From board room to situation room
Why corporate security is national security

Anthony Bergin, Donald Williams and Rhys De Wilde

Executive summary

Corporations already protect their assets and functions. Corporate security encompasses those managers who address the preventive ‘likelihood’ and the resilience ‘consequence’ elements of risk management and seek to secure the business from a wide range of hazards, including criminals, issue-motivated groups, terrorism, cyberattacks, environmental events, natural disasters, espionage and supply-chain disruption. However, considering the company’s capabilities as part of our national security capabilities isn’t normally a factor in business planning.

Our approach to national security planning should now include key companies and their supply chains: it’s time to rethink our national security approach in a more complex, dynamic and interconnected world. Our corporate sector is now a key component of our deterrent posture against a range of threats.
 Attacks on the private sector are a feature of what Elisabeth Braw, the director of the Modern Deterrence project at British think tank RUSI, calls *blended aggression*, ranging from economic coercion to cyberattacks and irregular warfare by proxies to undermine trust in the state.

As such attacks are likely to be directed towards private-sector assets, business owners and operators should be recognised as central to this country’s security.

Economic security is an essential element of national security, and it’s business that’s a robust engine room for a strong economy. Corporations are making valiant efforts to protect their assets and capabilities from attacks in the physical and cyber environments and do so for sound commercial reasons, but such attacks aren’t just matters of commercial concern to companies and their shareholders. They have significant potential to weaken national resilience.

Our study has found that a void exists between business and national security agencies when it comes to understanding each other’s capabilities and limitations.

Corporations have great perspective on what’s happening domestically and internationally that may affect their commercial operations. Some of the larger business entities have an in-house analytical capability or subscribe to specialist intelligence and analytical providers.

Most major companies have an operations or crisis centre. Corporations hold considerable data that may be of benefit to governments during and after incidents, but the private sector currently plays a limited role in national crisis exercises.

A phrase that’s gained some use among Australian corporate security professionals when talking about the desire for greater cooperation with the official national security community, is *dare to share*, which refers to security officials being willing to provide information that’s timely and of value in the prevention and mitigation of all risks faced by the nation.

There are some constraints relating to passing certain national security information related to international agreements, perceptions of corporate advantage and potentially foreign ownership, but those restrictions shouldn’t be insurmountable barriers: they don’t affect the intent to share, although they can affect the depth and timeliness of the sensitive information to be shared.

There are already in place some mechanisms, established by both the Australian Government and state governments, to ‘hook up’ with business on issues of national security, but the structures are fragmented between and within government departments and agencies and are often based on sector-specific silos.

Both government and corporate representatives indicated to us that sometimes the other party was intentionally or needlessly holding back essential information (business, in particular, sometimes wrongly believes the government is sitting on an information goldmine that it refuses to share), while expecting too much to be provided from the other party. This indicates a lack of understanding on both sides.

Several corporate security professionals observed to us that there isn’t much scope at the moment to discuss or even know what national security policy or legislation is coming ‘down the pike’.

Those corporations that are closely regulated by government (for example, in aviation, telecommunications, finance and banking) tend to know how to find the relevant security official within government. Companies and sectors not as closely regulated or integrated into the national security community have a difficult time identifying points of contact with the relevant agencies.

A secure and resilient nation can only be ensured through mutual obligation whereby both governments and corporations understand and are committed to developing and maintaining the measures required to safeguard Australia.

Business is generally not seeking financial incentives from government, such as tax breaks, subsidies for corporate back-up plans or special government status, as resilient companies ‘do the right thing’ when it comes to national security.
Business sees far greater value in national security agencies providing realistic and timely security-related information and an understanding of how their business fits within the overall concept of a resilient nation.

A key message of this Strategic Insights paper for national security agencies is that coordinating and cooperating with the private sector on national security may be inconvenient at times, but it’s a lot less inconvenient than being exposed to a range of security threats and challenges unprepared. Today, corporate security is national security.

This report makes 16 recommendations on how to strengthen corporate and government cooperation on national security.

For the Australian Government and national security agencies

1. In drafting national security policy and plans, due consideration should be given, where appropriate, to corporate business continuity planning.

2. A central hub within the Department of Home Affairs should be established to be responsible for ensuring, with corporate sector interaction, information transfer on national security risks and support for industry in understanding emerging security issues. The hub would be a communication forum for the business and government sectors to cooperate on issues related to potential threats and responses.

3. At the operational level, a Chief Security Officer Advisory Group should be established to work with such a hub. The advisory group, convened by the Department of Home Affairs, would consist of a small number of senior security, business continuity and resilience managers, as well as organisations such as the Australian Security Industry Association Limited (ASIAL) and the Forum of Australian Security Executives, which would represent the broader corporate sector.

4. The Industry Consultation on National Security (ICONS) should be reconvened to provide a forum for the Prime Minister and senior ministers to engage with CEOs on national security policy and issues. ICONS should highlight the interconnected dependencies of the corporate sector in maintaining national security and underline issues of mutual obligation when it comes to a safer Australia.

5. State-level joint cyber security centres (JCSCs) should become converged centres for integrating national security interaction between business and government. The JCSCs should be rebadged as joint threat management centres to establish two-way communication, analysis and planning not just on digital and cyber risks but on other security risks, such as foreign interference; activism and politically motivated violence; the security of offshore business activities; and disaster resilience.

6. The Australian Government and state governments should seek to expand the involvement of business in exercises related to all aspects of national security, including counterterrorism, health security, national disasters, military preparedness and cybersecurity. Exercising arrangements with business across those areas is an effective way to strengthen organisations’ security arrangements, including by ensuring that incident response plans, including communications processes, are up to date. The Swiss Security Network nationwide exercise is one model.

7. There should be a secondment program of national security agency personnel into the corporate security and more general risk management environment.

8. Wherever possible, ministers should be involved with business in national security and resilience forums.

For the corporate sector

1. Corporations should understand the costs of insecurity not just to their business but to national security more broadly.

2. Corporations should consider how their business continuity and resilience plans support national security and resilience.

3. CEOs of major corporations should participate in a revitalised ICONS to provide perspectives on what’s required and currently in place to produce a resilient nation.
4. A database of which business organisations to contact for specific capabilities relevant to national security planning should be established.

5. Corporations, which often stress-test themselves, should expand their involvement in official exercises related to all aspects of national security.

6. Major corporations, when selecting for the position of chief security officer, should be aware that the ability to obtain a national security clearance will be of benefit.

For the Australian Government, national security agencies and the corporate sector

1. All sectors should agree that there’s a mutual obligation to produce a secure and resilient nation.

2. Discussions should be held between the national security community and corporations on the essential contribution of corporate support to national security. The discussions should be held at CEO/board level and with senior officers responsible for security, business continuity and resilience; and crisis management.

Setting the scene

Codan is a multinational company that specialises in communications, metal detection and mining technology. It has offices in many overseas countries as well as in Australia. Exports account for 85% of Codan's business, and the total revenue of the company amounted to $169.5 million in 2016.¹

In 2011, Codan's engineers started noticing that faulty metal detectors returned to their offices for repairs had unfamiliar wiring. Codan concluded that its metal detectors had been reverse engineered and that it had experienced industrial espionage.

After spending significant amounts on private investigators, Codan found that 12 separate companies were manufacturing fake metal detectors. The fakes were traced back to Dubai. They were sold on from there to fuel the 'gold rush' in Africa in 2012 and were worth more than $10 million.²

The Australian Security Intelligence Organisation (ASIO) arrived at the Codan office in Adelaide to explain what had happened. On a business trip to China, a Codan executive had signed on to his hotel’s Wi-Fi with a company laptop. Cyber actors were able to insert malware into the computer, which went on to infect the company’s computer system in Australia.

The costs of the hacking were significant. As half of Codan’s revenue was generated from sales of metal detectors, the value shares in the company dropped from $45 million to $9 million in one year.³ Codan staff were laid off.

While ASIO was involved in gathering the intelligence relating to Codan’s losses, it wasn’t involved in the litigation process as the company attempted to pursue legal action.

While the economic costs were significant, the company also had national security assets to defend. Codan sold a portable transistor radio with end-to-end encryption that transmitted messages over long distances. This radio was used by British, Australian and US troops in operational zones.

Attacks on companies such as Codan should matter to us. The case shows how corporate security is now becoming more critical to our national security and the need for business (and not just corporate heavyweights) and government to cooperate when it comes to protecting our security.

Partly that’s because our businesses are much more globally focused than ever before, and partly it’s because our nation’s reliance on technology is unprecedented and continues to deepen.
Our infrastructure is becoming increasingly interconnected, creating new vulnerabilities. The threats we face are no longer directed just at our military forces, but also at companies such as Codan. The nature of warfare is changing, and we need a broader understanding of national security.

Technology is now central to strategic and economic power. Power struggles over commercial goals are now not just about corporate success or failure but are also setting the stage for kinds of foreign interference that weren’t possible before.

Our security agencies and businesses must work together to craft a common national security approach. That’s because in non-traditional warfare, or what the Australian Chief of the Defence Force General Angus Campbell calls ‘political warfare’ (which is below the threshold of direct military aggression), our corporate sector is now as much a target as our military forces.

Corporations already protect their assets and functions. Corporate security encompasses those managers who address the preventive ‘likelihood’ and the resilience ‘consequence’ elements of risk management and seek to secure the business from a wide range of hazards, including criminals, issue-motivated groups, terrorism, cyberattacks, environmental events, natural disasters, espionage and supply-chain disruption. However, considering the company’s capabilities as part of our national security capabilities isn’t normally a factor in business planning.

Our approach to national security planning should now include key companies and their supply chains: it’s time to rethink our national security approach in a more complex, dynamic and interconnected world. Our corporate sector is now a key component of our deterrent posture against a range of threats.

Blended aggression: it’s war, but not as we know it

Attacks on the private sector are a feature of the kind of non-traditional or hybrid warfare (sometimes called ‘grey-zone’ warfare) that’s being waged against Western societies by some governments.

Those forms of warfare are what Elisabeth Braw, the director of the Modern Deterrence project at British think tank RUSI, calls blended aggression, which includes economic coercion, cyberattacks and irregular warfare by proxies designed to undermine trust in the state. Adversaries can exert influence by cultivating connections with our business leaders by offering them commercial opportunities and thereby establishing a network of local affiliates with an interest in undertaking advocacy on an external power’s behalf. Foreign influence activities may be covert, coercive or corrupt.

Blended aggression attacks are likely to be directed towards business owners, business operators and private-sector assets that should be recognised as central to this country’s security.

This applies in particular to the digital domain (see box). The increasing interconnectedness of systems creates new capabilities and vulnerabilities for the corporate sector and its ability to deliver products and services, and the vulnerabilities will increase as more systems and devices become internet-connected. The digital domain enables states, criminals and issue-motivated groups to access and compromise personal, financial and intellectual property and data.
Cyberattacks on business

Cyberattacks by commercially motivated cybercriminals (who may also act on behalf of a government), state actors or businesses seeking competitive advantages are now occurring so regularly that cyber risks can affect the ability of a business to operate.

The economic cost of material breaches can be extremely damaging, so there’s a strong incentive for companies not to reveal when information is stolen.

Managing cybersecurity threats remains a major weakness in Australian organisations. According to the latest MinterEllison annual Perspectives on cyber risk report, only 45% of companies said that they regularly tested their data-breach response plan.9

The success rate of malicious cyber intrusions that aren’t technologically sophisticated demonstrates that the controls don’t match the threat: 60% of the 964 data breach notifications under the Notifiable Data Breach Scheme received from April 2018 to March 2019 were malicious.

Our major companies, as well as small and medium-sized enterprises (SMEs), will need to get more involved in government-led crisis management cyber exercises. Such exercises are run, but there are problems with funding, encouraging business to be involved and the role and capability of state governments.

A competitive private sector will drive better cyber protection. There are now industry-driven collective initiatives. Last year, for example, 34 global technology and security companies signed the Cybersecurity Tech Accord to advance online security and resiliency around the world. It’s an important step that already has broad support from many of the tech sector’s leaders and cybersecurity firms.10

Another example of an industry initiative is the Cyber Threat Alliance, which is a group of cybersecurity practitioners who work together to share threat information and improve global defences against advanced cyber adversaries.11

It’s tempting for government to just rely on the cybersecurity systems that companies already have in place, but attacks on business and exploitations of cyber weaknesses greatly affect national security. This is particularly the case after the privatisation of Australia’s essential services over the past 40 years.

In relation to counterterrorism planning, it’s expected that the national government will lead and industry will follow. But in the cybersecurity space, it’s industry that leads and the government that follows. That’s not necessarily a bad thing, but it results from industry owning and operating much of our digital infrastructure.

More broadly, government’s role is to set out what ‘good’ cybersecurity looks like and to set regulations that the market can use. In that way, government provides a cybersecurity service to assist corporations to protect their assets and functions.

Attacking our major businesses is one way of weakening the country as a whole: it’s not just shareholders and company employees who may suffer. A successful attack on a major bank, for example, could pose a contagion risk to the nation due to the finance sector’s high level of interconnectedness. The so-called Chinese ‘Cloud Hopper’ hacking campaign highlights the threat and challenges. The Chinese Ministry of State Security contracted IT service providers to steal corporate secrets from their customers. Former Australian National Cyber Security Adviser Alastair MacGibbon pointed out that ‘this was the theft of industrial or commercial secrets for the purpose of advancing an economy. The lifeblood of a company.’12

Economic security is an essential element of national security, and it’s business that’s the engine room for a strong economy. Corporations are making valiant efforts to protect their assets and capabilities from attacks in the physical and cyber environments, and do so for sound commercial reasons.

However, apart from a few sectors such as defence support and basic utility providers, our major companies don’t consider these kinds of attacks and their response to them as an element of national security.

But such attacks aren’t just matters of commercial concern to companies and their shareholders. They have significant potential to weaken our national resilience.
Identifying the void

In the course of this study, we spoke with a wide range of key players in Australia’s official national security community (including those in the disaster resilience area) and business executives from key sectors in the economy.

We found that there’s a void between the two sectors when it comes to understanding each other’s capabilities and limitations and a lack of recognition on both sides of the mutual obligation to work cooperatively to protect the nation’s security.

This report identifies the strengths and weaknesses of this two-way relationship and makes recommendations to improve the ability of our official national security agencies and business to safeguard Australia.

National security has traditionally been viewed as a government responsibility and the corporate sector has been seen as somewhat of a bystander, although that view has been changing in recent years in relation to cybersecurity and critical infrastructure security.

The Australian Government has the constitutional responsibility for defence, although the states have key roles in a range of security issues, particularly natural disasters and emergency management.\(^{13}\)

The federal government is responsible for intelligence services and federal law enforcement capabilities. It assists the state and territory jurisdictions by providing legislative frameworks, resources and national coordination. Its focus is on defence, counterterrorism, cybersecurity and critical infrastructure, including national security issues related to the foreign ownership of key assets.\(^{14}\)

State governments are responsible for law enforcement, direct community liaison, first response to security and other disruptive incidents, emergency management organisations, and command and coordination of security incidents within their jurisdictions.

There’s a high degree of engagement between business and state governments, partly because of geographical proximity and partly because it’s sometimes easier to establish private-sector relationships within state law enforcement and emergency management agencies.

We shouldn’t forget local government.\(^ {15}\) Local councils are responsible for the delivery of services, including the provision of immediate and long-term response and support capabilities for the full range of incidents and disasters. Some major companies work closely with local government agencies on disaster resilience.

A ‘corporation’ is defined by law.\(^ {16}\) In this this paper, we’re considering larger businesses or those in specific niches, the disruption of which could result in major national failure points. Larger businesses protecting their supply chains for their own self-protection are contributing to overall national resilience.

Small and medium-sized enterprises (SMEs) are particularly vulnerable to the disruption of critical parts of the supply chain. Supply-chain security is only as good as the weakest link, and SMEs potentially the weakest link.

Corporations, as good business practice, have mechanisms in place to protect their operations and to provide business continuity and resilience. Business tends to adopt an ‘all hazards’ approach, particularly in relation to business continuity and resilience planning.

The private sector allocates the resources that are justifiable to protect companies’ ability to deliver their products and services cost-effectively. Businesses normally have continuity plans in place, to be used if their capability to deliver goods and services is disrupted.
Corporate capabilities

Corporations have great ‘visibility’ of what’s happening domestically and internationally that may affect their commercial operations. Some of the larger business entities have an in-house analytical capability or subscribe to specialist intelligence and analytical providers.

Most major companies have an operations or crisis centre. If the organisation deals internationally, it can respond to a crisis anywhere it’s active. During the Christchurch shootings in March 2019, for example, many Australian businesses were able to identify how many staff were in the city. They contacted staff to ensure their wellbeing and provided instructions to them on what to do and where to go.

Corporations hold considerable data that may be of benefit to governments during and after incidents. The private sector, within the limits of the law, can provide details of transactions, movements, deliveries, histories and related information to assist with ongoing and post-incident security investigations.

However, it’s common for a business that holds relevant information that would be of interest to national security and intelligence agencies to be unsure about whom to contact within government.

By the same token, it appears that elements within our security and intelligence community aren’t always aware of the corporate capability to assist or how to access the necessary information from the private sector.

Corporations, within the limits of the law, can provide operational practical, timely and relevant support to government national security planning and operations, including our national intelligence community. However, the private sector currently plays a limited role in national crisis exercises, although it sometimes assists with training environments in security exercises, logistic support and specialist expertise. For example, businesses can and do support national disaster response by providing capabilities, such as transport, communications and even ‘bank in box’ deployable bank branches.\(^{17}\)

A joint government and private-sector tabletop exercise planned for the end of 2019 will test the business continuity and resilience of the Australian energy sector. The exercise is open to the electricity industry, such as market and power system operators, electricity generators, storage providers, transmission network service providers, distribution network service providers and retailers, as well as Australian and state government agencies that have a role in the energy sector and cybersecurity.

The exercise model is based on the GridEx model used by the North American Reliability Corporation’s Electricity Information Sharing and Analysis Center (although the scenario will be developed to meet Australia’s needs). Due to the sensitive nature of the scenario, the exercise won’t be open to the general public.\(^{18}\)

Participating organisations are expected to plan, coordinate, deliver and evaluate their involvement in the exercise and share exercise learning with the Australian Cyber Security Centre (ACSC) to inform a national exercise report.

Compliance strategies and public–private engagement

Dare to share

Our official national security community tends to consider much national security information as ‘sensitive’ and so not to be released to business.

But in relation to counterterrorism, for example, the perpetrators are well aware of their preferred attack methods. It’s the probable targets that need to know in what form an attack may occur and what immediate, cost-effective, reasonable countermeasures could be considered.

Much of the information that’s of benefit may be from open sources. Security and law enforcement agencies can analyse the information within the Australian context and should be able to produce a report or briefing in a format that doesn’t require a security classification.
Business representatives with whom we spoke in preparing this paper indicated that information from government in relation to threats often tended to be rather generic. They often suggested that more applicable information could be gained from open sources or subscriptions to private-sector intelligence or information providers.

On the other hand, many in our official security community suggested that the corporate sector doesn’t commit enough resources to security and doesn’t always understand the broader national costs of business ‘insecurity’. Some officials expressed a fear that ‘if we told business too much, it might leak’ and said that, in any event, when resources are limited there couldn’t be endless consultation with business.

Several business executives rejected the fear of ‘leaking’. A number of corporate security officers stressed that in their experience the private sector treated security material that had been provided by security agencies with respect and maturity.

Business executives with whom we spoke stressed that companies spend precisely what is required and justified, and that security is usually perceived as a cost centre with no directly observable or measurable income benefit. If government officials can convince them that more must be allocated, then they’ll respond.

The expectations of government and business could be made more realistic through greater understanding of what each other is capable of and what’s possible. A common theme in our discussions with business executives was that, at the national level, agencies tend to ‘talk to’ rather than ‘talk with’ the private sector.

This may be partly because government prioritises the considerable intelligence and analysis capability that it holds and doesn’t recognise the knowledge and ‘on the ground’ experience of business.

One notable exception is the relationship that the major Australian airlines have with the Australian Government (see box).

Airlines as better/best practice

Mature airline operators provide many best practice examples of government and corporate security cooperation.

Based on a long history of collaboration, the two largest airlines in Australia are closely integrated into government systems in a way that not all corporate entities can demonstrate.

It’s essential that the major domestic carriers and the national flag carrying airline hold a close relationship with government. Australia’s major airlines play an important part in assisting Australia and Australians when there are security threats domestically or overseas.

Airline–government relationships here and overseas can serve as a model for better cooperation on national security between business and government.

At the state level, there appears to be more effective dialogue through the joint cybersecurity centres operating in most capital cities (the centres are a federal initiative), crowded places forums for precinct security and the joint counterterrorism teams in the jurisdictions.

Some corporate security executives indicated to us that greater access to classified information would be of benefit. If an organisation or sector needs information to protect itself and the recipient isn’t cleared, will the information be provided by our security agencies? If the answer is probably ‘yes’, then the initial classification or a method of declassifying the information should be considered.

Chief security officers (CSOs) and equivalent business executives holding appropriate national security clearances would assist in the transfer of information and provide an added degree of validation to due diligence during a company’s selection of a CSO. Clearances help to bridge the trust gap and ‘translate’ priorities between business and government.
Particularly in the case of classification, intelligence and national security organisations could consider extending the use of ‘tear-line’ intelligence, in which elements of classified information are withheld but adequate information is provided for business to react to a particular national security threat.

Major corporations, when selecting for the position of CSO, should be aware that the ability to obtain a national security clearance will be of benefit when communicating with federal government agencies on sensitive information. Arrangements for alternative vetting procedures can be made for CSOs from Five Eyes countries.

A phrase that’s gained some use among Australian corporate security professionals when talking about the desire for greater cooperation with the official national security community, including the Australian intelligence community, is **dare to share**, which refers to security officials being willing to provide information that’s timely and of value in the prevention and mitigation of all risks faced by the nation.

There are constraints on passing on certain national security information related to international agreements, perceptions of corporate advantage and, potentially, foreign ownership, but those restrictions aren’t insurmountable barriers. They don’t affect the intent to share, although they can affect the depth and timeliness of the sensitive information to be shared.

The dare-to-share phrase captures this issue well and is a sound principle upon which to build a mutual commitment by business and government to an improved security information sharing partnership.

**Existing communication channels**

There are already in place some mechanisms, established by the Australian Government and state governments, to ‘hook up’ with business on issues of national security. Indeed, in some ways it’s a crowded space.

However, the structures are fragmented between and within government departments and agencies and are often based on sector-specific silos. There’s no central hub within the Australian Government where all national risks are brought together for coordinated consideration and where business can provide focused input.

**Council of Australian Governments**

The Council of Australian Governments (COAG) is underdone when it comes to engagement with business on national security. Even the ministerial councils that assist COAG on national security, such as the Law, Crime and Community Safety Council, exist ‘hand to mouth’; they don’t function strategically.\(^{10}\)

COAG should consider the role of business in the national security space and examine how to improve its own role as a strategic forum on national security. A special annual COAG meeting on security, involving business, may be a good place to start.

**Business peak bodies**

Some business councils, such as the Australian Industry Group and the Business Council of Australia, have some contact with the national security community. However, they aren’t particularly active in developing industry positions on key national security issues or undertaking security-related research that would greatly assist in advancing businesses’ role in national security strategy.

**Industry Consultation on National Security**

In the past, the Industry Consultation on National Security (ICONS) provided for senior (CEO-level) corporate members to meet relevant federal ministers to be briefed on national security issues. ICONS was set up in 2014, but is now effectively defunct, not having met over the past two years.

ICONS had mixed reviews in our meetings with business executives during our research for this paper. We were informed that government agencies didn’t always appear to understand that CEOs’ diaries are often booked up to a year in advance and that too often CEOs were, as noted above, spoken ‘to’ rather than ‘with’.
Some business executives stated that their CEOs were told what they could have gained from their own CSOs. Some noted that there were challenges in finding a common ground at ICONS, when CEOs from different sectors more often than not had disparate security concerns.

**Trusted Information Sharing Network**

The Trusted Information Sharing Network (TISN) was established in 2003 and is made up of eight sector groups, the Resilience Expert Advisory Group, the Oil and Gas Security Forum and a cross-sector space interest group. It’s supported by the Critical Infrastructure Security Division in the Department of Home Affairs. TISN is a sector-based forum to encourage discussion between relevant industry CSOs, business continuity and risk managers and government participants.

Some sectors have been better than others at transferring relevant information, and have a stronger security culture. The best TISN working groups are those that exist under natural monopolies and have a strong regulatory environment to operate within (such as water and electricity).

Sector groups within TISN generally meet two to three times a year in forums with government representation and support. In addition, the Critical Infrastructure Advisory Council oversees each of the sector groups. It comprises the chairs of each sector group, state and territory representatives, relevant Australian Government agencies and the Australian Local Government Association.

SMEs aren’t well represented in TISN. Supply-chain security is only as good as its weakest link, and they’re potentially the weakest link.

Some business executives involved in TISN suggested to us that those working groups that were functioning well already had sector-based security forums or contacts. They noted the importance of doing more work to better understand cross-sector dependencies. While some work has been done through TISN, more needs to be done.

**Business and Government Liaison Unit**

The Business and Government Liaison Unit (BGLU) within ASIO is a key point of contact between government and the private sector in relation to national security. Access is by application, and after vetting the applicant may be added to the distribution list. The BGLU delivers a suite of activities, including security guidance documents, briefing days and roadshows pitched at the CSO level.

CEOs and boards are engaged by ASIO’s senior leadership team. Some business executives informed us that bulletins of incidents, with some analysis, were often late and generic. The BGLU captures a large amount of quantitative and qualitative feedback on its work with industry and continues to improve the timeliness and relevance of its products. Specific information is passed on a one-to-one basis to known and trusted participants.

Some business executives noted that the emphasis is on government informing the corporate sector, rather than the BGLU being a forum for real two-way dialogue.

**Critical Infrastructure Centre**

The Critical Infrastructure Centre was established in January 2017 and is located within the Department of Home Affairs. It works across all levels of government and with business owners and operators to identify and manage national security risks to Australia’s critical infrastructure. It’s also responsible for administering the *Security of Critical Infrastructure Act 2018* and the telecommunications sector security reforms (TSSRs).
Crowded places forums and the Business Advisory Group

The state-based crowded places forums and the Business Advisory Group were established under the Australia – New Zealand Counter-Terrorism Committee. They appear to be working well and offer a good example of cross-sector cooperation and information transfer between business and government on terrorism-related issues.21

Australian Cyber Security Centre

The ACSC operates as part of the Australian Signals Directorate (ASD). Staff from the Department of Home Affairs, the Australian Federal Police, ASIO, the Australian Criminal Intelligence Commission, the Australian Defence Force and the Defence Intelligence Organisation are co-located at ACSC.

When serious cyber incidents occur, the ASD—through the ACSC—leads the government response to help mitigate the threat and strengthen defences. While cybersecurity was initially provided by the Computer Emergency Response Team, the team was integrated into the ACSC in July 2018.

Part of the ACSC’s aim when it was created was for it to reach out to business. Despite the fact that not all key businesses have heard of the ACSC, it’s been very active in working closely with business on cyber-related communications, reporting and incident response and sharing threat intelligence.

But business, which brings in the cyber breach data, should be in the ACSC through organisations such as the Australian Banking Association or the Business Council of Australia to look after their business constituents. Business should pay for that representation.

Joint Cyber Security Centres

JCSCs, which are part of the ACSC, operate in Perth, Sydney, Adelaide, Melbourne and Brisbane. The centres provide a secure hub for cybersecurity experts, including from business, to share information on the latest threats and security challenges.23 They’re funded to 2020.

Sectoral engagement is segregated at the JCSCs: Adelaide (defence industry, supply chain, health); Brisbane (energy); Melbourne (telecommunications); Perth (resources); and Sydney (banking and finance).

The JCSC model should be expanded to encompass other aspects of national security information sharing.

Australian Signals Directorate

Apart from ASD’s responsibility for foreign signals intelligence and support to military operations, it has responsibility for the ACSC as the lead agency on cybersecurity. ASD has a legislative mandate to include cybersecurity advice to businesses.


A disaster risk reduction industry advisory forum is being established by the Australia – New Zealand Emergency Management Committee (the peak interjurisdictional policy forum on emergency management and disaster resilience) and senior representatives of industry.

It’s expected that the forum will be operating by the end of 2019 and will meet up to three times a year. It will work with the emergency management committee to enhance collaboration and understanding between governments and industry on reducing disaster risk. The forum promises to be a good example of government and business communicating on how to reduce risks.
Department of Foreign Affairs and Trade

Australia’s Ambassador for Cyber Affairs works with elements of Australian business on relevant aspects of our international cyber strategy. The Competitiveness and Business Engagement Branch of the Department of Foreign Affairs and Trade (DFAT) provides services to Australian business to strengthen the international competitiveness of Australian business by progressing important stakeholder relationships and forging stronger corporate engagement at all levels of government.

However, DFAT’s approach doesn’t reflect the level of business–government cooperation that’s evident in the US Overseas Security Advisory Council. The council is a joint venture between the Department of State and US business that interacts on overseas security problems of mutual concern. It provides for regular exchanges of information concerning developments in the overseas security environment and recommends methods to mitigate risks to American private-sector interests worldwide.

Australian intelligence community

The ASD’s and ASIO’s business liaison functions are part of the Australian intelligence community (AIC) and have been noted above. More generally, the AIC is becoming more effective in forging relationships with business. The Office of National Intelligence is seeking to expand its links to the private sector by more active engagement with business groups on a one-to-one level and by speaking at conferences and business meetings. Those efforts have been widely appreciated by corporate leaders and are in line with the thrust of some of the recommendations related to the need for the AIC to engage business, academia and think tanks in the 2017 Independent Intelligence Review.

ASIO leadership has also been active over some years in reaching out to company boards on a regular basis. Many board members are on several company boards, so when an ASIO brief is given it’s a force multiplier to get many different forms of information out to a range of companies. Defence industry leaders are also briefed on security considerations.

Forum of Australasian Security Executives

On the corporate side, there are forums through which security, business continuity, emergency and related managers communicate and share information. There are professional associations which have national and international reach to members with considerable experience and expertise. In general, public-sector employees tend not to join such professional associations or attend the meetings.

Senior CSOs of the major corporations turning over more than $10 billion a year meet via the Forum of Australasian Security Executives.

The forum is a professional affiliation of corporate security executives occupying the most senior national or regional security roles in their organisations, with responsibilities relating primarily to security and business continuity management, including crisis and emergency management.

One of the primary goals of the forum is to provide strategic leadership and trusted advice on matters of national strategic importance by harnessing the collective experience, knowledge and resources of its members. Government representatives are invited to speak to it, and this offers an opportunity to openly discuss security issues of national and international breadth.

In some ways, the forum is similar to the US Business Executives for National Security group (see box.)
Business Executives for National Security

The Business Executives for National Security (BENS) group is a US non-profit and non-partisan organisation that aims to provide a forum for American business leaders to provide their experience to make national security agencies and corporations more resilient, efficient and effective.

Founded during the Cold War by American mining executive Stanley Weiss, the organisation hosts roundtable discussions, runs crisis management exercises, creates focused working groups and conducts research.²⁸

While its head office is in Washington DC, BENS participates in regional outreach across the US. More than 450 business leaders within the US volunteer to the organisation to provide support and expertise.

The leaders of BENS are drawn from mining, construction, real estate, legal services and finance. It stands outside of the bureaucracy but liaises closely with the US Government.

Mind the gap

There are problems with current mechanisms that hinder two-way dialogue between business and government on national security.

According to many business executives we interviewed, government agencies are too often in a habit of talking and not listening. They suggested that the information provided by some agencies wasn’t always relevant or what was required by the corporate sector.

At the broad level of information exchange, there’s a lack of a relationship between the corporate sector and government. It’s often easier for business to get information through the back door, when people who have government contacts initiate contact.

Both government and corporate representatives indicated to us that sometimes the other party was intentionally or needlessly holding back essential information (business, in particular, sometimes wrongly believes the government is sitting on an information goldmine that it’s refusing to share), while expecting too much to be provided from the other party. This indicates a lack of understanding on both sides.

Channels for the corporate sector to raise and discuss national security and resilience with government are often not clear. Several corporate security professionals observed to us that there isn’t much scope at the moment to discuss or even know what national security policy or legislation is being developed, such as encryption laws.

Government national security bodies wish to communicate with senior executives (primarily CEOs) who have a strategic view but not the specific risk-oriented detail. However, there appears to be little direct communication between government representatives and the broader professional body of CSOs and business continuity and resilience officers.

Those corporations that are closely regulated by government (for example, those in aviation, telecommunications, finance and banking) tend to know how to find the relevant security official within government. This is because they’re able to go through established contacts or because they know how to navigate the bureaucracy. Companies and sectors not as closely regulated or integrated into the national security community have a difficult time identifying points of contact with the relevant agencies.

Business executives informed us that the emphasis tends to be on the private sector trying to contact governments to seek information or to provide information. Corporations have managers responsible for specific risk areas, but significant risks of all types are brought before the CEO and board. There’s no equivalent single position within government where the consideration of all risks is centralised.
The segregation of risks by sector or the nature of the risk makes it difficult for the corporate sector to communicate with government and for the government to apply a comprehensive ‘all hazards’ approach to prevention and response.

Companies may have a dedicated employee in charge of government relations, but it’s often difficult to identify key contact points within government structures.

Our business interlocutors stated that some government representatives lacked understanding and respect when dealing with the corporate sector, even expecting that CEOs will be available for meetings at short notice.

Translating government priorities into corporate priorities requires more regular contact with business by relevant government agencies.

It’s important from the corporate perspective to start from a premise when talking with government that industry should be given space to talk about its problems that are security related and for government to say ‘Help me understand’ and ‘What can we do?’.

It’s about building a conversation.

With few exceptions, the expertise in protective security, rather than broader national security, rests within the corporate sector, as it does for business continuity and resilience and related management disciplines.

Very few government employees hold formal qualifications in protective security or the relevant internationally recognised certifications; nor are they usually members of the relevant professional organisations.

Corporate representatives observed to us that there appeared to be a high turnover of government contacts, possibly because ‘security’ positions are seen as just another job rather than one requiring subject-matter expertise and commitment.

This becomes an issue in government–business cooperation on national security when government officials attempt to ‘tell’ private-sector security specialists what to do and how to do it. One CSO informed us that it was sometimes difficult to hold a peer-to-peer conversation with an equivalent government official.

Greater interchange between government and corporate security, emergency management, resilience and other managers would be useful.

The secondment of government personnel into the corporate security and more general risk management environment, possibly with a return secondment of selected corporate staff (costs and work pressures permitting), would foster mutual understanding.

If national security in the broader sense of national resilience is to be achieved via public–private sector engagement, it will require top-down and bottom-up initiatives. An ICONS meeting, for example, must offer CEOs something other than what they already get from their CSOs, who often have global reach in terms of security information.

But truly, what’s ‘national security’?

Other than the business of government, almost everything else that Australia needs to function as a society is owned and or managed by the private sector.29

When it comes to critical infrastructure, there’s specific legislation30 (see box) and a Critical Infrastructure Resilience Strategy to protect the identified sectors. But the listed sectors aren’t comprehensive: the internet, for example, facilitates Australia’s corporate and governmental capability but its providers aren’t listed (unless it’s by inference through the telecommunications providers that have obligations under the Telecommunications Act).
Corporate security and mandating resilience requirements

This report prioritises collaboration between the corporate sector and government on national security, but the government does have ‘big stick’ legislative tools to force the private sector into compliance. For example, the telecommunications security sector reforms (TSSRs) build a framework to manage risks to Australia’s networks and facilities. The reforms came into force in September 2018.

Under the reforms, there’s a security obligation that carriers protect networks and a notification obligation to the government concerning changes to services.

There’s also an information-gathering power for the Secretary of Home Affairs and a compliance ability to direct a carrier’s behaviour.

The most far-reaching and intersectoral piece of legislation addressing corporate security is the Security of Critical Infrastructure Act 2018 (although the TSSRs have stronger industry obligations). The legislation came into force in July 2018.

The Act seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia’s critical infrastructure. It applies to approximately 165 assets in the electricity, gas, water and ports sectors.

Under the Act, the Minister for Home Affairs has the ability to direct an owner or operator of critical infrastructure to do, or not do, a specified thing to mitigate a national security risk when all other mechanisms to mitigate the risk have been exhausted.

The Critical Infrastructure Centre began operations in January 2017 and prioritises partnerships with business, but it can intervene using the legislation where significant national security risks exist to make sure business owners put measures in place to protect critical infrastructure from national security threats.

Managers of risks to national security should address both protecting the nation (the ‘likelihood’ of national disruption) and developing and maintaining a resilient nation (the ‘consequence’ element).

While corporations understand a broad range of risks, including security, financial, social, environmental and geopolitical risks, they don’t necessarily know how to engage with national security policy regimes, relevant national security officials or intelligence leaders.

In business–government cooperation on security, the key message from our national security agencies should be that a secure nation will by necessity be reliant on businesses continuing to protect their functions and being resilient. Good business practice is good national security.

Businesses need to avoid making decisions that put the nation at risk. They can achieve this by understanding how their sector fits within the broader concept of national security.

In relation to national security, government tends to concentrate on the likelihood element of the risk equation, providing the intelligence and resources to prevent a disruptive incident from occurring.

The consequence management aspects, should the risk be realised, are essential considerations for the business sector. ‘Resilience’ is defined in ISO 22316 as ‘the ability of an organisation to absorb and adapt in a changing environment’.

This should be a key objective underpinning business–government cooperation on national security.

A useful step was taken with a recent publication on disaster mitigation by the National Resilience Taskforce under the auspices of the Department of Home Affairs. Because of the scale and speed of extreme natural events, they have a similar potential to other security challenges that threaten our normal way of life across significant areas of the country.
The involvement of businesses organisations considering national resilience using an all-hazards approach enhances the ability of governments and corporations to communicate to their mutual benefit in preventing, managing and recovering from disruptive incidents.

Corporations have their own plans for maintaining business activities during periods of disruption, but greater integration of government and corporate plans will assist in planning for a resilient society in the face of both man-made and natural disasters.

National security should be viewed as an equal partnership between the Australian Government, the state jurisdictions and the corporate sector. A new relationship between business and the national security community is needed to protect the nation. It should be built on mutual understanding and respect.

The corporate sector has capabilities and limitations of which security agencies may not be aware, and vice versa.

The corporate sector needs to be realistic about what information security and intelligence agencies hold and can or will provide, but national security bodies need to be aware of the information-gathering and crisis-control capabilities of the corporate sector.

As noted above, expertise and qualifications in protective security, business continuity and resilience and related subjects as management disciplines resides primarily in the corporate sector rather than within government.

However, without a familiarity with government structures that allows businesses to direct their information or ask for advice, interaction between business security professionals and national security agencies is proving difficult.

National security officials don't necessarily know which private-sector businesses can provide the necessary information, intelligence or resources. A database of which organisations to contact for specific issues could be established.

Two levels of dialogue are required. The first level should be an engagement on national security matters between the Prime Minister, senior ministers and heads of agencies and the intelligence community with CEOs. The second level should be one where operational meetings could be held between the security agency executives and business CSOs and equivalents. This two-level dialogue would ensure that a nationwide cooperative security strategy could be developed with input from security agencies and the private sector.

To achieve such a level of dialogue, mutual understanding and respect are required. Corporate executives must understand the imperative of government to ensure that the nation has a strong deterrent to all forms of ‘blended aggression’.

National security officials must recognise that the corporate sector has responsibility for protecting the business assets and functions, that resource decisions must be justifiable, and that the expertise in protective security and organisational resilience rests predominantly in the corporate sector.

**Mutual obligation**

A secure and resilient nation can only be ensured through mutual obligation whereby both governments and corporations understand and are committed to developing and maintaining the measures needed to safeguard Australia.

It’s certainly not about business in any way trying to ‘sort out’ national security. Rather, it’s about the fact that, for the private sector to be profitable, it depends on national security. The corporate sector should have an obligation to contribute to that.

It’s about mutual benefit.

Corporations already commit the resources they believe are justifiable to protect their business, including its capability, reputation and sustainability. But this isn’t seen by security agencies, nor for the most part by business, in the context of protecting the nation. It’s seen in purely commercial terms.

If it could be demonstrated by government to corporate leaders that their combined efforts are critical to a secure and resilient nation, then the opportunity to work more cooperatively with business could be established.
Corporations would maintain good corporate practice, but with an awareness of national security requirements, and national security agencies can provide frameworks for better communication and information exchange.

In contributing to national security, business is generally not seeking financial incentives from government, such as tax breaks, subsidies for corporate back-up plans or special government status as resilient companies in order to ‘do the right thing’.

That’s because such measures for the most part are in place and, for the larger corporations, while financial incentives may be welcome, they would be minimal compared to business operating budgets.

This is unlike the Swedish approach, in which a commissioner has recently been appointed by the government to examine the role of incentives for business to contribute to national resilience (see box).

---

**Sweden’s ‘total defence’ planning and business**

Sweden’s approach of ‘total defence’ recognises that both the public and private sectors are key assets in national defence and national security efforts. The Swedish model is possibly the most mature in formalising relationships between government and business in national security planning.

The Swedish Government’s total defence priorities are outlined in a report titled *Resilience: the total defence concept and the development of civil defence 2021–2025*.35 The Swedish Defence Commission suggests that key companies should be identified and designated, and that dialogue between private actors should assess preparations for rationing, supply-chain security and defence preparedness.

The commission notes that private enterprises have knowledge, organisational structures and creativity to cross-pollinate the total defence planning process.

Swedish law requires businesses to participate in the total defence planning effort. Contracts between public actors and business are at the heart of this: signed contracts legally require a private actor in charge of a vital societal function or critical infrastructure to continue services and goods in times of crisis and war (meaning that the contract is without a *force majeure* clause.) How the financing of this is to be handled is central to government–business discussions in Sweden.

Sweden last year appointed a special commissioner, Elisabeth Nilsson (a Swedish business leader), to consider opportunities for incentivising the business sector to provide societal resilience and contribute to critical total defence needs. Nilsson will present her report to the government later this year.

Many business executives we spoke to argued that of far greater value than government incentives were realistic and timely security-related information and an understanding of how their business fits within the overall concept of a resilient nation.

Promoting mutual obligation as a corporate ideal will require top-down and bottom-up support within governments and corporations. It will require discussions between CEOs and the Prime Minister and, as noted above, between relevant business executives and national security officials.

**Moving towards good public–private partnerships**

The nation’s security and resilience can be enhanced by improved dialogue between national security agencies and the corporate sector. This will assist with mutual understanding and interoperability in national crises. There needs to be greater predictability in how business and government can work together in planning for national security matters.

Two-way communication will be effective in building links with business and government on security matters. In that way, businesses will feel as if they’re informing and contributing to the intelligence and national security community.
As key strategic sectors of our infrastructure are owned by the private sector, the government should coordinate security planning with the business sector to prepare for national emergencies in all sectors.

A whole-of-nation all-hazards approach to national security would assist in responding to the kinds of ‘blended aggression’ we’re seeing, in which the corporate sector is now being attacked.

The threats we face don’t recognise the walls that exist between Australian businesses and national security agencies. To safeguard Australia, we need to put more doors in those walls.

A key message of this paper is that corporate leaders need to understand what threats are out there and what are the most effective ways to manage them.

For national security agencies, a key message is that coordinating and cooperating with the private sector on national security may be inconvenient at times, but it’s a lot less convenient than being exposed to a range of security threats and challenges unprepared.

The paramount concern of businesses must be their shareholders and customers, but our corporate leaders need to view their business operations as part of national security, not just as commercial operations, and work with governments at the state and national levels.

At the same time, more can and should be done by the Australian Government and security and intelligence agencies to work even more closely with the corporate sector to develop the most cost-effective deterrence against a range of threats. Today, corporate security is national security.

Recommendations

A greater recognition by the Australian national security community of the importance of the corporate sector in all national security considerations is required.

For the Australian Government and national security agencies

1. In drafting national security policy and plans, due consideration should be given, where appropriate, to corporate business continuity planning.

2. A central hub within the Department of Home Affairs should be established to be responsible for ensuring, with corporate sector interaction, information transfer on national security risks and support for industry in understanding emerging security issues. The hub would be a communication forum for the business and government sectors to cooperate on issues related to potential threats and responses.

3. At the operational level, a Chief Security Officer Advisory Group should be established to work with such a hub. The advisory group, convened by the Department of Home Affairs, would consist of a small number of senior security, business continuity and resilience managers, as well as organisations such ASIAL and the Forum of Australian Security Executives, which would represent the broader corporate sector.

4. ICONS should be reconvened to provide a forum for the Prime Minister and senior ministers to engage with CEOs on national security policy and issues. ICONS should highlight the interconnected dependencies of the corporate sector in maintaining national security and underline issues of mutual obligation when it comes to a safer Australia.

5. State-level JCSCs should become converged centres for integrating national security interaction between business and government. The JCSCs should be rebadged as joint threat management centres to establish two-way communication, analysis and planning not just on digital and cyber risks but on other security risks, such as foreign interference; activism and politically motivated violence; the security of offshore business activities; and disaster resilience.
6. The Australian Government and state governments should seek to expand the involvement of business in exercises related to all aspects of national security, including counterterrorism, health security, national disasters, military preparedness and cybersecurity. Exercising arrangements across those areas is an effective way to strengthen organisations’ security arrangements, including by ensuring that incident response plans, including communications processes, are up to date. The Swiss Security Network nation-wide exercise is one model.36

7. There should be a secondment program of national security agency personnel into the corporate security and more general risk management environment.

8. Wherever possible, ministers should be involved with business in national security and resilience forums.

**For the corporate sector**

1. Corporations should understand the costs of insecurity not just to their business but national security more broadly.

2. Corporations should consider how their business continuity and resilience plans support national security and resilience.

3. CEOs of major corporations should participate in a revitalised ICONS to provide perspectives on what’s required and currently in place to produce a resilient nation.

4. A database of which business organisations to contact for specific capabilities relevant to national security planning should be established.

5. Corporations, which often stress-test themselves, should expand their involvement in official exercises related to all aspects of national security.

6. Major corporations, when selecting for the position of CSO, should be aware that the ability to obtain a national security clearance will be of benefit.

**For both the Australian Government, national security agencies and the corporate sector**

1. All sectors should agree that there’s a mutual obligation to produce a secure and resilient nation.

2. Discussions should be held between the national security community and corporations on the essential contribution of corporate support to national security. These discussions should be held at CEO/board level and with senior officers responsible for security; business continuity and resilience; and crisis management.
Notes

1 Codan Limited, Codan annual report, 2016, online.
3 Four Corners, ‘HACKED!’, ABC, 27 May 2013, online.
4 General Angus Campbell, speech to ASPI ‘War in 2025’ Conference, 13 June 2019, online; see A Bergin, R De Wilde ‘Spiders, posters and hoaxes: it is still war, but not as we’ve known it’, The Australian, 22 June 2019, online.
7 As noted by former prime minister Malcolm Turnbull in introducing the foreign interference bill, 7 December 2017, online.
8 See R Shah, Protecting critical infrastructure in an era of IT and OT convergence, Policy Brief 18/2018, ASPI, Canberra, online.
9 MinterEllison, Perspectives on cyber risk, 2019, online.
10 B Smith, ‘34 companies stand up for cybersecurity with a tech accord’, Microsoft on the Issues, 17 April 2018, online; Tech Accord, online.
11 Cyber Threat Alliance, online.
12 ‘Inside the West’s failed fight against China’s Cloud Hopper hackers’, Reuters, 26 June 2019, online.
13 A Bergin, Federating security, policy options paper, National Security College, Australian National University, August 2017, online.
16 The Corporations Act 2001 (Cwlth) defines a corporation: ‘Subject to this section, in this Act, corporation includes: (a) a company; and (b) any body corporate (whether incorporated in this jurisdiction or elsewhere); and (c) an unincorporated body that under the law of its place of origin, may sue or be sued, or may hold property in the name of its secretary or of an office holder of the body duly appointed for that purpose.’
17 A Bergin, All in a day’s work: business and Australian disaster management, ASPI, Canberra, December 2008, online.
18 In some ways, that’s a pity: the public needs training in what to do when there are longer term power outages. E Braw, ‘We must learn what to do if the lights go out’, The Times, 10 May 2019, online.
19 Bergin, Federating security.
20 An excellent example of practical advice provided by ASIO is the recently released Security managers guide: dynamic lockdown, 2019.
21 Security of Critical Infrastructure Act 2018 (Cwlth).
22 An ASPI study last year addressed the relationship between those agencies responsible for counterterrorism planning and the private guarding sector. The report noted government and industry cooperative programs such as Project Griffin (UK) and Project Shield (US). A Bergin, D Williams, C Dixon, Safety in numbers: Australia’s private security guard force and counterterrorism, ASPI, Canberra, October 2018, online.
24 Department of the Prime Minister and Cabinet, 2017 Independent Intelligence Review, Australian Government, Canberra, June 2017, online.
25 Examples include but aren’t limited to the Australian Security Industry Association Limited (ASIAL), ASIS International, ISACA, the Australian Information Security Association, the Facility Managers Association, the Venue Managers Association, the International Association of Venue Managers and the International Association of Emergency Managers. In the US, in particular, the professional associations have formal links with government; for example, ASIS International, online.
26 Authors’ interview with the Forum of Australasian Security Executives chairman.
27 The Forum of Australasian Security Executives is by invitation only, has strict controls over sharing commercial information and excludes providers.
28 Business Executives on National Security, Mission statement, online.
29 The role of government includes the provision of constitutionally mandated functions such as national defence; intelligence and associated capabilities; border protection, including biosecurity; and, at the state level, the provision of emergency services and associated capabilities.
30 Security of Critical Infrastructure Act 2018 (Cwlth) and similar federal and state/territory Acts designed to support critical infrastructure, such as the telecommunications security sector reforms.
31 Critical Infrastructure Centre, Critical Infrastructure Centre compliance strategy, Australian Government, Canberra, online.
32 Department of Home Affairs, National security, Australian Government, Canberra, 11 November 2018, online.
33 ISO 22316, Security and resilience—organisational resilience—principles and attributes.
34 Department of Home Affairs, Profiling Australia’s vulnerability: the interconnected causes and cascading effects of systemic disaster risk, Australian Government, Canberra, 2018, online.
36 H-J Käser and B Wigger, ‘The 2019 Swiss Security Network exercise: more than an exercise’, RUSI Commentary, 24 May 2019, online. Five years ago, the first exercise, involving participants from government, the private sector and the wider public, was undertaken. It focused on a pandemic and power outages. In November this year, the next exercise, again involving business, will focus on counterterrorism.
Acronyms and abbreviations

ACSC  Australian Cyber Security Centre
AIC   Australian intelligence community
ANU   Australian National University
ASD   Australian Signals Directorate
ASIAL Australian Security Industry Association Limited
ASIO  Australian Security Intelligence Organisation
BENS  Business Executives for National Security (US)
BGLU  Business and Government Liaison Unit
COAG  Council of Australian Governments
CSO   chief security officer
DFAT  Department of Foreign Affairs and Trade
ICONS Industry Consultation on National Security
JCSC  joint cyber security centre
SME   small to medium-sized enterprise
TISN  Trusted Information Sharing Network
TSSR  telecommunications sector security reforms
About the authors

**Anthony Bergin** is a senior fellow at ASPI. For 20 years, Dr Bergin served as an academic at the Australian Defence Force Academy, where he taught homeland security. From 1991 to 2003, he was the director of the Australian Defence Studies Centre. He served for four years as an adjunct reader in law at the ANU. Dr Bergin has been a consultant to a wide range of public- and private-sector clients and has written extensively on national security issues in academic journals, books and ASPI reports. He is a regular media commentator and contributes to ASPI’s *The Strategist*.

**Donald Williams** holds qualifications in security management as well as risk, project and resource management. He is a Certified Protection Professional and Registered Security Professional. He is a member of ASIS International, the Institute of Explosives Engineers and the International Association of Bomb Technicians and Investigators. He is the author of numerous papers and reports related to security.

**Rhys De Wilde** is a research intern at ASPI. He is completing graduate studies in national security policy at the ANU. Before joining ASPI he worked as a research assistant at the National Security College, ANU.

Acknowledgements

During the course of this study, we spoke with numerous corporate security executives from a wide range of industry sectors and with leaders from the official Australian national security community. All those who spoke to us did so on the condition of anonymity. We acknowledge the support of the Australian Security Industry Association Limited for this study. However, the views in this report are solely those of the authors and don’t represent the positions of ASIAL.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

About Strategic Insights

Strategic Insights are short studies intended to provide expert perspectives on topical policy issues. They reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.
From board room to situation room
Why corporate security is national security