Oct 20th, 10:30 AM - 10:55 AM

Towards an Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses

Darrell Eilts
Nova Southeastern University, de398@mynsu.nova.edu

Yair Levy
Nova Southeastern University, levyy@nova.edu

Abstract
Many small businesses struggle to improve their cybersecurity posture despite the risk to their business. Small businesses lacking adequate protection from cyber threats, or a business continuity strategy to recover from disruptions, have a very high risk of loss due to a cyberattack. These cyberattacks, either deliberate or unintentional, can become costly when a small business is not prepared. This developmental research is focused on the relationship between two constructs that are associated with readiness and resilience of small businesses based on their cybersecurity planning, implementation, as well as response activities. A Cybersecurity Preparedness-Risk Taxonomy (CyPRisT) is proposed using the constructs of *cybersecurity preparedness* and small businesses decision maker's *perceived risk of cyberattack*. This work-in-progress study will provide an empirical assessment of small businesses' level of cybersecurity preparedness relative to their decision maker's perceived risk of cyberattack. Subject matter experts (SMEs) will be used to validate a set of cybersecurity preparedness activities for small businesses in efforts to develop a benchmark scoring for the measure of cybersecurity preparedness. The SMEs will also identify weights for preparedness activities to enable benchmark scoring of cybersecurity preparedness that mitigate common cyber threats among small businesses. The construct of the decision maker's perceived risk of cyberattack is based on prior research. Additionally, this work-in-progress study will develop and validate the Cybersecurity Assessment of Risk Management to optimize Readiness and Resilience (cyberARMoRR) program for small businesses. The CyPRisT scores will be used to evaluate significant differences before and after participation in cyberARMoRR program.

Location
KC 462

Disciplines
Information Security | Management Information Systems | Technology and Innovation

SUMMARY

Small businesses are being targeted by cybercriminals and hackers due their inability to implement fundamental cybersecurity safeguards. Consequently, the impact of cybersecurity incidents on small businesses are disproportionately high because they typically have less resources to prepare and deal with cyberattacks. According to a study conducted by the Better Business Bureau, most small businesses do not survive more than two months after suffering a major data loss. Even when cyber threats are imminent, many small businesses remain under-prepared in dealing with risk. The ability of small businesses to establish a strong cyber posture has been associated with the disposition of the decision maker's (i.e., owner's or manager's) concern of cyber threat and risk perception. Thus, this work-in-progress study addresses the limited abilities of small businesses to mitigate cyber threats which leads many to significant losses after being subjected to cyberattack. A business's level of readiness is defined as an evaluation of how 'well-prepared' it is to prevent and protect from cyber threats. Resilience is having the ability to respond properly by adapting to changing conditions, recover from a cybersecurity incident, then assume close-to-normal operations within an acceptable time and total cost. Therefore, the business continuity of a small business is greatly dependent on their ability to mitigate cyberattacks and achieve an appropriate cyber posture of readiness as well as resilience.

This work-in-progress study seeks to develop and validate a Cybersecurity Preparedness-Risk Taxonomy (CyPRisT) to empirically assess small businesses cybersecurity posture then administer a program for improving their risk management. The Cybersecurity Assessment of Risk Management to optimize Readiness and Resilience (cyberARMoRR) for small businesses is a strategy program that will consist of cybersecurity preparedness activities, outcomes, resources, and references following a recommended implementation schedule. This developmental research follows a multiphase process with both qualitative and quantitative data collection methods. The instrument in development will be used for the assessment and benchmarking of *cybersecurity preparedness* as well as the decision maker's *perceived risk of cyberattack* based on common cyber threats. The construct of cybersecurity preparedness is an inventory-based measure of the prioritized cybersecurity activities guided by five functions of the NIST Cybersecurity Framework (*Identify, Protect, Detect, Respond, & Recover*). The decision maker's perceived risk of cyberattack is based on the impact and probability (likelihood) of common cyber threats identified in cybersecurity benchmark reports. Subject matter experts will be used to validate the measures of cybersecurity preparedness activities and perceived risk of cyberattack. The measures will be aligned with the program topics that will also be validated by the

SMEs. This developmental research design process integrates the phases to develop and validate the CyPRisT for empirically assessing the cybersecurity posture of small businesses with the intervention of the cyberARMoRR program intended to improve risk management though the implementation cybersecurity preparedness activities. Finally, any significant differences between the levels of small business cybersecurity preparedness as well as the decision maker's perceived risk of cyberattack before and after the cyberARMoRR program for small businesses will be analyzed and reported.