Paradise Valley Community College
College Identity Management System (CIMS) Implementation
Workstation Security Procedures

Purpose

The nature of higher education is to foster an open academic environment. That is at odds with the need to protect sensitive information. The concept of an open environment is quite contrary to the need to protect sensitive information. There is risk of exposure of information and data stored on Paradise Valley Community College (PVCC) workstations given constantly evolving and new vulnerabilities discovered every day. The risk of information and data exposure stored on PVCC workstations is high given the new and modified vulnerabilities that are launched daily worldwide. Organizations with enterprise computing systems that move and store large amounts of personal information over a large network are prime targets for data theft. And, although the risk is currently less apparent on mobile devices such as tablets and smartphones, the scope of attack could be much greater should vulnerabilities be discovered, as these new business tools access more college data.

Recently (2011) a university business office was the victim of a targeted email phishing campaign. The email was branded appropriately, appearing to come from the university's CFO, and contained a link that appeared to be part of the university's web site. Once the department employees went to the web site, malware was downloaded that installed a key logger. A key logger records every keystroke made on a given computer. It took some time for the university to discover the bank transfer of funds ($996,000) from them to an offshore entity.

Individuals in the business of spamming/phishing/web attacks are no longer "script kiddies", they are organized cyber crime professionals who are transnational, national, or local groupings of highly centralized enterprises created for the purpose of engaging in data theft for profit. With the implementation of CIMS/Active Directory, there are technical measures PVCC can take to ensure appropriate and long overdue data and technical resources protection. This procedure defines the level of access rights to PVCC workstations and strategies for mitigating the risks.

Definitions

There are various levels of access to a workstation.

- User Rights: Cannot install software
- Administrative Rights: Can install software

Personally Identifiable Information (PII) can be described as information that can be used to uniquely identify, contact, or locate a single person or can be used

with other sources to uniquely identify a single individual. That may be defined as a date of birth, social security number, driver's license number, etc. PII may also be considered FERPA protected information.

Workstation Protection Strategies

Protecting sensitive data requires a multi-tiered approach to mitigate the risks against unauthorized access to college computing resources and violating FERPA.

- Every PVCC workstation will have functioning security software installed, and local firewall enabled on employee workstations.
- Every PVCC staff, faculty are initially exempt, that handles FERPA protected information will have user rights to their desktop computer or laptop.

Mitigating the Risks

There are risks to allowing a faculty or staff member who handles limited or restricted information to have administrative rights. Adware/malware/spyware/ rootkits may still be installed on the machine by clicking on a link in an email or visiting sites and using desktop applications that are known to install malicious software such as gaming, illegal downloads of music/movies, gambling, etc. Repairing a workstation after an incident has been calculated to cost PVCC, an average of $2,000 per incident. The dollar figure is based on real incidents at PVCC over the past 3 years, and includes

- Prorated malware/anti-virus/rootkit remediation software costs;
- Staff time to remediate that includes removal of the computer from the network and working environment, and completely sanitizing and/or rebuilding the workstation;
- Employee productivity loss which incurs an organizational cost;
- IT managers time to counsel the employee about the risks and their responsibility in protecting Maricopa technical resources.

In order to mitigate further risks by employees with administrative rights

- The employee will have administrative rights taken away, after the first incident, until he/she meets with the Dean of Information Technology. This time will be used to help the employee understand the dangers of what caused the issue, and what they can avoid to further protect themselves and the institution from future threats.
- The employee will have all administrative rights removed after a second incident of workstation infection or exploit. Administrative rights will not be restored without administrative approval.

Impact on End Users

Employees who handle sensitive data, as defined above, will only be able to have software installed on their computers by submitting a request using the online form at http://www.pvc.maricopa.edu/it/software-requests