UNIVERSITY OF HAWAI‘I SYSTEM REPORT

REPORT TO THE 2009 LEGISLATURE

Report on Security Breach
at the University of Hawaii, Kapiolani Community College
April 15, 2009

HRS 487N-4

May 4, 2009

Subject: Report to the Legislature on Security Breach at the University of Hawaii

Date of Breach: April 15, 2009
Location of the Breach: Kapiolani Community College (KCC)
Nature of the Breach: Computer with Access to Sensitive Information Infected with Malware

Incident Description:
On April 15, 2009, KCC information technology (IT) staff was notified of a computer behaving strangely. The computer is used to process KCC financial aid applicants and while no sensitive information was stored on that computer, the computer was used to input student's personal information into the US Dept. of Education's financial aid website. The computer was also used to access a file server that is used to store personal information used for financial aid processing.

The responding KCC IT staff began scanning the computer to check for malware and found the computer to be infected with many different types of malware. Further investigation revealed that one malware in particular was described by an anti-virus company as having the capability to "steal user's sensitive data and communicate with specified internet websites". However, while trying to determine if the malware was active and had access and/or transmitted any sensitive information, the computer crashed and was unable to boot up again. KCC IT staff continued to try to access the hard drive and recover any information but were unsuccessful. Their attempts to recover more information spanned several days.

On April 22nd, a computer forensics consultant was retained to investigate further. He was off-island and was unable to pick up the hard drive until April 24th. His subsequent investigation revealed that the malware was installed and active but he was unable to find any evidence that any sensitive information was accessed or transmitted out of the computer.

Reports have been filed with the Honolulu Police Department and the FBI but neither law enforcement agency has requested delaying of notification.

Approximately, 15,486 individuals have been identified as being "at-risk" and notifications are being sent to these individuals at the postal mailing addresses on record.

A copy of the notification letter is included as Attachment A.

KCC has developed their Action Plan to prevent any recurrence of these types of incidents. A summary of this plan is included as Attachment B.

ATTACHMENT A

UNIVERSITY *of* HAWAI'I®
KAPI'OLANI
COMMUNITY COLLEGE

Office of the Chancellor

April 30, 2009

Dear «First_Name» «Last_Name»,

We are contacting you to inform you of a recent incident that may put you at risk for identity theft and to provide guidance on how you can protect yourself from financial harm associated with this and other potential risks.

On April 15th, a computer that had access to personal information of financial aid applicants was found to be infected with malware. The computer was removed from the network immediately and a forensic investigation initiated. A specific piece of malware was found on the computer that is believed to have the capability to "steal user's sensitive data and communicate with specified Internet websites."

The infected computer did not itself store sensitive information, but had access to a departmental server used for financial aid processing. The server files included information necessary for financial aid processing including name, address, phone number, date of birth and social security number. While our forensic investigation provided no evidence that any sensitive information was actually accessed by the infected computer, neither did it rule out that possibility. Therefore, we are providing this notice to all individuals whose personal information was on the server and who might be at heightened risk if unauthorized access occurred.

Those receiving this notice and identified as at risk include Kapi'olani CC students who applied for or were granted financial aid any time between January 1, 2004 and April 15, 2009, and prior loan borrowers. If you supplied parental information on your financial aid forms, your parents are also at risk.

Again, there is no evidence that your personal information was actually accessed. And no credit card, debit card or bank account information were stored on the server or placed at risk. Nonetheless, Kapi'olani Community College is taking this opportunity to urge any potentially affected individual to take routine protective measures against identity theft. We suggest that you:

- Obtain and carefully review your credit reports. You can order free credit reports from all three credit agencies at http://www.annualcreditreport.com or by calling 877-322-8228.
- Review your bank and credit card statements regularly and look for unusual or suspicious activities.
- Contact appropriate financial institutions immediately if you notice any irregularity in your credit report or any account.

If your identity or accounts have been compromised, you may take actions such as requesting refunds, closing accounts, and placing your credit records in a state of "fraud alert" or "freeze." More specific instructions about these options protecting yourself against identity theft and what to do if it happens to you is available at http://www.kcc.hawaii.edu/object/idalerts.html

Kapiʻolani Community College has taken steps to ensure that a similar incident does not recur. While University of Hawaiʻi policy calls for protecting computers with password-protected accounts and use of anti-malware software, the infected computer contained an older version of the security software, which is how the compromised computer is believed to have been infected. The college will be implementing additional security measures including minimizing the storage of sensitive information, employing encryption, verifying that computers used to access sensitive information are up-to-date with the latest version of anti-malware software and re-training all staff in safe computing practices. While there was no malice on the part of any college employee, the Honolulu Police Department and FBI have been notified of the incident and asked to investigate any potential criminal activity related to this incident. The university is also conducting an internal investigation to prevent similar situations from occurring and to improve our operational procedures.

We apologize for any inconvenience this incident has or may cause. If you have any questions or need additional information, you may call (808)734-9522 or go to http://www.kcc.hawaii.edu/object/idalerts.html Updates will be made to this website as new information becomes available.

Sincerely yours,

Leon Richards
Chancellor

ATTACHMENT B

CENTER FOR EXCELLENCE IN LEARNING,
TEACHING AND TECHNOLOGY
KAPI`OLANI COMMUNITY COLLEGE

ACTION PLAN: SUMMARY

In addition to the notification of affected individuals, KapCC has taken or plans the following actions:

- Ensure currency of anti-virus software on staff computers
- Evaluate data storage practices of financial aid office and institute changes as needed
- Evaluate and implement additional appropriate security measures to minimze future risks including but not limited to:
    - Consider additional layers of network security to prevent external attacks
    - Encryption policies and procedures for employees who handle sensitive data
    - A server dedicated solely for storage of sensitive data
    - Password reset policies
- Provide expert security training to KapCC employees