Chapter XIV

Security, Privacy, and Politics in Higher Education

Dan Manson, California State Polytechnic University, USA

Abstract

This chapter introduces the interrelationships of security, privacy and politics in higher education. University curriculum politics are ingrained through organizational structures that control faculty hiring, retention, tenure, and promotion, and self-governance policy bodies such as academic senates and faculty curriculum committees that control curriculum approval and implementation. Compounding the politics of curriculum are different constructs of security and privacy, with security viewed as a technical issue versus privacy as a legal and organizational issue. The author believes that multiple disciplines must learn to work together to teach the constantly changing technical, scientific, legal, and administrative security and privacy landscape. While university "ownership" of security and privacy curriculum may create new political challenges, it has the potential to help limit competing faculty, department and program politics.

Introduction

Since the first Internet worm was launched in 1988 by a Cornell graduate computer science student, higher education academics and administrators have struggled to address computer security and privacy issues while teaching and using information technology. In 1989, the American Council of Education (ACE) noted that universities "have an unusual concentration of people with computer expertise and the freedom and incentive to explore frontier technologies" (Elliott, 1988). Since then, the use of Internet-enabled technology in academia has increased exponentially, in fact "economic growth has been dominated by investments in information technology and higher education" (Jorgenson, 2003).

Reflecting societal and industry needs, information technology continues to be ingrained into the fabric of higher education. Internet access, electronic mail, and personal computing devices have become "mission critical" to university administrators, faculty, staff, and students. At the same time, there are growing academic concerns over internal and external compromise of computing resources and exposures of sensitive and confidential information, and industry needs for graduates that can address these issues in government and industry.

These concerns and needs raise the following question. What are the political issues that universities face in improving security and privacy on the campus and in the curriculum? It is the perspective of this chapter that the politics of security and privacy issues in higher education revolve around the following areas:

- **Technology:** The pervasive use of computer and Internet technology used in higher education today.

- **Policy:** The development, implementation and enforcement of security and privacy policies in higher education.

- **External environment:** The growth of security incidents in higher education, application of security and privacy legislation to higher education, development of government and academic accreditation of information assurance programs, and need for graduates with knowledge of computer security and privacy domains.

- **Curriculum:** The growth of security curriculum in higher education, and corresponding political and other factors involved in higher education developing, implementing and teaching information assurance curriculum.

- **Synergy:** The opportunities in combining academic and administrative resources in creating a higher education environment that supports teaching and practicing of computer security and privacy.

8 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/security-privacy-politics-higher-education/6871

Related Content

Detection of Drive-by Download Attacks Using Machine Learning Approach
Monther Aldwairi, Musaab Hasanand Zayed Balbahaith (2017). *International Journal of Information Security and Privacy (pp. 16-28).*
www.irma-international.org/article/detection-of-drive-by-download-attacks-using-machine-learning-approach/187074

Blockchain and NFTs in IP Management: Expert Insights on Benefits, Challenges, and Future Prospects
Severin Bonnetand Frank Teuteberg (2025). *International Journal of Blockchain Applications and Secure Computing (pp. 1-40).*
www.irma-international.org/article/blockchain-and-nfts-in-ip-management/369334

Web Content Filtering
Elisa Bertino, Elena Ferrariand Andrea Perego (2006). *Web and Information Security (pp. 112-132).*
www.irma-international.org/chapter/web-content-filtering/31085

Integrating Security and Software Engineering: An Introduction
H. Mouratidisand P. Giorgini (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 200-210).*
www.irma-international.org/chapter/integrating-security-software-engineering/23085

An Improved Intrusion Detection System to Preserve Security in Cloud Environment
Partha Ghosh, Sumit Biswas, Shivam Shaktiand Santanu Phadikar (2020). *International Journal of Information Security and Privacy (pp. 67-80).*
www.irma-international.org/article/an-improved-intrusion-detection-system-to-preserve-security-in-cloud-environment/241286