21 June 2014

Dr Carolyn Patteson
Executive Manager
CERT Australia
3-5 National Circuit
Barton ACT 2600

Prof John McMillan
Australian Information Commissioner
Office of the Australian Information Commissioner
Box 5218
Sydney NSW 2001

An open letter regarding “use” versus “disclosure” and a lack of effective controls for off-shoring.

Dear Dr Patteson and Prof McMillan,

As an information security professional I am writing to you, in your respective advisory roles regarding the protection of information, to inform you of the development of the proof-of-concept application *Through Glass Transfer (TGXf).*

The TGXf application demonstrates that:

- Any file that a user can read (*use*) can be downloaded (*disclosure*) via the screen, and;
- There are currently no technical controls to mitigate the proof-of-concept implementation.

Although technical vulnerability is constantly evolving (the proof-of-concept is defeatable), there is no foreseeable mitigation to the class of storage based covert channel vulnerabilities described and the general approach taken. This has the most impact when considering Australian enterprises that provide off-shore (overseas) partners with access to Australian data and processing infrastructure on-shore.

In technical terms, TGXf encodes binary data into packets that can be displayed on the screen of one computer and then captured (via camera) on another, where they are decoded and the data is stored on disk. By doing this, TGXf turns any display surface into a binary data transfer interface and bypasses enterprise security strategies (including defence-in-depth strategies).

When the revised Australian Privacy Principles came into effect in 2014 I wrote the proof-of-concept application and the supporting documentation (draft enclosed) in order to effectively communicate both the technical risk and the new legal implications.

I refer you to the *Australian Privacy Principles guidelines (Privacy Act 1988)*[1] - version 1.0, February 2014.

An Australian organisation (APP entity) that *holds* personal information [6.6], and makes that personal information available for *use* [6.8] but not *disclosure* [6.11(b)] to an *overseas recipient* [8.5] is accountable [8.1] for ensuring that the overseas recipient does not breach the Australian Privacy Principles [8.2]. Personal information is disclosed when the Australian organisation *releases the subsequent handling of the information from its effective control* [8.8], which includes *disclosure* through *unauthorised access, if it did not take reasonable steps to protect the personal information from unauthorised access* [8.10]. The *reasonable steps* include *implementing strategies to manage*, amongst other things, *ICT Security*, *data breaches* and *regular monitoring and review* [11.8].

Of the *six security considerations* [11.10] set out in the Australian National Privacy Principles, TGXf would appear to directly enable:

- *interference* when an overseas recipient instigates change to a computer system that *leads to exposure of personal information* [11.13], and;
- *unauthorised disclosure* when an overseas recipient *releases the subsequent handling of that personal information from [the Australian organisation's] effective control* [11.18].

This issue is not limited to Australia. Any modern legal or regulatory frameworks that rely upon the same distinction for *use* and *disclosure* to govern information confidentiality will have some business impact from the release of the TGXf software. One example is the United States' Health Insurance Portability and Accountability ACT (HIPAA).

In that regard, I have published an information site online to draw the attention of the information security industry to the problem (http://thruglassxfer.com/). I will also be presenting directly to the industry on the topic, at the COSAC/SABSA conference on Tuesday the 30th of September 2014 in Dublin.

I strongly urge your organisations to consider the technical and legal implications of the material enclosed here-in.

Sincerely,

Original signed by

Ian Latter

Enclosures (1): *ThruConsoleXfer (TCXf) White Paper – Midnight Code – v1.0 (Draft)*.

1 http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf