Chapter 11
Development of a Hybrid Policy Development Framework to Combat Cyber Threats During Crisis Events

Jason Peter Silver
Bournemouth University, UK

ABSTRACT

From the early months of 2019 to present day, the spread of the SARS COVID-19 virus has affected every aspect of modern-day life while having an especially substantial impact on the way that businesses carry out their day-to-day operations. The large spike in cybercrime can be accredited to the fact that most workers were thrust into a scenario that they were not prepared for. This could be due that most office workers lack technical skills that link into cyber security awareness and had previously relied on their in-office administrator to protect their business from outsider threats. Each office worker became an individual weak point that could be targeted outside of the protection of a configured office network. To minimise threats that companies may face when put into a crisis situation, this project will be conducted by carrying out research into cyber threat experiences that companies faced during the COVID-19 pandemic, analysing previously adopted methods and conducting surveys with various office workers to propose a solution that ensures workers are put at minimal risk.

1. INTRODUCTION

Throughout the Covid-19 Pandemic there has been a significant increase in cybercrime that has affected employees working from home. Employees being outside of the office has highlighted a weakness in the standard business cyber security model as the new threat landscape puts individual workers at greater risk being outside of the secure office. Since the pandemic began, worldwide governments have had to put into place several lockdown measures spanning several months to combat the virus at peak times (Institute for Government, 2021). During these lockdowns employees of all ranges had to carry out their

DOI: 10.4018/978-1-6684-7207-1.ch011

work digitally from home, this in turn created a large panic for business owners as they struggled to get their employees able to work digitally without losing out on any business. As a result of quickly switching to virtual working many businesses didn't consider the security measures that were needed to fully protect their employees while working from home, this neglect for cyber security/awareness has led to a rapid increase in cybercrime from the initial start of lockdown to present day with 59% of the increase being phishing/scam attempts (Interpol, 2020).

At time of carrying out this project the threat landscape clearly shows an increase in targeted attacks against employees that are working from home, the most common threats found throughout the pandemic include: Ransomware, Cryptojacking, Email related threats and Disinformation(European Union Agency For Cyber Security, 2021). The 2021 threat landscape also sees a specific increase in working from home employees being targeted by using attacks tailored around the fact that they may not be able to easily contact people from their office. The increase in cybercrime that has come about from Covid-19 has made it clear that there are significant gaps in a majority of businesses when it comes to their cyber security, which is why the need for a "Hybrid Security Policy Framework" that businesses can adapt to is so prevalent. These gaps in security that leave workers open to the aforementioned increased cyber threat have in part been caused by the lack of formality that comes with working from home. Due to the informality of working from home employees are likely to take a lax stance to security policies which when combined with out-of-date cyber awareness training can leave businesses exposed to threat actors (Kaspersky, 2020)

The proposed solution to tackle the risk of hybrid working in the case of future crisis events when working from home may be the only option for a business to carry out its day-to-day activities is to create a Cyber Security framework dubbed as a "Hybrid Policy Developmental Framework." This artefact will use data collected to determine areas in hybrid work that are most susceptible to cyber threat and require an adaptable hybrid working policy the most. The framework will include procedures that employees are to follow as well as cyber awareness resources created from research being carried out to identify the weak points in a business. This solution will be based around the "ELINAD" development framework mentioned later in the report, basing the artefact around this framework allows for consideration of new risks and threats that have been identified throughout the pandemic allowing for businesses to quickly adapt should they no longer have access to their office.

2. LITERATURE REVIEW

Cyber security has played an integral role in the successful running of businesses since the vast uptake of carrying out work on digital documents, automating tasks and making use of cloud computing (Markovitch & Willmott, 2014). The concept of cyber security is to ensure that the assets of organisations and its individual employees are protected from outside threats such as cyber criminals, these assets are often protected by physical measures, security software and policies that ensure a safe cyberspace environment is created in an office. One of the core values of cyber security is ensuring that the confidentiality, integrity, and availability of an organisation's information is kept in a strong stance; by ensuring these values are met organisations give themselves a strong foundation of security (von Solms & van Niekerk, 2013). Due to the circumstances that the Covid-19 pandemic created, a need for a greater understanding of cyberthreats has developed due to a vast increase in the types of threats that are common in today's threat landscape. The increase of cyber threats can be accredited in part to a sharp increase

Related Content