Threats to Information Protection - Industry and Academic Perspectives: An annotated bibliography

Michael E. Whitman
Kennesaw State University, mwhitman@kennesaw.edu

Herbert J. Mattord
Kennesaw State University, hmattord@kennesaw.edu

Follow this and additional works at: https://digitalcommons.kennesaw.edu/ccerp
Part of the Information Security Commons, and the Management Information Systems Commons

https://digitalcommons.kennesaw.edu/ccerp/2016/Academic/6

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in KSU Proceedings on Cybersecurity Education, Research and Practice by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.
Abstract
Threats to information assets have always been a concern to those responsible for making information useful and defending its value. The concepts of threat, threat agent, threat events and threat sources have evolved in recent years have very precise definitions. The article includes a summary of threat classification models used in academic research is provided along with a summary of recent industry threat assessment reports. Finally, the article shares results from a recent study, 2015 SEC/CISE Threats to Information Protection Report Including a Current Snapshot of the State of the Industry, are given.

Disciplines
Information Security | Management Information Systems

Comments
Only an abstract and summary are pushed in the Proceedings. The complete article can be found in the Journal of Cybersecurity Education Research and Practice.
SUMMARY

Threats and the agencies that bring the risk of loss from them have always been present in the realm of information protection. Since the first records were kept, maintaining the availability and integrity of the information was a vital element of every record keeping technology, from cuneiform on clay tablets to today’s digital records. The characteristic of confidentiality has been added to the essential list as information owners sought to preserve privacy and maintain secrecy. The importance of information protection comes to the fore as information owners and custodians strive to maintain the three primary characteristics of information which need protection – confidentiality, integrity and availability.

The purpose of the paper is to document the evolution and understanding of threats to information as a method of supporting academic research and instruction in cybersecurity. It also serves as a summary of the current threat environment experienced in the area of information protection. Only by understanding its adversaries can an organization hope to protect its information assets. Given the complex and ever changing threat environment, defense from attack relies on persistence in devising and maintaining defenses against attacks on systems that store, process and transmit information and also requires constant vigilance and awareness of emerging and changing threats.

Additional research is needed in behavioral areas of information security. These topics directly relate to understanding threats from an insiders and outsiders respectively. As General Sun Tzu Wu wrote “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle”. It is the task of all information security professionals, academics and those managers responsible for the protection of information assets to fully understand and know their enemy in order to effective protect their assets in the ongoing campaign against threats to information protection.