Submission to the Serious Data Breach Notification Consultation

(Consultation closes 4 March 2016 — please send electronic submissions to privacy.consultation@ag.gov.au)

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	**FireEye** Phil Vasic**,** Regional Director - ANZ
Contact details *(one or all of the following: postal address, email address or phone number)*	[contact details redacted]

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? NO

Your submission

Commercial and Administrative Law Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

By email: *privacy.consultation@ag.gov.au*

Friday 4 March 2016

Submission to the Serious Data Breach Notification Consultation

FireEye supports Serious Data Breach Notification as outlined in the draft *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*. We also welcome this opportunity to share our experience as international experts in cyber-security.

Since its formation in 2004, FireEye has become one of the world's leading providers of cyber security solutions. Applying our technology, intelligence, and expertise we help protect over 4,400 customers in 67 countries, including more than 680 of the Forbes Global 2000, by giving them the means to respond as quickly as possible to advanced cyber attacks. Our Mandiant Consulting group has responded to most of the major breaches in the headlines, including many that go unreported.

Today Australian businesses face numerous cyber threats, including cyber hacktivists, cyber criminals and sophisticated, state-sponsored threat groups. The latter group poses the most significant threat to Australia's economy, public safety and national security. FireEye has detected at least six Advanced Persistent Threat groups targeting organisations in Australia.

In this threat landscape, data breaches are inevitable, and they occur more often than many Australians may think.

Australia faces two significant challenges on the road to strengthening its cyber security posture: awareness, and disrupting threat actors. Breach notifications significantly assist with these two areas.

Outside of Australia's largest organisations, awareness about the threats posed by cyber threat groups and defensive strategies is limited and hinders adoption of technology and expertise to fend of advanced attacks. When organisations disclose they have been targeted and that they contained the breach, they significantly raise awareness of this issue.

The second major challenge is disrupting threat actors. When a cyber threat group successfully compromises a network, we often observe the group then use the same tools, tactics and procedures to conduct a subsequent compromise against another organisation. These organisations are often unaware of the vulnerabilities exploited previously, and so they remain vulnerable. Attackers can also reuse credentials across multiple networks.

However, when organisations disclose breaches and share this intelligence, other organisations are better able to defend themselves against advanced attacks. Shared intelligence is one of the best weapons in our arsenal against cyber attackers, and this legislation aids that.

Measures outlined in the draft *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* may also encourage business and industry to further enhance their cyber security posture, something which helps everyone in the fight against cyber and online crime.

Phil Vasic
Regional Director - ANZ