From: coe-l-bounces@lists.purdue.edu [mailto:coe-l-bounces@lists.purdue.edu] **On Behalf Of** Evans, Robert F.
Sent: Monday, April 23, 2012 12:30 PM
To: 'coe-l@lists.purdue.edu'
Subject: [COE-L] Purdue IT Security Incident Response

Dear College of Education,

The Education IT team recently attended Purdue IT Security Incident Response training. Because some of you have access to restricted and/or sensitive Purdue data, we want to communicate our checklist for how we must respond to an IT Security Incident in your area. We're sorry for such a long email that follows. The reality is that there is a lot going on behind the scenes in IT security and Purdue is legally bound by numerous federal, state and local laws to respond to IT security issues. We feel it is important to pass some information along and keep everyone in the loop...

WHAT IS AN IT SECURITY INCIDENT?

By IT Security Incident we basically mean that a Purdue-owned computing device has been accessed or modified ("compromised") by unauthorized users and/or malicious software (malware). This could potentially lead to a "breach/disclosure" of Purdue restricted and/or sensitive data. Such a data breach/disclosure is a violation of Purdue policy and potentially federal, state and local laws.

WHAT IS RESTRICTED AND SENSITIVE DATA?

Restricted data includes:

- Social Security Number
- Grades
- GPA
- Transcripts
- Personally Identifiable Information that students have opted not to make public
- See: http://www.purdue.edu/securepurdue/policies/dataConfident/restrictions.cfm

Sensitive data includes:

- Purdue ID Number (PUID)
- Birth Date
- Ethnicity
- Course Rosters

- See: http://www.purdue.edu/securepurdue/policies/dataConfident/restrictions.cfm

HOW DOES IT HAPPEN?

An "IT Security Incident" can happen in various ways. We've seen it happen as a result of surfing to a web site that causes the web browser to download malware which infects the computing device. We've seen malicious "payloads" come through email by way of executable programs disguised as tax updates, shipping confirmation, greeting cards, etc. We've seen email scams and targeted phishing schemes designed to lure a user to a fake "Purdue web site" where they are asked to log in with a Purdue career account, thus stealing Purdue IDs and passwords. Sometimes unauthorized users try brute force cracking of weak passwords, or network port scanning of insecure computing devices. Any of these can lead to a compromised computing device and a breach/disclosure of restricted/sensitive Purdue data.

HOW DO WE KNOW WHEN IT HAPPENS?

The central Purdue IT Security Group may notify the Education IT team if the central network intrusion detection system or other networked systems detect a potential compromise. Outside organizations may also notify Purdue if they detect suspicious activity originating from a Purdue computing device. For example, the Motion Picture Association of America (MPAA) will contact Purdue if they detect that a system is illegally distributing copyrighted movies.

If a College of Education user detects a potential security problem with their computing device, they should immediately **contact Education IT** (edit@purdue.edu, 765-494-2658). The user should let us know if the computing device in question contains or has access to restricted and/or sensitive Purdue data.

HOW DO WE HAVE TO RESPOND?

When the Education IT team learns of a potential problem, we will visit the computing device, assess the situation and determine if the problem is truly a compromised computing device or a routine software problem. If the computing device does seem to be compromised, and if it contains or has access to restricted/sensitive data, we will need to elevate the case to the central Purdue IT Security Group and below are the steps we need to take...

1. Education IT will immediately remove the network cable from the computing device (or turn off the network card) to isolate the device from the network. Removing access to the network means no further disclosure of data can occur through the network.
2. All office staff must stop using the computing device for any purposes. The computing device must be left untouched, powered on, and sitting idle until Purdue authorities arrive.
3. Education IT will notify the central Purdue IT Security Group that a computing device containing or having access to restricted/sensitive data has been compromised.

4. Within approximately 24 hours, the central IT Security Group will arrive and begin conducting forensic analysis on the computing device to determine if Purdue restricted/sensitive data has been **stolen**. Especially in cases involving restricted data, they will likely confiscate the internal hard disk (if applicable).
    a. Local user data stored on an internal hard disk will also be confiscated and may not be immediately returned to the user until the investigation is complete. Purdue IT Security staff will analyze data on the hard disk, along with Purdue network traffic logs, to determine if a data breach has occurred and to what extent the breach occurred.
5. If the central IT Security Group has removed the hard disk, Education IT will work with the office/user to replace the hard disk that has been removed so the computing device can again be used. The office may need to purchase a new hard disk for about $100.00 if Education IT is unable to locate a spare hard disk to install in the computing device.
6. Education IT will "reimage" the software on the computing device and work with the office/user to get them back up and running. When the central IT Security Group has finished their investigation, the user's local data should be returned. Education IT will work with the user to restore the data to the computing device.
7. If it is determined that a breach/disclosure of Purdue restricted or sensitive data has occurred, this will trigger a series of events that are included in the Purdue data breach checklist maintained by the central IT Security Group. These may include:
    a. Notification of Purdue administrators
    b. If social security numbers are involved, notification sent to the Indiana Attorney General's office which will begin its own investigation
    c. Notification sent to federal agencies if needed
    d. Notification sent to news media if needed
    e. Notification sent to users whose data has been disclosed
    f. Creation of a staffed 800 number hotline
    g. Free credit checks provided to all users affected by the breach/disclosure.
    h. As we understand it, all of these steps must be funded by the local unit/department

WHERE CAN THE FULL POLICY BE FOUND?

Purdue IT policies apply to everyone at Purdue, not just IT staff. So it's a good idea to be familiar with them. The Purdue IT Incident Response policy can be found here:

Purdue Incident Response Policy
http://www.purdue.edu/policies/information-technology/viib3.html

Data Classification
http://www.purdue.edu/securepurdue/policies/dataConfident/restrictions.cfm

Central Reporting Tools
http://www.purdue.edu/securepurdue/bestPractices/securityIncident.cfm

All Purdue IT Policies
http://www.purdue.edu/policies/information-technology.html

THANK YOU

Thank you for helping to keep Purdue data and IT resources secure! ☺

Regards,
The Education IT Team (edit@purdue.edu)

\\
robert evans
director \ office of information technology \ purdue university \ college of education

T 765.496.1819 F 765.494.5832
E bob @ purdue.edu R brng 6129
I http://www.education.purdue.edu/edit
"vision is the ability to see what is possible before it becomes obvious"