NZSM

New Zealand Security Magazine

July 2026

Tara Pulawski: The camera is not the country

Lincoln Potter: Zen and the art of security science

Johan van Rensburg: Security practice across the ditch

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

August 2026

Social Media

linkedin.com/company/defsec-media-limited

NEW ZEALAND

CYBER SECURITY RISK CONFERENCE

4 August 2026 | NZICC, Auckland

Own the risk.
Build your resilience.
Lead our response.

Secure NZ's digital economy, together.

Featuring:

Ryan Ko
Centre Director
UQ Cyber Research Centre

Catherine Buhler
Chief Information Security Officer
Fonterra

Simon Burson
Chief Information Security Officer
Auckland Council

Melissa Crawford
Director
Tech with Heart

Explore Event

Brought to you by

Brightstar

CyberTech NEW ZEALAND

Part of a wider tech experience at

NEW ZEALAND CIO INNOVATION SUMMIT & AWARDS

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 July 2026 issue of New Zealand Security Magazine, the second edition of our new shorter, sharper monthly publication!

Leading this latest edition of NZSM is a very smart piece of writing from Cyntion Managing Director Tara Pulawski. Tara argues that there are a range of objective considerations – from firmware quality, construction, support, network behaviour to real-world performance and more – that procurement teams should subject any CCTV camera to. And they should be doing this no matter the country of origin.

This is essential reading for electronic security and procurement professionals trying to make sense of the debates over Chinese cameras. Tara puts the political smoke and mirrors to one side in favour of a technical evidence-based approach that's just good sense.

In this issue, we acknowledge the winners of this year's NZ Outstanding Security Performance Awards, and we zero in on Lifetime Award recipient Lincoln Potter.

Lincoln is a New Zealand security industry living treasure with a unique professional trajectory that has seen him develop from security guard to installer to consultant and beyond. Despite its uniqueness, his is a story that is relatable across security practitioner domains and across levels of experience. He is the embodiment of an 'everyman' with exceptional qualities.

Unique and relatable, common and exceptional, Lincoln is a paradox wrapped in a contradiction wrapped in a wonderful human being. I hope you enjoy reading his story of achievement.

Also headlining this edition is an insight into Johan Janse van Rensburg's adventures in Aussie. As one of our recent professional exports to New Holland, Johan offers valuable comparative insights on the trans-Tasman markets – with some worthwhile takeaways for New Zealand security professionals. A great read!

Also in this NZSM, Auckland University of Technology Professor of Law Kris Gledhill explores whether 'move on' orders for rough sleepers will make cities safer, NZIPI Chair Daniel Toresen discusses the new standalone criminal offence for stalking and harassment, NZSA CEO Gary Morrison delivers his monthly update, a McKinsey survey finds geopolitical risk preparedness lacking, and Australia's PSPF gets an update.

Plus, the latest in NZ security sector news in this issue of NZSM, including a new visitor management solution for Gallagher, gaps in SME cyber insurance, cyberattacks target community sector, foreign intelligence agencies target job sites, new law targets antisocial road users.

A lot can happen in a month!

Keep safe.
Nicholas Dynon,
Lincoln.

serco

Bringing together the right people, partners, and technology to deliver integrated services that enable readiness

serco.com/aspac

Impact a better future

The Camera is not the Country

There are a range of objective considerations that procurement teams should subject any CCTV camera to – no matter its country of origin, writes Tara Pulawski, Managing Director of Cyntion.

Tara Pulawski is Managing Director at Cyntion, an operational intelligence platform provider. Having worked in electronic security for three decades, she specialises in software, AI and technology Development.

Country of origin is a poor shortcut for judging a camera. Firmware quality, construction, support, network behaviour and real-world performance matter far more.

Ask a group of security installers about Chinese cameras and the discussion usually becomes political before it becomes technical. One side sees cheap hardware, opaque cloud services and firmware assembled with all the elegance of a banana on wheels.

The other sees enormous manufacturing capability, aggressive pricing and products that often do the basic job perfectly well.

Both sides can produce examples. Neither side, by itself, has a procurement method.

The market is not East versus West

The camera industry does not divide neatly into East and West. It divides into engineering tiers.

At the bottom are products built almost entirely to meet a price point. They often reuse common system-on-chip platforms, inherited software libraries, reference designs and outsourced development. Support can be thin, documentation can be worse, and the product may effectively stop evolving once the shipment leaves the factory.

At the top are products with controlled firmware, better environmental testing, documented security processes and support that continues after the invoice is paid. Between those extremes sits most of the market, regardless of where the company is based.

The useful question is not "East or West?" It is: what evidence shows that this exact product, firmware branch and deployment design are fit for this exact job?

Firmware from another era

Some camera interfaces still feel as though they were preserved in amber. Configuration pages depend on proprietary Windows tools, browser compatibility modes or plug-in technology descended from the ActiveX era. The interface may look like 1991, but the real problem is not the colour scheme.

Legacy plug-ins expand the trusted software running on an administrator's computer, create compatibility problems and encourage people to weaken browser security just to configure a camera. A modern sensor wrapped in an old management stack can also contain outdated web libraries, weak session handling, unsafe input processing, hidden service accounts and update mechanisms never designed for hostile networks.

Public advisories and independent security research repeatedly show the same failures across network-camera products: hard-coded credentials, authentication bypass, command injection, exposed maintenance services, memory corruption and insecure firmware updates.

Some of these flaws are severe enough to allow remote compromise. Others turn cameras into convenient footholds for botnets or lateral movement into the wider network. This is not theory. It is a recurring industry pattern.

When the camera phones home

Put a packet capture beside many modern cameras and they will

attempt outbound connections almost immediately. Installers often call this "ET calling home".

Sometimes the reason is legitimate. Cameras use dynamic DNS, time synchronisation, licence checks, mobile push notifications, peer-to-peer remote viewing, firmware updates and cloud registration. High-numbered ports are also normal in peer-to-peer and NAT traversal systems.

Traffic to a Chinese server, or any foreign server, does not by itself prove a backdoor. It proves that the device is communicating with infrastructure outside the local network. That still deserves scrutiny.

The customer should know what data leaves, where it goes, who controls the service, what commands can be sent back, how authentication works, whether the feature can be disabled and what happens when the vendor stops operating the platform.

Peer-to-peer camera services are particularly awkward. They solve a real usability problem by connecting mobile applications to devices behind NAT without manual port forwarding. They also create a trust chain involving vendor servers, device identifiers, shared secrets and proprietary protocols. When that design is weak, server impersonation, traffic interception or full device compromise can follow.

The right response is not blind trust and it is not theatrical panic. It is network segmentation, egress control, DNS logging and verification. A camera should normally sit on a restricted network with only the destinations and protocols it genuinely needs.

A lack of security understanding at product level

One of the more worrying field observations is not a single vulnerability. It is the apparent lack of basic security understanding inside some product and research teams.

Representatives may be unable to explain whether encrypted communications use current Transport Layer Security (TLS), how certificates are validated, whether cloud traffic can be disabled or how credentials are protected.

Confusion between Secure Sockets Layer (SSL) and TLS is not harmless when it comes from people responsible for a connected security product.

SSL has been obsolete for years. In 2026, a manufacturer should be able to state exactly which TLS versions are supported, whether certificates are validated properly, how keys are protected and whether management, streaming, metadata and update traffic are encrypted.

The same problem appears in analytics. Manufacturers advertise artificial intelligence, deep learning, cognitive processing and intelligent recognition, while technical representatives sometimes cannot explain whether the product uses a trained machine-learning model, conventional computer vision, optical character recognition, rule-based processing or a mixture of these.

Customers do not need proprietary source code or model architecture. They do need a technically coherent explanation of the processing pipeline, validation method, known limitations, false-positive behaviour, update process and required image conditions.

When a manufacturer cannot say whether its analytics use machine learning or OCR, the problem is not secrecy. The problem is that the product may not be properly understood by the people selling it.

The same brain under different badges

Another repeated observation is the striking similarity between products sold by supposedly competing Chinese brands.

APIs can use almost identical command structures, configuration fields, error responses and undocumented behaviours. Web interfaces and firmware packages may

contain matching terminology, folder structures, libraries and even the same implementation mistakes.

There are legitimate explanations. Manufacturers may use the same chip reference design, software development kit, original-design manufacturer, analytics engine or outside contractor.

Staff and intellectual property may move between companies. In a market built on intense price pressure, direct copying is also possible.

From the outside, this can look like internal industrial espionage or uncontrolled copying. Similarity alone does not prove how the technology was obtained, so accusations need evidence.

It is also reasonable to ask whether state-backed research, public procurement, industrial policy and technology-development programmes contributed to common technical foundations during the industry's rapid growth. China has openly used these mechanisms to accelerate strategic industries.

Firmware similarities alone do not prove that the state supplied a common camera platform. The more defensible conclusion is that shared reference technology, public investment, common suppliers and aggressive imitation may all have played a part. The visible result is an industry where supposedly separate products can sometimes appear to share the same brain.

International products with local-market language

Broken English, inconsistent terminology, half-translated interfaces and leftover Chinese text remain common in products sold internationally. That may have been understandable when low-cost manufacturers first entered overseas markets. It is not acceptable in 2026.

Documentation and interface language are not cosmetic. They affect security configuration, alarm handling, firmware recovery, PRIVACY settings and an operator's ability to understand what the device is doing.

A badly translated option can reverse the apparent meaning of a control, hide a cloud dependency or cause an installer to leave an insecure service enabled. Manufacturers selling internationally should use professional technical translators and validate the wording with engineers and experienced operators.

The better Chinese manufacturers are improving rapidly. Some now provide credible documentation, international support teams and mature interfaces. Others still behave as though overseas customers should reverse-engineer the product after purchase.

Construction: the specification is not the enclosure

Firmware is only half the camera. Outdoor reliability depends on enclosure design, gasket compression, cable-entry geometry, membrane vents, fastener quality, corrosion protection, thermal cycling and installation practice.

A printed ingress-protection rating describes performance under a defined test condition. It does not guarantee that every production unit was assembled correctly, that seals will survive years of ultraviolet exposure, or that the installer will preserve the rating after terminating a cable.

At the lower end of the market, cost reduction can become painfully visible: thin castings, inconsistent gasket seating, poor cable glands, unprotected connectors and screws that corrode before the camera has earned back its installation labour.

Major manufacturers are not immune. We have seen condensation and water ingress in products carrying well-known names. A large logo does not stop water.

These claims should be backed by field evidence, service records, photographs and failure rates rather than treated as a universal feature of any country.

The economics are simple. A cheap camera may be perfectly sensible indoors, under shelter and within easy reach. The same camera can become a very expensive mistake on a coastal pole, above a fuel forecourt or at a remote site where the service visit costs more than the hardware.

The analytics gap

The newest sales language is no longer about megapixels. It is about intelligence: people detection, vehicle classification, face matching, intrusion zones, queue analysis and behaviour recognition. These functions can be useful, but the gap between a polished demonstration and a live site can be brutal.

Analytics depend on the pixels given to them. Low resolution, motion blur, bad lighting, arbitrary pose, poor camera angles, long distance, occlusion and dirty lenses all reduce performance. Rain droplets, infrared reflection, a slow shutter, heavy compression and excessive digital noise reduction can defeat an excellent algorithm.

This is why cognitive performance should be tested at the actual site, at night, in bad weather and with normal human behaviour. A daytime demonstration clip proves very little.

Poor analytics are not uniquely Chinese. Cheap edge processors may force simplified models, but expensive Western products also generate false alarms when the scene is badly designed or the settings were tuned for a brochure rather than operations.

The correct comparison is measured detection performance, missed events, false alarms and processing delay under the buyer's actual conditions.

The Western mirror

The strongest argument against nationality-based procurement is the record of the wider technology industry.

Major Western network and security vendors have released products with critical authentication bypasses, hard-coded credentials, remote-code-execution flaws and vulnerabilities that were actively exploited before many customers patched them.

Premium camera brands can also ship fragile firmware, broken upgrades, browser incompatibilities, licence problems and cloud outages. They can produce terrible night images when the lens is dirty, the infrared reflects from the dome, the shutter is wrong or the camera angle is useless. A premium logo cannot recover detail that never reached the sensor.

What mature suppliers more often provide is not perfection. It is process: clearer support ownership, published advisories, signed updates, longer firmware maintenance, documented hardening and a credible organisation to call when something goes wrong.

Those things have real value. They should still be verified rather than assumed.

There is more than one Chinese camera industry

"Chinese camera" describes a country of manufacture, not one engineering culture.

The category includes anonymous white-label products, original-design manufacturers selling the same platform under dozens of names, enormous vertically integrated suppliers, specialist industrial manufacturers and newer companies deliberately moving toward international security and usability expectations.

Some products are genuinely a mess: recycled firmware, questionable cloud dependencies, poor documentation and mechanical shortcuts.

Others are moving closer to Western standards and, in some functions, may already outperform established competitors. The market is allowed to contain both facts at once.

Value is a system calculation

A camera costing one quarter as much is not automatically better value. A camera costing four times as much is not automatically four times better.

Value includes installation labour, configuration time, cyber controls, replacement visits, firmware maintenance, image usability, integration effort, storage efficiency, licence cost and the operational consequences of missed or false events.

For a low-risk indoor application, a basic camera on an isolated network may be completely rational.

For evidential identification, critical infrastructure, biometric processing or a remote coastal site, the requirements should be much higher.

Procurement becomes sensible when the risk class is defined before the brand shortlist.

The better procurement question

The East-versus-West argument is attractive because it replaces investigation with a label.

It does not tell us whether the camera supports secure updates, whether cloud access can be disabled, whether the enclosure survives the site, whether the night image is usable, whether the analytics work or whether anyone will still issue firmware in five years.

Country of origin may still matter for supply-chain policy, legal obligations, data jurisdiction or geopolitical risk. Those are valid considerations when they are stated honestly. They are not a substitute for technical testing.

The right camera is the one that fits the solution. Test the product, constrain the network, verify the image, understand the cloud path and price the entire lifecycle.

Final thought

Chinese manufacturers deserve criticism where the engineering is poor, the security model is weak, the translation is broken or the cloud behaviour cannot be explained. Western manufacturers deserve the same treatment.

The industry improves when buyers stop purchasing mythology and start demanding evidence.

In the end, country of origin does not dictate quality. Many Western-branded cameras are manufactured in China, often using the same factories, components and supply chains as local brands. What should determine the choice is the quality of the finished product, the clarity of its documentation, the strength of its support, the security of its design and the transparency of the manufacturer.

The right camera is not the one with the right flag on the box. It is the one that is fit for the application, properly supported and honest about how it works.

Lincoln Potter: Zen and the art of security science

2026 NZ Outstanding Security Performance Awards Lifetime Achievement recipient Lincoln Potter has turned a career-long love affair with security science into an artform, writes chief editor Nicholas Dynon.

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

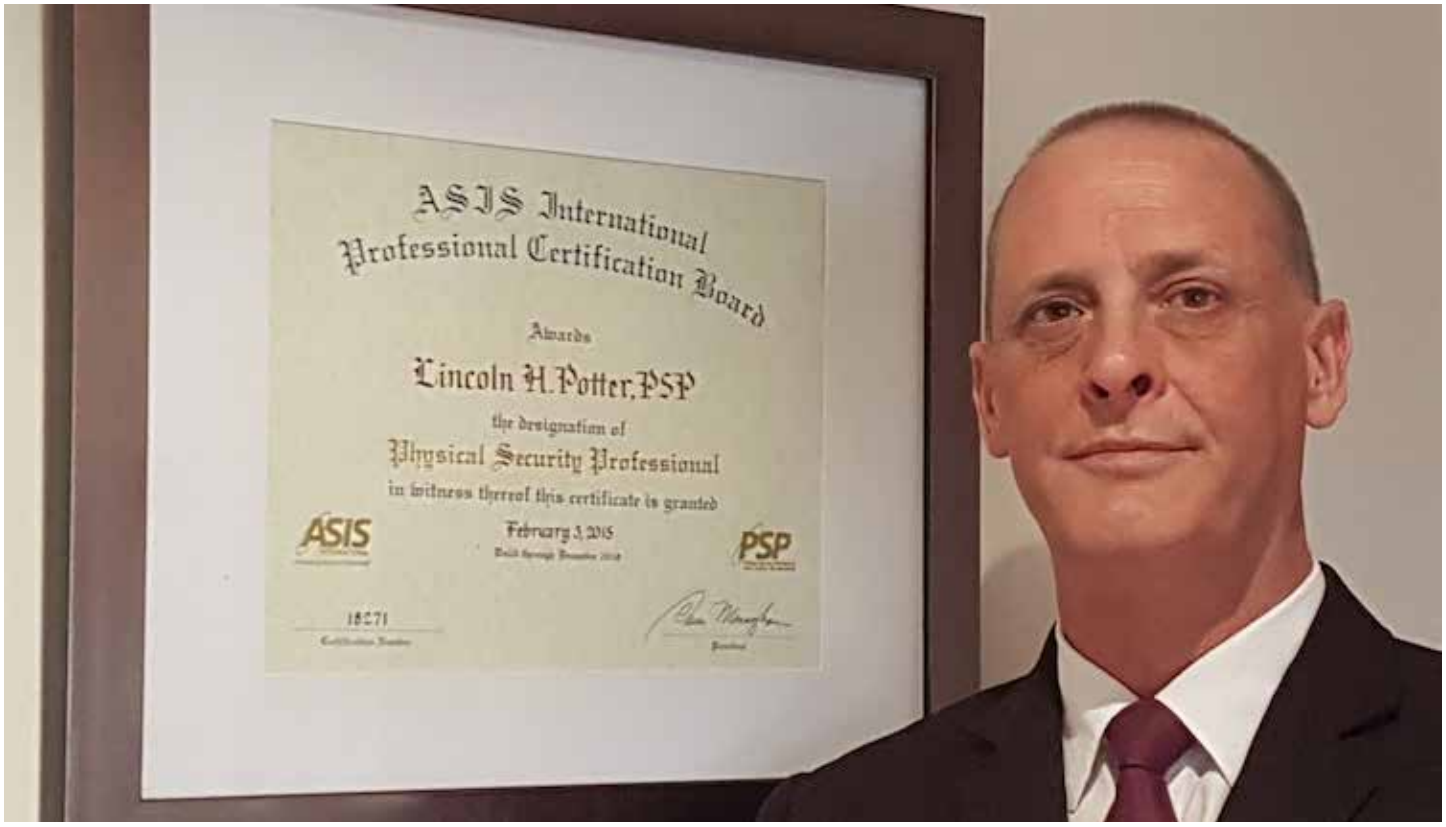
On 26 June, security consultant Lincoln Potter was recognised with the 2026 New Zealand Outstanding Security Performance Award (OSPA) for Lifetime Achievement. He now becomes the latest inductee into the international Security Hall of Fame.

Full disclosure. I'm a friend of Lincoln Potter. We go back about a decade. So ,what you're about to read – should you choose to continue reading – is unlikely to come across as an example of dispassionate, flawlessly objective journalism. But it will make for a good story.

I first came across Lincoln at the former NZSA office in Takapuna, Auckland. An enthusiastic – if not intense – trainer, he was putting Certificate of Approval candidates through their paces with a de-escalation scenario. He set the scene, he turned on the tension, he moved from one student to the next, correcting their stance, drawing their unknown inner authoritativeness out into the open, and doing so via a resonant frequency tuned just right. He knew his audience. After all, he'd been one of them.

And he'd had to work at it. Over many years. From all accounts, a young Lincoln Potter did not cut a physically imposing figure. Genetics dictated that no amount of gym work and protein supplementation was likely to fill out his patrol uniform in ways he would have preferred.

While mass can be helpful, Lincoln gravitated early to the idea that the absence of mass can be just as powerful – that presence and strength can be derived as much from space and the



intangible energies that we fill it with as it can from brawn and bluster. This drew him naturally to the martial arts.

He would ultimately spend years tempering his body in the suburban dojos of various Japanese martial art disciplines, complementing this with intellectual explorations into bushido (the way of the warrior) and a range of Eastern philosophical traditions – what he would refer to as types of 'shadow work', or behind-the-scenes self-improvement.

Whether the martial arts imbued within Lincoln a quiet sense of self discipline, whether it afforded him a degree of physical confidence, whether it gave him a couple of extra tricks up his sleeve in the heat of an exchange, or a transcendent ability to de-escalate, it – no doubt – supplemented the toolset he has used to carve out a uniquely exceptional career in security.

Decades later, there isn't much in the private security industry that Lincoln Potter hasn't done. He's held the torch and the keys, he's worked in close protection, cash in transit, guarding and patrols, eventually branching out into investigations, electronic security, training, and ultimately delivering security consulting services at the apex of the profession.

From the ground up

Lincoln commenced his security career in 1990 as a self-employed security operator providing venue security, personal protection and retail loss prevention services.

Although he may have grown up in Rotorua, he has invariably described himself as a West Aucklander, a badge of honour he has worn for much of his life. It's a badge, at least in Lincoln's case, that comes complete with wry underdog humour, a habitual and panoptical wariness, a sense of right and of wrong – and a heightened readiness to put the latter in its place when needed.

It's a readiness that's been well demonstrated in the retail setting. During a relatively short stint as a contracted loss prevention officer for Pak'nSave in the mid-1990s, he apprehended 473 shoplifters.

The initial two decades of his career saw him perform in a diverse range of security practitioner roles with increasing levels of superiority, while also achieving several certificates in guarding, patrolling, and close protection, and National Certificates in Security (Levels 2, 3 and 4).

He was employed by the Reserve Bank of New Zealand and then Television New Zealand providing in-house security between 1996 and 2006, spending his time between control rooms and patrol routes. During this period, he also worked for Chubb New Zealand providing cash-in-transit services and flexing his electrotechnical muscles installing security systems in residential and commercial properties.

Between 2006 and 2010, he worked in investigations as a self-employed surveillance operator, further expanding his suite of professional competencies.

Training and mentoring

In 2010, twenty years after starting out in security – Lincoln's security career took a turn towards training, auditing, and, ultimately, security risk consulting.

His influence on the early careers of security practitioners across New Zealand gained momentum with his appointment as a Security Tutor at New Zealand Career College where he delivered training in security – as part of a government initiative – to unemployed job seekers.

As a trainer, Lincoln's humble, humorous, and engaging style, and his ability to connect with people from diverse backgrounds and walks of life, found appeal among cohorts of new and aspirant security officers.

Having completed the National Diploma in Security (Levels 5 and 6) and qualifying as a NZQA Assessor to assess the Unit Standard 4098 in 2014, Lincoln continued his journey of professional mastery with the ASIS International Physical Security Professional (PSP) Board Certification in 2015, the NZSA Security Consultant Certificate of Competence in 2016, and the Building Networks Certification of Completion in IQP Compliance in 2022.

Between 2013 and 2025, Lincoln travelled extensively around the country as a New Zealand Security Association (NZSA) trainer and auditor delivering licensing training for security guards and crowd controllers, conducting audits of NZSA corporate member businesses, tutoring and assessing candidates for the National Diploma in Security, and advising security providers on compliance with industry codes and standards.

In this role, states David Horsburgh, a 2023 OSPAs Lifetime Achievement Award recipient, "Lincoln influenced the improvement of NZSA standards against which industry players were audited, thereby raising the quality of systems to create safe and secure environments and the protection of communities."

Lincoln concurrently acted as a security consultant to a wide range of customer organisations, delivering threat and risk assessments, lighting and CPTED analyses, advising on electronic and physical security controls, and generally uplifting their security risk maturity. The outcomes he achieved for his clients were recognised with several professional awards, including the 2016 New Zealand Security Award for Security Consultant of the Year, and the 2022 New Zealand Outstanding Security Performance Award (OSPA) for Outstanding Security Consultant.

Telling it how it is

Widely acknowledged as a security risk Subject Matter Expert, Lincoln's insights have been sought by national media outlets, conference organisers, industry associations, and professional security publications. In an investigative article published in April 2022 by both Radio New Zealand and *The New Zealand Herald*, journalist Farah Hancock wrote:

"Lincoln Potter has been in the security game for three decades; he's done retail security, trained security officers and close protection teams, studied security sciences, and the New Zealand Security Association suggests him as the person to talk to about CCTV."

"Sometimes he's found himself caught between CCTV system vendors and clients," she continues. "He's not always popular with vendors, as he has no qualms telling clients if they're being offered a system with unnecessary bells and whistles.

With a track record of articulating evidence-based positions on security matters, Lincoln articulates sometimes unpopular positions with clear-eyed objectivity and professional accountability. In Lincoln parlance, he's "not going to blow smoke in your face and tell you lies."

Several of his articles have been published by the *New Zealand Security Magazine*, including pieces identifying systemic issues preventing effective training in the security industry, first-of-its-kind technical guidance on the security-by-design construction of monitoring centres, insights on operationalising New Zealand's Protecting Crowded Places from Attack counter-terrorism guidance, and security officer-level insights on guarding in a "post-compliant society".

His "Guarding in a post-compliant society", an article published in the December 2017 issue of *NZSM*, somewhat prophetically argued that many of the difficulties being faced by front line security officers tended to have less to do with training gaps and more to do with the fact that members of the public were becoming less civil and less likely to comply with directives.

"Security officers have no special powers and the acts of law that support us are very weak," he wrote. "The key skill of officers thus lies in their ability to get people to acquiesce".

"The fact is that people are no longer prone to acquiescence. People will not comply anymore. The one thing that we relied on to do our job has gone and it's not coming back."

While most of us tend to associate the post-Covid world with a societal spiral into incivility and aggression in public spaces – and especially retail environments, Lincoln was deftly reading the room long before border closures and lockdowns brought the behavioural downsides of collective cabin fever to national attention.

To again borrow a phrase from Lincolnian lexicon, we have "angrier resting faces" than we used to.

Voluntary leadership

While his ability to communicate complex security concepts to non-specialist audiences have seen him commenting in the media and presenting at many speaker events, perhaps the most compelling examples of Lincoln's impact have been in his various voluntary roles within the security industry.

He has served as a member of the Crowed Places Security Advisory Group, the NZSA Security Consultants Special Interest Group and NZQA Special Interest Group, and the NZSA and NZQA Targeted Review of Qualifications. His voluntary leadership within the ASIS International NZ Chapter included serving as Treasurer and later as Deputy Chair and Head of the chapter's Shadow Committee.

It hasn't always gone well. The underdog from the west has low tolerance levels for bad behaviour, browbeating, and backbiting; and as ready as Lincoln has been to give of his time to voluntary teams he's just as readily walked away when he's sensed things were not quite right.

For the most part, it's been smooth sailing. His multi-year voluntary service for ASIS resulting in his being awarded a prestigious ASIS International Meritorious Service Award in 2018. Recognising exceptional service and dedication, the award is bestowed upon volunteers who go above and beyond in supporting their local chapters and the global security community.

Lincoln accepts the 2022 Outstanding Security Consultant award from OSPAs judge Dr Bridgette Sullivan-Taylor.

Wise counsel

An interesting and unsung example of Lincoln's impact is seen in his mentorship of 2025 New Zealand Security Awards Security Supervisor/ Operations Manager of the Year winner Nanaia Haua of Dunedin-based SPS Security. Nanaia was recognised for turning around the fortunes of SPS Security from a pending PSPLA-enforced closure that would have seen in excess of 100 staff lose employment.

The NZSA had recommended that SPS work with Lincoln to identify and implement changes needed to avoid the company's closure. Lincoln's analysis, advice and coaching were instrumental in getting the business back on track to a standard that met the PSPLA's requirements and ultimately drew public praise from PSPLA Chair Trish McConnell.

Importantly, the company retained its customers and staff, improved its performance, and became the subject of glowing testimonials.

Some last words

According to ASIS International Regional Vice-President, Ngaire Kelaher, who has known Lincoln for close to three decades, two of his qualities have consistently stood out.

"The first is his genuine passion for his work and the pride he takes in everything he does," Ngaire told me.

"Lincoln has always been deeply committed to the security profession, his clients, and the people they serve. He consistently strives to uphold the highest professional standards, and that commitment has never wavered."

The second, says Ngaire, is his dedication to continuous professional development.

"Over the decades, I've seen firsthand his ongoing commitment to learning, growing, and developing both personally and professionally. He actively seeks opportunities to expand his knowledge and improve his skills, setting an excellent example for others in the industry".

"His enthusiasm and sense of humour clearly reflect the genuine enjoyment he finds in being part of the industry."

Andrew Thorburn, past ASIS New Zealand Chapter Chair and security industry luminary, describes Lincoln as a "unique security practitioner, who has brought diverse practical experiences married to a deep understanding of the science of protective security and risk management."

"A long-time martial arts practitioner and archer," said Andrew, "his subsequent calm in the eye of a storm has enabled development and delivery of national training to New Zealand's leading brands providing services including security guards, security technicians, incident management, and corporate security to clients for over two decades."

Apparently, he's also an occasionally snappy dresser. "When Derek Kolstad created the John Wick franchise in 2014," said Andrew, "he needed look no further than an unassuming figure dressed in an all-black three-piece suit at the back of the security conference or industry awards room."

From his role in influencing many cohorts of early career practitioners along their development journeys to transforming businesses and influencing the uptake of industry codes and standards, very few individuals have done more to make New Zealand's security industry a better, more respected industry to work in.

Lincoln Potter is the very definition of a lifetime achiever, and I am honoured to be counted among his friends.

Crossing the Ditch: Reflections on security practice in New Zealand and Australia

Security professionals in New Zealand and Australia have much to learn from each other, writes security and risk specialist and former ASIS NZ Chapter Chair Johan Janse van Rensburg.

Johan Janse van Rensburg is an accomplished security risk professional and a former ASIS NZ Chapter Chair.

Having spent over two decades working in security across South Africa and New Zealand before recently relocating to Australia, I have found myself reflecting on a simple question: "What does security actually mean?"

At first glance, the answer appears straightforward. Most people think of security in terms of guards, CCTV cameras, alarms, and access control systems. Indeed, while these measures are important, they represent only a small part of what modern security has become.

My experience working in across South Africa, New Zealand and Australia has highlighted subtle yet important differences in how the profession is viewed, governed, and practised.

In New Zealand, security has traditionally been highly operational and relationship driven. Much of the profession evolved from practical experience, built on strong interpersonal relationships, trust, and an ability to solve problems pragmatically. Security professionals often wear multiple hats, simultaneously balancing operational delivery, emergency management, health and safety, investigations, business continuity, and physical security responsibilities.

This approach has many strengths. New Zealand security practitioners are often highly adaptable, resourceful, and capable of achieving effective outcomes with limited resources. The country's emergency management culture, shaped by earthquakes, natural disasters, and national crises, has also fostered strong resilience capabilities and a collaborative approach across agencies and industry.

At the same time, I have observed that security in New Zealand is still frequently perceived as an operational service rather than a strategic organisational capability. Security teams are often positioned lower within organisational structures and can struggle to gain executive visibility or influence broader business decisions.

Australia, by comparison, has demonstrated a more mature and structured approach in many sectors, particularly within critical infrastructure, government, and large corporate environments. (It does need some more work though).

Since moving to Australia, I have observed a greater emphasis on governance, enterprise risk management, assurance, and regulatory compliance. Security is increasingly viewed not simply as a protective function, but as an enabler of organisational objectives.

The introduction of the Security of Critical Infrastructure reforms, the widespread adoption of Enterprise Security Risk Management principles, and the growing use of frameworks such as AS HB 167:2025 have

accelerated this shift. Security discussions frequently occur at executive and board level, particularly within organisations responsible for nationally significant assets and essential services.

This perspective aligns with what I believe security fundamentally represents. Security is not a product. Security is not a department. Security is not a single technology or physical safeguard. Security is an organisational capability.

A contemporary definition might describe security as:

"The organisational capability to protect people, assets, information, and operations from threats through governance, risk management, resilience, and appropriate protective measures, ensuring confidentiality, integrity, availability, authenticity, accountability, and the continuity of organisational objectives."

The easiest way to understand this concept is to compare security to protecting a home. Most people assume home security consists solely of locking the front door. In reality, protecting a home involves much more. It includes understanding potential threats, establishing routines, installing appropriate protections, preparing for emergencies, and ensuring the family can recover if something goes wrong.

Organisations are no different. Security exists to protect people, assets, information, and operations from a wide range of threats, including criminal activity, cyber-attacks, insider threats, fraud, natural disasters, and human error.

Achieving this requires effective governance, clear accountability, robust risk management processes, organisational resilience, and security measures proportionate to the risks faced.

An analogy I often use is the human body.

Governance is the brain, providing direction and decision-making. Risk management represents the senses, identifying danger and informing action. Protective measures are the skin, immune system, and reflexes that defend against harm.

Resilience is an organisation's capacity to recover following disruption. Security, in its broadest sense, is an organisation's overall ability to survive and continue functioning.

Both New Zealand and Australia have much to learn from each other. New Zealand's strengths lie in its agility, pragmatism, and collaborative culture. Australia, on the other hand, excels in governance maturity, strategic integration, regulatory frameworks, and an increasing recognition of security as an enterprise-wide capability.

The future of the security profession lies in combining these strengths.

As security professionals, we must continue to move beyond traditional perceptions that centre solely on guards, gates, and technology. Security should be recognised as a strategic business capability that enables organisations to achieve their objectives, remain resilient, and continue operating effectively in an increasingly uncertain world.

Ultimately, security is not about protecting assets merely for the sake of protection. It is about enabling organisations, communities, and people to continue functioning, regardless of the challenges they encounter.

Will ‘move on’ orders for rough sleepers make cities safer – or revive Victorian era cruelty?

Weeks after being introduced, a bill to enable police to issue ‘move on’ orders has attracted unusually broad opposition, writes Kris Gledhill, Professor of Law, Auckland University of Technology.

Kris Gledhill is a Professor of Law at Auckland University of Technology.

A proposed law currently before New Zealand’s parliament would give police the power to move people on from public spaces if they are found begging, rough sleeping or otherwise causing a disturbance.

Under the Summary Offences (Move-on Orders) Amendment Bill, police would also be able to detain a person, collect their personal details, formally issue the order and serve it on them.

Recipients could even agree to have the notice served by email. It can last for up to 24 hours; and the police decide how far away the person has to move.

Breaching an order could result in a fine of up to $2,000 or three months’ imprisonment, while providing false details could attract a $500 fine.

Supporters say the bill – being considered by parliament’s Justice Select Committee and presently open to public consultation – will help police deal with disorderly behaviour and make town centres safer.

Critics argue it risks criminalising homelessness and poverty while doing little to address the underlying causes.

More than a century ago, colonial New Zealand law allowed people to be prosecuted as vagrants if they could not explain how they supported themselves.

There are uncomfortable echoes of that approach in the proposed legislation.

Like its Victorian-era predecessor, the bill reflects a view that people on society’s margins should be managed through the criminal justice system, rather than through social support.

Contradictions and carve-outs

Introducing the bill to parliament last month, Justice Minister Paul Goldsmith framed the move as part of a government commitment to "fixing the basics in law and order". The suggestion is it fills a gap.

A closer reading of the bill, however, reveals some clear limitations.

Its definition of "rough sleeping", for instance, expressly does not cover freedom camping. Its wording around "begging" also excludes so-called "chugging", where people solicit donations or memberships for non-government organisations.

That creates some curious anomalies. A homeless person asking passers-by for money could potentially be moved on, but not if they were collecting donations on behalf of a charity.

The bill also exempts people who are primarily engaged in promoting "a point of view, cause or campaign". This might mean someone protesting homelessness or poverty – even while sleeping rough or seeking donations – may be protected from a move-on order in circumstances where someone without a political message would not be.

Another point critics have seized upon is that police already have plenty of powers to draw upon if needed.

The Summary Offences Act 1981 already contains offences covering disorderly and offensive behaviour. Police can direct groups engaged in threatening or disorderly conduct to disperse and can require people to stop obstructing public rights of way, with failure to comply carrying its own penalties.

It therefore might be asked whether the Government is genuinely trying to "fix the basics" – or is simply playing politics at the expense of some of society's most marginalised people.

More questions than answers

Weeks after being introduced, the bill has attracted unusually broad opposition. Critics range from opposition parties, homelessness advocates and Māori organisations to Auckland Council.

Both the Ministry of Justice and Attorney-General have also raised concerns, the latter concluding that provisions targeting begging and rough sleeping would place an unjustified limit on rights.

Judges, for their part, have long recognised that people experiencing housing insecurity often find themselves in the criminal justice system.

Specialist courts such as Auckland's Court of New Beginnings and Wellington's Court of Special Circumstances attempt to address the underlying causes that bring people before the courts and help reduce the likelihood they will return.

To those who understand the complexities of homelessness, this might well appear a more logical approach than police officers repeatedly detaining people and issuing forms.

The new detention power also carries legal implications. People detained by police have the right to legal advice, meaning officers would need to advise recipients of those rights and facilitate access to a lawyer, even where issuing a move-on order may be a relatively brief process.

Elsewhere, there are important questions about police duties towards vulnerable people. What happens, for instance, if someone is moved on and subsequently comes to harm?

And what if that person is a teenager? Here, too, the bill raises questions. Police face significant legal restrictions when dealing with young people, and in many situations powers under the Oranga Tamariki Act 1989 will be more appropriate than issuing a move-on order.

The Select Committee is due to report back on the bill by early September. Whether it is a legislative priority before November's general election.

What is clear, however, is that the bill rejects a focus on homelessness as primarily a social problem and returns to the Victorian notion that homeless people are to be managed as a public nuisance through criminal justice powers.

This article was originally published in The Conversation on 12 June 2026.

2026 New Zealand OSPAs Winners Announced

Wulf Security takes home three gongs and Gallagher Security two in this year's Outstanding Security Performance Awards (OSPAs).

The security profession was the big winner on the night as Professor Martin Gill and the OSPAs once again shone their annual light on outstanding performance in New Zealand's security sector.

The presentation of the fifth annual New Zealand Outstanding Security Performance Awards (OSPAs) took place on Friday, 26 June 2026, in the Pakuranga Hunt Room at the Ellerslie Event Centre as part of the ASIS New Zealand Certification Celebration.

Security professionals from across New Zealand gathered to recognise and celebrate excellence, innovation and outstanding achievement across the security sector. Awards were presented across 11 categories, with the ceremony hosted by OSPAs Founder, Professor Martin Gill.

"Huge congratulations to every finalist. Only those who clear the judging threshold make the list, so getting there says something real about the work you do," said OSPAs Regional Advisor Luke Gough.

"And to the winners, very well deserved. Every one of you now goes through to the Global OSPAs to represent New Zealand on the world stage, and you have absolutely earned it."

In addition to the NZ OSPAs category winners, ASIS International certifiers and re-certifiers were recognised, as well as New Zealand's two 2026 Global OSPAs winners, Global Security's Shaun Laifone and Beca Applied Technologies' Ruth Tongotongo.

"Nights like these matter. Not just for the recognition, but for shining a light on a sector full of people quietly doing outstanding work, often without the spotlight," said Luke Gough.

The 2026 NZ OSPA winners are:

Outstanding In-House Security Manager/Director
Kurtis Heketoa – Te Whatu Ora – Counties Manukau

Outstanding Contract Security Manager/Director
Pat Wulf – Wulf Security Services

Outstanding Security Team
Profit Protection Team – The Warehouse Group

Outstanding Contract Security Company (Guarding)
Wulf Security Services

Outstanding Security Consultant
Rehan du Toit – Beca Applied Technologies

Outstanding Security Installer/Integrator
Nedax

Outstanding New Security Product
AccessNow – Gallagher Security

Outstanding Security Partnership
Profit Protection Future Forum – New Zealand Committee Members

Outstanding Security Officer
Samisoni Taufoou – Wulf Security Services

Outstanding Female Security Professional
Harriet Sommerville – Gallagher Security

Outstanding Young Security Professional
Simon Mackereth – Red Badge Group

Lifetime Achievement
Lincoln Potter

"The OSPAs would like to congratulate all finalists and winners for their outstanding achievements and thank everyone who contributed to making the 2026 New Zealand OSPAs a success," said the organisers. "A special thank you goes to our category sponsors for their valued support: Gallagher, Guardhouse & Luke Gough Consulting.

"We also extend our sincere thanks to the judges, ASIS New Zealand, and everyone who supported this year's awards programme and helped celebrate excellence across New Zealand's security profession."

Winners in selected categories will automatically qualify for the Global OSPAs and the Lifetime Achievement winner will be inducted into the Security Hall of Fame.

Outstanding Security Performance Awards

Australian Protective Security Policy Framework 2026 release now available

The 2026 update to the Australian Government's Protective Security Policy Framework (PSPF) introduces new guidance on emerging technologies and counters foreign intelligence and interference.

The Australian Government Department of Home Affairs last month published PSPF Release 2026. The PSPF is a protective policy framework for government agencies and related entities that plays a role similar to the New Zealand Government's Protective Security Requirements (PSR).

According to the Department of Home Affairs, PSPF Release 2026 reflects an ongoing commitment by the agency to "ensuring protective security policy remains responsive and fit for purpose, enabling the Australian Government to protect, deter and respond to current and emerging security threats."

This latest release introduces policy improvements on emerging technologies, including:

- transition planning post-quantum cryptography
- training on artificial intelligence (AI) use
- bring-your-own-device obligations.

The release also focuses on personnel security, including strengthening restrictions on personnel posting security clearance information on online platforms as well as addressing training on countering foreign interference.

In addition, the 2026 changes also enable future reforms to the Hosting Certification Framework and provides updates to the PSPF's information, personnel and physical security controls.

Of all the domains covered by the PSPF, it appears the most recent release leaves guidance on the physical security domain largely unchanged – apart from new information relating to Sensitive Compartmented Information Facility (SCIF) areas.

Among the SCIF-related content changes, the table "Security Zones Descriptions and Restricted Access" (Section 24.1, Table 38) now contains updated information on SCIFs. It states that the required security clearance for ongoing access is "Positive Vetting (PV) or TS-PA security clearance, with required compartment briefings, where TOP-SECRET systems are present."

Additionally, the table now states that restricted access to SCIFs includes: no public access; visitor access only for visitors with a need-to-know and with close escort; restricted access for authorised personnel with appropriate security clearance; and dual factor authentication for access control.

The other SCIF-related change is to be found close by at Section 24.2.2, where Requirement 199 now refers to the fact that the accreditation of SCIFs by the Australian Signals Directorate prior to operational use in done "in accordance with the National SCIF Accreditation Program".

Australian federal government agencies are required to apply the PSPF, while state and territory government agencies that hold or access Australian Government security classified information are required to apply the PSPF to regulate access to that information.

Non-government organisations and third-party service providers may be required to implement aspects or parts of the PSPF as detailed in relevant agreements between the Australian Government and the organisations/providers.

NZSA CEO's July Report

NZSA CEO Gary Morrison talks business sentiment, PSPLA licence requirements, good practice guidelines, NZSA AGM, NZ Security Awards, 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.

Traditionally my report provides an update on key matters within the security industry but this time I would like to comment on the positive changes happening within the New Zealand business environment.

Within the last two months there appears to have been a shift in business sentiment. It was evident in the coverage from Fieldays and was mirrored in discussions occurring across the floor at the recent SecTech Roadshow in Auckland, Wellington and Christchurch.

That same shift comes through in the latest 2degrees Shaping Business Study, which surveys businesses across the country about their outlook, challenges and priorities. The survey shows in excess of 60% of businesses expecting revenue growth this year and the picture it paints is of a business community that is realistic about the challenges it faces but is increasingly confident in its ability to navigate them.

Business sentiment has a significant impact on society. When businesses feel confident, they hire, invest and take risks. When they don't, they contract, defer and protect.

For several years the dominant business mode has been one of endurance, getting through, managing down and waiting it out. That has made some sense given the shocks faced including a pandemic, supply chain disruption, rapid inflation, sharply higher interest rates and a cost of living squeeze that has hit both consumers and businesses.

Thankfully, that perspective of endurance seems to be transitioning into a more forward-looking and optimistic position.

Part of what has enabled that broader shift seems to be attributable to a change in the political landscape and environment.

The Budget in May wasn't designed to excite anyone, it wasn't generous and it didn't try to be. What it was however was honest. It acknowledged trade-offs, restrained itself from promises it couldn't keep and treated New Zealanders as adults capable of understanding difficult choices. For the first time in a number of years, the signals felt like they matched reality rather than trying to paper over it.

Businesses seem to have noticed and responded. When the Government is straight with people about where things actually stand, it seems that businesses find it easier to plan, to invest and to back themselves. Certainty, even uncomfortable certainty, is more useful to a business than optimism that doesn't match the reality.

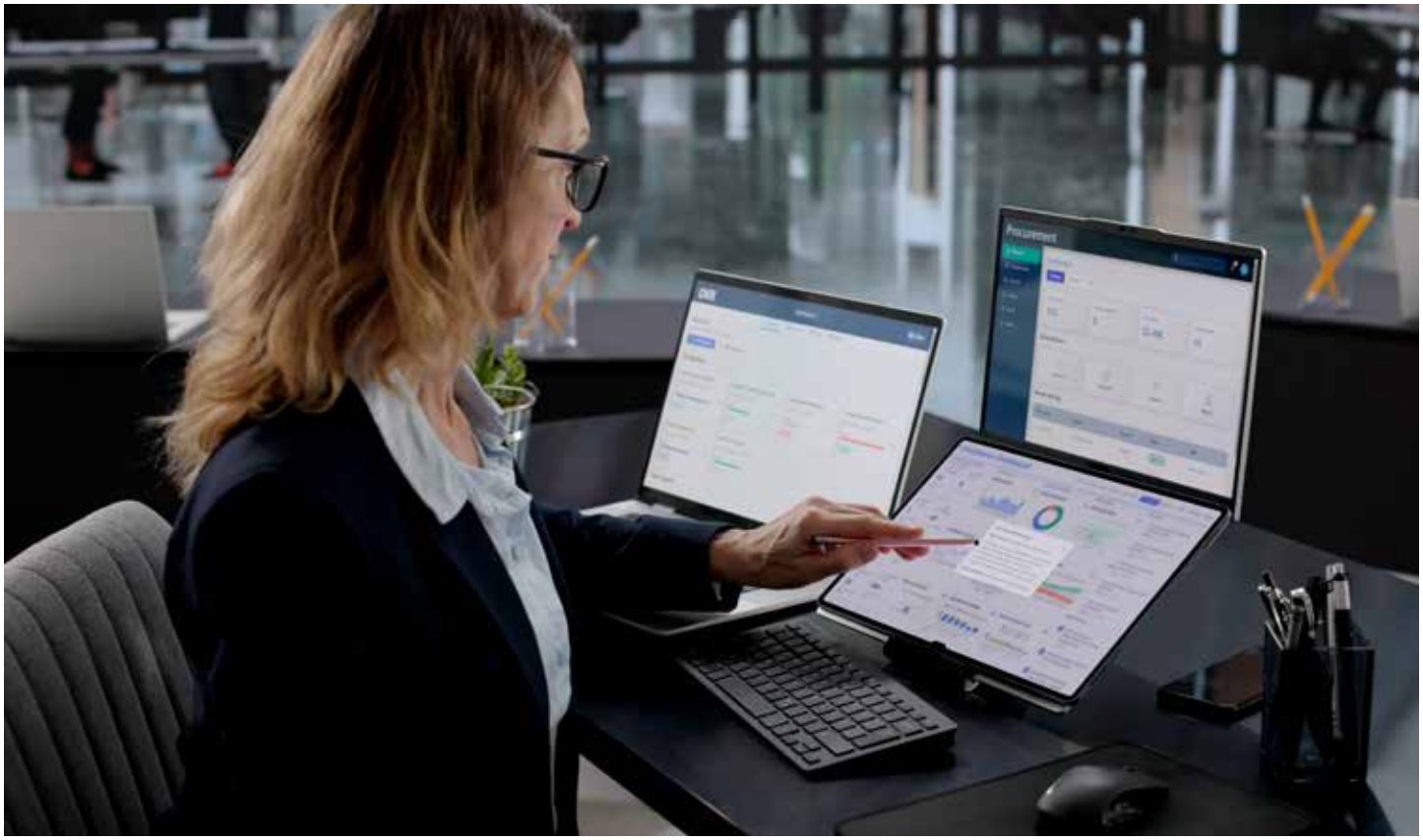
We can all agree that there are still issues and work to be done. Costs are still high, workforce pressures remain and productivity is stubbornly low meaning that business remains challenging. What we are seeing however is a general feeling that the direction feels right and that the mood has shifted from endurance to momentum.

The best news is that the security sector is well positioned to meet the needs of that momentum going forward.

Member News

Following on from my commentary above, I'm pleased to note the following business news:

Gallagher Group has announced that it is currently looking to recruit a further 100 employees to support the development of new generation security



software and hardware platforms. Initial recruitment is focused on software engineers, test engineers and product leaders. The hiring coincides with Gallagher Security's recent move of more than 200 team members into the Hamilton Innovation Park.

Intelligent Monitoring Group Limited, the owner of ADT Security New Zealand, has finalised the acquisition of BlueSky Holdco Limited, encompassing Tyco NZ and Red Wolf Security, from Johnson Controls. The purchase has added over 300 staff and 12 branch locations to IMG's portfolio and their combined workforce now exceeds 500 local staff.

PSPLA licence requirements for bureau monitoring and subcontracted services

The PSPLA has just provided a licensing guideline for businesses who contract third party licence holders to carry out particular classes of security work for their clients.

Sections 5 to 11 of the Private Security Personnel and Private Investigators Act 2010 defines the different classes of businesses which need to hold security licences. For each class the definition includes all those who are for valuable consideration carrying on business in that class. If a business is invoicing clients for a particular class of work, they would in most cases fit within the definition of carrying on business for valuable consideration in that class of work.

Any company or individual who is promoting themselves as offering a class of security business covered by the Act, and charging or invoicing their clients for that work, is required to hold a licence in that class even if they subcontract the work to an independent licence holder.

This will impact a number of security providers who hold the licence classes for their primary service, but not in the class where they contract to a third party.

Common examples include:

- Security Technicians or Electricians who charge their customers for monitoring but utilise a bureau monitoring provider (required to hold a licence as a Monitoring Officer).
- Security Consultants who offer or promote installation services but contract a licenced security technician or electrician to do the installation work (required to hold a licence as a Security Technician).
- Wholesalers or on-line retailers of security equipment that promote themselves as offering consultancy or installation services, charge their clients for that work, but use a third party licence holder to carry out the consultancy or installation work (required to hold a licence in class of Security Consultant and/or Security Technician).
- Security Technician or Electrician who offers a consultancy service but subcontracts the consultancy work to an independent licence holder (required to hold a licence in class of Security Consultant).
- A company that contracts with a client to provide guarding services but subcontracts the guarding work to other licence or certificate holders (required to hold a licence in the appropriate guarding classes).

A company licence holder who does not hold a licence in the correct classes should complete the online form on the PSPLA website, provide evidence of experience and competence, and pay the fee.

Evidence of experience and competence can include proof of NZSA membership (member certificate) or a letter from the party providing the subcontracted services.

Launch of new Good Practice Guidelines

The NZSA is pleased to announce the launch of two new Good Practice Guidelines:

Inspection and Maintenance of SS3/2 Access-Controlled Doors

Access-controlled doors play an important role in protecting people, property and assets. However, when these doors form part of a building's means of escape, they must also perform a critical life-safety function – allowing occupants to leave quickly and safely during an emergency. A door that fails to release when required can have catastrophic consequences, making regular inspection, testing and maintenance essential.

This guideline has been developed to promote a consistent, practical approach to the inspection and maintenance of Specified System 3/2 (SS 3/2) Access-Controlled Doors and provides information absent from the MBIE Compliance Schedule Handbook.

Application of Part 6A of the Employment Relations Act 2000

The New Zealand security industry operates in an environment where service contracts are regularly retendered, transferred between providers, outsourced, or bought in-house. These changes can have significant implications for both security officers and employers.

To provide greater employment security for workers affected by contract changes, security officers were included in the vulnerable worker protections contained in Part 6A of the Employment Relations Act 2000 from 1 July 2021.

Part 6A establishes rights for eligible security officers when security services are transferred from one employer to another and places obligations on both outgoing and incoming employers. The legislation is intended to support continuity of employment, preserve employment conditions, and provide a fair and orderly process when service contracts change hands.

This guideline provides practical guidance to help employers, employees, clients, unions, and other industry stakeholders understand and apply the requirements of Part 6A within the security industry.

The access Controlled Doors Good Practice Guideline can be accessed on the NZSA website and the Part 6A will be available within the next few weeks.

NZSA Position Statements

We are currently finalising two new Position Statements that should be available for release within the next few weeks.

The first covers the process for Children's Act (Vulnerable Children Act) Safety Checks for security personnel. A number of our members have reported challenges in obtaining what are known as VCA Checks due to Police Vetting Services declining requests on the basis that the roles concerned do not meet the statutory definition of a children's worker.

The Position Statement provides interim guidance whilst the NZSA looks to engage with New Zealand Police Vetting Services, Health New Zealand and relevant government agencies to seek further clarification regarding application of Children's Act safety checking requirements for security personnel.

The second Position Statement will provide clarity on the proposed Citizen's Arrest legislation and implications for the security industry. Whilst the proposed expansion of citizen's arrest powers may provide retailers and security personnel with additional options in certain circumstances, any exercise of these powers must be undertaken lawfully, safely and with appropriate regard for the welfare of all parties involved.

The Position Statement reinforces the health and safety obligations under the Health and Safety at Work Act 2015 and the requirement that citizen arrest activities must only be undertaken by personnel who have received appropriate training and who can demonstrate the competencies required to perform the role safely. Risk management, de-escalation and personal safety must remain central to considerations and citizen's arrest powers must be exercised only when lawful, necessary and proportionate.

New Codes of Practice for Security Consultants and Secure Destruction of Sensitive Materials

We are pleased to announce the introduction of two new NZSA Codes of Practice covering work performed by Security Consultants and the Document Destruction providers (secure destruction of sensitive materials).

Both documents have been developed following engagement with appropriate subject matter experts and the SCSIG (Security Consultant Special Interest Group).

Having these documents in place will now allow us to work on extending the Member Self-Audit program and the Member Accreditation Audits, to include members providing security consulting and document destruction services.

Copies of both Codes of Practice can be downloaded from our member management system Gecco. If you require login instructions please email nzsa@security.org.nz.

NZSA Self-Audit Program

The NZSA Self-Audit program commenced in April this year and has pleasingly received very positive feedback from those members who have already completed the self-audit process.

All Corporate Members are now required to complete the self-audit on a yearly basis and with the audits spread throughout the year to ensure an even workflow for our independent auditors.

The self-audits will take most members approximately 20 to 30 minutes online and effectively cover the key components of the NZSA Codes of Practice that are applicable to the member. The submissions are reviewed by one of our two independent auditors and where appropriate, they may provide guidance back to the member on areas of possible business improvement.

Resilience Planning for Security of Crowded Places Forum

We are thrilled that this year's Crowded Places Forum being held at Eden Park on the 21st and 22nd July has sold out, with in excess of 130 attendees and a waiting list.

Whereas last year's inaugural event was focused on launching the NZ Police Crowded Places Strategy of Escape, Hide, Tell, this year will be more targeted on providing learning and guidance opportunities for those responsible for the security of crowded places. The agenda covers a broad range of topics and quality local and international speakers and will include several desk top scenarios that will provide experiential learning.

As an added bonus, we are pleased to advise that the forum will be MC'd by journalist and political reporter Barry Soper.

NZSA AGM and Board Member Nominations

The NZSA AGM will be held on Tuesday 18th August in Auckland. In conjunction with the AGM, we will this year be seeking to appoint 3 new board members with Alision Kingdon, Brett Wilson and Matt Stevenson not seeking re-election this year.

Full details on the AGM and Board Member nominations will be provided in coming weeks.

New Zealand Security Awards Event

A reminder that the nomination window for the 2026 New Zealand Security Awards is now open, and with the closing date of Friday 31st July.

This is the supreme awards event for the New Zealand security industry and the winners across 19 award categories will be celebrated at the Awards Dinner to be held on the evening of Friday 11th September at Hui Hui, Parliament Building, in Wellington.

This is the chance to recognise high performers within your team and the nomination process is online here and easy to complete.

On a final note, congratulations to all winners at the OSPAs event held in Auckland last week, and in particular to Lincoln Potter who won the Lifetime Achievement Award. Lincoln spent a number of years working as an independent consultant to the NZSA and has been instrumental in developing industry training, codes of practice, and guidelines as well as being an NZSA auditor.

As always, we welcome all comments and feedback on NZSA or industry issues and activity.

Keep safe and well.

New Stalking and Harassment Offence: Implications for investigators and security professionals

Daniel Toresen, Chair, New Zealand Institute of Private Investigators writes that new legislation is likely to further distinguish compliant investigators and security professionals from non-compliant operators.

From 26 May 2026, the Crimes Legislation (Stalking and Harassment) Amendment Act 2025 comes into force, creating a standalone criminal offence for stalking and harassment for the first time in New Zealand law.

The legislation introduces penalties of up to five years' imprisonment for patterns of behaviour directed at another person where the conduct is known to be likely to cause fear or distress. Importantly, the law focuses on cumulative conduct rather than isolated incidents. A pattern may be established by specified acts occurring on at least two separate occasions within a two-year period.

This development is highly relevant to both the private investigation and security sectors. Certain legitimate professional activities may, in some circumstances, superficially resemble conduct contemplated by the legislation.

These may include surveillance, repeated attendances, following or monitoring individuals, covert online enquiries, contacting associates or witnesses, workplace enquiries, field intelligence gathering, and the use of digital tools.

The key distinction under the new framework will be lawful purpose, proportionality, professional conduct, and proper documentation.

The legislation contains protections for conduct undertaken for a lawful purpose, with reasonable excuse, or in the public interest. However, investigators and security professionals should expect complaint-driven scrutiny to increase, particularly in emotionally charged matters such as relationship disputes, family matters, employment issues, workplace conflict, and private domestic enquiries.

NZIPI considers the legislation reinforces the importance of:

- maintaining clear written client instructions
- confirming that investigations have a legitimate evidential, legal, commercial, safety, or public-interest purpose
- operating within strict professional and ethical boundaries documenting investigative rationale, decision-making, and proportionality
- complying fully with Privacy Act obligations
- maintaining robust operational policies and supervision of subcontractors and field staff
- exercising caution with covert online investigative techniques
- ensuring surveillance and field activity is necessary, proportionate, and properly authorised

In practical terms, this legislation is likely to accelerate the professionalisation of the industry and further distinguish licensed, compliant investigators and security professionals from unstructured or non-compliant operators.

Daniel Toresen, Chair NZIPI

Members engaged in surveillance, field attendance, online intelligence gathering, process serving, workplace investigations, domestic matters, or protective security work should review their operational procedures carefully.

NZIPI will continue monitoring the implementation of the legislation and its practical application within the investigative sector. We also encourage members to seek independent legal advice where necessary regarding their own operational practices.

As an industry, we must continue demonstrating that professional private investigation and security work in New Zealand is conducted lawfully, proportionately, ethically, and in the public interest.

Firms struggle with geopolitical risk preparedness

A growing number of organisations recognise geopolitical risk as a critical business threat, yet few are adequately prepared to respond in a proactive manner, according to a new McKinsey & Company survey.

The survey, which canvassed senior executives across several sectors and regions, highlights a widening gap between awareness of geopolitical disruption and the practical capability to manage it.

While most respondents identified geopolitical instability as a top-tier risk—alongside cyber threats and economic volatility—only a minority reported having mature frameworks in place to assess, monitor, and respond to such risks.

Notable among the survey's findings is a shift in perception in which geopolitical risk is no longer being viewed as a distant or abstract concern but as a direct operational and strategic issue. Events such as supply chain disruptions, sanctions regimes, regional conflicts, and great-power competition are increasingly shaping business decisions.

However, despite this recognition, many organisations remain reactive in their approach.

According to the survey, fewer than one-third of companies have established formal processes to integrate geopolitical risk into enterprise risk management systems. Even fewer have dedicated teams or leadership roles focused specifically on geopolitical analysis.

In many cases, responsibility for such risks is fragmented across functions such as strategy, compliance, and security, limiting the organisation's ability to form a coherent response.

A key weakness identified is scenario planning. While executives acknowledge the importance of anticipating geopolitical shocks, only a small proportion of organisations conduct regular, structured scenario exercises.

The findings also point to a lack of real-time intelligence capabilities, with many organisations relying on external reporting or ad hoc analysis rather than maintaining internal capabilities to continuously monitor and assess geopolitical developments.

On the flipside, the survey identifies a cohort of "geopolitically resilient" organisations that are taking a more structured approach. These organisations are more likely to embed geopolitical considerations into strategic planning, invest in internal analytical capabilities, and conduct regular scenario testing. They also tend to maintain clearer governance structures, with defined accountability for geopolitical risk at senior levels.

Ultimately, the survey findings suggest the need for closer integration between corporate security functions, risk teams, and executive leadership. Beyond its strategic implications, geopolitical risk has direct operational consequences, including impacts on personnel safety, physical assets, and business continuity, that organisations ought to be planning for.

On the basis that geopolitical complexity is likely to intensify, organisations should look to move beyond high-level recognition towards actionable capability. This includes developing integrated risk frameworks, enhancing intelligence functions, and aligning security, risk, and strategy disciplines to greater effect.

NZ security news in brief

Gallagher launches visitor management solution, SME cyber insurance gap, cyberattacks target community sector, foreign intelligence agencies target job sites, new law targets antisocial road users.

Gallagher Security launches visitor management solution

Gallagher Security has announced the launch of their Visitor Management Solution powered by Kenai, a cloud-native platform. The launch follows Gallagher's strategic investment in Kenai and its appointment as the platform's exclusive global distributor announced earlier this year.

Natively integrated with Gallagher's Command Centre, the Visitor Management Solution is deigned to deliver a smooth user experience for visitors and staff across multi-tenant and campus environments.

"Gallagher is focused on the expanded value that security infrastructure can unlock for our customers," said Mark Junge, Chief Executive of Gallagher Security. "Kenai is a natural extension of that."

Rob Salzwedel, Co-Founder and Chief Executive Officer of Kenai, said the partnership with Gallagher opens a new level of reach and integration for the platform.

"Kenai was built to extend well beyond the sign-in screen. Integrated with Gallagher's solution, organizations get a single ecosystem that handles visitor and employee flows, inductions, evacuations, asset management, and space bookings, all connected and visible in one place."

Mark Junge, Chief Executive of Gallagher Security.

Cyber insurance gap leaves SMEs exposed to cyberattacks

Cyberattacks are becoming an increasingly significant threat to small and medium enterprises (SMEs), yet insurance adoption remains disproportionately low. Limited awareness of cyber risks, affordability challenges, and evolving threat landscapes continue to leave many SMEs financially exposed.

As cyber incidents grow in severity and sophistication, closing the protection gap has become a pressing priority for insurers, says GlobalData.

According to GlobalData's 2025 SME Survey, 34.7% of global SMEs had experienced a cyber incident in the past three years. In Europe, German SMEs are the most vulnerable to cyberattacks, with this figure rising to 40.3%. Yet cyber insurance is often viewed as an unnecessary product, with just 16.8% of global SMEs stating they have a standalone policy in place.

While some SMEs may be protected against cyber risks as part of another insurance policy, low penetration rates are alarming, signalling that most SMEs could be underinsured.

"Low cyber insurance rates among SMEs suggest that many smaller businesses are still overlooking cover—possibly because they do not understand the value of such policies," said Beatriz Benito, Lead Insurance Analyst, GlobalData.

"Hackers will naturally view SMEs as easier targets," she said. "A sizable cyberattack will have a massive financial impact on a large corporation, but on a smaller, less resilient business, an unexpected cash drain can cause immediate insolvency if they are not protected by an adequate cyber insurance policy."

Civil society organisations targeted by cyberattacks

Resource-strapped civil society organisations, from journalists to human rights groups, are increasingly being targeted with attacks once largely associated with governments and major enterprise, according to new data from Cloudflare.

Today, Cloudflare has published its latest, to mark the initiative's 12th anniversary, highlighting cyber threats targeting organisations working in the public interest globally, including those operating in Australia and across APAC.

Distributed Denial-of-Service (DDoS) attacks were the most common threat against Project Galileo participants. DDoS attacks accounted for 81.6% of overall malicious traffic requests, with Human Rights orgs facing the highest volume of DDoS attacks.

Attackers attempted to exploit weaknesses in websites' code to access internal systems, with journalistic organisations seeing the highest volume of these threats.

Cloudflare identified 85 government-directed Internet outages, representing 46% of all disruptions that the company could identify across its global network. The restrictions frequently coincided with periods of elections, protests, and student exams.

Competenz appoints Ruth Cooper as Executive Director

Industry training organisation Competenz has appointed Ruth Cooper as Executive Director, bringing more than 30 years of leadership experience across tertiary and vocational education in New Zealand and Australia.

Ruth Cooper Executive Director of Competenz.

Most recently, Ruth led Workforce Development, Strategic Partnerships, Work Integrated Learning and Alumni Engagement for Strategic Education Inc across New Zealand and Australia, overseeing five vocational and higher education institutions. She has also recently completed a contract as Engagement Lead on the Government's International Education Going for Growth Plan at Education New Zealand.

Her previous leadership roles include Chief Executive of Yoobee School of Design and Deputy Chair of Quality Tertiary Institutions (QTI), Ngā Wānanga Kounga. Throughout her career, she has built a strong reputation for strategic leadership, organisational transformation and forging partnerships that create meaningful educational opportunities.

She brings a strong understanding of te ao Māori, tikanga and iwi relationships, reflected in the partnerships she has developed to support education and training outcomes for Māori, Pacific peoples and underserved learners across Aotearoa.

"Competenz has an incredible foundation built over 30 years and a deep connection to the industries it serves," she said. "My focus is on building on those strengths while ensuring we remain agile, responsive and forward-looking."

Job sites targeted by foreign intelligence agencies

The New Zealand Security Intelligence Service (NZSIS) has joined Five Eyes partners to highlight increased targeting of professional networking sites and online job platforms for intelligence purposes by China's military intelligence services.

It involves individuals, including New Zealanders, being targeted through job and professional networking sites because of their access to privileged or classified information.

National security clearance holders, military personnel and those with access to sensitive government information are particularly at risk.

A malicious approach often begins with an innocuous sounding request for something on a benign topic. This progresses to requests on more sensitive areas such as military issues, international relations or insights on government decision making.

"There are basic steps you can take to protect yourself, most of which is common sense," said NZSIS Director General Andrew Hampton.

"Be very careful about the information you put online about yourself. We're not saying don't use social media or professional networking sites – just don't tell the world you hold a national security

clearance or work with sensitive government or military information.

"Be wary of unsolicited offers or approaches online that appear too good to be true, even if they seem legitimate," he added.

The NZSIS Protective Security Requirements (PSR) website has a range of information and guidance to support national security clearance holders and anyone with access to sensitive information.

Launch of SafetyNet Critical Communications

Minister for Emergency Management and Recovery Mark Mitchell welcomed the launch of SafetyNet Critical Communications (SafetyNet) on 01 July.

SafetyNet, a new independent Crown company, replaces Next Generation Critical Communications (NGCC). With an expanded mandate, SafetyNet is intended to strengthen New Zealand's emergency preparedness and response capability and ultimately, deliver better support to communities across the country.

"SafetyNet has a solid platform to build from. It will continue to lead and facilitate the ongoing development of a shared, secure, modern emergency grade communications ecosystem for the public safety sector," said Mr Mitchell.

SafetyNet will offer organisations active in everyday safety and emergency management access to its Public Safety Network Cellular Services (PSN) on a commercial basis.

"SafetyNet will use its wide network of relationships to develop, deliver, and maintain investment in communication infrastructure and services," said Mr Mitchell. "The approach of 'build it once and use it many times' is a good model for the government and the public safety sector."

Rob Fyfe (Chair), Deborah Battel, Glen Sowry, Greg Lowe, and TJ Kennedy have been appointed to the Board of SafetyNet. They will be advised by a panel of experts comprised of the chief executives of Hato Hone St John, NZ Police, Fire and Emergency New Zealand, and Wellington Free Ambulance. Steve Ferguson has been appointed to the role of SafetyNet CEO.

Bill passed to tackle antisocial road users

It is hoped that Parliament's passing of the Antisocial Road Use Legislation Amendment Bill will enable police to crack down on boy racers, fleeing drivers, and other antisocial road users, with and Police Minister Mark Mitchell say.

"Communities across New Zealand have been forced to put up with illegal street racing, burnouts, fleeing drivers, intimidating convoys, disorderly dirt bike gatherings and siren battles for far too long," said Transport Minister Chris Bishop.

The new offences and penalties include:

- Establishing a presumptive sentence of vehicle destruction or forfeiture for those that flee Police, street racers, intimidating convoys, and owners who fail to identify offending drivers
- Giving Police more powers to manage antisocial vehicle gatherings by closing roads or public areas and issuing infringements
- Increasing the infringement fee for making excessive noise from or within a vehicle from $50 to $300

"These changes mean convicted fleeing drivers, street racers, and people participating in intimidating convoys can expect to lose their vehicles through destruction or forfeiture, unless limited exceptions apply," said Mr Bishop.

"The legislation also ensures penalties for excessive vehicle noise better reflect the impact this behaviour has on communities."

The Bill was recommended for passage by the Justice Committee following public submissions from councils, community groups, businesses and individuals.

Most changes will come into effect in six-months' time. The transition period allows for changes to be circulated with frontline staff and for judiciary and legal stakeholders to be able to the operationalise changes.

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.

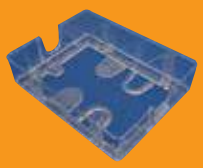
Visit www.asis.org.nz

ASIS INTERNATIONAL New Zealand Chapter

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

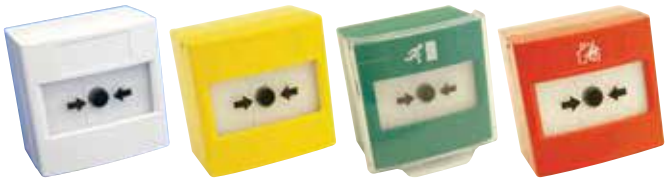
720-090 Ref. STI-13000-NC
NC Universal Stopper flush mount, clear
Options 9V battery horn, (5 colours),
custom label, loom for remote
12-25 v DC power and relay

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**