



Cyber-Security Newsletter

April 2009

STEPHEN F. AUSTIN STATE UNIVERSITY

INFORMATION TECHNOLOGY SECURITY OFFICE

Data Breaches

What is a Data Breach?

A data breach generally refers to instances where information has been subject to unauthorized access, often where the information is lost, stolen, or hacked into. This is of particular concern when that information is private, sensitive, or confidential. Organizations and individuals are responsible for protecting the information in their care, so proper safekeeping of this data is vital. Failure to do so can result not only in a breach but also in damage to reputation, significant fines or loss of revenue, and other negative consequences.

Data breaches occur all too frequently, and they can occur in large or small organizations in both the public and private sectors. The scope of this issue can be evidenced by the fact that more than 254 million records nationwide have been involved in breaches since February 2005. This figure represents only those that have been reported, so it may reflect only a portion of the actual occurrences. This is an issue that everyone must be aware of and take steps to mitigate.

We must also recognize that data manipulation is a potential threat. If we cannot trust the integrity of our data and know that it has not been altered inappropriately, our ability to carry out our mission and serve our customers becomes impaired.

Some examples of data that must be protected include:

- Customer or employee information with names, addresses, Social Security numbers, credit card numbers, passwords, and other identity-related information
- Intellectual property
- Financial information
- Health records of individuals

How is Data Compromised or Disclosed?

Attempts by hackers to steal names, Social Security numbers, credit card accounts, and other information are one method of obtaining data. Attackers may use social engineering, phishing, or other similar attempts to gain access. These activities can translate into very large sums of revenue for those in the organized crime world. While very sophisticated techniques are sometimes used to steal sensitive data, one of the most common threats comes from within the organization itself. According to Deloitte's 2007 Global Security Survey, 65% of respondents reported repeated external breaches. Of those incidents, 18% stemmed from unintentional data leakage. The report also indicates that some of the surveyed data breaches went undetected for extended periods. According to the [2008 Data Breach Investigations Report](#) by VerizonBusiness, 83% of attacks were not highly difficult and 87% of breaches were considered avoidable through *reasonable controls*. A full report is available for download. The loss or theft of data is not limited to electronic data loss or computer hacking. Other possibilities include physical loss of hard copy documents, theft or loss of laptops, tapes and flash-drive devices, or improper disposal of hardcopy documents.

Email your topic suggestions, questions, and comments to itsecurity@sfasu.edu



What Can I Do To Minimize Risk?

Breach Notification Laws are currently in place in forty-four states and the District of Columbia. They govern the notification of an individual whose personal information has or may have been disclosed.

Organizations and individuals must take proactive measures to minimize the risk of data breach. Everyone in an organization has a role in protecting information. The following examples offer advice on how to help prevent data disclosure:

- Follow your organization's cyber/information security policies.
- Know how your organization has classified information, and adhere to the appropriate controls in place.
- Follow proper procedures for the destruction or disposal of media that contains sensitive data.
- Participate in security awareness training.

Remember, cyber security is everyone's responsibility. Don't be the weakest link in the chain.

FTC—Red Flag Rules Enforcement to Start May 1st

Numerous laws and regulations control how organizations handle and protect sensitive information. Federal Trade Commission—Red Flag Rules went into effect January 1, 2008 but enforcement will begin on May 1st. The new regulation is intended to protect consumers from identity theft. Even though data security measures are in place, the Red Flag Rules picks up where technological measures leave off. It requires employees to be on the lookout for signs that identity theft is occurring. Since SFA extends "credit", the University is required to comply with the new regulation.

To comply, the University recently approved the Identity Theft Prevention policy. Several departments such as Human Resources, Student Financial Services, Office of the Registrar, and Admissions will be impacted by the Red Flag Rules. Employees must know how to identify, detect, and respond to suspected or real incidents of identity theft. These incidents may come to light through the presentation of suspicious identity documents or personally identifying information or through frequent address changes. Procedures within impacted departments must be developed to comply with the Identity Theft Prevention policy.

<http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>

Last Words—Conficker Follow-up

Virtually nothing happened on April 1st. The writers of the worm cleverly programmed it. All the hype focused on a payload to occur. However, infected machines set up peer-to-peer networks and were used to download code. Today, the infected machines are downloading the scareware program "SpywareProtect2009" through a peer-to-peer network. This scareware program performs the same way as the "AntiVirus 2009" program that displays bogus virus infection messages on the PC.

Nationwide there is a consortium working on Conficker solutions. The Conficker Working Group has implemented a coordinated, global approach to combating the Conficker worm. The working group has also developed a simple website to help individuals test for a possible Conficker infection. The test is based on the fact that Conficker blocks access to known remediation sites and tools. Basically, if you are not behind a proxy, and if you can't see one of the upper images in the test site, you need to worry. This is a simple, though not perfectly thorough, means of detection.

Conficker test page: http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

Powered by:

Brought to you by:



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM



MS-ISAC