Application of grounded theory in construction of factors of internal efficiency and external effectiveness of cyber security and developing impact models

Received 25 April 2022
Revised 1 August 2022
Accepted 4 November 2022

Durga Prasad Dube
Siksha O Anusandhan University, Bhubaneswar, India and
Department of Cyber Security, Reliance Industries Ltd, Mumbai, India, and
Rajendra Prasad Mohanty
Department of Management, Siksha O Anusandhan University, Bhubaneswar, India

Abstract

Purpose – As evident from the literature review, the research on cyber security performance is centered on security metrics, maturity models, etc. Essentially, all these are helpful for evaluating the efficiency of cyber security organization but what matters is how the factors of internal efficiency affect the business performance, i.e. the external effectiveness. The purpose of this research paper is to derive the factors of internal efficiency and external effectiveness of cyber security and develop impact model to identify the most and least preferred parameters of internal efficiency with respect to all the parameters of external effectiveness.

Design/methodology/approach – There are two objectives for this research: Deriving the factors of internal efficiency and external effectiveness of cyber security; Developing a model to identify the impact of internal efficiency factors on the external effectiveness of cyber security since there is not much evidence of research in defining the factors of internal efficiency and external effectiveness of cyber security, the authors have chosen grounded theory methodology (GTM) to derive the parameters. In this study emic approach of GTM is followed and an algorithm is developed for administering the grounded theory research process. For the second research objective survey methodology and rank order was used to formulate the impact model. Two different samples and questionnaires were designed for each of the objectives.

Findings – For the objective 1, 11 factors of efficiency and 10 factors of effectiveness were derived. These are used as independent and dependent variable respectively in the later part of the research for the second objective. For the objective 2 the impact models among independent and dependent variables were formulated to find out the following. Most and least preferred parameters lead to internal efficiency of cyber security organization to identify the most and least preferred parameters of internal efficiency with respect to all the parameters external effectiveness.

Research limitations/implications – The factors of internal efficiency and external effectiveness constructed by using grounded theory cannot remain constant in the long run, because of dynamism of the domain itself. Over and above this, there are inherent limitations of the tools like grounded theory, used in the research. Few important limitations of GTM are as below in grounded theory, it is comparatively difficult to maintain and demonstrate the rigors of research discipline. The sheer volume of data makes the analysis and interpretation complex, and lengthy time consuming. The researchers' presence during data gathering, which is often unavoidable and desirable too in qualitative research, may affect the subjects' responses. The subjectivity of the data leads to difficulties in establishing reliability and validity of approaches and information. It is difficult to detect or to prevent researcher-induced bias.

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 3 No. 1, 2023
pp. 41-70
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-04-2022-0009

Practical implications – The internal efficiency and external effectiveness factors of cyber security can be further correlated by the future researchers to understand the correlations among all the factors and predict cyber security performance. The grounded theory algorithm developed by us can be further used for qualitative research for deriving theory through abstractions in the areas where there is no sufficient availability of data. Practitioners of cyber security can use this research to focus on relevant areas depending on their respective business objective/requirements. The models developed by us can be used by the future researchers to for various sectoral validations and correlations.

Social implications – Though the financial costs of a cyber-attack are steep, the social impact of cyber security failures is less readily apparent but can cause lasting damage to customers, employees and the company. Therefore, it is always important to be mindful of how the impact of cyber security affects society as well as the bottom line when they are calculating the potential impact of a breach. Underestimating either impact can destroy a brand. The factor of internal efficiency and external effectiveness derived by us will help stakeholder in focusing on relevant area depending on their business. The impact model developed in this research is very useful for focusing a particular business requirement and accordingly tune the efficiency factor.

Originality/value – During literature study the authors did not find any evidence of application of grounded theory approach in cyber security research. While the authors were exploring research literature to find out some insight into the factor of internal efficiency and external effectiveness of cyber security, the authors did not find concrete and objective research on this. This motivated us to use grounded theory to derive these factors. This, in the authors' opinion is one of the pioneering and unique contribution to the research as to the authors' knowledge no researchers have ever tried to use this methodology for the stated purpose and cyber security domain in general. In this process the authors have also developed an algorithm for administering GTM. Further developing impact models using factors of internal efficiency and external effectiveness has lots of managerial and practical implication.

Keywords Grounded theory, Maturity model, Cyber security performance, Cyber security governance

Paper type Research paper

1. Introduction

To be competitive, grow, evolve and innovate at the same time, corporations across the globe are resorting to digital transformation. Digital transformation helps in enhanced data collection, greater resource management, data-driven customer insights, an overall better customer experience and encourages digital culture. This in turn brings in benefits such as improved collaboration, increased profits, increased agility and improved productivity. Essentially digital transformation is all about reimagining businesses in the digital world (Dube and Mohanty, 2020). While digital transformation is expected to bring business differentiations, this also creates a lot of uncertainty in terms of governance and risk management. The proliferation of assets expands the attack surface and thus the overall exposure. World Economic Forum (WEF), in their Risk report 2016 (WEF -2016) have raised questions on the societal implications of digital transformation (Accenture-2016).

Cyber security risk is now very prominent and is recognized by all the stakeholders from individuals to government and global multilateral organizations. Risks related to cyber security are included in top five global risks by WEF in world risk report −2021. With the emergence of new technologies like IOT, blockchain, etc. the dimensions of cyber risk have expanded. The effectiveness of the existing cyber-risk assessment approaches on technologies like IOT have been challenged by few researchers too (Radanliev *et al.*, 2021) As per the recent studies by Gartner (2019), overall spending on cyber security increased by 10.5% in 2019, with cloud security projected to grow 41.2% over the next five years. The main driver for this increase in spending is about the expanding need to be compliant with various laws and regulations related to intellectual property rights (IPR), data privacy and cyber security. With this increase in spending, it is obvious that the discussion on the ROI (return on investment), cyber security performance and above all the governance around cyber security also increased among all the stakeholders including the information security research community.

Information security governance is all about establishing a "desired" state of security and it is always the responsibility of the management to give due importance to information security as a business requirement, which will then drive and sustain the "desired state" of security This desired state is very dynamic as it must align with business objectives, technology penetration, associated threats and the risk appetite. Thus, there is a need for a generic set of guidelines for information security which should serve as a reference point for performance metrics. These guidelines should serve as a continuous improvement program (CIP) for the organizations to measure their information security posture on an ongoing basis. Essentially these CIPs are maturity models, which need to be all encompassing, considering all digital technologies and processes and need to be empirically validated. There are various maturity models on cyber security in the contemporary literature. Dube and Mohanty (2020) have presented a latest cyber security capability maturity model (CSMM). This internal maturity of IT organization is labeled as "Internal efficiency" (Simonsson *et al.*, 2007, 2010). In the similar way various scholars have stressed the importance of maturity models for information security organization (Stevanović, 2011; Karokola *et al.*, 2011; Salh, 2011; Watkins and Hurley, 2016; Zhao and White, 2017; Dube and Mohanty, 2020). These authors have proposed various factors for this internal maturity level of information/cyber security organization. Although these internal efficiency metrics of the Information security function are important but for the business leaders this is of moderate interest only; what really matters for them is the "External effectiveness" of services that the Information security organization delivers to the business, which is the actual performance of information security. So, the business parameters which are impacted by the efficiency of cyber security are called "External effectiveness". Thus there is a critical need for strategic integration of internal efficiency and external effectiveness at the management systems level. Therefore the research problems at hand are,

(1) Construct the factors of internal efficiency and external effectiveness of cyber security.

(2) Derive the impact of internal efficiency factors on the factors of external effectiveness

With this perspective, the literature review phase of this research started with an objective to explore if any research exists in defining the parameters of internal efficiency and external effectiveness of cyber security and their linkage.

2. Review of literature

Since the area of maturity model, performance evaluation, metrics broadly come under the area of performance management research, the literature review is initiated from "IT Governance Research" and then branched to "Cyber Security Performance Management" from there. The thematic representation of the branching of the literature is depicted in Figure 1. The theoretical differences between information and cyber security are not part of the scope of our research and hence these words will be used interchangeably.

2.1 IT governance and cyber security performance management

IT governance performance is essentially the quality and value that IT organizations provide by delivering the services, as seen from a customer perspective, i.e. business point of view. This concept is more aligned to the discipline of "strategic alignment", where a considerable amount of research has been done in mid 90s, which provide guidance on business/IT strategic alignment. Weill and Ross (2004) are probably the first few researchers who defined "IT governance performance as the effectiveness of IT governance". They have defined four performance and effectiveness parameters namely,

(1) "Cost-effective use of IT"

(2) "Effective use of IT for asset utilization"

(3) "Effective use of IT for growth"

(4) "Effective use of IT for business flexibility"

With the growth of digital technologies, the attack surface also has increased manifold and cyber security controls have become very essential. Consequently, research studies on cyber security performance have also picked up momentum.

After reviewing the contemporary literature in this theme, the cyber security performance research branches are classified as per Table 1:

2.2 Security metrics

The objectives of cyber security metrics for organizations are defined by (Black *et al.* (2008)) as follows.

(1) "Verify that their security controls are in compliance with a policy, process, or procedure"

(2) "Identify their security strengths and weaknesses"

(3) "Identify security trends, both within and outside the organization's control. Studying trends allows an organization to monitor its security performance over time and to identify changes that necessitate adjustments in the organization's security posture".

Over the past decade, measurement of performance has become increasingly important in the field of information security, and this is now mandated explicitly by "ISO/IEC 27001 standard (ISO/IEC, 2005)". Consequently, a substantial number of research studies have been initiated in this and its related areas too.

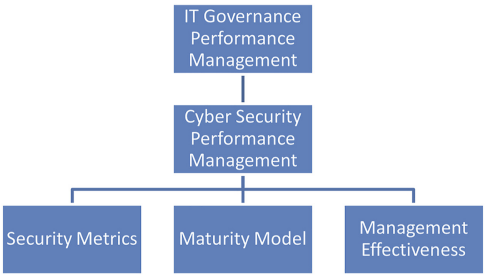

Figure 1.
Thematic representation of branching of literature of cyber security performance management

Area	Relevant papers reviewed
Security metrics	Boyer and McQueen (2007), Dogaheh (2010), Jafari *et al.* (2010), Mermigas *et al.* (2013), Holm and Afridi (2015), Barabanov *et al.* (2011), Chaula *et al.* (2005), Pendleton *et al.* (2016), Diesch *et al.* (2018)
Maturity model	Zhao and White (2017), Watkins and Hurley (2016), Stevanović (2011), Simonsson *et al.* (2007), PoppelbuB and Roglinger (2011), Ngwum (2016), Karokola *et al.* (2011), ISM3 Consortium (2007), C2M2 (2014), Becker *et al.* (2009), Dube and Mohanty (2020)
Management effectiveness	Zaini *et al.* (2018), Kanungo *et al.* (2011), Igor Bernik Kaja Prislan (2016), Chew *et al.* (2008)

Table 1.
Research on cyber security performance management

In the meantime, the regulatory framework across the world also got fortified and lots of new regulations came into existence which necessitated more governance around information technology sector. Of course, there are internal factors too, such as "needs to better justify and prioritize security investments, ensure good alignment between security and the overall organizational mission, goals, and objectives, and fine-tune effectiveness and efficiency of the security programs necessitated stronger governance mechanism and security metrics. (Rostyslav *et al.* 2011)". The performance measurement guide on information security published by NIST (2008) describes the process of designing security metrics.

2.3 Maturity model

Extensive literature study in cyber security maturity model was carried out. A total of 10 contemporary maturity models in cyber security and latest being the CSCMM (Dube and Mohanty, 2020), were reviewed. The summary of our review of literature on this subject are as follows.

(1) Since their attribution, maturity models have been subject to criticism. For instance, they have been characterized as "step-by-step recipes" that oversimplify reality and lack empirical foundation (Benbasat *et al.*, 1984; De Bruin *et al.*, 2005; King and Kraemer, 1984; McCormack *et al.*, 2009).

(2) As for practical application, typical purposes of use of MMs are broadly classified into three types namely; descriptive, prescriptive and comparative (De Bruin *et al.*, 2005).

- *Descriptive*
  - A maturity model serves a descriptive purpose if it can be applied for as-is assessments where the current capabilities of the entities under investigation are assessed with respect to given criteria (Becker *et al.*, 2009).
  - This is used as a diagnostic tool for understanding the current posture.
  - The derived maturity level can be reported to internal and external stakeholders and can be used as a governance tool.
- *Prescriptive*
  - A maturity model serves the prescriptive purpose if it indicates how to identify the desired maturity level and provide guidelines for improvement
  - This is also used as a tool for CIP and also serves as a governance tool.
- *Comparative*
  - A maturity model serves a comparative purpose of use if it allows for internal or external benchmarking.
  - This can be used for compliance purposes too where certain level of maturity is mandated by regulators, etc.

(3) Dube and Mohanty (2020) have compared nine contemporary maturity models against seven parameters and constructed a new maturity model, i.e. CSCMM, which has also been empirically validated by them. The nine maturity used for comparison purposes are as follows:

- SSE-CMM (1998)
- COBIT(PAM) (2013)

- NIST (2014)
- ISM3 (2007)
- OCTAVE (2003)
- SPMM (2005)
- ISMM (2016)
- Cyber security capability maturity model (CMM) 2014
- C2M2, 2014

(4) Cyber security capability maturity model provides a benchmark by which an organization can assess the current level of maturity of its practices, processes and set goals and priorities for improvement in cyber security (Rea-Guamán *et al.*, 2017).

(5) Rea-Guamán *et al.* (2017) also did a comparative study of four cyber security capability maturity model viz e C2M2, SSE-CMM, CCSMM and NICE and concluded that all cyber security capability maturity models are based on cyber security risk management, but only SSE-CMM and C2M2 measure risk management in a more specific way.

Most of the maturity models on cyber security are essentially meant to measure the internal efficiency of cyber security organizations. The authors have not come across any research around linking this internal efficiency with business performance.

2.4 Management effectiveness

The authors have studied various research papers to understand the management effectiveness of cyber security performance. Most of the research are around Return on investment (Kanungo *et al.*, 2011; Ababneh *et al.*, 2017), key performance indicators (KPI) (Igor Bernik Kaja Prislan, 2016). Zaini *et al.* (2018) in their study believe that information security is vital in protecting information resources and should be used as strategic resources for competitive advantages as part of organizational objectives. Having secure strategic information resources allow organizations to be dynamic in the unpredictable business environment. Igor Bernik Kaja Prislan (2016) emphasized the need for measuring information security performance and its linkage to management effectiveness and proposed a 10 by 10 information security performance measurement model. The model—ISP 10 × 10 M is composed of ten critical success factors, 100 KPI and six performance levels.

2.5 Research gaps

Based on the above literature review, the following research gaps are inferred:

(1) All the research papers studied by us on information security maturity models are essentially a CIP to increase the internal efficiency of cyber security organization.

(2) The authors have not come across any research around linking the internal efficiency to the business requirement.

(3) In fact, from the literature study, it is observed that overall, a gap in defining the parameters of internal efficiency and external effectiveness for cyber security.

(4) The measurement of security performance in general and the development of security metrics itself are in a very early research stage and quite underdeveloped (Savola, 2009; Savola and Heinonen, 2011; Zalewski *et al.*, 2014).

(5) Essentially how to measure security and defense level of the organization are the gaps in research (Vaughn *et al.*, 2003, Purboyo *et al.*, 2011, Alavi *et al.*, 2016).

(6) The practice and process of measurement are also a gap in the research. (Abu-Musa, 2010; Sowa and Gabriel, 2009; Bayuk and Mostashari, 2013).

3. Significant learning and the statement of the research problem

From the literature study and the research gaps, the following significant learning and the problem statement are derived:

(1) Cyber security performance management research is more related to the study of maturity models and security metrics.

(2) Maturity models are essentially measuring the internal efficiency of the cyber security organization and not related to the contribution of cyber security to business.

(3) Security metrics are more operational in nature and are essentially the key performance indicator (KPI) to measure the efficiency of cyber security organizations.

(4) There is a need to look at cyber security performance from a business perspective, i.e. to understand the extent to which the efficiency of cyber security organization contributes to the business performance; which is the effectiveness of the cyber security performance. Thus, the first step to achieve this objective is to clearly define the factors of efficiency and effectiveness and then develop models to derive the impact of Internal efficiency factors on the factors of external effectiveness therefore there are two broad research objectives.

- Construct the factors of internal efficiency and external effectiveness of cyber security.
- Derive the impact of internal efficiency factors on the factors of external effectiveness.

4. Research phases

After defining the problem statements, the further research is carried out in two phases.

The objective, research methodology, techniques, sample selection and finding of each phase of the research are as below. The overall phase of research is depicted in Figure 2.

5. Phase 1

5.1 Objective – construct the factors of internal efficiency and external effectiveness of cyber security

5.1.1 Research methodology. Since there is not much evidence of research in defining the factors of internal efficiency and external effectiveness of cyber security, the authors have chosen grounded theory methodology (GTM) to derive the parameters.

5.2 Grounded theory methodology

The objective of GTM is to enable the discovery of inductive theory. As per Martin and Turner, 1986, "It helps researchers to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data". Although developed five decades ago, by Glaser and Strauss (1967) GTM continues to become one of the most frequently used qualitative research methods in social science research.

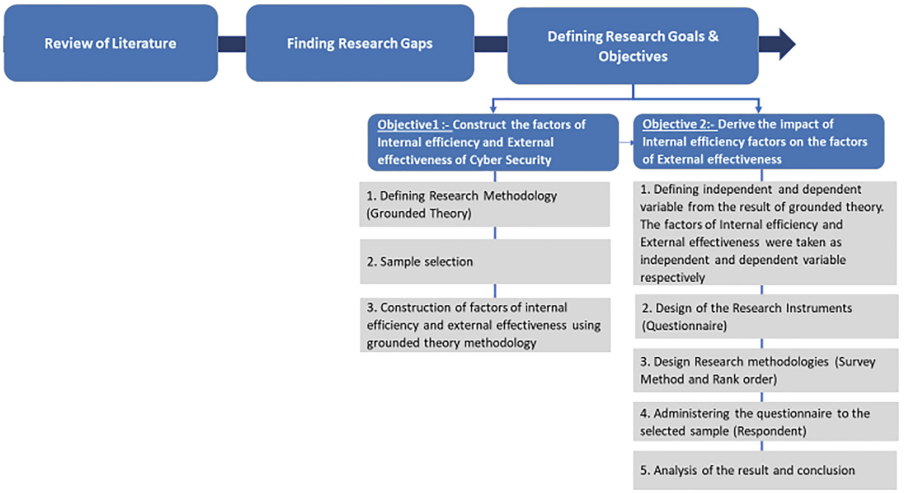

Figure 2.
Overall phases of research

GTM is very relevant for research on issues where there are very less prior research and thus a need for theory building. (Lehmann 2010; Seidel and Urquhart, 2013). As discussed above, in the literature study section, not much work has been done in empirical validation of internal and external effectiveness of cyber security. GTM has been increasingly used in information system research to study technological change and sociotechnical behavior in emerging research domains (Birks *et al.*, 2013; Matavire and Brown, 2013; Urquhart and Fernandez, 2006). GTM, with its espoused goal of theory development of unique issues, has now found broad application in information systems (IS) research (Wiesche *et al.*, 2017).

There are two perspectives of grounded theory: objectivist and constructive. Objectivist grounded theory is a Glaserian approach and based on etic position, where the researcher takes an independent position as an outsider from the respondents. Whereas constructivist grounded theory is a Straussian approach and is based on emic position, where the researchers co-construct the data and behave as an insider with the respondents, without influencing the respondents. (Taghipour, 2014). In this study emic approach is followed and an algorithm is developed (Figure 2) for administering the grounded theory research process.

5.3 Grounded theory algorithm

The steps in the algorithm are used to administer GTM with a focus group comprising of cyber security and business professionals. The authors have used the systems approach in developing this algorithm. The systems approach to the problem solution is such an approach which understands the studied phenomena and processes in complex internal and external contexts, (Dettmer, 2007; Hubálovský and Milková, 2010). The process is discussed in the following section (see Figure 3).

5.4 Steps involved grounded theory algorithm

5.4.1 Formulation of research objectives. Objectives of this part of the study are as follows.

(1) To find the most important factors that contribute to the efficiency of a cyber-security organization, which is referred as internal efficiency.

(2) To find the most important factors of the business that can be affected by the efficiency of a cyber-security organization which is referred as external effectiveness.

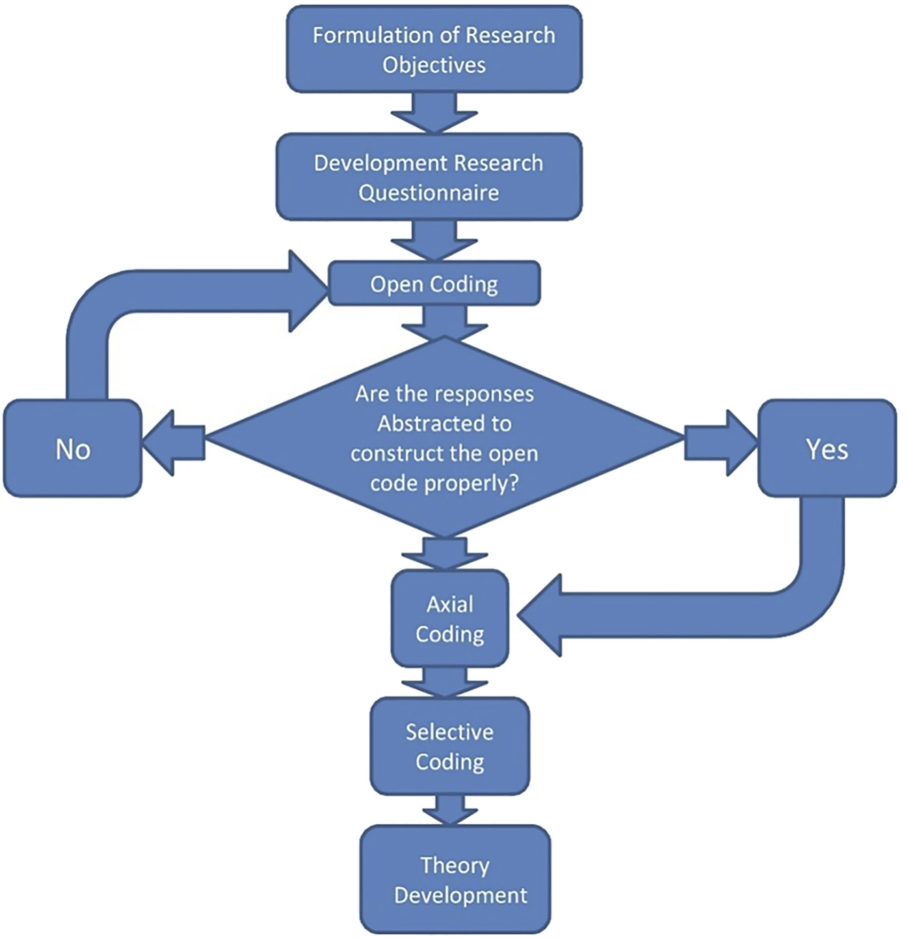

Figure 3.
Grounded theory algorithm

5.4.2 Development of research questions (RQ). For each objective three questions were designed which were used in the focused group discussion.

Objective 1 – To find the most important factors that contributes to internal efficiency of a cyber-security organization.

RQ1. What are the areas you feel that are especially important to sustain a strong cyber security posture in an organization?

RQ2. How do you measure the performance of cyber security in an organization?

RQ3. What are the important areas that affect the performance of cyber security in an organization?

Objective 2 – To find the most important factors of the business that can be affected by the efficiency of a cyber security organization.

RQ1. How do you determine the ROI on cyber security?

RQ2. What is the expectation of business from cyber security?

RQ3. What are the business parameters that can be affected by cyber security performance?

5.4.3 Sample selection. For this purpose, fifty professionals from five different business sectors and six various positions namely, oil and gas, telecom, banking and finance, retail, information technology and information technology enabled services (IT/ITES) were selected.

The positions held by the people at the time of discussion are: "Chief Information Security Officer (CISO")", "Chief Information Officer (CIO)", "Chief Technology Officer (CTO)", "Chief Finance Officer (CFO)", subject matter expert (SME).

All these senior professionals were invited to an eight hours workshop for discussion; and were explained on the objective of this research. This was followed by three rounds of discussion of almost 2 h duration with the focused group.

5.4.4 Data analysis techniques. We have used the traditional abstraction and coding techniques of grounded theory to derive theory from the data.

Grounded theory coding is a kind of content analysis to find and conceptualize the core issues from within the huge pile of the data. Throughout the analysis of an interview, for example, the researcher will become conscious that the interviewee is using words and phrases that highlight an issue of importance or interest to the research. This is noted and described in a short phrase. This issue may be mentioned again in the same or similar words and is again noted (Moghaddam, 2006).

Three levels of abstractions of the discussions among the focused group were done using open code, axial code and finally selective code to derive the theory, i.e. factors of internal efficiency and factors of external effectiveness of cyber security.

5.4.4.1 Open coding. Open coding in grounded theory method is the analytic process by which concepts (codes) to the observed data and phenomenon are attached during qualitative data analysis. It is one of the "procedures" for working with text as characterized by Strauss (1987) and Corbin and Strauss (1990). Open coding aims at developing substantial codes describing, naming, or classifying the phenomenon under consideration. Open coding is achieved by segmenting data into meaningful expressions and describing them in single word to short sequence of words. Open codes have scopes for further abstractions to derive axial and selective codes.

The open codes derived above were then further abstracted to find the axial code and finally the selective code.

5.4.4.2 Axial coding. This is the second phase of ground theory analysis. The word "axial" used by Strauss and Corbin (1998) is intended to put an axis through data. This axis connects identified categories in open coding. Axial coding puts categories back together to explore theoretical possibilities. So, axial coding identifies causal relationships, context, intervening conditions to interconnect data. So, the outcome of axial coding is an approach toward the central phenomenon of the data.

5.4.4.3 Selective coding. This is the third stage of grounded theory analysis. In this phase, the researcher selects one central aspect of data as a core category or final category and put his or her concentration on it. The aim of selective coding is to integrate and pull together developing analysis. So, a core category will be developed as an emergent concept. This stage displays those categories where more data are essential, which denote more theoretical sampling. This stage is also called systematic densification and saturation of the theory. (Onwuegbuzie *et al.*, 2009).

Formation of selective coding is based on axial coding. The framework of data analysis represents that selective coding is the last stage of qualitative data analysis.

5.4.5 Data analysis. Each question against each objective was discussed among the participants. The discussion was then abstracted to arrive at open code, axial code and finally the selective code.

While a sample of the analysis in deriving at the selective code for both objective 1 and 2 are mentioned in the Table 2, the entire analysis for each objective and against each question in Annexure 1.

Finally, from the above exercise of GTM the factors of internal efficiency and external effectiveness of cyber security are derived as below in Table 3.

6. Phase 2

6.1 Objective – developing model to identify the impact of internal efficiency factors on the external effectiveness of cyber security

After having constructed the factors of internal efficiency and external effectiveness, there is now scope to develop models to identify the impact of internal efficiency factors on the external effectiveness of cyber security. For this research paper, the following objectives are addressed.

(1) To identify the most and least preferred parameters lead to internal efficiency of cyber security organization.

(2) To identify the most and least preferred parameters of internal efficiency with respect to all the parameters external effectiveness.

6.2 Research design

In this study descriptive research design, and survey method is used. Accordingly, the questionnaire is developed and administered with designated sample/respondents.

Abstract of participant's expressions	Open code	Axial code	Selective code
Management intent for a strong cyber security posture, involvement of business stakeholders, regular top management reporting, strong policy and procedures; audit, assurance and compliance management Timely patching Well configured firewall CIP Incident response Latest tool and technologies Governance Patch management Roles and responsibilities, segregation of duties, management oversight; dashboard, Reporting Lack of Skill Skill	Strong governance Mechanism, Governance Mechanism, Security budget, CIP, metrics; maturity model	Cyber security Governance	Internal efficiency
Directly proportional to security breaches, breach will result into business disruption and then loss. Already happened in many companies. No business Interruption due to cyber-attack. No business loss. No down time. Loss of IPR will affect the competitiveness. Strong security for protection of IPR	No business interruption assurance to Business regarding CIA (confidentiality, integrity, and availability) of information business continuity no business disruption	Business continuity	External efficiency

Table 2. Abstraction of open code – axial code – selective code – sample analysis

Table 3.
Factors of internal efficiency and external effectiveness

Factors of internal efficiency (independent variable)	External effectiveness (dependent variable)
Cyber security governance	Business continuity
Cyber risk management	Regulatory and legal compliance
Vulnerability management	Preventing data and IPR loss
Compromise management	Facilitate digital transformation
Identity and access management	Cyber security awareness
Proactive monitoring of threat and vulnerability	Brand value
End user awareness	Customer acquisition
Legal and regulatory compliance	Profit
Appropriate and state of the art security technology solution	Revenue
Security architecture	Cyber intelligence
Cyber security skill	

6.3 Sampling framework

Purposive sampling was used to develop the sample of the current research. As per this sampling method sample members are selected based on their knowledge, skill and expertise regarding a research subject (Freedman, 2007). This is called non-probability sampling techniques. In the current study, the sample members are selected had based on their skill, expertise and relationship with the field cyber security and people from businesses who have expectation from cyber security.

The data collection method was online and by invitation only.

6.3.1 Structure of questionnaire. The questionnaire was divided into two parts, the first part collected data on internal efficiency and the second part on external effectiveness. Both the questionnaires were administered to the same set of respondents, together.

6.3.2 Internal consistency reliability. The internal reliability and consistency of the instrument is checked by using the "Cronbach's alpha" test. The results show that the internal consistency was high and scores for all the questionnaire was 0.98:

6.3.3 Selection of sample respondents. The data is collected from the 216 professionals, comprising of cyber security practitioners, SMEs, and business leaders from a cross section of industries such as BFSI (banking, financial services and insurance, retail, telecom, oil and gas, health and life science. IT/ITES sector).

6.4 Analysis of data and results

The questionnaires which were administered among the respondents were made in ordinal scale. Participants were asked to rate the parameters in the range of 1 to 5 on their impact on the internal efficiency/external effectiveness of the cyber security organization. (1 is least impact and 5 is the maximum impact). As the intervals in the ordinal scale are not equal, we have chosen "Rank order" to analyze the data and find out the preferred parameters. Rank orders represent ordinal scales and are frequently used in research (Kothari C R 2004) relating to qualitative phenomena.

There are many examples of ranking data in an array of academic disciplines, including education (Acuna-Soto *et al.*, 2021) psychology (Regenwetter and Rykhlevskaia, 2007), quality of life (Peiro-Palomino and Picazo-Tadeo, 2018), sociology (Harakawa and Iwahashi, 2021).

The breadth of these examples demonstrates the great utility of rankings as a tool for understanding human behavior and other scientific phenomena.

The data were analyzed with the following objectives in mind.

Objective 1 – To identify the most and least preferred parameters lead to internal efficiency of cyber security organization.

From the above Table 4, it is observed that the most preferred parameter of internal efficiency is legal and regulatory compliances followed by cyber risk management, cyber security skill, end user's awareness, security architecture, appropriate and state of the art technology solutions, compromise management, cyber security governance, identity and access management, proactive monitoring of threat and vulnerability and vulnerability management.

Objective 2 – To identify the most and least preferred parameters of internal efficiency with respect to all the parameters external effectiveness.

Objective 2.1 – To identify the most and least preferred parameters of internal efficiency with respect to business continuity.

From Table 5, it is observed that, cyber risk management is the most impacted parameter with respect to business continuity followed by vulnerability management, appropriate and state of the art technology solution end user awareness, cyber security governance, identity and access management, compromise management, legal and regulatory compliance, security architecture and proactive monitoring of threat and vulnerability with respect to business continuity.

Objective 2.2 – To identify the most and least preferred parameters of internal efficiency with respect to regulatory and legal Compliance.

From Table 6, it is observed that legal and regulatory compliance internal is the most impacted parameters to regulatory and legal compliance external followed by cyber security governance, cyber risk management, compromise management, proactive monitoring of

Parameters of internal efficiency	1	2	3	4	5	Rank order
Cyber security governance	0	0	14	102	107	985
Cyber risk management	0	0	5	90	128	1,015
Vulnerability management	0	0	11	29	133	814
Compromise management	2	0	19	77	125	992
Identity and access management	1	0	19	103	100	970
Proactive monitoring of threat and vulnerability	0	0	11	35	147	908
End user awareness	0	0	26	59	138	1,004
Legal and regulatory compliance	0	0	18	59	146	1,020
Appropriate and state of the art technology solution	4	0	15	76	128	993
Security architecture	2	1	10	88	122	996
Cyber security skill	0	0	14	73	136	1,014

Table 4. Most and least preferred parameters lead to internal efficiency of cyber security organization

Business continuity with all the parameters of internal efficiency						
Factors	1	2	3	4	5	Rank order
Business continuity_cyber security governance	0	0	48	128	40	856
Business continuity_cyber risk management	0	0	38	89	89	915
Business continuity_vulnerability management	0	3	45	110	58	871
Business continuity_compromise management	0	7	71	100	38	817
Business continuity_identity and access management	0	7	59	96	54	845
Business continuity_proactive monitoring of threat and vulnerability	9	37	55	84	31	739
Business continuity_end user awareness	4	12	52	62	86	862
Business continuity_legal and regulatory compliance	4	9	62	103	38	810
Business continuity_appropriate and state of the art technology solution	4	0	42	113	57	867
Business continuity_security architecture	0	33	63	82	38	773

Table 5. Business continuity with all the parameters of internal efficiency

Table 6.
"Regulatory and legal compliance" with all the parameter of internal efficiency

Factors	1	2	3	4	5	Rank order
Regulatory and legal compliance_cyber security governance	0	0	46	114	56	874
Regulatory and legal compliance_cyber risk management	0	9	45	90	72	873
Regulatory and legal compliance_vulnerability management	0	7	81	88	40	809
Regulatory and legal compliance_compromise management	4	8	42	96	66	860
Regulatory and legal compliance_identity and access management	4	28	76	72	38	766
Regulatory and legal compliance_proactive monitoring of threat and vulnerability	4	8	63	104	37	810
Regulatory and legal compliance_end user awareness	13	27	47	77	52	776
Regulatory and legal compliance external_legal and regulatory compliance internal	7	0	54	34	121	910
Regulatory and legal compliance_appropriate and state of the art technology solution	17	20	49	93	37	761
Regulatory and legal compliance_security architecture	4	15	58	112	27	791
Regulatory and legal compliance_cyber security skill	6	34	78	57	41	741

threat and vulnerability, vulnerability management, security architecture, end user awareness, identity and access management, appropriate and state of the art technology solution and cyber security skill.

Objective 2.3 – To identify the most and least preferred parameters of internal efficiency with respect to preventing data and IPR Loss.

From Table 7, it is observed that end user awareness and cyber risk management is most impacted parameters on preventing data and IPR loss followed by proactive monitoring of threat and vulnerability, vulnerability management, identity and access management, compromise management, security architecture, appropriate and state of the art technology solution, cyber security governance, legal and regulatory compliance and cyber security skill.

Objective 2.4 – To identify the most and least preferred parameters of internal efficiency with respect to facilitate digital transformation.

From Table 8, it is observed that cyber security skill is most impacted parameters on facilitate digital transformation followed by cyber risk management, identity and access management, security architecture, cyber security governance, appropriate and state of the

Table 7.
"Preventing data and IPR loss" with all the parameters of internal efficiency

Preventing data and IPR loss with all the parameters of internal efficiency						
Factors	1	2	3	4	5	Rank order
Preventing data and IPR loss_cyber security governance	0	15	60	122	19	793
Preventing data and IPR loss_cyber risk management	0	0	47	97	72	889
Preventing data and IPR loss_vulnerability management	0	7	51	101	57	856
Preventing data and IPR loss_compromise management	4	4	75	60	73	842
Preventing data and IPR loss_identity and access management	4	0	53	112	47	846
Preventing data and IPR loss_proactive monitoring of threat and vulnerability	0	0	47	105	64	881
Preventing data and IPR loss_end user awareness	0	9	43	78	86	889
Preventing data and IPR loss_legal and regulatory compliance	13	32	54	62	55	762
Preventing data and IPR loss_appropriate and state of the art technology solution	4	9	68	105	30	796
Preventing data and IPR loss_security architecture	4	4	70	98	40	814
Preventing data and IPR loss_cyber security skill	18	15	74	69	40	746

Facilitate digital transformation with all the parameters of internal efficiency						
Factors	1	2	3	4	5	Rank order
Facilitate digital transformation_cyber security governance	0	3	40	121	52	870
Facilitate digital transformation_cyber risk management	0	11	46	68	91	887
Facilitate digital transformation_vulnerability management	0	7	68	86	55	837
Facilitate digital transformation_compromise management	0	24	85	95	12	743
Facilitate digital transformation_identity and access management	0	7	45	89	75	880
Facilitate digital transformation_proactive monitoring of threat and vulnerability	0	7	56	103	50	844
Facilitate digital transformation_end user awareness	0	20	44	86	66	846
Facilitate digital transformation_legal and regulatory compliance	0	14	61	72	69	844
Facilitate digital transformation_appropriate and state of the art technology solution	0	11	43	111	51	850
Facilitate digital transformation_security architecture	0	7	58	90	61	853
Facilitate digital transformation_cyber security skill	0	7	36	75	98	912

Table 8. "Facilitate digital transformation" with all the parameters of Internal efficiency

art technology solution, legal and regulatory compliance, end user awareness, proactive monitoring of threat and vulnerability, vulnerability management and compromise management.

Objective 2.5 – To identify the most and least preferred parameters of internal efficiency with respect to cyber security awareness.

From Table 9, it is observed that end user awareness is most impacted parameters on cyber security awareness followed by cyber security governance, cyber security skill, security architecture, identity and access management, cyber risk management, proactive monitoring of threat and vulnerability, vulnerability management, legal and regulatory compliance, appropriate and state of the art technology solution and compromise management.

Objective 2.6 – To identify the most and least preferred parameters of internal efficiency with respect to brand value.

From Table 10, it is observed that, legal and regulatory compliance is the most preferred parameters with respect to brand value followed by compromise management, vulnerability

Cyber security awareness with all the parameters of internal efficiency						
Factors	1	2	3	4	5	Rank order
Cyber security awareness_cyber security governance internal	0	3	38	92	83	903
Cyber security awareness_cyber risk management	6	35	56	64	55	775
Cyber security awareness_vulnerability management	16	35	36	74	55	765
Cyber security awareness_compromise management	25	29	75	66	21	677
Cyber security awareness_identity and access management	4	6	82	93	31	789
Cybe rsecurity awareness_proactive monitoring of threat and vulnerability	4	39	40	93	40	774
Cyber security awareness_end user awareness	0	0	34	65	117	947
Cyber security awareness_legal and regulatory compliance	3	48	50	68	47	756
Cyber security awareness_appropriate and state of the art technology solution	21	32	52	81	30	715
Cyber security awareness_security architecture	0	29	70	60	57	793
Cyber security awareness_cyber security skill	0	7	49	91	69	870

Table 9. "Cyber security awareness" with all the parameters of internal efficiency

Table 10.
Brand value with all the parameters of internal efficiency

Brand value with all the parameters of internal efficiency Factors	1	2	3	4	5	Rank order
Brand value_cyber security governance internal	8	2	50	109	47	833
Brand value_cyber risk management	8	8	40	87	73	857
Brand value_vulnerability management	8	2	37	88	81	880
Brand value_compromise management	8	2	41	57	108	903
Brand value_identity and access management	8	9	100	75	24	746
Brand value_proactive monitoring of threat and vulnerability	0	10	35	108	63	872
Brand value_end user awareness	8	37	67	39	65	764
Brand value_legal and regulatory compliance	0	13	32	69	102	908
Brand value_appropriate and state of the art technology solution	4	19	71	73	49	792
Brand value_security architecture	4	12	64	113	23	787
Brand value_cyber security skill	8	29	63	67	49	768

management, proactive monitoring of threat and vulnerability, cyber risk management, cyber security governance internal, appropriate and state of the art technology solution, security architecture, cyber security skill, end user awareness and identity and access management.

Objective 2.7 – To identify the most and least preferred parameters of internal efficiency with respect to Customer acquisition.

From Table 11, it is observed that, end user awareness is the most preferred parameters with respect to customer acquisition followed by cyber risk management, security architecture, vulnerability management, cyber security governance internal, identity and access management, legal and regulatory compliance, compromise management, cyber security skill and proactive monitoring of threat and vulnerability.

Objective 2.8 – To identify the most and least preferred parameters of internal efficiency with respect to profit.

From Table 12, it is observed that legal and regulatory compliance is the most preferred with respect to profit followed by compromise management, proactive monitoring of threat and vulnerability, cyber risk management, cyber security governance internal, vulnerability management, appropriate and state of the art technology solution, security architecture, cyber security skill and end user awareness.

Table 11.
"Customer acquisition" with all the parameters of Internal efficiency

Customer acquisition with all the parameters of internal efficiency Factors	1	2	3	4	5	Rank order
Customer acquisition_cyber security governance internal	6	13	44	118	35	811
Customer acquisition_cyber risk management	6	4	60	102	44	822
Customer acquisition_vulnerability management	10	8	50	105	43	811
Customer acquisition_compromise management	7	18	80	68	43	770
Customer acquisition_identity and access management	10	4	59	108	35	802
Customer acquisition_proactive monitoring of threat and vulnerability	17	30	71	50	48	730
Customer acquisition_end user awareness	6	3	47	68	92	885
Customer acquisition_legal and regulatory compliance	13	29	45	71	58	780
Customer acquisition_appropriate and state of the art technology solution	10	14	47	90	55	814
Customer acquisition_security architecture	10	14	47	90	55	814
Customer acquisition_cyber security skill	16	24	74	53	49	743

Profit with all the parameters of internal efficiency Factors	1	2	3	4	5	Rank order
Profit_cyber security governance internal	6	22	54	101	33	781
Profit_cyber risk management	6	13	65	84	48	803
Profit_vulnerability management	6	14	91	56	49	776
Profit_compromise management	6	13	49	105	43	814
Profit_identity and access management	14	25	65	68	44	751
Profit_proactive monitoring of threat and vulnerability	10	16	39	101	50	813
Profit_end user awareness	31	27	44	61	53	726
Profit_legal and regulatory compliance	10	9	46	76	75	845
Profit_appropriate and state of the art technology solution	11	29	65	60	51	759
Profit_security architecture	10	30	67	71	38	745
Profit_cyber security skill	23	22	46	85	40	745

Table 12.
"Profit" with all the parameters of internal efficiency

Objective 2.9 – To identify the most and least preferred parameters of internal efficiency with respect to security architecture.

From Table 13, it is observed that business continuity is the most preferred with respect to security architecture followed by preventing data and IPR loss; facilitate digital transformation, legal and regulatory compliance, cyber intelligent, brand value, customer acquisition, profit, revenue and cyber security awareness.

Objective 2.10 – To identify the most and least preferred parameters of internal efficiency with respect to revenue.

From Table 14, it is observed that legal and regulatory compliance is the most preferred with respect to revenue followed by cyber risk management, vulnerability management, compromise management, cyber security governance internal, proactive monitoring of threat and vulnerability, security architecture, identity and access management, appropriate and state of the art technology solution, cyber security skill and end user awareness.

Objective 2.11 – To identify the most and least preferred parameters of internal efficiency with respect to cyber intelligence.

From Table 15, it is observed that preventing data and IPR loss is the most preferred with respect to cyber intelligence followed by cyber security awareness, business continuity, revenue, cyber security governance internal, regulatory and legal compliance, cyber intelligence, profit, customer acquisition, facilitate digital transformation and brand value.

Security architecture with all the parameters of internal efficiency Factors	1	2	3	4	5	Rank order
Security architecture_business continuity	1	15	35	81	91	915
Security architecture_regulatory and legal compliance	14	44	58	98	9	713
Security architecture_preventing data and IPR loss	0	0	177	28	18	733
Security architecture_facilitate digital transformation	0	1	183	26	13	720
Security architecture_cybersecurity awareness	13	12	187	10	1	643
Security architecture_brand value	1	10	187	25	0	682
Security architecture_customer acquisition	2	12	188	20	1	675
Security architecture_profit	7	12	191	0	13	669
Security architecture_revenue	8	11	187	16	1	660
Security architecture_cyber intelligence	0	3	184	28	8	710

Table 13.
"Security architecture" with all the parameters of internal efficiency

Table 14.
"Revenue" with all the parameters of internal efficiency

Revenue with all the parameters of internal efficiency Factors	1	2	3	4	5	Rank order
Revenue_cyber security governance internal	6	27	32	126	25	785
Revenue_cyber risk management	10	12	68	69	57	799
Revenue_vulnerability management	6	15	69	82	44	791
Revenue_compromise management	6	17	54	108	31	789
Revenue_identity and access management	10	23	55	102	26	759
Revenue_proactive monitoring of threat and vulnerability	2	17	69	111	17	772
Revenue_end user awareness	30	26	47	76	37	712
Revenue_legal and regulatory compliance	10	12	28	119	47	829
Revenue_appropriate and state of the art technology solution	10	26	53	102	25	754
Revenue_security architecture	6	32	64	63	51	769
Revenue_cyber security skill	14	36	54	89	23	719

Table 15.
"Cyber intelligence" with all the parameters of internal efficiency

Cyber intelligence with all the parameters of internal efficiency Factors	1	2	3	4	5	Rank order
Cyber intelligence_cyber security governance internal	0	6	43	140	27	836
Cyber intelligence_business continuity	0	3	54	93	66	870
Cyber intelligence_regulatory and legal compliance	0	0	73	99	44	835
Cyber intelligence_preventing data and IPR loss	0	3	24	77	112	946
Cyber intelligence_facilitate digital transformation	0	26	98	67	25	739
Cyber intelligence_cybersecurity awareness	0	4	32	113	67	891
Cyber intelligence_brand value	14	34	74	45	49	729
Cyber intelligence_customer acquisition	10	26	64	71	45	763
Cyber intelligence_profit	0	21	67	92	36	791
Cyber intelligence_revenue	0	6	62	96	52	842
Cyber intelligence_cyber intelligence	0	16	56	91	53	829

7. Discussion and major contribution to research literature

Consequent upon rapid digital transformation initiatives by corporations all over the globe, the attack surface has also increased manifold and cyber security risk is emerging as one of the prominent business risks. Performance evaluation of cyber security also has gained importance. From the literature review, it was evident that most of the research on cyber security performance are centered around security metrics, maturity, etc. Essentially, all these are helpful for evaluating the efficiency of a cyber security organization but what matters is how these factors of efficiency affect the business, i.e. external effectiveness, more importantly the integration. Thus, the first step to do further research on this is to derive the factors of internal efficiency and external effectiveness. Therefore, our effort in deriving these factors of efficiency and effectiveness is an innovative contribution and has multiple managerial and future research implications. The authors have further taken this research forward in developing model to identify the impact of internal efficiency factors on the external effectiveness of cyber security.

During literature study there is no evidence of research in the area of application of grounded theory approach in cyber security. Concrete and objective research on factors of internal efficiency and external effectiveness are also not found in the contemporary literature. This was a motivation for us, to use grounded theory and develop an algorithm to derive these factors. This is one of the pioneering, significant and unique research contributions. As per the literature review no researchers have ever tried to use this methodology for the stated purpose and cyber security domain in general.

The grounded theory algorithm developed by us can be used as a tool by future researchers to derive data/theory by using qualitative research methodology. The factors of internal

efficiency and external effectiveness derived by us has tremendous scope for further research in doing various impact analysis and correlation among factors of internal efficiency (independent variable) and external effectiveness (dependent variable). Practitioners at the strategic level should focus on integrating internal efficiency and external effectiveness. Information security executives should take a close look at their policy statements, metrics/goals, resource allocation, training, management review processes, etc. and begin to integrate them. Integrating systems will encourage cross-functional collaboration. Lack of integration will cause confusion by employees, who struggle to align their tactical priorities with the company's strategic objectives.

8. Concluding remark

The objective of the research is to contribute to the body of knowledge of cyber security governance and extend threads for the future researchers and practitioners in the area of cyber security. Construction of factors of internal efficiency and external effectiveness of cyber security and developing impact models are major contributions to the body of knowledge. Some of the interesting findings of this research which have significance for further research and also implications to the practitioners are as below.

The most preferred parameter of internal efficiency is legal and regulatory compliances followed by cyber risk management. Cyber risk management is the most impacted parameter with respect to business continuity followed by vulnerability management. Cyber security skill is found to be the most impacted parameters on facilitate digital transformation followed by cyber risk management. End user awareness is found to be the most impacted parameters on cyber security governance followed by cyber security skill. Legal and regulatory compliance is the most impacted parameters with respect to brand value followed by compromise management. End user awareness is the most impacted parameters with respect to customer acquisition followed by cyber risk management. Legal and regulatory compliance is again the most impacted parameter with respect to profit followed by compromise management. Business continuity is the most impacted parameter with respect to security architecture followed by preventing data and IPR loss. Legal and regulatory compliance is again the most impacted parameter with respect to revenue followed by cyber risk management and preventing data and IPR loss is the most impacted parameter with respect to cyber intelligence followed by cyber security awareness.

The sample size for both constructing the factors of internal efficiency, external effectiveness and developing the impact models although adequate but it contains only respondent from India. A global sample could have made a difference but considering the growth of IT and its application in business in India, we do not expect a much variation in the result.

The factors of internal efficiency and external effectiveness constructed by using grounded theory cannot remain constant in the long run, because of dynamism of the domain itself.

Over and above this, there are inherent limitations of the tools like grounded theory, used in the research. Few important limitations of GTM are as below.

(1) In grounded theory, it is comparatively difficult to maintain and demonstrate the rigors of research discipline. The sheer volume of data makes the analysis and interpretation complex, and lengthy time consuming. The researchers' presence during data gathering, which is often unavoidable and desirable too in qualitative research, may affect the subjects' responses.

(2) The subjectivity of the data leads to difficulties in establishing reliability and validity of approaches and information. It is difficult to detect or to prevent researcher-induced bias.

However, the choice of GTM is our conscious and judicious decision as sufficient data in the research literature were found on factors of internal efficiency and external effectiveness of cyber security. We were indeed very conscious about these short comings during our data

collection and cross-checked the emerging concepts against participants' meanings, asking experts if the theory "fit" their experiences in the second phase of our research while developing models/impact factors by using these variables.

In this research an impact model is formulated on the effect of factors of internal efficiency with the factor of external effectiveness. This analysis can be used by the future researchers for the following purposes.

(1) The results of the analysis have implications for further research in validation and developing model for industry segment and also on a cross industry comparison.

(2) Researchers also can-do various correlation among the factors of internal efficiency and External effectiveness to infer different dimensions.

References

Ababneh, H., Shrafat, F. and Zeglat, D. (2017), "Approaching information system evaluation methodology and techniques: a comprehensive review", *International Journal of Business Information Systems*, Vol. 24 No. 1, pp. 1-30.

Abu-Musa, A. (2010), "Information security governance in Saudi organizations: an empirical study", *Information Management and Computer Security*, Vol. 18 No. 4, pp. 226-276, doi: 10.1108/09685221011079180.

Acuña-Soto, C., Liern, V. and Pérez-Gladish, B. (2021), "Normalization in TOPSIS-based approaches with data of different nature: application to the ranking of mathematical videos", *Annals of Operations Research*, Vol. 296 No. 1, pp. 541-569.

Alavi, R., Islam, S. and Mouratidis, H. (2016), "An information security risk-driven investment model for analysing human factors", *Information and Computer Security*, Vol. 24 No. 2, pp. 205-227, doi: 10.1108/ICS-01-2016-0006.

Barabanov, R., Kowalski, S. and Yngström, L. (2011), "Information security metrics: state of the art", DSV Report series, pp. 11-007.

Bayuk, J. and Mostashari, A. (2013), "Measuring systems security", *Systems Engineering*, Vol. 16, doi: 10.1002/sys.21211.

Becker, J., Knackstedt, R. and Poppelbu, J. (2009), "Developing maturity models for IT management-A procedure model and its application", *Business and Information Systems Engineering (BISE)*, Vol. 1 No. 3, pp. 213-222.

Benbasat, I., Dexter, A.S., Drury, D.H. and Goldstein, R.C. (1984), "A critique of the stage hypothesis: theory and empirical evidence", *Communications of the ACM*, Vol. 27 No. 5, pp. 476-485.

Birks, D.F., Fernandez, W., Levina, N. and Nasirin, S. (2013), "Grounded theory method in information systems research: its nature, diversity and opportunities", *European Journal of Information Systems*, Vol. 22 No. 1, pp. 1-8.

Black, P.E., Scarfone, K. and Souppaya, M. (2008), "Cyber security metrics and measures", *Wiley Handbook of Science and Technology for Homeland Security*, pp. 1-15.

Boyer, W. and McQueen, M. (2007), "Ideal based cyber security technical metrics for control systems", *International Workshop on Critical Information Infrastructures Security*, Springer, Berlin, Heidelberg, pp. 246-260.

C2M2 (2014), *Cybersecurity Capability Maturity Model*, Version 1.1, available at: https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf (accessed 10 December 2017).

Chaula, J.A., Yngström, L. and Kowalski, S. (2005), *A Framework for Evaluation of Information Systems Security*, ISSA, pp. 1-11.

Chew, E., Swanson, M.M., Stine, K.M., Bartol, N., Brown, A. and Robinson, W. (2008), "Performance measurement guide for information security", No. Special Publication (NIST SP)-800-55 Rev 1.

Corbin, J.M. and Strauss, A. (1990), "Grounded theory research: procedures, canons, and evaluative criteria", *Qualitative Sociology*, Vol. 13 No. 1, pp. 3-21.

De Bruin, T., Freeze, R., Kaulkarni, U. and Rosemann, M. (2005), "Understanding the main phases of developing a maturity assessment model", *ACIS 2005 Proceedings*, p. 109, available at: https://aisel.aisnet.org/acis2005/109

Dettmer, H.W. (2007), *The Logical Thinking Process: A Systems Approach to Complex Problem Solving*, ISBN 13: 9780873897235.

Diesch, R., Pfaff, M. and Krcmar, H. (2018), "Prerequisite to measure information security", *Information Management and Computer Security*, Vol. 99 No. 7, p. 7.

Dogaheh, M.A. (2010), "Introducing a framework for security measurements", *2010 IEEE International Conference on Information Theory and Information Security*, IEEE, pp. 638-641.

Dube, D.P. and Mohanty, R.P. (2020), "Towards development of a cyber security capability maturity model", *International Journal Business Information Systems*. doi: 10.1504/IJBIS.2020.10014790.

Freedman, D.A. (2007), "Statistical models for causation", *The SAGE Handbook of Social Science Methodology*, pp. 127-146.

Gartner (2019), "Gartner says global IT spending to grow 3.7% in 2020", available at: https://www.gartner.com/en/newsroom/press-releases/2019-10-23- gartner-says-global-it-spending-to-grow-3point7-percent-in-2020

Glaser, B.G. and Strauss, A.L. (1967), "The discovery of grounded theory", *Strategies for Qualitative Research*, Aldine, Chicago.

Harakawa, R. and Iwahashi, M. (2021), "Ranking of importance measures of tweet communities: application to keyword extraction from COVID-19 tweets in Japan", *IEEE Transactions on Computational Social Systems*, Vol. 8 No. 4, pp. 1030-1041.

Holm, H. and Afridi, K.K. (2015), "An expert-based investigation of the common vulnerability scoring system", *Computers and Security*, Vol. 53, pp. 18-30.

Hubálovský, Š. and Milková, E. (2010), "Modeling of a real situation as a method of the algorithmic thinking development", *In Advanced Educational Technologies, Proceedings of 6th WSEAS/IASME International Conference on Educational Technologies (EDUTE'10)*, WSEAS Press, Kantoui, Sousse, Tunisia, pp. 68-72.

Igor Bernik Kaja Prislan (2016), "Measuring information security performance with 10 by 10 model for holistic state evaluation", doi: 10.1371/journal.pone.0163050.

ISM3 Consortium (2007), *ISM3-Information Security Management Maturity Model, ISM3 Consortium*, Spain, available at: https://ism3.com/ism3vsiso27001.php

ISO/IEC (2005), available at: https://www.iso.org/standard/39883.html

Jafari, S., Mtenzi, F., Fitzpatrick, R. and O'shea, B. (2010), "Security metrics for e-healthcare information systems: a domain specific metrics approach", *International Journal of Digital Society*, Vol. 1 No. 4, pp. 238-245.

Kanungo, S., Jain, V. and Forman, E.H. (2011), "Maximizing resource allocation effectiveness for IT security investments", *International Journal of Business Information Systems*, Vol. 7 No. 2, pp. 166-180.

Karokola, G., Kowalski, S. and Yngström, L. (2011), *Towards an Information Security Maturity Model for Secure E-Government Services: A Stakeholders View*, HAISA, pp. 58-73.

King, J.L. and Kraemer, K.L. (1984), "Evolution and organizational information systems: an assessment of Nolan's stage model", *Communications of the ACM*, Vol. 27 No. 5, pp. 466-475.

Kothari C R- Research Methodologies Methods and Techniques (2004), New Age Publishers.

Lehmann, H. (2010), "Grounded theory and information systems: are we missing the point?", *In 2010 43rd Hawaii International Conference on System Sciences*, IEEE, pp. 1-11.

Martin, P.Y. and Turner, B.A. (1986), "Grounded theory and organizational research", *The Journal of Applied Behavioral Science*, Vol. 22 No. 2, pp. 141-157.

Matavire, R. and Brown, I. (2013), "Profiling grounded theory approaches in information systems research", *European Journal of Information Systems*, Vol. 22 No. 1, pp. 119-129.

McCormack, K., Willems, J., van den Bergh, J., Deschoolmeester, D., Willaert, P., Stemberger, M.I., Skrinjar, R., Trkman, P., Ladeira, M.B., Valadares de Oliveira, M.P., Vuksic, V.B. and Vlahovic, N. (2009), "A global investigation of key turning points in business process maturity", *Business Process Management Journal*, Vol. 15 No. 5, pp. 792-815.

Mermigas, D., Patsakis, C. and Pirounias, S. (2013), "Quantification of information systems security with stochastic calculus", *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, ACM, p. 47.

Moghaddam, A. (2006), "Coding issues in grounded theory", *Issues in Educational Research*, Vol. 16 No. 1, pp. 52-66.

Ngwum, N. (2016), "Information security maturity model (ISMM)", available at: https://www.researchgate.net/publication/292607439_Information_Security_Maturity_Model_ISMM (accessed 10 November 2017).

Onwuegbuzie, A.J., Dickinson, W.B., Leech, N.L. and Zoran, A.G. (2009), "A qualitative framework for collecting and analyzing data in focus group research", *International Journal of Qualitative Methods*, Vol. 8 No. 3, pp. 1-21, doi: 10.1177/160940690900800301.

Peiró-Palomino, J. and Picazo-Tadeo, A.J. (2018), "OECD: one or many? Ranking countries with a composite well-being indicator", *Social Indicators Research*, Vol. 139 No. 3, pp. 847-869.

Pendleton, M., Garcia-Lebron, R., Cho, J. and Xu, S. (2016), "A survey on systems security metrics", *ACM Computing Surveys*, Vol. 49 No. 4, p. 62.

Pöppelbuß, J. and Röglinger, M. (2011), "What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management", *European Conference on Information Systems*, p. 28.

Purboyo, T., Rahardjo, B. and Kuspriyanto (2011), *Security Metrics: A Brief Survey*, doi: 10.1109/ICICI-BME.2011.6108598.

Radanliev, P., De Roure, D. and Burnap, P. (2021), "Epistemological equation for analysing uncontrollable states in complex systems: quantifying cyber risks from the internet of things", *Review of Socionetwork Strategies*, Vol. 15, pp. 381-411, doi: 10.1007/s12626-021-00086-5.

Rea-Guamán, A.M., San Feliu, T., Calvo-Manzano, J.A. and Sanchez-Garcia, I. (2017), "Comparative study of cybersecurity capability maturity models", pp. 100-113, doi: 10.1007/978-3-319-67383-7_8.

Regenwetter, M. and Rykhlevskaia, E. (2007), "A general concept of scoring rules: general definitions, statistical inference, and empirical illustrations", *Social Choice and Welfare*, Vol. 29 No. 2, pp. 211-228.

Rostyslav, B., Stewart, K. and Louise, Y. (2011), "Information security metrics: state of the art: state of the art".

Salh, M.F. (2011), "Information security maturity model", *International Journal of Computer Science and Security (IJCSS)*, Vol. 5 No. 3, p. 21.

Savola, R.M. (2009), "A security metrics taxonomization model for software-intensive systems", *Journal of Information Processing Systems*, Vol. 5 No. 4, pp. 197-206.

Savola, R. and Heinonen, P. (2011), "A visualization and modeling tool for security metrics and measurements management", *Information Security for South Africa*, No. 2011, pp. 1-8.

Seidel, S. and Urquhart, C. (2013), "On emergence and forcing in information systems grounded theory studies: the case of Strauss and Corbin", *Journal of Information Technology*, Vol. 28 No. 3, pp. 237-260.

Simonsson, M., Johnson, P. and Wijkström, H. (2007), "Model-based IT governance maturity assessment with CobiT", *Proceedings of the European Conference on Information Systems (ECIS)*, St.Gallen, Switzerland.

Simonsson, M., Pontus, J. and Mathias, E. (2010), "The effect of IT governance maturity on IT governance performance", *Information Systems Management*, Vol. 27 No. 1, pp. 10-24, doi: 10.1080/10580530903455106.

Sowa, S. and Gabriel, R. (2009), "Multidimensional management of information security – a metrics based approach merging business and information security topics", *Proceedings - International Conference on Availability, Reliability and Security*, ARES 2009, pp. 750-755, doi: 10.1109/ARES.2009.26.

Stevanović, B. (2011), "Maturity models in information security", *International Journal of Information and Communication Technology Research*, Vol. 1 No. 2.

Strauss, A.L. (1987), *Qualitative Analysis for Social Scientists*, Cambridge University Press, doi: 10.1017/CBO9780511557842.

Strauss, A. and Corbin, J. (1998), "Basics of qualitative research techniques".

Taghipour, A. (2014), "Adopting constructivist versus objectivist grounded theory in health care research: a review of the evidence", *Journal of Midwifery and Reproductive Health*, Vol. 2 No. 2, pp. 100-104.

Urquhart, C. and Fernandez, W. (2006), "Grounded theory method: the researcher as blank slate and other myths", *ICIS 2006 Proceedings*, p. 31.

Vaughn, R.B., Henning, R. and Siraj, A. (2003), "Information assurance measures and metrics-state of practice and proposed taxonomy", *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, IEEE, p. 10.

Watkins, L. and Hurley, J.S. (2016), "The next generation of scientific-based risk metrics: measuring cyber maturity", *International Journal of Cyber Warfare and Terrorism (IJCWT)*, Vol. 6 No. 3, pp. 43-52.

Weill, P. and Ross, J.W. (2004), *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business Press.

Wiesche, M., Jurisch, M.C., Yetton, P.W. and Krcmar, H. (2017), "Grounded theory methodology in information systems research", *MIS Quarterly*, Vol. 41 No. 3, pp. 685-701.

Zaini, M.K., Masrek, M.N., Johari, M.K., Sani, A. and Anwar, N. (2018), "Theoretical modeling of information security: organizational agility model based on integrated system theory and resource based view", *International Journal of Academic Research in Progressive Education and Development*, Vol. 7 No. 3.

Zalewski, J., Drager, S., McKeever, W. and Kornecki, A.J. (2014), "Measuring security: a challenge for the generation".

Zhao, W. and White, G. (2017), "An evolution roadmap for community cyber security information sharing maturity model", *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Further reading

Authors, available at: https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final

CMM (2014), *Cyber Security Capability Maturity Model (CMM) - V1.2, Global Cyber Security Capacity*, Centre University of Oxford, available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf (accessed 10 December 2017).

Peter, W. and Ross, J.W. (2004), *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results by Peter Weill and Jeanne W*, Harvard Business School Press Boston, Ross Boston, 1-59139-253-5.

World Economic Forum–Global Risk Report (2021), (weforum.org), available at: WEF_The_Global_Risks_Report_2021.pdf

(The Appendix follows overleaf)

Annexure 1

Analysis for each objective and against each question in arriving at open code, axial code and selective code

Objective 1 – Q1. What are the areas you feel that are very important to sustain a strong cyber security posture in an organization?

Open code	Properties	Abstract of participant's expressions
Strong governance mechanism	Management oversight, reporting, policy and procedures	Management intent for a strong cyber security posture, involvement of business stakeholders, regular top management reporting, strong policy and procedures; audit, assurance and compliance management Timely patching Well configured firewall CIP Incident response Latest tool and technologies Governance Patch management
Strong risk management practice	Part of overall enterprise risk management, risk based control implementation	Cyber security to be part of overall business risk management portfolio, cyber risk management practices to be in place, key risk and performance indicator. Risk management standard; vendor risk management, cyber insurance
Vulnerability management	Continuously looking at the material weaknesses of the system and applications	A strong vulnerability management program across the enterprise. Correlation of threat and vulnerability to find the material vulnerability, vulnerability management of all the information assets
Compromise management	Continuously looking at whether there is any stealth compromise in the enterprise	Regular and perpetual threat hunting to find slow and steady attacks and compromise
Business continuity	Information system resiliency	Recovery time objective, recovery point objective, regular business impact analysis
Secured network configuration	Network security and configuration management	Minimum base line security for all network components, secured network architecture, wireless security and access control
Identity and access management	Identification, authentication and authorization	Strong identification and authentication, authorization, federation and single sign on
System/end point security	Strong security Implementation in servers and endpoints	Anti-virus, anti-malware, endpoint detection and response (EDR), configuration management, patch management and minimum baseline security standard
Proactive monitoring	Continuous monitoring of threat, vulnerability and security posture	SIEM (security information and event management), 24/7 security operation center and security intelligence

Table A1.
Abstraction of open code – Objective 1 – Q1

(*continued*)

Open code	Properties	Abstract of participant's expressions
End user awareness	Cyber security awareness to all the stakeholders	Cyber security awareness is the key, insider threats, human firewall, awareness to all the stakeholders including the third-party service providers, end user awareness on Do's and Don'ts, data classification, awareness to vendors and workforce development for OT
Continuous improvement program	Maturity models	Operation management system for cyber security, set as-is and to-be state based on maturity models, and have projects to achieve the target state. Global benchmarking, continuous assessment and monitoring
Security solutions	Tools and techniques	Tools and techniques, state of the art technology solution. New generation security solutions
Security architecture	Security architecture	Proper architecture, cloud and big data security, security at the design stage
Cyber security skill	Hire and retain good cyber security professionals	Good cyber security professionals, cyber security skill linked with new generation threats, hire and retain good talent

Table A1.

Objective 1 – Q2. How do you measure the performance of cyber security in an organization?
In the same way here also, the authors have abstracted the participant's discussion to derive open code as per Table A2 below.

Open code	Properties	Example of participant's word
Maturity model	Continuous improvement program	CIP program. As is and to be analysis, strong OMS (operation management standard, benchmarked maturity model)
Metrics	Cyber security metrics	MTTR, MTTD, number of incidents reduced, phishing exercise
Compliance	Legal and regulatory compliance	Benchmarking, security policy violation. reduction of non-compliances
Cyber drill	Strong response mechanism	Cyber response, regular cyber-drill, red team exercise

Table A2.
Abstraction of open code – Objective 1 – Q2

Objective 1 – Q3. What are the important areas that affect the performance of cyber security in an organization?

Open code	Properties	Example of participant's word
Governance mechanism	Roles and responsibilities. management support, oversight	Roles and responsibilities, segregation of duties, management oversight; dashboard, reporting lack of skill Skill
Cyber defense	Orchestration, incident management	Orchestration; strong response mechanism; incident management
Security budget	Tools and techniques, budget, business support	Support from business Tools and techniques Budget
Cyber security skill	Cyber security skill	Lack of skill, training, re-skilling
Cyber security technology solutions	Tools and techniques	State of the art security solutions, preventing and detecting controls
Technology security architecture	Security architecture	Lack of proper security architecture, security is an after thought
Appropriate cyber security skill	Cyber security skill	Attrition, not able to hire and retain skills, training and re-skilling

Table A3.
Abstraction of open code – Objective 1 – Q3

Open code	Axial code	Selective code
Strong governance mechanism, governance mechanism, security budget, CIP, metrics; maturity model	Cyber security governance	Internal efficiency of cyber security organization
Strong risk management practice, business continuity	Cyber risk management	
Vulnerability management, secured network configuration, system/end point security	Vulnerability management	
Compromise management, cyber defense	Compromise management	
Identity and access management	Identity and access Management	
Proactive monitoring, cyber defense	Proactive monitoring of threat and vulnerability	
End user awareness	End user awareness	
Compliance	Legal and regulatory compliance	
Security solutions, cyber security technology solutions	Appropriate and state of the art security technology solution	
Security architecture, technology security architecture	Security architecture	
Cyber security skill, Appropriate cyber security skill	Cyber security skill	

Table A4.
Derivation of selective code from open code and axial code

The same exercise was also done for the following three questions for objective 2.

RQ1. How do you determine the ROI on cyber security?

RQ2. What is the expectation of business from cyber security?

RQ3. What are the business parameters that can be affected by cyber security performance?

Objective 2- Q1-How do you determine the ROI on cyber security?
The discussion with the focused group is abstracted below in Tables A5–A7.

Open code	Properties	Example of participant's word
Reduction of security breaches	Security breach mitigation	Directly proportional to security breaches, breach will result into business disruption and then loss. Already happened in many companies
Smooth and fast digital transformation	Adoption of newer technology to combat new generation threats and help digital transformation	Brake in the car. Business can run fast. Transformation becomes smooth. No cyber threats for digital transformation. Technology enablement of business processes will increase efficiency and hence the bottom line
Not quantifiable	Not quantifiable	ROI in security is a misnomer. No direct impact. Very difficult
No business disruption	Prevent business disruption due to cyber attack	Strong cyber security helps preventing business disruption due to cyber-attack. Directly related to bottom line
Better customer acquisition	Strong security helps customer acquisition	Strong security helps customer acquisition. Breaches negatively affect. Customer acquisition will positively affect bottom line
Better valuation	Brand differentiator	Strong security is a brand differentiator. Better brand better valuation
Prevent reputation loss	Security breaches will affect reputation	Security breaches will affect reputation. Reputation loss erodes valuation, customer acquisition. Non-compliance, lawsuits following security breaches affect the bottom-line

Table A5. Abstraction of open code – Objective 2 - Q1

Objective 2 – Q2. What is the expectation of business from cyber security?

Open code	Properties	Example of participant's word
No business interruption	Business interruption due to cyber attack	No business Interruption due to cyber-attack. No business loss. No down time
Have cyber intelligence	Proactive monitoring of threat	Preventing threat, proactive monitoring, threat prediction and proactive action and proactive intelligence
Ensure compliance	Compliances to laws and regulations	Compliance to all laws and regulation. Contractual compliance, no non-compliances
Preventing data and IPR loss	Data and IPR loss prevention	Prevent leakage of confidential Information and IPR. Data loss
Facilitate digital transformation	Support to new business initiatives using smart technology	Smart technology brings new threats; Good cyber security enables faster adoption. Security should not be the showstopper
Assurance to business regarding CIA (confidentiality, integrity and availability) of Information	Assurance to business regarding CIA of information	Ensure confidentiality, integrity and availability. Assurance to the management
All users should be made aware of requirements of cyber security	Cyber security awareness	Cyber security awareness should spread across all the users. Third party and contractors also should be to give cyber security awareness training. Internal threat very important

Table A6.
Abstraction of open code – Objective 2 – Q2

Objective 2 – Q3. What are the business parameters that can be affected by cyber security performance?

Open code	Properties	Example of participant words
Intellectual property rights (IPR)	Security of company patents and invention	Loss of IPR will affect the competitiveness. Strong security for protection of IPR
Corporate secrets	Security of company secret and confidential information	Protection of confidential information. Loss of company secrets will lead to business loss; data loss prevention
Reputation	Company good will and reputation are the greatest assets and needs to be protected	Cyber-attack leads to loss of confidence, loss of credibility
Compliance status: legal and regulatory	Legal and regulatory compliance	Legal compliance, regulatory compliance, contractual compliance. Noncompliance leads to serious complication. Company may be out of business
Brand value	Cyber security posture – a brand differentiators	Customer and stakeholder's confidence, strong security creates a brand value. Brand value generate profits
Profit	Cyber-attack leads to business disruption	Cyber-attack leads to business disruption, denial of services

(*continued*)

Table A7.
Abstraction of open code – Objective 2 – Q3

Open code	Properties	Example of participant words
Customer's acquisition	Cyber breaches erode customer's confidence	Cyber breaches erode customer's confidence. Customer centric companies like banks. Telecom, customer acquisition will be hugely affected
Privacy	Protection of personally identifiable information (PII) and SPDI (sensitive personal data or information)	Protection of privacy. Privacy breaches have broader legal and regulatory ramifications. Good security protects PII and SPDI
Opportunity	Opportunity loss due to cyber-attack and the consequent loss of sensitive information	Loss of sensitive data like business plan, strategy, IPR, etc. due to cyber-attack may lead to opportunity loss. May affect the bottom line too
Valuation	Cyber-attack erodes company valuation	Company valuation will be affected because of cyber-attack. Yahoo is the example
Revenue	Loss of revenue due to cyber breach	Cyber-attack leads to business interruption, loss of opportunity, loss of customers and hence loss of revenue
Production	Cyber-attack leads to production loss	Production will affect because of business interruption due to cyber attack
Awareness	Poor cyber security is directly related low level of awareness	Poor cyber security is directly related low level of awareness among stakeholders. Awareness is the key to success
Business continuity	Business continuity	Business is IT enabled. In case of disaster IT is required for business continuity. Availability is another requirement for information security. Business impact analysis

Table A7.

Derivation of selective code from open code and axial code

The open codes derived above were then further abstracted to find the axial code and finally the selective code. The results of this abstraction are shown in Table A8.

Table A8.
Open code, axial code and selective code – Objective 2

Open code	Axial code	Selective code
No business interruption	Business continuity	External efficiency
assurance to business regarding CIA (confidentiality, integrity and availability) of information		
business continuity		
no business disruption		
Compliance status legal and regulatory	Regulatory and legal compliance	
ensure compliance		
privacy		
Intellectual property rights (IPR)	Preventing data and IPR Loss	
corporate secrets		
preventing data and IPR loss		
Facilitate digital transformation	Facilitate digital transformation	
smooth and fast digital transformation		
All users should be made aware of requirements of cyber security	Cyber security awareness	
Awareness		
Reputation	Brand value	
Brand value		
Prevent reputation loss		
Valuation		
Better valuation		
Customer's acquisition	Customer acquisition	
Better customer acquisition		
Opportunity	Profit	
Profit		
Revenue	Revenue	
Production		
Have cyber intelligence	Cyber intelligence	
Reduction of security breaches		

Corresponding author
Durga Prasad Dube can be contacted at: dpdube@gmail.com