SECURITY
EXHIBITION + CONFERENCE

INDUSTRY WHITEPAPER 2019

SECURITY MARKET REVIEW

Navigating an Evolving Security Landscape

BROUGHT TO YOU BY

diversified
COMMUNICATIONS ▪ AUSTRALIA

EXECUTIVE SUMMARY

SECURITY EXHIBITION + CONFERENCE

Drawing on information sourced from a recent national survey of security industry professionals and their customers, the Australian Security Market Review 2019 offers valuable industry data, insights and trends, as well as predicted areas of growth over the next three to five years.

The survey respondents

Survey respondents consist of suppliers, installers, integrators and end users, who were all asked their opinions on topics such as product demand and spend, current and anticipated challenges, industry trends, expected growth areas, and technological advancements.

The findings

In positive signs for the industry, the majority of respondents believed that demand for security products will continue to grow over the next three to five years. This demand is being driven by a number of factors, including better affordability, the need to combat the rise in cybercrime, ease of integration into other systems and platforms, and the rapid growth of the Internet of Things (IoT).

Analysts agree with respondents on the need to combat cybercrime with better cyber security. The incidence of targeted cyber security attacks on Australian organisations is increasing, with research showing it more than doubled in the year to 2018. Therefore, a swathe of research is focused on how better cyber security is likely to benefit businesses and the wider economy.

Estimates suggest spending on cyber security measures is set to increase by 88 per cent by 2026, and Australian companies will have the opportunity to benefit from this spending. Growth will be driven by the movement towards digitisation, with spending on digital infrastructure, data, digital technologies and connectivity essential to key Australian industries.

Research also indicates the next decade will see the rapid growth in the Internet of Things (IoT) market, as connected smart devices continue to infiltrate companies and homes.

Industry-wide challenges

When it came to challenges the industry is currently facing now and expects to face in the future, the survey focused predominantly on suppliers. Many respondents identified keeping up-to-date with new technology as an ongoing challenge. Lack of qualified staff was also mentioned, as was educating customers on the benefits and value of security to their business.

These findings suggest a need for better training and accreditation of personnel within the Australian security industry to ensure staff have the skills required to respond to an increasing number of threats and to apply their knowledge in a dynamic environment.

A changing security landscape – in which both digital and physical threats are commonplace and quite often integrated – presents a new challenge for security personnel that will require new knowledge across a range of different environments and platforms.

Some security professionals have called for better regulation of accreditation to meet the demands of a growing industry that will not only be better equipped to deal with a complex security environment now, but also to adapt to new threats in the future.

Better industry-wide collaboration is required to help counteract a growing threat of terrorism and to counteract the threat of international cyber-attack. This can only be achieved with a highly professional security workforce that is also keeping up to date with rapidly changing technology.

Consultation with key government departments involved in Australia’s national security is also vital to ensure the security industry is a key player in protecting the country’s interests and assets, industry experts say.

How best to integrate physical and electronic security is a topic of great importance as professionals grapple with the need to maintain a security presence across multiple operational fronts.

In the respondents' answers, it was interesting to note that a number of suppliers also suggested the issue of automation replacing personnel as an issue that will present a growing challenge.

There is evidence to indicate that automation will result in fewer personnel. However, as this report will show, automation is also a potential area for growth within the Australian economy. Companies that have the foresight to adopt automated security technologies in coming years can leverage the financial gains this is likely to bring.

How companies will balance the operational advantages of using new technologies such as facial recognition with a need for privacy is still unclear and should also present a challenge to the industry in the next decade.

Major industry trends

When survey respondents were asked about major industry trends (both now and in the future), the rise in cybercrime and the evolution of new technology were the two main responses. It was to be expected, therefore, that current product trends identified included cyber security, CCTV monitoring and smart cameras, and biometrics and facial recognition.

Better cyber security in the corporate sector is on the minds of many industry leaders because of a range of attacks that have disrupted some businesses and crippled others in recent years. Cybercriminals are becoming increasingly sophisticated, employing a range of software applications.

To counteract the threat of cyber attack to Australian organisations, the Australian Government launched its Cyber Security Strategy in 2016. As part of this plan, more than $230 million has been invested in cyber security measures, including developing Academic Centres of Cyber Security Excellence to combat the problem.

Respondents also identified three areas that are expected to see significant growth in the foreseeable future, namely IP and the cloud, the Internet of Things (IoT) and biometrics and facial recognition. Driving this growth will be improved accessibility/reliability/affordability, increased demand and enhanced network speed and capacity.

Cloud services have matured over the past couple of years to the point that many Australian companies now operate with a "cloud first" or "cloud only" strategy for data storage.

The main driver of cloud adoption by companies is cost considerations and the need to balance capital expenditure with operating expenditure, studies have shown. Agility – the need to react with speed in the marketplace – is another key reason.

Research shows growth in the adoption of IT and the cloud is also being driven by the need for better cyber security. However, there are also concerns about keeping cloud data secure from cyber-attack as this form of data management is especially prone to misconfiguration attacks.

Used correctly, IoT devices can improve yields, make better predictions and reduce costs. Studies indicate that the adoption of these technologies could result in nationwide efficiency gains of between 15-40% across key industries.

Biometric technologies such as digital fingerprint, palm print, iris verification and voice recognition technologies have become key in the fight against identity fraud and theft and as tools for security personnel to identify individuals as potential threats.

Research points to facial recognition technology as being the key biometric technology that is likely to see widespread adoption in the next decade. Facial recognition technologies are especially useful when deployed by smart CCTV cameras. When used in this context, this technology can significantly increase the operational efficiency of security personnel.

There's no doubt the Australian security market is extremely robust and adaptable. What's more, technological advancements and customer demand forces professionals to continually evolve their product offering, which in turn drives innovation and ensures a secure future for the industry.

RESPONDENTS

OUR INDUSTRY AT A GLANCE

The findings presented in this report are captured from a wide cross-section of survey respondents involved in the Australian security industry, including leading experts, end users (Security Managers and alike) and consultants, installers, integrators, and suppliers of security products and services.

Looking at the survey group more closely, 48% of respondents identified as an end user/consultant, 21% identified as a supplier, 17% as an installer and 14% as an integrator.

In terms of business size, 32% of respondents said they worked for a company that had less than 10 employees, while 26% worked for a company that had more than 500 employees. That left a fairly even spread of respondents who worked for companies that employed somewhere between 10 and 500 people.

When end users and consultants were asked about the product areas of most interest to their organisation, biometrics and identification came out on top, closely followed by networking and integration, monitoring and control room equipment, and cyber and information security.

These results largely aligned to supplier responses when they were asked about the average customer spend by product area. Cyber and information security topped the list with $353,623, followed by biometrics and identification at $284,125.

The higher proportion of spending on cyber security is unsurprising considering the huge risk of cyber-attack, especially to small businesses in Australia.

Suppliers were also asked about the product areas they operated in. The results proved enlightening, with 59% involved with CCTV and monitoring and 52% in access control. Other notable areas included alarms and fire safety (33%) and network and integration (30%).

When suppliers were questioned about plans to move into other products areas over the next three years, nearly half the respondents had no plans at all, with 11% nominating home automation and 10% answering biometrics and identification.

Interestingly, these results suggest that companies may be somewhat overlooking the advantages of developing cyber security products despite this being an acknowledged trend, or lack the technical know-how to do so.

And, finally, suppliers were asked to identify their customers. The most common customer types were corporate end users (68%), followed by security integrators (65%) and security installers (52%).

DEMAND

A STEADY FLIGHT PATH

SECURITY EXHIBITION + CONFERENCE

In encouraging signs for the Australian security industry, the majority of survey respondents (suppliers) were confident that demand for their products would continue to increase over the next 12 months.

Many respondents reported steady product demand over the past 12 months, with no evidence to suggest this wouldn't continue throughout 2019 and beyond.

This was also the case when respondents were asked about the Australian security industry as a whole. The overwhelming consensus was there would be no decrease in demand across any product area over the next 12 months.

When the survey drilled further down into specific product areas, drones/UAVs/robotics was predicted to experience the highest increase in demand, followed by major events security, CCTV and surveillance, cyber and information security, and biometrics and identification.

Let's look at two of these key trends more closely.

1. DRONES/UAVS/ROBOTICS

Robotic technologies such as drones, UAVs and robots are considered to be at the forefront of what is being referred to as the "Fourth Industrial Revolution", a term used to describe the convergence of digital technologies with the physical world.

The largest number of survey respondents that believed a product category was going to increase in the next 12 months (9%) identified these as being drones, UAVs and robotics.

This new wave of intelligent automated technology is expected to be a huge financial growth opportunity for Australia in the coming decade. It has been estimated that robotic automation can boost Australia's productivity by $AU2.2 trillion by 2030.

For security, law enforcement and defence, the applications for robotic technology are varied and the potential to develop this industry in Australia is high.

Australia is considered a global leader in the research and development of cyber-physical systems, computer vision, field robotics, simulation and robotic visions and has developed a thorough plan to capitalise on this innovation through to 2030 (the Innovation and Science Australia – ISA – 2030 plan). However, as a nation, Australia has a long way to go before it is can truly be said to be a world leader in the automation industry.

Australia currently ranks 18th in the world when it comes to the application of industrial robots, with 50% fewer firms engaged in automation than the leading countries.

Drones and UAVs in Australian security applications

Analysts are expecting huge growth in coming years as drone and UAV products enter the Australian marketplace. In fact, research firm PwC estimates the emerging global market for commercial drones is expected to be worth US$127.3 billion by 2020, while the predicted global value of drone-powered solutions in the security industry is expected to be US$10 billion.

According to PwC's Australia's digital experience centre leader Nick Spooner, drones are making the transition from novelty item to indispensable business tool.

"Removing regulatory hurdles to encourage innovation and investment in technologies such as Unmanned Aerial Vehicles is vital if we're going to grow the Australian economy," he says. "The recent relaxation of regulations for commercial drone operations by CASA is a great first step."

Drones: Risks and challenges

Risks of commercial drone use include the risk of data theft, the possibility of loss of control, the chance of collisions with other aircraft, limited battery power and an increased company liability, to name just a few.

"For security, law enforcement and defence, the applications for robotic technology are varied and the potential to develop this industry in Australia is high."

Perhaps the biggest concern to private security companies is the possibility of data theft via security drones. One concerning finding from the Department of Homeland Security in the US is that overseas- manufactured drones include technologies that could be used to transmit data to hackers overseas.

While these challenges are unlikely to disappear with a one-size-fits-all solution, they will require consideration by security personnel to make the best use of this technology.

Security robots have arrived

Thirty-five per cent of survey respondents identified robotics as the security industry product category experiencing the greatest rate of innovation.

Robots capable of autonomously patrolling premises have only recently been introduced into Australia and are mainly in a trial phase by many organisations. These devices, it's thought, will be helpful in solving significant problems involved with security patrolling by bringing together detection, coverage, mobility, communication and reliability in one solution.

2. MAJOR EVENTS SECURITY: WHAT'S TRENDING

Survey respondents predicted major events security as the sector likely to experience the greatest increase in demand in the next 12 months, after drones, UAVs and robotics.

Increasing interest in this sector has been largely spurred on by a host of global terrorist attacks in the past five years, industry experts say. Australia has had seven such incidents – significantly less than those in many other first world nations – however they have created a culture of preparedness nonetheless.

The Federal Government has allocated a $570 million funding boost for counter-terrorism and anti-espionage operations in the 2019-2020 budget, including a major resourcing package for ASIO and the Australian Federal Police.

While these are federally funded measures, the important role that private security plays in Australia's national security and preventing terrorism is a key message that many government bodies and private security professionals are hoping to spread.

This message has been a focus of considerable discussion at industry events in the past 12 months, notability at The Business of Events Conference 2019, where the importance of readiness testing, crowd management, risk management and compliance were key discussion points.

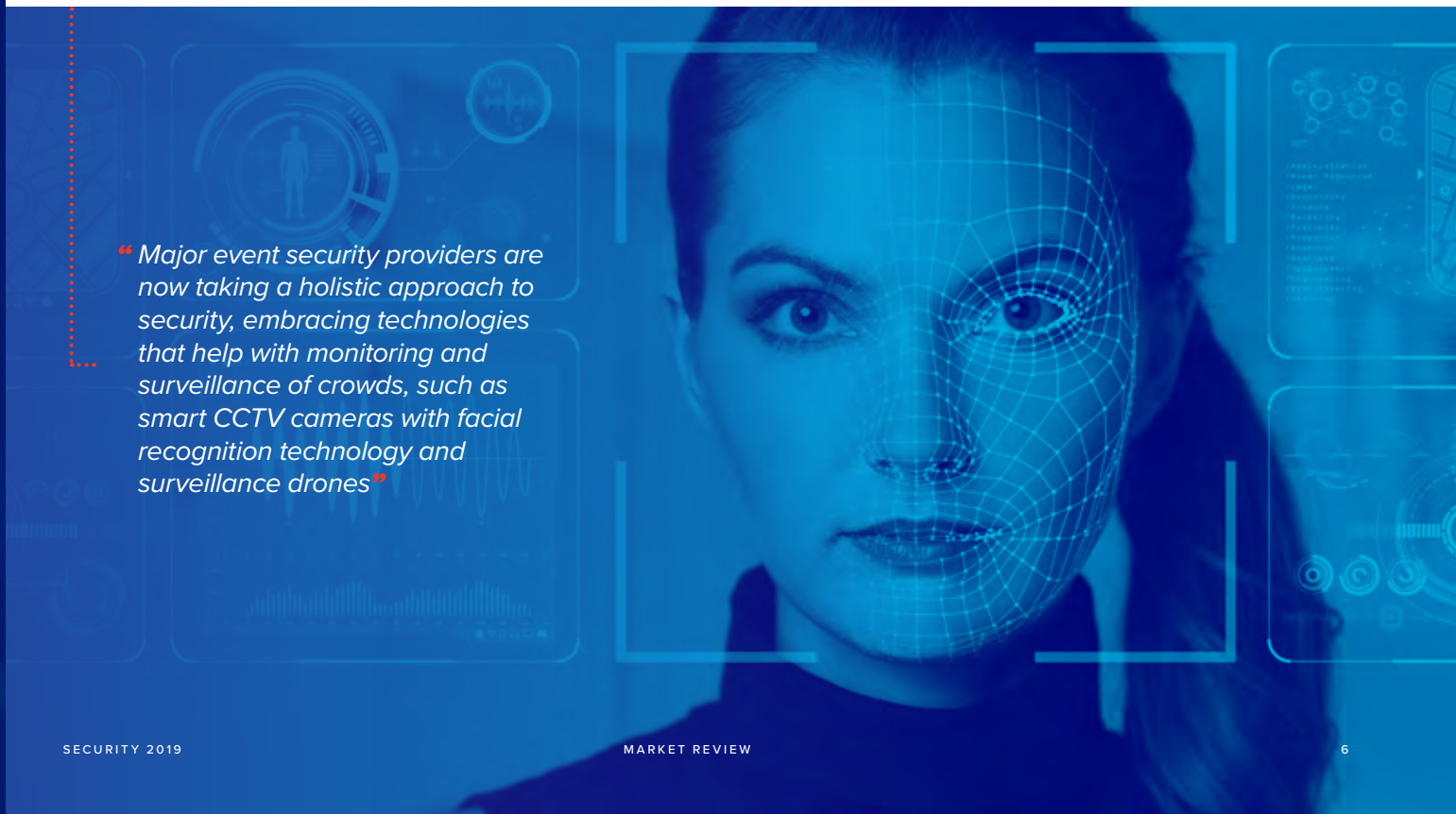
Major event security providers are now taking a holistic approach to security, embracing technologies that help with monitoring and surveillance of crowds, such as smart CCTV cameras with facial recognition technology and surveillance drones, while also employing tried and tested traditional and physical methods of security.

Key trends in this field include carrying out thorough risk assessments and undertaking elaborate consultation with event clients, says Darren Horne, senior manager, security and safety, at the Melbourne Convention and Exhibition Centre.

"Because of global incidents, clients are more aware of the threats to their own personal safety, so it's not just security managers thinking about security and safety," Horne says. "That means there is more emphasis on the planning phase of security and a greater consultation process with the client."

The development of AI software is going to have an impact, too. One such product, DCM by Dynamic Crowd Management, is an innovative, autonomous, data analytic solution that can measure the mood of crowds and was used as a crowd management solution at Vivid Sydney.

This software and other data analytic products like it are expected to see widespread application in major event security in the next decade.



"Major event security providers are now taking a holistic approach to security, embracing technologies that help with monitoring and surveillance of crowds, such as smart CCTV cameras with facial recognition technology and surveillance drones"

CHALLENGES

HARNESSING TECHNOLOGY TO DRIVE BUSINESS GROWTH

As with any industry, business challenges come in many different forms, whether it's staying abreast of evolving technology, meeting fluctuating customer demand or educating clients on the value of your offering. So what are the specific challenges faced by the Australian security market, both now and in the future?

Across the survey group, there were some common themes that emerged. Namely, keeping up to date with technology (50%), clients/stakeholders not accepting new technologies or understanding systems (50%), access to trained staff and education (49%), licensing and regulation (48%), and the rise of the Internet of Things (46%).

Additionally, there were three areas that respondents expected to be more challenging in coming years than they are presently; reactive upgrades, clients/stakeholders not seeing the value in security, and personnel being replaced by automation.

When respondents who identified as "suppliers" were asked about some of the challenges their customers experience, there were three main themes that emerged: keeping up to date with new technology, competition and the cost of upgrading.

Encouragingly, more than three-quarters of respondents were taking action to address the challenges faced by their customers. This action includes education and awareness (45%) such as training sessions and webinars, developing new products (20%) and providing low-cost solutions (14%).

Overall, however, these were the five key challenges identified:

- Keeping up to date with technology
- The case to integrate physical and electronic security
- Need for a modern accreditation system
- Will automation replace jobs?
- Why technology is a double-edged sword

Let's look at those more closely.

Keeping up to date with technology

Technology is integral to the security industry. Therefore it's somewhat concerning that survey respondents earmarked this as a challenging area.

Recent industry-changing technologies include the introduction of smart CCTV cameras, the use of drones and robots and the increasing introduction of artificial intelligence and machine learning. All of these technologies offer tremendous operational benefits, however they do require specialist skills and knowledge to operate.

In a rapidly changing industry, it is now considered critical for Australian security companies to have research and development strategies to find and acquire new cutting-edge technologies.

It's also important to note that while acquiring and integrating new technologies is a good first step for private security organisations, the benefit these technologies bring is critically dependent on the knowledge and skill base of security personnel and how these technologies are applied.

Arthur Baker, principal consultant at T&L Enterprises, says industry training standards need to be brought up to speed. "Australian standards are very basic and rudimentary," he says. "And they haven't been updated from the days of analog before we had IP networking and HD megapixel cameras.

"What's more, there is no uniformity of regulation from state to state. For instance, in Western Australia, to even get a security licence you need to have done courses in alarms and CCTV, but that's the only state with that requirement."

The case to integrate physical and security measures

The rise of connected, seamless electronic technologies as security tools is a big plus for security personnel. Formerly distinct technologies such as electronic access control systems, alarms, keycard readers and CCTV cameras are now connected to the internet and are increasingly synergistic.

While these technologies and their associated IoT technologies have allowed security personnel to centralise and simplify their operations, without proper organisational awareness about how to integrate physical, electronic and personnel security measures, companies remain vulnerable to a range of security threats, says Michael Taga'i, event security manager at the International Convention Centre Sydney (ICC).

"Electronic security, physical security and personnel have traditionally been considered as independent forms of security, but they are now all connected and rely on each other for the same end result," says Taga'i.

"For example, when it comes to preventing cyber-attack, you can have the best firewalls in place and ICT technicians on your side but if staff aren't trained not to click on spam emails, if they're not trained in protocols around using USB devices or in downloading and uploading data to your systems, it can easily result in a security breach," he says.

> *"What the technology is doing for me is just making my security response faster and more efficient."*
>
> JOHN LOMAX | THE STAR

The need for a modern accreditation system

Respondents indicated a lack of access to trained staff and education as one of the biggest challenges for the private security industry. This is a theme repeated throughout the private sector and it is strongly linked to a lack of career progression, say industry professionals.

John Lomax, general manager of asset protection at The Star Sydney, says companies need to take responsibility for training within their organisations to make sure staff can apply technologies effectively.

"It is critical to train people and it's also critical to train them the right way," he says. "At The Star, we are constantly training and updating staff. It's not about ticking off a box to say we've done it, it's about effective risk mitigation, ensuring my officers are up to date with the right set of skills."

An examination of the current career progression of security guards indicates the need for a security accreditation system that better matches the skill requirements of a rapidly changing industry.

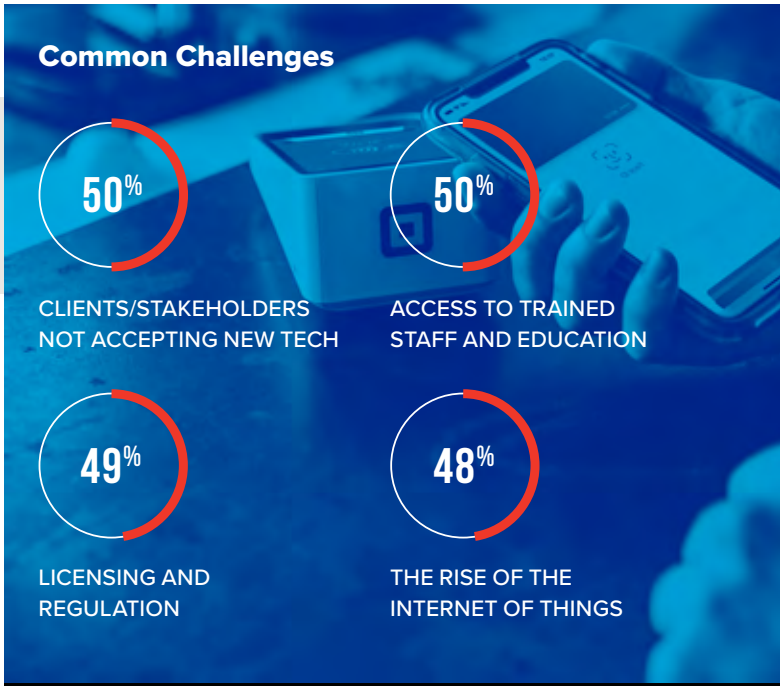
This is expected to reduce the staff shortfall that is particularly noticeable for the higher levels of security occupations, where a thorough integration of different kinds of security is required across an organisation's operations.

For example, many security personnel start off as entry-level Certificate II guards or crowd controllers and then progress on to supervisor once they have gained the appropriate level of experience.

However, there is no formal training or educational pathway from security officer to the role of management within the sector since the Certificate IV and Diploma tiers of accreditation relate more to risk assessment rather than the development of additional administrative skills.

Some employers have tried to solve this dilemma by offering their own training and development programs and this approach seems to provide some form of staff development to senior management. However, the lack of industry accreditation for senior security personnel means there is no industry-wide standard.

A new accreditation structure might include the establishment of a certificate that would award the title of Senior Security Officer or equivalent.



Will automation replace jobs?

While it's hard to predict the precise impact automation will have on the industry, there are reports across the markets that indicate that the continued shift towards mechanisation and automation of working processes could cause a significant reduction in jobs.

One alarming report, The Future of Work by the Organisation for Economic Co-operation and Development (OECD), predicts the loss of 14% of all Australian jobs within 15 years.

However, this figure doesn't take into consideration the economic benefits of employees moving to higher skilled occupations in the industry.

This is no small amount either. The expected income from automation-driven productivity gains through to 2030 is $AU1 trillion, while the benefit from transitioning the Australian

workforce to higher skilled occupations is expected to be $AU1.2 trillion by 2030.

Economic opportunities aside, there is still a strong need for a human presence in most security environments. The Star's John Lomax agrees.

"There is a strong case for technology," he says. "I can scan my whole premises in nine minutes when I would have had to have officers walking around for a considerable length of time to do that before. But I still need personnel on the floor and that's not likely to change."

"The need to have a fast human security response to threats is as strong as ever – because the technology has limitations. For instance, a CCTV camera can spot someone about to steal from a float, but it can't physically stop it happening. That's something only a trained staff member can do.

"What the technology is doing for me is just making my security response faster and more efficient."

Why new technology is a double-edged sword

According to technology futurist Shara Evans, new technologies that are likely to be useful for security professionals in the next decade could also be used for malicious purposes.

There are numerous examples of this, says Evans. "For example, artificial intelligence software and voice recognition software is being used to create deep fake audio and video that could be used to perpetuate all kinds of fraud and identity theft."

The other problem that the security industry faces is trying to regulate and control technologies that – while they aren't intended to be used maliciously – may actually do harm if the appropriate stops aren't put in place to prevent this.

One example is facial recognition technology. "There is research to show that facial recognition algorithms, because they've been developed to identify one particular morphological face – such as white males' faces – can quite often be inaccurate," Evans says.

"There's also the fear that this facial recognition technology could be used to create a kind of social credit system – such as those we're starting to see overseas, where you may find yourself socially disadvantaged because of the video capture of your identity, or facial expressions.

" Companies need to be aware of what kinds of data their collecting, how they're collecting it and why they're collecting it. In addition, there needs to be big penalties for companies that, through their own misuse, compromise consumer data and cause customers harm – that's the only way that they're going to take consumer data seriously."

" I can scan my whole premises in nine minutes when I would have had to have officers walking around for a considerable length of time to do that before. But I still need personnel on the floor and that's not likely to change"

JOHN LOMAX | THE STAR

TRENDS

SECURITY EXHIBITION + CONFERENCE

CYBER SECURITY AND EVOLVING TECHNOLOGY FRONT OF MIND

Faced with a rapidly evolving digital landscape, it's no surprise the survey group identified cyber security and the evolution of new technology as two of the major trends currently impacting the Australian market.

More specifically, 66% of respondents noted the rise in cybercrime was a major trend, with 67% identifying the evolution of new technology as another key trend. The increased importance of networking and integration (62%) was also seen as significant .

Other trends mentioned include an increase in cyber threats, the use of biometrics, and the rise of identity crime.

Here, a further exploration of these trending issues.

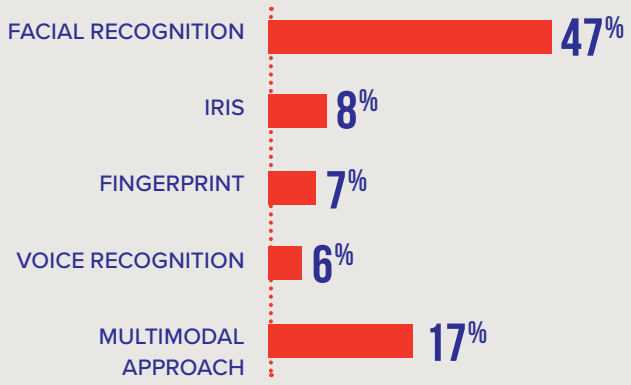
Biometrics and facial recognition

Survey respondents expected growth in this area thanks to increased demand (mainly from government agencies and industry requirements), affordability and enhanced security.

Backing up this view is a recent survey conducted by the Biometric Institute that found expected growth across a range of biometric technologies. The survey asked 310 biometric suppliers, end users and other business professionals about their expectations for biometric technologies in the next few years. The survey found that 47% of respondents considered facial recognition to be the most likely technology to boom. This was followed by iris recognition technology (8%), fingerprint recognition (7%) and voice recognition technology (6%).

Interestingly, 19% of respondents thought that a multi-model approach, whereby more than one biometric technology is used to verify individuals' identities, would be a large growth area.

Technology most likely to boom



Biometrics technologies have already been widely implemented by a range of different public and private groups in Australia. For example, the Department of Home Affairs collects biometric data including fingerprints and facial images of offshore and onshore visa applicants as a way of validating applicants' identities.

Identity crime is on the increase

The rise of identity crime in Australia is a worrying trend. Recent estimates suggest the annual cost of identity crime in Australia is approximately $2.65 billion.

An Australian Institute of Criminology (AIC) survey shows there was a significant increase in the number of people reporting lifetime victimisation as a result of identity fraud and misuse of personal information in the 12 months to 2017. Some 25.2% of survey respondents reported lifetime victimisation, up from 21.5% in 2016.

Interestingly, the survey found that criminals received most personal information about victims via the telephone (24.9% of victims), followed by face to face (23.4%) and email (21.4%). Fourteen per cent of victims were unsure of how ciriminals accessed their personal information.

New technologies

Looking ahead to the next three years, 60% of survey respondents anticipated the evolution of new technology to continue to be a major trend, as well as the creation of new markets (58%).

Evolving technologies such as mobile devices, cloud software and integrated access control systems are becoming more sophisticated. These are having an especially large impact on the security guard sector where their implementation can have an immediate impact.

One of the best examples is the smartphone. Smartphones are now being used to perform tasks such as checking cameras remotely, scheduling robotic patrols, clocking on and off work and to receive security alerts.

Other new technologies that are trending include CCTV monitoring with smart CCTV cameras, the application of drones, security robots and artificial intelligence algorithms.

These product trends align with the results about the product areas of most interest to customers, as well as the product areas suppliers are operating in (i.e., 59% said CCTV and monitoring).

Company Genetec makes a number of predictions about new technology trends the industry will likely experience this year and in the near future. These include:

- **The demand for video analytics will increase.** This includes an increase in demand for motion dection, privacy masking and people-counting technologies
- **Deep-learning AI algorithms will evolve to be able to solve domain-specific data problems.** For example, licence plate recognition systems will be able to differentiate between cars and trucks
- **Control room staff will get intuitive interfaces.** Long lists of cameras, doors and sensors built into control room interfaces will be replaced with visually engaging and intiutive user interfaces
- **Large companies will outsource access control to save costs.** This will mitigate the need to buy expensive servers and maintain them with IT staff.

Overall, the survey produced some interesting results around the topic of current and future trends impacting the industry. One thing's clear – cyber security and the evolution of new technology will continue to drive product innovation and service offerings for the forseeable future.

Risk of cyber security to Australian businesses

Cyber and information security was identified as a predicted growth area in our Australian Security Market Review 2017, and it's important to note the continued demand for this rapidly evolving product area.

Cyber-attack remains one of the most significant risks for Australian businesses. Statistics compiled by website Smart Company indicate how worrying these attacks are: in 2017 alone, 516,380 Australian businesses fell victim to cybercrime, while the average cost to a medium-sized business was AU$1.9 million.

But cyber-attack is not just an Australian problem: it's a truly international one, says Tony Vizza, director of cyber security advocacy APAC at (ISC)2.

"The World Economic Forum has published a list of the top 10 risks globally. Two of the top five risks are directly related to cyber security, whereas terrorism doesn't even come in the top 10 risks anymore. That gives you an idea about how significant a problem it is for businesses," says Vizza.

What's important in containing and preventing the cyber threat to Australian business is a level of awareness about the seriousness of the threat by both security professionals and business leaders.

Having first underestimated the risk in recent years, the corporate world is sitting up and taking notice. This is largely due to the Australian Government's regulation of cyber security in the past 18 months, particularly through the Notifiable Data Breaches Scheme.

While the new regulation represents a positive change for the corporate sector, Vizza is quick to warn about the dangers of businesses implementing a cyber security strategy simply for compliance reasons. He recommends business leaders take a proactive approach to cyber security, one that encompasses a full spectrum of cyber security prevention measures and also puts in place a response plan to deal with threats should they arise.

Cyber and information security: an opportunity for growth

Although cyber-attack presents a real and ever-present threat to Australia's corporate and public interests, there is an upside. Mainly that the Australian cyber security market is expected to triple in value from $2 billion in 2017 to $6 billion by 2026.

According to the Australian Government Disruptive Technologies Industry Capability Report, Australia is at the forefront to benefit economically from developments in safety and security online, with strong legislation and robust technical defences, say analysts.

Research from Gartner predicts Australian spending on information security is growing at an annual rate of 9.8% and is expected to reach $3.9 billion this year. The majority of spending will be on consulting, hardware support, implementation and IT outsourcing services, representing around $2.15 billion.

"In 2017 alone, 516,380 Australian businesses fell victim to cybercrime, while the average cost to a medium-sized business was AU$1.9 million."

GROWTH AREAS

SECURITY EXHIBITION + CONFERENCE

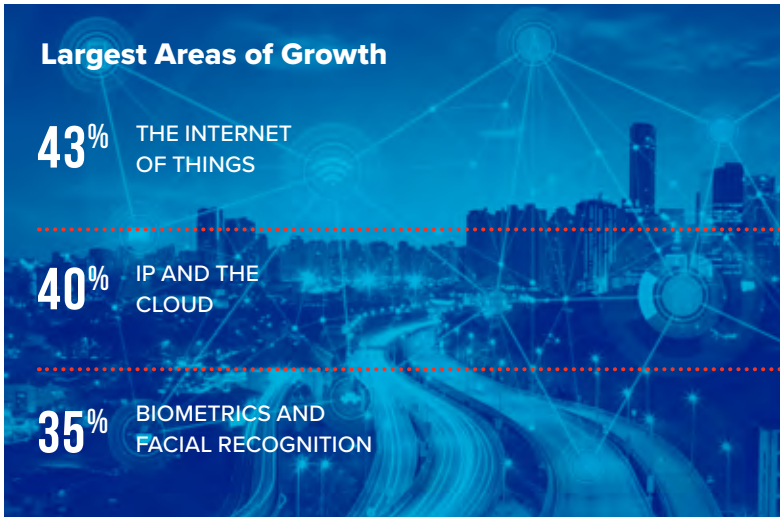
SECURITY IN A CONNECTED WORLD. THREAT OR OPPORTUNITY?

As previously discussed, there are a number of areas in the security industry that are experiencing increased demand. So where are the real growth areas and how is the Australian market placed to handle this challenging yet exciting growth.

When respondents were asked which areas will experience the largest growth over the next few years, there were three that stood out: the Internet of Things (43%), IP and the cloud (40%), and biometrics and facial recognition (35%).

Other growth areas mentioned include cyber security, CCTV/surveillance, automation, drones/UAVs/robotics, all-in-one solutions, system integration, smart and big data, mobile technology/BYOD, networking and integration, video monitoring, and access control.

Let's examine four of the main trends more closely: the Internet of Things (IoT); IP and the cloud; biometrics; and CCTV and facial recognition.



The boom in the Internet of Things (IoT)

In this segment, survey respondents saw growth as a result of increased demand for these devices, better affordability and improved network coverage and connectivity.

This response is in line with global predictions from market research firm Gartner, which estimates that the number of IoT devices in use globally will more than double in number to 20 billion by 2020.

The consumer industry is expected to remain the largest user of IoT devices, with an expected 12.8 million devices in use in consumer households globally by 2020.

In Australia, IoT-related products and services are increasing by 14% per year and the market is expected to be worth AU$30 billion by 2023.

According to Gartner, Smart TVs and digital set-top boxes will be the most common consumer IoT devices, while in businesses, smart meters and commercial security cameras will top the list.

Additionally, IoT applications specifically tailored to industry verticals, such as field devices and process sensors, are expected to reach 3.1 billion devices globally by 2020, while cross-industry IoT devices will more than double from 2.1 billion in 2018 to 4.4 billion units by 2020.

IoT: threat or opportunity?

Market research firm PwC estimates that across five Australian industries – construction, manufacturing, healthcare, mining and agriculture, which represent 25% of our GDP – the annual benefit of IoT technology to the economy will be between $194 and $308 billion over a period of eight to 18 years. This equates to a 2% productivity growth per annum that will be driven by the IoT.

An Australian IoT industry allowed to reach its full capacity could improve living standards, including benefiting health, safety and environmental outcomes. It will also allow Australian companies to become more competitive in the global marketplace and employ more staff.

Despite this significant economic opportunity, the growth of IoT is expected to see a corresponding growth in cyber-attack. By next year, it is expected that more than 25% of the identified cyber-attacks will involve IoT technologies.

This is because IoT presents a number of additional risk factors to cyber-attack than traditional IT environments. Some of these include:

- The high number of connected edge devices means that there are many entry points for cyber criminals to gain access to information.
- The huge amount of data being generated and collected means securing devices is very difficult.
- Many IoT devices are low-powered with minimal computing power and do not support cyber security systems.
- IoT allows for an interconnected ecosystem of devices which means cyber-attack on a system can affect any device on that system.

IP and the Cloud

Survey respondents believed growth in this area would come from better accessibility, reliability and ease of use, cost effectiveness, and improvements in network capacity and internet speed.

Analysts agree that this sector is likely to see significant growth. According to latest estimates from research firm IDC, Australia's managed cloud services market is predicted to increase from $1.1 billion to $2.86 billion by 2022.

Research from The Telsyte Australian Cloud Market Study 2019 indicates Australian companies are already utilising cloud services in large numbers. The study found that 84% of organisations have already taken a strategic approach to cloud computing, while one in four also have mature practices in place enabling them to move workloads from on-premises to the cloud.

Interestingly, the Telsyte study also named cyber security as both a driving factor as well as a challenge in adopting cloud computing. Some 40% of respondents indicated cyber security as a top reason for adopting cloud applications. However, 42% said cyber security remained a large concern.

Smart CCTV cameras: an advanced surveillance solution

Research firm IHS Markit estimates the market for video surveillance equipment in the Oceania region will grow annually at a rate of 4.8% to 2021.

Sydney's Star Casino relies heavily on smart CCTV cameras, says John Lomax, general manager of asset protection. The company uses fisheye cameras, as well as other types of cameras, and security personnel can view the footage of 30 cameras on one screen.

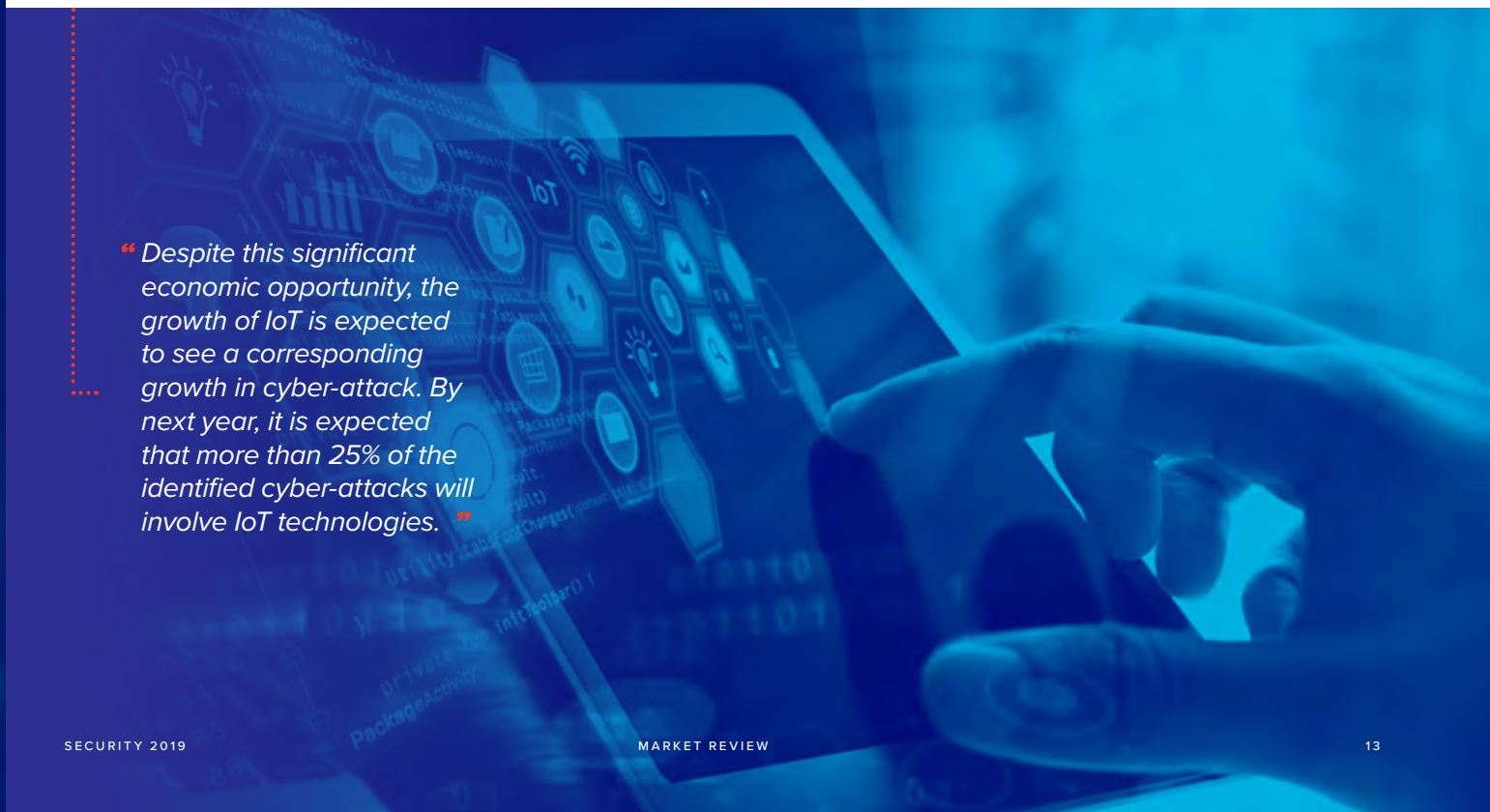
Lomax says the biggest advantage his smart CCTV cameras have been able to make for the business is the ability to do proactive scanning – catching incidents before they occur.

"Our surveillance/video console team can look through crowds of people for any signs of a potential threats or incidents and because our cameras are so good, we are able to pick up abnormal behaviours quickly. Because of this, we've seen a 25% to 30% reduction in violent incidents," he says.

Other growth areas

Respondents also named these seven areas as likely to boom in the near future.

- **Smart and big data.** Respondents believed that growth would largely be driven by emerging technologies and an increase in data generation and analysis.
- **Access control.** Growth has traditionally been attributed to legislative requirements such as in and around airports. Demand for these devices is also expected, especially in the retail and financial sector, where the protection of assets is paramount.
- **Video monitoring.** There was a perception among some respondents that growth will occur as society demands more of these types of surveillance tools.
- **Mobile technology/BYOD.** Survey respondents expected growth as a result of a greater reliance on mobile technology, as well as improvements in accessibility.
- **Automation.** The cost effectiveness and convenience of automation were thought be the driving forces behind growth in the next three years.
- **System integration.** Respondents expected growth as a result of cost effectiveness, reductions in service and maintenance costs, easier system management, and increased convenience.
- **All-in-one solutions.** They also noted that customers are increasingly seeking simple, cost-effective and integrated solutions, with one platform to control all their systems.



"Despite this significant economic opportunity, the growth of IoT is expected to see a corresponding growth in cyber-attack. By next year, it is expected that more than 25% of the identified cyber-attacks will involve IoT technologies."

TECHNOLOGICAL ADVANCEMENTS

KEEPING PACE WITH CHANGE

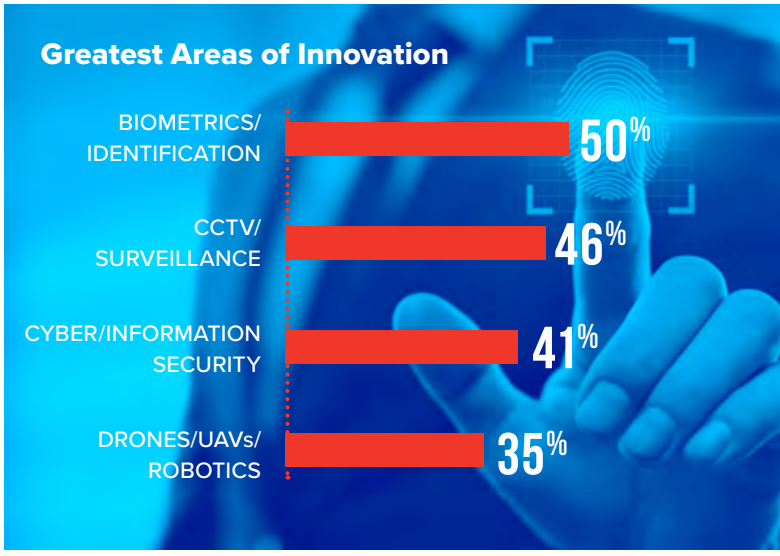
The survey found that 48% of respondents found it difficult to keep up with technological advancements and devices.

The two main reasons offered for this difficulty were the pace of technological advancements (41%) and the lack of time (23%) to research new developments, read about new products and train the appropriate people.

When asked about the subsets of the security industry that are seeing the greatest rate of innovation in technology, respondents identified biometrics/identification (50%), CCTV/ surveillance (46%), cyber/information security (41%), and drones/UAVs/Robotics (35%).

This innovation appears to be driven by an increase in the number and frequency of security threats, in addition to client demand for better, more efficient technology to combat these threats.

And finally, whether the respondent was an installer, end user, integrator or supplier, the general consensus across the board was that the need for newer, more technologically advanced products was slightly outstripping the rate at which new products are being developed.



Why the industry needs to keep pace with change

As technology rapidly changes, so too does the knowledge and operational requirements of security personnel. As was highlighted by the survey results, 4% of those surveyed said it was difficult to keep pace with technological change. As a result, it is not uncommon for private sector security firms to experience both knowledge and skills shortfalls which is often manifested as a lack of available skilled staff.

Apart from the need to alleviate these detrimental effects on the private sector, another important reason to professionalise the security industry is to secure Australia's national interests, says Dr Gavriel Schneider, Group CEO of Risk 2 Solutions and program director for the Australian Catholic University's (ACU) psychology of risk program.

"Australia is quite behind the rest of the world when it comes to leveraging the public and private capabilities of security," says Schneider. "One of the key things we have to start doing is looking at the security industry's role in securing Australia, Australian business and Australian assets.

"Conventionally, national security was something done by defence forces and other agencies, but if you follow global trends, the private security sector is increasingly stepping up and becoming critical role-players in securing their country's interests."

According to Schneider, one of the current problems is the compartmentalisation of the private security sector, which creates a lack of cohesion and reduces its operational capacity.

"The industry tends to be divided into pockets of services that are based on those services rather than what the overall intent is – such as security guards guarding premises and video surveillance personnel monitoring.

"There's a big shift that has to happen to a better industry awareness about the part that security organisations are playing on the greater scale. There's got to be a user, supplier and government maturity and understanding about the importance of each sector coming together to work unanimously if we're going to have an industry that adds value."

CONCLUSION

SECURING THE FUTURE

SECURITY EXHIBITION + CONFERENCE

As previously discussed, there are a number of areas in the security industry that are experiencing increased demand. So where are the real growth areas and how is the Australian market placed to handle this challenging yet exciting growth.

Whether protecting people, assets or information, security companies play a critical role in our everyday lives, which is why the industry as a whole needs to keep pace with an ever-changing security landscape.

Using information collected from a recent survey of security industry professionals and their customers, the Australian Security Market Review 2019 has provided valuable data and insights into the current market, as well as predicted areas of growth over the next three to five years.

The good news is that consumer demand isn't slowing down. In fact, the majority of survey respondents believe that demand for security products will continue to grow in the foreseeable future.

This demand is being driven by a number of factors, including better affordability, the need to combat the rise in cybercrime, ease of integration into other systems and platforms, and the rapid growth of the Internet of Things (IoT).

And while there's concern around the ability to keep up with technological advancements and the time it takes to adopt new technology, most respondents acknowledge the critical role technology plays in the security industry today – especially when it comes to areas such as home automation, biometrics, CCTV/surveillance, and access control.

When respondents were asked about major industry trends (both now and in the future), the rise in cybercrime and the evolution of new technology were the two main responses. It was to be expected, therefore, that current product trends identified included cyber security, CCTV monitoring and smart cameras, and biometrics and facial recognition.

Aligning with this was the fact that IP and the cloud, the Internet of Things (IoT) and biometrics and facial recognition were identified as growth areas. Driving this growth will be improved accessibility/ reliability/affordability, increased demand, and enhanced network speed and capacity.

While there are numerous challenges to overcome in the future as highlighted in this report, it goes without saying that security professionals who proactively embrace new technologies will be well positioned to take advantage of emerging growth areas.

Moreover, technological advancements and customer demand forces professionals to continually evolve their product offering, which in turn drives innovation and ensures a secure future for the industry.

REFERENCES

1. Accenture Security: 2018 State of Cyber Resilience
2. Australian Cyber Security Growth Network Ltd (2018): Australia's Cyber Security Sector Competitiveness Plan – 2018 Update.
3. Australia's Cyber Security Strategy 2016
4. Itnews Feb 21 2019: Toyota Australia hit by cyber attack.
5. Business News Australia March 13 2019: Kathmandu hit by hackers.
6. PwC for ACS (2018): Australia's IoT Opportunity Driving Future Growth
7. SUSE summary of report by Insight Avenue (2017): Online: https://www.suse.com/c/news/new-study-shows-cloud-adoption-boom-is-fueling-the-transformation-of-it/
8. Summary of report The Telsyte Australian Cloud Market Study 2019.
9. Australian Institute of Criminology Trends and Issues in Crime and Criminal Justice No. 569 March 2019.
10. Australian Small Business and Family Enterprise Ombudsman (2017): Cyber Security: The Small Business Best Practice Guide.
11. Australian Centre for Robotic Vision: A Robotics Roadmap for Australia 2019
12. Ibid 10
13. PwC May 2016: Global Market for Commercial Applications of Drone Technology Valued at over US$127bn
14. The Hon Peter Dutton media release March 30 2019: Funding Boost for Security Agencies.
15. Australian Strategic Policy Institute Special Report 2018: Safety in Numbers: Australia's Private Security Guard Force and Counterterrorism.
16. Organisation for Economic Cooperation and Development 2019: The Future of Work Report 2019
17. Ibid 11
18. Ibid 9
19. Australian Institute of Criminology Statistical Report 10 2017: Identity Crime and Misuse in Australia 2017
20. Genetec 2019: 10 Trends That Will Shape the Security Industry in 2019
21. Smart Company 2019: From Millions to Malware Cyber Attack in Australia by the Numbers
22. Australian Government Trade and Investment Commission 2017: Australian Disruptive Technologies report.
23. Gartner 2017: Gartner Says 8.4 Billion Connected Things will be in use in 2017
24. PwC 2018: Australia's IoT Driving Future growth
25. CRN 2019: Australian managed cloud services market to reach $2.8 billion in 2022