



FROM the CISO



By Scott Ksander
Executive Director
IT Networks & Security

Seymour Cray, founder of Cray Computers, used the phrase "creative avoidance" to describe the act of being "really busy" and not being able to find time to get something done that you really didn't know how to start. Sadly, this column has been the victim of creative avoidance for too long.

It seems that every year I write about all the bad things in the cybersecurity world and how we need to remain vigilant to protect our fellow Boilermakers. While that remains true, I want to also acknowledge that, basically, nothing really bad has happened at Purdue due primarily to your vigilance. I want to celebrate the fact that nothing bad happened! That's a difficult story to tell. So, let's take a moment and raise our glasses to celebrate a great year of nothing. Seriously, others in industry and even academia can't make that toast. I am proud of the work we have done. I hope you are too.

Having said that, let's review one more time that there is evil in the cyber world and we need to stay on our game. The recent "Symantec Internet Security Threat Report" for 2009 has some interesting facts and figures.

- In 2009, 60% of identities exposed were compromised by hacking attacks. (A marked increase from 22% in 2008)
- The top Web-based attacks in 2009 targeted applications that process PDF files (49% of the total)
- New "crimeware" kits now make it easier for unskilled attackers to compromise computers and steal information.

In this issue

CISO message	1
SiteAdvisor 3.0 Enterprise Plus	2
Center for Internet Security	3
Rules of the Road.	3
IT Policies Approved and Revised	4
Security Resources	4

In 2009, Symantec observed nearly 90,000 unique malware variants from just one basic crimeware kit.

- Symantec alone created 2,895,802 new malicious code signatures in 2009 (a 71% increase over 2008)

The educational sector accounted for 20% of the data breaches that could lead to identity theft during 2009, more than any other sector. This is a decrease, however, from 27% in 2008, when it was also the highest ranked sector for data breaches.

So, the bottom line is that we had a good year. Enjoy that. However, the cyber world is still a very dangerous place. Thanks for reading and, please, continue to be careful out there.

SiteAvidsor 3.0 Enterprise Plus

ITNS is now offering SiteAdvisor 3.0 Enterprise Plus via the ITNS ePO service. This McAfee product is a browser protection solution for Internet Explorer and Firefox which runs on ePO managed systems to protect users from web-based threats. It also provides extra protection when downloading files with Internet Explorer. SiteAdvisor helps users by notifying them about threats they could be exposed to while searching or browsing web sites. SiteAdvisor rates the web sites that you view. Each web site is given a safety rating: green, yellow, red, or gray.

SiteAdvisor helps users by notifying them about threats they could be exposed to while... browsing web sites.

The ratings look like this:



Safe: Very Low or no risk issues



Caution: Minor risk issues



Warning: Serious risk issues



Unknown: Not yet rated. Use caution.

Users are trained to be more aware of malicious web sites as well as their web searching and browsing activities. A report is also available for each web site, detailing test results and user as well as site owner feedback.

ITNS has done internal testing of SiteAdvisor 3.0 Enterprise Plus and found it to be a useful tool to mitigate web based threats seen through malicious web sites and phishing attacks.

The Enterprise version is only available for Purdue owned equipment and those using the ePO service. Please ask your IT support person for further details. If you want to use it on your personal equipment you can download it for free at: <http://www.siteadvisor.com/>

Security Tip Trading Post

Tip #1:

Many people use the gmail.com chat function to instant message with friends. Did you know Gmail automatically saves and archives these conversations for you? You have to manually turn off this function if you don't want your instant message conversations saved. To do this, access your account settings through Gmail, click on chat settings, and select the button that says "never save chat history."

Tip #2:

Be careful what items you post on social networking sites. Items that you post, even if later you wish to remove them, may be difficult to remove or could remain available due to the high probability that the site or its contents have been saved or archived to an Internet Archive or have been shared or downloaded by someone.

Tip #3:

Open Internet connections can expose your private and confidential information. Shut your computer down when you are not working on it.

Tip #4:

If a scammer takes advantage of you through an online auction or through online shopping, you need to report it to the Federal Trade Commission, at <http://ftc.gov>

SPOTLIGHT

Center for Internet Security

ITaP Networks and Security recently renewed Purdue's membership to the Center for Internet Security (CIS), and as such has the right to distribute the benchmarks 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 hundreds of security professionals worldwide. CIS offers the benchmarks and scoring tools for free from their web site.

Purdue University employees may obtain a user account on the CIS Members Site. To register, go to <http://members.cisecurity.org/> 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>).

To read more about CIS or the benchmarks, please visit:
<http://www.cisecurity.org/bench.html>.
<http://www.purdue.edu/securepurdue/best-Practices/adminResources.cfm>

Rules of the Road: Traveling Securely

At many airports, you can find a wireless access point in nearly every waiting area, and in all of the restaurants, coffee shops, etc. And because of that, it's easy to start using the Internet in the middle of the airport. Be aware that "Free WiFi" doesn't mean secure WiFi. Look for the airport secure free WiFi connections.

When traveling, carry your laptop computer with you at all times. Do not check it with luggage, leave it in a hotel, or in a car. These are not secure locations. If you cannot do this, then do not take your computer.

- If you must leave your laptop in the hotel, store your laptop in your in-room safe.

Rules of the Road continued

- If you log in to your computer in an unsecured place (such as a public area), change your password once you have returned to the safety of a secure location.
- Backup all important documents before you leave.
 - Always password protect any documents with personal financial information.
 - Before you travel, turn off and clear out the cookies on your machine so that Internet web sites don't automatically log on to allow access to your accounts.
 - Remove or protect anything that has sensitive information on your hard drive or better yet, upload those files to a secure server that can be accessed from anywhere and especially in case your laptop is stolen.
 - Record serial number, ESN, MAC, etc for tracking.
 - Encrypt your laptop.
 - Disguise your laptop: carry your laptop in a laptop backpack. They are more comfortable and don't shout "laptop."
 - Always use the VPN system when logging in to Purdue networks.

Safe Behaviors

- Never use free kiosks or Internet café computers to log in to Purdue accounts.
- Never log in to Purdue accounts without using VPN.
- Never leave your computer unattended.

If you will be traveling with a university laptop, remember to fill out and process the Form 12 for approval to request use of university property off campus. It can be found at:

<http://www.purdue.edu/bs-ba/pdf/Form12.pdf>

Assume you are going to lose it, have it stolen, or compromised and plan accordingly!!!

MILESTONES

IT policies approved and revised

Purdue's Executive Policy Review Group (EPRG) approved one new and two revised IT policies at their February meeting. The EPRG is a standing committee of Purdue University executives who provide institutional review, approval, or recommendation of approval of Purdue University System-Wide Policies. The president of the University appoints the committee members.

The new policy is the Data Classification and Governance Policy (V.1.8). This policy was drafted and approved by the University Data Stewards, the Security Officers (SO) Working Group, and IT Networks and Security (ITNS). The policy formalizes the University's "public," "sensitive," and "restricted" data classifications.

The revised policies were drafted and approved by the SO Working Group and ITNS.

The IT Executive Steering Committee approved them as well. They are:

Remote Access to IT Resources (V.1.6). This policy specifically allows remote access to University IT resources. Remote access is access to IT Resources from an electronic or other device not directly connected to the Purdue University wired or wireless networks, but not including accesses to such IT Resources where Remote Access is considered a primary function and normative use. For example, use of a Web browser to remotely access a Purdue University Web page is not covered by this policy. ITNS and the SO Group have issued a Remote Access Standard in support of this policy.

IT Resource Logging (V.1.7). This policy requires logging to be implemented on University IT Resources.

It recognizes that logging and log review is an important information security control.

Departments have flexibility in determining the detail contained in IT Resource logs for their area of responsibility. ITNS and the SO Group have issued a Basic Logging Standard in support of this policy.

All policies went into effect on March 1, 2010. They can be found at: http://www.purdue.edu/policies/pages/information_technology/info_tech.html

The new and revised policies were announced in the February 16, 2010 edition of Purdue Today.

The standards issued in support of the Remote Access and Logging policies are available at: <http://www.purdue.edu/secure-purdue/bestPractices/IT-Standards.cfm>

SECURITY RESOURCES

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

- *SiteAdvisor*
<http://www.siteadvisor.com/>
- *Federal Trade Commission*
<http://ftc.gov>
- *Center for Internet Security*
<http://www.cisecurity.org/bench.html>
<http://www.purdue.edu/securepurdue/bestPractices/adminResources.cfm>