Joint Committee of Public Accounts and Audit

Cybersecurity Compliance – Inquiry into Auditor-General's report 42 (2017-17) – 2 June 2017

ANSWER TO QUESTION ON NOTICE

Department of Defence

Topic: US and UK Cybersecurity Reviews

Question reference number: 2

Member: Brodtmann
Type of question: asked on Friday, 2 June 2017, Hansard page 17
Date set by the committee for the return of answer: 23 June 2017

Question:

Ms BRODTMANN: Thank you. I want to go to another submission that we received, from Ian Brightwell. He spoke about whitelisting and he had some interesting views on that. I will put those on notice. Further to our discussion on culture and driving cultural change through measurements and key performance indicators—articulated measures—his suggestion is that we should change to a different risk management or risk mitigation framework. His suggestion is to move to the US system or the UK system where those behavioural change elements are incorporated—the concept of self-assessment and continuous self-assessment is incorporated. Are you familiar with those systems—the US system's Cyber Resilience Review? It has a number of mechanisms that agencies need to look at, including the situational awareness issue that we discussed earlier at today's hearing. I would like your thoughts. This goes to the ASD, Mr MacGibbon and also Ms Mellor. I am sure you are aware of the Cyber Resilience Review that operates in the US and Cyber Essentials in the UK. His view is that they are far more comprehensive than the strategies we have in place and we should perhaps look to install them here.
Mr Lines: Thank you, Ms Brodtmann. That is actually a very good question because, in fact, there are multiple standards out there. There is the whole set of NIST standards of the US government. If you contract to the US government, there are now 210 controls you must complete if you are providing IT services to government. The resilience, as I understand it, is based around industry stuff, and Cyber Essentials is also an industry program. They are designed to do, in my understanding, slightly different things, but I will have to take the question on notice and come back to the committee because I cannot provide an effective answer today, except to note that there are lots of standards. The top four and the strategies to mitigate cyber incidents were to get away from technical controls to provide very simple advice to people about the things they needed to worry about, depending on their risk. They are not all designed to do the same thing—I think that is the fundamental answer—but I will come back to you.

Answer:

The Australian Signals Directorate's Strategies to Mitigate Cyber Security Incidents is a prioritised list of practical actions organisations can take to make their computers more secure. The advantage of this guidance is that it is customisable to each organisation based on their risk profile and the threats they are most concerned about.

Cyber security can appear complex and technical, but it is essentially another risk for boards and chief executives to manage. They are accustomed to managing significant risks, and cyber risk should be evaluated in the same way.

The Australian Signals Directorate recommends that all Australian government and non-government organisations implement a package of eight essential strategies as a baseline. Called the Essential Eight, this baseline makes it much harder for adversaries to compromise systems.

The Essential Eight provide succinct, specific, prioritised guidance to address the broad range of cyber threats faced by governments and businesses alike. The guidance can be tailored to meet an individual government and non-government organisation's risk and resource profile.

The Australian Signals Directorate's Essential Eight Strategies to Mitigate Cyber Security Incidents are so effective the Australian Signals Directorate recommends them as the cyber security baseline for all Australian organisations.

When the baseline maturity is achieved, it mitigates:
- targeted cyber intrusions
- ransomware
- malicious insiders
- business email compromise
- threats to industrial control systems and
- adversaries who have destructive intent.

Beyond the Essential Eight there are further steps organisations can take to protect themselves, and we encourage organisations to consider the Strategies in their entirety on the Australian Signals Directorate website.

The US's Cyber Resilience Review is a self-assessment program that contains 42 goals and 141 specific practices organised across ten domains – one of which is Risk Management.

The UK's Cyber Essentials Scheme is a government backed, industry supported scheme to help organisations protect themselves against common cyber attacks. Organisations apply a range of controls within an agreed framework to achieve one of two 'Cyber Essentials Badges'.

Both of these programs were designed to achieve a different purpose from the Essential Eight.

The US and the UK programs alone would not be sufficient to successfully protect Australian Government official information. In order to meet the Government's requirements, non-government organisations would have to follow the guidance in the Commonwealth's Information Security Manual, of which the Essential Eight form an important component.

Regarding self-assessment of cyber maturity, the Australian Signals Directorate has produced an Essential Eight maturity model to be used as a tool for self-assessment. This guidance shifts the focus from compliance to security, based on the individual organisations' unique needs.

The maturity model is applicable for organisations facing standard risks up to organisations that are likely to be constantly targeted by sophisticated adversaries, or otherwise operate in an extreme or high risk environment.

The maturity model is complemented by the Australian Signals Directorate's technical implementation guidance, found on the Australian Signals Directorate website.