Exploring Cybersecurity Awareness and Resilience of SMEs amid the Sudden Shift to Remote Work during the Coronavirus Pandemic: *A Pilot Study*

George Kassar ‡

‡ Ascencia Business School, Paris, France

Corresponding author: George Kassar (gkassar@ascencia-bs.com)

Abstract

The COVID-19 pandemic has caused a rapid shift to remote working, creating new challenges to cyber security, especially for SMEs, which are exposed to various cyber security risks such as phishing attacks, malware, and ransomware. To enhance SMEs' resilience to cyber-attacks, cyber security awareness is essential.

Resilience refers to the capacity to adapt and recover from significant disruptions or adversities, both for individuals and organizations (Masten 2018, Norris et al. 2007). It enables organizations to cope effectively with unexpected events, bounce back from crises, and foster future success (Duchek 2020, Lengnick-Hall et al. 2011). Resilience includes an adaptation aspect that allows firms to come out of a crisis stronger than before, which distinguishes it from robustness (Madni and Jackson 2009). Looking back at the peaks of the health crisis, it can be argued that the pandemic can be perceived as a "stress test" of unprecedented dimensions, challenging the resilience of business models, interconnected systems, societal institutions, and even entire economies (Tressel and Ding 2021). In the context of SMEs during the latter, resilience was perceived as their ability to face these challenges, such as supply chain disruptions, changes in consumer behavior, and government-imposed restrictions, etc. (Klein and Todesco 2021).

Cybersecurity is a broadly used term, whose definitions are variable, often subjective and uninformative. One of the most comprehensive definitions refers to cybersecurity as “the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights” (Craigen et al. 2014). Cybersecurity Awareness refers to the understanding and knowledge of these risks and the measures to mitigate them, which is considered as a crucial factor in protecting against cyber-attacks. Studies confirm that

cyber awareness training can improve knowledge and skills of employees, thereby reducing the risk of cyber-attacks and leading to more informed decisions (Hijji and Alam 2022)

Several models have explored the relationship between resilience and cybersecurity awareness, providing insight and useful lenses into the ways in which resilience may influence cybersecurity awareness and behaviors; two of these models are the Protection Motivation Theory (PMT) and the Dynamic Capabilities Theory (DCT). The PMT was initially developed by Rogers (1975), to describe how individuals are motivated to react in a self-protective way towards a perceived health threat. Adapted to cybersecurity, this theory proposes that individuals with higher levels of resilience are more likely to engage in protective behaviors in response to perceived cyber threats, due to increased threat appraisal and coping skills. (Li et al. 2022). On the other hand, the definition of dynamic capabilities as originally defined by Teece et al. (1997) is the ability of the firm to combine, develop and reconfigure external and internal expertise to respond to speedily changing environment. The DCT can be applied to the field of cybersecurity risk management to enhance organizational capabilities and improve response to emerging threats. (Barreto 2010, Naseer et al. 2018)

It is within this context that the present working paper scope aims at exploring the resilience of SMEs and the impact of their cybersecurity awareness amid the abrupt shift towards mass remote work during the pandemic and the subsequent increased cybersecurity risks and exposures. Accordingly, the outcomes of the observations and deductions from the literatures suggest the following proposition / belief statement:

P1: In time of crisis and abrupt challenges;

- the most practical model would be a combination of both Protection Motivation Theory (PMT) and Dynamic Capabilities Theory (DCT);
- as such, the relationship between cybersecurity awareness and resilience is critical, as promoting awareness can enhance the resilience of SMEs.

A pilot study was conducted to test the feasibility and effectiveness of the research design and data collection methods. The pilot was based on a qualitative research design drawing on data collection through an in-depth interview with conversational style approach as described by Schober and Conrad (1997), and data analysis based on the Braun and Clarke (2006) thematic qualitative analysis. A purposive sampling was used to interview three SMEs managing owners from Beirut - Lebanon, between Dec' 22 and Jan' 23.

The preliminary results of the pilot study provide initial insights of a practical model for SMEs based on a combination of the PMT and DCT which can help them develop a proactive approach to cybersecurity that incorporates both motivation and capability-building. Hence, four main themes emerged for developing the said approach. The 1st theme is conducting a thorough "risk assessment" of cybersecurity posture by identifying and assessing the level of potential threats and vulnerabilities using the PMT model. The

2nd theme is using DCT model to develop the "dynamic capabilities" necessary to respond to those risks, which includes investing in new technologies, training employees, and establishing a culture of awareness. The 3rd theme is "building motivation" among employees to take cybersecurity seriously, which can be achieved through the PMT model by highlighting potential impacts and rewarding good practices. Finally, the 4th theme is "continuous improvement", which involves ongoing monitoring, risk assessment, capability-building, and motivation-building using a combination of PMT and DCT models.

This work is a preliminary stage that requires further elaborations and generalizations. Yet, the findings from the pilot showed the potentials from integrating PMT and DCT models to enhance SMEs' cybersecurity posture and suggest that such approach could enable more proactive stance towards cybersecurity by fostering a culture of awareness, preparedness, and continuous improvement. These insights could be valuable for SMEs seeking to mitigate the risks associated with the increasing prevalence of cyber threats and attacks.

Keywords

cybersecurity awareness, SMEs, resilience, protection motivation theory, dynamic capabilities theory

Presenting author

George Kassar

Presented at

CABMR 2023 colloquium on Resilience and Cybersecurity, held on March 9, 2023, at Ascencia Business School – Collège de Paris, ISF campus, La Défense, Paris, France.

Conflicts of interest

The authors have declared that no competing interests exist.

References

- Barreto I (2010) Dynamic Capabilities: A Review of Past Research and an Agenda for the Future. Journal of Management 36 (1): 256-280. https://doi.org/10.1177/0149206309350776
- Braun V, Clarke V (2006) Using thematic analysis in psychology. Qualitative Research in Psychology 3 (2): 77-101. https://doi.org/10.1191/1478088706qp063oa

- Craigen D, Diakun-Thibault N, Purse R (2014) Defining Cybersecurity. Technology Innovation Management Review 4 (10): 13-21. https://doi.org/10.22215/timreview/835
- Duchek S (2020) Organizational resilience: a capability-based conceptualization. Business Research 13 (1): 215-246. https://doi.org/10.1007/s40685-019-0085-7
- Hijji M, Alam G (2022) Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors 22 (22). https://doi.org/10.3390/s22228663
- Klein VB, Todesco JL (2021) COVID-19 crisis and SMEs responses: The role of digital transformation. Knowledge and Process Management 28 (2): 117-133. https://doi.org/10.1002/kpm.1660
- Lengnick-Hall C, Beck T, Lengnick-Hall M (2011) Developing a capacity for organizational resilience through strategic human resource management. Human Resource Management Review 21 (3): 243-255. https://doi.org/10.1016/j.hrmr.2010.07.001
- Li L, Xu L, He W (2022) The effects of antecedents and mediating factors on cybersecurity protection behavior. Computers in Human Behavior Reports 5 https://doi.org/10.1016/j.chbr.2021.100165
- Madni AM, Jackson S (2009) Towards a Conceptual Framework for Resilience Engineering. IEEE Systems Journal 3 (2): 181-191. https://doi.org/10.1109/jsyst.2009.2017397
- Masten A (2018) Resilience Theory and Research on Children and Families: Past, Present, and Promise. Journal of Family Theory & Review 10 (1): 12-31. https://doi.org/10.1111/jftr.12255
- Naseer H, Ahmad A, Maynard S, Shanks G (2018) Cybersecurity risk management using analytics: A dynamic capabilities approach. Proceedings of the Thirty Ninth International Conference on Information Systems, San Francisco 2018..
- Norris F, Stevens S, Pfefferbaum B, Wyche K, Pfefferbaum R (2007) Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness. American Journal of Community Psychology 41: 127-150. https://doi.org/10.1007/s10464-007-9156-6
- Rogers R (1975) A Protection Motivation Theory of Fear Appeals and Attitude Change. The Journal of Psychology 91 (1): 93-114. https://doi.org/10.1080/00223980.1975.9915803
- Schober M, Conrad F (1997) Does Conversational Interviewing Reduce Survey Measurement Error? Public Opinion Quarterly 61 (4): 576-602. https://doi.org/10.1086/297818
- Teece D, Pisano G, Shuen A (1997) Dynamic capabilities and strategic management. Strategic Management Journal 18 (7): 509-533. https://doi.org/10.1002/(sici)1097-0266(199708)18:73.0.co;2-z
- Tressel T, Ding X (2021) Global Corporate Stress Tests—Impact of the COVID-19 Pandemic and Policy Responses. IMF Working Papers 2021 (212). https://doi.org/10.5089/9781513590820.001