SECUREPURDUE NEWS
www.purdue.edu/securepurdue

June 2011
Volume 8, Issue 4

All the news that's secure to print.

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

Often information security seems to focus on "gloom and doom" reports. However, there are signs that organizations are starting to take information security more seriously, and with positive results. The 2011 Verizon Data Breach Investigations Report stated that the amount of compromised data reported for 2010 breaches was at an all-time low. That number seems almost hopeful. The Verizon report is prepared by the Verizon RISK Team in cooperation with the U.S. Secret Service and the Dutch High Tech Crime Unit.

Despite that positive trend, we must continue to be vigilant in higher education. The Privacy Rights Clearinghouse, another group that monitors data breaches, reported thirty data breaches involving higher education institutions in 2011. And, this is only six months into the year. These thirty breaches involve 156,897 records.

The data breaches aren't just failures of technology. In one case, partially shredded personnel records were dumped along a roadside. Those records contained the names and Social Security numbers of University employees. In another incident, a person found documents near a freeway that contained student names and SSNs. Properly destroying data containing personal information might have prevented these breaches. Visit Purdue's data destruction resources at: http://www.purdue.edu/securepurdue/datadestruction/

Mobile device security is another area of focus. In the Privacy Rights Clearinghouse report, several data breaches involved stolen laptops containing personal information. Other incidents involved the loss of other kinds of portable devices with personal information stored on them. While not every loss of this type can be prevented, taking basic steps to safe-keep these devices is a good idea. Visit Purdue's mobile device security recommendations at: http://www.purdue.edu/securepurdue/bestPractices/mobileDevice.cfm

In this issue

Physically securing storage media is also important. In March 2010, storage media was stolen from a vendor that does work for the Federal Student Loans program. In that incident, a portable safe containing back-up CDs and DVDs was removed from the building by rolling the safe out on an office chair. While the media was recovered one month later, and did not appear to have been accessed, that incident could have led to the loss of over three million records containing the names, addresses, SSNs, and other information belonging to federal student loan borrowers.

The Verizon Data Breach Investigations Report shows that 96% of the breaches that it reviewed were avoidable, and 92% of the attacks were not technically difficult. 96% WERE AVOIDABLE!!! Other statistics are also interesting:

- 83% of victims were targets of opportunity
- 92% of attacks were not highly difficult (this is down from last year)
- 76% of all data was compromised from servers (this is up from last year)
- 86% of the breaches were discovered by a third party
- 96% of breaches were avoidable through simple or intermediate controls

Taking the protection of our data seriously isn't a sometimes job—it's an everyday job. This means that we can't take the summers or holidays off without making sure that

CISO continued Page 3

Personal Security Tips

Secunia Personal Software Inspector
Secunia is a free security tool that scans your personal computer for installed programs and lets you know if there are any vulnerable or out of date programs residing on it. The tool then provides a link so you can install the update in the newest version. It can auto update some of the basic programs that most of us use daily. (i.e. flash, reader, Java, etc.)

Brad Graves, IT security engineer says, "I tell everyone in my family to install it on their computers." This tool works well for managing your personal computer at home.

For more information about this tool, go to: http://secunia.com/vulnerability_scanning/personal/

Fear your account is compromised? Now what?

If you think that your account has been compromised, whether it is your Univeristy account or your bank account, there are a number of steps to take. The first step to take is to change your password and set of answers to the questions you have set up for your account. Changing your set of answers to the questions you set up may not be the first thing you think to do but will protect you from further compromise of your account.
If you believe your University account has been compromised, go to http://purdue.edu/securepurdue/ and click on the text, Change your Password, in the top left corner. If you believe you have been a victim of a crime, call the police.

Facebook and Social Media Use

Recent stories in the news have revealed embarrassing moments in the use of technology that were meant for private sharing but were set to public display. It pays to understand the technology before using it, especially when there are 400 million users of Facebook worldwide.
There are now advanced Facebook features to help you manage your privacy and security. To view your account settings, from any page in Facebook, the top right corner has the word Account, which links to both your privacy settings and your security settings. This article will highlight some of the new features and how to set them.

Privacy Management: Sharing on Facebook
The sharing feature in Facebook lets you manage who and what information you share with others. Friends Only is a good place to start and then be selective in granting Friend status. This feature is found under Account Settings, Privacy.

To manage your work, friends and family and personal life separately,use the Edit Friends option to create lists of people or web sites. You can use a limited profile to share with acquaintances and a more open profile with friends.

Don't give out personal location information to public view.

Control each time you post: allows you to set who sees each and every post. Before you post a status update, click the lock icon to choose who can see it.

Let Others Know Where You Are
With the Facebook app on your smartphone, you can let others know where you are at any moment by enabling this feature. You can connect with friends nearby or find local discount offers. Once you have connected with friends, you can turn this feature off for privacy.

Security Features
If you frequently use public computers or work on unsecured network connections, it is wise to set your browsing through Facebook to connect on a secure connection. This option is available from the Account link/Account Settings/Account Security. Check mark the option to browse securely.

If you choose to participate in social networking you will sacrifice a certain amount of privacy, but you can limit what you share. The strongest tools you have to defend your personal privacy on social networking sites are common sense, caution and a certain amount of paranoia.

SPOTLIGHT

Data Handling Requirements Help Protect Purdue Data

Purdue University manages all of its data under the University's Data Classification and Governance policy. This policy formalizes Purdue's "public," sensitive," and "restricted" data classifications. It also sets forth the formal structure for how Purdue manages the use of its data. The University's Data Stewards are responsible for making sure that data is classified appropriately and that procedures are established to properly use classified data.

The Data Stewards organization has members from across campus. As part of their responsibilities, the Data Stewards have developed handling requirements for the various types of University data. There are handling requirements for printed information, electronically stored information, and electronically transmitted information. The Data Stewards review these handling requirements on a regular basis.

It is the responsibility of those people using Purdue data to make sure that they use it correctly. When a person is using Purdue's data (whether in electronic or printed form), they are considered a "Data Custodian." A data custodian is an individual who needs and uses Purdue data on a daily basis as part of their assigned employment duties or functions. Data custodians must follow the data handling requirements created by the data stewards.

"Understanding and following the handling requirements is important," said Daniela Rivera, Data Steward for Administrative Computing, Housing and Food Services. "This is because there are so many different tools that data custodians use each day. It would be impossible for the data stewards to create different handling requirements for each different type of tool. Instead, data custodians need to follow already-established requirements for the types of data that they are using."

For example, SharePoint tool use is exploding on campus because the tool is such an effective way for members of the Purdue community to collaborate. "While SharePoint is a unique tool, there are not separate or special rules for handling data stored in SharePoint," Rivera said. Instead, the existing data handling requirements can guide SharePoint users.

Currently, use of the SharePoint tool falls under the classification: "Storage on fixed media, with access controls, accessible via the web."

The handling requirements for that classification can be found at: http://www.purdue.edu/securepurdue/procedures/dataHandling/electrStored.cfm

How a person uses data at Purdue depends on how that data is classified, not on the type of tool that a person is using. All Purdue University employees are responsible for using Purdue data appropriately. One way to make sure that you are using Purdue's data appropriately, whether it is in SharePoint or in any other way, is to learn more about Purdue's data handling requirements. The Data Stewards have created a number of educational resources to help data custodians properly use Purdue data.

Data custodians can also take a certification quiz to test their data handling knowledge. This is a one-time certification that is available at: https://www2.itap.purdue.edu/SSTA/certifications/ (you will need to log in with your Purdue Career Account credentials and choose "Enterprise Certifications" and then "Data Handling" in order to take the quiz).

You can learn more about data classification and handling at Purdue by visiting: http://www.purdue.edu/securepurdue/bestPractices/dataClass1.cfm

Data handling educational resources are available at: http://www.purdue.edu/securepurdue/procedures/dataClassif/Resources.cfm

CISO Continued from page 1

Purdue's data is protected. This job requires everyone's help. It is important that we all be mindful of where data is stored, how it is shared, and how it's destroyed.
Making sure we understand Purdue's information security policies and data handling requirements helps us in this job. You can read more about data handling in this issue of the newsletter.

Let's keep up the good work we have been doing and, as always, be careful out there!

CENTER FOR INTERNET SECURITY

ITaP Networks and Security recently renewed Purdue's membership to the Center for Internet Security (CIS), which allows Purdue staff continued free access to benchmark white papers and scoring tools for use within Purdue University.

CIS benchmarks and software scoring tools provide best practices for secure system configurations. These benchmarks are created by consensus from a dedicated group of security professionals worldwide. CIS offers the benchmarks and scoring tools for free from their website, as Purdue is a paid member of the organization.

Purdue University employees may obtain a user account on the CIS Members Site. To register, go to https://members.cisecurity.org/forums and click the "register" link. (this page is also accessible via a link from the home page of the public web site http://www.cisecurity.org).

The CIS Members Web Site contains discussion forums and is a place for groups working on new benchmarks and scoring tools to collaborate.

To read more about CIS or the benchmarks, please visit:
http://benchmarks.cisecurity.org/en-us/?route=downloads.benchmarks
http://www.purdue.edu/securepurdue/bestPractices/adminResources.cfm

Tips to Protect Your Privacy While Vacationing

If you are planning a vacation this summer, be sure to review these tips from the Privacy Rights Clearinghouse before you leave. You can read the full article at: http://www.privacyrights.org/summer-vacation-privacy-tips-2011

1. Clean out your wallet or purse.
Remove extra or unnecessary credit cards, social security card, library cards, anything you won't need while on vacation. Photocopy or make a list of remaining contents to keep in a safe place. Don't use a debit card that is also on your checking/savings account. Use credit cards instead. You might want to leave unnecessary keys at home as well.

2. **Don't broadcast your vacation.**
Share such information on social network sites, if you want, but only with close friends. Stop the mail and newspaper delivery so you don't broadcast to passers by of your home that you are away.

3. Plan ahead for cash withdrawals.
If you plan to use an ATM for cash while vacationing, use an account that does not have debit or check card privileges. An ATM only card can be requested from the bank. Be alert to signs of tampering of the ATM.

4. Connect to the Internet with care.
If you plan to take your laptop with you, don't leave it in the car, where it can easily be stolen. Be careful using free internet or Wi-Fi networks. Most hotspots are unsecured and unencrypted. Avoid accessing any sensitive information from a public computer. If accessing work information, use VPN to access data securely. Cell phones can also use VPN to access data from work.

5. Use the hotel room safe.
Put your wallet, laptop or other valuables in the safe.

SECURITY RESOURCES

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

- *2011 Verizon Data Breach Investigations Report*
  http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
- *Privacy Rights Clearinghouse Data Breach Tool*
  http://www.privacyrights.org/data-breach/new
- *Secunia Personal Software Inspector*
  http://secunia.com/vulnerability_scanning/personal
- *Center for Internet Security*
  http://www.cisecurity.org
- *Data Handling Resources*
  http://www.purdue.edu/securepurdue/procedures/dataClassif/Resources.cfm