Global Information Assurance Certification Paper

Communication Vulnerability - Compromise
Millie Furs
November 14, 2000

Security training is necessary at all levels in the corporate world: compromise of confidentiality, even at the lowest security level, can grow epidemically, and is not tolerable. Modern industry (healthcare, technology, and finance) must reduce risk. Every undereducated employee is an open portal. The probability that those openings cause exploitation is magnified when social nonchalance is combined with human error.

Firewalls, Tripwires, Honeypots and other perimeter devices cannot protect a network from social carelessness. These resources can protect or reduce the number of attacks that originate from the internet, but they cannot protect your system from insiders who do not preserve the integrity of computer security. Most incidents originate with a company's own employees. Some employees procure unauthorized sign-ons in order to relieve their workload, while others are more malicious.

Confidentiality, integrity and availability are key assets to a company's efficiency. These assets, however, need protection due to the increase in threats that originate from disgruntled employees. The internet has given past employees access to unprotected files, and attacks from present employees are untraceable without secure passwords. Confidentiality, integrity, and availability are key to a stable computer work environment. Threats, vulnerabilities and compromise are the precursors to compromise. It is in the best interest of every employer to inform their employees as to the need for these precautions because one breach in security can destroy a business. Lawsuits are another financial threat that can arise due to vulnerabilities.

(This provides another hurtle for hospitals)
Confidentiality in the health care field is the basis for good security practices. A company's financial advisors do not release potential buy-outs: litigation protects that information. Law protects the disclosure of medical records in the same way. Every patient who comes through the hospital doors assumes that their medical records will remain confidential. Patients expect, by right, to have their records kept secure and confidential. They assume that all information—from admission to final diagnosis and discharge—is secure and confidential, yet their information is often vulnerable due to the lack of appropriate attention given by hospital staff. If this information leaks through the hospital's security, the results could be catastrophic.

Often, employees assume a social environment in the workplace. This attitude can prove to be detrimental to the employer's interest as the court has held that personal health information is of the most sensitive nature. Any worker in any type of company can walk by a computer left on by the employee who is now on break. The lack of a password protected screen saver causes a breach of security for the information on the screen. What if it had something to do with this employees' family or neighbor? Would he be

obligated to tell the neighbor that the deal the two companies were planning had fallen through?? Or should he let them buy the information from him-and perhaps sell them the info needed to save the deal?? http://www.houstonchronicle.com/
This article is on the last page.

I feel the key to help prevent these types of issues are Training. Years ago when company's were first using PC's, everyone had access to all types of information. There were no viruses, worms, Trojan horses, or for that matter security threats. As the business world has grown and changed with the times, businesses rely on PC's to do their every day work.

Each employee, no matter what the job title is, should go through a computer awareness program-and it should be repeated on a yearly basis. Employees should be made aware of how to pick good passwords, never use your name, initials, SS#, or title. Good passwords are made of phrases (using a 1 for an l or I etc). You should use upper and lower case, alphanumeric along with special characters. Employees should be taught how often their passwords should be changed, (every 30 to 90 days) and how to keep your password secure. You should never write your password down or leave it on your desk where someone can see it. Worse yet, never post it on the P.C. because you keep forgetting it. Employees should know that when their employment is terminated, their passwords to all systems will be deleted or inactivated immediately. As shown in the article, http://www.newschannel5.com/ type (Wynette in the search), and you will see how someone used a vulnerability, compromised a system, and the companies integrity as well.

How did a research specialist use a former physicians password to gain access to the network?? Shouldn't the Information Services Department have been notified that the physician was no longer practicing there?? What were the polices and procedures of this particular company, for granting applications or inactivating/deleting passwords?? Was the procedure thought through, so that H.R. can notify departments of name changes, new hires, terminating employees? Did they understand the implications and seriousness, that could happen when there is a disgruntled employee, whose password is still in effect?

If people do not have the proper training, right from the beginning, then how can you deal with a compromise of the systems?? Communication goes a long way in solidifying a company. Training and communication are your basics for making a company thrive. If employees are not aware of security, passwords, confidentiality then how can the employer expect the employees to have any type of PC awareness?

Sited Sources

http://www.newschannel5.com "8/24/00Man admits he sold Wynette's Medical Records"
Tom Hanks 10/6/2000 URL:

http://www.newschannel5.com/cgi-bin/search.pl
http://www.hipaadvisory.com/live/index.htm
www.google.com/
www.houstonchronicle.com URL:
http://www.chron.com/content/archive/index.mpl
http://www.sans.org/momgate Introduction to the Sans Level One Introduction & Foundation URL:
http://www.sans.org/momgate/?a=VkBD8yF8jba&S=1.1
Deborah Tedford "Girl with HIV sues, says privacy violated" Houston Chronicle 10/4/2000 by Deborah Tedford URL:
http://www.google.com/search?q=deborah+tadford&hl=en&lr=&safe=off
-the article is listed below as you now need a password to enter their archives.

Oct. 4, 2000, 12:16AM
Girl with HIV sues, says privacy violated
Royal ISD denies disclosing condition
By DEBORAH TEDFORD

A middle-school student who is HIV-positive was ridiculed and harassed by fellow students after the principal used her as an example in a lesson about safe sex, according to a federal lawsuit.
Royal Middle School Principal Patsy Ann Parker warned students they would end up like the plaintiff if they didn't practice safe sex or abstinence, the lawsuit alleges.
The suit identifies the girl and her mother by pseudonyms, Jane Doe and Mary Doe. Their identities are filed under seal with the district clerk's office in Houston.
Tom Tasma, superintendent of the Royal Independent School District, declined to comment on the allegations. But according to the petition, the district has denied Parker made the disclosures.
Parker did not return a call seeking comment.
The girl and her mother are asking a federal judge to assess the district fines of $1,000 per disclosure for the negligent release of medical information and $5,000 per disclosure for the willful release of HIV-test results. The family is also seeking $125,000 in actual and punitive damages.
Attorneys for the family allege Parker violated the girl's right to privacy under the federal Family Education Rights and Privacy Act. That law guarantees that records maintained by schools, including health records, may not be disclosed without prior consent of the student or parent.
Additionally, the suit alleges the girl's constitutional rights to privacy and equal protection were violated.
According to the lawsuit, the girl was a student at Royal Middle School in Brookshire when a teacher approached her with questions about her HIV

status in September 1998. The teacher allegedly told the girl that Parker revealed the results of her HIV test to the faculty and staff.

During the fall of 1998, the girl was frequently ill and missed numerous days of class. But school district personnel failed to provide for the student's educational needs during her illness, the lawsuit says, and filed truancy charges against the girl's mother.

It was during the girl's absence that Parker is alleged to have held two student meetings—one for each sex—in which the girl's HIV status was discussed.

According to the suit, Parker used the girl as an example of why students should abstain from sex or practice safe sex.

"She warned the students to heed her advice or they could end up like the plaintiff. She warned the boys to stay away from plaintiff," the suit states.

Attorney Pamela Dickson contends in the suit that the resulting ridicule and harassment were so intense that the girl was forced to withdraw from school Jan. 20, 1999. The girl is being home-schooled by her mother, a single parent with a full-time job, the suit states.

The mother alleges that Tasma never discussed the matter with her until she filed a complaint with the U.S. Department of Education in May 1999. And even then, Tasma and Faye Brantley, RISD's coordinator of transportation, showed up at the mother's workplace saying they wanted to discuss transportation plans for the upcoming school year, according to the lawsuit.

The lawsuit states that RISD has not only denied making the disclosures but has even maintained that the girl was never enrolled at Royal Middle School.

Dickson, who did not return a call for comment, maintains in the lawsuit that Parker's conduct deprived the girl of educational opportunities equal to that of pupils whose HIV status is unknown and violated the Texas Health and Safety Code by disclosing confidential medical information.