2019

Cyber Security's Impact on SMEs and the Supply Chain

Jonathan Frank

Molly Davidson

Neil Morris

SADILP

November 2019

Concept Paper Question

Small to Medium Enterprises (SMEs) are increasingly becoming the target for cyber-attacks.

1. What risk does this present to supply chains?
2. Why are SMEs being targeted? and
3. What should we be doing to effectively and efficiently rise to the cyber security challenges?

Contents

Acronyms

Acronym	Definition
ACSC	Australian Cyber Security Centre
AIC	Australian Industry Capability
ASD	Australian Signals Directorate
DISP	Defence Industry Security Program
DOS	Denial Of Service
OAIC	Office of the Australian Information Commissioner
SME	Small to Medium Enterprise

Introduction

Small to Medium Enterprises (SMEs) and their supply chains are increasingly becoming the target for cyber-attacks in Australia.

An SME in Australia is defined as an incorporated company with less than 200 employees. The Defence Industry in Australia in made up from several major primes and around 3000 SME's, which make up approximately fifty percent of employment in the Australian defence industry.[1]

The Australian defence industry is well known for cutting edge technology and makes a significant contribution to defence products both in Australia and internationally. With the government announcing its Defence Industrial Capability Plan for SMEs with an emphasis on value-add work and strengthening Australian supply chains, SME's will be engaged more than ever to provide Australian solutions for defence and defence industry[2].

Further afield, Australian SME's also provide services and products to foreign militaries and defence industries. This worldwide customer base brings with it both opportunity and risk.

Cyber security threats have become prevalent in modern day defence industry and broader industries. Threats come in the form of foreign intelligence services, insider threats, terrorism, criminal groups, issue motivated groups and maverick individuals[3]. These threats pose a risk to industry, sovereign intelligence and Commonwealth information.

Cyber Security and Cyber Attacks

A cyber-attack is a deliberate act through cyber space to manipulate, destruct, deny, degrade or destroy computers or networks, or the information resident in them, with the effect, in cyber space or the physical world, of seriously compromising national security, stability or prosperity.[4]

Cyber security attacks come in many shapes and sizes, common threats include;

- Phishing, spear-phishing, whale-phishing campaigns;
- Email attacks - malware;
- Denial Of Service (DOS) attacks;
- Drive by attack - a common method of spreading malware;
- Cross-site scripting;
- Ransomware;
- Social engineering - often uses social platforms such as LinkedIn, Facebook, etc.
- Unsecure implementation of the internet of things; i.e. mobile phones (Siri), Google Home and Alexa by Amazon are always listening.

[1] Australian Trade and Investment Commission, Australian Defence Industry https://www.austrade.gov.au/local-sites/singapore/contact-us/australian-defence-industry

[2] Defence Industrial Capability Plan (Small to Medium Enterprises) http://www.defence.gov.au/SPI/Industry/CapabilityPlan/Docs/DICP-SME-Factsheet1.pdf

[3] Defence Industry Security program - Security awareness Training, 2019

[4] ACSC Threat Report 2015

Risks to SME’s and the Supply Chain

What is at risk if you don’t mitigate against a cyber-attack?

Cybercrime can have significant impacts on the whole of defence and defence industry, including SME’s and their supply chains. There are direct and indirect costs to cybercrime victims including:[5]

- Damage to personal and corporate brand identity and reputation;
- Impact on emotional and psychological wellbeing of individual victims;
- Financial losses from fraud and ransoms;
- Costs of responding to cyber-crime;
- System remediation costs;
- Flow-on costs to government support programs that assist cybercrime victims;
- Loss of business resulting in loss of employment opportunities;
- Operational disruption[6];
- Loss of competitive advantage; and
- Fines of up to $1.8 Million from failure to report mandatory data breaches to Office of the Australian Information Commissioner (OAIC).

In 2018, Perth-based shipbuilder Austal was the victim of a cybersecurity attack. It reported an unknown offender accessed its computer systems, accessing personnel email addresses phone numbers, as well as ship drawings and designs. The information was then offered for sale on the dark web in an extortion attempt. The information that was stolen was not a threat to national security but this example shows that even larger defence industry organisations can be victims of cybercrime.

Cybercrime trends

The BDO and AusCERT 2017/18 Cyber Security Survey results in Figure 1 demonstrates a growing trend in attacks from cyber and organised criminals, with the next most likely cyber attackers to be insiders and current employees.

Figure 1 also shows that in 2017 over fifty percent of cyber security incidents were from cyber criminals and organised crime[7]. The next primary risk is from insider threat, either deliberate, accidental or negligent. A good example of this is from Talisman Sabre; in 2018 Australia’s head of Joint Operations reported that the 2017 battle map had been uploaded to social media, putting the exercise and individuals at risk[8].

[5] ACSC Threat Report 2015
[6] BDO 2017/2018 Cyber Security Survey
[7] BDO 2018/2019 Cyber Security Survey
[8] Asia-Pacific Defence Report Vol 44, No 3, April 2018

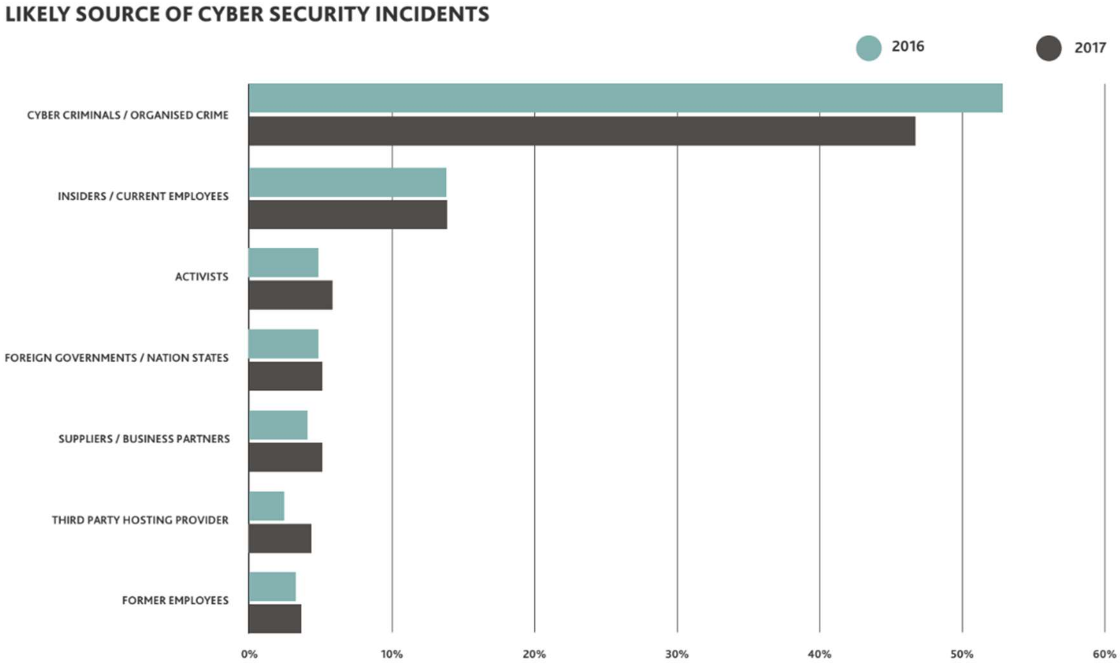

Figure 1 BDO and AusCERT 2017/18 Cyber Security Survey

The Defence Industry Security Program (DISP) Security Awareness training[9] depicts the six most prevalent threat actors for cyber-crime as shown in **Error! Reference source not found.**, with insider threat being one of these, supporting the BDO and AusCERT 2017/18 Cyber Security Survey results.

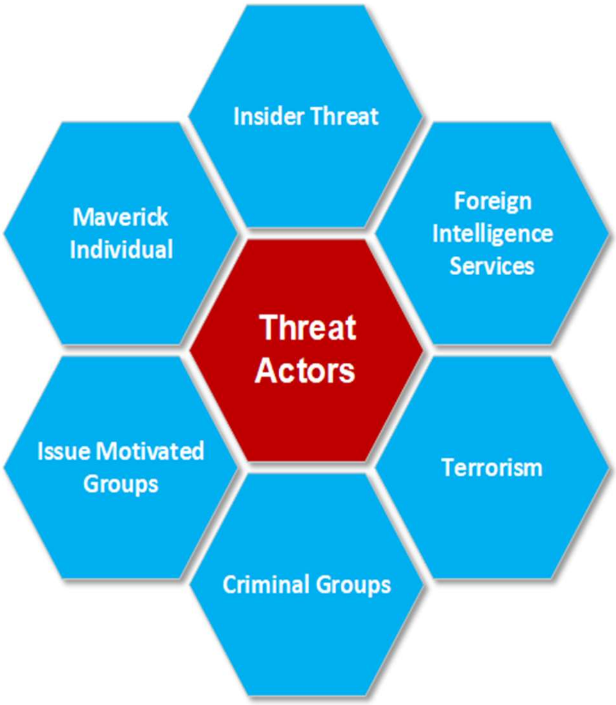

Figure 2 Six Most Prevalent Threat Actors for Cyber Crime

[9] DISP Security Awareness Training, 2019

Why are SME's being targeted?

While a large number of attacks are random, there is an increasing trend in targeted cyber-attacks. SMEs are attractive targets for a number of reasons:

- SMEs are being promoted more prominently Australia wide and worldwide due to Australian Industry Capability (AIC) initiatives implemented by the Commonwealth Government and in good news stories for the amazing work they do. This promotion puts SMEs in the spotlight and links the SME to defence or other areas of interest that hackers or foreign groups may profit from.

- SMEs are often small, family run, businesses with little to no defence industry experience, let alone cyber experience. Meaning that a hacker has less risk of failure when attacking and they require less effort to be successful.

- SMEs often don't have dedicated IT and security departments, meaning:
    - There is no in-house expertise or general awareness of cyber-attacks or security;
    - There is little to no maintenance or important security patching of operating system and software – leaving critical security flaws present; and
    - There are makeshift IT personnel that are simply not security aware in areas such as human resources, accounting or engineering.

- Cyber security or hardening controls are too expensive to implement. With cash flow often being an issue, hiring dedicated IT personnel, training up existing personnel or bringing in consultants is just not possible.

- SMEs can be easier to socially engineer and infiltrate. Being a smaller business, it is often easier to get information on significant roles in the business through social media and other means, and utilise this to gain access to other parts of the business. For example, the owner is often also the engineering manager and the Chief Financial Officer. This means the same person may have access to all of the valuable areas of the business and information, which is often not the case in larger organisations.

- Often in SMEs the companies IT infrastructure is shared with personal use. For example, the laptop which is being used for social media, personal email and applications is being used to store sensitive company data. This provides easy access to data for a hacker, as the data is often unsecure and can be easily infiltrated. Additionally, files are frequently being copied to and from the internet on a personal device making a cyber-attack more likely.

- SMEs often don't understand or appreciate security classification or trade restrictions on the information they share with other SMEs in their supply chain. Their staff are unaware of the value of this information which provides easy access for hackers or foreign intelligence services.

- Less rigorous supply chain and contract management. SMEs don't often have dedicated departments for this, meaning that required standards and procedures are not being met. A supplier can be a doorway into an SMEs business and data; the supplier can put an SME at high risk of attack if they are not aware of cyber security. For example in 2013, Target (United States) had a data breach where their server was accessed and credentials stolen through a third-party vendor. 40 million customer credit details were stolen, costing Target USD 202 Million.[10]

Defence Industry Feedback

After reviewing the literature and interviewing subject matter experts and SME's, the following was identified as their top cyber security issues:

1. **Cost to implement**
   The cost to implement cyber security can range from tens of thousands of dollars to many hundreds of thousands of dollars. The SME's that were interviewed for this paper disclosed that they have accessed external organisations to implement their cyber protection costing them from $30,000 up to $0.5 million. Alex Heidenreich from Diamond Cyber stated that "SME's are starting to ask for cyber resilience and literally cannot afford it"[11].

2. **Having the resources to implement and maintain ongoing cybersecurity**
   Most SME's don't have dedicated internal IT resources and often outsource IT services including IT security, monitoring, incident response, control validation and culture support (phishing assessments and personalised resilience updates). These initial and ongoing services have a cost.

3. **Finding subject matter experts/suitable software solutions**
   Finding independent and suitable subject matter experts was difficult for the SME's we interviewed. SME's often found that subject matter experts would be working for software suppliers and implementing that specific brand of software, instead of making an independent assessment and tailoring a cyber security package for their specific needs and risks.

4. **Employee acceptance, training and culture**
   SME's reported that making personnel aware of the need to implement cyber security change was sometimes difficult. User awareness training had been implemented by fifty percent of respondents, with the remaining SME's not yet implementing the training to date. The cost and time to create and execute training was also raised as an issue.

5. **Punitive damages from a breach (contractual obligations being pushed down)**

[10] NBC News, https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031
[11] Alex Heidenreich, Diamond Cyber, Concept Paper Questions email 2019

Larger companies and the Government are increasingly trying to address supply chain risk by imposing contractual information security obligations on SME's. This results in business risk associated with the increased cost of building cyber resilience, implementing technical, procedural, and people controls and presents a contractual risk if they are breached and have punitive damages awarded against them.

6. **Having procurement and contract management overhead to identify (and strengthen) the supply chain subcontracted work.**
   As large businesses deploy stricter cyber security protocols, the risk of cyber-attack is pushed to the weakest link in the supply chain which tends to be SME's or their supply chain. Having the ability to identify those SME's at risk and guide them or influence them to implement cyber security is difficult and time consuming for both big organisations and SME's.

7. **Confusion regarding the number of governing bodies and amount of information.**
   With the Defence Industry Security Program (DISP), Australian Cyber Security Centre (ACSC), the Essential 8 and Australian Signals Directorate (ASD) Top 4 being just a portion of the governing bodies and information surrounding cyber security, SME's reported confusion as to who to go to or which guidelines to use to assist them in their cyber security challenge. Similarly, access to grants, eligibility and the application process was also flagged as an area of complexity.

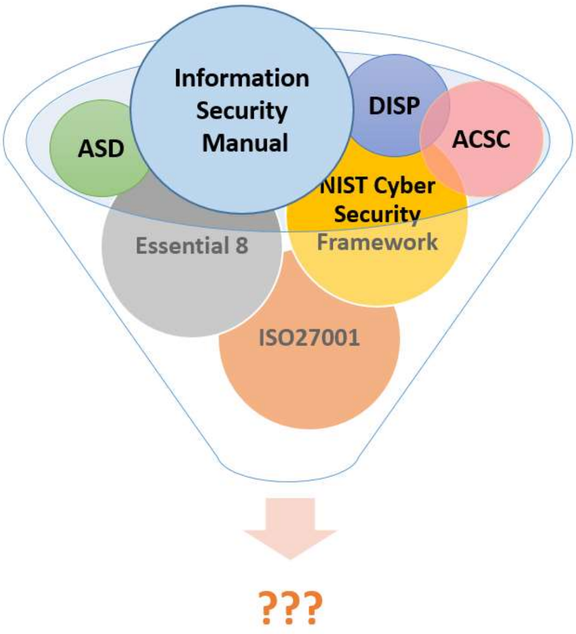

Figure 3 Governing Bodies and Guidelines

Recommendations

To make cyber security rollout more efficient and effective for SMEs in the defence industry, the following recommendations should be implemented:

- Cyber security policy and guidelines in Australia are complicated and confusing; making templated policies and procedures available freely or cheaply to SME's would assist in helping them in navigating the mine-field of cyber security information.
  It is recommended that this be provisioned or subsidised by the Government and implemented by the ACSC.

- Maintain a national database of cyber consultants and software to assist SME's. To aide selection and quality of industry experts, similar to the National Professional Engineers Register, ACSC should maintain a database of consultants to suit the specific industry and business type. In addition, a 'compare the market' type database for the software available would also assist SME's in selecting a more effective and suitable solution.

- The Commonwealth to better advertise to improve visibility and implementation of grants. A centralised body to list all grants, making searching, applying, support and execution of grants simpler. While also providing administration support for smaller SME's that do not have the overhead or resource to support the Grant application process.

- Online training and yearly refresher courses can be made cheaply by Government and subscribed to by SME's. This online training also removes the facilitator and associated fees, making a course like this value for money for the government. Australia has 3000 SME's, so there is scale to spread costs; i.e., 3000 SME's would spend approximately 40 hours each in creating a training package alone, that is 120,000 hours of lost productive time by SME's. This could be saved if this activity was done centrally by the ACSC. This database/record concept could grow to cover capabilities and other requirements and become a list of SME's that are 'defence ready'.

- Providing monitoring and incident response support to SME's at affordable rates, and proactively supplying support to enable cyber resilience. I.e.: a '000' cyber security help response line or helpdesk.

- Primes, which flow down costly cyber requirements within their sub-contracts to SMEs, should be made to assist with the implementation of cyber security (via funding/grants/skills). This is to change the culture and have a collaborative approach to cyber security, instead of the traditional ASDEFCON style system.

Ultimately, the impacts of cybercrime on SMEs and their supply chains can result in a failure to deliver important military capability which should be treated as a direct threat to national security. If these recommendations are successful, it will help build the defence industry supply chains cyber resilience by making implementation easier and cheaper, and addressing the higher risks factors of cyber-crime.