Cybersecurity: Security of Networks and Information in the Financial Sector

Ion GURAN
University Politehnica of Bucharest, Romania
ionut_guran@yahoo.co.uk

Abstract

The primary objective of this article is to develop an economics-based analytical framework for assessing the impact of government incentives/regulations designed to offset the tendency to underinvest in cyber security related activities by private sector firms. IT financial systems are exposed to the many dangers that require consistent efforts to operate safely. In recent years, network and information security (NIS) risks have become more complex and their impact may vary from a small to very high range, including a domino effect. This paper is meant to analyze the modalities to secure and protect the financial sector firms from the many dangers in the online transactions.

Keywords: financial sector security, cyber insurance, cyber security policy, cyber regulations

References

[1]. Network and Information Security in the Finance Sector - Regulatory landscape and Industry priorities, European Union Agency for Network and Information Security: https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector.

[2]. Increasing cyber security investments in private sector firms Lawrence A. Gordon, Martin P. Loeb*, William Lucyshyn, and Lei Zhou - Journal of Cybersecurity, 1(1), 2015, 3–17, http://cybersecurity.oxfordjournals.org/content/cybers/1/1/3.full.pdf.

[3]. Examining the costs and causes of cyber incidents, Sasha Romanosky, Journal of Cybersecurity, 2016, 1–15, http://cybersecurity.oxfordjournals.org/content/cybers/early/2016/08/08/cybsec.tyw001.full.pdf.

[4]. https://en.wikipedia.org/wiki/Computer_security.