PREPARE FOR DATA COMPROMISE

By M. E. Kabay, PhD, CISSP-ISSMP

Basic principles of information assurance and of security in general move us to establish mechanisms for defending valuable resources, methods for testing our mechanisms and then continuous process improvement to keep the mechanisms under revision to meet changing needs. We also need plan for failures.

Business continuity planning and disaster recovery planning cope with longer-range effects of computer security incidents; incident response plans cope with the immediate aftermath of a security breach. Unfortunately, the year 2005 has provided more examples of the need for such response plans than any good-hearted person would wish on the victims. Here are some pointers to cases of unauthorized data disclosure and system penetration. If you don’t have response plans in place, ask your upper managers what your organization would do if something like these disasters happened to you.

UNAUTHORIZED DISCLOSURES

In January 2005, Harvard University was discovered to be leaking data through a badly configured Website. Confidential prescription drug purchase information about employees and students was easily available to strangers in violation of Health Insurance Portability and Availability (HIPAA) regulations. < http://tinyurl.com/4uk7s >

In February, the Australian Website for Acer computers revealed details of recent orders to other shoppers including contact and delivery addresses (but not credit-card numbers). < URLs no longer on the Web >

Also in February, a vulnerability in the Mailman open-source program for e-mail lists was used to steal the password file of the Full Disclosure discussion group. < http://tinyurl.com/bc9or >

ChoicePoint allowed criminals to buy accounts; the thieves then stole credit-reports about 145,000 consumers. ChoicePoint officials themselves discovered the fraud by noticing abnormal patterns of searches carried out
by the identity thieves. The case came to light in February in part because of California's stringent new laws requiring data subjects to be informed of possible unauthorized disclosure of their data. <http://tinyurl.com/4g9vf>

Carnegie Mellon University, home of the highly respected Software Engineering Institute (SEI) and Computer Emergency Response Team Coordination Center (CERT-CC), discovered in April that data about 5,000 of their alumni, current graduate students, applicants and employees had been exposed to unauthorized access. <http://tinyurl.com/d82bh>

In May, Purdue University, home of the Center for Education and Research in Information Assurance and Security (CERIAS) reported the third security breach of 2005 allowing unauthorized access to confidential records of faculty and students. This time, over 11,000 people were informed of possible compromise of their personal information, including Social Security Numbers (SSNs). <http://tinyurl.com/cbeex>

In July, applicants to the University of Southern California discovered that the application data of several hundred thousand other applicants were exposed to view online. <http://tinyurl.com/dhz4o>

Cisco Systems left user passwords exposed on their Website and closed the hole the day it was reported in August as well as resetting all the passwords for its users. However, spokespeople for the company said that no sensitive data were compromised by the breach of security. <http://tinyurl.com/agbdy>

In December, the _Salem News_ reported that student psychological records including detailed case reports were left unprotected on their school's Web site for at least four months. <http://tinyurl.com/cr97s>

***

So what would you do if something like these incidents happened at _your_ site? Are you ready to handle

* the technical issues: identifying the problem, collecting and preserving evidence, measuring the extent of the damage and repairing the breach?
* the legal issues: identifying the victims, complying with contractual and other legal obligations to inform and protect them against the possible consequences of unauthorized disclosure of personal data, coping with psychological trauma and damaged morale, and deflecting personal lawsuits?

* the public-relations side: having a single spokesperson who has the facts, telling the truth, responding promptly to stakeholder concerns and having public information available in an appropriate way?

* * *

Next time, I'll look at some of the highly-visible penetration cases that occurred in 2005.

Copyright (c) 2006. All rights reserved.