Ohio University Coping with Information Breaches

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In May 2006, Ohio University (OU) announced that a “security violation was discovered on Monday, April 24” in which “The computer system contained biographical information for more than 300,000 individuals and organizations, including the Social Security numbers of more than 137,000 individuals” was penetrated by unknown persons. <http://www.ohio.edu/outlook/05-06/May/454n-056b.cfm> A later report indicated that another breach exposed the Social Security numbers and also health records of “60,000 people including all current students as well as some school faculty.” <http://news.com.com/Ohio+University+suffers+security+breaches/2100-7349_3-6071505.html>

Adam Dodge, a graduate student in Norwich University’s MSIA program, recently sent me a summary of the consequences of these breaches and others at the unfortunate school. As usual, I have edited the contributor’s original material for publication in this newsletter.

* * *

It seems that OU has begun to receive heated backlash from alumni regarding the recent information breaches suffered by the university. A June 12, 2006 article in the _Athens News_ by Jim Phillips reviews alumni reactions. <http://www.athensnews.com/issue/article.php3?story_id=25220> [Unfortunately, the newspaper’s Web site was offline when we were checking URLs; the article is mirrored at <http://www.merit.edu/mail.archives/netsec/msg01521.html>]. Reactions include disgust (some of it expressed in vulgar language) at the loss of reputation for OU; promises to stop any future donations; possible class action lawsuits; and a proposal from one alumna to bill OU for the time she has spent checking her credit reports.

These reactions raise interesting questions. What are the legal liabilities and responsibilities of an organization that exposes personal information to criminal hackers? Like many other organizations, OU has set up a hotline and several University Web sites with detailed instructions on steps individuals should take if their information was exposed <http://www.ohio.edu/datatheft/personalinfo.cfm>, how to protect your Social Security number <http://www.ohio.edu/datatheft/ssn.cfm>, and steps to take if you have been a victim of identity theft <http://www.ohio.edu/datatheft/identitytheft.cfm>. However, the help offered by OU on these Web pages is informational only. OU offers individuals exposed to possible identity theft are no monetary assistance in maintaining a watchful eye on their credit reports. Nor does OU offer any personal assistance in dealing the consequences of identity theft. Instead, OU recommends that individuals use free yearly credit reports and place an extended alert on their credit report, but only if they have already become victims.

These recommendations may be inadequate. Yearly credit reports are too far apart to catch and mitigate identity theft. OU recommends ordering free reports from each of the three major reporting companies at intervals throughout the year; however, even four months between reports offers identity thieves time to ruin their victims financially and cause immense damage to
their credit ratings.

Another response is to place an extended alert on one’s credit report, but that lasts only seven years. Personal information such as the Social Security Number can last forever unless one goes through the difficult process of getting a new one. How much good is seven years of protection for a 23-year-old college alumnus who could live for another 70 years?

Readers should consider their own organization’s use of Social Security Numbers, posting of unencrypted data on Web servers, and plans for responding to a breach of confidentiality involving stakeholder data. Adam and I think it is especially important to consult corporate counsel in planning such policies and responses. OU’s documents can provide a start, but we all have a lot to do to cope with these issues in ways that are appropriate for our own situations.

But what won’t do is to face such incidents without a contingency plan. As the old maps used to say about unknown lands thought to be dangerous, “There be dragons.”

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 Adam Dodge & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.