SECUREPURDUE NEWS
www.purdue.edu/securepurdue

March 2012
Volume 7, Issue 1

All the news that's secure to print.

FROM the CISO

By Greg Hedrick
Interim CISO

"What keeps you up at night?" I often get that question from peers, family, and colleagues. Interestingly, I've found myself responding differently over the years because the threat landscape is ever changing.

I'll start with the top three items that weigh most heavily on my mind at night (at least for now). First, I worry about the things I don't even know about yet. What new vulnerability or threat will wreak havoc tomorrow, this week, or next month? It could be a technology threat or vulnerability, a people threat or vulnerability, or a change to processes that introduce a new threat or vulnerability. These "unknowns" are immune to my schedule. It really doesn't matter if I want to take a vacation day. Keeping up with vulnerabilities and threats is something the security group struggles with on a daily basis; but it must be done, and it is exhausting.

Second, I worry about making sure that YOUR data is protected. Technology changes at a rapid pace. We continue to see mobile devices used internally for everything from teaching to business processing. In January, Symantec announced they had found 13 applications for the Android that contained "malicious" code. Do folks use these applications at Purdue and could one of these applications expose our data?" We continue to move and trust our data in the "cloud," but can we guarantee our institutional data is any safer? Students, parents, faculty, staff and alumni expect the data they have entrusted with us be kept secure. We must continue providing education, procedures, and technology solutions to help protect that data.

Finally, I worry about how to best balance security controls to reduce risk but also cause very little business impact. Most corporations have controls in place that won't allow you to access Facebook, sync with your personal computer system, use applications such as Dropbox, or in some cases read e-mail from an external provider. However, to allow research and collaboration, it's nearly impossible to prevent these activities at an academic institution like Purdue (and I might argue that we shouldn't anyway).

We have to consider using these applications to improve our business processes, communicate more effectively and hopefully reduce costs.

But, we should do so wisely and understand the risks that are inherent on the Internet. Does a person who handles confidential data really need to browse Facebook at work? Does he or she need to watch that funny dog video that a friend sent them via e-mail? Maybe, but probably not. These activities can put Purdue data at risk and we need to be mindful of that. This year I plan to focus on providing more education and awareness on these topics. We have invested in security awareness videos from SANS, which you will hear more about in the coming months.

I would be very interested in hearing from you about these topics so please drop me a note at hedrick@purdue.edu

Enjoy the newsletter and please continue to be careful out there!

In this issue

Setting Your Password on Your iPad

This article explains some common setups at Purdue University for the iPad. The information for this article comes from the GoldAnswers Knowledge Base Guides:

How do I connect to PAL2.0 with an iPhone, iPod Touch, or iPad? How do I set up my Exchange 2007 mailbox on my iPhone, iPod Touch, or iPad?

In your settings folder, select Joining other Wi-Fi networks

Tap Settings > Wi-Fi.
Available Wi-Fi networks appears under Choose a Network…
Select the Wi-Fi network you want to join.
NOTE: Some Wi-Fi networks require a password to join. Password-protected Wi-Fi networks are indicated by the padlock icon Inline Image.

Regularly backup (sync) your iPhone, iPod Touch, or iPad with iTunes on your home computer to make sure your information is safely stored. Check regularly for system updates to guarantee you are using the latest and most secure software.

Instructions for backing up your iPhone, iPod Touch, or iPad are available on the Apple Support website at this address http://support.apple.com/kb/HT1414.

Visit the Apple website at http://www.apple.com/ to download iTunes to your home computer if you don't already have it.

https://www.purdue.edu/goldanswers/app/portlets/results/viewsolution.jsp?solutionid=041117216283046

Importance of Risk Based Assessments and Security Controls

by Gregory Barnes

One of the focuses of our information security practices at Purdue is compliance. There are many laws that we must follow to protect the different types of data that we use everyday. While these laws are different in scope, many of them have a common requirement: Conduct a risk-based assessment to best understand how our information systems use data.

A risk assessment allows a broader view of how business processes work in a department and how information systems are used in that process. A risk assessment doesn't have to be a difficult process. Sometimes doing simple role-playing for worst case scenarios is an effective way to give a baseline of important risks a user or organization faces. When we conduct a risk assessment, we ask some basic questions. You can also ask these questions in your own department in order to reduce risk:

- What kind of data do you use in the department; is any data "sensitive" or "restricted" per University Policy?
- Is there a written procedure for off-boarding employees when they leave the department? Does this process insure that keys, access devices, and data are returned to the university?
- What kind of physical safeguards exist to protect workstations and other devices?
- Are mobile media devices used in the department, if so what for?
- Are local users trained in the University's incident response policy?
- Is the department following Purdue's information security and data handling policies?
- What kinds of situations might put our data, processes, or information systems at risk?

Once risks are known and prioritized, it becomes clearer which security controls are desired. Some controls or tools may be mandatory as required by laws or policy (like anti-virus software or a properly configured firewall). A risk assessment might also indicate other controls that can be eliminated or modified to ensure better security and more efficient business processes. A simple risk assessment process can let users better understand a data security strategy. While not all risks and threats can be mitigated, cataloging risks enables users to make wiser choices about using and protecting data.

SPOTLIGHT

Disposing of Your Old Cell Phone

About every two years, we all have a dilemma. How to dispose of our old cell phone. Our sons are more tech driven than we are so I won't be handing down my now antique version of technology to them.

In the past I have given them to the YWCA for the women's domestic abuse program. That was ok when all my phone had on it was some phone numbers. Now I have apps on it and I have entered passwords to websites while searching for things. With a data plan, you have many different data types stored on your phone:

- Contacts
- Phone logs
- Appointments
- Tasks
- Pictures
- Videos
- E-mail
- Voice notes and recordings
- SMS messages
- Application data
- E-mail attachments

All of this data is remembered and must be deleted. If you have stored data on the iCloud, that will need to be deleted as well, in the case of your phone being stolen and not password protected. Access to this data could be attained.

Permanent data deletion requires several steps. Removing the subscriber identity module (SIM) card is the first step. This alone is not sufficient as Smartphones have an operating system just like your computer. Instructing your cell phone to delete specific data will only delete the references to where the data is located but the actual information stays on the phone's operating system.

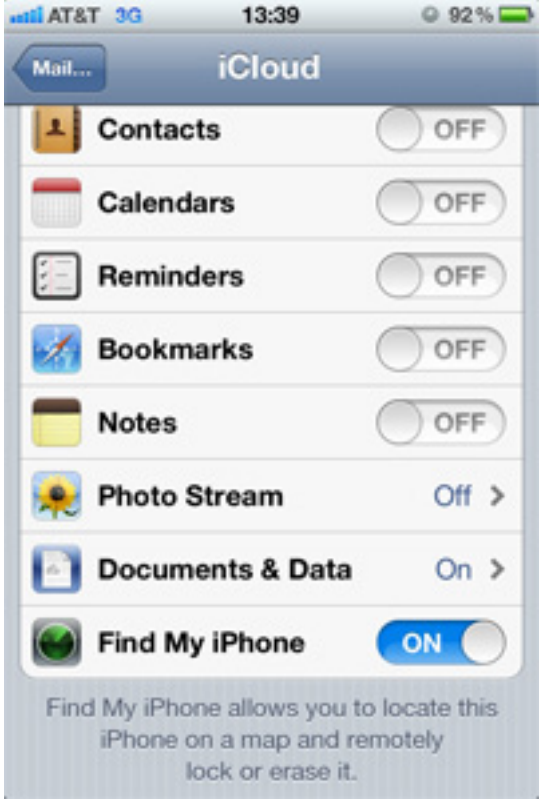
Finding Instructions to Delete the Data
To find online instructions on how to delete the data on your phone, search on terms like "delete data" or "reformat."

Remote Data Deletion

This requires advanced set up. This is necessary so that the feature is available in the event your phone is lost or stolen. The iPhone 3.0 software update, with an iCloud account, allows you to remotely wipe your phone's data in the event it is stolen or lost.

Steps to Set Up Your iPhone To Remote Wipe:
1. Set up an e-mail account on the iPhone or iPod.
2. Set it to **On**. The option to set it **On** will be located in your Settings/Mail, Contacts, Calendars - iCloud account.
3. Scroll to the bottom to activate **Find My iPhone**.

This will allow you to find your iPhone on a map and remotely either lock it or secure it. When we say it can "find it on a map", this does not mean it can precisely pin point the location but it will locate an area. Location services would need to be turned on. Locating the phone is only possible if the battery is still charged and the phone is turned on.



Once you've set up your device, you can access the Find My iPhone features—including Remote Wipe—by logging in to the https://www.icloud.com/#find
You can remote wipe the data.

CERIAS 13th Annual Information Security Symposium

CERIAS will host their 13th annual information security symposium on April 3rd - 4th. The topics will focus on mobile devices and the increasing interconnectedness of our networks and business processes related to the security and privacy of the data they store. There will be panel discussions on Big Data Analytics, Mobile Device Security, and SCADA System Security with views from academic, government and industry experts.

Howard A. Schmidt, Special Assistant to the President and Senior Director for Cyber Security, Office of the U.S. President will speak on April 3rd in the morning. Following Howard's talk will be the SCADA and Security presentation.

On the afternoon of April 3rd, they will host the Security Fireside Chat with Dr. Eugene Spafford, CERIAS, Mr. Schmidt, and Arthur W. Coviello, Jr., Chairman, RSA, The Security Division of EMC

The Keynote speaker on April 4th will be Arthur W. Coviello, Jr., Chairman, RSA, The Security Division of EMC

The closing presentation will be given by James Lewis, Director and Senior Fellow, Technology and Public Policy Program, CSIS.

To read more about the symposium and to register, go to: http://www.cerias.purdue.edu/site/symposium2012/

Greg Barnes Earns CRISC Certification

Greg Barnes, IT Security Risk Analyst in ITaP Security and Policy, has achieved the Certified in Risk and Information Systems Control (CRISC) designation. To learn more about CRISC certification please go to http://www.isaca.org/CERTIFICATION/Pages/default.aspx Congratulations Greg!

Data Stewards Publish Revised Handling Guidelines to Help Thwart Security Breaches

The Data Stewards organization at Purdue is committed to keeping employee information secure by creating guidelines and requirements for storing and using sensitive data. As part of that continuous effort, the organization recently published its revised data handling guidelines with additional examples to help individuals better understand how to protect University data.
All users of Purdue data, in any form and for any purpose, are called Data Custodians and are urged to contact the Data Stewards for guidance in cases that present handling questions or security concerns.

"There are laws that dictate the protection of certain data such as student records, Social Security numbers and health information," says Cheryl Gray, manager of human resources IT services. "As an employee of the University, it's important to understand how to appropriately handle the data we use in our jobs. If a student or employee's data gets compromised, there is a risk of stolen identity and financial impact. Not only would this be an embarrassment to the University, but security breaches could also result in federal penalties and fines."

To comply with these guidelines, Purdue employees should never collect Social Security numbers from individuals unless there is a legal requirement to do so. Moreover, employees should refrain from emailing documents containing sensitive or restricted information, as e-mail is not an approved or secure method for transmitting this type of data. The use of Purdue's secure Filelocker service (https://filelocker.purdue.edu/) is encouraged for the transmission of sensitive and restricted data when it is appropriate to transmit that data.

Additionally, Social Security numbers may not be used as a common identifier or as a database key in any electronic information system. University employees should also be familiar with the Indiana SSN Disclosure and Notice of Security Breach laws, which they can find in the Data Handling and Security training PowerPoint.
The full Social Security number policy may be found on the Purdue website. http://www.purdue.edu/policies/information-technology/viib7.html

These handling requirements are reviewed by the Data Stewards and information owners at least annually, or whenever significant changes are made to data or systems, and evolve as technology improves. Any comments regarding these requirements should be emailed to Data Stewards.
For additional information, contact datastewards@purdue.edu.

SECURITY RESOURCES

- Purdue GoldAnswers
https://www.purdue.edu/goldanswers/app/portlets/results/viewsolution.jsp?solutionid=041117216283046

- CERIAS Symposium
http://www.cerias.purdue.edu/site/symposium2012/