# NBR Special Report: Security – the future of corporate security

In this increasingly risky world, companies are exposed to security risks that are alien, expensive and difficult to mitigate. But the corporate security industry is developing new increasingly affordable solutions for large and small companies. There are also the questions of business continuity planning, crisis management and striking a balance between workplace environment, safety and health. All these minefields require business skills and innovation from both the security professionals and their corporate contractors.

## Traditional threats still at head of security risks

**Nick Grant**

Although a great deal has changed in the quarter of a century that Global Security founder and director Ross Johnson has been in the security industry, he says the No 1 threat to New Zealand businesses remains the same as when he started.

Yes, he acknowledges, cyber attacks do "grab the headlines" and are an important emerging area of concern, especially in terms of potential reputational damage if a data breach is publicised.

But the traditional threats of employee and contractor theft and burglaries "are still far more likely to affect a business owner," says Mr Johnson, whose clients run the gamut from residential households and suburban fish 'n' chip shops to large corporates.

As such, combatting the possibility of light-fingered workers – whether or not they're engaged in the modish euphemisms of "perking" or "shrinkage" or simply stealing – still starts with such old-fashioned standbys as "proper pre-employment screening processes."

Putting effort into employee engagement is also advisable: "People who work at having a good relationship with staff experience a lot less theft," Mr Johnson observes.

**INDUSTRY VETERAN:** Global Security director Ross Johnson

And, as has long been the case, these measures should also be complemented with such tools as closed circuit television (CCTV) and site access control.

### Tech benefits beyond security

Of course, the past 25 years has seen a vast improvement in the utility of security tools, thanks to technological advances that not only offer greater security but wider benefits as well.

"There's now so much more useable data being delivered that helps clients manage their businesses better," says Mr Johnson, thanks to the ability of modern security suites to spit out trending information as well as provide specifically tailored consolidated reports.

These can lead to enhancements in efficiency, which Mr Johnson illustrates with an anecdote about a manufacturing client.

"They have a lot of vehicles coming in and out every day," he says. "We were able to help them speed up the flow of those vehicles, which had a direct impact on the business' productivity.

"That was all due to newer technology being able to hold more information about the trucks – when each one is coming, what's on it, who's authorised it and so on – and therefore pre-screen and prioritise them."

Fully leveraging information age security systems can also mean improved compliance.

Take the new health and safety regulations coming into force on April 4, for example.

"There is a much greater obligation to ensure that contractors or other visitors to a site are briefed about any current hazards, and to track when they're coming and going and where they are on a site at any given moment," Mr Johnson says.

"Security systems are very good at that, especially new technology suites that are specifically designed to capture and advise new health and safety hazards."

Some can even provide online tutorials that identify what safety issues are in a particular building and allow visitors to pre-register for access once they've completed them. "And again, that introduces efficiencies."

There is also the accuracy offered by biometric technology, which measures such characteristics as fingerprints to authenticate an individual's identity.

Although Mr Johnson says less than 1% of Global Securities' clients use biometrics – one site he cites is Fletcher's Auckland international convention centre build – he expects there to be an increased uptake in the technology as a result of its

Continued on P22





## Technology enabling security threats combatting it as well

**Hamish McNicol**

Advances in technology have created new, "arms-length," security problems for modern businesses but these same advances are increasingly helping to solve them as well.

The most obvious security threats for businesses include burglary and physical attacks but the modern landscape has seen these threats expand into the realm of cyber-attacks.

SLS Security Group director David Morrissey says it is clear the threats to business are widespread but the days of this mostly being physical attacks are "long gone."

The emergence of threats to cyber security has resulted in a company's infrastructure, data security and IP protection being able to be "devastated" through "arms-length" abilities.

**PARAMOUNT:** Security threats to business are widespread but it is no longer limited to simply physical attacks Experts (from left) Graham Zuill, David Morrissey and Adrian Kereszteny explain why

"Cyber-attacks can be executed from thousands of kilometres away whereas traditional threats were locally based at a company's premises.

"It should be of paramount importance to every organisation, as the ability to trade relies heavily on the security of its business assets, staff and infrastructure."

Mr Morrissey says businesses are becoming more aware of the need to address security, partly because of high-profile cases such as Apple's recent refusal to allow the FBI access to an iPhone's data.

He says all businesses are susceptible to threats but some more so than others.

"Those that keep sensitive information or private persons' data have a higher threshold of responsibility.

"Those involved with major infrastructure, such as rail and airports, are also potentially more susceptible to attack."

Focus Digital director Graham Zuill says businesses need to evaluate their risk based on the market they operate in, installing security systems and protocols to reduce any threats.

All businesses face burglary risks, so fundamental preventions include a monitored alarm, closed-circuit television, safes and professional-quality locks.

But, while technological advances have threatened business security in new ways, it has also "significantly changed" the way they can manage it.

"The quality and speed of information transmitted over IP makes the systems an invaluable and cost effective investment.

"Some of the key benefits are being able to remotely access a site's CCTV cameras, network multiple sites' CCTV for centralised management, respond to alarm activations, change passwords and authorise site access."

### Forgeries 'almost extinct'

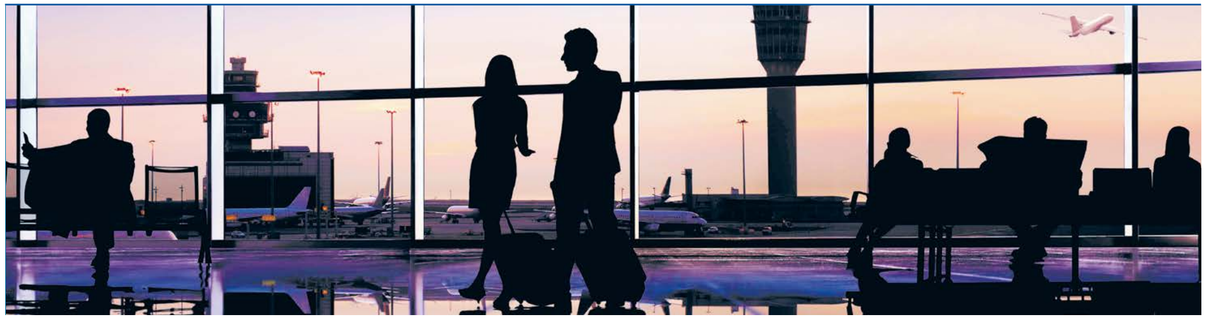
Key technological advances in the security field include systems such as optical character recognition (OCR), which is used in licence plate recognition and document scanning technology.

Image Analytics Pacific director Adrian Kereszteny says ID document scanners are "indispensable" to crime prevention, including money laundering and terrorism financing.

His company specialises in Automatic Number Plate Recognition (ANPR) technology and ID document scanners, used in over 70,000 applications across the world.

ID scanners can be used with immigration, banking, law enforcement, airport, access control and other systems, he says.

Continued on P21



# Staying safe while travelling

**Nathan Smith**

As these words were being written, Islamist militants kidnapped two Australian nationals in Burkina Faso, dependents of Indian businessmen were targeted for ransom and statistics predicted 3800 cyber-attacks would target New Zealand businesses in the course of the day.

It is an unsafe world. From the abductions of travelling executives to the targeted threats against the children or spouses of these individuals, the risk to businesspeople is increasing even in New Zealand. AIG estimates about 40,000 kidnap-and-ransom cases involving business travellers are reported every year.

And, according to the most recent Global Kidnap Report compiled by Neil Young & Associates International (NYA), a global risk and crisis management consultancy, the travel risk extends to lower-echelon executives as well, especially considering these executives generally aren't given their own personal protection details while travelling.

The report also says threats in Asia have varied and evolved between countries over the past year. In the Philippines, the Abu Sayyaf Group has heightened the kidnap threat to foreign nationals in the south, and a potential rise in "express and virtual kidnappings" in China may stem from the growing use of social media.

Most large organisations recognise the need for a specialised security expert. Often they are part of the C-suite of executives responsible for the security of the entire corporation, its employees and perhaps information data as well.

Yet many New Zealand businesses can't justify employing a permanent chief security officer (CSO). And even in the largest organisations, a CSO can't follow a travelling executive to every meeting around the world. And, since executives will face threats regardless, a proper security attitude can go a long way in protecting the individual and ensuring a safe return home.

Travel security for executives is similar to standard security: it requires practice and a good level of "situational awareness." This concept is explained by international strategic intelligence company Stratfor as a mind-set of relaxed awareness.

"We've found the most effective way to illustrate the differences between the levels [of awareness] is to compare them to the different degrees of attention people practise while driving. These five levels are "tuned out," "relaxed awareness," "focused awareness," "high alert" and "comatose."

"If one is tuned out while driving and something unexpected happens – say, a car ahead stops quickly – one will not see the problem coming and probably freeze. This happens also when a criminal catches someone unaware and unprepared," says Stratfor's vice president of tactical analysis Scott Stewart.

Because of this, the basic level of situational awareness that should be practised most of the time is relaxed awareness, a state of mind that can be maintained indefinitely without all the stress and fatigue associated with focused awareness or high alert. There is a difference, he says, between being paranoid and being alert, especially when travelling overseas.

The danger extends to the cyber world as well. New Zealand's Government Communications Security Bureau (GCSB) former acting director Una Jagose told the *National Business Review* "spear-phishing" – a cyber-attack targeting a particular individual – is becoming more common, along with "cyber ransom" attacks. Both of which often target executives.

"Spear-phishing makes up around 30% of the threats reported to or detected by the National Cyber Security Centre (NCSC)," Ms Jagose says.

Mobile devices and laptop computers are especially vulnerable when travelling. Not only do executives need them to conduct business but also the devices generally store sensitive data. Criminals looking for such information may not need to conduct a risky kidnapping if they can access an executive's computer instead.

Commercially available encryption can help defend against the exploitation, but avoiding exposing the device or laptop to compromising situations is more important. For instance, a computer should only store information relevant to the current visit. Carrying extra passwords, account numbers or data risk greater damage to the company if the machine is compromised.

Also, hotels generally supply secure internet access for guests. Criminals or perhaps rival companies may be monitoring the unsecured wi-fi services in the vicinity. So to avoid a device's internet signals being intercepted, logging on to a secured network is crucial for safety wherever an executive is travelling.

Mr Stewart says good security can be learned by anyone, not just the professionals. For example, a person can consciously increase their awareness level for short periods during the day. Perhaps to identify the exits when entering a building, counting the number of people in a restaurant or noting which cars take the same turns in traffic.

"Performing simple focused-awareness drills trains a person's mind to be aware of these things almost subconsciously when the person is in a relaxed state of awareness. Once a person is in such a state, they're far better prepared to handle the jump to high alert if the threat does change from potential to actual," he says.

nsmith@nbr.co.nz

> **Spear-phishing makes up around 30% of the threats reported to or detected by the National Cyber Security Centre (NCSC)**
>
> – Una Jagose





# Cyber-attacks – the ominous shadow over SMEs

**Jason Walls**

The business cycle is ruthless for start-ups and SMEs.

Traditionally, issues such as market volatility, poor planning, and market saturation are blamed for the failures of SMEs. But there is a relatively new threat that is often overlooked – cyber-attacks.

Although the alluring pull of being one's own boss and flexible hours has attracted many people – 97% of New Zealand enterprises are SMEs – cyber risks are an issue many SMEs don't take into consideration.

Global insurance broking and risk management firm Marsh ranks cyber-attacks as the third-biggest risk facing corporates and the second-biggest risk facing small businesses.

Deloitte head of cyber, privacy and resilience Anu Nayar says it is a similar story in New Zealand, and "it's not if [an SME] is going to be attacked, it's when."

He says cyber-attacks are an "extremely real" threat for SMEs because many businesspeople are new to the world of cyber.

"Also, a lot of SMEs now are incredibly reliant on technology and digital as the basis of their competitive advantage," he says, underscoring the importance of SMEs preparing for attacks.

**SMES MUST BE PREPARED:** Deloitte head of cyber, privacy and resilience Anu Nayar

Last year, Prime Minister John

**Continued P22**

## Three ways SMEs can better prepare for a cyber-attack

Deloitte cyber, privacy and resilience head Anu Nayar gives three tips on how SMEs can prepare for cyber-attacks:

**1. Understand the risks:** If the SME works with a bigger business or a business partner, there is a risk an attacker could be trying to get to the corporate through the SME's network. It's important to check any vulnerability and liaise with other partners.

**2. 'Crash your own gates':** Mr Nayar advises testing one's own system. He says it's important to "examine your own people and make sure basic hygiene security factors are followed in terms of secure systems and ensuring processes that can protect the data."

**3. Be prepared:** When an attack does occur, it's important SMEs have a game plan. Mr Nayar suggests running "cyber war games to test employees and make sure they are exercised for the proper response."

# Tech enabling security threats combats it too

**From P19**

"Devices scan, read and authenticate ID documents such as driver licences, passports and evidence of age documents.

"In the event that the scanned document is found to be counterfeit, or the person is on a 'black-list,' the system notifies the operator in real time."

Licence plate recognition technology is not only an efficient crime prevention tool, he says, but can also be used to improve traffic and pedestrian security.

This includes electronic toll collection, speed enforcement, red light enforcement, drive-off and theft prevention and parking management.

Mr Morrissey says such security innovations have resulted in solutions that "cross-pollinate" different sections of the workplace, moving security providers from simply dealing with security personnel to systems that can have benefits for areas such as marketing and human relations.

He says video analytics, which can detect situations and provide alerts in real time, are also emerging as a "primary tool" for business security.

"The fraud detection technology in use today is quite frankly so good that forgeries are almost extinct."

hmcnicol@nbr.co.nz

# Adding value saves time, cost

**Nevil Gibson**

Corporate security firms are adopting new practices and adapting to changing circumstances as they provide a range of services from health and safety procedures to protection against internal threats.

Matrix Security chief executive Scott Carter says it's more about adding value than just responding to alarms.

"Providing the right security technology and great service response is only the base line nowadays – you've got to become a trusted partner in protecting both people and assets," he says. "We've become an integral part of many customers' health and safety teams, as well as looking after crime prevention initiatives."

Matrix Security provides all the guarding operations at Yashili's new $220 million high-security milk powder plant at Pokeno. The site is fully fenced with electronic gates, video surveillance and access control to all key areas of production.

It is an example of how the digital era provides real accountability and transparency to security operations.

"Intelligent video surveillance, smart analytics and app-based automation or reporting are backed up with effective human intervention," Mr Carter says.

"You've got to have smart people using smart tools."

Gallagher provides high-tech security equipment to clients in 100 countries from its Hamilton base and other plants around the world.

Steve Bell, its chief technology officer, says identity is the key to internal security.

"Technology has moved from traditional keys that are untraceable, unmonitored and easy to copy to smart cards, PIN pads and now biometrics," he says. "Access is determined by a unique identifier, something that cannot be used by another person."

Perimeter security is used to detect, deter or delay intruders or escapees but it can also be turned into an opportunity for business continuity planning.

"It is the first point of access control to a site," Mr Bell says. "By combining these, you can determine not only who, where and when but most important, why? Are these people authorised to be where they are?"

Establishing this at the perimeter saves downtime and cost through preventing stoppages due to inadvertent site access, damage and injury.

"Having the capability to prevent harm to people or equipment through a multi-technology perimeter solution is hugely valuable."

*ngibson@nbr.co.nz*

# Traditional threats

From P18

falling cost and improved programming.

"Biometric technology used to struggle in environments where there were a lot of tradespeople, for example, because their generally worn and caloused hands were hard to read – now there are systems that get around that by reading veins instead."

**One-stop shop prop**

Given that Global Security bills itself as "New Zealand's largest full service security company," it's hardly surprising that Mr Johnson is keen to push the benefits to companies of dealing with just one security firm – just as they tend to have one IT or telco provider.

The majority of New Zealand businesses contract to multiple security providers for the understandable reason that they take a piecemeal approach to their security needs as their organisations grow – inheriting an incumbent security service when they buy a new building, for instance.

"But taking that approach means they're missing out on the full benefits – including lower costs, and improved compliance and productivity – of a truly integrated security solution in which every aspect is working in concert."

*ngrant@nbr.co.nz*

# Cyber-attacks – the ominous shadow

From P21

Key warned cyber-attacks will become more prevalent in the coming years.

"On a daily basis, it is not unusual for some government departments to have close to 6000 issues with people trying to get into their digital systems.

"If they're doing that to us, I don't know what they are doing to you guys," he said, referring to SME and corporate businesses.

Mr Key said he suspects a lot of chief executives and directors have the "it's not going to happen to me" mindset and urges companies to address cyber security risks.

"As you sit around the board table, I would start having conversations about cyber security. Ask your chief technology officer what they're doing about it," Mr Key said.

Massey University senior lecturer of defence and security studies Andrew Colarik agrees with Mr Key's comments but takes it one step further than just cautioning small businesses.

"All of New Zealand is at risk.

> **"It's not if [an SME] is going to be attacked, it's when**
>
> – Anu Nayar

Not just small businesses, everyone," he says

"We're an island nation so all of our logistics, ordering and communications are at risk. We're dependent on information technology for many areas in our economy."

Professor Colarik says smaller businesses tend to be much more at risk of cyber-attacks than larger ones.

But Mr Nayar says the risks to both are equal but for different reasons.

"For SMEs, the risk is they can sometimes be perceived as being an easier target," he says.

"They can also have simplistic technology deployments that have not yet been secured by design."

Although a lot of small businesses may do smart things to prevent attacks, many don't typically work on vigilance and resilience, Mr Nayar says adding it's important SMEs adapt and become more resilient.

"Resilience is about being able to monitor and detect when a threat has been successful. It's also good crisis management and boosting of response capability," he says.

*jwalls@nbr.co.nz*