The Need for Information Security Management for Small to Medium Size Enterprises (SMEs)

The domain of information is one of the defining attributes and characteristics of the modern age. As a society, more of us are employed generating, collecting, handling, and processing information than in any other time in our history, it has become the most important profession and continues to grow in its significance [Nemati 2007]. Although this technological advancement has brought about many improvements and has made our lives easier in a lot of areas, it has also increased the ability of those who wish to do us harm. Information security is crucial to our modern digital age and is only growing in relevance and importance [Santos-Olmo et al, 2016]. When describing and discussing the introduction and implementation of information security regimes in small and medium enterprises (SMEs) against implementation in much larger organisations, it is critical to frame the topic around three key contexts. These contexts add depth and insight to the description and discussion and help to highlight its various implications around the information security regimes. These contexts include: justifying the need for sound information security management in SMEs; ethical issues in information security management; and security training and education. Information security has recently been viewed as one of the foremost concerns [Santos-Olmo et al, 2016] and its implementation and management are serious issues that needs to be continually addressed and refined. By using these three contexts as a guide around which to frame our description and discussion, we can hope to illustrate and define the differences between introduction and implementation of information security regimes in SME's against those in much larger organisations.

In the modern digital environment, businesses of all sizes and shapes must utilise the information domain to ensure business success and continuity [Gordas & Price, 2016]. This also means that the security of this information is paramount to overall business outcomes and needs to be fundamentally incorporated into all levels of business operations. When examining the justification for sound information security management in SMEs, the old premise of “security through obscurity” is no longer applicable to SMEs as cybercriminals and threat actors will look for any and all weaknesses in any business model [Nemati, 2007]. To threat actors, it is a numbers game and any lead will have a dollar value attached to it. This dollar value equally applies to businesses where a breach or loss of information security can have disastrous effects [Abbas et al, 2015]. A primary area of concern regarding the justification of sound information security management in SMEs is that a lot of smaller scale businesses do not firmly believe that they can be a target of threat actors, as they are too small to bother with. Gordas and Price outline this mindset and argue that SMEs and larger organisations do not differ that greatly- they both used technology extensively and both suffer serious consequences in a data breach [Gordas & Price, 2016]. Abbas et al differ as they explain that most SMEs believe in security information and its importance to the organisation but are mostly reactive in their mindset and administration [Abbas et al, 2015]. Whether management of SMEs acknowledge the risk or not, the result is that they react in an unprepared manner which ultimately results in loss of business which affects reputation and financial bottom-line. On either side of the discussion around management and their intentions toward information security, what is apparent is that there is certainly justification for sound management and in-depth though to operations.

Another area of discussion that can illustrate the need for sound information security management and its justification is the underlying factors that are inherent in SMEs that render them unable to adequately introduce and implement information security regimes. These factors can be influenced from a number of avenues, but all revolve around the fact that they are SMEs and not larger organisations. SMEs contribute greatly to the various economies that they reside in, despite the many challenges that they can face. The majority of SMEs do not have the financial resources of larger organisations and suffer from limited budgeting, limited resource planning and ineffective time management [Santos-Olmo et al, 2016]. These challenges flow into information security and its management and implementation- depending on where its priority fits into overall business concerns. Without adequate financial and sponsorship input from management of SMEs, the priorities will never be forward thinking enough to incorporate the ever-changing security landscape [Gordas & Price, 2016]. SMEs have the potential to become more dynamic in the information security space than larger organisations as they are considerably more agile and have the capacity to ensure mitigation of the broad range of risks they face [RM Studio Team, 2020], but they require an overall shift in mindset that will enable this to occur. This agile approach will save the SMEs money, time, resources and effort and provides us with ample justification as to why SMEs need sound information security management.

The third discussion point around information security management and its justification revolves around they way this management is introduced and implemented and how it differs from SME to larger organisations. The information security problem is often characterised by complexity and various levels of interdependency [Taileh et al, 2007]. There are a large number of factors and elements that interrelate with each other, all of this can differ greatly between organisations of varying sizes. This difference in organisational makeup is seen to be a key determinant of how effective information security should be, and constitutes in large part to why SMEs do not have adequate security management in place. The information security problem can be seen to be aggravated by the fact that a large proportion of information security regimes are designed for, and tailored to, large scale organisations [Gordas & Price, 2016]. The useability and implementation of these regimes are not necessarily functional for SMEs and they do not have the skill or expertise to adequately redesign them to suit their own organisations. What is required, and can be seen as a major justification for sound management, is a dynamic, scalable, approach which allows SMEs to correctly implement a solution that fits with their unique business model [Gordas & Price, 2016]. Most recent academic thought on this process has illustrated the need for an effective and scalable strategy for an information security risk assessment procedure. This will adequately frame and prepare the ISMS, and therefore the organisation, to be able shape, deter, and respond to any threats that may arise. Gordas and Price discuss this at length and provide insight into how this approach will reduce the traditional burden that can come from the introduction and implementation of sound information security management policies [Gordas & Price, 2016].

An additional aspect that can help the justification in needing sound information security management in SMEs is the methodology that exists to facilitate the creation of the regime itself. Creating this regime from the ground up, or extensive adaptation of large enterprise policy, can be daunted for SMEs to undertake [Gordas & Price, 2016]. As discussed previously, this can be due to many factors, such as lack of expertise or financial constraints. The process of identifying and outlining the risks that exist is an important first step in any information security mitigation framework [Gordas & Price, 2016]. This simple strategy of risk management can be used to: establish the context; assess the risk; select the information security controls, implement missing control measures; and monitoring and evaluate the effectiveness if information security risk management. Although this process may be more familiar in larger scale enterprises, it is still highly useable and relevant for SMEs, and a critical way that InfoSec managers can justify the introduction and implementation of information security regimes to senior levels of business management. The first priorities for this process involve the mandatory organisational controls that involve the information security regime and the mandatory InfoSec controls that are already in place. [Abbas et al, 2015]. The next priority in order of work is initial information security controls, these will include items such as acceptable usage policies, home and mobile working, incident management, and network security [Abbas et al, 2015]. The third priority involves the intermediate information security controls, and these include: sensitive physical information; computer/network installations; cryptographic solutions; external network connections; and potential malware analysis [Abbas et al, 2015]. Through this phased and priority-based approach SMEs can tailor an efficient and effective information security regime to their own organisations and specific business models. This gives InfoSec managers and practitioners extensive justification for the sound introduction and implementation of information security regimes in SMEs, which offer an approach that is unique to larger organisations and overcomes a lot of the issues that can arise with the differences between the two, in the context in InfoSec management.

Through discussion of management level mindset, the underlying factors that affect security implementation, and how this implementation differs between SMEs and larger organisations, one can illustrate how there is significant justification for introduction and implementation of sound information security management in small to medium enterprises.

The second context around which to frame our description and discussion of the introduction and implementation of information security regimes in SMEs against implementation in larger organisations, is that of ethical issues that exist in information security. The foundations on which all secure systems are built and maintained are the moral principles and practices and the professional standards of all employees of the organisation [Pocatello, 2019]. Ethics in IT play a significant part of the overall business model and this remains true whether they are SMEs or larger enterprises. Effective and efficient information security regimes and the ethical underpinnings of an organisation are closely intertwined, without strong ethical leadership and practice an organisation will not be able to maintain a strong security posture. Also, without strong and effective information security policy and procedures- an organisation will not be able to maintain a soldi ethical standpoint [Pocatello, 2019]. This is true regardless of the size and scope of a business [Brey, 2007], and once again this illustrates to us the similarities between SMEs and larger enterprises in regards to the introduction and implementation of sound information security management.

The are several key issues relating to information security that pertain to ethics and this gives us an insight into how the introduction and implementation of sound security management can differ between small to medium enterprises against those of larger organisations. These issues can include: ethics and responsible decision making; confidentiality and privacy; piracy; fraud and misuse; liability; patent and copyright law; and trade secrets [Pocatello, 2019]. At first glance, these issues seem to only be pertinent to larger enterprises as they would appear the likely target of malicious or unethical actions by threat actors. However, SMEs are just as susceptible to these forms of unethical actions as larger organisations and some argue they are more at risk as any small breach to an SME could spell legal or financial disaster for the company [Nemati, 2007]. The individual ethical issues are straight-forward and do not require further unpacking, it is good however to illustrate the importance of two of these factors as they closely relate to the critical nature of introduction and implementation of sound security management regimes in both SMEs and larger organisations. These two factors are privacy and access right. Both factors of the ethical problems of information security are becoming more and more crucial in the modern and constantly evolving digital environment [Ashushrma378, 2020], as so much more of our personal information and identities are cacooned in the digital space. The issue of personal privacy becomes more important daily as the distribution of networks on a large scale occurs more frequently and the data and information transfer that travels along these networks is available for unethical actors to target [Ashushrma378, 2020]. Without the introduction and implementation of effective information security programmes, SMEs and large organisations will suffer from breaches that may occur. Again, this illustrates the similarities between SMEs and larger enterprise environments, as both are susceptible to loss or compromise of personal data of clients or customers [Nemati, 2007]. Where they differ can be seen in the long-term impact that this possible breach can have on the company. SMEs will suffer more form an unethical action by a threat actor as they will not have the resources or brand-name to outlast any long-term damage, due to adverse customer reaction or possible legal action.

Another key discussion point that needs to be addressed when illustrating the ethical issues that exist in information security management and how its introduction and implementation can differ from SMEs to larger enterprise can be seen when looking at the overall security culture of an organisation and how this closely relates to its overall information security posture. Technological innovation has brought the world closer together in many ways, this is especially true in the context of the information society that exists in our modern lives [Nemati, 2007]. The underlying security culture of an organisation will affect its complete security posture and also the possibilities of unethical behaviours or actions by both employees and external threat actors. Strong security culture will limit the exposure of unethical risks and will help to reduce the overall risk assessment rating of SMEs [RM Studio Team, 2020]. The more that organisations are proactive and responsive to threats or risks as they occur, the more likely that they are to be able to mitigate them before they can do serious harm. This is a key difference between SMEs and larger organisations as large enterprises generally have the means and motivation to create a strong security culture. It is much easier for them, despite the size of the organisation, to create and foster this culture as employees are used to strong directional leadership from management [Santos-Olmo, 2016]. However, the need is still great for SMEs to develop and grow this information security culture and mindset as it is crucial for the security position of the company. The issue remains that the introduction and implementation of this security culture will still need to be adapted and altered to suit each individual SME [Santos-Olmo, 2016]. This process can seem daunting to SMEs that do not have the expertise or experience in establishing this culture, but more and more resources are being created and adapted that are better suited to smaller-scale operational environments [Gordas & Price, 2016], this will enable SMEs to build and maintain a strong security culture and use it to address and overcome potential ethical issues that can arise. This aspect of the introduction and implementation of information security regimes affects SMEs and larger organisations in different ways, but it is important to remember that without a strong set of policies any sized organisation can fall victim to malicious or unethical actions by threats actors.

Small to medium enterprises constitute a major part of the global economic activity and due to the distinct characteristics of these organisations, a major part of any SME information security regime will revolve around end-user training and education [Taileh et al, 2007]. The introduction and implementation of any information security regime will centre around the proposed training and educational outcomes- both for SMEs and much larger enterprise environments. As a society, we are much more informed when it comes to matters that discuss our involvement in the digital world. The problem arises as this digital world evolves so rapidly and changes almost overnight [Gordas & Price, 2016]. Additionally, the use of the Internet in the conduct of most business operations has altered the business landscape to the point where a huge amount of training and education is needed to be 100% across all the different subtleties. For SMEs and large enterprise alike, losses can occur in many way, such as: loss of productivity; loss of business; and damage to organisational branding Taileh et al, 2007]. Education and training can greatly reduce the risks and potential impact that these issues can cause. In the digital age, knowledge is power and by providing the employees of SMEs and large enterprise with the knowledge that they need to help the organisation mitigate external and internal threats- they can become part of the solution, not just a factor in the overall problem.

The information security problem is often characterised by unique complexity and a high level of interdependence, it contains a large amount of factors and elements that interrelate with each other [Taileh et al, 2007]. Significant and ongoing training and education can help provide clarity to this highly interrelated environment and enable proactive and resourceful action to be accomplished by employees, which boost the overall security posture of the organisation- regardless if it is an SME or a large enterprise. A key difference that arises when discussion this issue is how consequences are viewed between SMEs and large organisations. Larger companies are fully aware, to an extent, of the costs that are associated with a poorly introduced and implemented information security regime [Gordas & Price, 2016]. Some argue that the main reason behind the actual prioritisation on corporate security regimes is the regulatory compliance requirements imposed on commercial entities [Taileh et al, 2007]. As SMEs do not fall underneath a large proportion of these regulatory requirements, they often do not prioritise the importance of mitigating these risks. Education into certain business requirements and education as to the reason for their existence and implications can assist SMEs in the introduction and implementation of information security regimes in their own organisations.

As mentioned in other contexts, the difference between SMEs and large enterprises means that the way that information security regimes are introduced and implemented need to be scalable and specifically tailored to their own unique circumstances [Gordas & Price, 2016]. An essential component of a SMEs information security strategy needs to focus on building awareness and conducting ongoing education in the threat environment that the business operates in and how employee actions ensure protection of data and enterprise services [Bada & Nurse, 2019]. A key reason for the need of extensive education and training in SMEs, as opposed to larger organisations, is that SMEs are being increasingly targeted due to perceptions of weak information security policy and procedures [Bada & Nurse, 2019]. The proliferation of digital technology facilitating business has produced many advantages, but a key disadvantage for SMEs is that it has provided potential threat actors with much more access and options to perform malicious and unethical actions against them. A primary reason for this targeting is the commonplace nature of weak information security- in both policy and knowledge and expertise of staff [Bada & Nurse, 2019]. Unlike large organisations, who have access to large training and educational resources, many SMEs have to build up this knowledge base from scratch, this can lead to many issues when it comes to its introduction and implementation to add value to the information security regime. A key difference between SMEs and larger organisations that the information security managers of SMEs can leverage is the behaviour and motivation of their staff members. Developing a strong security culture, built through a combination of education and ongoing training, can be a force-multiplier for SMEs as it will exponentially increase their overall security posture due to the small number of staff they need to be educated. This stands in stark contrast to larger enterprise who need to access a much larger pool of staff [Gordas & Price, 2016].

Traditionally, SME staff can be a difficult audience to reach [Bada & Nurse, 2019], as they may not understand the critical importance of good information security in the modern digital business landscape. Additionally, the ever-changing nature of cybercriminals and online threats has meant that it is difficult for SMEs to maintain situational awareness over information security concepts [Crespo et al, 2010]. This is another reason why effective and ongoing security education and training is a crucial element of SMEs overall security regime and one that needs to be periodically addressed and revaluated. In order to achieve this, SMEs must again take a tailored approach that best suits their organisation and business model. Management must start by identifying key assets and gaining an understanding of the pertinent threats and harms that can directly affect their business and day-to-day operations [Bada &

Nurse, 2019]. This will enable them to create a tailored approach to their education and training that will best improve their immediate security posture. A key finding of recent research has revealed that providing security advice alone is not sufficient, it needs to be a tailored effort that applies directly to each role and responsibility and how this will affect each part of the overall information security regime [Crespo et al, 2010]. As discussed at length previously, a wholistic and encompassing approach needs to be introduced and implemented, keeping key limiting factors of SMEs, such as financial and manpower constraints, in the forefront of management's mind. With this in-depth and tailored approach to introducing information security education and training, SMEs can attempt to bridge the gap that exists in security posture between themselves and much larger organisations and build a strong security culture. The overall security culture, created by education and training, can hold significant importance to maintaining security regimes in SMEs, and certain key aspects of this culture can play in its overall health: technical orientation; management orientation; and institutional orientation [Crespo et al, 2010]. If education and training are structured around these three differing professional viewpoints, more productive outcomes can be achieved in the information security space. A program of "security awareness" that enables staff and users to see and measure their progress in maintaining security fluency can also be used as an effective tool [Crespo et al, 2010]. The main objective of this process is to establish a security culture that is centred around ongoing education and proactive training and empowers users who works towards the companies goals of the information security mission statement. Traditionally these programs are focused on larger organisations, but can be easily modified and incorporated into SMEs and their smaller scale operations.

Through proper introduction and implementation of education and training in key concepts that involves the information security regime, SMEs can dynamically adapt and adjust to ensure the same level of security as is implemented in much larger organisations. By viewing the differences between SMEs and larger organisations in this context, we can see where the individual strengths and weaknesses are found. Education and training is a key concept that can further build upon and help maintain the information security posture of SMEs.

When describing and discussing the introduction and implementation of information security regimes in small and medium enterprises (SMEs) against implementation in much larger organisations, it is crucial to frame the topic around three key contexts. These contexts add depth and insight to the description and discussion and help to highlight its various implications around the information security regimes. These contexts include: justifying the need for sound information security management in SMEs; ethical issues in information security management; and security training and education. The modern age and world we live in is a digital one, with massive amounts of information being produced every single day. The security and integrity of this information is the responsibilities of all businesses who use and create the data, there is not distinction in this responsibility between large enterprises and SMEs. This responsibility to protect our data and information grows in importance everyday and it is crucial for everyone to understand how data is created and to what extent it is used [Nemati, 2007]. Information security has recently been viewed as one of the foremost concerns [Santos-Olmo et al, 2016] and its implementation and management are serious issues that needs to be continually addressed and refined. By using these three contexts as a guide around which to frame our description and discussion, we can hope to illustrate and define the differences between introduction and implementation of information security regimes in SME's against those in much larger organisations.

References

1. Abbas, Jawad. Mahmood, Hassn Khawar. & Hussain, Fawad. (2005) Information Security Management For Small And Medium Size Enterprises. *Science International Lahore*, 27(3), 2393-2398. Lahore, Pakistan.
2. Ashushrma378. (2020). Ethical Issues in Information Technology (IT). Retrieved from: https://geeksforgeeks.org
3. Bada, Maria. & Nurse, Jason R C. (2019) Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Journal of Information and Computer Security*. DOI: 1.1108/ICS-07-2018-0080.
4. Brey, p. (2007) Ethical Aspects of Information Security and Privacy. Security, Privacy, and Trust in Modern Data Management. Data Centric Systems and Applications. Springer Pub. Heidelberg, Berlin. Germany. Retrieved via: https://doi.org/10.1007/978-3-540-69861-6_3.
5. Crespo, Luis Enrique Sanchez. Parra, Antonio Santos-Olmo. Fernandez-Medina, Eduardo. Piattini, Mario. (2010) Security Culture in Small and Medium-size Enterprise. *Journal of Communications in Computer and Information Science*. DOI: 10.1007/978-3-642-16419-4_32. Presented at 'Conference on ENTERprise Information Systems', Portugal, 20-22 October, 2010.
6. Gordas, Vadim. Price, Geraint. (2016) Information Security for SMEs. *Submission of Technical Report*. Information Security Group. Royal Holloway. University of London. UK.
7. Nemati, Hamid. (2007) Information Security and Ethics: Concepts, Methodologies, Tools, and Applications. Published via ResearchGate: https://researchgate.net/publication/237344283_Information_Security_and_Ethics_Concepts_Methodologies_Tools_and_Applications.
8. Pocatello, Iri. (2019) *III Ethical Issues*. Published via NIATEC, Idaho State University.
9. RM Studio Team. (2020) *Information Security Challenges in SMEs*. Published via Risk Management Studio. Accessed via: Information Security Challenges in SMEs | Risk Management Studio
10. Santos-Olmo, Antonio. Sanchez, Luis Enrique. Caballerio, Ismael. Camacho, Sara. Fernandez-Medina, Eduardo. (2016) The Importance of the Security Culture Culture in SMEs. *In Regards the Correct Management of the Security*

of Their Assets. VIII Congreso Iberoamericano de Sguirdad Infromatica (CIBSI) Quito, Ecuador.

11. Talieh, Anas. Hilton, Jeremy. McIntosh, Stephen. (2007) Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. *School of Computer Science*. Cardiff University, UK.
12. Whitman, Michael E. Mattford, Herbert J. (2007) Management of Information Security. Fifth Edition. Chapters: 1; 2; 4;5. Printed in United States of America.