3-16-2024

Cyber Risk Quantification: A Teaching Case

A J. Burns
Louisiana State University and Agricultural and Mechanical College, ajburns@lsu.edu

CYBER RISK QUANTIFICATION: A TEACHING CASE

A J Burns
Louisiana State University
ajburns@lsu.edu

EXTENDED ABSTRACT

Cyber risk management is a growing area for teaching and research in cybersecurity (Baskerville et al., 2018). One key issue in allocating organizational resources against emerging cyber threats is the difficulty in quantifying risks stemming from cybersecurity incidents. This is a common problem in this domain exemplified by the reliance on semi-quantitative or qualitative risk matrices (e.g., NIST, 2012). Despite the broad applicability and flexibility of such risk assessment frameworks, chief information security officers (CIOs) and other industry leaders often express a need for more quantitative tools, especially as it relates to quantifying risk in terms of likelihood of occurrence and financial impact.

While many information systems (IS) programs are offering cybersecurity curriculum around practical hands-on offensive and defensive skills, perhaps fewer are teaching cyber risk management and quantification skills. With the recent focus on analytics in IS curriculum, cyber risk quantification is a natural complement to our cybersecurity teaching. This presentation will discuss how instructors can leverage available data sources to teach the basics of cyber risk quantification (CRQ). Figures 1 and 2 below exhibit some examples of how instructors can leverage open-source data[1] to teach cyber risk management and quantification.

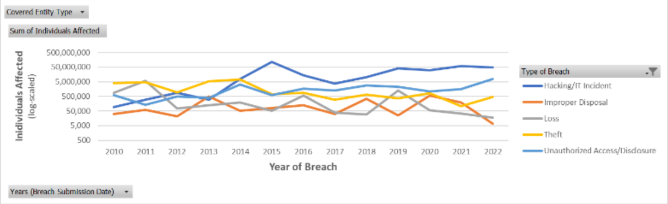

Figure 1. Breach Type Over Time

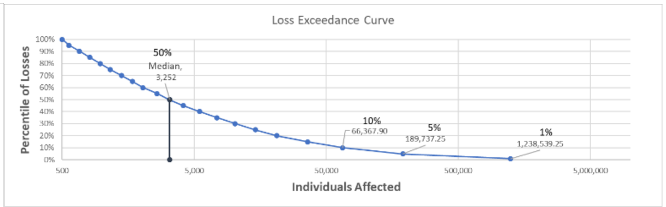

Figure 2. Losses per Incident

The goal of this presentation is to discuss ways to incorporate cyber risk quantification into cyber risk management courses. Conference participants will be asked to share their own journeys in developing cyber risk management courses.

Keywords

Cybersecurity, cyber risk quantification (CRQ), teaching case

REFERENCES

1. Baskerville, R., Rowe, F., & Wolff, F.-C. (2018). Integration of information systems and cybersecurity countermeasures: An exposure to risk perspective. *SIGMIS Database*, 49(1), 33–52.
2. NIST. (2012). Guide for conducting risk assessments. NIST Special Publication 800-30 Revision 1(Retrieved August 29, 2018, from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf