Data Security in Higher Education Institutions: Security Vulnerabilities from Employee’s Social Media Use

TREO Talk Paper

Chi-Lun Wu
University of Wisconsin – Green Bay
wuc01@uwgb.edu

Soo Il Shin
University of Wisconsin – Green Bay
shins@uwgb.edu

Ashley Luke
University of Wisconsin – Green Bay
lukeamo4@uwgb.edu

Abstract

Higher education institutions have adopted information security policies to formalize the use of social media (SM) for education and communication. Generally, the computer security policy and fair use of the Internet in organizations attempts to strengthen the security of student and institutional information. This study aims to explore vulnerabilities of student or institution’s information linked SM users’ behaviour behind their SM use with the role of the Internet and social media use policy in organizations. To achieve this study goal, we first examined the institutions’ Internet use policy particularly focusing on institutions of higher education in Midwestern Universities in the U.S. Second, we interviewed with the Chief-Information-Office (CIO) at the University to listen to a standardized Internet use policy and any associated risk with employees or students who are not complying with it. We also listened to how to manage potential issues of weak enforcement, resulting in security breaches regarding student and institutional information.

Our study finds that the Universities we considered have all security policies regarding the use of Internet but not clearly stated particularly regarding the SM use at working sites. Our findings from the interview with the CIO that he indicated the high compliance with strong enforcement regarding the Internet and SM use policy prevents security violations. However, the CIO said “The internet/email violations usually occur once or twice per year, and it mostly happens on social media websites”. Also, CIO mentioned an interesting aspect of security breach in higher education in that hackers do not consider university profitable targets, “…the 'bad guy' who are trying to steal data are looking for the monetarily valuable people. But, we caught a significant point from his interview, saying that “the University does not block any websites to all students and employees... We see everyone as an adult and students and faculty may use some websites for their research”. In terms of SM and email use, CIO holds his arguments that well-known SM websites such as Facebook or Twitter are not concerned since they already have control well the security vulnerability. However, he pointed out inter-departmental exchanging files seem more vulnerable if files contain sensitive information since those files can be caught by others unintentionally or intentionally, particularly if SM is used. Therefore, additional enforcement may be needed under the Internet and SM use in higher education.

Our study findings imply that social media use in institutions of higher education potentially is vulnerable so that policy should govern the fair amount of SM use at working sites in accordance with the CIO interview. Since the University that the CIO is currently working at has not blocked any websites, our study realized the level of security awareness depends totally on SM users and the ability of configuring privacy settings. In practice, we claim that the adoption of Internet and social media use policy can have a positive impact on reducing risks to data security based on the interview with CIO. Because the policy can outline the proper behaviour and use of SM to strengthen information security, we conclude that the Internet and social media use policies should warn its student and faculty members to refrain SM activities such as accepting friendship requests of strangers if they use SM during work. Future research suggests more interviews with CIOs from other institutions and measuring actual employees and students’ use of social media while they work. Also, outcomes of practical enforcements of policies from other institutions extend our current research findings.