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: Security Posture Surveys

Question reference number: 1

Senator: Smith
Type of question: asked on Friday, 2 June 2017, Hansard page 14
Date set by the committee for the return of answer: 23 June 2017

Question:

CHAIR: Turning to the clients, the Signals Directorate has been doing surveys of agencies and their security posture; is that correct?
Mr Lines: That is correct, yes.
CHAIR: How far progressed are those surveys?
Mr Lines: We do an annual survey, which looks at the implementation of the recommended strategies, their ability to repeat those profiles sensitive to the information they hold, for both the government and the public perspective, and the likelihood the agency would be targeted. They are the factors we look at.
CHAIR: You do annual surveys. So you have done one annual survey—you have done them for each year over the last 10.
Mr Lines: I could not say how long. This one is finishing today, actually.
CHAIR: Finishing today?
Mr Lines: It is due back in today—the current one, yes.
CHAIR: So 100 per cent of agencies would have been surveyed if it has been completed today?
Mr Lines: We send it out to 100 per cent of agencies; not 100 per cent respond.
CHAIR: That is interesting.
Mr Lines: We have no capacity to compel agencies.
CHAIR: To fill in a survey?
Mr HILL: We might.
CHAIR: So let's be clear: how many agencies would you have sent the survey to?
Mr Lines: I do not have that data with me. I will have to respond.

Answer:

The Australian Signals Directorate has conducted the cyber security survey since 2010, with subsequent surveys run in 2012, 2014, 2015, 2016 and 2017. The Australian Signals Directorate invited all agencies under the Public Governance, Performance and Accountability Act 2013 and, prior to 2013, the Financial Management and Accountability Act to take part.

In 2016, the survey was sent to all Public Governance, Performance and Accountability Act 2013 agencies, of which 50 responded.

This year's survey is still open, having been extended. As at 23 June 2017 it has been sent directly to 190 agencies, with the Australian Signals Directorate having received 74 responses.

The invite, and two reminders to complete the survey, were also posted to the Australian Signals Directorate's central online community portal for government Information Security professionals, OnSecure.

The Australian Signals Directorate follows up on non-respondents by contacting each agency.

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: Changes to List of Agency Risk

Question reference number: 3

Senator: Smith
Type of question: asked on Friday, 2 June 2017, Hansard page 20
Date set by the committee for the return of answer: 23 June 2017

Question:

CHAIR: If you let us know what those risks are, that would be great. And Mr MacGibbon, could you just let us know how many times the secretary's board meets? And, Mr Lines, I am curious to know—without giving away classified information—if that list of agencies that have presented a risk regularly changes how you might communicate that back to us, or if it is a consistent and stable list of agencies that present the greatest risk? Perhaps you could try to give us a sense of whether it is a moving feast from the government's point of view or whether it is a stable list of agencies. Does that make sense?
Mr Lines: Yes.

Answer:

- When assessing agencies' cyber security risk, the Australian Signals Directorate draws on highly-skilled technical expertise to determine the maturity of network security and validate the extent of implementation of the Top 4, as well as intelligence assessments, experience in responding to and remediating cyber incidents, and knowledge of malicious actor's patterns of behaviour and observed activity. The Australian Signals Directorate also considers a range of other factors when assessing an agencies' risk rating, including the likelihood of targeting by malicious actors, the impact if the system was taken offline, and privacy considerations. Risk, in this case, is not an assessment of an agency's capability to defend itself against malicious cyber activity.
- Compiling all of this information, an agencies' cyber security posture is assessed using a maturity model based on the repeatability of agency cyber security practise, their survey responses, and the assessed risk. This process identifies an agencies' level of cyber security maturity, and critically, whether their security posture is sufficiently mature to reduce the level of risk assigned to it.

Changes in the agency risk ratings

- The majority of agencies that were in the high risk category in 2014 were elevated to the extreme risk category in 2016 – a new category that was introduced the same year. None were downgraded in 2016. Extreme risk agencies are considered so important to the Government that the Australian Signals Directorate offers them highly tailored advice and assistance.
- In 2016 the Australian Signals Directorate also added some government systems of national interest to the high and extreme risk categories, as they form part of the government's digital service delivery agenda.

Joint Committee of Public Accounts and Audit

Cybersecurity Compliance – Inquiry into Auditor-General's report 42 (2016-17) – 2 June 2017

ANSWER TO QUESTION ON NOTICE

Department of Defence

Topic: Submission 2 from Ian Brightwell

Question reference number: 4

Senator: The Committee
Type of question: provided in writing
Date set by the committee for the return of answer: 6 July 2017

Question:

Regarding Submission 2 from Ian Brightwell:
a. One of Mr Brightwell's recommendations was to remove whitelisting from the mandatory list of strategies and focus on implementing a full set of ICT general controls to a level appropriate to the agency risk assessment. What are your thoughts on this recommendation?
b. Another of Mr Brightwell's recommendations is the suggestion that government Chief Information Security Officer positions not be combined within the technology delivery area and have a direct reporting line to the CEO. What are your thoughts on this recommendation? Can you please list the government agencies that have a direct CISO report to the CEO, and the government agencies that don't.

Answer:

Making whitelisting non-mandatory

1. Mr Brightwell recommended removing [application] whitelisting from the mandatory list of strategies and [instead] focus on a full set of ICT general controls to a level appropriate to the agency risk assessment.

Application whitelisting is one of eight strategies that the Australian Signals Directorate has developed to help technical cyber security professionals prioritise their efforts to mitigate cyber security incidents. Called the Essential Eight, the guidance provides practical and specific advice to defend against targeted cyber intrusions, ransomware and external adversaries with destructive intent, malicious insiders, 'business email compromise' and industrial control systems.

The Essential Eight is informed by the Australian Signals Directorate's experience responding to cyber security incidents and performing vulnerability assessments. It is also informed by the Australian Signals Directorate's penetration testing of Australian government organisations.

Application whitelisting helps prevent malicious software and unapproved programs from running.

As such, it is the Australian Signals Directorate's view that implementing application whitelisting remains one of the most effective defences an agency can undertake to defend against cyber security incidents, and the Australian Signals Directorate would not support any move to make application whitelisting anything other than mandatory.

The Australian Signals Directorate also produces the Australian Government Information Security Manual. The purpose of the Information Security Manual is to assist Australian government agencies in applying a risk–based approach to protecting their information and systems. The advice in this manual is specifically based on the Australian Signals Directorate's experience in providing cyber and information security advice and assistance to the Australian government. The controls are designed to mitigate the most likely threats to Australian government agencies.

The Information Security Manual and the Essential Eight are complementary documents, and implementing the Essential Eight does not remove the obligation on an agency to consider the remaining Information and Communication Technology controls in the Information Security Manual within the context of their own risk environment.

Therefore, it is also the Australian Signals Directorate's view that the requirement for whitelisting to be mandatory does not remove the obligation on an agency to implement additional relevant controls from the Information Security Manual to a level appropriate to that agency's risk assessment.

Chief Information Security Officer reporting arrangements across government

2. Mr Brightwell has suggested that 'government Chief Information Security Officer positions not be combined within the technology delivery area and have a direct reporting line to the CEO'. Also, the committee has requested that ASD provide 'a list of government agencies that have [the Chief Information Officer] direct report to the CEO, and the government agencies that don't (sic)'.

The Information Security Manual addresses the roles and responsibilities of the Chief Information Security Officer. Specifically, the Chief Information Security Officer sets the strategic direction for information security for their agency.

The Information Security Manual also contains Control 0714 which stipulates:

Agencies must appoint a senior executive, commonly referred to as the [Chief Information Security Officer], who is responsible for coordinating communication between security and business functions as well as overseeing the application of controls and security risk management processes.

The Whole of Government Information Security Manual issued by the Australian Signals Directorate is silent on how an agency should make such an appointment, and it is also silent on any arrangements relating to lines of reporting or additional responsibilities.

Regarding the request that the Australian Signals Directorate provide a list of agencies '..that have [the Chief Information Security Officer] direct report to the CEO, and the government agencies that don't (sic)', there is no obligation on agencies to report to the Australian Signals Directorate on their specific employment arrangements so this information is unknown to Defence.