THE WEAK LINK IN INFORMATION SECURITY

David W. Miller, Ph.D.
Department of Accounting & Information Systems
College of Business & Economics
California State University, Northridge
david.w.miller@csun.edu

July 11, 2006

Presented at the July meeting of the
Accounting & Information Systems Department Alumni Association

I'll begin with a quiz. Besides representing famous security breaches that compromised personal data on millions of individuals, what do the incidents from the following organizations have in common: ChoicePoint, BankofAmerica, Ameritrade, CitiFinancial, and the Department of Veterans Affairs?

The short answer is that they are *not* the result of hacking. The longer answer begins with an explanation that these are just five of the over 220 such breaches reported since the ChoicePoint incident of February 2005[1]. In total, close to eighty-nine million records have been compromised. Seventy-five of the breaches—just over one-third—resulted from an outsider hacking into the organization's system. But, as I stated, these five are not from that group. The five listed in my quiz are among the nearly two-thirds of the breaches that are related in some way to the behavior of individuals within the organization or a partner of the organization. Eighty-three of the incidents (more even than hacking) resulted from lost or stolen hardware. Other leading causes of breaches have been data or documents being inadvertently exposed online or through email (34) and dishonest persons inside the organization (13). In only two instances were passwords compromised and there have been only four incidents in the form of social attacks (But, note that the ChoicePoint breach that heads this chronology resulted from some pretty unsophisticated social engineering).

Most large organizations, particularly those that handle large quantities of sensitive personal information take reasonable technological precautions to protect their data and system from outsiders. While no system can be made perfectly secure in the current state of the technology, IT professionals have a good grasp of the sorts of threats that exist and install effective measures to counter these threats. Furthermore, non-IT managers and executives up to and including the "C-level" of the organization understand the importance of protecting this data and are willing to fund the resources needed to add secure structure to information systems. Pressure to improve system integrity has come from external influences as well. Regulations such as the Sarbanes-Oxley and HIPPA legislation have raised the need for systems controls and have forced IT managers to adopt a comprehensive view of data and systems and incorporate system and security controls into the system design process. So, while there is still more that can be done, much has already been done to protect information technologies from outsiders and to design systems that can stand up to data audits.

What is less well understood is the role and effect of users in systems security. Actually, I think that it is probably well understood that data and systems are compromised through the behavior of users, but this is not well documented. Nearly all organizations make some attempt to have users understand the importance of protecting the data and systems but rarely extend beyond password policies in their attempt to control user behavior. I am not sure why the technologies get so much more attention than user security issues. I believe it is in part because the technology issues are easier to grasp and are "cleaner" compared to the fuzziness of dealing with human behavior. I think that it is easier too to conceive of the technological security solutions since they are aimed at protecting the organization from an outside aggressor. I imagine that it is difficult to conceive of the members within the organization as "threats" to the data and systems. It would certainly help to look at the problem more as a management issue than as a threat issue. That is because, while some insider aggression does occur (13 in the chronology), such data and system compromises represent but a small percentage of the causes of breaches. Whatever the reasons, it is obvious that organizations need to do more to prevent data and system breaches resulting from the behavior of individuals within the organization.

So just what should an organization do? First, there needs to be a comprehensive program within the organization that expressly addresses the behaviors of data and system users. This program needs to be clearly stated in a Security Policy that needs to incorporate and complement the organizational policy, mission, vision and values. The security policy must be communicated to each data and system user along with the consequences that will incur if the policy is violated. It has been shown that presenting the security policy during new employee orientation, while necessary, is not sufficient to assure long-term adherence to the policy. If the policy is not reinforced, employees will become complacent and even forget many of the rules set forth in the policy. Therefore, the organization will need to have some form of security education, training and awareness (SETA) program. A SETA program can and should take many forms. Formal training, preferably presented by outside contractors, should be complemented by informal discussion and hands on training. Information security is an ongoing process and the program to help prevent employees causing breaches of sensitive data should be ongoing as well.

I'll conclude by describing what we are doing at CSU, Northridge to help individuals and organizations deal with these sorts of security issues. First, is that the entire Information Systems Faculty has adopted a vision of Information Security that is permeating our entire curriculum. Second, I and others have gotten or are pursuing further education in information security and assurance[2]. A new course (IS 497B; Information Security and Assurance) has been offered that emphasizes issues in information security management and program and policy development. Beginning with the Spring 2007 term we are proposing to offer a corresponding course (IS 497C; Principles of Information Security) that will provide a conceptual view of data and system security, the threats posed to the system and measures that can be taken to protect the data and system. Responding to the need expressed by employers, we are developing a minor in information systems that can be taken by Accounting majors to prepare them for careers in information systems audit. Our longer-term goals center on our acquiring designation as a Center for Academic Excellence in Information Assurance Education (CAEIAE) from the Department of Homeland Security and National Security Agency. This designation will open us up to receive resources to build a wide-ranging information security and assurance program including professional certificate programs and undergraduate and graduate degree programs. The information Systems Faculty is determined to position CSU, Northridge as a major player in information security and assurance education.

Notes:

1. Privacy Rights Clearinghouse, *A Chronology of Data Breaches Reported Since the ChoicePoint Incident*. Retrieved online (July 5, 2006) at: http://www.privacyrights.org/ar/ChronDataBreaches.htm
2. I attended the information assurance capacity building program at Carnegie Mellon University, summer 2005 and Dr. Jeff Zhang is attending, summer 2006; Dr. Donna Driscoll attended the IA bootcamp at Cal Poly Pomona, summer 2005