Guest editorial

Karen Renaud

Exploring Research at the Intersection of Intellectual Capital and Cyber Security

by Karen Renaud

Introduction

In 1983, Peter Russell preciently described the world as a global brain with an increasing number of connection networks and nodes. Dumay and Edvinsson (2013) mention Russell's description, and point out that the Internet now connects around 5 billion brains, integrating knowledge work across the globe. They also argue that knowledge is essentially a "social process" meaning that the interconnections facilitated by the Internet are crucial in expediting organizational knowledge flow. Knowledge is an organizational asset that contributes to organizational value (Sen, 2018). To capture the dimensions of this knowledge asset within organizations, the term Intellectual Capital (IC) was coined, and is described by Choong as "*the result of the network effect of utilizing various intellectual, human, capital and organizational resources*." (Choong 2008, p. 616).

Choong (2008) explains that IC is composed of (1) human capital, (2) structural capital, and (3) relational capital. Rastogi (2002) adopts a knowledge-centric perspective of IC, defining it as an organization's "*knowledge management nexus*". Dal Mas (2018) explain that IC research has been characterized by "waves". Researchers in the first wave sought to arrive at a shared terminology for IC and its components. The second wave then focused on the measurement, management and reporting of IC. The third wave is characterized by studies into IC "in context", examining managerial considerations. Dal Mas reports that a recently emergent fourth wave widens IC's perspective beyond organizations to the wider society. One societal area that has recently come to the fore is the interplay between IC and Cyber Security (Renaud *et al.*, 2019).

Cyber breaches occur with such frequency that they hardly cause a ripple on our collective consciousness. The successes of cyber criminals belie the serious efforts governments and researchers are undertaking to remedy this situation. While technical security measures have improved a great deal over the last few years, insecure human behavior still constitutes something of a challenge. The humans in question inhabit a variety of roles: ranging from the average computer users to the software developer, the person who maintains organizational systems and also managers who resource information security activities within their organizations.

This special issue contributes to the fourth wave of research into IC, mentioned by Dal Mas (2018), bringing together two important and crucial fields impacting businesses across the globe: Intellectual Capital and Cyber Security.

We received a total of 21 submissions for this special issue, and accepted 8 (38%). Two of the eight specifically address privacy-related behaviors, with four tackling human security-related behavioral aspects. These papers can be linked to the human component of IC. Ferguson *et al.*'s paper uses a justice theory lens to propose folding ethical considerations into traditional digital forensics investigation frameworks. The final paper is conceptual in nature, rounding off this special issue by leading us to question our stances when it comes to the security ceremonies people engage in, and the impact of society on these. This editorial commenced by arguing that knowledge is a social process. The final paper focuses our attention on how cyber activities are impacted by cultural and societal context, and links to relational aspect of IC. The structural component of IC is implicit in these papers, as an essential facilitator of communication and knowledge sharing.

Paper Summaries

Hsu *et al.*'s paper considers how people respond when organizations voluntarily embrace GDPR and finds a positive impact on their customers' willingness to divulge personal information. The second privacy-related paper was written by Al-Fannah *et al.*, and considers how browser developers could counteract the privacy invasive practice of browser fingerprinting, which has the potential to violate privacy.

Han focuses on the cyber security capacity of managers, and their attitudes towards compliance. Han finds that managers' attitudes and problem-solving skills have a crucial impact on employees' attitudes towards compliance. He *et al.* considers how best to encourage employees to form intentions to engage in cyber security behaviors and reports that the use of evidence-based malware reports is better than regular training. Giwah *et al.* studied the factors that influence mobile users towards engaging in protective behaviors. They found that threat severity had a negative impact while threat susceptibility had a positive impact. This suggests that efforts which focus on the severity of a data breach are likely to be less effective than those focusing on the likelihood of being caught up in a data breach.

Yigit Ozkan *et al.*'s paper addresses an area of great concern: SME cyber security. Large organizations are getting better at securing their systems and training their employees but SMEs are often too small to have dedicated cyber security staff, or do not have the resources to protect themselves to the same degree. Yigit Ozkan *et al.*'s paper proposes a maturity model that SMEs can use to gauge their existing state of cyber security, and then explains how to improve it.

Ferguson *et al.*'s paper investigates the tension between the legitimate needs of digital forensics investigators and the privacy rights of citizens. They derive a set of ethical principles from intellectual capital principles, privacy principles and investigation guidelines. They then map these onto digital forensics investigation stages to propose PRECEPT (*Privacy-Respecting EthiCal framEwork*). PRECEPT was refined in collaboration with digital forensics investigators. In PRECEPT, the paper proposes a technically and investigatively sound forensic methodology that incorporates checks and balances to ensure that respect for the IPR of individuals and organizations is a fundamental part of a digital crime investigation.

Bella's paper is aspirational and futuristic: he envisions cities with different "cultures" and considers how security ceremonies would take place within these cities. This is a paper that encourages us, the readers, to step back and consider how the ceremonies we design for users are being shaped by our own paradigms, preconceptions and lenses.

Conclusion

The variety demonstrated by these papers gives us a sense of the wide range of activities human-centered security and privacy researchers are engaging in. Step by step, the research community is making a difference, and it has been a privilege for me to edit this special issue.

References

Choong, Kwee Keong. (2008), "Intellectual capital: definitions, categorization and reporting models", *Journal of Intellectual Capital*, Vol. 9 No. 4, pp. 609-638.

Dal Mas, F. (2019), "The relationship between intellectual capital and sustainability: An analysis of practitioner's thought", In *Intellectual Capital Management as a Driver of Sustainability* (pp. 11-24). Springer, Cham.

Dumay, J. and Edvinsson, L. (2013), "IC 21: reflections from 21 years of IC practice and theory", *Journal of Intellectual Capital*, Vol. 14 No. 1, pp. 163-172.

Russell, P. (1983), *The Global Brain: speculations on the evolutionary leap to planetary consciousness*. Los Angeles: JP Tarcher.

Renaud, K., Von Solms, B. and Von Solms, R. (2019), "How does Intellectual Capital Align with Cyber Security?", *Journal of Intellectual Capital*, Vol. 20 No. 5, pp. 621-641.

Sen, Y. (2019), "Knowledge as a valuable asset of organizations: Taxonomy, management and implications", In *Management Science* (pp. 29-48). Springer, Cham.