Chapter 24
Network and Data Transfer Security Management in Higher Educational Institutions

Winfred Yaokumah
https://orcid.org/0000-0001-7756-1832
Pentecost University College, Ghana

Alex Ansah Dawson
https://orcid.org/0000-0002-6728-4357
Kwame Nkrumah University of Science and Technology, Ghana

ABSTRACT

This chapter explored communications security through the use of an empirical survey to assess the extent of network and data transfer security management in Ghanaian higher educational institutions. Network security management controls consist of monitoring of networks, posture checking, network segmentation, and defense-in-depth. Data transfer security management includes encryption, media access control, and protection of data from public networks. Data were collected from information technology (IT) personnel. The ISO/IEC 21827 maturity model for assessing IT security posture was used to measure the controls. Overall, the result showed that the institutions were at the planned stage of communications security management. In particular, network monitoring, defense-in-depth, and the protection of data from public networks were the most applied controls. Conversely, posture checking was the least applied control. Higher educational institutions need to review their communications security plans and better manage network and data transfer security controls to mitigate data breaches.

DOI: 10.4018/978-1-6684-3698-1.ch024

INTRODUCTION

The increasing number of data breaches in higher educational institutions, coupled with high complexity of emerging network technologies, poses a challenging environment for security professionals and systems administrators to put in place adequate protection on campus networks (Custer, 2010; HEISC, 2014). Computer networks and data transfer technologies have evolved significantly (Choras, 2013). Data transfer technologies encompass the breadth of digital data flows both within an organization and between external entities across network infrastructures. Digital data flow includes transfer of data, voice, video, and the associated signalling protocols. Securing information flow traversing networks requires effective network infrastructure management (HEISC, 2014). Therefore, systems administrators need to learn, understand, and know how to configure networking software, protocols, services, and devices; deal with interoperability issues; install, configure, and create interfaces with telecommunications software and devices; and troubleshoot systems effectively. Information security professionals must understand and analyze security features and fully recognize vulnerabilities that can arise within each of the systems components and then implement appropriate countermeasures (Harris, 2013).

There have been reports on increasing numbers of security incidents in the recent times (Koch et al., 2012). According to the Verizon's annual report, 76% of data breaches were carried out through network intrusion (Verizon, 2013). There have also been a significant number of reported incidents in connection with the widespread adoption of social media (Benjamin & Chen, 2012; Chandramouli, 2011). The rapid pace of data breaches can be attributed to the growing number of network users, human vulnerabilities, the vulnerabilities in applications and operating systems, and the complexity of network infrastructures that connect several devices. As emerging technologies proliferate, organizations have become increasingly vulnerable to cyber-attacks (Pfleeger & Caputo, 2012). In particular, higher educational institutions have been experiencing data breaches in the recent times due mainly to vulnerabilities in the campus network infrastructure. Many security incidents occur over the networks as a result of inadequate management of networks and data transfer services.

Information technologies have changed the way in which higher education is delivered (Martínez-Argüelles, Castán, & Juan, 2010). Higher educational institutions use and store large volumes of data, including personal information of employees and students, sensitive institutional business data, and faculty research data. But the practices to design and institute strong and effective controls to safeguard data are often at odds with higher education's values of collaboration, openness, and sharing (Coleman & Purcell, 2015; Custer, 2010). Notwithstanding, higher educational institutions must protect sensitive and critical data (Gregory & Grama, 2013). A recent study points to the growing number of cyber-attacks on colleges and universities (Garg, 2016); heightening concern among students, parents, alumni, and donors regarding the security of the personal information these institutions store, process and transmit. According to a survey conducted by Symantec, 10% of all the reported data breaches involve the education sector (Symantec, 2014). A rather current statistics show that 35% of all data breaches come from the educational institutions (Garg, 2016). This alarming phenomenon is making information security a growing concern for higher educational institutions (Gregory & Grama, 2013).

While the effect of data breaches usually focuses on the harm to affected individuals, data breaches affect the institution experiencing the breach. Depending on the nature of the breach, potential direct financial costs of a data breach may include legal representation, fines, and the expense of notifying affected individuals (Grama, 2014). In particular, higher educational institutions may face reputational consequences and consumer confidence, which can result in a loss of alumni donations and a reduction