Extending Affordable & Understandable Cyber Plans to SMBs Potentially Offers the Highest Value & Greatest Impact Worldwide Re: Cyber Attacks

Rick Trilling, Brown University, EMCS 2020 Master in Cybersecurity:

ABSTRACT:

During a cyber breach or attack is not the time to determine what actions to take. Yet the cost of custom cyber plans, prepared in advance by external Managed Security Service Providers (MSSPs) and/or internal CISOs, today is beyond the means of many Small to Medium Businesses (SMBs) – which account for 90% of businesses worldwide. A cyber resource of value to so many SMBs may therefore have a substantial potential impact regarding cyber breaches and attacks.

Given the prohibitive cost of MSSPs and CISOs, SMBs require an alternative approach to proactively building cybersecurity resilience capabilities. I propose, through this research project, to create a series of generic plans, combined with easily understood directions and inquiries for generating customization, that will allow an SMB to create a cybersecurity plan in-house, at a cost that they can reasonably afford and without needing to acquire cyber expertise.

Planning in modern business functional areas, like operations and strategic management, was first available only from large consulting firms at considerable expense in the middle of the 20th century. Yet this eventually became readily and affordably available to anyone via generic, customizable plans with simple directions that non-experts could understand. An analogous approach to cybersecurity planning, distributed widely and affordably, is inevitable. Yet though cybersecurity planning will likely eventually follow that same path, it is mission-critical now, and we simply cannot wait that long; thus the impetus for making such planning tools widely available as soon as possible.

The author has completed the first phase of this research (aggregating and compiling information) and has been granted a sabbatical to complete the second phase (developing the generic plans, questions and directions for dissemination).