SECUREPURDUE NEWS
www.purdue.edu/securepurdue

June 2007
Volume 1, Issue 7

All the news that's secure to print.

Revisiting SSN remediation: How the laws affect Purdue

The October 2006 issue of SecurePurdue News highlighted two Indiana state laws that went into effect July 1, 2006, and increased the consequences for knowingly or carelessly disseminating Social Security numbers (SSNs) and other personal information. While existing Purdue policies regarding the handling of confidential data helped the University with compliance, the new laws still required the University to examine its business processes, particularly with respect to the business use of SSNs.

In response, many University departments worked together with University legal counsel to document where the new laws had unintended effects. This led to another effort to develop a strategy for asking the Indiana state legislature to review the laws' effects on state educational institutions like Purdue.

Due to the advocacy of the University, Senator Brandt Hershman (R-Wheatfield) introduced an amendment to the SSN disclosure law on Jan. 11 of this year, which Indiana governor Mitch Daniels signed into law on May 4.

The amendment modifies the law to permit disclosures of SSNs in instances where protections are in place to ensure that the data is handled safely and appropriately. The amendment effectively allows state educational institutions to enter into contracts that involve the disclosure of SSNs when adequate safeguards are built into the contract to prevent any impermissible use or disclosure of SSNs. The amendment also allows state educational institutions to disclose SSNs to state, local, or federal agencies or to persons with whom a state, local, or federal agency has a contract to perform the agency's duties and responsibilities.

The law also allows disclosures where permitted under the Family Education Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). The amendment also clarifies that an individual may give consent in electronic form to the disclosure of his SSN to a state educational institution.

Morgan Olsen, Purdue's executive vice president and treasurer, said he was pleased that the Indiana legislature was willing to consider reasonable amendments to the original SSN disclosure law because the law had many unintended negative consequences for the University.

"Purdue offers students and staff valuable business transactions and services—for instance, verification of good grades for car insurance discounts and financial aid assistance—that often rely on the use of SSNs and were unintentionally caught within the scope of the original law," Olsen said. "The amendments to the SSN disclosure law authorize those transactions and services where the University has put in place many safeguards designed to protect the transmission and disclosure of SSN. They also allow Purdue to comply with other legal requirements without violating the SSN disclosure law. It remains critically important for all of us to be aware of the law and best practices that help ensure compliance with it."

See SSN, Page 2

In this issue

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

As I sit here writing this column, I am reminded that today I read a release about another SSN exposure at an Indiana college and there is a story running now on the evening news about data exposures at the Indianapolis Public School Web site. It seems like these announcements are almost weekly occurrences. It is no surprise that people are upset, and, as so often happens when people are upset, they proclaim, "There ought to be a law!" As we know, there is a law now in Indiana that prescribes penalties when certain sensitive data is exposed improperly. As public frustration grows, there inevitably follows the proclamation, "Someone should be held accountable!"

I believe we are quickly approaching the point where public authorities will have to respond to the cries for accountability

See CISO, Page 3

Summer daze at Purdue

Keep your computer safe over the summer

Summer vacation is an opportunity for Purdue faculty and staff to take time off, visit other places, and recharge their internal batteries. It can also be an opportunity for the bad guys to take advantage of their absence. Here are a few ways to keep computers, data, and personal information secure while still enjoying fun in the sun.

Lock it down

First and foremost, computers must be kept in a secure location. Whether that location is an office on campus, at home, or while traveling, physical computer security is the first consideration when leaving the office for an extended period of time.

> Laptop theft is the second most common crime in the U.S. — FBI

Many people simply leave their computers on their desk when they leave for a vacation. If the office has a lock on it, lock it securely. If it doesn't, work with departmental information technology (IT) contacts to secure portable computers in another locked place.

"Physical security may be the most obvious step to take, but certain aspects of physical security are routinely overlooked," says Addam Schroll, security and privacy analyst for ITaP. "For example, if other people have access to the room, as with a shared office, it's not really locked. If you share an office with someone, then your computer security is in their hands."

Some people decide to take their computers with them on vacation, especially those who use laptop computers. Travelers are among the targets of laptop thieves. According to Safeware Insurance statistics, more than 600,000 laptop computers were stolen in 2005, costing businesses and consumers an estimated $720 million in lost hardware, and $6.7 billion in lost proprietary information. According to the FBI, the average laptop theft results in a deprival of $89,000 in lost equipment, software, and proprietary data, and more than 97 percent of all stolen laptops are never recovered.

"Make sure you have possession of your computer at all times when you're traveling," Schroll says. "Thieves are looking for distracted travelers who don't expect to be a target."

Turn it off

Vacationers who leave their computer on and unattended for more than a week create an opportunity for computer hackers to exploit software vulnerabilities at their leisure. One of the easiest ways to combat hacking is to simply turn the computer completely off. According to Schroll, a computer that is turned off is a much harder target.

"Once a computer is fully and completely turned off, it is a much greater challenge for a hacker to exploit you," Schroll says. "It changes from a purely technological protection to both a physical and technological protection. [Hackers] now have to find a way to physically turn on your machine, and then hack the software technology that further protects it."

Purdue computer users need to coordinate with departmental IT services before turning off a Purdue-serviced computer for an extended period of time. There may be a specific procedure for later restoring the computer to a fully-virus-protected state because the computer will have likely missed regularly scheduled virus-protection updates.

Keep it to yourself

Another point to consider when leaving for an extended period of time is the use of the ubiquitous "bounce message." A bounce message is the email response designed to automatically alert email senders that their would-be audience is out of the office. Bounce messages are sometimes used to fulfill or protect an important business need, so use them if necessary. However, consider carefully the implications of using one before making the decision. Bounce messages can:

- Alert spammers that the employee's email address is a legitimate target, prompting more spam.
- Reveal personal information written in the automatic response email.
- Inform hackers as to the available amount of hacking time before the employee returns.
- Give up others' contact information as resources to contact in an emergency.
- Create spam for fellow members of legitimate automated mailing lists.
- Lead to automatically being removed from some mailing lists.

"It is much better if you can get by without using a [bounce] message, and instead simply inform the right people about your upcoming absence," Schroll says. "If you must have a bounce message for business purposes, be aware of the risks associated with including certain bits of information. If you are concerned about information given out, then use the bare minimum necessary."

SSN, from Page 1

While the amendments help clarify the legal parameters of SSN use at educational institutions, knowing Purdue's policies regarding SSN use in particular, and data handling in general, will help Purdue ensure compliance with the law.

To read the amendments and for more information about compliance with, and response to, the SSN law at Purdue, visit http://www.purdue.edu/securepurdue/breach/.

To read Purdue's information security policies and to find the University's data handling requirements, visit http://www.purdue.edu/securepurdue/bestPractices/.

SECURITY RESOURCES

Use the following resources to educate yourself about security and privacy issues surrounding computers and data networks.

• IT Incident Response Report Form
http://www.purdue.edu/SecurePurdue/incidentReportForm.cfm

• CISSP information and certification process
http://www.isc2.org

• CIS benchmarks
http://www.cisecurity.org/bench.html

• CIS benchmarks registration
http://members.cisecurity.org/

• Purdue Air Link setup instructions
http://www.itap.purdue.edu/airlink/setup/winxp.cfm

SECURITY TIPS

McAfee VirusScan has now been replaced with McAfee Home Edition for use on home computers.

Home Edition offers both virus scanning technologies and anti-spam tools to keep your home computer free from malicious software.

To download your own copy of McAfee Home Edition, browse to the SecurePurdue Web site at www.purdue.edu/SecurePurdue and click the **Downloads** tab near the top of the page.

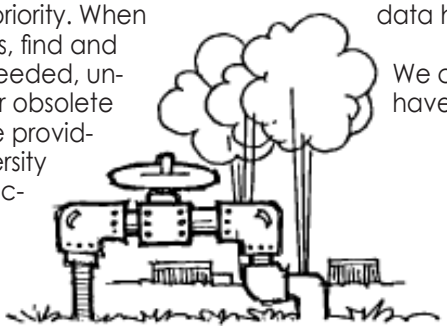
Follow the instructions on the page. You will need your career account login and password.

CISO, from Page 1

and seek to hold individuals responsible. Rather than fearing being held accountable, we must push forward and be the example of best practice and appropriate care. I know many areas of campus have worked very hard to take remediation steps over the past two years. Those efforts are to be applauded, and I urge them to continue their successful efforts and help serve as examples for all of us.

The fact is, however, that exposures of data from Purdue University have continued despite our efforts. The law requires that notice of these events be filed with the Indiana Attorney General, whose office has asked increasingly detailed questions about the steps we are taking to further protect sensitive data and the names of those responsible. Saying that we are "continuing to work hard," while true, is not going to be a sufficient answer much longer. Unfortunately, this is not an area where technology alone can "solve" this problem. While there are tools to monitor and scan for transmitted or stored sensitive data, they are not sufficient as the only step in locating potentially vulnerable data. We cannot depend solely on technology. We must also draw upon human searching and analysis skills.

I know that analyzing years of stored data on a server or PC isn't a simple task. We all have a long list of difficult tasks, and we are trying hard to manage our priorities on a day-to-day basis. My message today is that taking time to consider, recall, or search for potentially vulnerable sensitive data before it is accidentally exposed or hacked must be a very high priority. When we, ourselves, find and remove unneeded, unnecessary, or obsolete data, we are providing the University its best protection against possible exposure of that data.



I am well aware that, for many, this isn't a popular message. For some this just feels like another "unfunded mandate from some security guy." I hope you will consider that this isn't just something that a security group invented to make your life more complicated. We have a continuing duty to our students, staff, faculty, alumni, supporters, and friends to protect the data that they have entrusted to us in the same way we would expect them to protect our data in their care. This is not only the law, but it is the right thing to do. We are honoring that trust, and we have made significant improvements in our data handling and protection.

We can't rest in our endeavors. We still have much more to do.

STEAM-CIRT NEWS

STEAM-CIRT is a security team and IT incident response team organized under the ITNS group within ITaP.

For more information about STEAM-CIRT and for security updates throughout the month, visit the STEAM-CIRT Web page at:

http://www.purdue.edu/securepurdue/steam/

Top 10 Purdue email viruses

At right is a 30-day snapshot of the most active email viruses on the Purdue campus.

The maximum occurrences found in one day are listed with the names of each major virus.

Viruses	Max. Occurrences
W32/Mytob-GH	5915
W32/Dolebot-A	5392
W32/MyDoom-O	1391
Mal/DorfRar-A	1044
W32/Sality-AA	381
W32/Mytob-FO	337
W32/Mytob-BV	201
W32/Bagle-Zip	187
W32/Netsky-P	137
W32/Mytob-D	99

30-day snapshot as of May 29