Octal0g1k
ANSWERING YOUR CYBER CHALLENGES

Cyber Risk management and Business Continuity for Small and Medium Enterprises: An Advisory

Introduction:

The COVID19 pandemic has made operations much difficult for small and medium enterprises (SMEs) for new work culture and creation of remote work environment (if possible). The COVID19 has had an unprecedented global impact on SMEs and according to a McKinsey report on SMEs in the big five European economies – France, Germany, Italy, Spain and the United Kingdom, 50% SMEs estimated that they would not survive longer than 12 months, despite the various forms of government assistance[1]. COVID19 also presented cyber risk challenges as SMEs had to quickly adapt and move to the remote working model and thus had to dig in deep into their pockets to set -up an appropriate infrastructure. Business continuity became the corner stone strategies for most SMEs.

Cyber risk has multiplied in the year 2020 and according to Fintech News, phishing attempts rose 600% since February 2020 and cloud-based attacks rose by 630% between January and April 2020 alone[2]. Thus, the remote work environment presented new opportunities for cyber criminals and made SMEs realise the importance of cyber risk management and business continuity. The question of Cybersecurity has become indispensable for any SMEs in banking, insurance, e-commerce or fintech sector and utilising cloud services and remote working methods keep their businesses running.

Cyber risk management is not just about internet and computers, but it involves people, information systems, processes, culture, and physical surroundings as well as technology. Cyber security aims to create a secure environment where businesses can remain resilient in the event of a cyber breach. Attacks in the form of hacktivism and phishing have become an everyday event and a comprehensive cyber risk management is not a viable option for SMEs with regards to time, resources, and investment required. The pandemic has made companies aware that they would not be able to grow and sustain, if they is not enough emphasis given to cyber resilience and risk-based frameworks and thus pre- emptively prepare to identify and mitigate a cyber breach.

Business Continuity for SMEs:

Business Continuity as a process builds a framework for organizational resilience. It ensures that businesses are capable enough to continue its core functions and essential operations without getting gravely impacted by unplanned events. The first step at building business continuity is to look at mitigating risk that pose immediate threats to essential resources. Identification of critical

1 COVID-19 and European small businesses | McKinsey

2 The 2020 Cybersecurity stats you need to know - Fintech News

resources and undertaking a risk assessment are at the heart of building a robust business continuity plan. Systems need to be created that have processes of prevention and recovery inbuilt to deal with threats and disaster.

Critical IT Systems must be designed to be able to pre-empt a cyber breach and take pro-active action. In addition, recovery mechanisms should be place, to start afresh from an 'ok' state of information before a cyber breach. Thus, in today's world having a full – proof business continuity plan (BCP) with 100% incident management is impossible. What works is having a structured recovery strategy, which falls back onto the best-known state, when a cyber breach takes place with an in-built escalation management system. The more complex the IT systems architecture, the more advisable to have more than one incident management system. Protection of Personally Identifiable Information (PII) must be given top priority as part of the BCP, especially in sectors such as financial and insurance.

An effective cyber business continuity lies in its planning and strategy implementation that incorporates and mitigates known threats and prepares for unknown threats and has an pre-empt model of minimising impact, when a cyber breach takes place, but invigorating second line of defences and cutting – off access to critical information such as implementing multiple fail-safe switches in an IT infrastructure architecture.

The following form the three elements of a successful BCP for an SME.

1. **Resilience:** Resilience ensures that SMEs gather an idea, as to how an event or a disaster would affect the business and how well the systems and processes put in place would respond to this disruption.
2. **Recovery:** Recovery looks deep at the risks and identifies the most vulnerable and how which assets would be able to get back sooner and faster than others and prioritising these essential operation processes and services for recovery. The categorisation of can be swapped in order of importance of the threat at hand.
3. **Contingency:** Creation of a proactive strategy that presents a course of steps taken by the SME in response to a business impact event and this must incorporate components of risk management and reflect upon recovery planning

Figure 1: Three essential elements for a successful BCP

Cyber Risk Management: The term risk management is the process to identify, assess, and control risk or threats related to an organization's earning & capital. In the framework of risk management, the possibility of threats from different sources is considered carefully. The risk could be anything, from accidents, legal liabilities, errors to financial uncertainty. In lieu of an increasingly complex IT environment, it is recommended that organisations must focus on a comprehensive 'Cyber Risk Management' strategy with focus on threat detection and response, rather than on prevention-centric strategies. Cyber risk management process identifies, analyses, assesses, and

communicates a cyber-related risk and accepts, avoids, transfers, or mitigates it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

Good cyber security teams are those that can reduce their mean time to detect (MTTD) and mean time to respond (MTTR) and thus, reduce an enterprises risk of experiencing a high-impact cyber incident or data breach. Today's complex global environment requires any organisation an approach to cybersecurity that focuses on reducing MTTD and MTTR where threats are detected and killed early in their lifecycle, thereby avoiding downstream consequences and costs. This is easier said than done for an SME.

Cyber breach life cycle: All cyber-attacks follow a unique pattern and identifiable steps that are a common nature and must get guarded against at each level to minimise risk.

1. Reconnaissance: Identifying the potential targets i.e., sensitive information
2. Compromise: Gaining access to the internal network
3. Command and Control: Utilising the compromised device / hardware with a remote access, thus establishing long-term access
4. Acting as Genuine: Compromising and impersonating an authorised user
5. Target Acquisition: Having compromised multiple access points, the deep understanding of the IT environment and its reactions to changes
6. Go for the kill: Corrupting the systems, stealing intellectual and personal information, disabling mission critical systems, shutting down access to counter measures

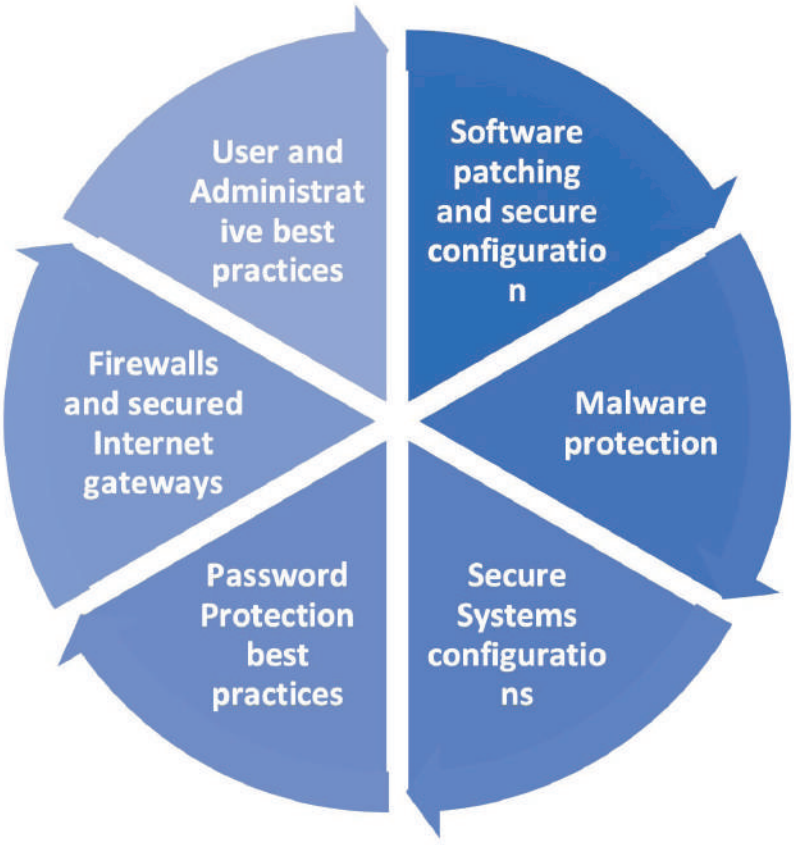
An SME challenge to Cyber Risk Assessment and Management: SMEs are not equipped with an end- to-end framework of implementing a cyber breach life cycle, and as most of an SMEs risk management services might be outsourcing, the SME is confronted with how much resources and capital to invest on pre-emptively mitigating a cyber breach? As SMEs have a small business footprint the efficacy of building an extensive planning and implementation structure that covers all the processes of cyber risk management is a stupid idea. Customised cybersecurity frameworks are needed and basic security guidelines are required to be applied in a smart and simpler way. Some of the fundamentals that could be applied to an SME level cyber risk assessment comprises of the following 6 steps.

1. Firewalls and secured internet gateways
2. Software patching and secure configurations
3. User and Administrative accounts best practices
4. Password protection best practices
5. Malware protection
6. Secure system configurations

The global risk and information security standards: Standards assist to define, design and undertake measures protecting an organisations assets and resources and support at adopting solutions that are globally recognised. Standardised cyber risk solutions such as NIST Cybersecurity Framework do full- fill a baseline criterion and standards such as ISO 27000 (a family of standards over forty in total) do provide for an overall management of information security; For example, the ISO 27001:2013 is the most widely known risk-based standard approach for the information security management system but adopts a global vision of business, process, people and technology risks and ISO 27005 is designed to assist in the implementation of information security, based on a risk management approach. Similarly, ISO risk standards such as ISO 31000:2018 relating to risk management and the

ISO 22301:2019 commonly termed as Business Continuity Management System (BCMS) standard are an end-to-end security and resilience frameworks that certifies an organisations capability at recovering from disruptive incidents.

Figure 2: SME 6 step Cyber risk assessment



Way forward for a Small and Medium Scale Enterprise (SME):

In cyber world risk and business continuity must be applied together at every step of the process and this can result in an effective and efficient cyber business management systems lowering the risk and the potential negative effects of a crisis and financial loss. Cyber risk management and Business Continuity management are interconnected. The following 4 measures are the key recommendations for an SME in curating a resilient business continuity planning.

1. Identification of threat possibility and sketch out the communication plans. Creating a roadmap to mitigate major identifiable threats
2. Standard risk management solution: The survivability of SMEs will often get threatened by cyber risks. Prioritising cyber risk standards and risk management solutions shall reduce cyber threat intensity and facilitates effective business continuity planning.
3. Effective testing, maintenance and upgrade: The proficiency of an effective business continuity is seen through an effective cyber risk management. SMEs must keep testing, maintaining, upgrading, and evaluating their threats on a continuous basis. An SME must keep tweaking its BCP avoiding faster detection and deploying a minimum response capability to reduce the damaging impact of a cyber incident.