aamri

Association of Australian
Medical Research Institutes

SUBMISSION TO AUSTRALIA'S 2020 CYBER SECURITY STRATEGY NOVEMBER 2019

Contact:
Professor Jonathan Carapetis AM
President
Association of Australian
Medical Research Institutes
ABN 12 144 783 728

PO Box 2097
Royal Melbourne Hospital VIC 3050
president@aamri.org.au
www.aamri.org.au

About AAMRI

The Association of Australian Medical Research Institutes (AAMRI) is the peak body for medical research institutes (MRIs) across Australia. Our 54 members undertake over one-third of all government funded medical research and work on a broad spectrum of human health issues. Their research ranges from fundamental biomedical discovery through to clinical research, including clinical trials.

Introduction

Medical research can involve collecting and analysing vast quantities of sensitive patient data. It is vital that this data is stored securely and can only be accessed by authorised researchers as it can contain commercially-sensitive or sensitive patient information. Any breaches could potentially undermine community confidence in the medical research sector.

The greatest difficulty facing large parts of the not-for-profit sector, which includes most of the medical research sector, is finding the resources required to deal with growing cyber security challenges. As the level and sophistication of the cyber security threats increases the greater resources that are required in response. The availability of appropriate resources and expertise will continue to be a challenge as the sector does not have level of financial resources to draw on that large multi-national companies do, but inevitably faces a similar level of threat.

The strategy should put forward practical recommendations that help ease the financial burden cyber security threats are placing on the not for profit medical research sector, as well as increase the technical expertise within the sector. This can include helping to facilitate the sharing of best practice, as well as providing free or low cost access to expertise and resources. It can also include providing a framework to help the sector identify best practice in preventing cyber security incursions.

AAMRI would like to make the following specific recommendations:

Recommendations

ACSC to provide ongoing advice and services

The role of the Australian Cyber Security Centre (ACSC) should be continued and its resources enhanced in recognition of growing cyber-security threats. The ACSC should provide ongoing security advice, provide recommendations or endorsements for cyber education standards, awareness, incident response and escalation capabilities. Specific divisions with the ACSC that focus on particular needs of the medical research sector, as well as the broader not-for-profit and research sectors.

Cyber security framework/standards

The strategy should recommend a single Australian cybersecurity framework or set of standards. There are at present too many frameworks and this creates inconsistencies and confusion for organisations. This Australian based framework could be tailored according to organisation size, industry and maturity level to allow organisations determine how best to

comply. Ideally, this framework would provide guidance on how to achieve and align with good security practice. It would be worth considering developing something similar to the UK's Cyber Essentials.[1]

Register of approved security products

A register which contains details of approved, endorsed or banned software and hardware security products should be maintained. Approved products may have differing ratings based on their capabilities and include details of banned products that are known to have security vulnerabilities. The register could potentially provide endorsements in a similar way to C-Tick.[2]

[1] See https://www.cyberessentials.ncsc.gov.uk

[2] See https://www.ipaustralia.gov.au/tools-resources/certification-rules/614687