University Information Technology Services for Cybersecurity Awareness and Protection

Cong CUI¹,a, Qing-hua TU¹,b, Erik SEIDEL²,c and Song-jie WEI²,d*

¹Division of Informatization Construction and Management, Nanjing University of Science and Technology, Nanjing, Jiangsu, China
²School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, Jiangsu, China

¹cuicong@njust.edu.cn, b tqh@njust.edu.cn, c erikseidel@gmail.com, d swei@njust.edu.cn

*Corresponding author

Keywords: Information Service, Cybersecurity Training, Campus Network

Abstract. Information technology (IT), including computers and computer networking, has provided major benefits to modern education and research activities in universities. However due to security vulnerabilities, campus computers and networks are under severe threat of cyber attacks, which undermine the effectiveness of IT practice on campus. While reactive anomaly detection and recovery capabilities are effective as countermeasures when encountering cyberspace attacks, precautionary cybersecurity awareness and protections are more promising in surviving the dynamic, heterogeneously evolving future cybersecurity threats. This paper overviews the significant cybersecurity threats in modern universities, and surveys and categorizes what kind of services the campus IT departments are obligated to provide for user awareness and resilience on cyber attacks. While we review the security aspects of current IT services in Chinese universities and identify those significant parts missing, suggestions are made to migrate the gap between the current sole security detection and reaction, and the necessary security awareness plus readiness.

Introduction

The fast-paced development of information technology has had a significant impact on the way in which research, teaching and learning is conducted in modern universities. New and emerging technologies, such as the Internet, email, wireless network and mobile devices, greatly facilitate and transform the traditional process of faculty and students’ activities in campus life. Computer communication networks and computation-capable electronic devices play an indispensable role in on-campus learning and resource distribution, collaborative and distance learning, audio-visual education, course delivery and management, etc.

In order to fulfill the requirements of information technology teaching and research, and to provide reliable services, university IT departments need to maintain both the accessibility and security of computer, network, and data resources, and to ensure the integrity and confidentiality of information. The physical and logical reliability of these resources should be protected against threats such as unauthorized intrusions, malicious misuse or inadvertent compromise.

This paper discusses the key security elements and protection approaches on campus information security, with respect to the training and guiding services on the security awareness of information technology users on campus. We review and discuss the most effective approaches on reinforcing each aspect of campus information security, including user account, data, software, computer and network.

1. Security Threats on Campus Computers and Networks

As computing and computer networking assumes an ever more critical role in the university environment, cybersecurity questions have increasingly come to the fore and the online threats to
the campus and the university have become an ever present concern to university administrators and IT staffs. This is in line with trends throughout society as a whole. As Gordon Snow, then Assistant Director of the FBI’s Cyber Division, pointed out in his testimony before Congress in 2011, ‘the number and sophistication of cyber attacks has increased dramatically over the past five years and is expected to continue to grow’ and that ‘The threat has reached the point that given enough time, motivation, and funding, a determined adversary will likely be able to penetrate any system that is accessible directly from the Internet’ [1]. Thus, given the increased importance of IT in the modern campus environment and the nature of the threat posed, it is more important than ever to tackle this problem head on.

Tackling this problem is not always a straightforward matter however. As Kelly points out, universities must find a way to balance the needs of an open, collaborative university environment with the necessity of maintaining the security of campus IT infrastructure and data in as unobtrusive a manner as is practicable under the circumstances [2]. A key part of implementing such a balanced solution is by raising the awareness on the part of the users of the importance of cybersecurity, installing in them an appreciation of the importance of following certain basic but crucial cybersecurity procedures not only for their own benefit but for that of the whole community as well and by providing them with practical, easy to comprehend and comprehensive guidance and instructions in cybersecurity matters. As examples of good practice in cybersecurity awareness training and guidance, the following section offers a brief review of the cybersecurity guidance typically offered in leading American and British universities.

2. Campus Cybersecurity Guidance

The campus cybersecurity guidance provided by universities is broad in scope and covers many aspects, many of which overlap to some extent. For the sake of clarity this section is divided into three parts, each of which covers one major aspect of cybersecurity which is found in most if not all campus cybersecurity guidance from relevant universities, namely computer/workstation security, Internet and software security, and data security.

2.1 Computer/Workstation Security

An important aspect of computer & network security on university campuses is workstation security. Securing workstations is necessary to ensure that workstations connected to the campus network are free from the sorts of computer viruses & malware which might negatively affect other workstations & network health. Most university guidelines place considerable emphasis on encouraging users to exercise care with regards to computer passwords. For example Colby University advises users to ‘require a password to log on to your computer’ and to decline ‘to allow anyone else to use your computer unless they use their own accounts’ [3].

Both Colby University and another university included in this review, the University of California at Santa Cruz, provide detailed guidelines for choosing secure passwords. As with most ‘password checklists’, they place an emphasis on choosing passwords which cannot be easily guessed and recommend using both upper case & lower case characters in the passwords along with the inclusion of numbers in order to increase password strength [4]. UC Santa Cruz also recommends that passwords be easy to remember and encourages users not to write them down. Many universities surveyed recommend that users change passwords on a regular basis. In addition, some guidelines recommend that computer screens should be locked whenever the user is not physically present.

Although in the case of computer/workstation security, most guidelines place primary emphasis on passwords, many guidelines also included sections on securing the room wherein the computer and/or workstation is locates. For example, Colby University suggests that users secure their workspaces ‘by locking doors and windows as appropriate’ and to ‘turn your computer off at night or when you are sleeping (so it is off the network)’ [3].
2.2 Internet and Software Security

Internet and software security includes best practices for securing workstations from virus attacks and other security threats originating from the Internet. This category has significant overlap with the workstation security category above. Most university guidelines place considerable emphasis on two aspects, namely anti-virus software and precautions to be taken when downloading files from the Internet. For example, Colby University recommends that users ‘regularly check for and download software updates’ (which usually include security patches and fixes) and to ‘employ anti-virus software and ensure that it is up to date’. Most guidelines also advise users to take particular care when downloading files from the Internet and discourage them from downloading from unknown or otherwise suspicious sites.

Guidelines regularly include various other related pointers, such as warning users not to click on web browser pop-up windows unless they are from a trusted source, learn to recognize fraudulent messages and to delete all emails from unknown sources. Most guidelines also strongly advise against clicking on hyperlinks found within emails—especially those in emails from unknown sources as malicious use of hyperlinks are a common means of infiltrating system software & gaining privileged access to the system (also known as ‘phishing’).

2.3 Data Security

Data security is another important aspect of computer security. Many universities also offer guidance & set clear policies concerning security data. Many of the guidelines place special emphasis on the proper handling of personal data by university employees. For example the University of Manchester states that ‘personal data should only be removed and stored temporarily off the university’s central servers in exceptional circumstances’ and that ‘personal data must never be kept on laptops, PCs, or portable storage (such as USB drives) unless the device or the file has been encrypted [5]. In many jurisdictions such requirements are also mandated by relevant legislation.

As for other less sensitive data, university guidelines often recommend that backups be made on a regular schedule and that the backups be kept in secure locations. With the growing popularity of data encryption and the increased availability and ubiquity of relevant software and operating system services, it has also become more common for universities to include sections on encrypting data in their online security guidelines & reference material.

Many universities also recommend in their guidelines that special care be taken to backup and save logs and other system state information so that it might be referred to at a later date should the need arise. This is of particular importance in cases where systems have been compromised and the nature of the attack, its source and whether or not it still represents a threat to the university environment still need to be investigated and ascertained. For example, Boston University recommends that system logs be transferred to central servers on a regular schedule and provides detailed instructions to accomplish this on various operating system environments (vid. PC/Windows, Mac OS, UNIX/Linux).

Discussion

As the demands of maintaining online security grow and as computing and IT play an increasingly important role in the university environment, universities IT departments are paying ever greater attention not only to providing their user communities with the knowledge resources they need to be safe online but also putting more time and resources into offering training courses to their users and other interested parties. Most universities now offer security training & awareness courses for their students & employees training courses which cover all the aspects reviewed above. Some of these courses are taught in the classroom whilst others are offered online. A typical example of such training courses is one offered by the University of Southern California which, according to its online description, is mandatory for all employees and focuses on making instilling
in the course takers an awareness of basic cybersecurity principles, the risks one may encounter online and the necessity to take appropriate measures to alleviate such risks [6].

Such offerings are more prevalent in most western universities than they are in Chinese universities. Indeed one way by which Chinese universities right improves their cybersecurity readiness would be to increase their offerings of such training courses and indeed to take proactive measures to install within the university’s communities an appreciation for the importance of knowing and applying relevant cybersecurity measures in their daily lives. This would help to correct the generally lax attitude towards cybersecurity and the lack of knowledge of relevant rules and procedures amongst the users, which is one of the major weaknesses of Chinese universities when compared to their Western counterparts in questions of cybersecurity preparedness.

Acknowledgement

This research was financially supported by the National Science Foundation under contract No. 61472189, and by the CERNET Innovation project No. NGII20160601 on the Next-generation Internet. The authors are grateful to these grants.

References


