NZSM

New Zealand Security Magazine

August 2026

Crowded Places Forum smashes it out of ball park

The Wulf Way: Wulf Security takes home the gongs

Alarm monitoring tech has changed – time to update

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**

Loktronic

Loktronic Limited 35 years servicing NZ's Security Industry
SINCE LNZ 1989

Visit our revamped **website** where you can see **product information, prices** and **place orders.** Go to **www.loktronic.co.nz**

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**

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

September 2026
Analytics and the future of guarding and patrols

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 August 2026 issue of *New Zealand Security Magazine*, the third edition of our new shorter, sharper monthly publication. We're keen to get your feedback on the new format, so please drop us an email and let us know what you think.

Leading this latest edition of NZSM is a summary of the New Zealand Security Association's highly successful second annual Security of Crowded Places Forum, which saw a shift in crowded places focus from protection alone towards preparedness and connectedness.

While violent extremism remains a significant consideration in the crowded places space, the forum highlighted that organisations must also contend with violent offending, public disorder, insider threats, cyber-enabled disruption, severe weather events and other complex emergencies capable of rapidly affecting public safety.

Wulf Security enjoyed a remarkable evening at the 2026 New Zealand OSPAs in June, walking away with three category winners, including Samisoni Taufoou for Outstanding Security Officer, Pat Wulf for Outstanding Contract Security Manager/Director, and Wulf Security for Outstanding Contract Security Company (Guarding). We feature their winners and finalists, and we explore what makes this high performing guarding company tick.

A new report from the Australian Strategic Policy Institute (ASPI) urges operators of critical infrastructure and other organisations to treat ageing technology as a governance issue rather than simply an IT problem. The idea that unsupported tech is a security vulnerability is something our industry has been banging on about for years... has the message finally gotten through?

With video verification and video monitoring options now widely available, it's time to update response plans, suggests Graeme McKenzie in his article "Alarm monitoring tech has changed – have your response plans kept up?" It's a great read.

Also, in this NZSM, Professor Jose Pina-Sánchez and Associate Professor Toby Davies of the University of Leeds ask does traffic drive street crime? Their research study demonstrated that low traffic neighbourhoods are one way in which cities are trying to reduce the amount of street traffic.

Plus, the latest in NZ security sector news, including clarification from the PSPLA on licensing obligations for businesses using subcontractors; ACT Party proposes a new Accredited Security Operator (ASO) licence class to empower guards to protect the public until police turn up; and Kahl Betham to step down as Gallagher Group CEO and Executive Director.

All this and more in this month's edition of NZSM!

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

Cyber Criminals Are Not Breaking In - They're Logging In

Across New Zealand, organisations and individuals are discovering that breaches are now a common reality. Three incidents amongst many recently are particularly salient.

Uber driver scam: When attackers target people, not systems

In June 2026, a Wellington Uber driver lost more than $700 after falling victim to an impersonation scam. The attacker posed as Uber support, claimed to be investigating a complaint, and several hours later convinced him to provide a one-time verification code on his phone to close the case after "investigation". Using that code, the scammer gained access to the account, changed the linked bank details and withdrew the driver's earnings using Uber's instant cash-out option.

Canvas data breach: When trusted platforms become the weak link

In May 2026, several New Zealand universities and tertiary institutions were caught up in a global cyber incident involving Canvas, a widely used learning management system. Attackers exploited a vulnerability within the support ticket system in Canvas's "Free for Teacher" environment to access the broader cloud-hosted database, affecting thousands of education institutions and exposing the risks organisations face when relying on third-party technology platforms.

Institutions including the University of Auckland and AUT were notified that data held within Canvas may have been accessed, including user information such as names, email addresses, student IDs and Canvas messages. The NZ National Cyber Security Centre (NCSC) actively engaged with local universities as damages and impacts continue to be assessed.

Manage My Health breach: When sensitive data becomes the target

In late 2025, Manage My Health experienced a cyber incident that exposed the risks of protecting highly sensitive personal information in an increasingly connected healthcare environment. Attackers gained access using compromised credentials to exploit a vulnerability in the platform's Application Programming Interface (API), allowing them to enter the platform as an authorised user rather than breaking through the system's external defences. Once inside, they were able to access and copy documents stored within the My Health Documents module, which contained sensitive health-related information uploaded by users and healthcare providers. After review, it was announced in May 2026 that around 400,000 documents of 99,000 patients were affected.

The lessons are clear: cyber vulnerabilities can come from any direction. Fundamentally, a human element runs across these incidents. The focus must be on understanding vulnerabilities, strengthening controls and most importantly having beforehand capable partners ready to respond. For organisations with hundreds or thousands of employees, preventing every compromise is unrealistic.

The Cyber Security Risk Conference 2026 (

Part of the CIO Innovation Summit and Awards experience, the Cyber Security Risk Conference 2026 will bring together cyber leaders, executives and cyber risk professionals to shine a light on how organisations can navigate today's evolving threat landscape - from strengthening prevention to responding when incidents occur.

The is an conference is an invaluable opportunity for business leaders to equip to better protect their organisations: the threats are evolving and the consequences warrant such focused and strategic conversations.

The Cyber Security Risk Conference 2026 takes place on 04 August at the NZICC, Auckland.

Cocaine tightens grip on NZ workplaces

The Imperans Q2 State of Workplace Drug Use report notes cocaine, ATS and cannabis are all on the rise compared to last year.

Cocaine use is on the rise across New Zealand workplaces. That's a key finding of the latest Imperans Report, a quarterly analysis of drug use in the workplace prepared by The Drug Detection Agency (TDDA).

Growing cocaine use is not the only workplace concern in Q2, 2026. Among all positive results across New Zealand, compared with year-on-year (YoY) substance detections are as follows.

- Cocaine: 2.8% of positive tests, up 68.5% YoY
- ATS (including methamphetamine): 32.7% of positive tests, up 5.2% YoY
- Cannabis: 64.4% of positive tests, up 1.7% YoY

If there is a silver lining, it's that opioid use (including oxycodone) is down. Opioids were present in 18.2% of positive tests, in Q2, down 14.0% YoY.

This quarter, 2.8% of all screens conducted by TDDA indicated the presence of drugs, showing a slight downward trend compared with 3.0% in Q1. Cocaine accounted for 2.8% of positive tests in Q2, up 68.5% YoY, and setting aside the seasonal Q4 peak, its highest level in a year.

"It is becoming increasingly likely that cocaine, buoyed by cartels and other South Pacific drug trade activity, is something employers even in white collar industries need to worry about. The substance is becoming highly available due to supply networks rather than just a one-off spike," said Glenn Dobson, chief executive of TDDA.

ATS, including methamphetamine, accounted for 32.7% of positive tests, up 5.2% YoY, after easing since Q3 2025. Businesses in the South Island should take note, as the region is seeing the largest spike in positive rates.

Opioids accounted for 18.2% of positive tests, down 14.0% YoY, while cannabis accounted for 64.4% of positive tests, up 1.7% YoY. Detection rates for both remain stubbornly high.

"Cocaine and ATS interfere with the way the brain judges risk, producing misplaced confidence and slower decisions at exactly the wrong moment," said Mr Dobson. "On safety-critical sites, where a small margin or a split second can be the difference, that combination can turn deadly fast."

Cocaine

Cocaine is spreading nationally, reaching its highest level in a year across several regions below:

- Canterbury: 3.1% of positive tests, up 375.8% YoY
- Otago: 4.5% of positive tests, up 146.2% YoY
- Hawke's Bay: 5.3% of positive tests, up 81.3% YoY
- Manawatū-Whanganui recorded cocaine detections of 5.1% of positive tests in Q2.

ATS

The YoY rise in ATS runs strongest through the South Island:

- Southland: 44.0% of positive tests, up 200.8% YoY
- Otago: 25.4% of positive tests, up 153.7% YoY
- Bay of Plenty: 34.4% of positive tests, up 84.4% YoY.

The quarterly ATS picture suggests employers should watch further north too. Auckland East, Hawke's Bay, Northland, Taranaki and Tasman have all turned sharply upward in recent quarters.

Opioids

Opioids are settling nationally, though some regions keep climbing:

- Gisborne: 26.3% of positive tests, up 216.0% YoY
- Taranaki: 14.3% of positive tests, up 62.0% YoY
- Wellington: 18.6% of positive tests, up 56.6% YoY
- Otago: 41.8% of positive tests, up 27.7% YoY.

Does traffic drive street crime? Our study investigated

Low traffic neighbourhoods are one way cities are trying to reduce the amount of street traffic, write Professor Jose Pina-Sánchez and Associate Professor Toby Davies of the University of Leeds.

Jose Pina-Sánchez is Professor of Quantitative Criminology at the University of Leeds.

Toby Davies is Associate Professor in Criminal Justice Data Analytics at the University of Leeds.

Picture a busy road running through a residential neighbourhood. The noise, the fumes, the danger to cyclists and pedestrians – all familiar concerns. But here is one you might not have considered: that traffic may also be making your street more prone to vandalism, burglary and violence.

That is what our new research, using data from tens of thousands of households across England, Scotland and Wales, suggests. We found that when motor traffic increases in a neighbourhood, residents' assessments of street crime go up.

At first glance, there is no obvious reason why traffic should influence crime. However, a closer look at crime theory reveals several plausible pathways.

The most direct mechanism is guardianship: the idea that everyday surveillance by residents and passersby helps keep crime in check. Influential American urbanist and activist Jane Jacobs famously called this "eyes on the street".

While it might seem that traffic provides a ready supply of guardians in the form of drivers, their deterrent effect is negligible. Instead, heavy traffic undermines guardianship in multiple ways: wide roads and parked cars fragment public space and obscure sightlines, outsiders are less likely to stand out, and, if traffic discourages walking, there are fewer genuine guardians to keep an eye on things.

Newmarket, Auckland

Aerial view of residential neighborhood rooftops in South Auckland

Traffic also erodes the social fabric. Research consistently shows that busy roads undermine community ties: neighbours talk less, look out for each other less and feel less ownership of shared spaces.

Criminologists describe communities' ability to sustain these kinds of social ties and shared norms as "collective efficacy". Its absence is one of the strongest predictors of violent crime. Chronic stress from traffic noise and congestion is also a likely driver of aggression and antisocial behaviour.

Finally, "broken windows" theory holds that visible disorder (potholes, noise, litter) signals neglect and invites further incivility. Traffic contributes to all of these.

What we found

To test these ideas, we used data from Understanding Society, a large-scale longitudinal study that followed thousands of UK households across three survey waves between 2011 and 2018.

Crucially, the study records both residents' assessments of crime in their area and interviewers' evaluations of whether the street they live on carried heavy traffic. Because these two measures were collected separately, any shared bias in how they are recorded is minimal.

Looking at residents' own perceptions – rather than recorded crime – avoids some of the biases inherent in police data, including under-reporting and changes to recording practices. As well as providing a stable measure over time, this captures what residents actually experience on their streets, including everyday, low-level offences that are rarely reported to police.

We used fixed-effects models, which compare each household to itself over time, effectively stripping away background differences between neighbourhoods (such as wealth and density) that might otherwise affect crime. This means our findings reflect what happens when traffic changes within the same neighbourhood, not simply that busier areas might be more crime-prone.

The results were consistent. When a neighbourhood went from low to high traffic, residents' assessments of vandalism increased by around 9%, burglary by 6%, and violence by 6.5%.

We also found support for the collective efficacy mechanism. As traffic increased, residents reported that neighbours were less willing to help each other – a direct measure of community bonds fraying. That erosion of mutual trust, in turn, was associated with higher perceived crime.

To check our findings, we accounted for potential differences in how interviewers recorded traffic levels. These checks demonstrated that our headline figures are, if anything, likely to underestimate the effect.

Our findings align with, and complement, recent studies that have directly tested this relationship.

Research on London's low traffic neighbourhoods – schemes that restrict through-traffic on residential streets – found that their introduction led to roughly a 10% reduction in recorded crime. Those studies used a quasi-experimental design with high validity, ours uses a national observational approach that can be applied more broadly. Together, they build a compelling case.

What this means for policy and crime prevention

Low traffic neighbourhoods and 20mph zones are already justified on road safety, health and environmental grounds. Our findings add crime reduction to that list.

Many crime prevention strategies, such as the UK's Secured by Design guidance for new residential developments have, historically, promoted designs which discourage pedestrian accessibility. This is intended to make it harder for offenders to enter and escape.

However, if reducing walkability pushes people into cars, and cars make streets less safe, then those well-intentioned design choices may be making things worse by generating crime elsewhere. Effective crime prevention needs to consider the entire urban layout.

This article was originally published on 30 June 2026 in The Conversation.

Industry voices reinforce Crowded Places Forum resilience message

The NZSA's Security of Crowded Places in New Zealand Forum sparks plenty of security sector chatter on LinkedIn in the days following the annual event.

The conversations sparked during the New Zealand Security Association's 2026 Security of Crowded Places Forum have continued well beyond Eden Park, with attendees from across the security sector describing the event as a timely reminder that preparedness, collaboration, and continual learning remain fundamental to protecting New Zealand's public spaces.

Held over two days, the forum brought together security professionals, government agencies, venue operators, emergency responders and consultants to explore practical approaches to strengthening resilience in crowded places. While speakers delivered a wide range of technical and operational presentations, participant reflections shared in the days following the event revealed a strong consistency in the messages that resonated the most.

Presenter Taylor Kimpton, Director and Strategic Risk & Governance Lead at ICARAS Security Consultants, posted on LinkedIn that effective risk management ultimately depends on making advice understandable for those responsible for managing security on the ground.

"The dinosaur is a threat... It exists, it could cause harm. Risk is when the dinosaur can actually reach someone," he explained, using an analogy from his presentation. "You can't remove every threat from the world. You can absolutely control access, layout, detection, and what happens in the first three minutes."

In the crowded places context, Kimpton pointed out, risk assessments only have value if they are practical for those responsible for operating venues.

"My argument was pretty simple: A beautiful risk assessment sitting in a folder isn't managing anything. The test is whether the person who owns the place can actually use it... If the people who own the risk understand it, they'll manage it well. That's the whole job."

Reck Reck, Business Development Manager at Red Wolf High Level Security and Secretary of the ASIS International New Zealand Chapter, said one observation captured the importance of the forum: "Complacency is the biggest gift we can give to risk."

Reflecting on the event, he said that one theme echoed throughout the day: "resilience isn't something you buy. It's something you build."

Among the presentations that left the strongest impressions on Reck were Richard Scott's call to "Drill, drill,

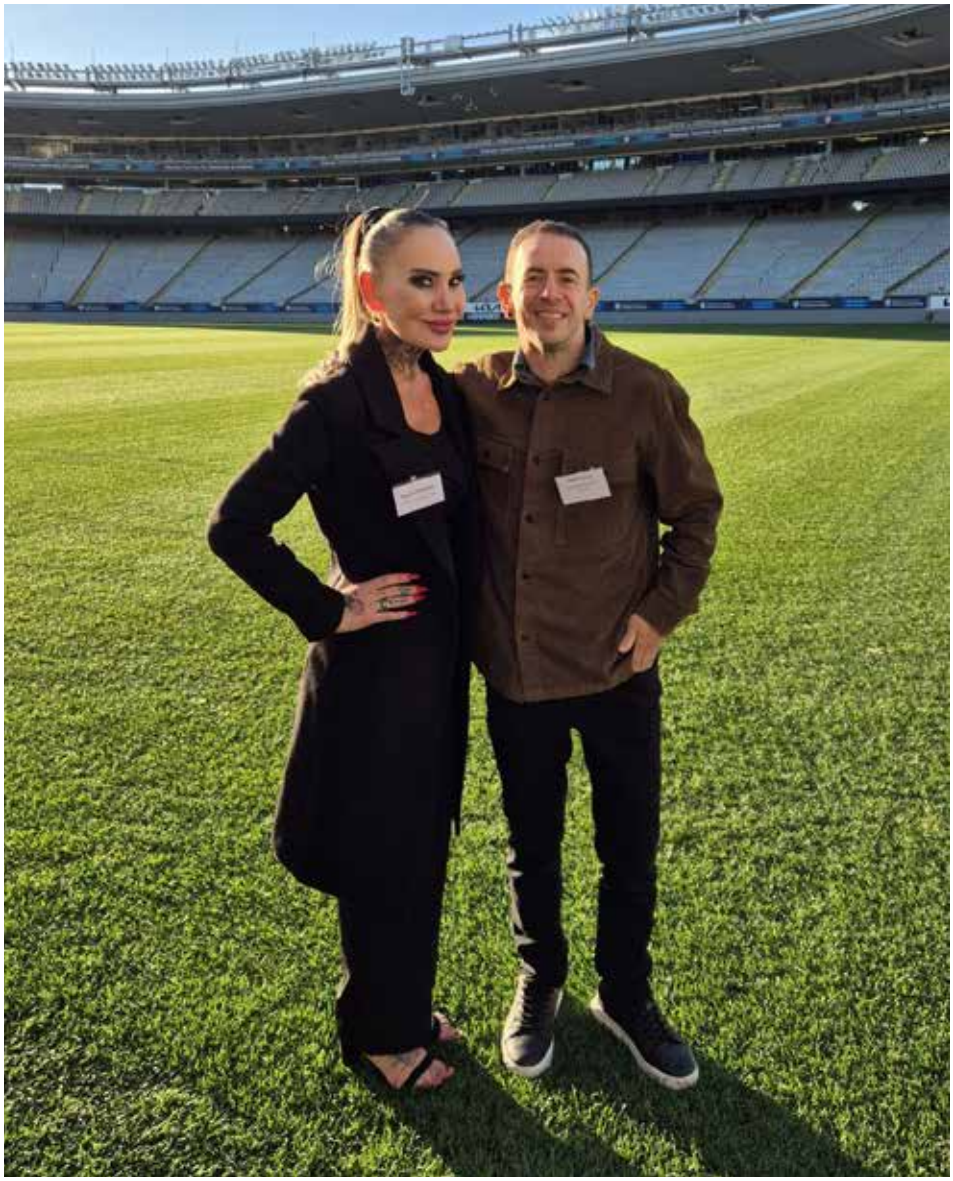


Image: Ngaire Kelaher/LinkedIn

drill. Practice, practice, practice", John Yates' reminder that "There's no right or wrong way to do this [drill]. The only wrong way is not doing it at all", and Paul Nemme's observation that "The goal is not to reach perfection, but to find gaps."

"What struck me most was that, despite the different perspectives, the message was consistent: preparation matters," Reck wrote.

"The organisations that respond best to incidents are usually the ones that have invested the time to understand their risks, challenge their assumptions, and practise before they need to perform."

The value of bringing industry and government together was another recurring theme.

Adam Lynch, Principal Consultant at Reliance Risk, described the forum as an opportunity for "Police and industry, same room, honest about the gaps in our current tools and opportunity for ongoing enhancement."

"Security plans are easy to write and hard to prove," he said, noting that risk profiling and auditing are becoming increasingly important as organisations seek to demonstrate that critical controls are genuinely effective.

Senior Prevention Adviser Richard Scott said the event reinforced the importance of close collaboration between Police, site owners and the private security sector.

"The protection of Crowded Places is the responsibility of all New Zealanders," he said. "Having Police working closely with private security and site owners is vital as they are on the frontlines of locations and events. Improving interoperability between sites, security and Police is an absolute must to ensure the right decisions are made in those first few hectic minutes."

New Zealand Police Emergency Communications National Operations Manager Mike Higgie also highlighted the importance of thinking beyond traditional emergency response.

"Effective emergency response does not begin when a first responder arrives," he said. "It begins from the first point of contact."

Several participants also pointed to the practical benefits of the forum.

FIRST Security Chief Operating Officer Nick Gibbs said the event had identified "some definite actions to implement in the coming months to better support our clients and the wider community," while FIRST Security described the forum as providing "valuable insights and practical advice on strengthening security, enhancing public safety, and working together".

Mark Knoff-Thomas, Chief Executive of the Newmarket Business Association, said New Zealand must avoid complacency as global security challenges become increasingly relevant domestically.

"We have to work hard on not becoming complacent as a country – the distance between 'overseas' and 'here' is much smaller than it used to be," he said. "Building resilience is a shared responsibility."

Such messaging was echoed by Senior Security and Risk Consultant Ngaire Kelaher, who described the forum as "incredibly informative" and praised the launch of the NZSA's CrowdSafe NZ internet resource as "an outstanding online library of practical resources" to strengthen resilience across the sector.

For many attendees, the strongest takeaway was not any single presentation but the consistency of the messages delivered throughout the two-day programme. Whether discussing emergency exercises, technology, risk management or Police coordination, participants repeatedly returned to the same conclusion: resilient organisations are built through preparation, collaboration and continual improvement long before an incident occurs.

The Wisdom of Crowds: From crowded places protection to resilience

The New Zealand Security Association's second annual Security of Crowded Places Forum highlights shift towards preparedness and connectedness, writes 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.

Published in 2004, James Surowiecki's The Wisdom of Crowds posts that the pooling of information that occurs in a large group results in decisions that are often better than those that could have been made by any single member of the group.

Surowiecki would no doubt be pleased that his thesis rang true in the collective outcomes achieved by the 140 delegates who gathered at Eden Park over two days in late July for the NZSA's second annual Security of Crowded Places Forum.

While individual presentations covered topics ranging from hostile reconnaissance and protective security through to artificial intelligence, emergency exercises and crisis communications, a recurring theme was that crowded places security is moving beyond a protection-focused model to one centred on organisational resilience.

Security practitioners have long understood that protecting venues extends beyond installing cameras, deploying guards or controlling access points. Yet events of recent years—from the Christchurch mosque attacks to the Bondi Junction stabbings,

Eden Park. Image: Eden Park Trust.

Image: Mike Higgie/LinkedIn

alongside an evolving global threat environment—have fundamentally reshaped expectations of what constitutes effective security in public spaces.

In addition to deterring and responding to threats, operators of crowded places are increasingly expected to demonstrate ongoing resilience: the ability to prepare for, respond to and recover from incidents that may emerge with little warning and evolve rapidly and within the crucible of intense public scrutiny.

Bringing together representatives from central government, New Zealand Police, the New Zealand Security Intelligence Service (NZSIS), venue operators, emergency services, consultants, technology providers and private security companies, the two-day programme reflected an increasingly mature national conversation about protecting public spaces.

A shared responsibility

Opening the forum, Police Minister Mark Mitchell acknowledged the increasingly important contribution made by New Zealand's private security industry in safeguarding communities and protecting critical public spaces.

While government agencies continue to monopolise roles in national security and emergency management, responsibility for crowded places is starting to be recognised as extending beyond the public sector alone. Venue operators, event organisers, businesses, consultants, security providers, emergency services and local government all contribute to creating safer public environments.

The speaker list of the forum itself reflected this collaborative approach. Delegates heard perspectives from the Department of the Prime Minister and Cabinet (DPMC), New Zealand Police, NZSIS, Hato Hone St John, Eden Park, Scentre Group, Beca, and AUT among others.

Preparedness begins before the emergency

Rather than presenting security as the responsibility of specialist practitioners alone, speakers consistently described resilience as an organisational capability requiring commitment from executive leadership all the way through the organisation to frontline staff.

Since its introduction following the Christchurch terrorist attacks, the Crowded Places Strategy has provided organisations with practical guidance for assessing risk, strengthening preparedness and improving emergency planning. Yet presenters acknowledged that preparedness remains uneven across the country, with some organisations embracing regular exercising and capability development while others continuing to rely on static plans and a tick-a-box approach.

Senior Sergeant Richard Scott challenged delegates to think differently about emergency planning. Security plans, he suggested, should never be viewed as finished documents, but rather as living frameworks requiring continual testing, refinement and adaptation as organisations evolve and threat environments change.

His observation that "it wasn't raining when Noah built the ark" captured the central idea that preparedness begins before

Image: Ngaire Kelaher/LinkedIn

the emergency. Major incidents rarely provide warning, meaning that organisations have only two opportunities to prepare: before the emergency begins—or not at all.

Forum speakers reinforced that preparedness extends well beyond documented procedures to governance structures, clearly defined decision-making authority, staff training, communications protocols, relationships with emergency services and realistic exercising under operational conditions.

Preparedness also benefits from the contributions of professionals beyond security and emergency services, including architects, engineers, planners, venue managers, executive leadership teams, frontline staff, and technology specialists. Architects and engineers, for example, can play a role in designing security and resilience into crowded places and public spaces.

Resilience is built through capable people, well-rehearsed processes and trusted relationships. It begins long before an emergency and continues long after the immediate response has concluded.

Building relationships before they matter

Recognition that crowded places security is becoming progressively more collaborative was indeed a common thread throughout the forum – the idea that no single organisation possesses all the capabilities required to manage a complex public emergency.

Police require timely information from venue operators; venue operators depend upon emergency services; private security providers work alongside facilities managers, event organisers, contractors and local authorities; and government agencies provide strategic guidance while industry implements practical measures on the ground.

Repeatedly, delegates heard that effective coordination during emergencies depends largely upon relationships established long before an incident occurs: joint planning meetings, shared exercises, regular communication, clearly understood responsibilities, and familiarity between organisations.

These activities often determine whether multiple agencies function as a coordinated response or simply as individual organisations working in parallel.

Exercising for uncertainty

Emergency plans, delegates heard repeatedly, are only as effective as an organisation's ability to implement them under pressure.

Paul Nemme of New Zealand Police drew upon extensive experience in planning active armed offender exercises to explain that successful exercises are not intended to validate existing plans. Rather, they are designed to expose weaknesses before a real incident does.

Too often, organisations unconsciously design exercises that confirm their preparedness rather than challenge it. Participants know broadly what will happen, communications proceed largely as expected and the exercise concludes with reassurance rather than genuine organisational learning.

The more valuable exercises, delegates heard, deliberately introduce uncertainty where unexpected complications emerge that require

Image: NZSA/LinkedIn

participants to adapt rather than simply follow predetermined procedures: communications fail, key decision-makers become unavailable, or information proves incomplete or contradictory.

Such scenarios more closely reflect the realities of emergency management, where decision-makers rarely possess perfect information and where events frequently unfold differently from what emergency plans anticipate.

Comprehensive debriefing, structured lessons identified, and the incorporation of improvements into future planning were presented as equally important components of the exercise cycle.

Lessons from Bondi and beyond

If preparedness represented the strategic theme of the conference, the attack at Westfield Bondi Junction provided its most compelling practical case study.

More than a year after the tragedy, Bondi continues to shape thinking about crowded places security across Australia and New Zealand. If nothing else, the event demonstrated how rapidly an ordinary public setting can transform into a complex, dynamic locus of emergency.

Speakers focused on the operational realities of such an event: How quickly can situational awareness be established? How effectively do security personnel communicate with police responders? Who assumes decision-making authority as events unfold? What information is genuinely useful during the first few minutes?

Rather than treating Bondi as an isolated Australian incident, delegates were encouraged to regard it as an opportunity to critically examine their own organisations with fresh eyes.

Would, for example, current emergency procedures function under comparable conditions? Would staff understand their respective responsibilities? Would responding emergency services receive the information they require quickly enough to influence operational outcomes?

The first 300 seconds

Security practitioners often devote significant effort to preventing incidents from occurring. Yet, as multiple presentations highlighted, once a major incident does occur, the first few minutes tend to determine its trajectory.

Decisions made during this period influence not only the effectiveness of the immediate response, but also the safety of occupants, the ability of emergency services to intervene and, ultimately, the nature of the organisation's recovery from the incident.

It was therefore unsurprising that discussions repeatedly returned to what several speakers described as the "first 300 seconds".

A panel featuring representatives from New Zealand Police, Eden Park and Red Badge Group examined precisely what occurs during those critical moments following an active armed offender event.

While every incident is unique, police explained that their operational priorities remain consistent: the immediate objective is to locate, isolate and stop the threat. Everything else—including casualty management, investigation and business recovery—depends upon that initial response.

Within this context, security teams must understand not only their own emergency procedures but also how those procedures interface with Police operations once responding officers arrive on scene.

Police emphasised, for example, that they do not require lengthy situation reports during the opening stages of an incident. Instead, they need concise, actionable information: where the offender is believed to be, whether multiple offenders are involved, what access routes are available and any immediate hazards likely to affect responding officers.

Equally important is identifying who will meet police on arrival and who possesses sufficient situational awareness to provide accurate information without delaying operational decision-making.

Although they appear simple considerations, speakers noted that they often become points of confusion during real emergencies when organisations have not previously exercised their procedures under realistic conditions.

Technology as an enabler

Technology inevitably featured prominently throughout the forum, with speakers discussing advances in analytics, situational awareness and information sharing, reflecting the rapid pace of technological change

across the security sector. Yet, while technologies are becoming more capable, there was agreement that people remain decisive.

Artificial intelligence may assist in identifying anomalies within CCTV footage. Integrated platforms may consolidate information from multiple sources. Automated alerts may reduce response times and improve situational awareness. Yet none of these capabilities remove the requirement for experienced professionals capable of interpreting information, exercising judgement and making decisions under pressure.

Throughout the programme, technology was consistently presented as a force multiplier rather than a replacement for skilled security practitioners.

While technological capability continues to advance rapidly, speakers repeatedly emphasised that equal attention must be given to staff training, organisational culture, and leadership capability. Sophisticated systems deliver little value if personnel lack confidence in using them or if organisational processes fail during rapidly unfolding incidents.

Learning from practitioners

While the formal presentations provided strategic context and operational insights, the Knowledge Café sessions delivered some worthwhile practical outcomes.

Shifting the conversation away from the lectern and into small-group discussions, the Knowledge Cafés allowed practitioners from different sectors to identify the challenges they face within their own organisations and, importantly, the practical improvements they intended to make upon returning to work.

Regardless of whether delegates represented government agencies, major venues, local authorities or private security companies, many identified similar priorities.

Organisations intended to review emergency management documentation, assign clear Coordinated Incident Management System (CIMS) roles, increase the frequency of scenario-based exercises, and strengthen executive engagement in security planning.

Image: Adam Lynch/LinkedIn

Others highlighted opportunities to improve first aid capability, reinforce staff awareness of the "Escape. Hide. Tell." Campaign, and ensure frontline personnel understood their responsibilities during the critical opening stages of an incident.

Participants also recognised that preparedness is not created by policies alone. Effective resilience depends upon staff confidence, leadership commitment and an organisational willingness to continually review, question, and improve existing arrangements.

Several delegates also highlighted opportunities to strengthen collaboration across the wider security profession, including greater engagement with New Zealand Police, improved information sharing between organisations and stronger links with universities and research institutions to support evidence-based security practice.

Changing role for security industry

Several presentations reinforced a changing security industry dynamic in which customers are increasingly seeking advice that encompasses governance, resilience, emergency planning, exercising and organisational preparedness.

Security practitioners are increasingly expected to not only understand relevant technologies and operational procedures, but to also contribute to enterprise risk management, business continuity planning, and executive decision-making. Security is becoming progressively integrated into broader organisational resilience strategies.

Whether discussing protective security principles, emergency exercises, technology integration or police coordination, speakers consistently framed security as an organisational capability requiring contributions from leadership teams, operational managers, frontline employees and external partners.

While violent extremism remains a significant consideration in the crowded places space, organisations must also contend with violent offending, public disorder, insider threats, cyber-enabled disruption, severe weather events and other complex emergencies capable of rapidly affecting public safety.

Resilience to such threats is increasingly becoming a governance issue rather than just an operational one. Boards and executive teams are now expected to demonstrate not simply that security measures exist, but that their organisations possess the capability to respond effectively when confronted by unexpected events.

While the security industry has long been defined simply by what it protects, increasingly it will be defined by the resilience it helps others build.

Gallagher Group CEO Kahl Betham to step down in 2027

Gallagher Group has announced that Group CEO and Executive Director Kahl Betham will step down from his leadership roles at the end of financial year.

Kahl Betham is Gallagher Group Group CEO and Executive Director

Betham will remain in the position until 31 March 2027 to oversee an orderly transition, with Gallagher confirming there will be no changes to the Group's strategy or operational priorities during the succession process. Gallagher Security and Gallagher Animal Management will continue to be led by their respective Chief Executives, Mark Junge and Rob Clayton.

The announcement marks the end of a career that began in 1997 when Betham joined Gallagher as a software engineer. He went on to lead Gallagher's global Security business from 2015, was appointed Group Deputy CEO in 2019, and became Group CEO in 2021.

During his tenure as Group CEO, Gallagher has experienced significant international expansion. The privately owned Hamilton-headquartered company has grown to employ more than 1,700 people globally, serving customers in more than 160 countries across its Security and Animal Management businesses.

The company said annual revenue has doubled over the past five years and is on track to exceed NZ$700 million during the current financial year, with ambitions to reach NZ$1 billion in annual revenue within the next few years.

Gallagher Board Chair Steve Tucker said Betham had led the organisation through a period of sustained growth and strong commercial performance.

"Kahl is a strong leader who has led the company through a period of rapid growth and remarkable outcomes for our people, customers, and business," Tucker said.

He added that the company's values-led culture and global reputation had been strengthened under Betham's leadership, noting Gallagher's recent recognition as both Best Large Business and Supreme Winner at the New Zealand International Business Awards.

Reflecting on his decision, Betham described leading Gallagher as "an absolute honour and privilege", acknowledging both the challenges and achievements of recent years. He said the company had achieved NZ$142 million in revenue growth over the past year alone, representing a 33 per cent increase despite difficult global economic conditions.

Betham said the timing felt right after almost 30 years with the business, particularly while his children were still young. Looking ahead, he indicated he intends to focus on supporting New Zealand's technology sector by investing in and supporting emerging technology companies.

"I remain fully committed to leading the business through the remainder of FY27," he said, adding that Gallagher's long-standing commitment to innovation positions the company well for continued global growth.

The leadership transition will be closely watched across the electronic security industry. Under Betham's leadership, Gallagher Security has continued to strengthen its position as one of the world's leading providers of integrated access control, perimeter protection and site management technologies, with a significant presence across critical infrastructure, government, commercial and high-security markets worldwide.

Past its use-by date: Unsupported technology poses growing security risk

A new report from the Australian Strategic Policy Institute (ASPI) urges operators of critical infrastructure and other organisations to treat ageing technology as a governance issue rather than simply an IT problem.

Unsupported digital infrastructure is becoming an increasingly significant cyber security vulnerability, particularly as artificial intelligence accelerates the discovery and exploitation of software weaknesses, argues the just-published report.

Produced with support from Cisco, Past its use-by date: Turning End-of-Life Technology Risk into National Advantage contends that many organisations continue to operate systems long after vendor support has ceased.

While these platforms often remain functional, they become progressively harder to defend against contemporary cyber threats because they can no longer receive security updates, adopt modern identity standards or support emerging technologies such as post-quantum cryptography.

The authors distinguish between technology that is merely old and technology that has reached the end of its supported life. The report argues that the real issue is not age alone, but the accumulation of "technical debt" and "maintenance debt" as organisations continue relying on systems that can no longer meet modern security expectations.

As AI-driven cyber tools mature, attackers can identify and exploit these weaknesses at unprecedented speed, compressing the window available for defenders to respond.

The report also highlights several emerging trends that make delayed technology replacement increasingly risky. These include AI-assisted vulnerability discovery, the looming transition to post-quantum cryptography, and the growing convergence of operational technology (OT) and information technology (IT), which is expanding the cyberattack surface across critical infrastructure sectors.

Together, these developments strengthen the business case for proactive modernisation rather than continued reliance on compensating controls.

To illustrate the challenge, the report examines comparative case studies from Australia, South Korea and the Philippines, concluding that each confront similar problems: fragmented ownership, deferred investment decisions and uncertainty over who is ultimately accountable for replacing unsupported technology.

Australia, while comparatively mature in cyber governance, is identified as still carrying significant exposure through legacy systems across government and critical infrastructure.

Rather than framing technology replacement purely as a cost, the report argues that structured modernisation should be viewed as a strategic investment that improves resilience, enables adoption of newer security capabilities and reduces long-term operational risk.

It calls on governments to strengthen procurement policies, improve lifecycle governance and create clearer accountability for end-of-life systems. Businesses, meanwhile, are encouraged to integrate technology lifecycle planning into enterprise risk management and board oversight.

Perhaps the report's strongest recommendation is the establishment of a governance standard whereby unsupported systems are not permitted to remain in service by default. Instead, every system operating beyond vendor support should require formal executive approval, documented risk controls, a funded replacement pathway and scheduled review.

NCSC: Quarter One 2026 sees significant cyber incidents

The National Cyber Security Centre (NCSC) Cyber Security Insights report for the period 1 January – 31 March 2026 shows individual New Zealanders hit.

In Q1 the NCSC responded to three C2 category or 'highly significant' incidents, the first type of these incidents since the 2021/22 financial year. C2 category incidents impact key sensitive data or cause disruption to essential New Zealand services in organisations of national significance.

These types of incidents typically have the potential to impact a wide range of people and organisations and often involve highly sensitive information.

In this report the NCSC outlines lessons that other organisations can learn about ensuring sensitive data is protected.

"Ensuring basic cyber security measures such as multi-factor authentication, managing who has full access to the network, and protection of the network edges were in place could have helped to defend against these incidents" said NCSC Chief Operating Officer, Mike Jagusch.

"Organisations have an obligation to protect their customers' and their sensitive personal information by securing their networks with NCSC's recommended, or similar, minimum-security standards".

Overall, the NCSC responded to 1,164 incidents throughout the first quarter of 2026. This is a very slight increase from the previous quarter, with phishing and credential harvesting being the most common type of incident reported.

Direct financial loss in Q1 totalled $5.6 million, a significant increase of 76% from the previous quarter, with individual New Zealanders accounting for $5.2 million of that loss. Despite increasing, this figure is below the average loss over the last two years.

The report also offers insight into the implications of Frontier AI and how these models can be used both for and against cyber incident prevention.

"Frontier AI models will change the cyber threat landscape for organisations because of the ability for malicious actors to find and exploit vulnerabilities at unprecedented speed and scale," said Mike Jagusch, "but they also have the potential to be used to assist defence and protect systems at a similar scale and pace. For now, the best way to prepare is getting the basic security measures in place."

The NCSC has recently published new guidance for cyber defenders and for business leaders to help them understand the risk of Frontier AI products.

Key data highlights

- The NCSC responded to 77 incidents that required specialist technical support. This is a 14% decrease from the 90 in Q4 2025.
- Three of these were categorised as C2 or 'highly significant'. These are the first C2 incidents recorded by NCSC since the 2021/2022 financial year.
- 1,087 incidents were reported that did not require specialist technical support in Q1, up 4% from Q4 2025.
- Phishing and Credential Harvesting was the most common type this quarter with 437 incidents.
- $5.6 million in direct financial loss was reported in Q1 2026, a 76% increase from the previous quarter's $3.2 million.
- Incidents $10,000 and over made up $5.4M (97%) of reported loss despite consisting of only 42 incidents.

The Wulf Way: Wulf Security dominates 2026 NZ OSPAs

With two individual awards, a company award, and an additional two finalists, guarding provider Wulf Security's 2026 Outstanding Security Performance Awards gala dinner was a night to remember.

Wulf Security enjoyed a remarkable evening at the 2026 New Zealand OSPAs in June, walking away with three category winners, including Samisoni Taufoou for Outstanding Security Officer, Pat Wulf for Outstanding Contract Security Manager/Director, and Wulf Security for Outstanding Contract Security Company (Guarding).

In addition to its category wins, the company also posted two finalist short-listings, including Katalina Vete for Outstanding Female Security Professional and Joseph Teremoana Tere for Outstanding Young Security Professional.

With its three category wins, the team from Wulf Security dominated the 12-category programme, with Gallagher Security finishing the evening close behind with an impressive two category wins.

The impressive haul makes Wulf Security the third New Zealand security provider to have achieved a single-year OSPA trifecta.

Historically, the OSPAs has seen a three-category sweep in all but one of its five years in New Zealand. FIRST Security led the way, winning three categories in 2023 and then again in 2024, with FIRST's Brian Switalla also taking out 2024's Lifetime Achievement award. In 2025, Optic Security Group collected a three gong haul.

"To be recognised alongside the best in the industry is a privilege, and we want to extend our congratulations to all the finalists and winners who continue to raise the standard of security in our communities," stated a

Wulf Security announcement.

"These achievements are a direct reflection of the dedicated people who make up the Wulf Security family. To our entire team: thank you. Every day, you bring our core values to life. It is through your unwavering professionalism and daily reliability that we deliver for our clients."

Founded in 2016 by Director Pat Wulf, Wulf Security Services was established with the vision of creating a service built on trust, professional excellence, and genuine care for people.

A Samoan-owned business, its foundation rests firmly on its four core values of aiga (family), professionalism, reliability, and tautua (service).

With a footprint that has grown to cover Auckland, Wellington, Christchurch, and Great Barrier Island, its services include static guarding, mobile patrols, event security, and infrastructure protection.

Samisoni Taufoou: Outstanding Security Officer

Having been with Wulf Security since its inception, Samisoni is described as the very fabric of the organisation. Over a decade of frontline service and team supervision, he has driven operational excellence by demonstrating that a high standard of security is achieved through emotional intelligence and human connection.

"Samisoni Taufoou exemplifies Wulf Security's values through a decade of heart-led service, balancing firm authority with deep compassion,"

stated Samisoni's OSPA winner's profile. "Highly awarded and trusted in high-risk environments, he consistently elevates operations and team culture. Judges praised his authentic star quality, daily positive influence, and embodiment of the organisation's ethos."

Among stakeholders who praised Samisoni's performance, John Carter, former Project Manager at Mako Construction (now Project Director at Starke Windows and Doors), commended Samisoni's leadership heading up the project security team at The Botanic Silverdale, noting his attention to detail and communication with subcontractors and village residents.

"Samisoni possesses the rare ability to be firm when required while remaining deeply compassionate, resolving complex frontline challenges without generating unnecessary conflict," stated an announcement by Wulf Security.

"From earning internal client awards from Mako Construction to bringing his own family into the business, Samisoni truly lives our core values of aiga (family) and Tautua (service)."

Pat Wulf: Outstanding Contract Security Manager / Director

Pat Wulf has led the development of the company since its inception. "By embedding his Samoan heritage into our daily operations," stated a company LinkedIn post celebrating his OSPA win, "he has challenged the traditional, often adversarial status quo of the industry to champion an approachable, relationship-driven security model."

Pat is credited with moving the company away from intimidating black uniforms to a new signature pink polo offering, which is said to act as a highly effective visual de-escalation tool that fosters open dialogue over confrontation.

Under his guidance, 'The Wulf Way' philosophy ensures the company's personnel act as reliable brand ambassadors, while his focus on aiga has built a loyal, stable, and highly effective frontline team.

"Pat Wulf has reshaped the security industry through 'The Wulf Way', blending Samoan values with approachable, reliable service," states Pat's OSPA winner's profile. "Known for replacing black uniforms with pink polos, he builds trusted, personable teams. Judges praised his visionary shift toward friendly, welcoming security that people genuinely feel comfortable engaging with."

Wulf Security: Outstanding Contract Security Company (Guarding).

Marking Wulf's 10-year anniversary, this recognition reflects a decade of sustained growth, operational excellence, and a commitment to trying to transform the security industry from the inside out.

"With 97% staff retention, strong national partnerships, and deep community impact, judges praised its cultural authenticity, innovation, and industry-shaping approach to modern security," states Wulf Security's OSPA winner's profile.

The company has also sought to make an impact on the communities it serves, sponsoring grassroots organisations like the ARL, College Rifles, and McAuley High School, while providing meaningful employment and mentorship pathways for rangatahi.

"This nomination belongs to our exceptional frontline officers and our dedicated management team who ensure that premium protection and human compassion always go hand in hand," stated a company LinkedIn post.

Joseph Teremoana-Tere: Finalist

Joseph Teremoana-Tere was named a finalist for Outstanding Young Security Professional. At just 21 years old, Joseph has established himself as an exceptional operational all-rounder for Wulf Security, seamlessly transitioning between fast-paced retail and high-energy hospitality environments to dynamic construction sites.

"Where Joseph truly excels is in his specialised role as a concierge at the Auckland Temple. This high-profile site requires the ultimate balance of strict access control, cultural sensitivity, and diplomacy," stated a Wulf Security announcement. "Joseph navigates these complex interpersonal dynamics with a maturity well beyond his years, ensuring site compliance while preserving a peaceful, welcoming environment."

Katalina Vete: Finalist

Katalina Vete was named a finalist for Outstanding Female Security Professional. Operating as the primary ambassador at a Tip Top facility, she manages a highly complex flow of staff, contractors, and logistics heavy transport.

"She consistently demonstrates that vigilance and approachability are not mutually exclusive, using exceptional customer service as a highly effective tool for compliance and site safety," stated Wulf Security.

A multiple-time winner of the 'Wulf Security Superstar of the Month' award, Katalina has also drawn praise from customers for her professionalism and unwavering diligence.

New ACT Party policy proposes new security licence class

The ACT Party has proposed a new Accredited Security Operator (ASO) licence class to empower guards to protect the public until police turn up, writes 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.

Under the proposal, announced 03 July, guards holding a new Accredited Security Operator (ASO) licence would have elevated – but limited – powers to keep shared spaces safe

"Business owners want protection from trained, uniformed professionals. But Police can't respond quickly to every call. Security professionals have the potential to fill the gap" stated the announcement.

The announcement highlighted that New Zealand has twice as many licenced security officers as police officers, but they currently have no more authority than any other citizen.

"The Government has already given some guards elevated powers with ad hoc legislation, such as Parliamentary Security," stated the announcement. "ACT will allow retailers, business associations, shopping strips, and transport operators to access a higher calibre of protection."

ASOs would receive training and education to understand the limits of their power and how to safely deal with situations, with accreditation to a formal education standard delivered by approved training agencies, and licences issued by the Private Security Licensing Authority.

"There will be strong safeguards in place," states the policy document. "Any ASO in breach of the code of practice will have his or her licence revoked and, with it, any legal privileges it provides."

Under the plan, licensed Accredited Security Operators, would be able to:

- Require a person's name and address on private premises and detain until Police arrive if they refuse and won't leave.
- Issue a written, conduct-based exclusion notice on the occupier's behalf where there are reasonable grounds, running for up to three years and applying across multiple premises, such as across a business association.
- Remove people who threaten safety, cause damage, or breach a venue's conditions of entry.
- use reasonable force to remove or detain a person, or to prevent re-entry after entry has been refused or an exclusion issued,, Force must be proportionate, a genuine last resort after a reasonable chance to comply, and must cease the moment the person complies or Police arrive.
- Carry out consent-based entry and safety searches, where refusing a search means no entry. They will also have clear statutory authority to request a consent-based search on the premises where they reasonably suspect a safety risk or prohibited item.

Peak bodies support policy

The New Zealand Security Association (NZSA) has voiced its support for the policy announcement.

"Whilst some of these powers currently exist in certain circumstances, the proposed measures will bring certainty that is currently lacking, and will give appropriately trained and licensed security professionals real capability to keep the wider community safe," commented NZSA CEO Gary Morrison.

ACT's spokesperson for retail crime, Dr Parmjeet Parmar.

"The measures proposed within the policy are very closely aligned with the submissions made by the NZSA to the Ministerial Advisory Group for Victims of Retail Crime and reinforce the importance of any additional powers being supported by stringent vetting, training and licensing processes.

According to Mr Morrison, the NZSA has had discussions with the PSPLA on how the changes could be implemented, and the peak body has developed the framework for a training program for Accredited Security Operators, along with annual refresher training.

"Whilst not specifically referred to within the ACT Party policy announcement, the NZSA supports the carrying of approved hand-cuffs by Accredited Security Operators but we do not support or encourage the use of defensive weapons such as pepper sprays or batons," he continued.

"It is our view that safety of staff, and those in the immediate vicinity, is paramount and that any decision to detain offenders should be as a last resort and where in the judgement of the Accredited Security Operator, it is safe to do so."

According to Retail NZ Chief Executive Carolyn Young, the peak retailers' body supports any changes that would provide advanced training to security guards "to allow them to appropriately and safely manage these higher-risk situations."

"It is vital any additional powers for specially accredited security guards would need to remain reasonable and proportionate, but many retailers may benefit from having security staff that could remove customers who are threatening safety or causing harm, for example," stated Ms Young.

"We see this policy as fitting nicely alongside the changes to trespass laws for retailers that are currently being considered by select committee," she said.

"Retail NZ is supportive of advanced security guards, and we see this as a more appropriate alternative to the enhanced citizen's arrest provisions that have been developed as part of the Crimes Amendment Bill."

ACT MPs elaborate

"Every licence holder will have to go through specialised advanced training and education. This is not something that any Tom, Dick, or Harry could just pick up. Stringent vetting will ensure only the right people with the right capability will be approved," said ACT Leader David Seymour.

"These powers will apply on private premises, but when combined with citizens' arrest powers currently going through Parliament, will give licenced professionals real capability to keep the wider community safe.

"ACT's policy will unlock communities' potential to protect themselves, without relying solely on the taxpayer or a stretched Police force."

"ACT's policy means businesses can take real action, sharing the services of highly-effective security professionals," said ACT's spokesperson for retail crime, Dr Parmjeet Parmar. "It reflects the reality that, until the Police arrive, communities need real authority to stand up for themselves against thieves and thugs."

PSPLA clarifies licensing obligations for businesses using subcontractors

The Private Security Personnel Licensing Authority (PSPLA) has issued guidance clarifying that businesses cannot avoid licensing obligations by subcontracting security work to independently licensed contractors.

The one-page Licensing Guideline, released on 25 June, is likely to have implications for security consultants, electronic security providers, guarding companies, wholesalers and other businesses that contract security services to third parties.

According to the guidance, where a business promotes, offers, or invoices clients for a particular class of regulated security work for valuable consideration, it will generally be regarded as carrying on business in that class and must therefore hold the relevant security licence—even if the work itself is performed by independent licence holders.

The PSPLA illustrates the principle through a number of practical examples.

A security consultant that markets installation and monitoring services, invoices the client for those services, but engages licensed contractors to undertake the work is still required to hold licences in the relevant classes. Likewise, a business promoting installation services while subcontracting the physical installation to licensed technicians must still hold a security technician licence.

According to the PSPLA, this also extends to wholesalers and online retailers of security equipment that offer installation or consultancy services, as well as technicians or electricians who provide consultancy services but subcontract that component of the work to another licence holder. In each case, the business or individual contracting directly with the client must hold the appropriate licence for the class of work being offered.

The guidance further confirms that a company contracting with a client to provide guarding services cannot rely solely on the licences or Certificates of Approval held by subcontracted guards. The contracting business itself must hold the appropriate guarding licence.

The PSPLA bases its interpretation on sections 5 to 11 of the Private Security Personnel and Private Investigators Act 2010, which define the classes of businesses required to hold security licences.

According to the Authority, businesses invoicing clients for a regulated class of security work will generally fall within the statutory definition of carrying on business in that class.

While the guidance does not introduce new legislative requirements, it provides greater certainty around how the existing Act will be interpreted and applied in practice.

For security businesses, particularly those operating contractor-based business models, the new guidance serves as a timely reminder to review licensing arrangements, service offerings, contractual structures and invoicing practices.

Businesses that market, sell and contract regulated security services should ensure they hold licences in every class of work they offer, regardless of whether those services are ultimately delivered by employees or independent subcontractors.

Enhanced citizens' arrest powers to become reality

Citizens' arrest powers are a step closer to becoming law with the Crimes Act Amendment Bill scheduled to start its final reading in Parliament this week.

According to a 04 August 2026 media release, the Crimes Act Amendment Bill, which includes stronger penalties for retail crime, attacking first responders, coward punches, and dealing in slaves, will commence its final reading in Parliament this week.

"The economic cost of retail crime in New Zealand is in the billions," said Justice Minister Paul Goldsmith. "Retailers and security guards face abuse and assault that no New Zealander should be subjected to."

"Our government is committed to fixing the basics in law and order, and that means ensuring retailers are being effectively protected, are empowered to stop offending, and that offenders are caught and deterred from doing it again," he said.

"Where others may flee, first responders and front-line corrections workers run towards danger to help those who need urgent assistance. Assaulting them puts multiple lives at risk, so there must be greater consequences for these terrible acts of violence.

"We know how dangerous coward punches are. People can be killed or suffer lifelong brain injuries, yet perpetrators often receive lenient and insufficient sentences. That changes with this legislation.

"We promised to have this passed into law before the next election. We're delivering. This legislation will take effect within a week of this Bill passing into law."

The Crimes Act Amendment Bill includes:

- New specific offences for assaulting first responders or front-line corrections workers.
- Three new specific coward punch offences.
- Additional citizen's arrest powers.
- A new shoplifting infringement regime.
- Strengthening trafficking and people smuggling laws to stop criminals using loopholes to evade real consequences for crime.

"A 'coward punch' gets its name for obvious reasons. These attacks affect everyday Kiwis and are often committed by cowardly attackers, who strike when the victim is distracted,

Mr Goldsmith said in announcing the proposed legislative change a year ago.

"We know how dangerous they are. People can be killed or suffer lifelong brain injuries, yet perpetrators often receive lenient and insufficient sentences."

Changes in relation to citizens' arrest powers are:

- Amending the Crimes Act so that citizens can intervene to stop any Crimes Act offence at any time of the day. (Currently some - including theft under $1000 - apply only between 9PM and 6AM).
- Requiring that a person making an arrest contact Police and follow Police instructions.
- Clarifying that restraints can be used, when reasonable, when making an arrest.
- Changing the defence of property provisions to the Crimes Act so it is clear that reasonable force may be used.

Alarm monitoring tech has changed. Have your response plans kept up?

With video verification and video monitoring options now widely available, it's time to update response plans, suggests Graeme McKenzie, Technical Manager at Alarm Watch.

When I installed my first security alarms back in 1983, it was for the NZ Post Office. We didn't really worry about the alarm responses. We just installed the gear and made it work. Someone else up the chain worked out what happened if it activated.

Years later, in 1992, when I joined Alarm Watch (called Electroguard at the time), we had a bureau with a local monitoring station and we took a much more hands on approach to what happened when an alarm activated.

Back then the choices were pretty simple: Alarm activates; send a guard; then call the client or key holder on their landline.

That was pretty much it.

As the years went by, we started our own monitoring station, and as everyone embraced cell phones, we started adding more contacts to the call list. Then came text messaging, and later, app notifications, when we introduced our Monitoring App. But really, in essence we were still just dispatching a guard and calling a contact.

Fast forward to today and things have changed dramatically.

With video verification and video monitoring options, operators now have far more interaction with the site. They have much more information about what may be happening, with live video or event footage being presented directly to both the operator and the end user.

That makes the response planning far more important than it has ever been. Today we have much better visibility of what may be happening, but we also have many more questions that need to be answered before the monitoring station can respond correctly.

- What level of false alarms might be expected from camera analytics?
- Are the cameras internal, external, or both?
- Will the system only send alerts when unauthorised people are onsite?
- Is the property fenced off to the public?
- What do we do if nothing is visible?
- What do we do if we see people?
- What do we do if we don't see people?

- What do we do if we see a vehicle?
- What do we do if we see animals?
- What do we do if we believe the alerts are being caused by the weather?
- What do we do if we can't access the cameras?
- What would the client consider suspicious behaviour for this site?

The days of making assumptions are gone. We have so much more information, and so many more decisions to make. Every site is different, every client is different, and every response plan should reflect that.

As installers and monitoring stations, we need to spend the time with our clients to understand what they want to happen when an event occurs. Simply adding cameras to the mix and advising the operators to look at them does not automatically make a good response.

The technology has come a long way, and AI is rapidly changing the way we do a lot of things, but the best monitoring outcomes still come from having a clear response plan in place before the first alarm ever activates.

Loktronic

Loktronic for Fire Protection Products

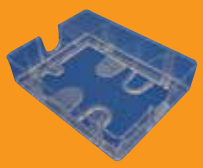
Loktronic

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**

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

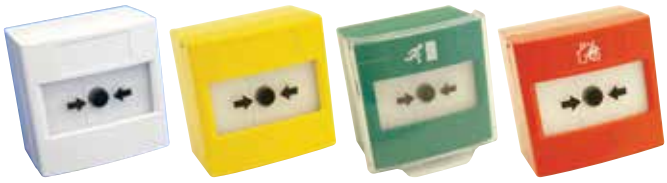
720-090 Ref. STI-13000-NC
NC Universal Stopper flush mount, clear
Options 9V battery horn, (5 colours),
custom label, loom for remote
12-25 v DC power and relay

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**