JISSec
Journal of Information Systems Security

RETHINKING SCIENTIFIC REPLICATION IN CYBERSECURITY

The Journal of Information Systems Security is a publication of the Information Institute. The JISSec's mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

Print ISSN: 1551-0123
Online ISSN: 1551-0808
Volume 20, Issue 2

www.jissec.org

Gurpreet Dhillon

University of North Texas, USA

Abstract

Scientific research goes beyond mere replication and includes a broader concept known as robustness, which entails applying diverse analyses to the same dataset. In this editorial note, we delve into the significance of replication research within the field of cybersecurity. Furthermore, we explore various genres of replication studies and their relative importance. The Journal of Information Systems Security actively encourages the publication of replication studies, and the primary objective of this editorial note is to establish comprehensive guidelines for such studies.

Keywords: Replication Studies; Trusting research; Journal of Information Systems Security.

Scientific research hinges on its ability to be supported by new data, extending far beyond simply redoing experiments or surveys using the same techniques and data – a process known as reproducibility. It also encompasses robustness, which involves applying different analyses to the same dataset. For example, Camerer et al. (2018) conducted a study aiming to replicate experiments published in Nature and Science from 2010 to 2015. Their findings showed that successful replication occurred in only about half of these cases. Interestingly, even in successful replications, the effect sizes were generally smaller than those reported in the original studies. Specifically, for the 13 studies meeting the statistical significance criterion for replication, the effect sizes in the replications were, on average, 75% of those in the original studies. Furthermore, in cases of unsuccessful replication, little to no evidence supported the original findings. The average relative effect size was almost zero for the eight studies that did not meet statistical significance criteria for replication. This raises a critical question: How much can we rely on scientific findings?

Given the significance of cybersecurity and the rising incidents of breaches and infiltrations, establishing trust in published findings is imperative for several reasons:

1. Building on existing findings is crucial to advancing our cumulative understanding. This cumulative knowledge is not confined to a particular country, context, or organizational setting. Scientific and academic research often starts by examining and extending previous work. This approach ensures that we are continually expanding and refining our understanding rather than reinventing the wheel with each study. Each piece of research contributes to existing knowledge by confirming previous findings, offering novel insights, or, in some cases, challenging and revising what we thought we knew. This process is fundamental to the scientific method and aids in gradually developing a more comprehensive understanding of a topic.

2. While contributions may not apply, generalizability is desirable. As noted by Lee and Baskerville (2003), "Because the field of information systems (IS) is not just a science but also a profession (and therefore has professional constituents such as IS executives, managers, and consultants), the generalizability of an IS theory to different settings is important not only for purposes of basic research but also for purposes of managing and solving problems that corporations and other organizations experience in society" (p. 221). This perspective holds true, especially in cybersecurity, which has practical implications for both managers and organizations. Therefore, when behavioral assertions are made and validated in a specific context and then generalized, the consequences can be significant.

In cybersecurity, replication research has never been more important due to its severe implications. Traditionally, replication is perceived as merely repeating a study's methodology to verify its initial findings. However, this view oversimplifies the process by neglecting nuances, such as the need for cultural adaptations in global studies or the inability to recreate historical events like earthquakes or past elections. Researchers often replicate methods because the underlying theories are vague, or the methods are not well understood. This is rather than believing that repeating the same steps is the key to replication. Some examples of replication studies in cybersecurity include: Shori et al (2023), Madhuvarshi et al (2023), Kaur et al (2023) and Srivastava et al (2023).

The debate between "direct" and "conceptual" replication is intriguing but may overlook the core issue. The crucial aspect is understanding how replication contributes to knowledge expansion. Replication should be seen as a fresh perspective: any study that sheds light on a previous claim, regardless of the results. This shifts the focus from repeating steps to interpreting outcomes and their implications for the original claim. Defining what qualifies as replication can be challenging, as biases and unexpected errors can influence interpretations, or glitches can affect results. The most appropriate way to address these challenges is through ongoing replication.

Replication is not a solo endeavor; it is a collective journey. Researchers should establish clear theories from the outset. The most effective theories outline how they can be tested and challenged through replication. It often takes multiple replication rounds to trust a claim. Furthermore, replication refines theories with new evidence, especially when exploring the uncharted territories of scientific knowledge. It provides solid reference points in scientific discovery's fluid process. However, it is essential to remember that no replication is an exact copy of the original; there is always some level of generalization to the current conditions.

Successful replications under various conditions help theories evolve, making them more precise. Conversely, consistent replication failures can lead to narrower theories. Determining whether a failed replication disproves an original claim or identifies a boundary condition is complex and evolves with our growing understanding.

The term "conceptual replication" is often used for studies that address the same question with different methods. While these studies are worthwhile, many do not fit our definition of replication, as they focus more on testing generalizability than actual replication. True replication requires a deep understanding of both theory and method, ensuring that the results directly relate to the original claim. Often, this means adhering closely to the original methods, especially in the early stages of theoretical and methodological development. This is known as "direct" or "close" replication. Replication using different methodologies signifies theoretical and methodological maturity. The following are some guidelines for conducting replication research in cybersecurity.

Guidelines for Conducting Replication Research in Cybersecurity:

1. **Understanding the Importance of Replication**:
    - Recognize that replication research in cybersecurity is crucial due to its significant implications for security and risk management.
2. **Broadening the Concept of Replication**:
    - Understand that replication goes beyond mere methodological repetition and should consider cultural adaptations, unrepeatable historical events, and the need to interpret outcomes.
3. **Shifting Focus to Knowledge Expansion**:
    - View replication as an opportunity to contribute to knowledge expansion by shedding light on previous claims, regardless of the results.
    - Emphasize the importance of interpreting outcomes and their implications for the original claim.
4. **Defining Replication**:
    - Acknowledge that defining what qualifies as replication can be challenging due to biases, errors, and unexpected issues.
    - Address these challenges through ongoing replication and careful documentation.
5. **Collaborative Approach**:
    - Understand that replication is a collective endeavor, and researchers should establish clear theories from the outset.
    - Develop theories that outline how they can be tested and challenged through replication.
6. **Multiple Replication Rounds**:
    - Recognize that it often takes multiple rounds of replication to establish trust in a claim.
    - Appreciate the iterative nature of replication in refining theories.
7. **Evolution of Theories**:
    - Understand that successful replications under various conditions help theories evolve, making them more precise.
    - Acknowledge that consistent replication failures may lead to narrower theories.
8. **Interpreting Replication Failures**:
    - Realize that determining whether a failed replication disproves an original claim or identifies a boundary condition can be complex and may evolve with growing understanding.

9. **Direct or Close Replication**:
    - Differentiate between "direct" or "close" replication and "conceptual replication."
    - In the early stages of theoretical and methodological development, consider closely adhering to original methods for a more faithful replication.
10. **Methodological Maturity**:
    - Understand that using different methodologies signifies theoretical and methodological maturity.

References

Camerer, C.F., Dreber, A., Holzmeister, F. et al. (2018) Evaluating the replicability of social science experiments in Nature and Science between 2010 and 2015. Nature Human Behaviour 2(9), 637–644.

Kaur, M., Smith, K., Dhillon, G. & Kaur, J. (2023). Antecedents and outcomes of information privacy concerns: A replication study in rural India. Association of Information Systems Workshop on Information Security and Privacy, Hyderabad, India, Dec 10.

Madhuvarshi, A., Smith, K., Dhillon, G. & Kaur, J. (2023). Understanding Generation Z's information security behaviors regarding penalties, pressures and perceived effectiveness. Association of Information Systems Workshop on Information Security and Privacy, Hyderabad, India, Dec 10.

Shori, S., Dhillon, G., Smith, K. & Kaur, J. (2023). Cybersecurity challenges due to the unethical exploitation of AI by Generation Z. Association of Information Systems Workshop on Information Security and Privacy, Hyderabad, India, Dec 10.

Srivastava, S., Dhillon, G., Kaur, R. & Dhillon, S. (2023). Information Disclosure in Digitally Evolving Rural Landscapes: A Case Study in India. TREO, International Conference on Information Systems (ICIS), Hyderabad, India, December 10-13.

Gurpreet Dhillon holds the G. Brint Ryan Endowed Chair of Artificial Intelligence and Cybersecurity at the University of North Texas, USA. He also holds honorary appointments at the University of KwaZula-Natal, South Africa and Universidade de Lisboa (University of Lisbon], Portugal. Gurpreet earned a Ph.D. from the London School of Economics. He received an Honorary Doctorate from Örebro University, Sweden in 2019. Several of his research papers have been published in FT50 journals. Additionally, he has been featured in the Wall Street Journal, the New York Times, USA Today, Business Week, CNN, NBC News, and NPR.