

National Security

PRACTICE NOTES

Advancing domestic and national security practice
January 2007



The future of private security

Athol Yates

This *National Security Practice Note* aims to provide security professionals and organisations with an understanding of the sector-wide trends and individual market segment trends. It is designed to help them assess the future of their business and reposition themselves to take advantage of likely developments.

Introduction

It is obvious to all that the private security market is growing. But this generalisation doesn't help security professionals or security providers to position themselves to take advantage of changes in demand and supply. Some segments of the security market will grow, others will shrink and others will require fundamentally different skills than are the norm today.

Typical analysis of market trends is based on the traditional segmentation of electronic, manpower and physical security. However, this segmentation is becoming increasingly meaningless as it does not reflect the reality of the security market. It also inhibits analysis of where the market is heading as it assumes all activities fit into one of the three categories and ignores a large number of growing niche areas which, together, make up a sizeable element of the market.

The changing security market requires security providers to revisit their analysis of what is happening in their sector. Predicating corporate planning on the average security industry growth of 6-8% will inevitably lead to significant under or over estimation in any one segment.

This article aims to provide security professionals and organisations with an understanding of the sector-wide trends and individual market segment trends. It is designed to help them assess the future of their business and reposition themselves to take advantage of likely developments.

Defining private security

When assessing the future of the private security market, the starting point is to define what it consists of. This is complex because of the diversity of the sector.

It encompasses professionals, ranging from a \$150,000 p.a. security manager of a heavily protected nuclear research facility; a \$90,000 p.a. public servant security manager at a cultural institution who is responsible for both in-house and contracted security guards; a \$70,000 analyst responsible for pulling together open-source information for threat assessments; and a \$17/hour casual patrol officer.

These examples illustrate the lack of homogeneity across the sector and thus require its breakdown into segments. The conventional categorization is listed in table 1 and reflects the State licensing categories.

This traditional categorisation ignores a large range of security-related functions which can be seen in today's organisations as they secure and maintain their personnel, assets, information and intangibles (eg reputation). These include:

- Business continuity
- Risk management
- Corporate emergency response (as distinct from emergency services such as ambulance)
- Information security

In addition, organisations are increasingly contracting in a range of niche security services to help them manage their security risks and provide continuity or growth. These niche security services include:

- Threat information (eg National Open Source Intelligence Centre)
- Kidnap and hostage recovery for executives overseas (eg Universal Risks)
- Highly specialised security advice (eg APTES)

- structural blast design engineers)
- Prison and detection centre operations (eg Australasian Correctional Services)
- Security media, public affairs and business analysis.

Finally, there are organisations which provide the policy and regulatory framework for the security sector. These functions include:

- Regulation of the security sector, eg Licensing boards
- Security policy development, eg the Critical Infrastructure Branch of the Attorney-General's Department
- Security related industry and professional associations, eg Business Continuity Institute

Few of these activities are brand new. The majority have existed for many years but have not, until



The Australian Homeland Security Research Centre undertakes independent, evidence-based analysis of domestic security issues.

National Security Practice Notes is a publication series that covers topical issues which are of critical importance to building national and domestic security capability.

National Security Practice Notes is part of the research program of the Australian Homeland Security Research Centre.

The Centre's 2007 research priorities include:

- Performance measures for domestic security policy
- The appropriate sharing of security costs and benefits between business and society
- National security capability development
- The role of the private sector security in national security

About the author

Athol Yates is the Director of the Australian Homeland Security Research Centre which is a non-partisan think-tank on domestic security.

Athol Yates
Executive Director
Australian Homeland Security Research Centre
Tel 02 6161 5143, Fax 02 6161 5144
PO Box 295, Curtin ACT 2605
Australian Institute of International Affairs Building
Level 2, 32 Thesiger Court, Deakin ACT 2600
info@homelandsecurity.org.au
www.homelandsecurity.org.au
Copyright 2006. All rights reserved.
ISSN1449-9630 (Print)
ISSN 1449-9649 (Electronic)

recently, been considered as central to securing and maintaining an organisation's personnel, assets, information and intangibles.

While this broader range of security activities is not formally recognised by Australia's security industry and professional associations, security practitioners are initiating collaboration across these areas. This is illustrated in Canberra where practitioners got together to form a Security Special Interest Group, which is a joint activity between the Risk Management Institute of Australia and ASIS, with an open invitation to Business Continuity Institute members.

Three of the most notable characteristics of the non-traditional security activities are that they enjoy above average pay rates, are profitable, and require an educated buyer to differentiate between the various price-quality options.

Estimates of the size of the security sector depend heavily on how the sector is defined. If the traditional definition of security sector is used (which is the licensed sector), then there are more than four private security personnel for every police officer.

If the large range of security-related functions, niche security services, and policy and regulatory framework organisations are added, then the number of people employed in the security sector is more than 190,000.

Growth trend pre-dates 2001

The Australian security market will probably increase between six and eight percent each year for the next five years. This assumes the economy grows at the same rate and the international security situation remains unstable. Some segments will probably grow substantially more than others, and several will grow below the market average.

It is important to note the growth figures are quite separate from profitability growth. Some segments, such as guarding, will continue to increase in turnover but their profitability is unlikely to increase.

To appreciate how growth affects your segment, it is essential to understand the reasons for growth. There are a number of gross generalizations about the causes of growth across the market or for some market segments, and these can be misleading.

It is frequently stated that the September 11, 2001 attacks fuelled a massive growth in security spending in Australia. A common refrain is that the security sector is booming because the government has allocated over \$6.7 billion since 2001 for counter-terrorism purposes. However, only about 20% of this has been accessible to the private security sector, much of which going to the niche security providers. The rest has been spent on wages, buildings and non-security products (including defence equipment) and services.

While in some market segments this expenditure has provided the impetus for rapid expansion, it has had a marginal effect in the total market. An example of the former is Sydney airport where security expenditure was \$16.6 million in 2001 and will be \$48 million in 2007. Another segment to benefit is CCTV providers

where the government's enthusiasm for cameras following the London rail bombings is driving a large number of new projects and upgrades.

However, counter-terrorism expenditure has had marginal impact for most security providers, especially those which have been suppliers to the corporate or home security market.

Another alleged reason for the growth is claimed to be that the security companies and the media are fuelling a fear of crime, leading to more people purchasing security. This assertion can be easily challenged as there is little evidence of security expenditure peaks and troughs following the media's level of crime coverage.

| | |
|--|--|
| Inquiry Agent | <p>This group is sub-divided into:</p> <ul style="list-style-type: none"> • legal work agent who provides material for lawyers in civil and criminal cases, such as interviewing witnesses, locating evidence, and serving legal summonses direct to recipients (process serving). • commercial inquiry agent who hires out investigators to carry out tasks ranging from debugging, liability investigation, workplace investigations into theft or harassment and pre-employment checks. • domestic investigation agent who undertakes personal inquiries, such as checking partner fidelity, identifying the location of children in custody battles and locating heirs and missing persons. |
| Guard/Security Officer | Provides protection through static guarding, patrol, call out, screening (as at airports), and cash-in-transit. |
| Crowd Controller | Protects patrons in places of entertainment. |
| Bodyguard | Protects individuals. |
| Security Manager | Oversees all aspects of security within an organisation. |
| Equipment – Manufacturer & Distributor | Researches, manufacturers, markets and sells security equipment. |
| Equipment Installer | Installs and services security equipment including locks, alarms, biometrics and CCTV. |
| Control Room Operator | Monitors security cameras, access control and alarm systems. |
| Trainer | Trains security skills and competencies. |
| Security advisor | Provides advice on security equipment or security methods and principles, including security risk assessment, audits and vulnerability assessments. |

Table 1

The reality is that growth in the security market has occurred due to long-term societal and institutional changes. These changes started in the mid-1980s, were felt significantly in the 1990s, and have continued today. The September 2001 US attacks and general fear of crime have contributed to this growth, but have not been the prime causes of it.

Proof that the trend predates 2001 can best be seen by the number of security licences issued in Victoria over the last 15 years. Between 1992 and 2000, the number of security licences increased by about 14% per year. Between 2000 and 2006 the number increased by about 20%.

So what is behind the changes?

Below is a list of the major factors which have driven growth in the security market:

1. A desire by governments to reduce the public provision of services which can be delivered by the private sector. Both Labor and Coalition governments have pursued this for a mixture of ideological, financial and pragmatic reasons. Ideological because the private sector is believed to be intrinsically more efficient than the public sector; financial because outsourcing offers a way to reduce costs; and pragmatic because it allows union power to be reduced and offers an arrangement for plausible deniability (where the government can shift blame for any failures to a contracted party, such as with detention centres).
2. Public and corporate disillusionment with traditional policing. This disillusionment has arisen from the perceived inability of police to prevent crime and provide what the victim considers an appropriate response, and also from a lack of nuanced services.
3. Recognition by more sophisticated organisations that a holistic approach to security (which includes risk management, protection and continuity) is a sound business measure and delivers a return on investment.
4. The transfer of tasks that are not considered core from police to the private sector.
5. Increasing acceptance of the legitimacy of private security, and a growing understanding of the benefits that it offers such as flexibility, discretion, revenue protection, and savings.
6. Growing wealth and portability of assets,

meaning there are more targets of crime of a higher value, which require more protection. Increased protection has also been driven by the need to compensate for the reduction in natural surveillance of business premises due to the growing separation of commercial, industrial and residential areas.

7. General increase in the fear of crime.
8. A belief by clients that they can reduce their exposure to litigation by hiring security service providers, hoping that aggrieved parties will sue the security provider and not the client.

These underlying trends will almost certainly continue into the foreseeable future, ensuring that growth continues in the 6-8% band.

Overlaying this market-wide trend is a series of market segment trends. These need to be considered when predicting growth in the segment you work in. The trends are:

1. Policing trends
2. Client dissatisfaction
3. Regulation reform
4. Informed clients
5. Segments which are responsive to incidents
6. Convergence

Market segment trends

1 Policing trends

One of the greatest indicators of the private security sector's future is the trends in Australian law enforcement. Many of these have a direct impact on both the work opportunities and the culture/skills of the security sector's staff, and also on the types of products and services demanded by clients.

The five main law enforcement trends which will influence the shape of the market are:

1. Continued reduction in non-core law prevention and enforcement functions
2. A move towards reassurance policing
3. Continued efforts in implementing intelligence-led policing
4. Continued focus on measurable outputs to manage performance
5. Renewed attempts at police-private security partnerships

Continued reduction in non-core law prevention and enforcement functions

Over the last few decades, police services have picked up many non-law enforcement tasks because it is one of the few government services which operates 24 hours a day and has a deployable workforce. Increasingly, this is being reversed, with tasks which do not require expensively trained police and which could be done more cost effectively by the private sector being outsourced.

These include:

- the issuing of non-police warrants
- the provision of wide load escorts
- driver's licence tests
- photographs for insurance and other purposes
- transportation of prisoners
- the issuing of gaming and betting permits
- security escort duties
- vetting of liquor and firearms licences
- acting as clerk of court
- security to government premises.

Opportunities exist for private sector providers to capitalize on this trend by influencing the decision making process to speed up the outsourcing and position themselves as the organisation best able to deliver it.

Move towards reassurance policing

Police services have shifted resources to community policing and raising their public presence as a response to the public's increased anxiety about crime and the perceived failure to prevent crime. Their aim is to increase the satisfaction with the police and improve the public perception of safety.

These measures recognise that public reassurance is as legitimate a role for the police as solving crime. This is because feelings of safety are key to increasing people's well-being which is important for both politicians and for the economy. People who consider that they, their family and their property are safer are more likely to vote for the incumbent and push up consumer confidence, meaning they spend more on general goods and services.

The implication for private sector providers is that security must not only prevent crime but also reassure the client, their staff and customers. Providers which can structure their services to generate the additional

benefits of generating revenue will be very attractive. An example of this change is transit security. While armed guards on trains may demonstrate to the travelling public that a forceful response is available, it is not particularly reassuring to see that weapons may be required. If ticket inspectors are instead deployed, they provide reassurance that assistance is available, plus they increase revenue by reducing the number of travellers who are willing to take the risk of travelling without a ticket.

Continued efforts in implementing intelligence-led policing

Intelligence-led policing has been a priority in all police services since the late-1990s. The aim is to integrate intelligence and investigation information, and then use this intelligence to target daily, strategic, and, importantly, tactical police efforts. The practical outcomes of intelligence-led policing, as identified by the UK National Criminal Intelligence Service, are:

- targeting offenders (especially the targeting of active criminals through overt and covert means)
- the management of crime and disorder hotspots
- the investigation of linked series of crimes and incidents
- the application of preventative measures, including working with local partnerships to reduce crime and disorder.

While there have been some notable successes of intelligence-led policing, it has had some problems in achieving its potential for three reasons.

Firstly, all staff need to see themselves as intelligence gatherers and provide that information easily in a way that can be analysed. Secondly, it requires an analysis and production capability which is resourced and sustained, and that is not simple or inexpensive. Thirdly, it requires that operational commanders understand the significance and limitations of the intelligence gathered and use it appropriately in their decision making.

Intelligence-led security services offer opportunities for the private sector. However, there are limitations. Intelligence-led security depends on information access, and the ability to fuse information from open source intelligence providers and police sources. It also requires an educated client who uses the

information appropriately, meaning it is risk-based. It requires the client to be able to rapidly respond to new information and be able to tolerate some intelligence-led failures.

The greatest impediment to organisations selling intelligence-led services is the inability to sell the intelligence to the client.

Continued focus on measurable outputs to manage performance

Police services will continue their focus on performance management by measuring outcomes such as response times to incidents. This is despite the fact that many of the outcome measures may not stand up to scrutiny. For example, research reveals that improving response times to calls for service does not reduce crime.

The rationales for measuring performance are both the simplistic adage that "if it can't be measured, it can't be improved", and the need to have some figures to demonstrate to the public the value of the police, mostly for political purposes.

Measuring activities (rather than outcomes) is common practice in the private sector. Some are done to check that the service has been delivered, such as recording the time that a patrol visited a premise. However the best use of measurement is to demonstrate the value of the work and why more money should be spent on it. An example of this is anti-fraud work. In the case of investigation into vehicle theft, accidents, arson and welfare fraud, measurements show that concrete results are obtained in 70 to 90% of investigations such as the recovery of assets, dropping of insurance claims and convictions. Further measurement reveals that for every \$1 spent on an investigation, it recovers about \$3 to \$6. With such evidence, it is easy for security providers to demonstrate their value.

Given the increasing focus on measurable outcomes, security providers will do better if they can provide sound and independent evidence of the cost-benefits of their solutions, and will continue to grow if they can demonstrate the savings their work generates.

Renewed attempts at police-private security partnerships

Since 2001, there has been a renewed interest in police-private security partnerships. The benefits of

making the private sector a partner in crime-prevention are not new. Various attempts have been tried in the past with limited success. For example, in the ACT there were regular information exchanges between the private sector and the police, organised by the police security liaison committee, but these lapsed around 2001.

Currently, most jurisdictions are pursuing partnerships based on the UK Project Griffin approach. Project Griffin brings together local police and building security guards to help protect the so-called 'Ring of Steel' within the City of London. Components of the project include:

- a one day course for private security staff covering bomb recognition, action at a scene, cordon powers and terrorist reconnaissance
- deployment of staff with high-visibility fluorescent tabards to assist in cordon control and anti-terrorist initiatives such as exterior patrols
- a telephone conference call every Friday providing intelligence on terrorism and local crime issues.

Several Australian States are implementing variations on this scheme. The benefits of being involved for the private security sector include:

- Gaining information from law enforcement regarding threats and crime trends
- Involvement in exercises and planning what aids response and recovery to incidents
- Developing personal relationships
- Boosting law enforcement's respect for the security field
- Increasing training opportunities
- Increasing staff retention as working on partnership activities is attractive
- Attractiveness for clients of having strong links with the police services

While there is significant potential for police-private security partnerships, it is important to note there are significant impediments to making them work. Organisations which intend to target the opportunity need to understand why many past partnerships have floundered. The main reason has been a lack of information sharing due to mistrust and misinformation.

The police may be unable to share information due to security classification, or may be unwilling to for fear

the information may be misused. The private sector may not want to share information because its release may hurt profitability.

Mistrust often arises because each group views the other as having separate goals and as competition. Finally, misunderstandings can arise as neither side has a good understanding of what the other does in reality, or what the other side is capable of doing.

2 Client dissatisfaction

Complaints from clients about the quality of security staff, products and services are not new. Commonly heard criticisms are that staff are under-trained and under-motivated box shifters who are not client or outcomes focused. Post-September 2001, a new complaint has been heard that the private security sector does not have the surge capacity to meet the need of clients if the nation moves to a heightened national security alert level.

These problems have been exacerbated by the clients themselves. For example, they sack their internal, usually well-trained, security staff and hire cheaper, usually less well trained staff, and then complain about the quality of the cheaper staff. When presented with a higher trained and more expensive workforce and a lower-trained and less expensive workforce, clients are often reluctant to pay for the former. In addition, many clients do not have the ability to judge value for money when presented with options and therefore simply choose the lowest cost. Finally, they fail to plan effectively and assume that their requirements will be met upon demand. An example of this was the shortage of security guards at the Commonwealth Games. This was predictable given a confluence of the following factors - lack of engagement of security providers in the planning of the event, the introduction of new training requirements for licence holders, and the ability for security staff to leave their work for higher paying catering work at the Games.

In some segments of the market, clients will pay for better quality of security staff, products and services. These include those organisations which are in the public eye and are an identifiable terrorist target, for example icon buildings and national stadiums. Generally, these organisations employ high quality security professionals who can argue internally for suppliers which offer best value rather than lowest price. They are also more likely to be innovators and

leading-edge customers who will have mixed in-house and contract security workforces, pooled training of staff from a range of like-minded businesses, and integrated security, emergency service and building management systems.

As the number of better educated organisations which seek superior security staff, products and services grow, so too do the opportunities for private sector providers who have got superior offerings. Identifying the needs of these high-value clients will be easy. Building confidence that your organisation can actually deliver what you claim will be much harder with these often sceptical security buyers.

3 Regulation reform

The last few years have seen some significant regulatory reform of the security sector. Further reform is inevitable because the existing regulations are generally inadequate, ineffective and piecemeal.

There are many reasons for this including a focus on merely a segment of the security industry, political knee-jerk reactions to high profile security failings, and the inability of security associations to reach a unified position and lobby effectively for more comprehensive regulation.

While the national review of security industry training, competency, accreditation, registration and standardization will address many existing problems, it is bound to fail to address others. For example, it will probably not address the disconnection between having a security advisor's license and having competence in the area of advice, or the need to license public sector security professionals.

If applied across the board, regulatory models like licensing boards and co-regulation will fail to address the problems of restricting entry to competent individuals and organisations.

The consequence of this will affect the future of a number of market segments as it continues to allow low quality operators to enter and operate in the market. For some segments, such as crowd control, it will decrease the attractiveness of working in this market segment because of increased training and licensing costs. However for most, regulatory reform will have marginal impact.

4 Informed clients

One of the key reasons many security projects do not meet expectations is the client does not have appropriate skills and education resulting in a failure to effectively specify their needs, evaluate the options, manage contracts and monitor implementation.

The challenges to becoming an informed client are increasing as technology rapidly evolves. For example, selecting cameras is not a straightforward exercise. Standard, thermal and infra-red cameras all offer quite different benefits and costs. Determining the applicability and limitations of each, and then selecting the correct mix, requires considerable knowledge and experience.

Over time, the challenges for a client to stay on top of their subjects will only increase due to the integration in security management of both different technologies (eg electronic and physical) and disciplines (eg risk and continuity).

The solution for many organisations is to hire former police, military or industry professionals. Each profession has particular strengths, but deep and wide security professionals who use their professional judgment and can access information and other skills are required.

The relative lack of knowledge of clients means there are increasing opportunities to provide expertise and assistance to enable them to make informed choices including technical evaluation of vendor options, security contract management and training.

5 Segments which are responsive to incidents

There are a number of segments of the security market which are highly responsive to security incidents. An example of one is the counter-terrorism market. When a new terrorist incident occurs overseas, governments and, to a far lesser degree, businesses increase their spending to counter the threat. This phenomenon was seen after the Jakarta embassy attack, the 2001 World Trade Centre attacks and the Madrid and London rail bombings.

Some incidents result in expenditure across all sectors and an example of this is CCTV. Following the 2005 London bombing, the Australian Government

developed the National Approach to Closed Circuit Television and many organisations are now rolling out large numbers of CCTVs.

Other segments also increase their expenditure after incidents. For example, since the loss of electronic data by US CitiGroup when information tapes on 3.9 million customers were lost in transit, a number of Australian organisations have spent more on data protection and secure transportation.

The implication of segment responsiveness is that opportunities will quickly arise if incidents occur. For example, if there was a dirty bomb or chemical weapon detonated in an urban area anywhere in the world, there would be a huge demand for radiological sensors and enhanced building filtration systems. Organisations should attempt to predict the impact on their market if different types of attacks materialise.

6 Convergence

Convergence is occurring in both technological and knowledge domains of security practitioners.

In the areas of technology, there is increased convergence of electronic, information and physical security. They are all becoming integrated, as this offers superior outcomes at a lower cost. Systems are being deployed today that blend a range of previously stand-alone technologies such as biometrics, access cards, chemical sensors, intrusion detection and alarm systems. Also, security systems are merging with building management systems like fire detection and environmental control. The commercialisation and plug-and-play nature of many devices means that supply competition will increase, driving down margins. The integration market, particularly with legacy electronic elements, means that the low-volume, high margin and high risk market will also grow.

Another consequence of the improved capability of electronic security technology will be the displacement of personnel with technology in instances such as control room monitoring. Conversely, this reduction in security visibility will mean there will be increased demand for reassurance security, particularly if it can protect or generate revenue.

A significant new market will be home automation and, most likely, this will be centralised around a

security system's central processors. Obviously, video surveillance, video analytics software and identity security will continue to grow.

Convergence of knowledge domains which are required to be mastered by security practitioners is also occurring. Increasingly, practitioners need to be able to integrate a range of separate disciplines into a total security solution that involves managing assets, personnel and information risks, providing a first response to emergencies before the emergency services arrive to take control, and restoring functions as quickly as possible following an incident.

This means there will be a growing demand for organisations and people which can bring the once disparate disciplines of risk management, business continuity, information security and corporate emergency response together.

Conclusion

There are many other trends that are going to shape Australia's private security sector. These include the ageing of the population, the raft of industry standards under development and the influx of non-English speaking staff, returned soldiers and retired national security public servants into the security market.

To plan for the future, security providers and professionals need to identify all the trends affecting their markets and either capitalise on them or shift to more profitable segments.

While growth of the security sector is assured, don't be lulled into believing that yours is too.

*A version of this article was published in the January 2007 edition of the *Security Solutions* magazine.*

Security Professionals' Congress 2007

Shaping the future of the security profession

9 & 10 May 2007
Grand Hyatt, Melbourne



KEY FOCUS

- Changing role of security in organisations
- Career paths, expectations and rewards
- Educational and competency market needs
- Security as a profit generator
- Merging security and other business functions including business continuity and emergency management
- Best practice for public and private security – are they different?
- Security professional – specialist or generalist?

Special Offer – Until 15 April 2007

All two-day registrations before 15 April 2007 will receive a complimentary edition of the newly published *Security Risk Management Body of Knowledge*, valued at \$385 RRP.

See page 6 for details



This project is supported by the Australian Government Department of the Prime Minister and Cabinet.



www.securityprofessionals.org.au