Cybersecurity Challenges in Small and Medium Enterprise (SMEs)

Hamid Jahankhani, Lakshmi N. K. Meda, and Mehrdad Samadi

Abstract Over the past decade, digitalization has played a greater role in improving the business stature of small business by opening new venues, extending their reach, and thereby improving value producing opportunities. It also brought the small businesses additional responsibilities of having to deal with the security risks and threats which are ever-present on the digital platform. This chapter aims to review and analyse the cybersecurity risks in small businesses due to the adaption of new digital technologies. The chapter discusses the security risks and challenges dealt by small business, the key constraints in implementing a security program to comply with the legal and regulatory requirements, and how the cloud technology can answer many of those challenges.

Keywords Information governance · SME · Cybersecurity · Security information and event management (SIEM) · Cloud computing · Risk management

1 Introduction

This review chapter is designed to examine the process of SMEs' compliance with cyber security policies.

A small or medium enterprise (*SME*) is a company under independent ownership and operation, and which is not viewed as a leading firm in its sector (SBA, 2015). The American Small Business Administration uses a measure based on the value of the company and size of the workforce to categories the scale of a firm in a given industrial sector SBA (2016), U.S. Censés Bureau (2013).

H. Jahankhani (✉)
Northumbria University London Campus, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk

L. N. K. Meda · M. Samadi
Northumbria University London, London, UK

H. Jahankhani et al. (eds.), *Blockchain and Other Emerging Technologies for Digital Business Strategies*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-98225-6_1

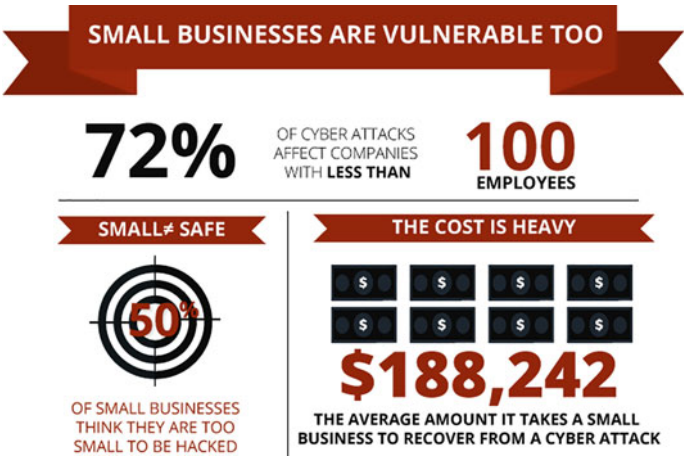

Fig. 1 Small Business security stature [3]

Information technology has increased the potential of small businesses and created vast wealth-building opportunities. The advent of various new technologies, platforms, applications had catapulted small businesses to the forefront of industrialisation and created excellent markets to showcase their business prowess. Although small businesses have been leading from the front in implementing various new technologies to improve their business, they often fell behind to improve the information security measures relative to these new technologies [1]. SMEs often lacked the resources and security strategies to counter the ever-aggressive cyber criminals. Threats such as phishing, malware, spam, ransomware etc., often led to devastation for small businesses [2]. Figure 1 shows the current security stature of small businesses.

Cybersecurity is generally offered the least priority by small business when conducting day-to-day business. According to Lurey [4], 66% of decision makers in SME's believe an attack to be unlikely, which is in contrary to the reality where 67% experienced a cyberattack. An estimated 1.6 million small businesses fall prey to cyberattacks every year (Nominet UK, 2021). The importance of security can be understated as an attack can be devastating to a small business evident by the fact that 60% of SME's are out of business within six months of an attack [5]. With the usage of smartphones, tablets and IOT devices within SMEs, securing the information and assets is of more importance than ever.

Many a times, small business owners do not have a great understanding of the information risks and information security obligations from an industrial and regulatory standard point of view. In a survey by Osborne [6] on small businesses, one of the key issues has been the lack of knowledge and resources in implementing and handling security processes. The lack of strong cybersecurity solution is evident by the following picture which shows the lack of appropriate security measures in small businesses.

Armenia et al. [7] believes that small enterprises, while not equipped with the necessary skills and knowledge to streamline the cybersecurity process, are still required to handle cybersecurity issues owing to the increased number of cyberthreats. It essential for business owners to look at cybersecurity as an integral part of business and to implement the required security policies, guidelines, and procedures and to streamline them with all the core functions of the business.

Another key constraint for small businesses is the lack of infrastructure, human resources, and the budget to implement a comprehensive IT security system. A survey by UK government [8] revealed that while small business owners are concerned about the cybersecurity risks, many lack the resources to implement a cybersecurity solution, and with merely 33% providing any sort of security training. In a similar study, 81% stated that additional resources and time would benefit to address cybersecurity problems [9]. With 52% of SMBs agreeing to the lack of IT staff within the business [10], and the lack of appropriate resources [11], cyberthreats are an inevitability for small businesses.

One of the latest technologies offering a solution to cybersecurity challenges within small business is the Cloud. Cloud is a multi-discipline technology that offers various types of solutions to small businesses and creates a level playing field to succeed in the business world. Cloud is simply described as computing capabilities accessible over a communication medium, typically, the internet. According to Moskowitz [12], small businesses are more attracted towards cloud solutions. Cloud based computing services, applications and infrastructure solutions benefits the budget and resource constraint small businesses with an ideal way to implement IT solutions. With many "pay-as-you-go or even free solutions" [13], cloud has become an affordable and viable technology for small businesses. Several cloud-based solutions in data storage, hosting services, high-performance infrastructure services, analytical applications, real-time data solutions, support services, e-learning solutions etc., enables the small businesses to focus their resources on business management instead of on procuring infrastructure and people to maintain an effective IT infrastructure.

According to recent studies, the potential of cloud solutions is evident by the growth of SMEs and the fostering business practices in small businesses. Assante et al. [14] suggest that by using cost-effective and integrated cloud solutions, small businesses can enter the markets without any large investments into IT infrastructure. The adoption of cloud-based security solutions can oversee a small business implement the required cyberdefenses strategies to comply with the legal, regulatory requirements and to mitigate any cybersecurity threats. Cloud security solutions provide with the necessary flexibility and scalability to a small business while being cost-effective. Many security solutions such as Cisco Umbrella, Fire Eye's ETP etc., use cloud technology to provide efficient, robust, and up-to-date comprehensive security to any small business without the need for any additional hardware. With most of the cloud security providers offering solutions with multiple security services such as storage, data sharing, backup, hosting etc. as a single setup solution, it makes perfect sense for small businesses to identify an appropriate solution befitting their security needs and to secure their business.

2 Implications for Social Change

SMEs face many challenges, not least their growing need to keep from harm themselves against future cyber-attack.

Gartner [15] noted the growing threat posed by cybercrime, and predicted that the cost to businesses from these attacks would rise to around $6 trillion by 2021. Due to the increase in the number of cyber-attacks, spending on ICT security rose to over $86.4 billion in 2017. The geographical areas of Asia and South America have the highest numbers of recorded cyber-attacks. The highest ranked country by percentage of ICT devices or systems attacked was India (12.87%), followed by Taiwan (9.21%), Malaysia (8.01%) and South Korea (5.56%). Those states with the lowest percentage include Denmark (0.65%), Czech Republic (0.55%), and Finland (0.34%).

Between 2006 and 2020, the USA recorded 156 significant cyber-attacks, which was higher than the total combined number of attacks in the UK, India and Germany (Visual Capitalist, 2021). A cyber-attack is considered "significant" when a government organization, or a company in the defence or high-tech industries is involved and the financial impact exceeds $1 million, Carmen Ang (2021). The consequences for cyber criminals who are apprehended are severe. For example, a convicted cybercriminal in the USA can expect to be given a 20- year prison sentence if the attack involves a government institution and the attack puts national security at risk. However, cybercrime continues to grow around the world, in spite of the identified consequences involved if caught, with particular countries apparently being more at risk of attack than others.

SMEs in general provide approximately 80% of all jobs World Economic Forum (2010), which demonstrates the key importance of such companies to the state economic growth. Despite their importance, many SMEs have failed to adopt adequate advanced cybersecurity systems, and thus their risk of suffering cyber-attack has increased due to the fact that they have automated their ICT processes over recent years Serianu (2017). While larger scale organizations have invested in adequate security measures due to their higher perceived level of risk, SMEs are left at greater risk because they cannot always afford the necessary protective measures, exposing them to greater damage when an attack occurs. SMEs in general face several challenges, especially the high costs of cybersecurity systems, limited funds, and inadequately trained staff. As part of overall business risks, many SMEs have incorporated the issue of cybercrime as part of their risk exposure, with many investing in antivirus systems as part of their security package. However, SMEs lag behind their larger corporate counterparts when it comes to the adoption of cybersecurity systems [16]. Consequently, SMEs need to develop their resilience to cyber-attacks by devising a clear cyber security plan including procedures and instructions for staff. The concept of cyberspace is now an essential feature of contemporary life.

Throughout the 1980s, banks in particular faced cyber threats from those working inside the industry, as well as from the first instances of malware, which was able to replicate itself in ICT systems. Incidents of cybercrime grew rapidly during the

1990s as the Internet became increasingly widely used. During the early 2000s, cyber-attacks against large websites were repulsed for the first time, while other forms of cyber-attack emerged, notably the theft of individual users' data and identity. In the second half of the 2000s, script injection and scripting across sites were employed for the first time, followed by the development of Tor software as well as online black-market platforms such as "Silk Road" in the second decade of the 2000s.

In the 2010s, the amount of cybercrime on the Internet has increased dramatically, particularly that involving ransomware and Nanded [17]. The inherent weaknesses of a company's security system mean that it is at greater risk of cyber-attack, and adequate allocation of both resources and technology are essential to ensure sufficient protection and security Antonescu and Birău [18].

3 Information Security Risk Management

In 2016, it was predicted that by 2021 cybercrime would cost organizations around the world around $6 trillion per year. Moreover, a report entitled Sputnik and produced by Atlas VPN revealed that cybercrime had cost organizations around the world over $1 trillion by 2020. A report by McAfee [19] showed that 20% of the participating organizations had no cyber security plans, consequently many such organizations were vulnerable to cyber-attacks. The impact of cybercrime includes, not only financial losses, but also loss or destruction of data, decreased productivity, the disclose of individuals' personal data, corporate financial data, with the resulting loss of reputation to the organization concerned Cybersecurity Ventures [20]. The issues of cybercrime are likely to increase as the numbers of Internet users are predicted to rise to 6 billion by 2022 and 7.5 billion by 2030 Cybersecurity Ventures [20].

Cybersecurity has become an essential security policy concern all around the world as ICT has become increasingly widely used and e-commerce has grown in scale [21]. It was noted by Ponsard et al. [22] that, due to the rapid increased use of ICT, cyber security is largely not addressed by organizations, while emerging new threats place unprotected organizations at higher risk of cyber-attack. Simultaneously, Watkins [23] found that the cost of implementing cyber security systems has risen due to the rise in the frequency and complex nature of attacks against industrial targets. A study by Klaper and Hovy [24] concluded that governments suffer especially damaging consequences from cyber-attacks, while individual users can learn to protect themselves against the worst consequences if such attacks happens. However, many kinds of sensitive data becomes vulnerable to cyber-attack whenever an individual's or organization's computer system is connected to the Internet. In this way, cybercrime can cause disruption to businesses, and makes customers feel concerned about their own data, leading to damage to the company's reputation.

For businesses in the SME sector, managing cybersecurity remains a significant issue due to the fact that their resources are more limited than established organizations, while they face a similar level of threat [25]. Hayes and Bodhani [26] noted that

SMEs are more vulnerable to cyber-attack largely because their data is under-valued by their management.

The management of ICT security in SMEs can be considered a branch of specific business computing systems which focuses on issues of security arising from information technology Polkowski and Dysarz [27].

According to Twisdale [28], cybersecurity remains a threat for SMEs and any related companies, and the fact that bigger scale firms have begun to address this issue means that SMEs are at even greater risk of cyber-attack. However, SMEs can still make themselves resilient in terms of cyber risk compared to bigger companies even though they have more limited available resources. Henson and Garfield [29] also note the divergence between cyber security practice in SMEs and their larger counterparts, with SMEs still having a great deal to put in place to catch up with the latter.

The management of cyber risk relates to any processes that have been implemented in order to limit the risks posed by cyber-attacks. Cyber-risks are defined as those risks arising from cyber threats. The main cyber risk management factors adopted by SMEs are as follows.

3.1 Information Technology Capability and Investment

Businesses frequently do not recognize the importance of cybersecurity, and the main reasons for this include the issues of time, price and the complex nature of security systems Henson and Garfield [29]. However, studies have indicated that the majority of organizations conduct a range of assessments to check their level of cyber security, including audits, penetration tests and vulnerability checks. Despite this, most firms are unaware of the level of investment they are making in this area, therefore there is room for improving resource allocation when it comes to cyber security issues Research data (2019). Findings by Hills and Atkinson [30] indicated that the resources of many SMEs and their levels of investment in cybersecurity are limited, despite the fact that such businesses increasingly rely on ICT systems and the availability of these [31]. The perception of the benefits of investment in cyber security is limited to that of security according to Kluitenberg [32], while a study by Fielder et al. [33] concluded that due to the shifting nature of cyber threats, investment in security is still a challenge for many companies, even those who have adequate resources at their disposal.

3.2 Management Attitude Toward Security

Studies indicate that most organizations have not yet fully developed their cybersecurity systems, which in many cases are operated by an internal employee as one of their additional duties Research data (2019). However, a nominated person to focus

on this role is essential if an organization is to develop and implement an effective cybersecurity system. Sadok and Bednar [25] note that SMEs should develop their security system by involving their employees and other insider stakeholders in both analysing the risks they face and developing their cyber security policy. In this way, the entire organization backed by support from managers can be fully involved in the development of a cybersecurity procedure Ponsard et al. [22].

3.3 Training and Awareness

According to Topping [34], awareness is an essential element of ICT security systems, although SMEs have not always viewed themselves as being at risk of cyber-attack, and often see security as being expensive and technically complex.

Aldawood and Skinner [35] found that the lack of awareness among employees is a more serious issue than companies' technical weaknesses, and consequently organizations need to focus on training staff about cybersecurity issues. Organizations' main information system users are at high risk from cyber threats, leading to both economic and data losses for individuals, corporate and governmental bodies Nilsen et al. [36], consequently SMEs should prioritise cybersecurity training for their employees Valli et al. [37].

4 Does Cloud Answer the Cybersecurity Challenges in SMEs?

Kurpjuhn [38] believes that the cybersecurity threats to a SME is as significant as a large organisation. The author states the SMEs prioritisation of business resources towards growth rather than on the security and strongly believes that cybersecurity should be a priority regardless of the business size. The authors discuss the SMEs inclination towards Cloud solutions but expresses concerns regarding the Cloud provider security breaches with examples such as Dropbox, iCloud etc.

In a study of Cybersecurity implications in small businesses, Tam et al. [39] states that most of the traditional security solutions currently in use are biased towards large businesses "in terms of scale, cost and usage" and are unsuitable for small businesses, and that more research is needed towards cybersecurity in small businesses. The authors state that the business landscape in SME is different to large organisations in terms of technical requirements and mentions the lack of technical knowledge in business owners. The authors state the potential of Cloud to traditional cybersecurity products and specifies examples such as common network scanning tools which only work in local infrastructure and not on a cloud. While the research is carried out on small businesses within Australia, the research work is true to small businesses all over the world.

In a case study of SMEs offering internet-based services, Lindström et al. [40] stressed the importance of data collection, storage, and communication. In a network of various connected devices, distributed functions, and automations systems, the real challenge according to the authors is not having cybersecurity procedures and functions in the base plan. The authors felt that "cybersecurity should not add unnecessary additional work" to businesses but current security solutions are not adaptable to small businesses which also deters the implementation of a cybersecurity solutions in a small business.

A different perspective of cybersecurity is expressed by Lloyd [41] in which he believes that advantages of cybersecurity should be discussed lot more than the business data breaches, disruption, penalties etc. The author believes that by having a robust cybersecurity programme, small businesses can create products that can achieve substantial business growth. The author clearly states that implementing the best business practices and achieving cyber resilience can be daunting but not insurmountable and is the key for small businesses to thrive in the digital world.

The importance and the benefits of Cloud platforms for SMEs is affirmed by Sultan [42] as far as in 2011. The author stated that virtualisation and grid computing, the fundamental technologies behind Cloud computing, delivers the SMEs with benefits of implementing new technologies into the business and to improve the efficiency of IT resources without any significant investment. The author stressed on the fact that the pay-as-you-go structure of most cloud solutions would be an attractive proposition to SMEs and start-ups. The author did arise concerns of relinquishing control, security and privacy issues, reliability issues etc., but felt that the benefits outweigh the concerns and Cloud can offer better security in real-time when compared to next-to-none security solutions used mostly in small businesses.

The concept of utilising Cloud as a solution for IT security issues and as a reliable way of secure communication was discussed by Zelenay et al. [43]. The authors strongly believed that the lack of resources, infrastructure and knowledge often compromises the information security in a small business. The authors believe that Cloud can become a revolutionary change in the world of IT services and will boost the role of IT in developing businesses. The benefits of Cloud to Traditional IT services were compared and the authors detail the significance of Cloud in terms of costs, speed, security, performance, scalability, and productivity. A list of some sample cloud services offering excellent data security were mentioned.

In an analysis of Information and Communication Technologies (ICT) in small businesses in Tanzania and Poland, Nycz et al. [44] states that the implementation of cloud security solution requires careful planning in choosing a reputable cloud service provider and the required services to maximize the returns for the investment by the business. The authors state the unstable business environment in small businesses due to the business owners not paying enough attention to the application of security codes and practices. The authors developed a hybrid model to secure ICT in Private Cloud Computing and tested the model successfully in a small IT company to prove the efficiency.

Assante et al. [14] pointed out the business improvements and technical efficiency as key prospects for small businesses along with the benefits of low costs, efficient

data movement, agility, and scalability. The authors analysed data from a survey among SMEs from seven different nations and stressed the importance of utilising Cloud technologies to acquire the relevant cybersecurity strategies to stay ahead of competition. The authors briefly stated about the challenges such as reliability, lack of control and security as barriers that SMEs might face while adopting cloud technologies.

A Service Oriented Architecture (SOA) based novel framework for cloud migration is proposed by Nussbaumer and Liu [45]. The authors felt the need for a business to understand its processes and requirements before migrating to the cloud. The authors proposed that the key requirements for small business cloud solution are cost, flexibility, performance, security, reliability, service and support. Even though the authors tested the framework using a business scenario, the developed framework did not include an economical perspective, hence the authors believe that the framework should be complemented with additional work on the economical feasibility before the complete effectiveness can be measured.

One of the key difficulties often faced by the small business is the ability to understand the security requirements of the business and the lack of knowledge to categorize the requirements in a systematic way which is key in choosing a proper cloud security solution. Godfrin [46] developed a cloud search model to identify the security and legal requirements for a business by providing answers to some simple questions as an input to the search. The search accesses a repository to identify a suitable solution which can be contemplated by the business according to their resources and feasibility. The authors developed a repository of several cloud services which are suggested after identifying the functional, non-functional, and legal requirements of a business. The system is sampled by IT professionals and works as it is supposed to, according to the authors.

The regulatory obligations of Cloud providers were discussed by Lovrek et al. [47], The authors discussed about the various types of cloud service architectures and the security concerns of consumers that arise due to the data processing that happens at a different location and believes that a regulatory framework for cloud services will determine the acceptability of the service. The authors stressed the requirement for a balance between strict regulation and complete freedom while keeping the key service conditions of protecting consumer data, quality of service, and possibility for cloud provider change as prime objectives of cloud providers.

5 Cybersecurity Frameworks

5.1 NIST Cybersecurity Framework

The American National Institute of Standards and Technology has created a framework consisting of a core set of cybersecurity policies, stages of implementation and overall profile which can assist many organisations, including SMEs in improving

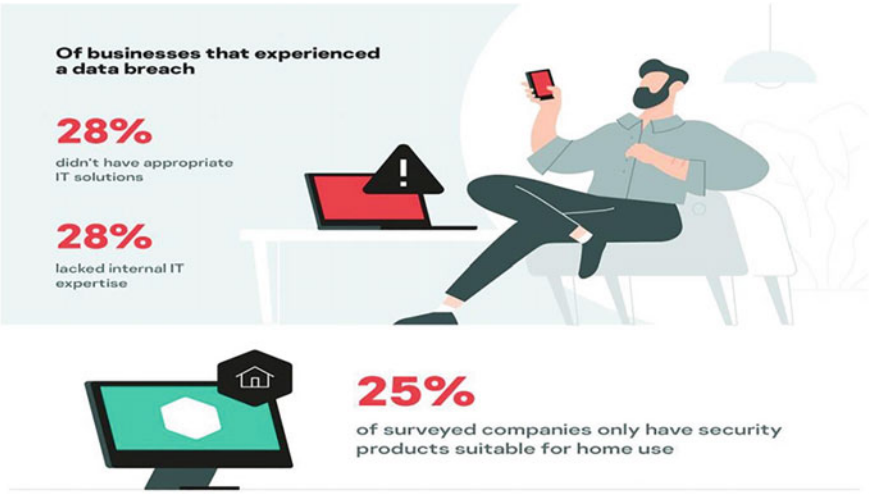

Fig. 2 Lack of appropriate security measures [49]

their cybersecurity systems NIST [48]. This framework allows for flexibility and thus it can be adopted by companies who are just beginning to build their cyber security response, or by larger scale companies with similar scale budgets NIST [48].

The framework consists of five modules as follows:

- The Identity module leads to the development of a cross-organisational approach regarding awareness and management of cybersecurity risks.
- The Protect module focuses on the infrastructure needed to develop and implement adequate security systems.
- The Detect module helps the organisation to develop adequate means of detecting the origin of cyber-attacks in a short time.
- The Respond module puts in place adequate responses to cyber-attacks which have already been identified.
- The Recovery module allows for future resilience plans to be developed as shown in Fig. 2 (Infused Innovations 2019).

5.2 The Center for Internet Security (CIS) Critical Security Controls

A set of specific controls which can be adopted to prevent cyber-attacks has been developed by a combination of national security, law enforcement, forensic and incident response organizations, and these controls can be used by firms when first developing their cyber security response. Moreover, Gerberding [50] notes that this set of controls is not as comprehensive as alternative cybersecurity frameworks.

5.3 COSO Enterprise Risk Management Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) adopted a framework which enables organizations to develop risk management strategies which consider the constantly changing need to respond to evolving cyber security risks COSO (2018). The framework consists of three concepts, namely the objectives, components and structure of the organisation. Organisations can use the control components to both identify their cyber profile and defend themselves effectively against cyber-attacks Deloitte (2015).

Control environment: identifies the management's assessment of cyber risk within the organization and their degree of awareness of steps already taken to manage this risk. Risk assessment: assesses how much the organization and its stakeholders understand the impact of how any potential cyber-attack might affect their objectives in terms of the operation, reporting and compliance. Control activities: identifies the level of internal risk management which has been written and implemented by the company to address cyber risks, according to their own internal standards. Information and Communication: this involves both internal and external methods of communication and how these are adequately secure in order to minimize cyber risk. Monitoring Activities, identifies existing systems in place for monitoring cyber risk, the controls devised and how any weaknesses are dealt with.

5.4 ISO/IEC 27001

The ISO standard offers organisations a template allowing them to set up, implement, operate, monitor, maintain and improve their Information Security Management System (ISMS). Many SMEs seek to acquire ISO27001 in place of enhance their security of ICT system, while most organizations acquire ISO17001 which shows they comply with a set of regulations and business rules which refer to the security of data.

Acquiring ISO/IEC 27001 requires the organization to complete six steps in a cross-organizational collaborative approach, as shown below:

1. Define security policy.
2. Define and scope the Information Security Management System.
3. Carry out internal risk assessment.
4. Manage identified Risk.
5. Determine the control objectives and controls for implementation.
6. Prepare applicable security statement.

5.5 Italian Cybersecurity Framework

A specific framework has been devised for the Italian market, based on the NIST framework and consisting of the core, profile and implementation stages. It enables businesses to compare their own practices against a baseline set of cybersecurity risks and procedures so that improvements can be made.

Marco and De Luca [51] note that this framework is applicable to a wide range of businesses, including SMEs and based on their individual size and characteristics. Both NIST and the government of Italy were involved in the development of this framework, but it can be applied to businesses in other locations.

5.6 Control Objectives for Information and Related Technologies (COBIT)

The adoption of COBIT offers organisations a framework within which they can develop clear ICT security policies and ensure good practice in this area. It consists of a range of ICT controls leading to the achievement of a well-defined organisational framework for use with ICT management, based on a set of regulations which must be complied with ISACA (2018). There are four key areas which COBIT covers, as described below:

1. **Plan and Organise:** focuses on how technology is used by the organisation and any improvements which may be required to ensure its goals and objectives are met.
2. **Acquire and Implement:** identifies the organization's ICT requirements in terms of obtaining, installing and maintaining the technology based on the company's existing business processes.
3. **Delivery and support:** develop a strategy to manage delivery services.
4. **Monitor and evaluate:** devises an evaluation process to ensure that the ICT system being used by the organization continues to meet the original design objectives and to ensure compliance with any identified regulations.

5.7 Information Technology Infrastructure Library (ITIL) Framework

This framework helps organisations to identify their security needs and put an integrated ICT security strategy in place based on their own requirements. The process begins with a set of non-specific guidelines which organisations can use to devise their own strategic plan, and which is not specific to any particular industry or technology.

Once these baseline requirements have been identified, companies can plan, implement and evaluate their security strategy. The guidelines consist of the following elements:

1. **Service Strategy**: examines the organization's capabilities and identifies how security can be managed in terms of designing, planning and implementing the strategy.
2. **Service Design**: focuses on service management needs in terms of designing developing the necessary strategy.
3. **Service Transition**: develops further strategies to improve capability when new or amended services are put into operational practice.
4. **Service Operation**: focuses on measuring the effectiveness of any support service involved in the strategy in order to guarantee value for the organization and the service provider.
5. **Continual Service Improvement**: develops plans to create and maintain value for customers.

5.8 Information Security for Small and Medium Sized Enterprises (ISSA) 5173 (UK)

In 2011, ISSA 5173 working group sets out recommendations on information security controls for small and medium enterprises. SME are targets of vulnerability to cyber-attacks. They are easy targets for cybercriminals due to limited resources, knowledge and infrastructure. Because SMEs have a fragile structure, they may be destroyed after a cyber-attack and data breach. Larger companies can protect themselves against attacks depending on their budget, but they also depend on the security of SMEs. Cybercriminals try to pave the way for larger companies through SMEs that have lower security. As a result, the security of SMEs is one of the major socio-economic challenges. The document published by ISSA, aimed at helping to provide an appropriate level of security for SMESs.

6 The Most Common Types of Cyber-Attacks in Businesses

According to Borna news Borna News (2021), the rapid rise of ransom cyber- attacks shows that cyber risk is not limited to one sector or industry in the economy and is becoming a financial and security threat worldwide. Cases of cyber-attacks are expected to become more widespread and complex, as the risk of hackers being caught is relatively low and the benefits of these illegal operations are high. According to the Fitch Ratings Borna News (2021), the increase and intensification of attacks is a negative factor in the credit rating of companies.

During 2020, the number of cyberattacks aimed at extortion worldwide increased by 485%, and ransomware attack was one-quarter of the total cyberattacks that took

place in the previous year. On the other hand, it is estimated that the cost of these operations was $20 billion. The number of extortionate cyberattacks in which the victim company is threatened with disclosure of stolen data is also on the rise; 77% of all attacks happened in the first three months of this year.

The increasing number of such attacks has increased the costs imposed on victims. According to the Xavier Institute Borna News (2021), the average ransom demanded in cyber-attacks was $220,000 in the first three months of this year. This shows a growth of 43% compared to the fourth quarter of 2019. New cases of cyber-attacks could add to the international efforts of governments and the private sector to prepare for such attacks.

Companies that do not have advanced and up-to-date security networks and systems are more vulnerable to cyber-attacks than other companies. However, the risks of falling victim to a cyber-attack are much higher for large and influential organisations. Hackers attack all sectors of the economy, but some parts are more attractive to them than others.

Speciality service companies such as small law firms and financial services companies are attractive targets for hackers because of their high vulnerability. Cyber-attacks against schools and health care providers doubled last year to 2354 Borna News (2021). The critical point is that the ransom does not guarantee hackers will give the stolen files to the victim or avoid publishing them, and paying a ransom can put a financial services company at greater financial risk.

Governments and corporations must believe in the growing threat posed by cyber-attacks and take the necessary measures to counter them. Cyber-attacks of any kind have a significant impact on companies and the economy, although they cannot be stopped entirely. However, their risk must be mitigated, and the motivation of hackers must also be reduced as much as possible.

The biggest unforeseen problem for small business owners in the last decade were tax matters, while today, with the growth of businesses, it can be said that the threats posed by cyber-attacks have replaced this. In its 2019 Global Risk Report, the World Economic Forum lists data misuse and cyber threats as the fourth and fifth most serious risks facing businesses around the world, respectively.

Whether a small business or a technology giant company, every company has vulnerabilities that hackers can exploit in today's world. On the other hand, hackers can target any business, regardless of its size. Start-ups and small and medium-sized businesses are more vulnerable to cyber-attacks than other businesses due to their cohesive and small structure.

According to the Forbes website Myba (2020), ransomware attacks, especially those involving RYUK which targets companies and institutions, was set to increase by 300% in 2020, with most of these attacks focusing on small businesses in the United States. Smaller firms are more vulnerable because they do not have sufficient resources to build a robust cyber security infrastructure and need to pay more attention to security guidelines and protocols.

Cybercrime has changed dramatically over the past few years and has spread to such an extent that a small or medium-sized enterprise alone does not have the knowledge and ability to deal with it. Today, hackers also start a business and sell

their anti-cyber tools and expertise in various packages and services to lower-level hackers, encouraging the growth and spread of attacks. Phishing attacks, denial of service (DoS), ransomware, and malware are common attacks that SMEs should be aware of.

- *Phishing Attacks*: A type of social engineering-based cyberattack in which hackers use disguise methods, such as fake bank portal sites or site payment pages, to access and steal users' information.
- *DDoS attacks*: Attempts to permanently or temporarily interrupt a company's online services, including sites and mobile applications.
- *Ransomware attacks*: In this type of attack, all or part of the company's critical data is stolen or encrypted by complex algorithms. The hacker then demands large sums of money to release and hand over the data key.
- *Malware Attacks*: In this type of attack, hackers inject malicious software into the operating system in various ways, thereby providing a platform for ransom or damage.

7 Security Information and Event Management (SIEM)

According to Raja et al. [52], SIEM (Security Information and Event Management) is known as the combination of different Security Event Management and Security Information Management. The major role of SIEM is to collects data and information of events from different devices and arrange them into a common format. All the events are gathered and collected for analysing the behaviour and functioning of the entire system. The analysis and monitoring of the single sources of the event can help in detecting the events of attacks such as Probe/DoS. This method is utilized for analysing the flood attacks of SYN TCP through the application of the RETE algorithm on the network. In this system, an alert alarm will sound in the case of a TCP SYN attack commitment.

Vielberth et al. [53], stated that most large and medium business organizations are utilizing the SIEM in their Centres of Security Operations so that they can get a higher level of awareness regarding cyber security practices. The utilization of SIEM will let the organizations collect and analyze the different information related to security measures in a centralized manner. This will help them in enhancing the process of threat detection and increase the reaction time to any of accidents.

As per the research conducted by Corcoran (2018), it has been mentioned that attack frequency has increased and as a result different business organizations are getting targeted by new and different attackers, hacking with more sophisticated attacking tools.

The attacks are being done on various levels in the organization's OSI models. So according to Corcoran (2018), the different business organizations need to implement the multiple layers and protocols of cyber security in order to avoid the issues and address them more effectively. But this implementation does also have a limitation that all the data and information collected in this can be mixed and it will

become difficult to correlate the different facts for deriving better results. In order to improve this, the organization need to encourage the use of Security Information and Event Management in their cyber security practices. The implementation of Security Information and Event Management will help the different business organizations in segregating all the information and filter it according to the utilization for different purposes. The utilization of Security Information and Event Management will facilitate the organization with centralized storage space for all the information related to the cyber security of the organization, for improving the different systems that are required in the organization for enhancing the security of information. Security Information and Event Management will help the business organization to defend the different vulnerabilities and attacks on their data and information. In this research, the main emphasis is provided on the benefits that are gained by the organization on adopting the SIEM and its implementation process for achieving the appropriate and effective results. Moreover, a proper explanation of the different recommendations that can help the organization in improving the process will also be provided through this research.

8 Conclusions

The importance of information security in any business cannot be understated as security risks can become threatening to the existence of the business itself if not dealt accordingly. The security risks to small businesses are no less than a large organisation and the consequences are even more damaging to a small business. The lack of required knowledge, infrastructure, security personnel, and resources often turn small businesses highly vulnerable to cyberattacks. Cloud based security solutions provides the cash-stricken small businesses with the necessary comprehensive security services to handle day-to-day threats and to secure the business from outside threats. The key characteristics of cloud security solutions such as flexibility, scalability, cost-effective, less technical, and ease of deployment often prove to be a great combination to secure a small business. The compliance of cloud solutions in accordance with GDPR, Data Protection Act, and other regulatory standards will be carried out.

References

1. Help Net Security (2021) What are the most common cybersecurity challenges SMEs face today?—Help Net Security. Help Net Security. Available at: https://www.helpnetsecurity.com/2021/07/07/smes-cybersecurity-challenges/. Accessed 5 Aug 2021
2. Witts J (2021) The top 5 biggest cyber security threats that small businesses face and how to stop them. Expert Insights. Expert Insights. Available at: https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/. Accessed 9 Aug 2021

3. Yazbeck E (2021) When it comes to Cybersecurity, the small and medium business community needs to do better. SMC Consulting. Available at: https://www.smcconsulting.be/when-it-comes-to-cybersecurity-the-small-and-medium-business-community-needs-to-do-better/. Accessed 15 Aug 2021
4. Lurey C (2019) Cyber mindset exposed: keeper unveils its 2019 SMB cyberthreat study—keeper security blog—cybersecurity news & product updates. Keeper Security Blog. Available at: https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/. Accessed 26 July 2021
5. Galvin J (2018) 60 Percent of small businesses fold within 6 months of a cyber attack. Here's How to Protect Yourself. Inc.com. Available at: https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html. Accessed 28 July 2021
6. Osborne E (2015) Business versus Technology: sources of the perceived lack of cyber security in SMEs (Working Paper). Oxford University Research Archive, p 10. Available at: https://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e/download_file?file_format=pdf&safe_filename=01-15.pdf&type_of_work=Working+paper. Accessed 6 Aug 2021
7. Armenia S, Angelini M, Nonino F, Palombi G, Schlitzer M (2021) A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decis Support Syst 147:113580. https://doi.org/10.1016/j.dss.2021.113580. Accessed 8 Aug 2021
8. UK government (2020) https://www.gov.uk/government/statistics/cyber-securitybreaches-survey-2020/cyber-security-breaches-survey-2020
9. Gough O (2016) Majority of businesses neglecting cybersecurity due to lack of resources. Small Business. Available at: https://smallbusiness.co.uk/majority-businesses-neglecting-cybersecurity-2535173/. Accessed 10 Aug 2021
10. Umawing J (2019) SMBs lack resources to defend against cyberattacks, plus pay more in the aftermath—Malwarebytes Labs. Malwarebytes Labs. Available at: https://blog.malwarebytes.com/business-2/2019/10/smbs-lack-resources-to-defend-against-cyberattacks-plus-pay-more-in-the-aftermath/. Accessed 9 Aug 2021
11. Benz M, Chatterjee D (2020) Calculated risk? A cybersecurity evaluation tool for SMEs. Bus Horizons 63(4):531–540. https://doi.org/10.1016/j.bushor.2020.03.010. Accessed 7 Aug 2021
12. Moskowitz S (2017) The small and medium-sized enterprise (SME). Cybercrime and Business, pp 45–68. https://doi.org/10.1016/B978-0-12-800353-4.00004-X. Accessed 6 Aug 2021
13. Ricci R, Battaglia D, Neirotti P (2021) External knowledge search, opportunity recognition and industry 4.0 adoption in SMEs. Int J Prod Econ 240:108234. https://doi.org/10.1016/j.ijpe.2021.108234. Accessed 12 Aug 2021
14. Assante D, Castro M, Hamburg I, Martin S (2016) The use of cloud computing in SMEs. Procedia Comput Sci 83:1207–1212. https://doi.org/10.1016/j.procs.2016.04.250. Accessed 10 Aug 2021
15. Gartner (2017) Business impact of security incidents and evolving regulations driving market growth
16. Verbano C, Venturini K (2013) Managing risks in SMEs: a literature review and research agenda. J Technol Manag Innov 8(3):186–197. https://doi.org/10.4067/S0718-27242013000400017
17. Pathak PB, Nanded YM (2016) A dangerous trend of cybercrime: ransomware growing challenge. Int J Adv Res Comput Eng Technol 5(2):371–373
18. Antonescu M, Birău R (2015) Financial and non-financial implications of cybercrimes in emerging countries. Procedia Econ Finance 32:618–621
19. McAfee (2018) Economic impact of cybercrime—no slowing Dow
20. Cyber Security Ventures (2017) 2017 Cybercrime Report
21. Kaur S, Sharma S, Singh A (2015) Cyber security: attacks, implications and legitimations across the globe. Int J Comput Appl 114(6)
22. Ponsard C, Grandclaudon J, Dallons G (2018) Towards a cyber security label for SMEs: a European perspective. In: ICISSP, pp 426–431

23. Watkins B (2014) The impact of cyber attacks on the private sector.no. August, 1-1. Whetten DA (1989) What constitutes a theoretical contribution? Acad Manage Rev 14(4):490–495. The framework outlines 7 points which you can use to evaluate your research work.
24. Klaper D, Hovy E (2014) A taxonomy and a knowledge portal for cybersecurity. In: Proceedings of the 15th annual international conference on digital government research. ACM, pp 79–85
25. Sadok M, Bednar PM (2016) Information security management in SMEs: Beyond the IT Challenges. In: HAISA, pp 209–219
26. Hayes J, Bodhani A (2013) Cyber security: small firms under fire (Information Technology Professionalism). Eng Technol 8(6):80–83
27. Polkowski Z, Dysarz J (2017) It security management in small and medium enterprises. Sci Bull-Econ Sci 16(3):134–148
28. Twisdale JA (2018) Exploring SME vulnerabilities to cyber-criminal activities through employee behavior and internet access (Doctoral dissertation, Walden University)
29. Henson R, Garfield J (2016) What attitude changes are needed to cause SMEs to take a strategic approach to information security? Athens J Bus Econ 2(3):303–318
30. Hills M, Atkinson L (2016) Towards cyber-resilient & sustainable SMES: the case study of added value from a large IT reseller
31. Santos-Olmo A, Sánchez L, Caballero I, Camacho S, Fernandez-Medina E (2016) The importance of the security culture in SMEs as regards the correct management of the security of their assets. Future Internet 8(3):30
32. Kluitenberg H (2014) Security risk management in it small and medium enterprises. In: Proceedings of 20th Twente student conference on IT
33. Fielder A, König S, Panaousis E, Schauer S, Rass S (2018) Risk assessment uncertainties in cybersecurity investments. Games 9(2):34
34. Topping C (2017) The role of awareness in adoption of government cyber security initiatives: a study of SMEs in the UK
35. Aldawood H, Skinner G (2018) Educating and raising awareness on cyber security social engineering: a literature review. In: 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE). IEEE, pp 62–68
36. Nilsen R, Levy Y, Terrell S, Beyer D (2017) A developmental study on assessing the cybersecurity competency of organizational information system users
37. Valli C, Martinus IC, Johnstone MN (2014) Small to medium enterprise cyber security awareness: an initial survey of Western Australian business
38. Kurpjuhn T (2015) The SME security challenge. Comput Fraud Secur 2015(3):5–7. https://doi.org/10.1016/S1361-3723(15)30017-8. Accessed 2 Aug 2021
39. Tam T, Rao A, Hall J (2021) The good, the bad and the missing: a narrative review of cybersecurity implications for Australian small businesses. Comput Secur 109:102385. https://doi.org/10.1016/j.cose.2021.102385. Accessed 2 Aug 2021
40. Lindström J, Eliasson J, Hermansson A, Blomstedt F, Kyösti P (2018) Cybersecurity level in IPS 2: a case study of two industrial internet-based SME offerings. Procedia CIRP 73:222–227. https://doi.org/10.1016/j.procir.2018.03.302. Accessed 11 Aug 2021
41. Lloyd G (2020) The business benefits of cyber security for SMEs. Comput Fraud Secur 2020(2):14–17. https://doi.org/10.1016/S1361-3723(20)30019-1. Accessed 18 Aug 2021
42. Sultan N (2011) Reaching for the "cloud": How SMEs can manage. Int J Inf Manage 31(3):272–278. https://doi.org/10.1016/j.ijinfomgt.2010.08.001. Accessed 6 Aug 2021
43. Zelenay J, Balco P, Greguš M (2019) Cloud technologies—solution for secure communication and collaboration. Procedia Comput Sci 151:567–574. https://doi.org/10.1016/j.procs.2019.04.076. Accessed 4 Aug 2021
44. Nycz M, Martin MJ, Polkowski Z (2015) In: 2015 7th International conference on electronics, computers and artificial intelligence (ECAI). IEEE, Bucharest. https://doi.org/10.1109/ECAI.2015.7301182. Accessed 19 Aug 2021
45. Nussbaumer N, Liu X (2013) Cloud migration for SMEs in a service oriented approach. In: 2013 IEEE 37th annual computer software and applications conference workshops. IEEE. https://doi.org/10.1109/COMPSACW.2013.71. Accessed 16 Aug 2021

46. Godfrin (2016) Legal requirements and identifying data security for cloud service. In: 2016 Second international conference on science technology engineering and management (ICONSTEM). Chennai: IEEE. https://doi.org/10.1109/ICONSTEM.2016.7560948. Accessed 19 Aug 2021
47. Lovrek I, Lovrić T, Lucic DL (2012) Regulatory aspects of cloud computing. In: SoftCOM 2012, 20th international conference on software, telecommunications and computer networks. IEEE. Available at: https://ieeexplore.ieee.org/document/6347661/authors#authors. Accessed 11 Aug 2021
48. NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity
49. Owen-Jackson C (2021) How to protect your small business from cyber-threats. Secure Futures. Available at: https://www.kaspersky.com/blog/secure-futures-magazine/small-business-cybersecurity/29177/. Accessed 25 Aug 2021
50. Gerberding K (2017) NIST, CIS/SANS 20, ISO 27001—simplifying security control assessment
51. Marco B, De Luca R (2015) Financial distress and earnings manipulation: evidence from Italian SMEs. J Acc Finance. Available at SSRN: https://ssrn.com/abstract=2596295
52. Raja MSN, Vasudevan AR (2017) Rule generation for TCP SYN flood attack in SIEM Environment. Procedia Comput Sci 115:580–587. https://doi.org/10.1016/j.procs.2017.09.117
53. Vielberth M, Pernul G (2018) A security information and event management pattern. In: 12th Latin American conference on pattern languages of programs, vol 1, no 1, pp 1–12