macquarie
TELECOM GROUP

Submission to the Joint Committee of Public Accounts and Audit

Inquiry into Cyber Security Compliance

April 2017

Introduction

Macquarie Telecom Group (MTG) is pleased to have the opportunity to provide its views to the Committee's inquiry on some aspects of the cyber security stance and compliance of Federal Government agencies, in the context of the ANAO's recent audit report.

MTG is an independent, ASX-listed Australian business founded in 1992 that provides services in the telecommunication, data-hosting and cloud computing, and Government markets. It focuses solely on medium sized businesses and state and Federal government clients.

Macquarie Government and Secure Internet Gateway

MTG provides Secure Internet Gateway to more than 30 government agencies through the Federal Government's Lead Agency Gateway Program, under its Macquarie Government branded business unit.

The Lead Agency Gateway Program was introduced after a 2009 review revealed that there were more than 120 different gateways to the Internet across the Federal Government. This was creating both inefficiencies and uneven and uncertain levels of security. Weaknesses in the cyber security stance in an agency can put not only that agency at risk, but potentially create exposure for others that have interconnected ICT environments.

The Lead Agency Gateway program sought both to create efficiencies and to create a more consistent security across the Federal Government by reducing the number of gateways to eight,

each managed by a lead agency, either internally or through an outsourcer under contract. Smaller agencies were then assigned to sit behind the Gateway provided by these lead agencies. This meant they benefited from the price, terms and conditions of the lead contract, and were assured of being able to access a set of security services specified in the program and reflected in the lead contract.

The program was until recently managed by the Department of Finance, but has recently been moved to become the responsibility of the Digital Transformation Agency.

MTG submits the SIG program has been a great success in raising the cyber security stance of the Federal Government as a whole.

Combining the demand and resources of many agencies of many sizes has ensured smaller agencies have access to security technologies, provided as a service. In many cases, these smaller organisations do not have the internal resources to manage and maintain modern Internet and email firewall technologies and monitoring. Acquiring these as a services means they have available to them the same technologies deployed to protect the very largest departments.

Additionally, as the volume of traffic managed through the SIG has increased, the Security Operations Centre in MTG has been able to deploy new technologies, such as big data tools, to identify and respond to risks and malicious content.

Importantly for the purposes of the present inquiry, this program assists agencies maintain compliance with Australian Signals Directorate guidelines such as the Top 40. For example, when a piece of firewall software is update by Macquarie Government on its Secure Internet Gateway, every one of the more than 30 agencies behind the Gateway benefits immediately.

However, there are aspects of the program that Macquarie submits could be examined to consider whether even stronger security outcomes could be achieved for Government organisations and the Government as a whole.

Firstly, it has been possible for agencies nominated to sit behind one of the lead agencies to receive exemptions from the Department of Finance. The basis on which these exemptions are sought and have been granted is not visible to MTG.

Secondly, some agencies have simply not joined the program, despite being assigned to lead agency groups and without specifically being granted exemptions. The Department of Finance has seemingly not had the power and/or the willingness to compel agencies to participate in the program, which leaves some small organisations still self-supplying. It is unclear whether these agencies are doing so on the basis that their internal controls are meeting the requirements of the SIG contracts, but it should be noted that some of these agencies are relatively very small.

Thirdly, the ability of individual agencies to negotiate some of the specific services and service configurations that they receive under the umbrella SIG contract is a strength and a weakness. It means that the services can be tailored to best meet the needs of agencies, for example, by applying different rules governing Spam filtering.

However, it has also meant that some agencies have not applied the full toolkit of security measures available to them through the SIG. In some cases, this is because the legacy equipment and systems

in their internal ICT environments are too antiquated to support the cyber security applications in the SIG.

Conclusion

MTG last year commissioned the National Security College to produce a survey-based study to examine processes and awareness of cyber security in the management in medium sized agencies and businesses.

This survey found organisations of this size were struggling to manage cyber security risk, as evidenced by the lack of senior management and specialised attention it received. [i]

The lead agency gateway program provides a model of how governments can assist smaller agencies to overcome some of the difficulties created by the limited resources necessarily available to them. It allows them to benefit from demand aggregation to support a government-wide security investment, while maintaining a degree of autonomy over how their cyber defences are deployed.

However, if the framework is not carefully balanced and subject to oversight, there is a danger that smaller agencies could adopt a “compliance mentality” rather than a risk management mentality. That is, agencies might make the mistake of thinking that if they comply with the minimum requirements of the government simply by participating in the program, and, in so doing, that they meet the necessary standards to be cyber secure.

This is likely to be a mistaken belief for three reasons. Firstly, a discussed above, their internal systems need to be properly configured and kept up to date so that elements such as the Secure Internet Gateway are operating to best effect.

Secondly, outsourced elements such as the SIG are one crucial component of a cyber security technology package, but there are additional internal protections and defences that should also be employed in conjunction with the Gateway.

Finally, cyber security is uniquely fast moving and it is important that agencies are aware that the threat vectors are constantly changing, demanding responses if the level of security is not to be compromised.

The Lead Agency Gateway program provides a means for agencies to gain insights into emerging and changing threats, and learn from each other and from the Gateway operator.

If agencies do the minimum they need to do to comply with the policy rules, they are unlikely to be keeping ahead of the threat landscape.

But if the program is seen as a platform providing infrastructure and insights that can be shared and evolved, the “weakest link” problem can be materially reduced.

MTG is happy to provide further information if the committee believes it would be helpful, including through providing evidence to the committee in public hearings.

Please contact: David Forman
Senior Manager Industry & Policy
[redacted]

[i] Weakest links: cyber governance and the threat to mid-sized enterprises
http://nsc.anu.edu.au/news-events/news-20161102