

## Why Can't We Protect Our Data?

Approximately six months ago, I received a letter from my credit union explaining that a company with which I had done business had experienced a computer breach that may have resulted in the loss of some of my personal information. The credit union noted that I now needed to be on the lookout for activities indicative of identity theft. I couldn't believe it! How could this be? I have been doing computer and network security work for the past fifteen years and am probably about as paranoid as anyone can be. I don't do business on the Internet, and I certainly know better than to input my credit card number or Social Security number to Web pages. But it did happen to me, and I later learned how: a local retailer stored account and driver's license information from one of my checks on a networked computer. That computer was hacked into and consequently put all of my data at risk.

These days, fewer and fewer people would be surprised by my story. It seems that no organization is exempt from experiencing such computer breaches, and the chances of receiving such a notice are growing. Between February 2005 and July 2006, the personal data in more than 89 million records of U.S. citizens were put at risk. Further, of the 237 reported data breaches, 83 took place in higher education.<sup>1</sup> To be quite frank, this situation scares the heck out of me. We *must* demand more from the organizations that store our personal information. Substantial changes in computer practices across businesses and higher education institutions require our immediate attention.

With all the thousands of security solutions that are available, why is protecting sensitive data so difficult? Why are security breaches so common? A dizzying assortment of technical solutions are available: network firewalls, personal firewalls, operating system patching solutions, anti-virus, anti-spyware, intrusion-detection or intrusion-prevention systems, and security management systems. Shouldn't we be able to keep our most sensitive data safe?

The answer to this question needs to be a resounding "yes!" But we're failing to take some necessary steps. Computer and network security is not only about purchasing the latest security technology. Yes, technical solutions have their place, but we need to take a hard look at another area: personal responsibility. We all must accept personal responsibility for the ways our computers are used and how we handle the data we're responsible for. We must begin introducing changes within our institutions and corporations and in our personal behaviors to truly address the growing computer security threats, the risks to an institution's reputation, and the heightening security legislation. We must know the sensitivity of the data that are in our control and the risks to which we expose those data when making poor computing decisions.

The vast majority of computer breaches that I've investigated over the past few years have been the result of poor personal choices, weak computer practices, and less-than-satisfactory data-

**Our failings are not in technology but rather in our inability to instill personal accountability.**

handling procedures. Poor personal choices—such as clicking on any random attachment that arrives in an e-mail or installing programs, such as screen savers, from the Internet—expose computers and the data within them to viruses and spyware. Poor computer practices—such as using weak or no passwords with accounts,

turning off automatic updates, and not running anti-virus applications—leave computers more susceptible to compromise or infection. Less-than-satisfactory data-handling procedures—such as keeping copies of old and unused spreadsheets that contain hundreds of Social Security numbers rather than moving such information to longer-term and safer storage—continuously put data at risk. These security problems cannot be solved by technology alone. Until we start assuming this responsibility and consequently changing our computing behaviors, no amount of technology will have the needed effect. Typically, the weakest security link in any organization is people.

The following is a list of things that I believe every computer user should know how to do and should make a practice of performing regularly on every computer he or she uses—especially those computers that access or store sensitive information:

1. Identify and remove all unnecessary files, such as spreadsheets and documents, that contain Social Security numbers, credit card numbers, driver's license numbers, or other such information if no longer required.

2. Set good passwords on all accounts. Numerous computers have no passwords set at all or have such weak passwords that they can be guessed in under a minute. Such accounts are quickly compromised.
3. Keep software and operating systems up-to-date. Both Microsoft Windows and Apple Mac OS can be configured to automatically check for and install updates. With an average two-day delay between security fix and published compromise code, this is imperative.
4. Approach e-mail attachments with care. Before opening any attachment, the recipient should consider whether the sender is known *and* if the attachment is expected. If the answer to either of these questions is “no,” then the recipient should not open the attachment.
5. Run anti-virus software. Since so much business is performed using e-mail, this is a mandatory application to help identify viruses.
6. Limit access to the computer. Turn file-sharing off unless absolutely necessary. If file-sharing is necessary, configure it with a strong password.
7. Run a personal firewall. Both Microsoft Windows and Apple Mac OS have built-in personal firewalls that should not be turned off. This provides some defense from others who may be scanning the computer, looking for vulnerabilities. Consider other commercially available firewalls as an additional step.
8. Turn off the computer when it is not in use. Unless the computer must be kept running for services such as backups, it should be turned off when not in use. It is impossible to compromise or infect a computer that is not running.
9. Regularly check for spyware. Spyware is often installed on computers when other applications are installed or when Web sites are visited. Spyware can track a computer user’s behavior on the Internet and pop up customer-specific advertisements. The applications are currently free on the Internet and are easy to use.

It might be easy to examine the list of responsibilities described above and discount them as being too technical for many users or redundant to the services

provided by the local technical support. I believe, however, that unless we begin to expect such things from all members of our community, our data will continue to be at risk due to people working from home and accessing sensitive data from personally owned, configured, and maintained computers.

In addition to each of us accepting the personal responsibility to protect the data in our control, we must also begin introducing and supporting some cultural changes. This is particularly true in higher education. Practices that were acceptable just five years ago are unacceptable now due to the increased threat of IT data theft, computer breaches, and identity theft. The broad and common use of Social Security numbers on campuses needs to be significantly curtailed, tightly controlled, or if at all possible, completely eliminated. We need to clearly understand which data require increased protection, where those data are stored, how they are transmitted, and who has access to them. Further, we need to ensure that we closely monitor access to those data to ensure that security and business processes are providing those data with the required protection.

We must also begin introducing computing standards within our institutions. Even though this might be a little difficult due to the extremely decentralized nature of campus IT support, it is the decentralization and the resulting inconsistent technical support that make this such a critical requirement. Introducing simple requirements such as operating system patch level, password complexity, anti-virus solutions, and access control can probably address over 90 percent of security challenges.

Colleges and universities are well known for being wide open from an Internet point of view and from an ease-of-hacking perspective. Such openness is due to the variety of people being supported, the research being conducted, and the wide array of Internet services being used by campus communities. We need to think differently about this openness as we strive to provide better data protection. Not all institutional computers require such openness or access. Administrative computers that store student admissions or financial aid data (probably both containing Social Security numbers and

financial information) should not be so open. Further, some services offered on the Internet are simply too risky to be used on campus computers, especially ones that process confidential data. Some of the new Google services quickly come to mind. These services need to be eliminated from general institutional use.

To begin to take institution-wide steps to better protect the academic community’s personal data, every higher education institution needs to address the following questions:

1. What are the data that the institution needs to protect?
2. Where are these data within the institution?
3. Are formal processes in place to grant and remove access to these data?
4. Is access to these data sufficiently controlled?
5. Are mechanisms in place to ensure that access to these data is not being abused?
6. Are processes in place to assess and audit risks to these data?
7. Who is responsible for the security and protection of these data?
8. Are processes in place to identify and appropriately respond to compromised computers?
9. Can the institution explore how the Internet is used and begin making changes that increase security?

Although higher education has made some progress toward better security and data protection, we have a long way to go to adequately protect our data. Our failings are not in technology but rather in our inability to instill personal accountability for data protection and common computer practices. Higher education institutions need to make some decisions and provide some leadership in order to answer some of the tougher questions and to raise the accountability of the academic community.

**Note**

1. “A Chronology of Data Breaches Reported since the ChoicePoint Incident,” Privacy Rights Clearinghouse Web site, <<http://www.privacyrights.org/ar/ChronDataBreaches.htm>>, July 25, 2006.

**Steve Schuster is Director of IT Security at Cornell University.**