Cyber Threats to Health Information Systems: A Systematic Review

Raul Luna[i], Matthew Myhra[i], Emily Rhine[i], Ross Sullivan[i], Clemens Scott Kruse[ii], PhD, Security+
i. MHA student, ii. Assistant Professor, School of Health Administration, Texas State University

Problem / Question

Recent legislation empowering providers to embrace the electronic exchange of health information leaves the healthcare industry increasingly vulnerable to cybercrime. The objective of this systematic review is to identify the biggest threats to healthcare via cybercrime.

Objective

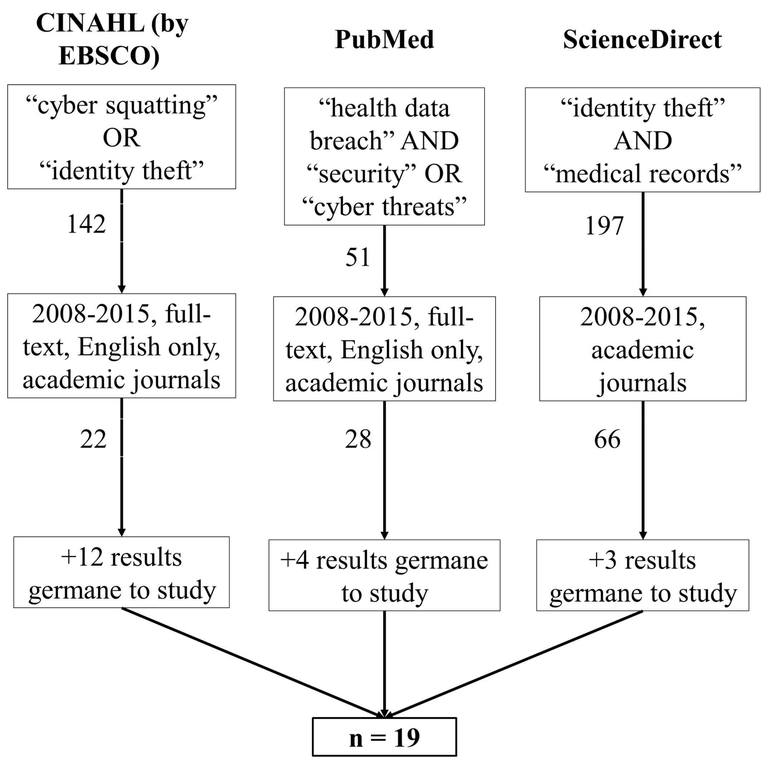
The rationale behind this systematic review is to provide a framework for future research by identifying themes and trends of cybercrime in the healthcare industry.

Methods

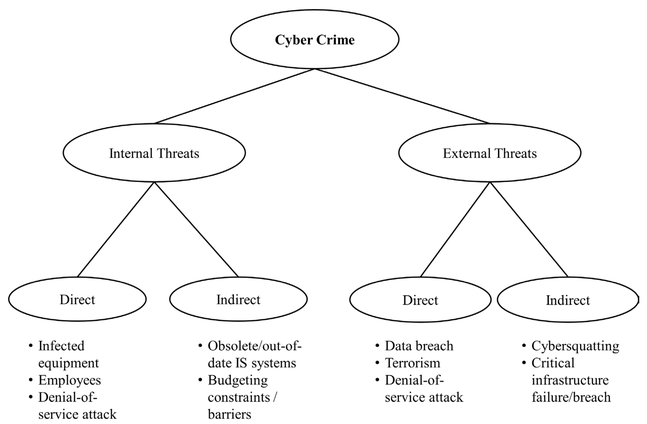
The authors conducted a systematic search through the CINAHL, Academic Search Complete, PubMed, and ScienceDirect databases to gather literature relative to cyber threats in healthcare. All authors reviewed the articles collected and excluded literature that did not focus on the objective.

Sample of Threats

Search of Research Databases



Categorization of Results



Publication

Manuscript published 10/19/2015, DOI 10.3233/THC-151102
Technology and Health Care, PMID: *26578272*
Official Journal of the European Society for Engineering and Medicine

Definition of Some Cyber Threats

Cyberterrorism: The convergence of terrorism and cyberspace directed towards a computer or network of information. This attack or breach steals information to damage or cause fear to an individual or group [10].

Cyber Security: All practices, procedures, and technologies used to protect networks such as HISs from unauthorized access or attack from hackers.

Cybersquatting: When a person other than the owner of a well-known trademark registers that trademark as an Internet domain name and then attempts to profit from it either by ransoming the domain name back to the trademark owner or by using the domain name to divert business from the trademark owner to the owner of the domain name [23].

Data breach: The acquisition, access, use, or disclosure of unsecured data, in a manner not permitted by the HIPPA.

Denial-of-Service: Short for denial-of-service attack is a type of attack on a network designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols

Excerpt from Analysis

Title	Synopsis
Medical Data Breaches: Notification Delayed is Notification Denied [5]	Summarized data-breach laws (US and Europe), the HITECH Act, assessment of penalties, causes of theft of PHI, and costs for both pt and HCO.
Cybersquatting Gives the Web a Bad Name Again [6]	Introduced cybersquatting in various industries and financial implications associated with extortion. Provided possible defenses.
A Little Information Goes a Long Way: Expertise and Identity Theft [7]	Differentiated ID theft versus ID fraud. Showed behavioral traits criminals in cybercrime exhibit and various levels of criminality.
Responding to Organized Crime Through Intervention in Recruitment Pathways [8]	Identified 3 levels of organized crime, the processes involved in recruitment, and the opportunities that motivate participants in organized crime.
A New Security Model to Prevent Denial-of-Service Attacks and Violation of Availability in Wireless Networks [9]	Describe denial of service (DoS) attacks on the IT infrastructure. Authors provided 2 solutions to mitigate the damage inflicted by cyber attackers.
Cyberterrorism: Is the U.S. Healthcare System Safe [10]?	Defined cyberterrorism and discussed hypothetical scenarios that would impede pt care and disruption of services.
Detecting Inappropriate Access to Electronic Health Records Using Collaborative Filtering [11]	Provided insights on inappropriate access and proposed a collaborative-filtering approach to predict inappropriate accesses. Results significantly improved performance over existing methods.
Using a Prediction Model to Manage Cyber Security Threats [12]	Introduced a mathematical model to predict the impact of an attack based on major factors that influence cyber security.
Concern about Security and Privacy and Perceived Control Over Collection and Use of Health Information are Related to Withholding of Health Information from Healthcare Providers [13]	Assessed the perceptions and behaviors of US adults concerning security of protected health info and how likely they are to withhold info from providers.
Security Practices and Regulatory Compliance in the Healthcare Industry [14]	Analysis identified 3 clusters (leaders, followers, and laggers) based on security practice patterns. Provided security practice benchmarks for HC administrators and policy makers.

Conclusion

The industry has now come to rely heavily on digital technologies, which increase risks such as denial of service and data breaches. Current healthcare cyber-security systems do not rival the capabilities of cyber criminals. Security of information is a costly resource and therefore many HCOs may hesitate to invest what is required to protect sensitive information.