office of the privacy commissioner
new south wales

Own motion inquiry / investigation

The University of Sydney

Privacy and Personal Information Protection Act 1998 **June 2011**

This report is placed in the public domain pursuant to section 36 (2) (h) of the Privacy and Personal Information Protection Act 1998 and made under the powers of section 36 (2) (l) of that Act.

Introduction

In January 2011 there were media publications about the security of the University of Sydney's website. In particular, on 20 January 2011 allegations were raised in the media that student personal information was accessed in an unauthorised way on the University of Sydney administrative website.[1] Additional information that University students provided indicated that any person could enter a student number on the University's website address line on their web browser and access that student's records without entering a password. The personal information included the student's name, address, subject enrolled in and fees payable.

The NSW Acting Privacy Commissioner commenced own motion enquiries under section 36(2)(l) of the *Privacy and Personal Information Protection Act 1998* (PPIP Act).[2]

The issue of concern was the possible contravention of section 12(c) of the PPIP Act, which obliges public sector agencies that hold personal information to ensure:

> *"that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse…"*

The course of the investigation

The January 2011 "flaw"

In response to the Acting Privacy Commissioner's enquiries the University advised that it was informed about the issue on 19 January 2011. Its response to the flaw was that:

- On 20 January 2011 it disabled that part of its website that allowed viewing of the self-serve areas of the student records,
- Sent a communication to students about the flaw,
- Rectified the flaw, and
- Engaged a security consultancy company to independently test and verify the resolution of the flaw.

The University also advised that the consultancy company tested the website for further potential flaws in the programming in the week to 27 January 2011 and they identified one other potential risk for information leaks.

A security enhancement to deal with the risk was deployed onto the system on 29 January 2011.

[1] Sydney Morning Herald 20 January 2011 – http://www.smh.com.au/technology/security/uni-failed-to-secure-vulnerable-web-data-20110119-19wqf.html

[2] Section 36(2)(l) empowers the Acting Privacy Commissioner to investigate any privacy related matters that the Acting Privacy Commissioner thinks appropriate.

The February 2007 "flaw"

The media reports also referred to a failure by the University to address the same information security risk when it was first reported to the University in 2007.

The University's response to the Acting Privacy Commissioner's enquiries was to the effect that:

- A similar flaw was identified in February 2007. The University repaired the code error that allowed unauthorised access to student records on the University's website by way of introducing a security "patch."
- When updates to the software were made later in 2007, the "patch" was not re-introduced into the system due to an oversight.
- The University has since developed a software control system that mitigates the risk of software component parts being listed on the software code repository without all of the updates to that software (including security patches).

In a further briefing provided to staff of this Office the University explained that the flaw in January 2011 was not an outcome of the failure in 2007 to re-install the security "patch."

Discussion

Digital and web-based technologies obtain an increasingly powerful place in our relationship with service providers, including public sector agencies, because they enhance opportunities for our prosperity, social inclusion and convenience. Additionally, these technologies allow significant savings to be made to administration costs because they promote a more efficient management of customer transactions and other communications.

Increasing the uptake of web-based facilities requires public sector agencies to maintain their clients' confidence that personal information will be protected, whether it be from intentional or accidental hacking into their databases.

Small businesses and individuals, who have limited capacity at implementing effective information protection programs, may at times be unknowingly operating compromised online systems.

Large corporations and public sector agencies have available to them dedicated resources in the form of:

- intrusion detection systems
- sophisticated firewalls
- IT security staff
- chief information officers
- chief technology officers.

This entitles the community to expect from them higher rates of awareness of information security risks and vigilant breach prevention programs.

Section 12 of the PPIP Act imposes a positive obligation on the University to take all reasonably available security measures to ensure a student's personal information recorded on the University's web-accessible records through the many transactions students complete on-line does not become available to unauthorised persons and bodies.

Determining what is reasonable requires a balancing exercise that takes into account the following two factors:

- On the one hand, the facilities and specialist staff available to the University regarding the management of its web-based student transaction systems, and
- On the other hand, the awareness the University should have that it holds sensitive personal information about thousands of people, which, if it fell into the wrong hands, could lead to potential physical[3] and financial threats to them,[4] or cyber stalking.[5]

[3] Where disclosure of one's address may result in physical threats to them.
[4] Where disclosure of names and dates of birth may result in identity fraud and financial loss to them.
[5] Where disclosure of a student's private email address may result in unsolicited and/or inappropriate emails potentially escalating to other types of threats and other escalation.

The information leaks in January 2011 resulted from what can be simply described as a programming error that allowed access to student records directly from one's web-browser without the need to enter a password.

Balancing the two factors mentioned above the Acting Privacy Commissioner is of the view that, with appropriate testing, the flaw was avoidable and that the University had not taken reasonably available steps to avoid the risk that the leaks would eventuate.

Conclusion

The Acting Privacy Commissioner finds that the University did not meet its obligations under section 12(c) of the PPIP Act in respect of the student personal information leaks in January 2011.

In light of the steps the University took to fix the problem, as noted above, and further advice it has provided about the introduction of security reviews and testing of the penetration potential of various information systems, the Acting Privacy Commissioner considers that the University responded to being informed of this breach of security with urgency and effectiveness. The Acting Privacy Commissioner considers that there is no need to take further action in relation to this investigation.

The Agency subject of this Inquiry / Investigation has been provided with a draft report and has consented to the publishing of this final report by the Acting Commissioner.

John McAteer
Acting Privacy Commissioner
Information and Privacy Commission

28 June 2011