Chapter 7
Cybersecurity and Data Breaches at Schools

Libi Shen
University of Phoenix, USA

Irene Chen
University of Houston – Downtown, USA

Anchi Su
University of California – Los Angeles, USA

ABSTRACT

Has anyone considered his/her family information going viral and through his/her trusted, chosen school district? This is an age where a mis-sent e-mail with student data can represent enormous liabilities, and a lost laptop can cause newspaper headlines. School institutes are facing new cyber security challenges in the Information Age. A number of school institutes were grappling with the loss of confidential information and protecting students on the Internet. How should school authorities react in case of data breach? What should they do to prevent data breaches at schools? What are upcoming trends in cybersecurity? The purpose of this chapter is to explore data breaches at K-12 schools as well as to examine the ways to improve cybersecurity. In this chapter, the researchers attempt to provide suggestions, solutions, and recommendations on cybersecurity after examining the problems of data breaches.

DOI: 10.4018/978-1-5225-1941-6.ch007

Copyright ©2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

The world is changing drastically due to the introduction and development of the Internet, high-tech products (e.g., laptop computers, smartwatches, tablets), social networks (e.g., Facebook, LinkedIn, Twitter, Instagram, YouTube), communication Apps (e.g., Skype, LINE, WeChat, WhatsApp, Snapchat), emails (e.g. Google, Yahoo), and so on. Personal information is required for the aforementioned technology gadgets and is stored in databases. Although these products are beneficial for people to communicate in the new world, there are also high risks because hackers can break into these systems to steal for personal gain. As the Congress found, "Many information technology computer systems, software programs, and similar facilities are vulnerable to attacks or misuse through the Internet, public or private telecommunications systems, or similar means…. Protecting, reprogramming, or replacing affected systems is a matter of national and global interest" (H.R. 4246, p.2).

Data breach has been a critical issue for schools in recent years. Based on Identity Theft Resource Center's Data Breach Reports, there were 783 reported data breaches with 85,611,528 records exposed in the categories of banking/ credit/ financial, business, education, government/military, and medical/healthcare in 2014; 57 (7.3%) breaches are educational with 1,247,812 records exposed (ITRC, 2014). In 2015, there were 780 reported data breaches with 177,866,236 records exposed in the categories of banking/credit/ financial, business, education, government/ military, and medical/healthcare; 58 (7.4%) breaches were educational with 759,600 records exposed (ITRC, 2015). In 2016, there were 657 reported data breaches with 28,648,522 records exposed in the categories of banking/credit/ financial, business, education, government/ military, and medical/healthcare; 65 (9.9%) breaches were educational with 410,514 records exposed (ITRC, 2016). Educational data breaches have gone upward in the past three years. These data involved public or private educational facilities from pre-schools through university level, but excluded after-schools or tutoring organizations.

Identity thieves target young children more aggressively in recent years. Based on Child Identity Theft Report 2012, 10.7% of children had someone else using their social security numbers, and the rate of identity theft for children was 35 times higher than the rate of adults in the same population (May, 2012). Criminals are targeting the youngest children and 15% of the victims were five years old and younger; "child identity thieves used their victims' Social Security numbers to open credit cards and secure auto loans, student loans, mortgages, and business lines of credit" (May, 2012, p.1). Additionally, "$1.5 million was the largest fraud committed" and "one child had six suspects using her social security number" (May, 2012, p.1). School data breaches leave young children vulnerable.

29 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/cybersecurity-and-data-breaches-at-schools/173132

Related Content

Data Security in Clinical Trials Using Blockchain Technology

Marta de-Melo-Diogo, Jorge Tavaresand Ângelo Nunes Luís (2023). *Research Anthology on Convergence of Blockchain, Internet of Things, and Security (pp. 607-625).*

www.irma-international.org/chapter/data-security-in-clinical-trials-using-blockchain-technology/310471

Security Architectures for B3G Mobile Networks

Christoforos Ntantogianand Christos Xenakis (2008). *Handbook of Research on Wireless Security (pp. 297-317).*

www.irma-international.org/chapter/security-architectures-b3g-mobile-networks/22054

E-Commerce and Cybersecurity Challenges: Recent Advances and Future Trends

Hina Gull, Dina A. Alabbad, Madeeha Saqib, Sardar Zafar Iqbal, Tooba Nasir, Saqib Saeedand Abdullah M. Almuhaideb (2023). *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications (pp. 91-111).*

www.irma-international.org/chapter/e-commerce-and-cybersecurity-challenges/314076

A Secure Cloud Storage using ECC-Based Homomorphic Encryption

Daya Sagar Guptaand G. P. Biswas (2017). *International Journal of Information Security and Privacy (pp. 54-62).*

www.irma-international.org/article/a-secure-cloud-storage-using-ecc-based-homomorphic-encryption/181548

An Optimized Reputation-Based Trust Management Scheme for MANET Security

Aida Ben Chehida Douss, Ryma Abassiand Sihem Guemara El Fatmi (2018). *Security and Privacy in Smart Sensor Networks (pp. 63-85).*

www.irma-international.org/chapter/an-optimized-reputation-based-trust-management-scheme-for-manet-security/203781