TREO
Technology, Research, Education, Opinion

Data breach response: a view from self-presentation theory

Stephen Jackson, Ontario Tech University, Stephen.Jackson@uoit.ca

A data breach, defined as the unauthorized release or access to private/confidential information, is a growing problem for firms across the globe. While there has been a growing trend in the number of studies investigating data breaches in recent years, much of the attention to date has been on the technical issues, particularly the ways to *prevent* and *detect* security threats, with fewer studies focusing on the area of *response*. More specifically, response examines the ways in which an organization reacts to a data breach after a suspected incident has been discovered.

Within response, one area of research to be further explored is data breach notification. This is particularly important given the increased enforcement of mandatory data breach notification legislation across different parts of the world. One rationale for this legislation is the requirement for firms to not only reveal to stakeholders (e.g., interest groups, employees, government bodies, investors and customers) that important data may have been jeopardized, but the very act of notification can also prompt stakeholders to exert pressure on the firm whereby stimulating the organization to strengthen its data security measures (Sen & Borle, 2015).

Notwithstanding the importance of data breach notification, a budding line of enquiry, but in need of further exploration, has acknowledged that notifications may be crafted by business managers in a manner which attempts to present the organization impacted by a data breach in a more favorable way (Jackson, 2019). An underlying motive for engaging in such self-presentation tactics is that data breaches can be seen as a form of negative news, which can be linked to loss of managerial reputation, tarnished prospects, as well as the possible reduction of financial benefits which one can receive. Drawing on self-presentation theory, the aim of this paper is to explore the different self-presentation strategies which may be used by business managers when responding to a data breach incident. Alternative explanations are also considered.

References

Jackson, S. (2019). An Investigation of the Impact of Data Breach Severity on the Readability of Mandatory Data Breach Notification Letters: Evidence from U.S. Firms. *Journal of the Association for Information Science and Technology*, 70, (11), 1277-1289.

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems, 32*(2), 314-341.