Antecedents for Enhanced Level of Cyber-Security in Organizations

Abstract

Purpose: This study aims to identify and investigate the antecedents for an enhanced level of cyber-security at the organisational level, from both the technical and the human resource perspective, using Human–Organization–Technology (HOT) theory.

Design/methodology/approach: The study has been conducted on 151 professionals who have expertise in cyber-security in Indian organisations in sectors such as retail, education, healthcare, etc. The analysis of the data is carried out using Partial Least Squares based Structural Equation Modelling technique.

Findings: The results suggest that 'legal consequences' and 'technical measures' are the most important antecedents for an enhanced cyber-security level in the organisations. The other significant antecedents include 'role of senior management' and 'proactive information security'.

Implications: This empirical study has significant implications for organisations as they can take pre-emptive measures by focusing on the important antecedents and work towards enhancing the level of cyber-security.

Originality/value: The originality of this study is combination of technical and human resource perspectives in identifying the determinants for an enhanced level of cyber-security in the organizations.

Keywords: Cyber-Security; Organisation; Antecedents; Structural Equation Modelling.

1. INTRODUCTION

Due to the ever-changing nature of cyber-attacks, the digital world calls for an enhanced level of cyber-security in every organisation and businesses (Borrett *et al.,* 2014; Arachchilage and Love, 2014). In line with the latter, Fielder *et al.,* (2016) and Taib *et al.,* (2019) also voice their concerns and state that with the increasing multiplicity and scope of these anonymous cyber-attacks, their is need for organisations to prioritise how they safeguard themselves (Schaik et al., 2018). Few examples of such attacks include data breach in the retail industry – Target (2013) and Home Depot (2014)[1,2], data breach of Yahoo (2016)[3], network hacking of Sony Pictures Entertainment (2014)[4], etc. The financial services industry was most affected by cyber-attacks in the year 2014, while the healthcare industry got most affected in the year 2015[5]. Thus, many firms in healthcare are now adopting measures to prevent themselves from cyber-attacks. The cyber-security of an organisation is not only governed by the technical capabilities of the organisations (McCormac et al., 2017). It is equally dependent on the human resources deployed in the organisations. Thus, the current study aims to investigate the antecedents of enhanced cyber-security at the organisational level from both the technical and the human resource perspective.

---

[1]https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#6d374f4de795

[2] http://www.homedepotbreachsettlement.com/

[3]https://www.cnbc.com/2017/02/15/yahoo-sends-new-warning-to-customers-about-data-breach.html

[4] https://www.vox.com/2014/12/14/7387945/sony-hack-explained

[5]https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-threats-by-industry/#gref

The cyber-security at the organisational level can be determined by various factors, which include the role of senior management in enhancing cyber-security in organisation in terms of their perceived organisational support and commitment towards IT security (Boss et al., 2009; Jarvenpaa & Blake, 1991; Barton *et al.,* 2016). Other antecedents include the strategies adopted for IT security (McFadzean *et al.,* 2011; Nassimbeni *et al.,* 2012; Tang & Liu, 2015), nature of business of the firm (Barton *et al.,* 2016), the presence of proactive information security measures, and technical measures adopted by the organisation to enhance cyber-security at the organisational level. The legal consequence of violations and enforcement of cyber-laws are some of the other antecedents for enhanced cyber-security found from the literature (Herath & Rao, 2009). The personality traits of employees including their agreeableness and conscientiousness towards security policy implementations and their attitude towards compliance are yet other antecedents derived from the literature review (Boss *et al.,* 2009; Mishra & Dhillon, 2006; Shropshire *et al.,* 2015).

The objective of this study is multifold. *Firstly*, the study helps in identifying the important antecedents for enhanced level of cyber-security in the organisations. *Secondly*, the study is first of its kind to investigate the enhanced level of cyber-security in organisations from both technical as well as human resource perspective. *Thirdly*, the study has implications for company managers, policymakers, and cyber-security experts. To achive these objectives, the antecedents are identified from thorough literature review and discussion with experts. The prominent antecedents are then identified by Partial Least Square based Structural Equation Modelling (PLS-SEM) technique. The data is collected from 151 professionals at various levels of management (junior, mid-level, senior manager), working in sectors such as retail, education, healthcare, etc. The study has significant implications for organisations and businesses, i.e. pre-emptive measures and work towards enhancing cyber-security is required at large.

Apart from the introduction, the paper has been divided into five sections. Section 2 deals with the background literature and hypothesis development. Section 3 illustrates the methodology, and Section 4 describes the results. Finally, Section 5 concludes the study stating the limitations and future scope of the work.

2. BACKGROUND LITERATURE AND HYPOTHESIS DEVELOPMENT

The study derived the factors influencing the enhanced cyber-security in organizations from Human–Organization–Technology (HOT) theory. The HOT framework was initially developed for Health Information Systems (HIS) (Yusof *et al.,* 2008). The HOT framework is built on previous models of IS evaluation, including the IT-Organization Fit Model and the IS Success Model. The framework propagates that the more technology, human and organization fit with each other, the higher the potential of HIS. The technology factors in HOT framework includes factors like system quality, information quality and service quality. The human factors in the HOT framework include factors like system use and user satisfaction. Similarly, the organizational factors in the HOT framework include structure and environment. The HOT theory is based on the premise that apart from technical issues, human and organizational aspects are also crucial in identifying the important factors for enhancing cyber-security in

organizations (Ahmadi *et al.,* 2015). Human factors that can influence cyber-security includes the role of senior management and personality traits of the IT Security manager. Organizational factors of HOT includes Strategies adopted by Senior Management of the organization, legal measures adopted for enhanced IT Security and proactive information security measures. Technological factors of HOT theory includes technical measures adopted for enhancing cyber-security.

2.1 Role of Senior Management

The role of senior management refers to the support, commitment, participation of the senior management towards the organisations. The role of senior management towards the development and management organisations is well studied by various researchers across the world (Garrity 1963; Doll 1985; Jarvenpaa & Blake 1991; Dora, et al, 2013). For our study, we categorise the role of senior management into the following four streams: *legitimacy through regular participation*, *commitment*, *evaluation*, and *ethical leadership*.

2.1.1 Legitimacy through regular participation of senior management

Legitimacy through regular participation consists of the set of activities such as review of IT security design, planning and development of Information Security Policies (ISPs) followed by the successful implementation (Jarvenpaa & Blake 1991; Hu *et al.,* 2012). Often, businesses view their cybersecurity spends as a cost center, and therefore information security investments in related training, technology purchases, and process improvements through Information Security Assessment (ISA), and improved Information Security Culture (ISC), are deemed as a burden for the entire organisation. (Kaspersky, 2017). Therefore, the active and regular participation of senior IT managers in ISA exercises such as Security Education, Training, and Awareness (SETA), security implementation and strategic decision-making (Dhillon & Torkzadeh 2006), is often viewed as a positive reflection of information security compliance and has a positive effect on an enhanced level of cyber-security in the organisation.

2.1.2 Commitment of Senior Management

The existing literature in Information Systems Security (ISS) has extensively reported that the commitment of senior management is necessary to achieve an enhanced information security environment in organisations (HöNe & Eloff, 2002; Kankanhalli *et al.,* 2003; McFadzean *et al.,* 2006). Further, Da Veiga & Eloff (2007) reported that the commitment of senior management could play a crucial role in inculcating a tolerable level of ISC that could lead to establishing a successful Information Security Governance (ISG) framework. Hu *et al.,* (2012) found that if the employees perceived a more substantial top management commitment, it would positively motivate and reassure employees to pledge to compliance behaviour by participating in SETA and acquire necessary skills. Holgate & Hardy (2012) found that choosing the primary owners of ISG from the representatives of senior management of an organisation would further facilitate to establish the locus of ISGs concerning various governance mechanisms.

2.1.3 Ethical Leadership Behaviour of Senior Management

In an organisation, leaders are those whom employees trust and respect. Leaders also have the power to determine rewards or punishments for the employees' behaviours. Therefore, a leader plays a vital role in modelling the attitudes and manners exhibited by their subordinate employees (Mulki *et al.,* 2009). In line with Brown *et al.,* (2005), ethical leadership can be defined as "the demonstration of appropriate conduct through personal actions and interpersonal relationships, and the promotion of such conduct to followers through two-way communication, and decision-making". Ethical leadership plays a vital role in influencing the behaviours of employees (Mayer *et al.,* 2010). On the other hand, Kacmar *et al.* (2011) found a positive association between ethical leadership and employee Organisational Citizenship Behaviour (OCB). Therefore, with the enforcement of organisational rules through ethical leadership, employees will perceive a highly ethical climate (Mayer *et al.,* 2010; Shin *et al.,* 2015). Xue *et al.* (2018) proposed that ethical leadership would promote the generation of positive information security climate in the organisation. They further noted that ethical leadership would also help to measure the negative effect of information security climate on ISP violation intention among employees through direct and indirect means. Thus, ethical leadership among senior management might enhance cyber-security in the organisation.

2.1.4 Regular Evaluation by Senior Management

Although senior management commitment, ethical leadership and participation alone does not guarantee adequate information security at the operational, strategic compliance levels, they are strong prerequisites for active growth, execution, and subsequent compliance with ISS controls (Boss *et al.,* 2009). Therefore, ISS compliance among employees and subsequent evaluation by senior management helps to improve the effectiveness of ISS controls and supplements their presence, instead of solely depending on them (Dhillon & Mishra, 2006; Herath & Rao, 2009). Additionally, researchers noted that senior management and primary stakeholders needed good situational awareness about the incumbent IT risk levels (such as strategic, operational, financial) (Franke & Brynielsson 2014; Dora, Kumar, Gellynck, 2016), or of the external ISS background (Webb *et al.,* 2014). Therefore, organisations where managers can maintain a strong link between ISS control compliance by employees, and their subsequent evaluation can achieve an enhanced cybersecurity level.

As a result of the above discussions, we hypothesize that:

H1: Role of senior management (such as legitimacy through participation, commitment, evaluation, and ethical leadership) plays a positive role towards an enhanced level of cyber-security in the organisation.

2.2 Strategies Adopted by Senior Management

The strategies adopted by the senior management, in general, align with the business strategies of the organisation (Chang & Yeh 2006; Nassimbeni *et al.,* 2012). For our study, we have categorised the *strategies adopted by senior management* towards an enhanced level of cyber-security in the organisation, into the following five streams: *clear vision*, *institutionalised IT security governance*, *risk management controls*, *reward policy*, and *information sharing*.

2.2.1 Clear Vision about IT Security Strategies

Effective Information Security Management (ISM) is not a standalone activity, but it is established on a well-developed, and inter-linked IT strategy spread across the entire organisation (Seeholzer, 2012). Often, there exists a one-to-one correspondence between the behaviour of top management and the characteristics of organisational culture (such as transformative vision about IT security implementation in the organisation) (Ke & Wei, 2008). By championing the new initiatives, and model ISPs, the senior management can articulate a clear vision, strategy and can set a measurable IT security goal. Setting the right strategy may also include the organisational statements of core values, rationale, vision, strategic plans, ISS at operational-level, and ISS investments (Baskerville & Dhillon, 2008). Such actions render significant legitimacy to ISA activities, SETA programs, enrich information security cultures (ISC), followed by framing of ISPs and controls. ISS strategies must be adopted by senior management in organisations, and they should be able to evaluate the efficacy of IS security as well as communicate its value to the organisation (McFadzean *et al.,* 2011; Nassimbeni *et al.,* 2012; Tang & Liu 2015). While the IT strategy and organisation strategy for information security can percolate from the business strategy of an organisation, it essential that there remains an explicit synchronisation between each of these dimensions (Baets, 1992; Bharadwaj *et al.,* 2013). Recently, one of the studies have analyzed the adoption of the International Information Security Management System Standard ISO/IEC 27001 by using web-mining approach (Mirtsch *et al.,* 2020)

2.2.2 Institutionalised IT Security Governance (ISG)

Organisations draft IT governance procedures to ensure thorough execution of ISPs and security procedures (Warkentin & Johnston, 2006; IT Governance Institute, 2006). According to Moulton & Coles (2003), ISG for an installed information system in an organisation is the "establishment and maintenance of the control environment to manage risks relating to C-I-A-NR (Confidentiality, Integrity, Authenticity, and Non-Repudiation) of information and its supporting processes and systems." Von Solms (2003) noted that an effective ISG must consist of successful and distinct implementation of both IT Governance and Corporate Governance. Over time, as organisations evolve, their ISGs also mature. Within this phase of change, however, they must strive to maintain a high level of information assurance (Moulton and Coles, 2003; COBIT 2005; Von Solms, 2005). In this context, IT governance and organisational design play a significant role in fulfilling the commitment of ISM. Thus, ISGs and ISS controls can also support regulatory compliance for the organisation. Finally, ISGs can support a firm to achieve ISS controls to be benchmarked and be embedded in key business processes (Dhillon & Mishra, 2006). Therefore, through the ISGs, organisations must verify whether the business goals and vision are in alignment, and whether do they lead to executable IT security goals.

2.2.3 IT Risk Management Controls

What follows directly from the establishment of ISG-s, are the following Information Security Risk Management (ISRM) objectives, which includes: *(i)* identification of sufficient controls at the strategic level, *(ii)* whether they map with the outlined ISPs, and *(iii)* the degree to which these controls should be centralised or decentralised (Van der Haar & Von Solms, 2003; Von

Solms, 2003; Von Solms, 2005; NIST 2013). The NIST framework presents a set of controls that an organisation needs to implement the C-I-A-NR of information security assurance and conform to the drafted ISPs. Often, certain dimensions of the C-I-A-NR triad could pose more important than others. For instance, Knowles *et al.* (2015) noted that availability becomes the most important dimension in industrial control systems, thus making the triad as A-I-C-NR. Recently, one of the studies have conducted a cyber risk analysis for smart-grid and applied the model on the case study of an electric utility (Smith and Paté-Cornell, 2018).

2.2.4 Reward Policy for Employees' ISP Compliance

The extant literature on organisational theories highlights the role of sanctions and rewards to encourage the desired compliance behaviour among employees (Huselid, 1995; Herath & Rao 2009). Rewards are tangible or intangible forms of compensation (such as salary increments, promotions, and written appreciation letters) that an employee receives from the employer as recognition of ISP compliance (Bulgurcu *et al.,* 2010). Rewarding employees for positive compliance behaviours are recently gaining popularity as incentive mechanisms. Recent studies have discussed their possibility in the context of information security (Boss & Kirsch, 2007; Pahnila *et al.,* 2007). Further, while rewards and sanctions generate external motivations for an enhanced OCB, intrinsic values of employees can support their internal motivations to abide by regulations (Tyler & Blader, 2005). In contrast, Siponen *et al.,* (2014) had shown that rewards could be detrimental on the intrinsic motivation of employees to comply, especially when they were tangible (such as gift coupons, or awards). Otherwise, rewards may also work well in organisations, where sanctions on information security behaviour do not stop violation among employees. Bulgurcu *et al.* (2010) examined whether intrinsic benefits/safety of resources/rewards can stimulate the ISA of an employee. Hence, senior management in organisations needs to adopt a reward policy for ISP compliance and motivate an enhanced ISC.

2.2.5 Information Sharing as an IT Security Strategy

Sharing of information about IT risks among firms can encourage them to adopt a relatively proactive, rather than a reactive, approach towards investing in security technology and ISPs, such as the tendency to defer necessary investments (Liu *et al.,* 2011; Skopik *et al.,* 2016; Safa and Solms, 2016). The USA federal government has supported the establishment of industry-based Information Sharing and Analysis Centers (also known as ISACs). Governments in other nations have established Computer Emergency Response Teams (CERTs), where they directly broadcast alerts, tips, major attacks, exploits, and disclosed vulnerabilities (CERT, 2019). These information-sharing activities have several advantages: *(i)* lower risk of security breaches in the future, *(ii)* identification and repairing of vulnerabilities in organisational IT systems, *(iii)* increased sales resulting from more effective security products, and (iv) improved reputation among consumers (Gal-or & Ghose, 2006; Skopik *et al.,* 2016). However, Gordon *et al.,* (2003) noted that when firms shared security information among themselves, they wanted to free ride and had reduced their investment incentives, thereby leading to possible discouragement among the ISACs. In contrast, Gal-Or & Ghose (2005) found that most firms perceived information security investments and information-sharing activities as "strategic complements". Hausken (2006) has also demonstrated that the interdependence, and not their

mutual competitiveness, is the key attribute of information-sharing. Hence, organisations need to find out whether they are actively contributing to ISACs by sharing relevant, actionable cyber-threat information.
As a result of the above discussion, we hypothesize the following:

H2: Strategies adopted (such as vision, institutionalised IT security governance, risk management controls, reward policy and information sharing) for IT security by senior management, play a positive role towards an enhanced level of cyber-security in the organisation.

2.3 Technical Measures for Enhanced IT Security

Organisations invest in technologies for improving security to prevent becoming victims of possible cyber-attacks. For our study, we categorise the technical measures for increased IT Security, into the following three streams: *proactive and reactive prevention mechanisms*, *cyber-incident management*, and *minimise correlated risks*.

2.3.1 Proactive and Reactive Prevention Mechanisms

Technical measures for information security refer to the application of all possible contemporary security technologies to the existing IT assets of the organisation (Venter & Eloff, 2003; Gartner, 2009). Much of academic literature in the discipline of computer science and cryptography has been dedicated to the invention of these technical measures (Choo 2011; Ab Rahman & Choo, 2015; Sureshkumar *et al.,* 2019). Broadly, they are categorised into two types - proactive and reactive. Proactive technology tools are those preventative measures that are built upon in a bid to secure data or resources before a security breach can occur. Reactive technology tools are those preventative measures, which are being applied by the organisation in a bid to secure data or resources as soon as a security breach is detected (Venter & Eloff, 2003). Often organisations rely upon historical data on cyber-attacks to build both of these measures and applied at the network, host, or application level (N-W/H/A) within the organisation. Cryptography is a proactive technology measure because it safeguards data before a potential threat can materialise. It is performed by successfully encrypting the data and prevent it from frequent attacks such as wiretapping, sniffing, and snooping attacks (Biswas & Patra, 2018). Similarly, the recent use of Cyber-Threat Intelligence (CTI) as a proactive technology measure in the analysis of external sources such as dark forums to identify ongoing and popular attack vectors and mitigate the organisation from future cyber-attacks (Samtani *et al.,* 2017; Biswas *et al.,* 2018). An Internet firewall is a software tool installed on a specially configured computer that serves as a blockade to unauthorised users. Firewalls are reactive technology measures because they are used to act against specific security incidents as soon as they occur. Therefore, organisations must find out whether they are investing in proactive/reactive technology measures to reduce chances of cyber-attacks in the organisation. The proactive information security measures include techniques such as those of digital signatures, cryptographic keys, digital certificates, and anti-virus and anti-phishing scanners. On the other hand, reactive information security measures include techniques such as those of Access controls, firewalls, passwords, and remote access, biometrics and intrusion detection

systems. Recently, one of the studies has proposed a comprehensive model to manage cybersecurity incidents called SOTER (Onwubiko and Ouazzane, 2019).

2.3.2 Regularly Manage Cyber-Incidents and Vulnerabilities

A security incident can be any of the following, e.g. attempted intrusion, data breach, successful compromise, or an active threat. In the context of cyber-security, incident management is the process of recognising, managing, recording and examining security threats and incidents in real-time. Since the incident, response activities for cybersecurity events are relatively new to organisations, the effective functioning of Cybersecurity Incident Response Teams (CSIRTs) is not yet fully developed (Steinke *et al.,* 2015). In fact, a recent study by Martin et al., (2017) pointed out that a robust incident management and response system should be present in organisations, and that will lead to improved cyber resilience. Recently, one of the studies have presented seven pillars of cybersecurity, which includes Patient, Persevering, Persistent, Proactive, Preventive, Predictive, and Preemptive (Carayannis *et al.,* 2019)

2.3.3 Minimise Correlated Risks

Shared software vulnerabilities can often lead to correlated failures of IT systems that are interconnected and can escalate the cyber-risk of the entire organisational network. Therefore, IT managers need to carefully choose software with uncorrelated vulnerabilities while building system configurations (Chen *et al.,* 2011; Temizkan *et al.,* 2017). Diversification of correlated cyber-risk enables efficient assessment and mitigation of cyber-risks and reduces "software monoculture" (Chen *et al.,* 2011; Temizkan *et al.,* 2017; Biswas & Mukhopadhyay, 2018). Chen *et al.* (2011) have developed a simulation-based study to identify the correlated risks arising due to shared software vulnerabilities across multiple software platforms. Current research has adopted various techniques, such as *(i)* benchmarking to identify vulnerable sections within software codes (Larsen *et al.,* 2015), and *(ii)* within operating system platforms Garcia *et al.,* (2016), to achieve diversity. Hosseini *et al.* (2016) examined the propagation of malware across software platforms laden with shared vulnerabilities through epidemic modelling. Lagerström *et al.* (2017) examined the relationship between the architecture couplings of software codes with shared vulnerabilities across various platforms. Biswas & Mukhopadhyay (2018) proposed a {risk, benefit} metric applying Markowitz optimisation to indicate the quality of software products, and their optimal procurement ratios. Finally, we noted that organisations need to address the possibilities of correlated risks across multiple software platforms through shared vulnerabilities.

As a result of the above discussions, we hypothesize the following:

H3: Technical measures (such as proactive and reactive prevention mechanisms, cyber-incident management, and minimise correlated risks) play a positive role towards an enhanced level of cyber-security in the organisation.

2.4 Legal Measures Adopted for Enhanced IT Security

Legal frameworks and regulatory sanctions against cyber-attacks can disincentives malicious attackers from committing cyber-crimes. For our study, we categorise the legal consequences faced by an organisation, into the following streams: repo*rt prior cyber-attacks to regulatory*

authorities, *practice law-enforced surveillance methods*, and *adhere to national and international cyber-legislation frameworks to discourage cyber-attacks*.

2.4.1 Report Prior Cyber-Attacks to Regulatory Authorities

According to the General Deterrence Theory (Williams & Hawkins, 1986), the severity of legal sanctions could deter individuals from indulging in criminal activities. Roumani *et al.,* (2015) and Chen *et al.,* (2011) also found that attackers regularly probed organisational networks to recognise software vulnerabilities that are not patched by users, and eventually exploit them. The potential costs of sharing security information could have a snowball effect, and ensuing negative publicity could lead to the loss of market shares (Cavusoglu *et al.,* 2004). According to the CSI-FBI survey, firms undertook different measures as a preventive action after cyber-incidents. Of them, twenty-seven per cent of firms reported their breaches to federal law enforcement agencies, and twenty-six per cent to legal counsels, (Gordon *et al.,* 2009; CSI-FBI, 2010). Sometimes, firms adopted a staggered form of the public announcement of data breaches, such as the theft of personally identifiable information in the cases of Target data breach and LinkedIn data breach. In these cases, the victim organisation reported intrusion(s) to individuals/customers whose personal data was breached and then to the public media (HBR, 2015). Therefore, robust proactive mechanisms at the organisational level, that include incident reporting policy, and compliance with the existing ISGs, can mitigate cyber-attacks in future (Breaux & Baumer, 2011; Hathaway *et al.*, 2012; Ghappour, 2017; Ratten, 2019).

2.4.2 Practice of Law-Enforced Surveillance Methods

While corrective action against cyber-attacks is mostly reactive in nature, firms need to participate in proactive Cyber-Threat Intelligence (CTI) (Samtani *et al.,* 2017; Biswas *et al.,* 2018). Likewise, regulators need to frame contemporary guidelines that will take care of difficult issues (such as ethical hacking and cyber-analytics-based mitigation measures). A recent study by Samtani *et al.,* (2017) noted that CTI is a far more effective practice to thwart cyber-attacks and hacking attempts on a business firm, than employing passive and reactive measures such as firewalls, antivirus, IDS, and SETA exercises. Often, attackers discussed attack techniques on hacker forums visible only on the Dark Web, thereby obscuring any digital attempts of future tracking. Organisations in the USA primarily conduct electronic surveillance based on the Electronic Communications Privacy Act of 1986 and the Foreign Intelligence Surveillance Act of 1978 (Solove, 2003). In this context, Ghappour (2017) proposed the legalisation of certain cyber-analytics activities and found that the governing authority of the US Congress could help regulate the nature and scope of these techniques.

2.4.3 Adherence to Cyber-Laws Enforced by the Central Government

Stringent legal sanctions (Ehrlich, 1996) on black market sales of exploits, penalising cyber-attacks on commercial organisations, as well as critical national infrastructure, helps policymakers at the national level to recognise the economic impact of these malicious activities (Stockton & Golabek-Goldman, 2013). According to the General Data Protection Regulation 2018, businesses must report the possibility of any data breaches within 72 hours if they suspect an adverse effect on user privacy (Albrecht, 2016; GDPR 2018). On violation, the involved party can be penalised up to 4 per cent of the annual global turnover or a sum of

20 million euros. Extant studies (Breaux & Baumer, 2011; Hathaway *et al.,* 2012; Fischer, 2013) also noted that robust cyber-laws at the federal level, ISGs at corporate-level and incident management policy at operational-level could drastically mitigate the chances of cyber-attacks. For instance, the CSI-FBI Computer Crime and Security Survey (CSI-FBI, 2006) showed that the Sarbanes Oxley Act of 2002 (SOX) had made a substantial impact across industries through mandatory compliance to data privacy of users. Further, most of the IT managers agreed that the necessary compliance with the SOX Act had raised the level of interest in IS security in their organisation. The Cybersecurity and Infrastructure Security Agency Act of 2018 enforces organisations to comply with ISACs and information-sharing teams to fight cyber-crime. Often, these legal measures can evoke fear and desist attackers from launching cyber-attacks in the future.

Organisations also need to adhere to international legal frameworks that are pertinent to cyber-security and data privacy in matching industries. For instance, botnet-based attacks can be launched from any geographical location in the world (Hui *et al.,* 2017). Attackers may even relocate their command-and-control servers to other countries where legal frameworks for cybersecurity are relatively weaker (Cremonini & Nizovtsev, 2009). Often, these phenomena can result from a displacement effect triggered by strong national cyber-laws in a country (Png *et al.,* 2008). For instance, when the legal sanctions against cyber-attacks become stricter in the USA., it may prompt attackers to relocate their resources to other countries.
Thus, based on the above discussions, we hypothesize that:

H4: Legal factors (such as, reporting prior cyber-attacks, practice law enforced surveillance methods, and adherence to cyber-legislation frameworks) play a positive role towards an enhanced level of cyber-security in the organisation.

2.5 Proactive Information Security Measures

The primary goal of a security-compliant ISS is to ensure the confidentiality, integrity and the availability of business-level data within an IT system. Organisations can maintain the satisfactory levels of C-I-A-NR only if the IT security policies and procedures are comprehensive, accurate, and finally put into practice (see Fig. 1) (Warkentin & Johnston, 2006; Bulgurcu *et al.,* 2010). Therefore, if the IT managers, software developers, and finally, the end-users are not convinced of those IT security policies and procedures, they will not execute successfully. Fig. 1 explains the flow of ISPs (based on the strategies adopted) that translate into the IT security procedures and finally are practised in the organisation. For this study, we categorised proactive information security measures adopted towards an enhanced level of cyber-security in the organisation, into the following streams: regular review and update of ISPs, presence of SETA programs and appearance of proactive information security measures. Recent work suggested proactive environmental scanning and locating potential threats and attacks for handling the cyber-attacks (Appiah *et al.,* 2020)

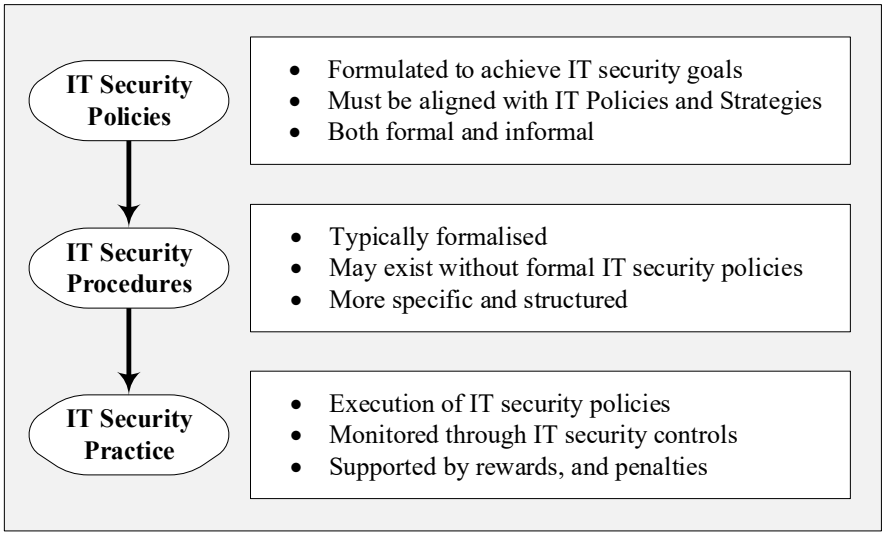

Figure 1: IT Security Policy – Procedure – Practice
(Adapted Source: Warkentin & Johnston, 2006)

2.5.1 Information Security Policies (ISPs) – Frame and Update Regularly

A fundamental approach to address cyber-risks in organisations is through the early adoption of pertinent and well-documented ISPs, by following the steps which include: *(i)* specifying the standards, and responsibilities for users of IT assets and resources (Bulgurcu *et al.,* 2010; Lowry and Moody, 2015), *(ii)* acceptable user behaviour towards consumption of business-level information, and *(iii)* controlled use of IT assets (Palmer *et al.,* 2001; Rees *et al.,* 2003; Knapp *et al.,* 2009; Bulgurcu *et al.,* 2010). Such adoption of ISPs will facilitate the prevention, detection, and response towards security incidents. Employees in an organisation are generally unaware of organisational vision and strategies (see Fig. 1) and their roles and responsibilities toward fulfilling this objective (Warkentin & Johnston, 2006; Werlinger *et al.,* 2009). Sipior *et al.,* (2018) found that after the infamous *Petya* ransomware attack at a USA hospital, the ISG owners needed to update their ISPs and business continuity plans. Therefore, as a future step, the organisation can plan to improve its employees' awareness and compliance with the revised ISP. Doherty & Fulford (2006) noted that organisations who regularly updated their ISP were less likely to suffer security breaches, in terms of both likelihoods as well as impact. In a recent systematic review of information security literature, Cram *et al.,* (2017) have pointed out a new stream of research that discusses the benefits of timely adjustments and fine-tuning of ISPs. Often, these policies are clichéd due to little/no changes since implementation, need the addition of revised scope (such as changes in information technology, and user behaviour), and finally the adoption of new compliance and guidelines from the industry and legal frameworks (Chen *et al.,* 2012). Fig. 1 presents the stage-wise formulation of ISPs, IT security procedures, and finally adopting them into IT security practices through supplementary sanctions, and rewards for employees in the organisation.

2.5.2 Security Education, Training, and Awareness (SETA) Programs

Organisations employ SETA programs and their exercises to counter security threats and promote employee compliance behaviour towards ISPs (Crossler & Bélanger 2006; D'Arcy *et al.,* 2009). Both ISPs and SETA exercises are IS risk management measures that are delivered

at low-cost but can generate high ROI (Whitman, 2003). For instance, the SETA programs include employee training to *(i)* improve their ISA issues, *(ii)* legal and regulatory consequences of unauthorised data access and tampering, and *(iii)* educate on software copyright laws. Furthermore, they plan to provide employees with necessary skills to comply with ISPs and necessary security processes (D'Arcy *et al.,* 2009; Lee & Lee 2002; Puhakainen & Siponen, 2010; Straub & Welke 1998; Whitman *et al.,* 2001). Contrary to technological solutions, which are expensive to implement, and are never fail-safe, SETA programs act as efficient human solutions, which organisations administer first and then follow with IT security tools (Whitman, 2003). Herein lies the simplicity of managing SETA programs in their practice and organisational effectiveness. For instance, D'Arcy *et al.* (2009) found that a high ISA among employees could mitigate the intention to misuse the IT systems and processes at the workplace. On the other hand, Haeussinger & Kranz (2013) also note that SETA programs are capable of improving ISS by increasing ISA about potential IS risks and ISPs. Further, there is a need for balancing the spending related to cybersecurity tools with operational efficiency (Ekelund and Iskoujina, 2019).
Thus, based on the above discussions, we hypothesize that:

H5: Presence of proactive information security measures (such as the regular update of ISPs, and presence of SETA programs) play a decisive role towards an enhanced level of cyber-security in the organisation.

2.6 Personality Traits of the IT Security Manager

The personality traits of an individual can be recognised in numerous ways. One of the earliest work by Allport and Odbert identified 4500 personality traits of individuals (Allport & Odbert, 1936). Various scholars have tried to reduce the personality traits into a meaningful and manageable structure. The Five-Factor Model (FFM) of personality traits has emerged as the "model of choice" (Briggs, 1992). Goldberg's Big Five factor is one of the most widely used FFM consisting of *extroversion*, *agreeableness*, *emotional instability*, *conscientiousness*, and *intellect* (Goldberg, 1992). We have used Big Five Personality Traits as a construct in this study because of its broad applicability in issues related to human behaviour for tackling information systems security.

Extroversion can be defined as the individuals who are full of life, energetic, gregarious, dominant, and outgoing (Goldberg, 1992; McCrae & Costa, 1991). *Extraverts* generally tend to focus on feelings that help them associate with others (Osatuyi, 2015). *Agreeableness*, on the other hand, can be defined as the individual's act of being sympathetic, trusting, selfless and straightforward (Goldberg, 1992; McCrae & Costa, 1991). Highly agreeable individuals are generally altruistic, and they tend to avoid any form of conflict with others (Goldberg, 1992; McCrae & Costa, 1991). *Emotional instability* is a trait that reflects neuroticism and the extent of individuals' reactions to stressful conditions. Individuals with this trait are defined by depressed, anxious, stressed, volatile, suggestible, and fearful (Goldberg, 1992). *Conscientious* individuals are rational, logical, and competent (Goldberg, 1992; McCrae & Costa, 1991). Conscientious individuals tend to be orderly and are very particular and attentive to all the details (Goldberg, 1992; McCrae & Costa, 1991). Intellect or openness to experience refers to

an individual's propensity to try new things, to learn, to be intellectually challenged, and curious (Goldberg, 1992; McCrae & Costa, 1991). The individuals who have high intellect tends to be more creative, empathic, artistic, and aesthetically responsive (McCrae & Costa, 1991). Thus, we propose that the personality traits of the information security manager play a dominant role in enhancing the cyber-security level of organisation. Thus, based on the above discussions, we hypothesize that:

H6: Personality traits of the information security manager (such as extrovert, agreeable, open to new ideas, moody, and ability to deliver) play a positive role towards an enhanced level of cyber-security in the organisation.

2.7 Enhanced Cyber-Security in Organisations

Most organisations need to measure their level of cybersecurity after incorporating necessary measures such as the proactive role of senior management, strategies adopted for IT security, technical standards, legal frameworks, regulatory guidelines, and finally the positive personality traits of the IT security managers (D'Arcy *et al.,* 2009). For this study, we categorised the measurement of enhanced cybersecurity in an organisation, into the following streams: *current cyber-security maturity levels and assessment*, *adopted security control measures (such as C-I-A-NR)*, *improved efficacy (such as technological, process and organisational)*, and *extensible for dealing with external and internal deficiencies*.

2.7.1 Cyber-Security Maturity Levels and Assessment

Cybersecurity maturity frameworks support the procedures to measure the current state of cybersecurity in an organisation (Le & Hoang, 2016). Among the earliest Capability Maturity Models (CMM) were proposed by Humphrey (1989) and White (2011), who applied the CMM for software quality assessment. If the need arises, an organisation can also extend these models to address various aspects and domains of IT security risks. For instance, the ISO:IEC:27001 was drafted to enable the choice of appropriate IS controls which could ably protect the IS assets and additionally offer system assurance to the organisational stakeholders (ISO, 2005). Later NIST proposed the Information Security Maturity Model (ISM2), which helped firms in the accurate evaluation of the degree of current cybersecurity maturity through qualitative assessment in the following five dimensions: *policy*, *processes*, *implementation*, *testing*, and *integration* (NIST, 2005). Gartner developed an IT score-based Information Security Awareness Maturity Model that could track the information security development of an organisation through the following five levels: *initial*, *developing*, *defined*, *managed*, and *optimising* Gartner (2009). IBM built the Information Security Framework as a business-level security reference model to connect business drivers with IT security and risk management, based on standards and common practices (IBM, 2007). Similarly, NIST created the Cybersecurity Framework in 2014 to impose the federal-level regulations on responsible firms for critical infrastructure protection (NIST, 2014).

Table 1 provides a summary of recent cyber-security maturity and assessment frameworks examined from the existing literature.

Table 1: Summary of Cyber Security Maturity Models from Extant Literature

#	Name	Year	Author(s)	Objectives
1	Information Security Management Systems	2005	ISO	IT risk management in the context of security standards.
2	Information Security Maturity Model	2007	National Institute of Standards and Technology (NIST)	Review, measure ISPs and the current level of ISA in firms.
3	Information Security Awareness Maturity Model	2009	Gartner	IT risk management and measurement of awareness in big firms.
4	Information Security Framework	2009	IBM	Analyse security gaps between IT strategy and technology implementation.
5	Cyber Security Framework	2014	National Institute of Standards and Technology (NIST)	Impose ISGs, ISPs, and technical cybersecurity measures at the federal level.
6	Cyber Security Capability Maturity Models (C2M2)	2015	Curtis & Mehravari (2015)	Cybersecurity framework implementation in critical infrastructures.

IT risk management involves the use of enterprise risk management techniques in the realm of information technology to cope with systemic or operational risks arising from the usage of information technology in organisations (Coles and Moulton, 2003; ISACA, 2009). Whether an organisation adheres to a systematic methodology to tackle IT risks can be signalled by its formation, regular maintenance, and timely update of its ISMS (Dhillon and Backhouse, 2000). IT risk management is a continuous process that organisations follow, and associated techniques involve these distinct steps – understand, measure, and subsequently mitigate (Debreceny, 2013). Ruan (2017) presents a summary of qualitative and quantitative IT risk management methodologies that have been widely employed by organisations.

2.7.2 Assurance of Security Control Measures lead to Efficacy (Technology, Process, Organisation)

Through information security assurance at an organisation, it desires to recognise whether the imposed security control(s) are in effect, meet the C-I-A-NR and the explicitly identified functional requirements in the control statements/ISPs (von Solms *et al.,* 1994). They also help the stakeholders to examine and confirm whether the above assurance steps lead to a better cyber-security environment in the organisation than earlier (Ross *et al.,* 2009). Thus, organisations must honour the C-I-A-NR of the information assets, and consider it as the primary objective of ISM (Dzazali *et al.,* 2009). Unfortunately, senior management at most organisations perceives information security as a technical problem. In contrast, the reality is that successful enforcement of ISPs and SETA are a managerial hurdle and not a technical one (ITGI, 2005). To begin with, the *confidentiality* of an information system lies in concealing necessary information from being accessed by unauthorised individuals (von Solms *et al.,* 1994; NIST 2013). For example, cryptography, encryption and other technical measures ensure confidentiality of business-level data during transmission between multiple IT systems. Next, the *integrity* of the information system ensures that any business-level data remains an accurate and unaltered depiction of the original information (von Solms *et al.,* 1994; Ross *et al.,* 2007).

Further, organisations need to comply with strict guidelines regarding an appropriate categorization of information and related infrastructure and consequently maintain a consistent level of cyber-security assurance. To address this problem, the National Institute of Standards and Technology (NIST) developed a set of Federal Information Processing Standards (FIPS)[6] and guidelines that adhere to the Federal Information Security Management Act (2002). The most widely used FIPS standards are FIPS-199 and FIPS-200[7]. FIPS guidelines provide a minimum level of security required for business information and related infrastructure allowing a range of risk-levels (such as *lo*, *mid*, *hi*) to categorize the associated information system. For instance, the information system for acquisitions at an e-commerce firm needs to manage the following: (a) sensitive *contract information* from its suppliers and pricing mechanisms for buyers, as well as (b) regular *business activities* and *administrative information*. Using the FIPS framework, the security categorizations (i.e., C-I-A) for type (a) and type (b) are SC_1 = {(C, *mid*), (I, *mid*), (A, *lo*)} and SC_2 = {(C, *lo*), (I, *lo*), (A, *lo*)}, shown in Figures 2(a) and 2(b), respectively. Finally, these security categorizations are combined as *max* {SC_1, SC_2} to calculate the potential impact on the overall information system of the e-commerce firm as SC_3 = {(C, *mid*), (I, *mid*), (A, *lo*)} and shown in Figure 2(c).

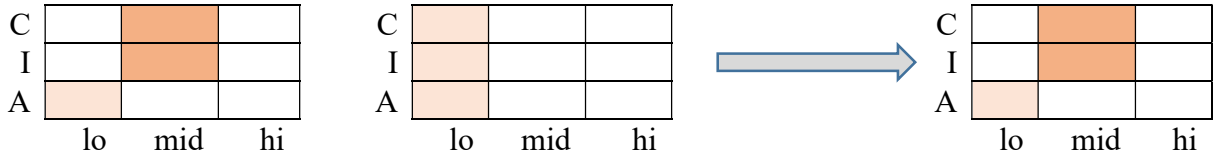

Figure 2(a): SC_1 Figure 2(b): SC_2 Figure 2(c): SC_3

Often, attackers conduct man-in-the-middle (M-o-M) attacks to intercept business-critical data and modify it before the intended receiver can access it. Finally, the *availability* of the information system ensures that the concerned information is always readily accessible to the authorised user(s) (von Solms *et al.,* 1994; NIST 2013). Historically attackers have launched denial-of-service (DoS) attacks the websites of popular e-commerce firms (such as Amazon, eBay), social networks (such as Orkut, Facebook), banks (such as Bank of Spain, HSBC) to disable/disrupt their services. Therefore, after adherence to security control measures in organisations, their enhanced cybersecurity can be measured with the help of strict conformance to C-I-A-NR levels across the organisation—finally, these adopted security control measures to technological efficacy, process efficacy, and organisational efficacy.

2.7.3 Extensible for Dealing with External and Internal Deficiencies

Availability of a comprehensive and robust set of security metrics is essential to meet various business objectives in an organisation. For instance, the European Union (EU) has issued a Directive on Network and Information Security (ENISA, 2015). Another case of externally enforced usage of cybersecurity regulations is while meeting security demands at the third-party levels to comply with contractual service-levels. Although regulations exist for specific

[6] Compliance FAQs: Federal Information Processing Standards (FIPS): https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips
[7] Current Federal Information Processing Standards (FIPS): https://www.nist.gov/itl/current-fips

business use-cases, there are hardly any cybersecurity regulations, which are generic across various industrial IT systems (Le & Hoang, 2016). However, this is rapidly changing with new regulatory frameworks that cover national-level critical infrastructures in particular. Such as, during target breach, the attackers first compromised the IT systems of the facility provider Fazio, a third-party entity, and reached till the customer database of Target (HBR, 2015). Further, CMMs can only ensure bare minimum compliance rather than achieving an aspired level of cybersecurity maturity which will deal with the evolving IT risks, high demand of usage (A-I-C-NR), as well as guarding against advanced attacks (Ross *et al.,* 2007).

A study by Knowles *et al.,* (2015) shows that a degree of flexibility in security maturity models can address each dimension of cyber-space specifically or extend their existing dimensions to cope up with the emerging cyber-spaces. For instance, new attack vectors such as ransomware (a variant of malware) have emerged in recent times, which are marked with ransoms and extortions. The WannaCry, Petya and Locky ransomware has wreaked havoc in European organisations by demanding millions of ransom money to unlock their compromised IT systems and files (Techrepublic, 2017). Additionally, these deficiencies could be internal to the organisation, such as improving the existing risk posture, integrate cybersecurity during the product development period (to reduce the possibility of software vulnerabilities, and build secure source codes), support decision-making at strategic levels (such as, during the installation of new ERP systems) (Jansen, 2009; Roumani *et al.,* 2015), and finally, estimate the ROI on security investments.
The overall research model for the study is illustrated in Fig. 2.

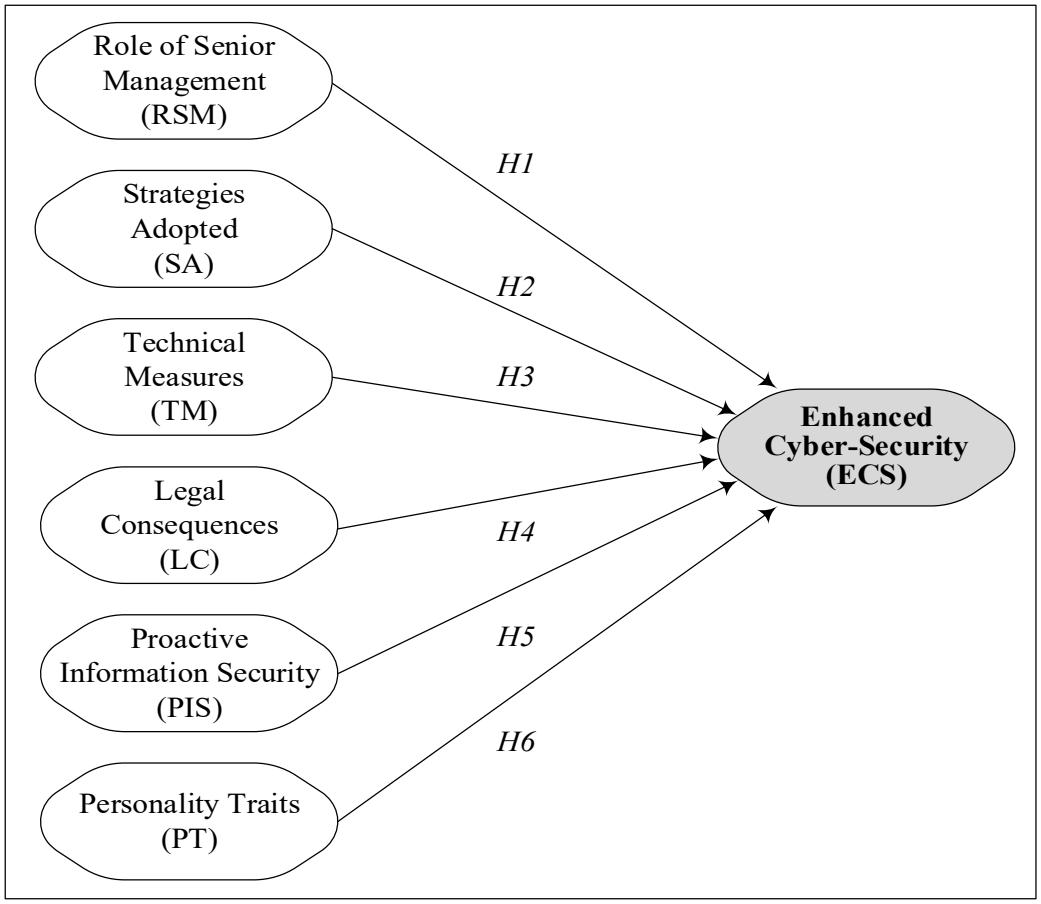

Figure 3: Proposed Research Model

3. METHODOLOGY

3.1 Questionnaire Development

The survey method is used to collect data and test the proposed hypotheses. For the purpose of collecting the data, a questionnaire was prepared. The first part of the questionnaire included demographics of the respondents such as sector, years of experience, education level, etc. The second part of the questionnaire included constructs and their respective measurement items. The measurement items for each construct were adopted from a thorough literature review. We used four items for '*Role of Senior Management*', five items for '*Strategies Adopted*', six items for '*Technical Measures*', three items each for '*Legal Consequences*' and '*Prospective Information Security*' and five items for '*Personality Traits*'. Four items are used to measure the dependent construct '*Enhanced Cybersecurity*'. The items are measured using a 5-point Likert scale (1: "Strongly disagree"; 5: "Strongly agree"). The authors' ensured the content validity of the questionnaire from the literature review and discussion with experts. In accordance with the suggestions from the experts, few items were re-worded, thus providing enhanced understanding and readability for respondents of the questionnaire. The measurement items of each construct are given in Appendix 1.

3.2 Data Collection

The data is collected from professionals who have experience in cyber-security in sectors such as retail, healthcare, education, etc. in Indian firms. The data is collected by the data collection firm, *NexGen Market Research*[8]. In total, 398 professionals are contacted for filling the questionnaire, from which 151 completed responses are finally used for further analysis. The overall response rate is 37.93%, which is considered as good in survey studies (Malhotra & Grover, 1998). The characteristics of the respondents are presented in Table 2. Most of the respondents are in the middle and senior positions in their respective organisations.

Table 2: Characteristics of Respondents

	Number	**Percentage**
Gender		
Male	116	76.82
Female	35	23.17
Education		
Graduate	57	37.74
Post-Graduate	79	52.31
Doctorate	15	9.93
Level in the Organisation		
Lower	2	1.32
Middle	99	65.56
Higher	50	33.11
Experience		
Less than 2 years	5	3.31
2 – 5 years	21	13.90
5 – 10 years	88	58.27
10 – 20 years	35	23.17
More than 20 years	2	1.32

3.3 Common Method Bias (CMB)

CMB can be an issue in survey studies of this kind. To minimise CMB, we conducted the survey with multiple respondents such as middle and senior levels in organisations and working in different functions (Sreedevi & Saranga, 2017). Further, Harman's single-factor approach is used to analyse the concern of CMB (Harman, 1967; Podsakoff & Organ, 1986). According to this approach, the measurement items considered in the model are subjected to un-rotated Exploratory Factor Analysis (EFA). The EFA shows that the first factor explains 41.86% of the total variance, thereby indicating that CMB is not an issue in the collected data (Cheng, 2011).

[8] http://www.nexgenint.com/

3.4 Data Analysis Method

PLS-SEM technique has been used to test the hypotheses in this study. PLS-SEM has been preferred over the covariance-based SEM primarily due to the following reasons: *firstly*, PLS-SEM is a non-parametric method and does not have any restrictions on the normal distribution of data (Chin, 1998); *secondly*, PLS-SEM method provides more statistical power and does not requires large sample size and can be applied with relatively small sample sizes (Chin, 1998; Reinartz *et al.,* 2009). Smart PLS 3 software has been used in this study to carry out the analysis.

4. RESULTS

4.1 Assessment of Measurement Model

Firstly, convergent validity is assessed from factor loading values. The loading of the item, PT4, was found to be less than the recommended value of 0.7. Thus, it was removed from the model. The loadings of three items SA4, SA5 and TM1 though are lesser than 0.7, but since the values are very close to 0.7, they are retained in the model. The factor loadings for all the other items are found to be more than 0.7 (Hair *et al.,* 2006), and are statistically significant. The loadings and the corresponding t-values for all the items are shown in Table 3. Further, all the constructs have an average variance extracted (AVE) values more than 0.5 (Fornell and Larcker, 1981), which further indicates adequate convergent validity. The Dijkstra–Henseler's ρ value for each of the construct is also more than 0.7 (Henseler *et al.,* 2016). Construct reliability is assessed by Cronbach's alpha and Composite Reliability (CR) values. All the constructs have Cronbach's alpha and CR values more than 0.7 (Fornell & Larcker, 1981), indicating adequate construct reliability. The AVE, CR, Dijkstra–Henseler's ρ and Cronbach's alpha values are shown in Table 4.

Discriminant validity is analyzed by examining the cross-loadings of items considered in the model. The cross-loadings indicate that values load higher on the intended constructs, which indicates acceptable discriminant validity (Yadlapalli *et al.,* 2018). The cross-loadings of items are given in Table 5.

Table 3: Factor Loadings

Construct	Item	Factor loading	t-value
ECS	ECS1	0.732	12.884
	ECS2	0.729	11.977
	ECS3	0.785	19.907
	ECS4	0.730	12.903
	ECS5	0.752	15.349
LC	LC1	0.823	26.013
	LC2	0.815	25.860
	LC3	0.822	22.316
PT	PT1	0.742	13.373
	PT2	0.811	25.927
	PT3	0.774	15.204

	PT4	Removed	-
	PT5	0.775	17.439
PIS	PIS1	0.836	28.314
	PIS2	0.776	18.512
	PIS3	0.775	14.335
RSM	RSM1	0.833	15.077
	RSM2	0.890	33.484
	RSM3	0.771	14.714
	RSM4	0.838	21.27
SA	SA1	0.745	14.241
	SA2	0.747	12.360
	SA3	0.707	13.147
	SA4	0.695	12.951
	SA5	0.694	13.925
TM	TM1	0.680	10.919
	TM2	0.730	15.205
	TM3	0.770	16.470
	TM4	0.710	14.725
	TM5	0.770	16.967
	TM6	0.740	13.166

Table 4: Measurement Model

Construct	AVE	Cronbach's Alpha	Composite Reliability	Dijkstra–Henseler's ρ
ECS	0.556	0.800	0.862	0.801
LC	0.673	0.757	0.861	0.759
PT	0.602	0.780	0.858	0.780
PIS	0.634	0.711	0.838	0.717
RSM	0.696	0.853	0.901	0.858
SA	0.516	0.767	0.842	0.772
TM	0.536	0.827	0.874	0.830

Table 5: Cross-Loadings of Measurement Items

	ECS	LC	PT	PIS	RSM	SA	TM
ECS1	0.732	0.534	0.591	0.556	0.532	0.536	0.527
ECS2	0.729	0.512	0.503	0.520	0.490	0.540	0.553
ECS3	0.785	0.574	0.499	0.510	0.520	0.539	0.609
ECS4	0.730	0.588	0.472	0.610	0.591	0.586	0.566
ECS5	0.752	0.480	0.580	0.528	0.520	0.543	0.554
LC1	0.632	0.823	0.553	0.532	0.489	0.507	0.572
LC2	0.569	0.815	0.496	0.479	0.469	0.417	0.462

LC3	0.574	0.822	0.579	0.603	0.523	0.589	0.573
PIS1	0.636	0.584	0.582	0.836	0.525	0.536	0.604
PIS2	0.539	0.512	0.443	0.776	0.516	0.551	0.572
PIS3	0.567	0.465	0.523	0.775	0.571	0.529	0.476
PT1	0.532	0.430	0.742	0.524	0.442	0.484	0.517
PT2	0.523	0.474	0.811	0.392	0.456	0.483	0.522
PT3	0.574	0.552	0.774	0.515	0.495	0.481	0.551
PT5	0.565	0.589	0.775	0.584	0.515	0.555	0.598
RSM1	0.514	0.380	0.463	0.521	0.833	0.601	0.482
RSM2	0.638	0.544	0.551	0.595	0.890	0.660	0.590
RSM3	0.589	0.513	0.486	0.535	0.771	0.495	0.481
RSM4	0.623	0.550	0.545	0.586	0.838	0.635	0.560
SA1	0.633	0.463	0.560	0.538	0.670	0.745	0.553
SA2	0.532	0.383	0.476	0.509	0.662	0.747	0.526
SA3	0.484	0.424	0.447	0.454	0.383	0.707	0.626
SA4	0.453	0.498	0.434	0.487	0.439	0.695	0.539
SA5	0.515	0.449	0.384	0.427	0.375	0.694	0.583
TM1	0.533	0.404	0.454	0.460	0.449	0.680	0.690
TM2	0.527	0.539	0.499	0.485	0.383	0.556	0.729
TM3	0.545	0.489	0.463	0.471	0.389	0.524	0.767
TM4	0.486	0.454	0.514	0.467	0.403	0.493	0.710
TM5	0.560	0.479	0.585	0.499	0.499	0.537	0.769
TM6	0.638	0.506	0.576	0.635	0.635	0.632	0.735

4.2 Structural Model Assessment

The structural model tests the path relationships between latent constructs considered in the conceptual model. We used Bootstrapping method to test the statistical significance level of path coefficients (Hair *et al.,* 2011). The path coefficient values between latent constructs, p-values and t-values are shown in Table 6. Hypotheses H1, H3, H4 and H5 are found to be statistically significant at $p < 0.05$, while hypothesis H6 is statistically significant at $p < 0.1$. Hypothesis H2 is found to be statistically insignificant.

The adjusted R^2 value for the dependent construct 'Enhanced Cybersecurity in Organisations' is found to be 0.725, which confirms that the structural model possesses substantial predictive power (Chin, 1998). The Stone-Geisser's (Q^2) value of dependent construct 'Enhanced Cybersecurity in Organisations' is greater than zero (equal to 0.357), which also confirms that the model has adequate prediction (Zhang & Yang, 2016). The model fit is corroborated from standardised mean square residual (SRMR) value, which is found to be 0.075, thereby indicating adequate model fit (Hu & Bentler, 1998).

Table 6: Hypothesis Testing

Hypothesis	Path	Path Coeff. (β)	p-value	t-value	Supported?
H1**	RSM → ECS	0.174	0.023	2.278	Yes
H2	SA → ECS	0.134	0.186	1.324	No

H3**	TM → ECS	0.189	0.026	2.233	Yes
H4**	LC → ECS	0.217	0.002	3.115	Yes
H5**	PIS → ECS	0.167	0.025	2.253	Yes
H6*	PT → ECS	0.129	0.093	1.683	Partially supported

***Hypothesis is significant at p<0.05*

**Hypothesis is significant at p<0.1*

5. DISCUSSIONS

The digital world has made a significant amount of progress in the recent years. Today, by using digital technology, one can successfully pursue any complex task. However, any business activity that is performed on digital devices needs to be secured from the risk of being impaired by the possible cyber-attacks (Seo and Park, 2019). In this regard, IT risk management has gained greater importance in firms, and they need to identify those factors that can help in achieving an enhanced level of cyber-security in organisations. Among others, these primarily include *proactive information security measures*, the *role of senior management*, *strategies adopted for IT security*, *technical measures*, and *personality traits*. This paper empirically examines the antecedents to an enhanced level of cyber-security in organisations using the data collected from 151 professionals in various sectors and by applying PLS-SEM technique.

The results show that *legal consequences*, *technical measures*, the *role of senior management*, and *proactive information security measures* are the most important antecedents to improve and establish an environment of enhanced cyber-security in organisations. Among these three, *legal measure* is the most vital antecedent for an enhanced level of cyber-security (β=0.217). In this regard, organisations need to follow the law enforced surveillance methods to protect against the cyber-attacks. They should also implement an organizational process where any cyber-attack or data breach is reported to the regulatory agencies. Next, we find that *reporting prior cyber-attacks to regulatory authorities* through compliance with the existing ISGs (Hathaway *et al.*, 2012; Ghappour, 2017), *law-enforced surveillance* using proactive CTI (Samtani *et al.,* 2017), and finally, *adherence to cyber-laws* (Png *et al.,* 2008) all contribute to an enhanced cyber-resilience. These findings are congruent with extant literature on cyber-security legal frameworks (Fischer, 2013), and relevant in the recent business environment with the announcement of privacy laws such as GDPR, SOX, and HIPAA.

Technical measures adopted by the organisations is found to be the second most important determinant for an enhanced level of cyber-security (β=0.189). It suggests that firms need to invest in information security software and implement both proactive and reactive tools (Venter & Eloff, 2003) to prevent cyber-attacks. Proactive information security measures include digital signatures, digital certificates, anti-virus, and anti-phishing scanners (Choo 2011; Ab Rahman & Choo, 2015), whereas reactive measures include access controls, firewalls, biometrics and intrusion detection systems (Curtis and Mehravari, 2015; D'Arcy and Galletta, 2009). Next, robust incident management and response system should be present, which will lead to improved cyber-resilience in organisations (Van der Haar & Von Solms, 2003). Further, firms should perform regular vulnerability assessments, and system scans to track and then

remove security vulnerabilities from infected systems (Roumani *et al*., 2015). Finally, managers should ensure that diverse OS platforms, applications and network software are installed in IT systems to minimize the chances of correlated failures (Chen *et al.,* 2011; Larsen *et al*., 2015; Temizkan *et al.,* 2017). One of the latest studies also found that technical measures related to cyber-attack and cyber experience is an important antecedent for cybersecurity in social enterprises (White *et al.,* 2020).

Role of senior management is found to be the third most crucial determinant for an enhanced level of cyber-security (β=0.174). Congruent to extant studies (HöNe & Eloff, 2002; McFadzean *et al.,* 2006), we found that *commitment of senior management* was the most significant contributing factor among managers. Senior managers of an organisation need to be committed to enhance the level of cyber-security. We suggest this can be achieved through the establishment of a reformed information security culture that could lead to implementable security goals (Da Veiga & Eloff, 2007). Whereas, in contrast to Xue *et al*. (2018), our study reported *ethical leadership behaviour* as the least essential factor among senior management. Technological measures alone cannot improve the cyber-resilience of an organization to the desired level of maturity. Therefore, managers should regularly assess the level of incumbent cyber-security and work towards continuous improvement goals (Webb *et al.,* 2014). In this context, findings from our study echoed those reported by Boss et al. (2009), Dhillon & Mishra (2006), and Herath & Rao (2009). Finally, senior managers must conduct regular evaluation of employees' compliance with those ISPs (Warkentin & Johnston, 2006).

Proactive information security measures have been observed to be the next significant determinant for enhanced cyber-security (β=0.167). In this respect, we found that most employees believe that regular reviews and updates of the existing ISPs at their organisations could lead to enhanced cybers-ecurity. Contrary to technological measures, which are expensive, and are never fail-safe, SETA exercises are efficient social remedies, which organisations can administer first and then follow with IT security tools (Whitman, 2003). Therefore, if the IT managers and software developers are convinced of the ISPs employed by the senior management, they will be practising them, which will lead to regular and relevant updates for improvement (Warkentin & Johnston, 2006; Bulgurcu *et al.,* 2010). Our finding strongly resonates with those reported by extant studies in this context (Doherty & Fulford, 2006; Knapp *et al*., 2009; Cram *et al.,* 2017). Organisations should regularly conduct exercises and training, which can provide employees with an awareness of cyber-security (Dhillon & Backhouse, 2000; Dhillon & Mishra, 2006). Our results matched with Haeussinger & Kranz (2013), who also noted that SETA exercises are capable of improving information security through increased awareness about potential IS risks and implementable ISPs.

Personality traits is also found to be one of the determinants for enhanced cybersecurity. From results, we have found that IT managers who have the personality traits of neuroticism (among the big five personality traits) do not exert any significant impact on the enhanced level of cyber-security in organisations. This result indicates that the associated item PT4 did not load efficiently onto the construct *Personality Traits.* It also shows that the *neurotic* personality (i.e., self-conscious, moody, worries a lot, gets angry, frustrated and feels lonely) of an information

security manager may not play a significantly positive role towards enhancing the cyber-security decisions in an organisation. Extant studies have reported mixed findings regarding the effect of neuroticism in cybersecurity decisions. Bashir and associates (Bashir *et al*., 2015; Wee and Bashir, 2016; Bashir *et al*., 2017) found that the participants in a cybersecurity competition scored the lowest on neuroticism among the Big Five Personality traits, with females scoring higher than males. On the contrary, McBride *et al*., (2012) found that neurotic individuals, who possessed a lower self-efficacy, were less likely to violate cybersecurity protocols. However, other personality traits among Goldberg's Big Five, such as *extraversion*, *agreeableness*, *openness*, and *conscientiousness* have sufficient influence on the adoption of ISPs, practising SETA exercises, and senior managers' commitment towards an enhanced level of cybersecurity in an organisation. We found the support of our results in existing research as well (Goldberg, 1992; McCrae & Costa, 1991; Bashir *et al*. 2017), where open, agreeable, extrovert and highly intellectual individuals can bring significant changes in cybersecurity levels in an organization.

Finally, results suggest that the *strategies adopted* by the managers did not have any significant impact on the enhanced level of cyber-security. While our findings were contradictory to extant studies that successfully examined organisational strategies to influence the maturity levels of cybersecurity (Chang & Yeh 2006; Pérez-González *et al*., 2019; Nassimbeni *et al.,* 2012; Tang & Liu 2015), we posited that the conflicting results could be due to the lack of visibility of these strategies among the respondents in our study. Additionally, the lack of any significant positive effect of IT security strategies on the enhanced level of cybersecurity in organisations could be due to the choice of the industry sectors for our study, i.e., retail, education, and healthcare in the Indian context. While, for studies conducted in the U.S.A. and U.K.: (a) the healthcare data is highly sensitive and regulated by the government due to the availability of EHRs; (b) retailers are highly efficient and regularly communicate between supply-chain partners; and (c) the education sector has seen massive interests from the common public and private organisations alike (Newhouse et al., 2017; Cabaj et al., 2018). In contrast, IT managers in India did not perceive IT security strategies to influence the cybersecurity of organisations in a significant manner for these industry sectors. Additionally, IT managers might have adopted security strategies at the organizational level such as (i) clear vision about the cybersecurity goals, (ii) institutionalised IT security governance, (iii) exercise risk management controls, (iv) a favourable reward and incentive policy for employees, and (v) mutual sharing of critical information on IT infrastructure and software among ISAC members. However, many of these organizational IT security strategies, ISGs, and judgements were not explicitly visible to all the employees of an organization, unless they were part of the linked and executable decisions. Thus, information security management needs to be established on a well-developed and inter-linked IT strategy spread across the entire organisation (Seeholzer, 2012). Finally, senior management should adopt those strategies successfully, be able to evaluate the efficacy of cybersecurity maturity levels, and successfully communicate its value (McFadzean et al., 2011; Tang & Liu 2015).

6. CONCLUSIONS

With the progress of the digital world, there needs to be an enhanced level of cyber-security in organisations. The cyber-security level depends on several factors, such as technical capabilities, human resources, information security measures, etc. In this paper, we investigate the determinants for enhanced cybersecurity level in organisations. *Firstly*, determinants are identified by thorough literature review and discussed with experts. The critical determinants are then analysed by PLS-SEM technique using the data collected from 151 professionals in sectors such as retail, education, healthcare, etc. in India. The results show legal consequences, technical measures, the role of senior management and proactive information security measures to be the most important antecedents for enhanced cybersecurity levels in organisations. The study provides managers with the factors that need to be most focused for enhanced level of cyber-security in their respective organisations. Organisations can take pre-emptive measures and work toward improving the level of cyber-security.

6.1 Implications to Theory and Practice

The study provides implications for research as well as practice. The study can be used for developing insights for both managers and academicians.

Implications to Research: The present study explores the antecedents which impact the enhanced level of cyber-security in the organisations. The results of this study have several important research implications. Firstly, this is the first study of its kind which investigates the Cyber-security not only from a technical perspective but also from a human resource perspective. Secondly, the research found out that the legal consequences after a cyber breach, technical measures adopted by organizations, the role of senior management and proactive information security measures adopted by organizations are the most important antecedents for enhanced cybersecurity levels in organisations.

Implications to Practice: The findings of our study offer several significant managerial implications, especially for CISOs, information security managers, and related departments. *Firstly*, managers need to focus on the critical antecedents/factors that lead to an enhanced level of cyber-security in their respective organisations. While *legal consequences*, *technical measures, the role of senior management,* and *proactive information security measures* are found to be significant, personality *traits* and *strategies adopted by the IT security managers* are relatively weaker antecedents of organizational cyber-security. Therefore, IT security managers can focus on the significant factors and their sub-factors only. The security managers can further take pre-emptive measures towards enhancing the cyber-security in their firms, thereby leading to an enhanced cyber-security environment.

Secondly, we found that *senior management plays an influencing role* in improving organizational cyber-security through regular participation, self-commitment, evaluation, and ethical leadership. Across the organization, senior managers must pledge to an improved information security culture, established legitimacy through self-participations in ISA

exercises and SETA drills, leading to a display of ethical leadership and regular evaluations[9]. We found that an *enhanced effect* is visible sans the personality traits of the IT managers who executed the strategic decisions. This observation is of particular interest given the fact that novel technologies such as big-data projects are often unsuccessful after implementation because of the lack of organizational alignment (Bean and Kiron, 2013) and ineffective managerial best practices (Ross et al., 2013). Our study posited a similar effect for improving the effectiveness of the antecedents of enhanced cyber-security in organisations.

Thirdly, we found that *proactive information security* plays an essential role in enhancing the current level of organizational cyber-security. These processes include whether the organization regularly conducts SETA exercises for its employees, recurrently manages cyber-incidents and vulnerabilities and logs them for predictive analysis (if required), and minimise correlated risks. Additionally, the IT infrastructure must be equipped with proactive information security measures (such as digital signatures, cryptographic keys, and anti-phishing scanners) instead of reactive measures (such as access controls, firewalls, passwords, and remote access, biometrics and intrusion detection systems). These findings have significant implications for the parent organization as well as auxiliary IT hardware and software industries and managed security service providers (MSSP). While business organisations gradually become less dependent on reactive measures, this will create new demand in the market for proactive hardware and software (such as spear-phishing filters[10]), MSSPs, as well as for cyber-security professionals to impart SETA training[11].

Fourthly, we have shown that the *legal consequences* of cyber-attacks is the most influential antecedent of enhancing cyber-security in organisations. This finding has interesting but diverse implications for the legislative department of a business organisation, and that may vary across countries. In India, the sole governing cyber-law is the Information Technology Act (2000)[12], while companies in the U.K. must adhere to the Computer Misuse Act (1990), the General Data Protection Regulation, the Data Protection Act (2018), and the Network and Information Systems Regulation (2018) [13]. In contrast, there exists a robust and effective state and federal framework for cyber-legislation in the U.S.A[14] [15]. In each of these countries, the defence institutions, govt. departments and the military offices primarily control cyber-security legislation and policies. Therefore, we recommend the *inclusivity* of business organisations, as they participate in commercial transactions, and are often targets for malicious attacks.

[9] Why senior leaders are the front line against cyberattacks (McKinsey Digital): https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks

[10] Spear Phishing Market is expected to grow to USD 1,401.6 million by 2022 (PRNews): https://www.prnewswire.com/news-releases/spear-phishing-market-is-expected-to-grow-to-usd-14016-million-by-2022-300468847.html

[11] The curious case of India's cybersecurity skills gap and prevailing opportunities (DataQuest): https://www.dqindia.com/the-curious-case-of-indias-cybersecurity-skills-gap-and-prevailing-opportunities/

[12] Cyber-laws in India: https://www.meity.gov.in/content/cyber-laws

[13] A comparison of legal and regulatory approaches to cyber security in India and the United Kingdom: https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf

[14] Federal Laws Relating to Cybersecurity: https://fas.org/sgp/crs/natsec/R42114.pdf

[15] Cybersecurity Issues and Challenges: In Brief: https://fas.org/sgp/crs/misc/R43831.pdf

Additionally, there are enormous scopes for legal consultants, private and public organisations to contribute towards up-to-date and robust cyber-laws and policies.

6.2 Limitations and future directions

Beyond our contributions to the extant research, we recognise that our study has few limitations. These limitations may hold the potential in contributing towards the future research studiesin this area. We have collected only the quantitative data for capturing the enhanced level of security. The collection of qualitative data would give additional insights concerning the enhanced level of cyber-security. Also, the data was collected from users who are based in India; hence the results cannot be generalized in the global context. The study can be extended by collecting data from other sectors, and results can be compared with this study to check whether there are any differences in antecedents for enhanced cybersecurity among different sectors. Finally, interrelationships between the antecedents can be identified using techniques such as interpretive structural modelling, analytic network process, DEMATEL, etc.

References:

Ab Rahman, N. H. and Choo, K. K. R. (2015), "A survey of information security incident handling in the cloud", *Computers & Security*, Vol. 49, pp. 45-69.

Ahmadi, H., Nilashi, M., & Ibrahim, O. (2015). Organizational decision to adopt hospital information system: An empirical investigation in the case of Malaysian public hospitals. *International journal of medical informatics*, *84*(3), 166-188.

Albrecht, J. P. (2016), "How the GDPR will change the world", *European Data Protection Law Review*, Vol. 2, pp. 287.

Allport, G. W. and Odbert, H. S. (1936), "Trait-names: A psycho-lexical study", *Psychological Monographs*, Vol. 47 No. 1, pp. i. https://doi.org/10.1037/h0093360

Appiah, G., Amankwah-Amoah, J., & Liu, Y. L. (2020). Organizational Architecture, Resilience and Cyber-attacks. *IEEE Transactions on Engineering Management*.

Arachchilage, N. A. G. and Love, S. (2014), "Security awareness of computer users: A phishing threat avoidance perspective", *Computers in Human Behavior*, Vol. 38, pp. 304-312.

Baets, W. (1992), "Aligning information systems with business strategy", *The Journal of Strategic Information Systems*, Vol. 1 No. 4, pp. 205-213.

Bashir, M., Lambert, A., Wee, J. M. C., & Guo, B. (2015). An examination of the vocational and psychological characteristics of cybersecurity competition participants. In *{USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.

Wee C., Bashir M. (2016) Understanding the Personality Characteristics of Cybersecurity Competition Participants to Improve the Effectiveness of Competitions as Recruitment Tools. In: *Nicholson D. (eds) Advances in Human Factors in Cybersecurity. Advances in Intelligent Systems and Computing,* Vol 501. Springer, Cham. https://doi.org/10.1007/978-3-319-41932-9_10

Bashir, M., Wee, C., Memon, N. and Guo, B. (2017), "Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool", *Computers & Security*, Vol. 65, pp. 153-165.

Baskerville, R. L. and Dhillon, G. (2008), "Information systems security strategy", *Policy, Processes, and Practices*, pp. 15.

Bean, R. & Kiron, D. (2013). Organizational alignment is key to big data success. *MIT Sloan Management Review*, *54*(3), 1-6.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A. and Venkatraman, N. (2013), "Digital business strategy: toward a next generation of insights", *MIS Quarterly,* Vol. 37 No. 2, pp. 471-482.

Biswas, B. and Patra, S. (2018), "Forecasting Problems in Cybersecurity: Applying Econometric Techniques to Measure IT Risk", in B. B. Gupta (Ed.), *Computer and cyber security: principles, algorithm, applications, and perspectives*. CRC Press.

Biswas, B. and Mukhopadhyay, A. (2018), "G-RAM framework for software risk assessment and mitigation strategies in organisations", *Journal of Enterprise Information Management*, Vol. 31 No. 2, pp. 276-299.

Biswas, B., Mukhopadhyay, A. and Gupta, G. (2018), "Leadership in Action: How Top Hackers Behave - A Big-Data Approach with Text-Mining and Sentiment Analysis", in *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 1752-1761.

Borrett, M., Carter, R. and Wespi, A. (2014), "How is cyber threat evolving and what do organisations need to consider?", *Journal of Business Continuity & Emergency Planning*, Vol. 7 No. 2, pp. 163-171.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A. and Boss, R. W. (2009), "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 151-164.

Briggs, S. R. (1992), "Assessing the Five-Factor Model of Personality Description", *Journal of Personality*, Vol. *60* No. 2, pp. 253–293.

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, 75, 24-35.

Chen, P. Y., Kataria, G. and Krishnan, R. (2011), "Correlated failures, diversification, and information security risk management", *MIS Quarterly*, Vol. 35 No. 2, pp. 397-422.

Cheng, J. H. (2011), "Inter-organisational relationships and knowledge sharing in green supply chains—Moderating by relational benefits and Guanxi", *Transportation Research Part E: Logistics and Transportation Review*, Vol. 47 No. 6, pp. 837-849.

Chin, W. W. (1998), "The partial least squares approach to structural equation modeling", *Modern methods for Business Research*, Vol. 295 No. 2, pp. 295-336.

Cho, J., Park, I. and Michel, J. W. (2011), "How does leadership affect information systems success? The role of transformational leadership", *Information & Management*, Vol. *48* No. 7, pp. 270-277.

Choo, K. K. R. (2011), "The cyber threat landscape: Challenges and future research directions", *Computers & Security*, Vol. 30 No. 8, pp. 719-731.

Cram, W. A., Proudfoot, J. G. and D'Arcy, J. (2017), "Organisational information security policies: a review and research framework", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 605-641.

Curtis, P.D. and Mehravari, N. (2015), "Evaluating and improving cybersecurity capabilities of the energy critical infrastructure", In Technologies for Homeland Security (HST), 2015 IEEE International Symposium, pp. 1-6

D'Arcy, J., Herath, T. and Shoss, M. K. (2014), "Understanding employee responses to stressful information security requirements: A coping perspective", *Journal of Management Information Systems*, Vol. 31 No. 2, pp. 285-318.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98.

Debreceny, R. S. (2013). Research on IT governance, risk, and value: Challenges and opportunities. *Journal of Information Systems*, *27*(1), 129-135.

Dhillon, G. and Backhouse, J. (2000), "Information system security management in the new millennium [technical opinion]", *Communications of the ACM*, Vol. *43* No. 7, pp. 125-128.

Doherty, N. F. and Fulford, H. (2006), "Aligning the information security policy with the strategic information systems plan", *Computers & Security*, Vol. *25* No. 1, pp. 55-63.

Doherty, N. F. and Fulford, H. (2008), "Information Security Policies in Large Organisations: The Development of a Conceptual Framework to Explore Their Impact", In *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 2727-2744). IGI Global.

Dora, M., Kumar, M., Van Goubergen, D., Molnar, A., & Gellynck, X. (2013). Operational performance and critical success factors of lean manufacturing in European food processing SMEs. *Trends in food science & technology*, 31(2), 156-164.

Dora, Manoj, Maneesh Kumar, and Xavier Gellynck. "Determinants and barriers to lean implementation in food-processing SMEs–a multiple case analysis." *Production Planning & Control* 27.1 (2016): 1-23.

Dzazali, S., Sulaiman, A. and Zolait, A. H. (2009), "Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organisations", *Government Information Quarterly*, Vol. *26* No. 4, pp. 584-593.

Ehrlich, I. (1996), "Crime, punishment, and the market for offenses', *Journal of Economic Perspectives*, Vol. 10 No. 1, pp. 43-67.

Ekelund, S., & Iskoujina, Z. (2019), "Cybersecurity economics–balancing operational security spending", *Information Technology & People*, Vol. 32 No. 5, pp. 1318-1342

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. and Smeraldi, F. (2016), 'Decision support approaches for cyber security investment", *Decision Support Systems*, Vol. 86, pp. 13-23.

Fischer, E. A. (2013). "Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions," Congressional Research Service, Library of Congress, Washington DC.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18*(1), 39-50.

Gal-Or, E. and Ghose, A. (2005), "The economic incentives for sharing security information", *Information Systems Research*, Vol. *16 No.* 2, pp. 186-208.

Garcia, M., Bessani, A., Gashi, I., Neves, N. and Obelheiro, R. (2014), "Analysis of operating system diversity for intrusion tolerance", *Software: Practice and Experience*, Vol. *44* No. 6, pp. 735-770.

Ghappour, A. (2017), "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web", *Stanford Law Review*, Vol. 69, pp. 1075.

Goldberg, L. R. (1992), "The development of markers for the Big-Five factor structure", *Psychological assessment,* Vol. 4 No. 1, pp. 26-42

Gopal, R. D. and Sanders, G. L. (1997), "Preventive and deterrent controls for software piracy", *Journal of Management Information Systems*, Vol. 13 No. 4, pp. 29-47.

Gordon, L.A. and Loeb, M (2003), "Expenditures on competitor analysis and information security: A managerial accounting perspective", In: Bhimani, A. (Ed.), Management Accounting in the New Economy. Oxford University Press, pp. 95–111.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., Richardson, R, (2005), "CSI/FBI computer crime and security survey", *Computer Security Journal*, Vol. 21 No. 3.

Haeussinger, Felix, and Johann Kranz, (2013), "Information security awareness: Its antecedents and mediating effects on security compliant behavior." in *proceedings of International Conference on Information Systems, 2013,* Milano.

Hair, J. F., Ringle, C. M. and Sarstedt, M. (2011), 'PLS-SEM: Indeed a silver bullet", *Journal of Marketing Theory and Practice*, Vol. 19 No. 2, pp. 139-152.

Hair, J., Black, W., Babin, B., Anderson, R. and Tatham, R. (2006). *Multivariate data analysis*, Pearson Prentice Hall, Uppersaddle River, N.J.

Harman, H.H. (1967), *Modem Factor Analysis*. University of Chicago, Chicago

Hausken, K. (2007), "Information sharing among firms and cyber-attacks", *Journal of Accounting and Public Policy*, Vol. *26* No. 6, pp. 639-688.

Henseler, J., Hubona, G. and Ray, P. A. (2016), "Using PLS path modeling in new technology research: updated guidelines", *Industrial Management & Data Systems*, Vol. 116 No. 1, pp. 2-20.

Herath, T., and Rao, H. R. (2009), "Encouraging information security behaviors in organisations: Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165.

Holgate, J. A., Williams, S. P. and Hardy, C. A. (2012), "Information Security Governance: Investigating Diversity in Critical Infrastructure Organizations", In *Bled eConference*, pp. 379-393

HöNe, K. and Eloff, J. H. P. (2002), "What makes an effective information security policy?', *Network Security*, Vol. *2002* No. 6, pp. 14-16.

Hosseini, S., Azgomi, M. A. and Rahmani, A. T. (2016), "Malware propagation modeling considering software diversity and immunization", *Journal of Computational Science*, Vol. *13*, pp. 49-67.

Hu, L. T. and Bentler, P. M. (1998), "Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification", *Psychological Methods*, Vol. *3* No. 4, pp. 424-453

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing employee compliance with information security policies: The critical role of top management and organisational culture", *Decision Sciences*, Vol. *43* No. 4, pp. 615-660.

Hui, K. L., Kim, S. H. and Wang, Q. H. (2017), "Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks", *MIS Quarterly*, Vol. *41* No. 2, pp. 497.

Humphrey, W. S. (1989). *Managing the software process*. Addison-Wesley Longman Publishing Co., Inc.

ISACA. 2009. The RiskIT Framework: RiskIT Based on COBIT. Rolling Meadows, IL: ISACA.

Jansen W. (2009), Directions in Security Metrics Research, NISTIR 7564, *National Institute of Standards and Technology*.

Kacmar, K. M., Bachrach, D. G., Harris, K. J. and Zivnuska, S. (2011), "Fostering good citizenship through ethical leadership: Exploring the moderating role of gender and organisational politics", *Journal of Applied Psychology*, Vol. *96 No.* 3, pp. 633.

Kim, S.H., Wang, Q.H. and Ullrich, J.B. (2012), "A Comparative Study of Cyberattacks," *Communications of the ACM*, Vol. 55 No. 3, pp. 66-73.

Knapp, K.J., Morris, R.F., Marshall, T.E. and Byrd, T.A. (2009), "Information security policy: an organisational level process model", *Computers & Security*, Vol. 28 No. 7, pp. 493-508.

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P. and Jones, K. (2015), "A survey of cyber security management in industrial control systems", *International Journal of Critical Infrastructure Protection*, Vol. *9*, pp. 52-80.

Lagerström, R., Baldwin, C., MacCormack, A., Sturtevant, D. and Doolan, L. (2017), "Exploring the relationship between architecture coupling and software vulnerabilities", in *International Symposium on Engineering Secure Software and Systems,* Springer, Cham, pp. 53-69

Larsen, P., Brunthaler, S. and Franz, M. (2015), "Automatic software diversity", *IEEE Security & Privacy*, Vol. 13 No. 2, pp. 30-37.

Le, N. T. and Hoang, D. B. (2016), "Can maturity models support cyber security?", in *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, pp. 1-7.

Liu, D., Ji, Y. and Mookerjee, V. (2011), "Knowledge sharing and investment decisions in information security", *Decision Support Systems*, Vol. *52* No. 1, pp. 95-107.

Malhotra, M. K. and Grover, V. (1998), "An assessment of survey research in POM: from constructs to theory", *Journal of Operations Management*, Vol. 16 No. 4, pp. 407-425.

Martin, G., Martin, P., Hankin, C., Darzi, A. and Kinross, J. (2017), "Cybersecurity and healthcare: how safe are we?", *BMJ*, Vol. *358*, pp. 3179.

McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *RTI International-Institute for Homeland Security Solutions*, *5*(1), 1.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017), "Individual differences and information security awareness", *Computers in Human Behavior*, Vol. *69*, pp. 151-156.

McCrae, R. R. and Costa, P. T. (1991), "Adding Liebe und Arbeit: The full five-factor model and well-being", *Personality and Social Psychology Bulletin*, Vol. 17 No. 2, pp. 227–232.

Mishra, S. and Dhillon, G. (2006), "Information systems security governance research: a behavioral perspective", in *1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference*, pp. 27-35

Moulton, R. and Coles, R. S. (2003), "Applying information security governance", *Computers & Security*, Vol. *22* No. 7, pp. 580-584.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication*, *800*(2017), 181.

NIST, J.T.F.T.I., (2013), "Security and privacy controls for federal information systems and organizations", *Technical Report.*

Osatuyi, B. (2015), "Personality Traits and Information Privacy Concern on Social Media Platforms", *The Journal of Computer Information Systems*, Vol. 55 No. 4, pp. 11–19.

Palmer, M. E., Robinson, C., Patilla, J. C. and Moser, E. P. (2001), "Information security policy framework: best practices for security policy in the e-commerce age", *Information Systems Security*, Vol. 10 No. 2, pp. 1-15.

Pérez-González, D., Preciado, S. T. and Solana-Gonzalez, P. (2019), "Organizational practices as antecedents of the information security management performance", *Information Technology & People*, Vol. 32. No. 5, pp. 1262-1275

Podsakoff, P. M. and Organ, D. W. (1986), "Self-reports in organisational research: Problems and prospects", *Journal of Management*, Vol. *12* No. 4, pp. 531-544.

Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through information systems security training: An action research study", *MIS Quarterly*, Vol. *34* No. 4, pp. 757–778.

Ratten, V. (2019). The effect of cybercrime on open innovation policies in technology firms. *Information Technology & People*, Vol. 32 No. 5, pp. 1301-1317

Reinartz, W., Haenlein, M. and Henseler, J. (2009), 'An empirical comparison of the efficacy of covariance-based and variance-based SEM", *International Journal of Research in Marketing*, Vol. *26* No. 4, pp. 332-344.

Ross, Jeanne W., Cynthia M. Beath, and Anne Quaadgras. (2013). You may not need big data after all, *Harvard Business Review*, 91(12), pp. 90-104.

Roumani, Y., Nwankpa, J. K. and Roumani, Y. F. (2015), "Time series modeling of vulnerabilities", *Computers & Security*, Vol. 51, pp. 32-40.

Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security*, *65*, 77-89.

Safa, N. S. and Von Solms, R. (2016), "An information security knowledge sharing model in organizations", *Computers in Human Behavior*, Vol. 57, pp. 442-451.

Samtani, S., Chinn, R., Chen, H. and Nunamaker Jr, J. F. (2017), "Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence", *Journal of Management Information Systems*, Vol. 34 No. 4, pp. 1023-1053.

Seo, B. G. and Park, D. H. (2019), "The effect of message framing on security behavior in online services: Focusing on the shift of time orientation via psychological ownership", *Computers in Human Behavior*, Vol. 93, pp. 357-369.

Sipior, J. C., Bierstaker, J., Borchardt, P. and Ward, B. T. (2018), "A Ransomware Case for Use in the Classroom", *Communications of the Association for Information Systems*, Vol. *43 No.* 1, pp. 32.

Siponen, M., Mahmood, M. A. and Pahnila, S. (2014), 'Employees' adherence to information security policies: An exploratory field study", *Information & Management*, Vol. 51 No. 2, pp. 217-224.

Skopik, F., Settanni, G. and Fiedler, R. (2016), "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing", *Computers & Security*, Vol. 60, pp. 154-176.

Solove, D. J. (2003), "Reconstructing electronic surveillance law", *Geo. Wash. L. Rev.*, Vol. 72, pp. 1264.

Sreedevi, R. and Saranga, H. (2017), "Uncertainty and supply chain risk: The moderating role of supply chain flexibility in risk mitigation", *International Journal of Production Economics*, Vol. 193, pp. 332-342.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., ... and Tetrick, L. E. (2015), "Improving cybersecurity incident response team effectiveness using teams-based research", *IEEE Security & Privacy*, Vol. *13* No. 4, pp. 20-29.

Sureshkumar, V., Amin, R., Vijaykumar, V. R. and Sekar, S. R. (2019), "Robust secure communication protocol for smart healthcare system with FPGA implementation", *Future Generation Computer Systems*, Vol. *100*, pp. 938-951.

Taib, R., Yu, K., Berkovsky, S., Wiggins, M. and Bayl-Smith, P. (2019), "Social Engineering and Organisational Dependencies in Phishing Attacks", in *IFIP Conference on Human-Computer Interaction,* Springer, Cham, pp. 564-584

Temizkan, O., Park, S., & Saydam, C. (2017), "Software diversity for improved network security: optimal distribution of software-based shared vulnerabilities", *Information Systems Research*, Vol. *28 No.* 4, pp. 828-849.

Rayome, A. (2017), "The top 10 worst ransomware attacks of 2017, so far", available at https://www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/ (accessed 12 August 2019)

Van der Haar, H. and Von Solms, R. (2003), "A model for deriving information security control attribute profiles", *Computers & Security*, Vol. 22 No. 3, pp. 233-244.

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J. and Kusev, P. (2018), "Security and privacy in online social networking: Risk perceptions and precautionary behavior", *Computers in Human Behavior*, Vol. 78, pp. 283-297.

Veiga, A. D. and Eloff, J. H. (2007), "An information security governance framework", *Information Systems Management*, Vol. 24 No. 4, pp. 361-372.

Venter, H. S. and Eloff, J. H. (2003), "A taxonomy for information security technologies", *Computers & Security*, Vol. *22* No. 4, pp. 299-307.

Von Solms, B. and Von Solms, R. (2004), "The 10 deadly sins of information security management", *Computers & Security*, Vol. *23* No. 5, pp. 371–376.

Von Solms, S. B. (2005), "Information Security Governance–compliance management vs operational management", *Computers & Security*, Vol. 24 No. 6, pp. 443-447.

Warkentin, M, and Johnston, A.C. (2006). "IT security governance and centralized security controls", in *Enterprise information systems assurance and system security: Managerial and technical issues*. IGI Global, 2006. 16-24.

Warkentin, M., and Johnston, A. C. (2006), "IT Security Governance and Centralized Security Controls," in *Enterprise Information Assurance and System Security: Managerial and Technical Issues, M. Warkentin, and R. Vaughn (eds.), Hershey, PA: Idea Group Publishing*, pp. 16-24.

White, G.B. The community cyber security maturity model. in Technologies for Homeland Security (HST), 2011 IEEE International Conference on. 2011. IEEE.

White, G. R., Allen, R. A., Samuel, A., Abdullah, A., & Thomas, R. J. (2020). Antecedents of Cybersecurity Implementation: A Study of the Cyber-Preparedness of UK Social Enterprises. *IEEE Transactions on Engineering Management*.

Whitman, M. E. (2003), "Enemy at the gate: threats to information security", *Communications of the ACM*, Vol. *46* No. 8, pp. 91.

Xue, B., Xu, F. and Warkentin, M. (2018), "Critical role of ethical leadership on information security climate and employee ISP violation behavior", in *Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy* (Vol. 1).

Yadlapalli, A., Rahman, S. and Gunasekaran, A. (2018), "Socially responsible governance mechanisms for manufacturing firms in apparel supply chains", *International Journal of Production Economics*, Vol. 196, pp. 135-149.

Yusof, M. M., Kuljis, J., Papazafeiropoulou, A., & Stergioulas, L. K. (2008). An evaluation framework for Health Information Systems: human, organization and technology-fit factors (HOT-fit). *International journal of medical informatics*, *77*(6), 386-398.

Zhang, H. and Yang, F. (2016), "On the drivers and performance outcomes of green practices adoption: an empirical study in China", *Industrial Management & Data Systems*, Vol. 116 No. 9, pp. 2011-2034.

APPENDIX 1: CONSTRUCTS AND MEASUREMENT ITEMS

- **Enhanced Cyber Security (ECS)**
  - ***ECS1:*** *Does your organisation regularly perform cyber-security assessment exercise?*
  - ***ECS2:*** *Does your organisation follow the security control measures such as those of Confidentiality, Integrity, Authenticity and Non-Repudiation?*
  - ***ECS3:*** *Has the implemented security controls in your organisation lead to technological efficacy, process efficacy, and organisational efficacy?*
  - ***ECS4:*** *Is the current model extensible for dealing with emerging cyberspaces (external deficiencies), that may lead to enhanced cybersecurity in your organisation?*
  - ***ECS5:*** *Can the existing Risk Management framework incorporate system drawbacks (internal deficiencies) to upgrade the current cybersecurity level in your organisation?*

- **Legal Consequences (LC)**
  - ***LC1:*** *Do you think that if the firms reported prior cyber-attacks to regulatory authorities, it could lead to enhanced cyber-security in organisations?*
  - ***LC2:*** *Is your company following the law enforced surveillance method to protect against cyber-attacks?*
  - ***LC3:*** *Is your company following the law enforced by the central government regarding data protection?*

- **Personality Traits (PT)**
  - ***PT1:*** *Do you think the Information Security Manager in your company is extrovert by nature?*
  - ***PT2:*** *Do you think the Information Security Manager in your company is agreeable by nature?*
  - ***PT3:*** *Do you think the Information Security Manager in your company is open to new ideas regarding information security?*
  - ***PT4:*** *Do you think the Information Security Manager in your company is moody in nature and experience his feelings as anxiety, worry, fear, anger, frustration, envy, jealousy, guilt, depressed mood, and loneliness?*
  - ***PT5:*** *Do you think the Information Security Manager in your company has the quality to do his work/ duty well and thoroughly*?

- **Proactive Information Security (PIS)**
  - ***PIS1:*** *Do you think that the IT security team regularly review and update the drafted Internet Service Policies at your company?*
  - ***PIS2:*** *Does your company have generic Security Education, Training, and Awareness (SETA) programs?*
  - ***PIS3:*** *Do you believe that your company have proactive information security measures?*
- **Role of Senior Management (RSM)**
  - ***RSM1:*** *Whether senior management of your company is committed to ensuring a high level of cyber-security?*
  - ***RSM2:*** *Does the regular participation of senior management in information security initiatives lead to an enhanced level of cyber-security in your company?*
  - ***RSM3:*** *Does a regular evaluation of compliance with information security policies is conducted by senior management in your company?*
  - ***RSM4:*** *Does ethical leadership among senior management enhances the level of cyber-security in your company?*

- **Strategies Adopted (SA)**
  - ***SA1:*** *Do the senior managers of the firm possess a clear vision about information security in the organisation?*

- ***SA2:*** *Are the business goals of your company lead to executable IT Security goals?*
- ***SA3:*** *Whether there are sufficient Information Security Risk Management controls at the strategic level in your company?*
- ***SA4:*** *Does the management adopt a reward policy for employees who comply with Information Security Protocols?*
- ***SA5:*** *Is your company actively contributing to the Information Sharing and Analysis Center by sharing of relevant, actionable cyber threat information to other companies?*

- **Technical Measures (TM)**
  - ***TM1:*** *Does your company invest in tools such as those of Digital Signatures; Cryptographic Keys?*
  - ***TM2:*** *Does your company invest in tools such as those of Firewalls; Access control Passwords; Biometrics?*
  - ***TM3:*** *Is your company able to manage cyber incidents effectively and take remedial measures?*
  - ***TM4:*** *Is there a provision in your company to perform regular vulnerability assessments and periodic system scans to track and remove security vulnerabilities?*
  - ***TM5:*** *Are there contingency plans in place at your company to cope and recover from any security breach?*
  - ***TM6:*** *Are the IT systems installed with OS /Apps/ Network software with uncorrelated vulnerabilities to minimize risks of correlated failure in the organisational IT systems?*