Chapter 1
Adaptive Incident Response Plans for Cyber Resilience in Small and Medium Enterprises:
Analysis and Increase of Cyber Security for a Small Enterprise by Designing an Incident Response Pl

Vincent Lennard Kraus
Bournemouth University, UK

ABSTRACT

This study addresses the lack of cyber-security present in a small petrol station, with a supermarket on the inside, in Dorset, England. A mixed-methods approach is implemented to create a more in-depth study to gather as much information as possible. Suggestions for implementing anti-virus software or the appropriate firewall setup are provided to enhance those problem areas. Detailed evidence for gathered information in the process is included. The solution addresses the problem by tackling the lack of cyber-security and incident response at the enterprise by providing the company with a detailed and industrial standard incident response plan. The plan consists of contact details, steps in the response process, and additional steps for some of the most likely cyber-attacks in retail, such as ransomware. A conclusion consisting of future improvements and drawbacks to set objectives and success criteria is given.

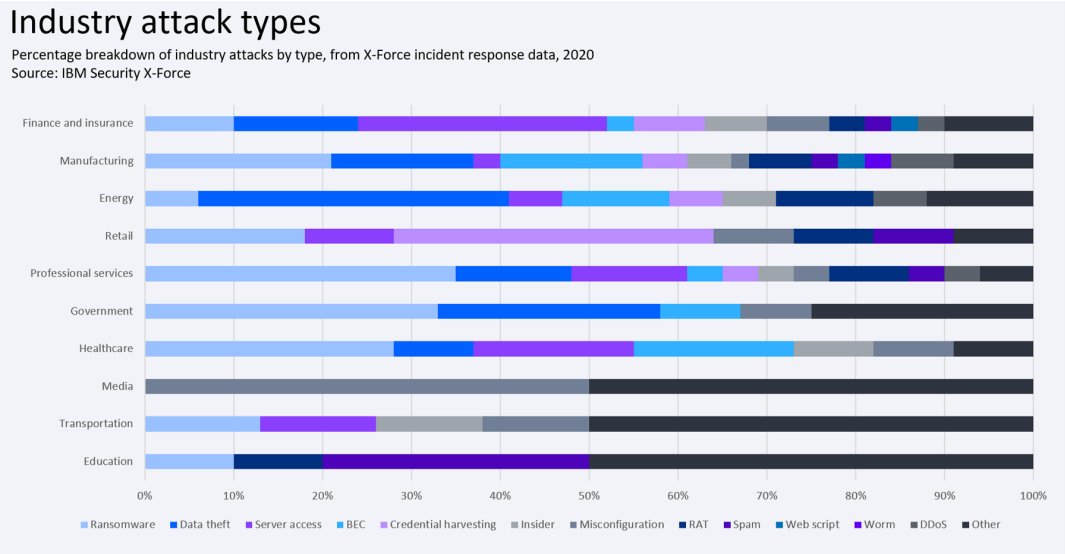
1. INTRODUCTION

Cyber-attacks are a common threat that influences society, including enterprises up to entire states and many more (Goutam, 2015). Every year new technology is released, and more, e.g., automated processes, are implemented. Moreover, more extensive data is used, transmitted, and stored on devices resulting in the need for higher security to protect the systems and data from unauthorised access (Bendovschi, 2015). Cybercriminals performing cyber-attacks seek to compromise the confidentiality (C), integrity

DOI: 10.4018/978-1-6684-7207-1.ch001

(I), and Availability (A) of systems to, e.g., compromise intellectual property to sell it for their financial gain (Holt, Smirnova, and Chua, 2016). Figure 1 provides information about the top ten industries affected by cyber-attacks.

Figure 1. Industry Attack Types in Percentage (Kessem, 2021)



As a result of the increase in cyber-attacks and the tendency to use technology in companies and the overall world, the implementation of cyber security appears to be vital (Goutam, 2015; Bendovschi, 2015). Moreover, not only big enterprises are being targeted by cybercriminals, but previous breaches have also been shown. Small business size does not provide safety from cybercriminals (Raghavan, 2017). This study focuses on the problem domain of analysing the overall cyber security in the small enterprise in Dorset, England. An in-depth investigation of the enterprise's systems and software used is necessary. Furthermore, recommendations for better cyber security in the enterprise get identified and implemented where possible. Finally, an incident response plan is implemented (solution) to give staff appropriate information on dealing with cyber-attacks such as ransomware.

The cyber security problem is that the enterprise potentially does not have strong enough security measures in place. Moreover, they might use outdated hard- and software, leading to cybercriminals compromising the enterprise at ease. The small enterprise has suffered from a ransomware attacks in the previous years hence why it is essential to enhance the security, if not done appropriately so already. They have seen the impact a cyber-attack can have on the small enterprise. With the Retail industry being ranked at place four, as seen in figure 1, it seems significant for the small enterprise to have high cyber security measures in place. Additionally, the small enterprise has no appropriate incident response hence why it is vital for them to implement one, to save valuable time in the response process. Likely, the small enterprise could not handle the cyber-attack without a delay or a full shop closure. Study research questions do current cyber security measures for the enterprise align with the industrial standards and