether or not the category attracts a sufficient number of nominations. Change is the natural order of things, so don't assume a category you've previously nominated someone in is either unchanged or still there at all.

If in doubt, have a go!

There can be a lot of preconceived ideas when it comes to the awards. Some people see them though a tall poppy syndrome lens, while others see them as little more than a marketing exercise. Such perceptions are unreasonably cynical and wrong.

Some employers don't nominate their people for awards because they think that an award-winning employee is more likely to be poached by competitors. If that's their fear, they're clearly doing something wrong.

Disappointingly, there are some conspiracy theorists in the industry who peddle the fiction that awards sponsors are somehow more likely to end up winning an award. If you look at the sponsor lists going back several years, you'll see that many of them didn't actually field any nominees or record a win. Such baseless speculation is dumb, and it does a disservice to the industry and, in particular, to the volunteer judging panel.

There also exists a misperception that only nominees who are 'super heroes' win awards. This is false. In the main, finalists and winners are really just people who meet the category criteria really well through their commitment and hard work.

For the Patrol Officer and Security Officer of the Year categories specifically, the criteria do state that the award recognises excellence, commitment and professionalism "including service to customers and outstanding acts." And here we do often find amazing stories of bravery, compassion, and heroism, although they are not a prerequisite.

Results in recent years do seem to indicate that "outstanding acts" tend to trump "service to customers", and the measure of "outstanding" is often pegged to the level of danger faced by the nominee during the act in question.

In Australia, such acts are covered by the Australian Security Valour Medal (ASVM), a category within the Australian Security Medals Foundation (ASMF) Awards, which, in turn, is part of the annual Australian Security Industry Awards. In my opinion, acts of valour or heroism are indeed worthy of a medal, and – as I wrote last year – I believe there is a case for a similar annual medals-based award in Aotearoa New Zealand in accordance with a framework similar to the ASMF.

It's worthwhile noting, however, that recipients of the NZSA's Saved a Life Medal (which are awarded at times during the year) will be honoured with a roll call at the New Zealand Security Awards night and automatically included as a nominee under the appropriate award category.

Lastly, if you haven't nominated someone for an award previously, have a go. The New Zealand Security Awards is an important annual event not just because it's a stage upon which to acknowledge high performing colleagues. It's a showcase of our industry to the broader community, and an enduring record of the wonderful stories of excellence expressed in the nominations you submit.

Make this the year you get nominating. If you're thinking about nominating a colleague but you're a little unsure whether to do so, just do it!

Finalists announced for the 2026 New Zealand Outstanding Security Performance Awards

With a panel of independent experts from across the New Zealand security industry concluding its, the finalists of the 2026 New Zealand Outstanding Security Performance Awards (OSPAs) have been revealed.

The New Zealand OSPAs, returning for its fifth year, has attracted its highest number of entries, with its judging panel having faced a challenging task in narrowing down the submissions to select only the very best.

"We are delighted to return to New Zealand once again and are encouraged the entry numbers are growing each year," said OSPAs founder Professor Martin Gill.

"All those that have made it to the finalists list should be very proud, as only those that reach a score threshold go forward to the next phase of the competition."

The 2026 finalists are:

Outstanding In-House Security Manager/Director
Kurtis Heketoa – Te Whatu Ora – Counties Manukau
Riaan Kruger – Southern Cross Healthcare
Charlie Tukuafu – Port of Auckland

Outstanding Contract Security Manager/Director
Anna Barragan – Global Security Solutions
Rana Taimur Anwar – P4G Security
Pat Wulf – Wulf Security

Outstanding Security Team
Port of Tauranga Security Team – ABL Group
CM Health Team – Optic Security Group
Kowhai Park Solar Farm Construction Security Team – P4G Security
Secom Guardall New Zealand
Profit Protection Team – The Warehouse Group

Outstanding Contract Security Company (Guarding)
Global Security Solutions
Red Badge Group
Secureflight
Wulf Security Services

Outstanding Security Consultant
Nathan Hauraki-Cray – Global Security Solutions
Chris Kumeroa – Global Risk Consulting
Rehan du Toit – Beca Applied Technologies
Lee Turpitt – Watchu Security

Outstanding Security Installer/Integrator
Advanced Security Group
Semih Dikmenli – DC Security
Daniel Malan – Global Security Solutions
Millennium Technology
Nedax Systems NZ
Secom Guardall New Zealand

Outstanding New Security Product
Hub BP Jeweller – Ajax
DoorBell – Ajax
MotionCam Outdoor HighMount (PhOD) Jeweller – Ajax
AccessNow – Gallagher
gxStorAccess – Millennium Technology

Outstanding Security Partnership
Profit Protection Future Forum – NZ Committee Members
Red Wolf High Level Security and Rabobank
The Warehouse and Leading Solutions

Outstanding Security Officer sponsored by Guardhouse
Wayne Lee – The Warehouse
Manjinder Singh – Global Security Solutions
Samisoni Taufoou – Wulf Security Services
Carly Watson – Secureflight

Outstanding Female Security Professional
Eteta Chung-Anthony – Global Security Solutions
Amy Hoyne – Beca Applied Technologies
Michelle Macdonald – Secureflight
Rainbow Manley – October Protection
Kristina Rabbitt – Advanced Security Group
Jennifer Radonich – The Warehouse Group
Kylie SaintClaire – Auckland Council
Harriet Sommerville – Gallagher
Katalina Vete – Wulf Security

Outstanding Young Security Professional
Anthony Charlton – Secureflight
Simon Mackereth – Red Badge Group
Pushpinder Singh – Global Security Solutions
Joseph Teremoana-Tere – Wulf Security Services

Protege GX cybersecurity changes: What you need to know

ICT has announced a new series of quarterly Protégé GX updates aimed at delivering stronger protection by default. The first update is available now.

In the first of a new series of quarterly updates, Protege GX 4.3.402 receives bolstered security with stronger password defaults, encrypted connections (TLS 1.2/HTTPS), and a new path forward for browser-based access.

According to ICT, there are a few things you'll need to do when upgrading existing sites. At a high level:

- Plan to upgrade server, clients, SOAP and web client together
- Confirm encrypted connections are in place before the upgrade
- Notify operators they'll need to set a new password at next login
- Decide whether to upgrade the legacy Web Client or move customers to the new Web App

The headline rule: upgrade everything together. Server, clients, SOAP, and web client need to move at the same time. If they don't, parts of the system won't communicate.

What's changing

Stronger passwords by default. ICT is tightening operator password requirements so every Protege GX system starts from a stronger baseline. After upgrading, operators will be prompted to reset their password the first time they log in — a quick, one-time step.

This applies to operator accounts used by SOAP integrations and mobile apps as well, so it's worth identifying those ahead of time. Those applications will fail to connect until the passwords are updated.

Protege GX components will now only talk to each other over encrypted connections — TLS 1.2 between server, clients and SOAP service, and HTTPS for web client, entry station, and mobile app traffic.

For sites already running encrypted communications, this is business as usual. For sites still running unencrypted connections, some setup work is required prior to upgrade.

There's also a server compatibility check worth doing early: 4.3.402 requires a 64-bit OS and a current SQL Server version (2016 or later). Most sites will already be there, but older installs may need a server migration as part of upgrade planning.

Together, these changes line Protege GX up with what IT and security teams now expect by default: encryption in transit and strong credential hygiene out of the box.

A new option: the Protege GX Web App

This release coincides with the general availability of the Protege GX Web App — ICT's modern web-based replacement for the legacy Protege GX Web Client.

ICT will be rolling out feature parity with the legacy Web Client over the coming months. This means that when upgrading a site, you currently have two paths open to you:

- Stay on the legacy Web Client and apply the encryption updates, or
- Move to the new Web App as the web access experience going forward

If your customers rely on specific Web Client features, the Protege GX Web App Installation Manual has the current feature comparison so you can decide which path fits each site.

More detailed information is available from the ICT website and App Note 366.

Nextro wins NZ Project of the Year at Axis Oceania Partner Awards 2026

Nextro takes out the Project of the Year - New Zealand award at the annual Axis Communications Oceania Partner Summit on Australia's Gold Coast.

Auckland-based integrator and managed network and security services provider Nextro has been awarded Project of the Year - New Zealand at the Axis Communications Oceania Partner Awards 2026.

The awards, which recognise outstanding partner and distributor achievements delivered throughout 2025, were held at a gala awards celebration during the annual Axis Oceania Partner Summit on Queensland's Gold Coast between 05 and 08 May 2026.

Hosted under the theme "Unite & Ignite for Growth", the awards celebrated excellence in innovation, collaboration, customer outcomes, and business growth across the security and technology industry.

Nextro was recognised for its successful delivery of a significant physical and electronic security project for a New Zealand critical infrastructure client, showcasing the Nextro team's ability to design, integrate, and deploy complex security solutions that deliver measurable outcomes for customers operating New Zealand's critical infrastructure.

"Winning the Project of the Year for New Zealand is a tremendous honour and reflects the capability and dedication of the Nextro team," said Martyn Levy, Managing Director, Nextro.

"This award is a testament to the trust our clients place in us to deliver complex, mission-critical, security projects," he continued. "We are proud to be recognised by Axis Communications for the outcomes we have achieved together for New Zealand's critical infrastructure organisations."

This is not the first time Nextro has been recognised on the Axis Oceania awards stage. At the 2024 Axis Oceania Partner Awards on Denarau Island, Fiji, Nextro was awarded both the Fastest Growing Partner of the Year - New Zealand and the Partner of the Year for the Transportation category - New Zealand, underscoring the company's rapid growth and sector expertise across transportation and critical infrastructure.

Nextro is also Genetec's top and multi award-winning partner in New Zealand - and the critical infrastructure project that won the award was a unified solution built on Axis and Genetec platforms.

"We are incredibly proud to celebrate the achievements of our partners across Oceania," said Wai King Wong, Regional Director Oceania, Axis Communications.

"This year's summit was centred around the theme 'Unite & Ignite for Growth,' and these award winners truly represent what that means in action - innovation, collaboration, resilience and a commitment to delivering exceptional outcomes for customers across our region. The strength of our partner ecosystem continues to be one of our greatest advantages."

Among the Partner of the Year category winners were Convergint (Oceania), Advanced Security Group (NZ), ARA Security (NSW), and Optic Security Group (ACT), with Channel Ten Security Imports taking out Distributor of the Year – New Zealand.

Emergency management technology upgrade earmarked for Budget 2026

The Government has announced new investment in emergency management systems through Budget 2026, aimed at improving response times, coordination.

Emergency Management and Recovery Minister Mark Mitchell said the funding will address current limitations in how emergency management data is collected and shared, noting that existing systems are fragmented and can delay access to critical information.

"This investment will ensure faster, more effective response and recovery, better situational awareness and coordination across agencies, and reduced harm to New Zealand communities from hazards such as storms, floods and earthquakes," said Mr Mitchell.

Central to this is the delivery of modern technology platforms that will enable the development of a Common Operating Picture (COP), which will provide emergency personnel with a shared, real-time view of information such as hazard maps, evacuation data, infrastructure status, population distribution, and available resources.

The COP is designed to ensure that personnel across agencies and locations have access to consistent, up-to-date information, supporting decision-making before, during, and after emergencies.

The COP forms part of the broader Emergency Management Sector Operational Systems (EMS-OS) programme. In addition to shared situational awareness, EMS-OS will introduce tools to support operational tasking, inter-agency collaboration, and resource management throughout response and recovery phases.

Emergency Management and Recovery Minister Mark Mitchell

The programme also includes upgrades to the National Warning System, with the aim of improving the speed and accessibility of public alerts during emergencies.

The Government has indicated that EMS-OS will explore the use of automation and artificial intelligence to assist in processing large volumes of information during major events. Potential applications include the analysis of satellite imagery and spatial data following earthquakes, floods, or severe weather.

"For example, after a major earthquake, flood or severe weather event AI-assisted analysis of satellite imagery and spatial data could help identify areas were buildings, roads, bridges, or other critical infrastructure may have been damaged," said the Minister.

Such analysis could assist responders in identifying impacted areas, prioritising ground assessments, and informing decisions related to access, welfare, and recovery planning.

The country's exposure to natural hazards, including earthquakes, storms, and flooding, has been cited as a key driver for the investment. The Government expects the new systems to improve situational awareness, enhance coordination across agencies, and support more effective response and recovery efforts.

The EMS-OS programme sits alongside other planned reforms, including the proposed Emergency Management Bill and the Strengthening Emergency Management Roadmap, which Cabinet has agreed to in principle.

According to the Government, the combined programme of work is intended to strengthen the overall emergency management system and improve the country's ability to respond to and recover from major events.

Race to the Bottom: European report evidences what we already know

Latest International Security Ligue report into the procurement of security personnel services in Europe finds misalignment between procurement practices and the operational realities of modern security delivery, writes Nicholas Dynon.

Procurement of Security Services – Europe analyses the raw data of 40,000+ bid announcements and contract awards for security personnel services, finding that tender processes continue to prioritise lowest-cost bids over quality, capability, and long-term value. A race to the bottom. Sounds familiar?

"Across Europe, price remains overwhelmingly dominant in procurement decisions for guarding services, with an average weighting of 85% since 2018," states an International Security Ligue introduction to the report.

"This places security procurement closer to refuse collection and cleaning services than to other professionalised service categories — despite the mission critical nature of security work and the risks associated with contract failure."

While the report notes that although this approach is often justified under public procurement rules designed to ensure transparency and fairness, it systematically undermines service quality.

When contracts are awarded primarily on cost, providers are incentivised to reduce wages, limit training investment, and operate with minimal staffing resilience. This is a particularly perverse outcome for providers of security personnel – a labour-intensive sector highly dependent on training, supervision, and organisational culture.

Unsurprisingly, the report identifies a correlation between low-cost procurement models and higher rates of staff turnover, reduced professionalism, and inconsistent service delivery. In high-consequence environments—such as transport hubs, critical infrastructure, and crowded places—this can translate into degraded situational awareness and slower response times.

Despite this, the report also highlights signs of a growing importance of compliance and professionalisation within Europe's security sector, with buyers increasingly expected to consider labour conditions, regulatory compliance, and corporate governance.

But they are green shoots only. These considerations are often inconsistently applied, says the report, particularly where procurement teams lack specialist understanding of security operations.

Procurement-security disconnect

One of the report's more significant insights is in relation to the disconnect between procurement functions and security outcomes.

In many organisations, procurement decisions are made by generalist procurement teams with limited input from security professionals. This invariably results in contracts that are poorly aligned with operational requirements, lack appropriate performance metrics, or fail to account for emerging threats.

Accordingly, the report argues that security procurement should be treated as a strategic function that requires close collaboration between procurement specialists and security leaders in order to be done right.

Role of technology

The role of technology further complicates the procurement landscape, says the report. The integration of advanced surveillance systems, analytics, and automation is reshaping the delivery of security services. However, procurement frameworks have not always kept pace.

Contracts are often structured around traditional guarding models, with limited flexibility to incorporate technology-enabled solutions, inhibiting innovation and locking organisations into outdated service models – the traditional physical security versus electronic security dichotomy.

The report calls for procurement approaches that are outcome-focused rather than input-based, enabling providers to propose integrated solutions that combine personnel, technology, and intelligence. It's a suggestion whose time has well and truly come.

Contract length

Short-term contracts, often driven by procurement cycles, can discourage investment in training, technology, and workforce development, the report

found. Security providers operating under uncertain contract horizons are less likely to invest in long-term capability building.

Longer contract durations coupled with robust performance management frameworks, it points out, can create incentives for continuous improvement and innovation.

Impact on working conditions

The report also examines the impact of procurement practices on workforce conditions. Despite being the backbone of service delivery, security officers' working conditions are heavily influenced by procurement decisions that aren't made with them in mind.

Low-cost contracts tend to lead to lower wages, reduced job security, and limited career progression. This, in turn, affects recruitment and retention, exacerbating skill shortages in the sector.

The report positions workforce quality as a critical determinant of security outcomes, arguing – perhaps ambitiously – that procurement models must explicitly account for labour standards and professional development.

Cost, quality, and value

From a policy perspective, the report advocates for a shift towards "most economically advantageous tender" (MEAT) models that balance cost with quality and value. This includes the use of weighted evaluation criteria that consider training, experience, technological capability, and organisational resilience.

Some European jurisdictions have already adopted such approaches, demonstrating that it is possible to reconcile regulatory compliance with higher-quality outcomes.

However, the report is not uncritical of the industry itself, acknowledging that security providers must also adapt, improve transparency, demonstrate measurable value, and invest in capability. Buyers are increasingly demanding evidence of performance, including data on incident response, customer satisfaction, and operational effectiveness.

Providers that can articulate their value proposition beyond cost are better positioned to succeed in more sophisticated procurement environments.

Competition vs collaboration

A key tension identified in the report is the balance between competition and collaboration. While competitive tendering is essential for market efficiency, overly aggressive competition on price can erode the sustainability of the sector.

The report suggests that procurement frameworks should encourage collaboration, knowledge sharing, and long-term partnerships between buyers and providers. This is particularly important in complex security environments where coordination between multiple stakeholders is required.

In summary

The European experience offers insights and takeaways that relevant to the sector closer to home. Many of the dynamics described—price-driven procurement, fragmented standards, and workforce challenges—are persistently evident in the New Zealand market.

For buyers, a key takeaway is that security procurement should be reframed as a risk management function rather than a cost minimisation exercise. This requires a more sophisticated understanding of how security services are delivered, the factors that influence performance, and the trade-offs inherent in procurement decisions. It also requires stronger integration between procurement, security, and executive leadership.

For security providers, competing solely on price is unlikely to be sustainable in the long term. Providers must demonstrate capability, invest in their workforce, and embrace technology to deliver measurable outcomes. Those that can align their offerings with the evolving expectations of buyers will be better positioned to navigate the changing procurement landscape.

In finding that current procurement models often fail to deliver optimal security outcomes, the report isn't necessarily breaking new ground. But with more than 40,000 data points, it provides unprecedented evidence that traditional procurement models are indeed failing.

The evidence suggests that a recalibration is required, moving away from price-centric models towards approaches that recognise the complexity and criticality of security services. This is – evidently – easier said than done.

NZSA CEO's May Report

In this abridged version of his May newsletter, NZSA CEO Gary Morrison talks vulnerable workers, ACC changes, business start-up guidance, NZSA board cadet vacancy, and more.

Gary Morrison is CEO of the New Zealand Security Association (NZSA). A qualified accountant, Gary was GM of Armourguard Security for New Zealand and Fiji prior to establishing Icon Security Group.

Isn't it amazing how quickly events can change in today's world! Two months ago, my commentary was reflecting on how the new year had kicked off in a positive manner with our members reporting strong business growth and improving economic indicators. Today it is a very different picture as events totally outside of our political control now look likely to see New Zealand's growth stall, inflation to rise rapidly and cause ongoing concerns about fuel supply continuity.

Whilst this has significantly impacted business confidence levels, it is pleasing to note that the security sector has proven to be very resilient to economic challenges, and I remain confident that my earlier prophecy of a busy year for our members will prove correct.

Fuel supply

The ongoing closure of the Strait of Hormuz has significantly impacted fuel supply throughout the world however New Zealand's stocks, either landed or in-transit, remain reasonably strong due to our supply agreement with Singapore.

We have previously communicated the Government's Fuel Response Plan 2026 that includes four escalating phases and whilst there is no short-term pressure to move from the current Phase 1, we have registered our sector with MBIE as an Essential Service provider, and identified those specialist service areas (such as Hospital security staff) that should be considered as either Band A - Life Supporting Services or Band B – Economically Important Services, should there be a need to move to Phase 4 and prioritise fuel supply.

To support our own knowledge of the composition of the security vehicle fleet we conducted a brief survey of members that indicated the following breakdown: Petrol 34%, Diesel 33%, Hybrid 32%, and Electric 1%.

We will monitor this on a regular basis and expect that we will see a continued uptake in hybrid vehicles in lieu of petrol and diesel as technology improves and running costs come under increased focus.

Part 6A – Vulnerable Workers

In July 2021 an amendment was made to the Employment Relations Act 2000 that added certain types of security services to the employees protected by Part 6A of the Act (continuity of employment if employees' work affected by restructuring). This extended the same protections to Security Officers as those already held by cleaning, catering and some laundry and caretaking workers.

Following the amendment being passed, the NZSA provided its members with guidance on application of the legislation based on advice from our lawyers, and as followed by other impacted industries. In simplified terms, our interpretation was that the legislation provides the right for employees to transfer to a new employer on their existing employment terms and conditions where a contract transfers to a new provider.

This interpretation was recently challenged by one of our members based on an opinion provided by their legal representatives.

Given that this is an important issue for the industry, and in the absence of any precedent setting case law, the NZSA consulted with the member and

agreed to contract Michael Heron, KC, to review the legislation and provide a definitive legal opinion.

Michael Heron's legal opinion supported the NZSA's interpretation (and that of other industry sectors) and we now intend to engage with the HRSIG (Human Resources Special Interest Group) to develop a Good Practice Guideline covering application of Part 6A in a security context. The Guideline should be available on the NZSA website later this year.

ACC changes

ACC announced several changes in April that will impact levy invoices due in July. Key changes include:

- All payment plans will now incur interest (plans previously provided a 6 month no interest plan).
- Penalties now have a 30-day payment period and penalty interest at 1.7% per month.
- Businesses in the Experience Rating Scheme will incur a 7.2% Levy increase.

Business start-up guidance

New Zealand has a culture of encouraging people to start up their own businesses however the sad reality is that some 90% of start-ups fail.

Whilst the numbers are not that high for the security industry, it still happens regularly and is a cause for concern given it impacts customers, staff and the reputation of the industry.

As the regulator for the security industry, the Registrar for the PSPLA is very mindful of this risk and has traditionally used caution when granting company or individual licences for those who do not have experience in running a business.

Given the absence of any recognised training in the fundamentals of running a business, the NZSA has developed an online training programme that includes 4 modules plus references and links:

1. Getting started: Who can set up a business; Establishing what type of business; Registering the business.
2. Financial Fitness: Accounting and financial obligations; Professional advice and support.
3. Gaining and maintaining a security license: Company and personal security license; Annual security license returns.
4. Good business practices: Health and Safety requirements; Policies and operating procedures.
5. Reference documents and links.

The Business Start-Up Guidance modules are nearing completion and will be available on the NZSA Training Hub within the next few weeks.

It is also interesting to note that there has been strong interest in the programme from other sectors such as Commercial Cleaning and Electrical who experience similar issues with business start-ups. They are considering how they can utilise the training modules and integrate their own specific licensing or regulatory requirements.

Compliance advisory support – new partnership

The NZSA has partnered with Rosemary (Rosie) Killip of Building Networks to provide members with access to specialist compliance advisory support on an as-needed basis.

The partnership gives NZSA access to expert advice on access control compliance, including practical guidance on FAQs for members.

This arrangement strengthens NZSA's ability to give members clear, practical guidance on SS3/2 requirements, building consents, exempt work, Certificates of Acceptance, IQP work, and related compliance issues. To contact Rosie, see the Building Networks website.

Rosie is also assisting the NZSA currently with a submission to MBIE concerning the Draft Compliance Schedule Handbook that fails to provide any example of required inspections and lacks specifics.

Nominations for NZSA Board Cadet position

As covered in our last newsletter, we launched the NZSA Board Cadet programme in 2024 providing an opportunity for representatives from two organisations to join the board in a non-voting capacity.

The programme provides a fantastic opportunity for talented individuals looking to develop their skills and capabilities, particularly in governance focused roles and the current cadets speak very highly of their experience.

We have one vacancy coming up in the next few months and have started advertising the role.

NZSA Membership renewals

A massive thank you to all members who have recently renewed your NZSA membership.

As a Not for Profit with voluntary membership, our continuation is always dependent on having the support of our members and to see such a high proportion of invoices paid within the first month validates that we must be providing benefit and value to our members.

Also, a reminder to those who are under cashflow pressure, we are happy to arrange a monthly payment plan.

John Wick and the Art of Physical Security Risk Management

So what do John Wick and the New Zealand Government's Protective Security Requirements (PSR) have in common? ICARAS Security Consultants explores a few lessons from the underworld.

The John Wick franchise has enthralled audiences with its balletic gun-fu, unflinching intensity, and intricate lore of a hidden assassin world governed by codes, gold coins, and unbreakable rules.

Beneath the relentless action sequences lies a surprisingly rich canvas for examining physical security risk management. The films portray layered defences, controlled environments, vigilant personnel, and rapid crisis responses in a high-stakes underworld.

While dramatised for cinematic effect, these elements offer thoughtful parallels to real-world protective practices, particularly those encouraged by New Zealand's Protective Security Requirements (PSR).

The PSR promotes a disciplined, risk-based approach to safeguarding people, assets, and information. It emphasises understanding what needs protection, designing proportionate controls, validating their effectiveness, and maintaining them over time.

In the John Wick universe, security is rarely static or generic. Measures appear carefully calibrated to specific threats, from rival factions to personal vendettas. This focus on purposeful design highlights a vital principle: the most effective security programmes stem from a rigorous process that links every mitigation directly to an identified risk.

Mapping the Threats: Risk assessment in a dangerous world

John Wick's world is one of perpetual vulnerability. Protagonists and antagonists alike navigate environments where threats can emerge from any direction: rival assassins, powerful criminal organisations, or breaches of sacred neutral ground such as the Continental hotels.

The franchise implicitly demonstrates the value of constant threat awareness. Locations are assessed for their exposure, whether it is the public accessibility of a bustling hotel lobby or the isolation of a remote safe house.

In practice, this mirrors the foundational step recommended by the PSR: understanding exactly what must be protected and why.

A superficial review rarely suffices. Organisations that work with specialist security risk management consultancies gain a significant advantage here. A methodical assessment ensures that subsequent controls are not chosen arbitrarily but are explicitly designed to address genuine, prioritised risks. This disciplined process helps avoid the temptation of broad-brush solutions and creates defences that are both targeted and efficient.

Controlling the Perimeter

Few elements in the John Wick series are as iconic as the Continental Hotel's strict neutrality and layered access protocols. Keycards, biometric measures, armed concierges, and a rigid code of conduct combine to restrict entry and maintain order. Even in the heat of conflict, these controls buy precious time or enforce consequences for violations.

The films illustrate how effective access control deters casual intruders and delays determined ones. In the real

world, robust access strategies, ranging from physical barriers and electronic systems to trained verification personnel, form a cornerstone of physical security.

When properly aligned with a prior risk assessment, such measures protect sensitive areas without creating unnecessary obstacles for authorised users. They reflect the personnel security dimension of protective practices, where trust is managed through vetting, accountability, and clear protocols.

Vigilance and Awareness: Security personnel and surveillance

The franchise frequently showcases both overt and covert security teams operating alongside surveillance systems. From the Continental's concierge network to rooftop lookouts and discreet monitoring, these elements provide situational awareness and rapid threat detection.

Characters rely on intelligence gathered through human networks as much as technological means, underscoring that surveillance is most powerful when integrated into a broader intelligence picture.

In reality, well-trained security personnel combined with thoughtfully positioned cameras, motion detection, and monitoring capabilities enhance detection and response. The key lies in calibration: systems should deliver actionable insights rather than endless footage.

When surveillance supports an overall risk management framework, it contributes to early warning and informed decision-making, much as the PSR advocates for cohesive protective measures across an organisation.

Fortified Refuges: Secure design and safe havens

Safe rooms and reinforced spaces appear as critical last lines of defence in several instalments. These fortified areas, complete with reinforced doors, communication links, and emergency provisions, offer temporary sanctuary during overwhelming assaults. Their portrayal, though heightened for drama, highlights the importance of secure-by-design principles in architecture and layout.

Real-world applications of secure design extend beyond panic rooms to include hardened entry points, compartmentalised facilities, and layouts that naturally deter or delay intruders. When integrated thoughtfully, such features complement access controls and surveillance, creating overlapping layers of protection that align with assessed risks rather than generic standards.

The Human Element: Personnel readiness and crisis response

John Wick himself embodies adaptability, resourcefulness, and decisive action under extreme pressure. Supporting characters, from hotel staff to tactical teams, demonstrate the value of preparedness through drills, clear command structures, and the ability to improvise when plans unravel. Crisis scenes, though stylised, emphasise that effective response depends on people who understand their roles and can execute protocols calmly.

This aligns closely with the PSR's emphasis on building organisational resilience through capable personnel. Regular training, scenario-based exercises, and a culture of continuous improvement ensure that teams can detect, delay, and respond effectively. Crisis planning becomes not merely a document but a living capability that integrates physical defences with human judgment.

Protecting What Matters: Information and operational security

Even in a world of bullets and blades, information holds power. Delivery of messages via carrier pigeons or coded exchanges, the careful guarding of ledgers and contracts, and the control of sensitive operational details all play subtle but important roles. Breaches of information can escalate threats dramatically, turning a contained situation into a full-scale conflict.

In contemporary settings, protecting sensitive data, schedules, client details, and procedural knowledge forms an essential supporting layer. When information handling protocols are aligned with physical and personnel measures, they create a more resilient overall posture.

The PSR framework encourages organisations to treat information protection as integral to the broader security effort, ensuring consistency across domains.

Real-world lessons from the silver screen

The John Wick films entertain through exaggeration, yet they quietly champion several enduring truths. Access control, surveillance, secure design, personnel preparedness, and crisis planning work best when woven into a coherent, risk-driven programme.

Isolated technologies or hastily implemented measures rarely deliver lasting value. Instead, success arises from a structured process that begins with thorough assessment and ensures every control serves a clear purpose.

Organisations benefit greatly when they adopt this methodical approach rather than relying on generic reviews or equipment-focused proposals. Specialist security risk management consultancies bring the expertise to translate assessed risks into proportionate, integrated solutions. This focus on process helps create defences that are not only robust but also sustainable and adaptable to evolving circumstances.

While no one expects real-world security to match the operatic intensity of John Wick's exploits, the underlying principles remain relevant. Whether protecting corporate assets, critical infrastructure, or high-profile venues in New Zealand, a disciplined risk management lens, informed by frameworks such as the PSR, provides the foundation for genuine resilience.

The next time you watch John Wick reload amid chaos, consider the quieter architecture of security that makes the scene possible. In both fiction and reality, the difference between vulnerability and strength often lies not in firepower alone, but in foresight, integration, and a commitment to doing security the right way.

This article was originally published in the ICARAS Security Consultants blog.

NZ is criminalising sexualised deepfakes – banning apps that make them should be next

If New Zealand wants to meaningfully address image-based sexual abuse in the age of generative AI, we have to go further than criminalising it, writes Cassandra Mudgway, Senior Lecturer in Law at University of Canterbury.

New Zealand is changing the law to make sexualised deepfakes a crime. But this alone may not be enough to counter the rise in AI-generated fake sexual material.

This week the Deepfake Digital Harm and Exploitation Bill is set to go through its first reading, with support across the political spectrum. The amendment will make creating, sharing or selling sexually explicit deepfakes without consent a criminal offence.

It comes in response to the rapid spread of such material, including the rollout of Elon Musk's Grok AI chatbot on X, which people used to digitally undress women and girls and generate potentially three million sexualised images.

New Zealand is not alone in confronting the problem. The United Kingdom, Australia, South Korea and the United States have already introduced or expanded laws to criminalise creating and sharing of non-consensual deepfakes.

Criminalisation is an important first step and brings New Zealand in line with developments elsewhere. But stemming the tide of sexualised deepfakes will also require regulation of the technology itself.

Deepfakes mostly target women

Deepfakes are AI-generated images, audio or video designed to make it appear that a real person said or did something that never actually happened.

With image-based sexual abuse, this usually means using AI to create convincing but fake sexual material of a person without their consent.

Sometimes, technology is used to manipulate ordinary photos pulled from social media into explicit imagery. Other AI systems can generate entirely fabricated sexual content from a text prompt alone.

The abuse is overwhelmingly directed at women. One widely cited study found 98% of deepfake videos online were pornographic and mostly targeted women.

For victim-survivors, the harms are significant regardless of whether the image is created from a real original or completely fabricated. People report humiliation, fear, anxiety, loss of control and violation of sexual autonomy.

Gaps in New Zealand law

The new bill is designed to fill gaps in the current law.

At present, New Zealand does not have a criminal offence specifically

directed at sexualised deepfakes. Existing laws may apply, but they were not designed for AI-generated abuse.

The Harmful Digital Communications Act 2015 criminalises posting harmful digital communications and has already been used in at least one prosecution involving a sexualised deepfake. However, the offence requires proof that the defendant intended to cause serious emotional distress and that this actually resulted.

Those requirements can be difficult hurdles for victim-survivors of image-based sexual abuse.

A new offence introduced into the act in 2022 sought to address this for so-called "revenge porn", making it a crime to share an intimate visual recording without consent.

This sat alongside existing offences in the Crimes Act. The concept of an "intimate visual recording" was introduced in the early 2000s to deal with covert filming with hidden cameras.

Parliament was responding to conduct known as "upskirting" and "downblousing" – forms of abuse overwhelmingly targeting women and girls in spaces where they had a reasonable expectation of privacy, such as bathrooms or changing rooms.

The law therefore focused on whether a person had been secretly recorded. But deepfakes complicate that framework because no recording may have occurred at all. This means current law may be clearer when an intimate image is real than when it is entirely fabricated.

Beyond criminalisation

The deepfakes bill attempts to remove that uncertainty by expanding the legal definition of an "intimate visual recording" to include images that are "created, synthesised or altered".

But the bill also reflects a broader pattern in New Zealand's response to image-based sexual abuse: the law tends to evolve only after new technologies expose gaps in existing protections.

First, it was hidden cameras and covert recordings. Then it was revenge porn. Now generative AI. Criminal law has been reactive and is not future-proofed enough to cover new technology-facilitated sexual harm.

The rapid development of new technologies means criminalisation alone is unlikely to stop the spread of sexualised deepfakes.

The tools to create deepfakes are cheap, fast and increasingly easy to access. A recent investigation by the Tech Transparency Project identified dozens of "nudify" and face-swap apps available through both the Apple and Google app stores. These apps can generate sexualised images from ordinary photographs within seconds.

Despite app store policies prohibiting sexually explicit or degrading content, many of these tools remain readily accessible, often disguised as image-editing apps.

Addressing regulation of high-risk apps

Generative AI systems rely on enormous datasets scraped from the internet, frequently including images of women and girls used without their knowledge or consent.

The result is that women's bodies are increasingly becoming both the raw material for AI systems and the targets of abuse generated by them. That is why New Zealand needs to think beyond criminal law and address regulation.

Australia is moving to ban nudification apps and websites. So is the United Kingdom and the European Union. New Zealand should follow suit.

More broadly, New Zealand should consider a regulatory framework for high-risk AI systems, particularly for technologies capable of generating non-consensual sexual content.

This could include mandatory safety guardrails in image-generation systems, stronger obligations on app stores and platforms distributing these tools, and transparency requirements around AI training data.

The Deepfake Digital Harm and Exploitation Bill is an important step forward and parliament should pass it. But if New Zealand wants to meaningfully address image-based sexual abuse in the age of generative AI, criminal law cannot be the end of the conversation.

This article was originally published on 19 May 2026 in The Conversation.

Su Kaur celebrates 10-year milestone with FIRST Security

Su Kaur has notched up a stellar decade with FIRST Security during a career that has seen her rise from security guard to a range of regional management roles.

Su Kaur has just celebrated 10 years with FIRST Security. Her recent leadership and managerial roles, including Auckland Operations Manager and Waikato Branch Manager, have been the result of an impressive rise through the ranks.

"I started my journey on the front line as a Security Officer, learning firsthand the realities of the role - long hours, high-pressure situations, and the importance of staying calm and professional at all times," Su posted recently. "Those early experiences built the foundation for everything that followed."

She is currently FIRST's Contracts Manager – Rail and Events, a testament not only to her capability and commitment to excellence, but also to her significant expertise in public transport security.

"Over the years, I've had the opportunity to grow through a range of roles, each bringing new challenges and responsibilities," she said. "From managing teams to navigating complex client expectations, there were plenty of moments that pushed me outside my comfort zone - but those were also the moments where the most growth happened.

"Today, I am proud to be working as a Contracts Manager, leading teams and contributing to the success of the business. It's a role that comes with responsibility, but also a strong sense of purpose - especially knowing where I started."

Su's achievements were recognised at the national level in 2022 with her being awarded a coveted Women in Security Awards Aotearoa (WiSAA) gong in in category of Leader.

She has also achieved shortlisting as a finalist for several awards, including in the OSPAs (Outstanding Female Security Professional 2025, and Outstanding Contract Security Manager/Director of the Year 2023) and New Zealand Security Awards (Security Consultant of the Year 2025, Security Supervisor / Operations Manager of the Year 2022).

In support of her ultimately successful WiSAA nomination, one of Su's colleagues who had been to deployments in the field that Su had managed, noted that her leadership skills were first class.

"She plans, reviews and executes operational requirements with military precision," he said. "Whilst being a quiet person, Su leads from the front and is very much a 'leader' compared to manager. People follow Su, as they respect her."

The esteem in which Su is held among her colleagues was reflected in a FIRST Security internal "Tuesday Shout-Out" recognition award in June 2019, and in February 2023 when she was named FIRST Security's 2022 Strive Office Employee of the Year.

"Su is a truly valued member of our team who consistently goes above and beyond to support and look after her staff," stated an announcement by FIRST Security in relation to Su's decade milestone. "Her leadership, care for her people, and strong work ethic make a real difference every day."

Inception Turns 10: A Decade of Evolution

Inner Range's Inception has just celebrated its 10th birthday – a journey marked by continued innovation, evolution, and a balancing act between power and simplicity.

Inception has officially turned 10 years old, marking a major milestone in the Inner Range story. What began as a bold new idea in May 2016 has grown into one of the most widely trusted access control and security platforms in its class.

"From day one, Inception was designed to challenge the status quo by bringing modern, web-based technology to an industry still relying on legacy systems" said Steve Mitchell, Director of Product and lead developer on the Inception platform.

"Ten years on, that original vision is not only intact, but it has also evolved into something far greater and far more powerful than we initially had planned."

"When Inception was first released, it was positioned as a web powered security system built for today's customers, not yesterday's technology" states Mitchell. At its launch on 09 May 2016, Inception delivered:

- Web connected architecture
- Easy remote connectivity, via IR SkyTunnel, providing direct access without IT port forwarding
- Support for up to 32 doors and 32 areas
- 512 inputs / 512 outputs
- 2,000 users
- 50,000 event capacity
- No software licences
- Browser based configuration and management

These capabilities were groundbreaking at the time and laid the foundation for a new generation

of integrated security systems, and Inception's impact didn't go unnoticed.

"In 2017, we were extremely proud when Inception was awarded the ASIAL Access Control Product of the Year, recognising its innovation, usability, and market relevance" Mitchell continues.

"This recognition confirmed what installers and end users were already experiencing in the field, that Inception was changing expectations of what an access control platform could be."

Evolving into a Powerhouse

Over the last decade, Inception has continued to evolve, with today's platform supporting:

- 128 doors / 256 readers
- 96 areas
- 1,024 inputs / 1,024 outputs
- 10,000 users
- 250,000 offline events
- Built-in web interface
- No mandatory software or maintenance fees
- Seamless mobile connectivity via IR Connect mobile application unifying Inception Access Control & Intrusion with IR Video surveillance into a single end user interface.

With the above achieved via firmware updates, with no hardware replacement required, the platform sought to deliver a futureproof solution for customers.

Part of Inner Range ecosystem

Today, Inception sits within the Inner Range connected ecosystem, a unified platform that brings access control, intrusion detection, video, and automation together.

Native and high-level integrations include IR Connect, IR VideoIR Mobile Access, and REST API for third-party integrations, alongside supported integrations with Milestone, Hanwha, ASSA ABLOY Aperio wireless locks, Control4, and ELAN Home Management

"Ten years on, Inception has grown beyond just a product, it's evolved into a proven platform trusted globally across tens of thousands of sites and thousands of Integrator partners," said Mitchell.

Security Industry News Round Up

In this month's security industry news round up, Matrix Security officer prevents fire, career milestones for Gareth Bacon and Tim Holden, Red Badge in One Stadium opener, SecTech NZ about to land, and much more.

Midnight patrol stops fire before it escalates

According to a recent Matrix Security blog post, at Just after 11:30pm, during a routine patrol at one of its commercial client's sites in Royal Oak, Auckland, patrol officer Raymond Townsend detected footsteps where there should not have been any, followed by the smell of smoke.

Moments later, a small fire was discovered at the rear of the secured site, as well as an unidentified unauthorised individual in the shadows. The officer immediately withdrew to a safe position and notified the Matrix Security Contact Centre via RT, requesting Police and FENZ support. A backup patrol officer, Meripa Masau, was also dispatched to assist.

As a fire crew arrived, the individual emerged from a concealed area and attempted to leave the site. A clear description was quickly broadcast, allowing Police to locate and detain the individual nearby shortly afterwards.

Evidence from the fire scene was secured, and fire crews confirmed that if the incident had not been reported when it was, the outcome could have been significantly worse. The site was locked down, cleared, and secured, with no damage to buildings and no further risks identified. An arrest was made for unlawfully being on the property, with further charges pending.

"This incident was handled effectively," stated the client. "The appropriate emergency services, FENZ and NZ Police, were contacted promptly. Thanks to the patrol guard providing a clear description of the offender, Police were able to apprehend him later. Communication after the event was thorough, and we were kept well informed via phone and email."

Allied Security grappling champion goes national

Ministry of Social Development (MSD) Allied Security guard Ryan is now a national grappling medallist.

Ryan recently competed at the New Zealand Grappler Summer Slam Nationals in Auckland and earned a medal after two fights in the GI division.

Brazilian Jiu-Jitsu is a relatively new sport in New Zealand it has experienced a huge amount of growth throughout Aotearoa in the past five years. According to New Zealand Grappler, there are now approximately 250 gyms nationwide with around 10,000 members.

Ryan has been training Brazilian Jiu-Jitsu for only a year and this was just his second time at the New Zealand Grappler Summer Slam Nationals.

"For those who know Ryan they know he is not someone who does things by halves, on the job or off it," stated an Allied Security post announcing his achievement. "He has been with us for four years as a MSD guard and goes above and beyond to help his team and those around him."

15 year milestone for FIRST's Gareth Bacon

FIRST Security National Manager – ATM Services Gareth Bacon has achieved 15 years of service with the nationwide security provider.

"Over the years, Gareth has taken on many roles across the business," stated an announcement from FIRST Security. "His experience, leadership, and willingness to mentor others have made a lasting impact on those around him."

Gareth started out in security with Chivalry Security Providers in 2005, rising to the rank of Operations Manager prior to joining FIRST in April 2011. In the ensuing 15 years, Gareth took on a range of leadership roles, including a secondment as National Operations Manager for Managed Isolation and Quarantine Facilities during COVID.

Following a stint as Branch Manager in Wellington over 2025, Gareth returned to Auckland to take up his current role as National Manager ATM Services in March 2026.

"Gareth is a highly valued member of the team, and we thank him for his dedication, loyalty, and ongoing commitment to excellence," stated the announcement. "Here's to many more successes ahead!"

Red Badge in One Stadium opener

The first major sporting event at Christchurch's new One New Zealand Stadium took place on the weekend of April 24–26, 2026. The venue officially opened with the Super Rugby Pacific "Super Round," featuring a sold-out opening match between the Crusaders and the Waratahs.

The stadium has 25,000 permanent seats with capacity for a further 5000 temporary seats, and has a maximum capacity of 37,000 for concerts. A big team from Red Badge was there to ensure the safety and security of the event.

According to Red Badge, the big event was preceded by significant preparations. "In the lead-up, our team has been on site for the past two weeks getting familiar with the venue and refining processes," explained a Red Badge update on LinkedIn.

"These moments have been about preparation, coordination, and making sure everything runs as it should... It's the kind of groundwork that sits behind every major event - steady, detailed, and led by experienced people."

Security of Crowded Places in New Zealand Forum 2026

The New Zealand Security Association has issued an invitation to security industry providers, stakeholders, and owners and operators of crowded places and venues to the 2026 Security of Crowded Places in New Zealand Forum.

Following the success of the inaugural 2025 Forum, the NZSA is staging the event for a second year to continue building knowledge, skills, and capability around protecting New Zealand's crowded places.

The Forum, to be held 21-22 July at Auckland's Eden Park, will cover the latest developments in New Zealand's Crowded Places Strategy and associated resources.

Learning outcomes will be particularly relevant for senior managers and training managers within security providers, security consultants, and those with direct responsibility for crowded places and venues.

Presentation topics and speakers are being finalised and will include: The New Zealand threat environment; NZ Crowded Places Strategy and resources; International trends and developments; Technology developments; and A review of recent incidents and post-incident learnings.

The Forum will also feature Knowledge Cafe sessions — collaborative workshops where participants will share knowledge and help develop better capability.

Gallagher Security sponsors Safety Summit 2026

Gallagher Security has announced that it is a sponsor of Safety Summit 2026, New Zealand's conference for health and safety professionals

Taking place on 15 October 2026 at The Majestic on Durham, Christchurch, Safety Summit will bring together some of the most respected voices in safety leadership. This year's speaker lineup includes James Laughlin, Dr. Alexandrina (Alia) Bojilova, Moni Hogg, Matt Jones, Nicola Knobel, and Paaka Westrupp.

"At Gallagher Security, we believe that protecting people and places starts with strong, informed leadership. That's why we're excited to be part of an event that puts safety leadership front and centre."

SecTech NZ about to land

SecTech NZ opens 11-5pm at Eden Park in Auckland on 09 June. Attendees can register in advance of the event for free parking, and Tool Shed prize draw tickets are available for collection at the door.

"SecTech NZ is the perfect opportunity for security installers, integrators, locksmiths, consultants, and security and facilities managers in government and commercial organisations, to get their hands-on the latest security products and technologies," stated event organisers.

"You'll see all the latest CCTV, access control, alarms, video analytics, security AI, authentication, automation, electronic locking, security communications, key management, video intercoms and loads more. You'll also get to discuss your operational issues with the teams of 27 professional security exhibitors in one room."

With doors opening at 11am, drinks and nibbles will be served at 3.30pm, with the Tool Shed prize draw at 4pm.

The Auckland event will be followed by SecTech Wellington at HNRY Stadium on 11 June and SecTech Christchurch at Te Pae on 16 June.

ASIAL 2026 conference speakers announced

Celebrating 40 years in 2026, ASIAL's Security Exhibition & Conference will bring together security professionals, industry leaders and innovators from across Australia to explore the challenges shaping our industry and the strategies needed to stay ahead.

Featuring 19 expert speakers, the event will deliver practical insights on emerging threats, resilience, technology, leadership and risk management in an increasingly complex operating environment.

Under the theme 'Strengthening Security in an Era of Increased Complexity and Risk', the event will explore practical strategies to build adaptive capability, integrate risk intelligence, leverage emerging technologies and cultivate leadership that thrives in uncertainty.

Speakers will present on such topics as Strengthening Security Posture in an Era of Increasing Complexity and Risk - Security Intelligence and National Resilience (Dr Nicola Lochhart); Sovereignty as Risk Management: Clarity, Trade-offs, Accountability (Mark Richards); The Convergence Point: How AI, Body Cameras and Drones are Reshaping Physical Security (Jonathon Tindale); and Beyond IT/OT: Closing the Physical Intelligence Gap in Critical Infrastructure Security (Ian Clark).

25 year milestone for Wesco Anixter's Tim Holden

Tim Holden has celebrated 25 years with Wesco Anixter NZ – a quarter century with the New Zealand distributor.

"Over the years, Tim has built an outstanding career as a Telecommunications Technical Support Technician, specialising in on-prem telephony systems," announced Wesco Anixter. "His deep technical expertise, paired with a practical, solutions-focused mindset, has made him a trusted resource for customers and colleagues alike.

"What truly sets Tim apart is his commitment to always going the extra mile to deliver the right outcome, along with his dedication to continuous learning to keep pace with an industry that never stands still.

"Thank you, Tim, for your dedication, professionalism, and contribution over the years and congratulations on this well-deserved milestone!"

ASIS INTERNATIONAL
Advancing Security Worldwide®

REACH NEW HEIGHTS
in Professional Excellence

ASIS accredited certifications can help you reach your career goals.

PCI®
Professional Certified Investigator
Board Certified, ASIS International

Validates your ability to conduct security investigations through the effective use of surveillance, interviews, and interrogations. Designed for those with 5 years of related experience.

"PCI is an important element in the ASIS Certification programme, dovetailing into both CPP and PSP for a comprehensive understanding of broader security industry objectives. An effective and reliable investigation depends on objectivity, thoroughness, relevance, accuracy and timeliness. PCI helps identify critical investigative outcomes, including evidence collection, case management, and the process of offender detection, identification, interview and prosecution. Good physical security designs, together with robust policies and procedures are key elements in a successful investigation. The PCI certification provides an insight into how these pieces interrelate."

- David Horsburgh, MSc CPP PSP PCI

WHY EARN THE PCI DESIGNATION?

- Provides independent confirmation of your specialized skills in security investigations
- Gain global recognition by your peers and industry
- Get a competitive edge in the marketplace
- Enhance your career and earnings potential
- Enjoy personal satisfaction and professional achievement

Be one of the many ASIS board certified practitioners who are leaders, mentors, and trusted strategic partners, serving both their organizations and the profession.

WHY SHOULD AN EMPLOYER HIRE ASIS CERTIFIED PROFESSIONALS?

- Build a strong, dedicated team committed to high standards and continuing professional development
- Promote ongoing education of critical job knowledge and skills
- Feel confident that your staff are using best practices
- Recruit the most qualified professionals
- Reinforce or elevate your organization's reputation and credibility

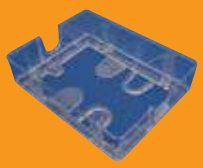
Increase the competency level of your staff by supporting your security professionals in their certification journey.

Visit www.asis.org.nz

fired up protection

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

720-054 Ref. STI-1100
Stopper 11 Flush mount with
9 V battery powered horn.
255mm H x 179 mm W x 135 mm D
Optional label, any text, printed in house



720-056 Ref. STI-1300-2
50 mm spacer for Stopper 11;
255mm H x 179mm W x 63 D

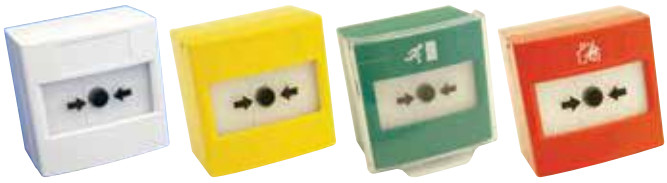
720-090 Ref. STI-13000-NC
NC Universal Stopper flush mount, clear
Options 9V battery horn, (5 colours),
custom label, loom for remote
12-25 v DC power and relay

720-096 Ref: STI 13410NW Enviro Stopper,
Conduit entry top and bottom, no horn
Back box IP66, Front section IP56
Options 9V battery horn, (5 colours), custom label,
loom for remote 12-25 v DC power and relay

720-097 Ref. STI- 13200NC
Universal Stopper with 40 mm spacer, no horn
Options 9V battery horn, (5 colours), custom label,
loom for remote 12-25 v DC power and relay

720-060 Ref. STI-6518
Bopper Stopper Flush mount, no horn

All STI Stoppers are made of tough, UV stabilized polycarbonate. Hi or Lo volume horn output.
Any text labels produced in house at **Loktronic**



720-352 720-354 720-356 720-358

Indoor Model Reset Call Points
720-352 (white;) 720-354 (yellow); 720-356 (green); 720-358 (red)
One product with both Surface and Flush mount options
Approved to EN54-11
Material: Polycarbonate
Current rating: 3 Amps @ 12 - 24 v DC, 3 Amps @ 125 - 250 v DC
Optional clear cover
2 x SPDT switches
Positive action that mimics the feel of breaking glass
Visible warning flag confirms activation
Simple polycarbonate key to reset operating element – no broken glass
Dimensions in mm: 87 x 87 x 23 (flush); 87 x 87 x 58 (surface)

720-64G 720-062R 720-062W

IP67 Outdoor Model Reset Call Points
720-062W (white); 720-062R (red); 720-064G (green)
Conduit entry; 1 top, 2 bottom
Approved to EN54-11
Material: Polycarbonate / Glass Reinforced Nylon
Current rating: 1 Amp @ 12 - 24 v DC, 6 Amps @ 125 - 250 v DC
Optional clear cover
2 x SPDT switches
Positive action that mimics the feel of breaking glass
Visible warning flag confirms activation
Simple polycarbonate key to reset operating element – no broken glass
Dimensions in mm: 89 x 89 x 90

Battery Load Tester Ref. 730-101
ViTECH, strong, lightweight aluminum case, 5,15 and 30 amp battery load tester for fire and alarm use.
Weight: 500gms, Size: 165mm x 90 x 70mm.

Fire Brigade Alarm: (Closed/Open) Ref. 730-231
ViTECH branded Type X (730-230) and Type Y (illustrated) models with temperature compensated pressure transducers with digital display showing pressures for defect, re and pump start.

Anti-Interference Device
Ref. 730-400 series
ViTECH AID for sprinkler valve monitoring; ts all ball valve sizes.

Loktronic

Loktronic Limited Unit 7 19 Edwin Street Mt Eden Auckland 1024
Ph 64 9 623 3919 • Fax 64 9 623 3881 • 0800 FOR LOK
mail@loktronic.co.nz • **www.loktronic.co.nz**