



## Future of the Australian Security Profession

This National Security Briefing Note analyses the future of the Security Profession

### Why the need to rebuild the industry

Australia's security sector can best be described as marginal. It is marginally profitable, marginally meeting customer needs, and marginally attractive to employees.

This situation is not new and the problems are well known. So why has the sector been marginal for so long?

Part of the answer to this is that because there is no consensus on where the sector should be, reform initiatives have petered out.

This Note presents a roadmap for reform of one key element of the security sector which will have flow on benefits for the entire sector. It is based on the assumption that the sector's aim should be to become a profession which is valued by clients, the public, and the security workforce. An essential requirement for this to occur is that it becomes more profitable which will allow more funds to be invested in raising the skills and capability of the sector.

### The myriad problems facing the security sector

The first stage in rebuilding the security sector is to identify the problems. This then allows solutions to be developed that maximise the gains for all stakeholders, while developing compensation mechanisms for those that may lose out from the reforms.

Athol Yates is the Executive Director of the Australian Homeland Security Research Centre. While he was a member of the Interim Security Professionals' Taskforce, his views in this article are his own. For information on the Security Professionals' Taskforce, see [www.securityprofessionals.org.au](http://www.securityprofessionals.org.au).

Below is a breakdown of problems by stakeholder groups.

#### *Security business owners and investors*

The key problem facing security business owners and investors is the sector's financial viability. Profitability for some segments of the sector is below average industry levels. For instance, the security manpower segment has a profitability of about 5-10%; security consulting has about 10-15%. The average Australian industry profitability for business services is 20%.

The low profitability has several problems. The first is that the low rate of return means that it is difficult to invest in the business, resulting in less investment for new equipment, training and innovation. The second is that low profit means that there is no potential to pay higher wages. Thirdly, there is continual pressure to reduce costs. If the pressure gets too severe, some businesses may sacrifice their long-term viability by cutting staff training, not meeting licensing requirements, and failing to meet the client's contracted requirements.

A fourth problem with low profitability is that high cash flow is essential to remaining afloat. This need for cash can result in businesses seeking work that offers no profit, only cash flow.

Profitability pressures also occur due to the ease with which new companies can enter the security sector. Establishing a security business does not require significant capital or face difficult licensing requirements. For example, a one-man company providing security risk assessment can do this out of their home, or a patrol security business can work out of their cars.

Micro businesses in particular can underbid more established businesses as they do not have the overheads of administration, staff training and marketing costs.

### *Clients*

The problems from the client's perspective relates to the very nature of security. Security aims to deter, detect, delay, respond and attribute any potential or actual breach. If it does this successfully, no security breach or crime occurs. Thus the benefits of security can be invisible, and the costs are the only thing noticed by clients. If the value of security is not advanced, clients naturally question the need for security and seek to minimise its costs.

Thus, a key problem for clients is the perception that the costs of security outweigh their benefits. The cause of this is principally that the security return on investment is not sold effectively to the client. Examples of ways to better sell the value of security is to collect statistics on security incidents and bring them to the attention of management, and quantify the cost of security incidents on business operations and provide them to the client's finance group.

Another problem is that the security task does not meet the client's requirements. This can be because the original scope of work was inadequate, or due to the failure of security staff to integrate and balance non-security issues into their decisions. Another cause may be the inability of clients to judge value for money. For clients with little knowledge of security, it may be difficult to judge competitive service offerings, particularly if it requires professional judgment rather than comparing simple metrics such as hours of work and page lengths.

Whatever the cause of this problem, the result is dissatisfaction with the security activities.

### *Community*

The community's concerns with the security sector are a product of their personnel experience and media coverage of the security sector. Personal experience of security is normally limited to passing through security screening at airports or clubs, and viewing security personnel at work around town. A deeper understanding of the work of the security sector would occur if they were involved in actual incidents. However as very few people are ever involved in incidents, their knowledge of security incidents inevitably comes from the media. As media coverage is mostly negative in nature, the only coverage of security incidents depicts security failures. Consequently, these rare failures, such as



#### **About the AHSRC**

The Australian Homeland Security Research Centre undertakes independent, evidence-based analysis of homeland security (the domestic dimensions of national security).

The Centre's vision is to be one of Australia's leading independent sources of research on domestic security policy and programs for the government, industry, the community and the media.

Many of the Centre's activities are run in partnership with other organisations which reflects its philosophy that collaboration is the key to ensuring optimal outcomes in national security.

The Centre is not aligned with any political party or funded by government grant. The Centre is fully self-supporting and is funded by its commissioned studies, events and sales of publications.

the David Hooks death and the involvement of outlaw motor cycle gang involvement in security, become the accepted narrative of the security industry.

Governments and police

Governments and police problems with the security industry come as a response to public concerns of the security industry. This is illustrated in how the government responded to the public outrage over the death of David Hooks.

Without the stimulus of public outcry, reforms of the security industry would follow the path of other industries. That is, it would slowly evolve as various public policy macro-trends are applied to it. For instance, the reforms to harmonise security licensing arises out of the macro-trend of national competition policy set in train over 15 years ago.

A small sub-group of government and police, just like the rest of the community, also have problems with the existence of the private security sector. This is ideological in nature as it considers that security should be a function of the state because it involves the application of sanctioned violence. A much smaller group has problems with the security industry as it is perceived to reduce employment for its members.

### *Employees*

The problems for security industry workers are no different in principle from employees in other sector. All employees are seeking individual job satisfaction based on a range of factors including the level of pay and benefits, the perceived fairness of the promotion

system within a company, the quality of the working conditions, leadership and social relationships, and the job itself. The key job satisfaction factors relating to the job are the variety of tasks involved, the interest and challenge the job generates, and the clarity of the job description and requirements.

While some aspects of job satisfaction can be influenced by the employer, such as variety of work and recognition within the company, much of it is outside their control.

In the security sector, particular problems that employees have include the public's lack of respect and belief in the importance of the work, limited career advancement opportunities and lack of portability of skills between States.

### How could the security sector be rebuilt

Rebuilding the security sector cannot be done according to one master plan. The security sector is too large and diverse to allow central planning. There are simply too many legacy issues, different drivers, different regulators, and vested interests, to develop an effective whole-of-sector plan.

The impracticality of a whole-of-sector plan is revealed if one considers that every item in the list of essential activities below needs to be addressed for all segments of the security industry. This is a list of activities required for major change management activities.

- A compelling need for change.
- A well-communicated, shared understanding of this need for change.
- Acceptance that any change management plan will only succeed if the following stages are undertaken:
  - o Adequate resources given for the change.
  - o Open and consistent communication with all stakeholders.
  - o Participation and support by all stakeholders.
  - o Visible and continuous executive sponsorship.
  - o Being in touch with those affected by the change.
  - o Structured approach to managing change.
  - o Recognising employees as key contributors to the change initiative.
  - o Training to prepare team members.

Rather than striving to reform the entire sector, it would be more effective to focus on one segment of it. That segment should be the security professionals segment.

If the security continuum is considered as having personnel who work in the tactical, operational and strategic sectors, then security professionals predominantly relates to those working at the senior end of the operational sector and those in the strategic sector. As an illustration of the security continuum, Figure 1 details job descriptions in the continuum for physical security.

Security professionals are quite distinct from security professionalism that encapsulates the professional delivery of a security product or service. The term security professional in no way implies that security professionalism is limited to security professionals.

A key characteristic of security professionals is that they are required to take responsibility for security projects and programs in the most far-reaching sense. They provide significant input into the shaping of security decisions and the environment in which the security system functions.

This requires that they:

- understand the requirements of clients and of society as a whole;
- work to optimise social, environmental and economic outcomes over the lifetime of the product or program;
- interact effectively with the other disciplines, professions and people involved;
- ensure that the security contribution is properly integrated into the totality of the undertaking.

The work of security professionals is predominantly intellectual in nature. Security professionals have a particular responsibility for ensuring that all aspects of their work are soundly based in theory and established practice. One hallmark of a security professional is the capacity to break new ground in an informed and responsible way.

Security professionals may lead or manage teams appropriate to these activities, and may establish their own companies or move into senior management roles in security and related enterprises.

### Why focus on security professionals

Building security professionals into a recognised and strong segment of the security sector will generate huge benefits to the security professionals themselves and to other segments of the security sector. This is because the gains obtained for security professionals will flow on to the other sectors. This will occur via two mechanisms. Firstly the other segments will see their gains and be motivated to reform themselves. Secondly, security professionals will recognise that to maintain their gains, the rest of the security industry must not undermine them. Consequently security professionals will push the other segments to reform, which will include providing education articulation, pathways for career advancement and removal of disreputable businesses.

Another reason to focus on the security professionals segment of the security industry is because it will be relatively easy to do so due to type of people who work in it. Security professionals are educated, articulate, used to working collaboratively, and already have worked on professional volunteer activities. These characteristics mean that they can effectively organise and advocate easily. The organisation of reform in this area is also made easier due to the absence of existing vested interest in the segment and the lack of interest in capturing financial gain. The latter issue is significant as building security professionals into a strong segment has little to do with financial reward. It is mostly motivated by the need to improve security professionals' status, competence and job satisfaction. With these factors, change is much more likely than in other segments of the security sector.

### The new industry in 20 years' time

The security industry in 2028 will be markedly different from today. The most important change will be that security will be seen as a profession. It will have the same professional standing as those working in the building and construction, health and legal sectors.

The security profession will have the following characteristics:

- Distinct body of knowledge
- Agreed and enforced standards of behaviour/ethics
- Standards of education
- Formal requirement for professional development
- College of peers to judge standards

It will also have more formalised segments with groupings around security specialisations and security management and leadership, and levels within segments. It will also have pathways between segments and levels. These will align with the Australian Qualifications Framework (AQF) providing education and career paths. See figure 2.

### The reform agenda for security professionals

The initiating point of the reform agenda was the first Security Professionals' Congress held in Melbourne in May 2007. The Congress was attended by approximately 150 delegates representing all aspects of the security profession including in-house security managers (from the public and private sectors), consultants, ITC specialists, physical security consultants, security engineers, procedural specialists, facility managers, risk managers, emergency managers, business continuity consultants, academics and educationalists.

Organisations participating in the Congress were:

- ASIS International – ACT, Victoria, NSW & New Zealand Chapters
- Australian Homeland Security Research Centre
- Australian Information Security Association
- Australian Institute of Professional Intelligence Officers
- Engineers Australia
- Information Systems Security Australia
- Institute of Security Executives
- International Association of Bomb Technicians and Investigators – Australian Chapter
- Risk Management Institution of Australia
- SECIA
- Victorian Security Institute

Other groups were invited but declined to participate for a host of reasons including availability.

Three common themes emerged from the Congress which would improve the security profession. They were:

- The requirement to formalise qualifications, certifications and professional recognition.
- The need to alter the perception of the security profession.
- The need to establish a group representing the security profession.

On the day prior to the Congress, there was a meeting of professional associations representing security professionals. Representatives of twelve associations attended from Australian-based and international organisations, and there were also representatives from New Zealand.

The key topic of the professional associations' meeting was the ability to work together to promote the security profession. It was recognised that no one body represents the needs of all security professionals or speaks on behalf of the broader profession.

The Australian Homeland Security Research Centre (AHSRC) organised, coordinated and hosted the Congress and the meeting of associations in May. It paid for the accommodation of key representatives of the security professionals to engage them in the activity. Don Williams CPP coordinated the Congress program and facilitated the Congress.

Following the Congress, the Interim Security Professionals' Taskforce was formed. Its objectives were to initiate the reform process. The people on the taskforce were there as knowledgeable individuals and not as representatives of particular organisations. Taskforce members are:

Don Williams  
Brett McCall  
Julian Talbot  
Michael Kinniburgh  
Peter Anderson  
Jason Brown  
Paul Murphy  
Bruce Howard  
Athol Yates  
Brian Kelly  
Steve Barlow  
Richard Clarke  
Peter Wythes

The work of the Interim Security Professionals' Taskforce is supported by the Australian Government Attorney-General's Department.

On 4 March 2008, the Taskforce released a discussion paper on the options for security professionals entitled *Advancing Security Professionals*.

The purpose of this paper is to generate discussion on the following major questions facing the security professionals. Specific questions asked in the paper are:

- How are security professionals defined?
- What are the key standards for professional practice?
- How can the status and recognition of security professionals be improved?
- What should be the minimum standards, qualifications and continuing professional development requirements for security professionals and their specialisations?
- What is an appropriate regulation/registration/licensing/accreditation system?
- What are the best ways to enhance accountability for the work of security professionals?
- How can the voice of security professionals be best represented to government, industry, professional associations, the community and the media?

Consultative forums on the discussion paper will be held around Australia in April 2008.

### Key issues in the discussion paper

Below are the key issues in the discussion paper.

#### *The need for standards for professional practice*

Professional practice standards are those standards which security professionals need to comply with in order to uphold the public interest; to ensure the integrity of the work for which they are responsible, and to discharge their professional obligations.

Standards cover professional knowledge, practice and engagement. The standards should all contribute to the following objectives:

- Independence and objectivity
- Confidentiality
- Proficiency
- Due professional care
- Maintaining up-to-date expertise
- Continual improvement
- Ethical behaviour
- Responsibility to society and the environment
- Responsibility to the client or employer

From a client's perspective, the reasons that standards, competence and continuing professional development requirements are important are because

they provide protection from poor service and goods, and provide guidance on the quality of professionals.

Some specialisations of security professionals already have many of the required standards, but others have none.

Thus the consultation process needs to identify the existing standards and gaps where standards need to be developed.

### *Improving the status and recognition of security professionals*

As a group, professionals enjoy a high social status, regard and esteem conferred upon them by society. This status is not an inherent right, but is granted by society. It arises primarily from:

- Higher social function of their work, regarded as vital to society as a whole and thus having a special and valuable nature.
- Existence of technical, specialised and highly-skilled work often referred to as professional expertise.
- Training involving obtaining specialist education and qualifications.
- Entry to the profession based on competence.
- Training requiring regular updating of skills.

For professionals, maintenance of public status depends on the public's belief that professionals are trustworthy and provide the level of expertise expected of them.

While there is no consensus on how to raise the status of professionals, there appear to be two distinct groups of thought. The first is that a series of actions can raise the status of a profession. The second is that no overt action can be effective in raising the status of a profession. Increases in status will occur naturally if the professional produces unique and valued high-quality work, and makes a significant contribution to society.

If action is believed to be effective in raising the status and recognition of a profession, below are most important actions that the security profession could take:

- An increase in positive media coverage of security professionals
- The introduction of awards for security professionals

- An increase in remuneration
- Security professionals featuring in media programs, notably news broadcasts and documentaries
- Representation of the concerns of security professionals to politicians
- Security professionals giving talks to non-security groups
- Security professionals informing other professional groups (e.g. engineers and project managers) of the work of security professionals
- An increase in entry standards for security professionals
- An increase in the inter-personal skills of security professionals so that they can better communicate in the workplace, industry and to the community
- Legal protection of term security professional
- The introduction of specific licensing requirement for security professionals
- Promoting a security professional post nominal
- The creation of a representative voice for security professionals
- Inviting non-security practitioners to meetings of security professionals

Thus the consultation process needs to decide if a program of action would raise the status, trust and recognition of security professionals, and if so, what actions would be most effective.

### *An appropriate regulation/registration/licensing/accreditation system for security professionals*

The regulation/registration/licensing/accreditation systems vary across State and Territory jurisdictions and elements of the security industry.

The system for certain elements of the security industry is well-developed and targeted in areas such as crowd controllers and installers.

However, for security professionals, the systems are mostly irrelevant as they either do not apply to groups of security professionals, or they provide no indication of competence (or other public good benefit).

Examples of the former are that the systems do not apply to information security consultants and government security advisors. Examples of the latter are that the systems provide no indication of competence when selecting professionals in security facility design and blast design.

Thus the consultation process needs to decide if a national system should be developed for security professionals or, alternatively, should specialisations of security professionals fall under existing schemes run by various groups.

### *Enhancing accountability of the work of security professionals*

Currently, clients find it difficult to determine the standards that security professionals would be measured against. This is due to the lack of knowledge, practice and engagement standards and appropriate licensing systems.

The licensing regimes for consultants in some jurisdictions set standards for qualifications (usually a Cert IV) and for registration as a business, insurance coverage, etc, but these do not directly reflect standards for ethical or professional behaviour of security professionals.

Most of the security-related industry or professional organisations have codes of conduct. A common concern is that disciplining members for breaches of codes of conduct is done infrequently by the organisations as it results in members resigning before disciplinary action is finished. Enforcement also results in lost membership fees for the organisation.

Some contracts require minimum levels of Professional Indemnity (PI) insurance but the relevance of the insurance cover to the work undertaken is not often verified. PI coverage should reflect that the applicant has demonstrated to the insurance provider that they are an acceptable risk in terms of qualifications, experience and business practices for the work that they undertake. Requiring participants to demonstrate PI coverage for the work undertaken would help make them more accountable.

The consultation process needs to examine the available mechanisms to hold security professionals accountable, and if these are deemed inadequate, identify how they can be improved.

### *Advancing the views of security professionals to government, industry, professional associations, the community and the media*

One success factor essential to driving change in any industry is the need for a strong voice. However, there

are numerous voices representing elements of the security continuum.

For example, ASIAL, the Institute of Security Executives and the Victorian Security Institute represent elements of the security industry, and ASIS International and Risk Management Institution of Australia represents individual security consultants and managers.

The number of security-related organisations makes it difficult to promote a common agenda. In addition, government policy makers and regulators find it difficult identifying the views of the security profession.

There are six main options for advancing the voice of security professionals to government, industry, professional associations, the community and the media.

Figure 3 is a table identifying these options.

The consultation process needs to examine the strengths and weaknesses of each option and select the preferred model.

## **Conclusion**

Until May 2008, the future direction of security professionals is being argued and debated. All options are open and will be canvassed at the Consultative Forums around Australia. If stakeholders cannot attend them, they can email in their views to [admin@securityprofessionals.org.au](mailto:admin@securityprofessionals.org.au).

The Taskforce will be collating opinions and developing a recommendations paper which will be discussed at the security associations' meeting on 24 May 2008 in Melbourne. Following this, at the 2008 Security Professionals' Congress on 25 and 26 May, the recommendations will be further discussed and the refined recommendations will be endorsed. A Security Professionals' Taskforce will be elected at the Congress to convert the recommendations into reality.

## Future of the Australian Security Profession

	Chief Security Officer	Security Manager	Security Operations Manager	Supervisors	Shift Leaders	Security Staff
	STRATEGY		OPERATIONS		TACTICAL	
	Strategy and Planning		Implementation and Development		Compliance and Operations	
	1 to 3 year	< 12 months	< 3 months	<30 days	1 to 3 shifts	Less than duration of one shift
Activities	Strategic Planning & Sec Mgmt Systems Performance Agreements Stakeholders	Quality Assurance Assessment of systems	Rostering Analysis of activities (Eg: GCS, Supervisor Activity Plans, Compliance with SOP's)	Oversight day to day operations Liaison at local level	Facilitate smooth operation of security activities Security audits Conduct QA checks and remedial training Staff duties as required	Access Control Customer Service Emergency response, disaster recovery, business continuity Troubleshooting Security tasks (patrolling, sysadmin, etc)
Responsibilities	Standard development and implementations	Standard development and implementations	Ensure consistency of operations across all sites and all shifts	Ensure security staff work to Standards & SOP's Monitor maintenance and administrative activities Implement and report on Group plans	Leadership of operational units Ensure compliance with standards	Compliance with SOP's Personal discipline and presentation Knowledge of SOP's
Training	Approval & resourcing Training Plan Briefings to Supervisors Delivery of strategic and specialist training	Development and updating Training Plan Maintain Training Register and monitor plan for compliance Monitor Quality of Trg	Coordinate training activities Develop training materials Ensure logistics and competent instructors	Train large groups Develop training material and aids	Train small groups and on one OJT Contribute to development of training program	Participate in training Feedback & Improvement suggestions to trainers Personal training and development at posts and in own time
Interfaces	Division Heads and C-Suite Senior external groups (Government, Senior Law Enforcement Officials, etc) Suppliers & Contractors	Regional external Groups (Regional Police and Government officials and group, etc) Internal middle management	Local external groups (Police, Community groups etc)	Supervisors in other departments and contracting companies Administrative personnel	Day to day follow up of tasks with supervisors and admin personnel from other internal groups	Customers, clients and visitors to site

Figure 1: Job descriptions in the continuum for physical security

## Future of the Australian Security Profession

AQF	Qual	Physical	People	Management	Information	ICT
11	PhD	Technical Specialist or Senior Consultant				
10	Masters Degree	Chief Security Officer (CSO) or Senior Consultant				
9	Graduate Diploma	Chief Security Officer (CSO) or Senior Consultant				
8	Graduate Certificate	Physical Security Consultant	Personnel Security Consultant	Security Risk Management Consultant	Information Specialist	ICT Security Specialist
7	Bachelor Degree	Security Manager	Vetting Manager	Security Manager	Intelligence Manager	ICT Security Manager
6	Advanced Diploma (Certification e.g. CPP)	Operations Manager	Vetting Manager	Security Manager	Intelligence Analyst	
5	Diploma	Agency Security Adviser	Vetting Supervisor	Team Leader	Intelligence Collector	ICT Security Adviser
4	Certificate IV	Installer	Senior Vetting Officer	Supervisor	Intelligence Operative	Security Admin
3	Certificate III	Control Room Operator	Vetting Officer	Team Leader		
2	Certificate II	Guards*				

\* In Victoria Cert III is the entry-level qualification for a security guard.

Figure 2: Alignment between the Australian Qualifications Framework and security workforce segments

## Future of the Australian Security Profession

Option	Explanation
Status quo	Continue with the current situation
Regular, informal meetings of security professionals	Regular informal meetings of professionals could be held to discuss topics of interest and concern; this could be achieved through an annual congress
An association of associations	An association of associations could be formed where security-related professional bodies meet and discuss topics of interest and concern, and develop collegiate responses
Lead association	A lead association could be appointed to represent others; this option, while providing a single point of contact, may suffer from extended discussion over which organisation is best suited to lead
An associated society	<p>An associated society could be created within an existing parent body</p> <p>The associated society would invite individual members and a prerequisite could be membership of an existing security-related professional body</p> <p>An associated society would adopt the codes of conduct, compliance and accountability standards of the parent organisation</p>
A new security professional institute	<p>A new security professional institute could be formed that would require minimum standards for members, possibly including membership of an existing security-related professional body</p> <p>An institute could have sub-groups/colleges for each specialisation representing the specific requirements of each sector</p> <p>An institute could attain standing as a recognised professional body with membership being respected by clients and peers</p>

Figure 3