Scientific Research Publishing

Journal of Computer and Communications, 2026, 14(1), 66-86
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Relating Cyber Security Budget to Organizational Strategy: An Empirical Analysis

R. R. K. Sharma[1], Niraj K. Vishvakarma[2], Avirag Bajpai[3], Vimal Kumar[4,5], Shivam Sharma[1]

[1]Department of Management Studies, Indian Institute of Technology, Kanpur, India
[2]Indian Institute of Information Technology, Lucknow, India
[3]Larsen & Toubro Institute of Project Management, Vadodara, India
[4]Department of Information Management, Chaoyang University of Technology, Taichung
[5]R and D Institute of Science and Technology, Avadi, Chennai, India
Email: rrkiitk@gmail.com, nirajkumar.v@gmail.com, aviragbajpai@gmail.com, Vimaljss91@gmail.com, rrks@iitk.ac.in

How to cite this paper: Sharma, R.R.K., Vishvakarma, N.K., Bajpai, A., Kumar, V. and Sharma, S. (2026) Relating Cyber Security Budget to Organizational Strategy: An Empirical Analysis. *Journal of Computer and Communications*, **14**, 66-86.
https://doi.org/10.4236/jcc.2026.141005

Received: December 15, 2025
Accepted: January 17, 2026
Published: January 20, 2026

Abstract

Corporate data is highly valuable and firms deploy cyber security infrastructure to protect its valuable infrastructure. Information systems technology (IST) and cyber security infrastructure (CSI) literature is dominated by computer scientists and experts. It is well known that the environment drives the strategy of firm; and strategy of firm in turn drives the organizational structure and systems (including the Information Systems Technology (IST) used and the Cyber Security Infrastructure (CSI) deployed. In literature strategy of firm is related to Internet of Things (IoT) type, RFID and Business Process Engineering. On similar lines, in literature, the dimensions of IST flexibility are related to strategy of the firm. On similar lines we relate cyber security budget (CSB) and cyber security infrastructure (CSI) to strategy of the firm. Literature has identified two basic strategy types, that is, cost leadership or defenders (here firms mass produce to deliver products at least cost) and prospectors (differentiators) (who charge a premium for giving additional features in the product). It has been argued that in cost leaders most important departments are production and finance (marketing is low in importance as customers of the low income group strata of the society are willing to wait for the cheapest product) and hence these firms have internal orientation and are insulated from the market place; whereas in differentiators marketing and R&D are most important departments and here customer related data and data on product designs are to be most confidential, and these are spread out in the market place. Insulated factories do not need high CSB whereas when marketing is important CSB needs to be that much higher. When products are targeting the same customer and have similar features, etc., firms (differentia-

tors) go for plant within a plant (PWP). Hence CSI also tends to get modular and it reduces cost. Due to high obsolescense in the IST/CSI technology compatibility across different generations compatibility is a big issue. Differentiators tend to acquire modern IST and CSI and have compatibility issues and increased cost. If high rapidity is desired of CSI then costs are higher. Hence we give following six hypotheses: H1: highly modular CSI will tend to reduce costs; H2: highly compatible CSI will reduce costs; H3: High rapidity of CSI will increase the costs; H4: High modernity of CSI will tend to increase costs; H5: cost leaders will have less CSB and H6: Differentiators will tend to have higher CSB. Data from 76 firms gave full support to the above proposed hypotheses.

Keywords

Organizational Strategy, Cyber Security Budget, Modular and Compatible Cyber Security Infrastructure, Rapidity and Modernity of Cyber Security Infrastructure

1. Introduction and Background Literature

Today, cyber security is more than simply a technology issue; it is also a business enabler. It is well recognized that strategy drives the structure and systems of the organization [1]. Therefore, change your business model to include cyber security as part of your strategic planning process. Organizations that do this will be better prepared to deal with unplanned interruptions. In addition, the allocation of funds for cyber security should be a key priority for all businesses. According to current trends, many organizations allocate 10 percent of their IT expenditures to cyber security initiatives [2].

Creating greater public knowledge can help avoid a considerable number of attempted breaches. Structured training sessions are one of the most cost-effective kinds of training available. Employees that demonstrate superior cyber security knowledge and skills may be rewarded by their companies [3].

In computing, cyber security refers to a collection of methodologies, technologies, and procedures that are used to secure computer systems, networks, and data against cyber-attacks or unauthorized access. The primary purpose of cyber security is to protect all organizational assets from attacks both from the outside and from within the organization. According to estimates, companies are currently spending an additional 4.2 percent to as much as 20 percent of their total IT expenditure on maintenance and support. Generally speaking, a cyber security standard is a collection of rules that a company must follow to be granted authorization to do specific duties, such as accepting online payments or storing medical information. Among the other requirements outlined in the standards, a company's system must be up to date and free of vulnerabilities, and it must generate network reports regularly.

When it comes to business strategy, it is a pattern of organization settlement that defines and discloses a company's objectives, purposes, or goals and the primary policies and methods used to achieve these goals. Specifically, our whole study methodology is built on two widely acknowledged strategic typologies: cost leaders and Differentiators [4].

Cost leadership

Cost leadership is a business strategy that aims to provide customers with the lowest priced goods and services possible to maximize profits and gain a competitive edge. Improved economies of scale, production learning, unique input materials accessibility, and/or smart alliances with manufacturers, retailers, and/or customers can all help to reduce costs [3].

Differentiation

Differentiation is an organizational approach that aims to distinguish a good or service from identical products or services offered by competitors by making it stand out from the crowd. Differentiation is essential for effective marketing, strategic positioning, and long-term competitive advantage. However, when taken to extremes, the difference may be harmful because customers will not accept the validity of the effort or will perceive it as an unnecessary luxury if it is too serious [3].

An organization is a social unit made up of people who are organized and managed to accomplish a common purpose. Every firm has a structure in place that sets and governs employee interactions, as well as the tasks they accomplish and the roles, obligations, and rights they have to fulfill those activities. A centralized organization is defined by a pyramidal decision-making system in which decision making happens at the top. Employees at various levels of an organization can have some discretion in making business choices when working in a decentralized organizational structure. In this environment, there is room for unique thought processes and creativity, which may be used to benefit the corporation as a whole or even a specific goal.

Miles and snow *et al.* [5] have related organizational structure dimensions (standardization, specialization, centralization, formalization and complexity of work flow) to the strategy of the firm. Interested readers can go through that paper. Besides, it has been argued in business literature that strategy and structure drive the choice of systems (such as incentive systems, control systems, performance monitoring systems etc.) including the information systems. Thus there is enough theoretical basis to relate strategy and systems. In particular, Miles and Snow [5] showed that cost leaders have high standardization, specialization, centralization and formalization and low complexity of work flow; and that differentiators have low standardization, specialization, centralization and formalization and high complexity of work flow [5].

2. Research Gap

Cyber security is a top issue for nearly everyone in some shape or another in 21

century. Like many other essential business activities, maintaining a company's cyber security infrastructure usually needs a monetary investment and hence requires financial allocation. Cybersecurity is here to stay, and it's expanding at an incredibly rapid rate. Therefore, in the recent years, cyber security must be prioritized as a business and financial priority. To keep pace with the dynamic and ever-changing cyber threat environment, it is imperative that adequate resources be allocated to the infrastructure necessary to maintain cyber security. If current trends are to be believed, companies are spending 10% of their IT budgets on cyber security, on average.

It is our primary goal to link the amount of money spent on cyber security to the various forms of organizational strategy.

3. Theoretical Framework

Cyber security infrastructure (CSI) properties such as modularity, rapidity, modernity, and compatibility with the cyber security budget; and how the organizational strategy determines the cyberattacks withstanding capacity of a firm, which can be classified as either "Basic minimal" (Firm can withstand 85 percent of cyberattacks) or "Highly involved". Based on the above factors, the following hypothesis has been proposed.

3.1. Modularity

System development costs may be reduced by repeatedly using the same software and hardware components in Cyber Security Infrastructure (CSI), which is defined as the degree to which components, software, or modules can be reused in system development [6]. However, every new product will require a new set of algorithms to be developed, which will add to the overall cost. See the following link for a writeup on traditional vs modular IT infrastructure: https://ca.insight.com/en_CA/content-and-resources/2017/10172017-traditional-vs-modular-it-infrastructure.html; A writeup on modular cyber security infrastructure can be seen at: https://www.ciscopress.com/articles/article.asp?p=1626588&seqNum=3.

As a result, we may say:

($H_{1.a}$): Firms with highly modular Cyber Security Infrastructure (CSI) will have much less cyber security budget.

($H_{1.b}$): Firms with less modular Cyber Security Infrastructure (CSI) will have much more cyber security budget.

3.2. Compatibility

Several scholars have conducted a substantial study on compatibility, as seen from the available literature [7]. Compatible CSI systems share the same file formats. For systems to communicate and share data efficiently, they must be compatible. This means that different systems, components, or activities within systems must

function together seamlessly. A system is considered compatible if the results of processing in one system may be promptly and directly accessed by other organisations that use comparable but not identical software. Businesses with highly compatible Cyber Security Infrastructure (CSI) will thus have to pay less than organizations with less compatible Cyber Security Infrastructure (CSI). A writeup on compatible cyber security infrastructute can be found at: https://sprinto.com/blog/best-cybersecurity-tools/.

As a result, we may say:

(H2.a): Firms with highly compatible Cyber Security Infrastructure (CSI) will have much less cyber security budget.

(H2.b): Firms with less compatible Cyber Security Infrastructure (CSI) will have much more cyber security budget.

3.3. Rapidity

The capacity of a cyber security infrastructure to supply information when it is required is referred to as rapidity [7]. For rapidity to be achieved, it is necessary to standardize all CSI components and parts across the board. Key choices to be taken in manufacturing organizations include the strategic positioning of the product, as well as the precise timing of the product's debut based on a proper market orientation. To make these judgments, the organization's cyber security infrastructure (CSI) must respond swiftly to acquire the necessary information and make it available whenever it is needed. CSI characteristics such as speed can be related with the business/market environment circumstances, which can be either stable or dynamic, and can be considered a separate CSI feature.

We may conclude that in a dynamic environment, high rapidity is necessary, which necessitates a high cyber security budget; in a stable environment, less rapidity is required, necessitating a lower cyber security budget; and in a hybrid environment, both are required. For advantages/disadvantages of cybersecurity infrastructure look up the following link: https://webandcrafts.com/blog/advantages-and-disadvantages-of-cyber-security .

As a result, we get the following:

(H3.a): Firms with less rapid Cyber Security Infrastructure (CSI) will have much less cyber security budget.

(H3.b): Firms with highly rapid Cyber Security Infrastructure (CSI) will have much higher cyber security budget.

Modernity

According to the term "modernity", the amount to which Cyber Security Infrastructure is based on current items and technical developments is measured (Chanopas *et al.* [7]). It refers to the use of cybersecurity infrastructure that is up to date with current technological developments [8]. Compared to organizations operating in a more stable environment, organizations that provide a wide range of products and tailored services/products will be required to spend more on cyber

security budget.

A writeup on modern cybersecurity infrastructure can be seen at: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/; and at https://www.simplilearn.com/top-cybersecurity-trends-article.

As a result, we have the following:

(H4.a): Firms with less modern Cyber Security Infrastructure (CSI) will have much less cyber security budget.

(H4.b): Firms with highly modern Cyber Security Infrastructure (CSI) will have much less cyber security budget.

When the transactions of organizations are exposed to external world, then one requires a highly involved cybersecurity infrastructure and vice-versa. According to Miles and Snow *et al.* [5] marketing and R&D are important departments of firms with differentiation strategy and these are exposed to external world and needs protection from cyber threats (marketing information is diffused in the external world and needs to be protected; also company's designs made by R&D are existing in markets as a part of test marketing) and need more cybersecurity budget. Whereas in cost Leader firms, the important departments are production and finance and these are not exposed to external world and are "internal" departments; and thus need lesser involved cybersecurity infrastructure and lesser budget. Factories of cost leaders will function smoothly even if all computers and networks are disconnected from the external world (or internet). Cost leaders have very few large plants and need minimal communication between them; whereas differentiators need and have multi-plant strategies so that each customer segment is served with priority. Latest advances allow customer of a differentiator to schedule their order on the shop floor by using internet (to add to customer's delight) and thus expose its production data to the external world; and hence their cybersecurity is more involved and has higher budget. Hence we have the following hypotheses.

(H5.a): Cost Leader firms will have lower cybersecurity budget (CSB)

(H5.b): Differentiators will have higher cybersecurity budget (CSB).

(H6.a): Cost leaders will have basic minimal cybersecurity infrastructure (CSI).

(H6.b): Differentiators will have highly involved cybersecurity infrastructure (CSI).

Hypotheses are summarized in Table 1 below.

Table 1. Summary of developed hypothesis.

Hypothesis No	Cyber Security Infrastructure Dimensions	Cyber Security Budget
H1.a, b	High Modularity	Lower the cost
H2.a, b	High Compatibility	Lower the cost
H3.a, b	High Rapidity	Higher the cost
H4.a, b	High Modernity	Higher the cost

Continued

H5.a	Cost Leader Firms	Low CSB
H5.b	Differentiators Firms	High CSB
H6.a	Cost Leader Firms	Basic minimal CSI
H6.b	Differentiators Firms	Highly involved CSI

4. Questionnaire Development and Sampling

Data for the empirical research of the theoretical frameworks is collected through the use of structured questionnaires, which are administered to participants. The goal of the survey was to record the firm's operational strategy based on the responses so that it could be classed as either a cost leader or a differentiator based on the results. The questionnaire was divided into four tables in **Appendix**: Table A1 was used to evaluate the sort of strategy that a business employs, Table A2 was used to examine organizational structure, and Table A3 was used to determine the firm's cyber security infrastructure. However, elements relevant to cyber security training, cybersecurity budget, and computer network security infrastructure capability are included in Table A4. The detailed questionnaire is given in the Tables A1-A4 at the end of the paper.

Data Analysis and Findings

In order to construct this study, information was gathered from cyber security specialists, information security professionals in various enterprises at various levels of responsibility, and strategic management groups. A number of persons who are specialists in the disciplines of cyber security budgets, as well as researchers who work in the same sectors, were also consulted for their input.

K Mean Clustering

K-means clustering is a type of supervised learning used to organize and group unlabeled data. The method assigns each data point to one of the K groups depending on its attributes. The k-means clustering technique categorizes data points based on how similar their features are to one another. The centroids (means) of k clusters are used to label the data, with the variable K representing the number of groups. Each data point is iteratively assigned to one of the K groups based on the properties provided by the algorithm [9] [10]. The final clusters are formed using the information gathered on a company's strategy and technical uncertainties, together with the funding allocated to cyber security. We just set K = 2 so that either the CSB is low or high as we are considering only two strategy types, that is cost leaders and differentiators.

In the end, final clusters are created from responses acquired according to questionnaire criteria on firm's strategy, firm structure aspects and technical uncertainty, in addition to cyber security budget and cyber threat capabilities.

As shown in Tables 2-5, the end means of the majority of a firm's strategy parts are lower for group 1 than for group 2, despite the fact that both groups have

higher end means. In other words, high cyber security budgets are associated with Cluster 2, and low cyber security budgets are associated with Cluster 1. The categorization can be reinforced by taking into consideration the means that have been gained in terms of structural dimensions.

Specialization, standardization, formalization, and centralization are all low in firms with a high cyber security budget, but process complexity is high in organizations with a high cybersecurity budget. Those organizations with a minimal cyber security budget are characterized by a high level of specialization, formalization, and centralization, while also having a relatively low level of process complexity. Last but not least, cyber security budget clusters, technical unpredictability, and cyber threat capacity are all factors to consider.

Table 2. Strategy variables final cluster centers.

Strategy variables	Cluster 1	Cluster 2
STR1	4.833	1.321
STR2	1.271	4.857
STR3	1.604	4.214
STR4	1.458	4.536
STR5	1.417	4.464
STR6	1.458	4.679
STR7	4.396	1.536
STR8	4.271	1.643
STR9	1.271	4.854
STR10	4.375	1.357
STR11	1.313	4.607
STR12	1.333	4.679
STR13	1.438	4.393
STR14	4.688	1.143
STR15	1.333	4.786
STR16	1.438	4.857
STR17	1.667	4.321
STR18	1.521	4.607
STR19	1.583	4.536

Cluster 1 consists of 48 companies that exhibit the criteria of low cyber security budget companies as described above. Enterprises in this category account for 63.158 percent of the total number of businesses under investigation. Cluster 2 has 28 companies that meet the criteria for corporations with a High Cyber Secu-

rity Spending Capacity. These companies account for 36.842 percent of the total. The total number of firms that were investigated. There are no missing values in the data that has been collected.

Table 3. Structure variables final cluster centers.

Structure variables		Cluster 1	Cluster 2
Centralization	CEN1	4.813	1.464
	CEN2	4.479	1.571
	CEN3	4.417	1.643
	CEN4	4.333	1.429
Specialization	SPL1	4.333	1.607
	SPL2	4.354	1.607
Complexity	COMP1	1.438	4.393
	COMP2	1.583	4.286
	COMP3	1.604	4.357
	COMP4	1.438	4.357
	COMP5	1.438	4.464

Table 4. Cyber security variables final cluster centers.

Cyber Security Variables		Cluster 1	Cluster 2
Technological Uncertainty	TU1	1.583	4.286
	TU2	1.708	4.214
	TU3	1.479	4.679
Cyber Threat Capacity	CT1	1.458	4.857
	CT2	1.479	4.571
Cyber Security Budget	CSB1	1.235	3.880
	CSB2	1.608	4.560

Independent Sample t-test

The null hypothesis for the t-test is that the means of the two populations are the same. As a result, either the null hypothesis is accepted or rejected. The K-means clustering algorithm was utilized to discriminate between two different samples for our investigation. High budget and low budget cyber security budget groups were represented by these two independent samples, both high budget and low budget groups. We used the four characteristics of Cyber Security Infrastructure (CSI), modularity, compatibility, speed, and modernity, as the dependent variable in our analysis. Each dimension was analyzed independently for each of the two samples.

Table 5. Independent sample t-test results.

S. No.	Parameters	t-test for equality of means							Null Hypothesis
		t	df	Sig.	Mean Difference	Standard error difference	95% confidence interval of difference		
							Lower	Upper	
H1 (a, b)	MOD1	20.203	74	0.000	3.098	0.1533	2.792	3.403	Rejected
	MOD2	15.881	74	0.000	2.860	0.1800	2.501	3.21	Rejected
H2 (a, b)	COM1	18.144	74	0.000	3.208	0.176	2.856	3.560	Rejected
	COM2	18.061	74	0.000	2.982	0.165	2.653	3.311	Rejected
	COM3	17.944	74	0.000	3.014	0.168	2.680	3.349	Rejected
H3 (a, b)	RAP1	16.429	74	0.000	2.970	0.180	2.610	3.330	Rejected
	RAP2	15.618	74	0.000	2.809	0.179	2.451	3.167	Rejected
	RAP3	16.019	74	0.000	2.892	0.180	2.533	3.252	Rejected
	RAP4	16.619	58	0.000	2.752	0.165	2.422	3.083	Rejected
H4 (a, b)	MON1	17.613	74	0.000	2.958	0.167	2.623	3.292	Rejected
	MON2	15.130	74	0.000	2.669	0.176	2.318	3.021	Rejected

Table 6. Hypotheses H5.a, b and cross tabulation.

		Cyber Security Budget Cluster		Total
		High Budget	Low Budget	
Strategy Cluster	Cost Leader	3	41	**44**
	Differentiator	28	4	**32**
Total		**31**	**45**	**76**

Table 7. Chi-square results.

	Value	df	Sig.
Pearson Chi-Square	49.934	1	0.000
Likelihood ratio	56.747	1	0.000
Valid Cases	76		

Table 8. Hypotheses H6.a, b and cross tabulation.

		Cyber Security Infrastructure Cluster		Total
		Basic Minimal	Highly Involved	
Strategy Cluster	Cost Leader	41	3	**44**
	Differentiator	4	28	**32**
Total		**45**	**31**	**76**

Table 9. Chi-square results.

	Value	df	Sig.
Pearson Chi-Square	49.934	1	0.000
Likelihood ratio	56.747	1	0.000
Valid Cases	76		

(H0: μ1 = μ2) and (HA: μ1 ≠ μ2):

- For hypothesis H1 (H1.a, H1.b), concerning Cyber Security Infrastructure (CSI) modularity (MOD1, MOD2), Levene's test gives F-statistic of 0.259 with a Sig. value of 0.612. Equal variance is assumed among the two groups for CSI Modularity. The mean value of CSI modularity is higher for Low Cyber Security Budget firms than High Cyber Security Budget firms, *i.e.*, μL > μH (4.395 > 1.535), resulting in t statistic value of 15.881 with a sig. value of 0.000. There exists a significant difference in means of CSI modularity among the two budget groups. Hence, the null hypothesis is rejected, and subsequently, H1 (*i.e.*, H1.a and H1.b) is supported.
- For hypothesis H2 (H2.a, H2.b), concerning Cyber Security Infrastructure (CSI) compatibility (COM1, COM2), Levene's test gives F-statistic of 1.554 with a Sig. value of 0.217. Equal variance is assumed among the two groups for CSI Compatibility. The mean value of CSI compatibility is higher for Low Cyber Security Budget firms than High Cyber Security Budget firms, *i.e.*, μL > μH (4.708 > 1.500), resulting in t statistic value of 18.144 with a sig. value of 0.000. There exists a significant difference in means of CSI compatibility among the two budget groups. Hence, the null hypothesis is rejected, and subsequently, H2 (*i.e.*, H2.a and H2.b) is supported.
- For hypothesis H3 (H3.a, H3.b), concerning Cyber Security Infrastructure (CSI) rapidity (RAP1, RAP2), Levene's test gives F-statistic of 0.254 with a Sig. value of 0.615. Equal variance is assumed among the two groups for CSI Rapidity. The mean value of CSI rapidity is higher for High Cyber Security Budget firms than Low Cyber Security Budget firms, *i.e.*, μH > μL (4.428 > 1.458), resulting in t statistic value of 16.429 with a sig. value of 0.000. There exists a significant difference in means of CSI rapidity among the two budget groups. Hence, the null hypothesis is rejected, and subsequently, H3 (*i.e.*, H3.a and H3.b) is supported.
- For hypothesis H4 (H4.a, H4.b), concerning Cyber Security Infrastructure (CSI) modernity (MON1, MON2), Levene's test gives F-statistic of 0.481 with a Sig. (p-value) of 0.490. Equal variance is assumed among the two groups for CSI Modernity. The mean value of CSI modernity is higher for High Cyber Security Budget firms than Low Cyber Security Budget firms, *i.e.*, μH > μL (4.357 > 1.667), resulting in t statistic value of 15.130 with a sig. value of 0.000. There exists a significant difference in means of CSI modernity among the two budget groups. Hence, the null hypothesis is rejected, and subsequently,

H4 (*i.e.*, H4.a and H4.b) is supported.

Results of tests to verify hypotheses 5 and 6 are given in Tables 6-9.

The results validate our hypothesis that the Cyber Security Infrastructure used by a firm is significantly dependent on the company's cyber security budget. We can also relate the Cyber Security Infrastructure properties with the type of strategy that an organization follows *i.e.*, cost leader and differentiators. In the next section we will see the relation between organizational strategy and cyber security budget *i.e.*, cost leaders will have much less cyber security budget and differentiators will have much high cyber security budget from this conclusion we can say that organizations with cost leadership strategy will have CSI which is high in modularity, compatibility and low in rapidity, modernity and organizations with differentiation strategy will have CSI, which is low in modularity, compatibility and high in rapidity, modernity.

Summary of hypotheses supported by data is given in Table 10 below. It is to be noted that all hypotheses are supported.

Table 10. Summary of investigations of all developed hypotheses.

Hypothesis No	Cyber Security Infrastructure Dimensions	Cyber Security Budget
H1.a, b	High Modularity	Supported
H2.a, b	High Compatibility	Supported
H3.a, b	High Rapidity	Supported
H4.a, b	High Modernity	Supported
H5.a, b	Cybersecurity Budget	Supported
H6.a, b	Cybersecurity infrastructure	Supported

Final categorization of strategy of firm and the cyber security budget (whether high or low) is given in Table B1 of **Appendix B**.

5. Conclusions

Cost leaders will have a lower cyber security budget than differentiators since they (cost leaders) are "internally" oriented organization. Cost leaders have assured markets and have much fewer links with the external world (in fact Miles and Snow [5] said that they have very weak marketing dept.) and their Cyber Security Infrastructure is highly centralized, according to Gartner (CSI). And differentiators are "externally" oriented organizations and have complex linkages to their external environment. In fact, business literature confirms that cost leaders have low environmental uncertainty and differentiators have "high" environmental uncertainty and their (differentiators) cybersecurity budget is higher. Thus it appeals to intuition that cost leaders don't require very involved CSI; whereas Differentiators need highly involved CSI. Data supports this as hypotheses H5 and H6 are verified by data.

This study is able to associate high modularity, high compatibility, low rapidity and low modernity CSI with cost leaders; and low modularity, low compatibility,

high rapidity and high modernity CSI with differentiators (hypotheses H1-H4 are supported).

Thus our study says thay first identify the strategy of the company and then decide its cyber security budget and then determine the levels of attributes (such as modularity, compatibility, rapidity and modernity) of the CSI.

There may be other dimensions of CSI (other than modularity, compatibility, rapidity and modernity) such as scalability, latency and loose coupling, etc. that are yet to be related to strategy of the firm. This is a useful future research direction. Also a new strategy type has emerged that is "innovators" (with sub types of continuous innovation, modular and architectural innovation and radical innovation) and there is a need to relate this "innovation" strategy type to CSI. This again, we feel this is a topic of future research.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Chandler, A.D. (1967) Strategy and Structure: Chapters in the History of Industrial Enterprise. The MIT Press.

[2] Mazzoccoli, A. and Naldi, M. (2021) Optimal Investment in Cyber-Security under Cyber Insurance for a Multi-Branch Firm. *Risks*, **9**, Article No. 24. https://doi.org/10.3390/risks9010024

[3] Bullock, J.A., Haddow, G.D. and Coppola, D.P. (2018) Cybersecurity and Critical Infrastructure Protection. In: Bullock, J.A., *et al.*, Eds., *Homeland Security*, Elsevier, 189-226. https://doi.org/10.1016/b978-0-12-804465-0.00008-x

[4] Porter, M.E. (1980) Competitive Strategy: Techniques for Analyzing Industries and Competitors. Free Press.

[5] Miles, R.E., Snow, C.C., Meyer, A.D. and Coleman, H.J. (1978) Organizational Strategy, Structure, and Process. *Academy of Management Review*, **3**, 546-562. https://doi.org/10.5465/amr.1978.4305755

[6] Teufel, S., Teufel, B., Aldabbas, M. and Nguyen, M. (2020) Cyber Security Canvas for SMEs. In: Venter, H., *et al.*, Eds., *Information and Cyber Security*, Springer International Publishing, 20-33. https://doi.org/10.1007/978-3-030-66039-0_2

[7] Chanopas, A., Krairit, D. and Ba Khang, D. (2006) Managing Information Technology Infrastructure: A New Flexibility Framework. *Management Research News*, **29**, 632-651. https://doi.org/10.1108/01409170610712335

[8] Hamrioui, S. and Bokhari, S. (2021) A New Cybersecurity Strategy for IoE by Exploiting an Optimization Approach. 2021 12*th International Conference on Information and Communication Systems* (*ICICS*), Valencia, 24-26 May 2021, 23-28. https://doi.org/10.1109/icics52457.2021.9464595

[9] Vishwakarma, N.K., Singh, R.K. and Sharma, R.R.K. (2019) Internet of Things Architectures: Do Organizational Strategies Matters? *Business Process Management Journal*, **26**, 102-131. https://doi.org/10.1108/bpmj-03-2018-0092

[10] Ahmad, A. and Dey, L. (2007) A K-Mean Clustering Algorithm for Mixed Numeric and Categorical Data. *Data & Knowledge Engineering*, **63**, 503-527. https://doi.org/10.1016/j.datak.2007.03.016

Appendix A

Table A1. Strategy.

Select the number from the scale below that describes the strategy of your organization most appropriately.
1—Not high, 2—Little high, 3—Moderately high, 4—High, 5—Very high.

Item	Statement	Response
STR1	The capability of your organization to compete on price is	1 2 3 4 5
STR2	The capability of your organization to make rapid design changes or introduce new products quickly.	1 2 3 4 5
STR3	The capability of your organization to provide high performance product is.	1 2 3 4 5
STR4	The capability of your organization to deliver products quickly is.	1 2 3 4 5
STR5	The capability of your organization to provide after sales service is.	1 2 3 4 5
STR6	The capability of your organization to advertise and promote the product is.	1 2 3 4 5
STR7	The capability of your organization to distribute product broadly is.	1 2 3 4 5
STR8	The capability of your organization to deliver a broad product line is.	1 2 3 4 5
STR9	The capability of your organization to aggressively innovate product is.	1 2 3 4 5
STR10	The importance of expertise of top managers in their operational areas is.	1 2 3 4 5
STR11	The importance of strictly following deadlines in your organization is.	1 2 3 4 5
STR12	The capability of your organization to make frequent engagements with the new market trends is.	1 2 3 4 5
STR13	The capability of your organization to spend more resources on high end products is.	1 2 3 4 5
STR14	The importance of short term results over long term results.	1 2 3 4 5
STR15	The importance of increasing market share by introducing innovation and change.	1 2 3 4 5
Select the scale below to answer the next questions. 1—Highly disagree, 2—Disagree, 3—Neither agree nor disagree, 4—Agree, 5—Highly agree.		
STR16	There is no blueprint for your organization's strategy.	1 2 3 4 5
STR17	Strategy frequently changes.	1 2 3 4 5
STR18	There are no established procedures in your organization for doing things.	1 2 3 4 5
STR19	It is not important to strictly follow the established procedures.	1 2 3 4 5

Table A2. Structure centralization.

Select the scale below to answer the next questions.
1—Strongly disagree, 2—Disagree, 3—Neither agree nor disagree, 4—Agree, 5—Strongly agree.

Item	Statement	Response
CEN1	There is more reliance on rules and standard procedures in your organization.	1 2 3 4 5
CEN2	Most of the decision-making is concentrated in top management hands.	1 2 3 4 5
CEN3	Your organization have more levels of management with narrow spans of control.	1 2 3 4 5
CEN4	Your organization's way of decision-making system increases the processing capabilities of managers.	1 2 3 4 5
Specialization. Please select the number from the scale below. 1—Very low, 2—Low, 3—Moderate, 4—High, 5—Very high.		
SPL1	To what extent specialists are hired in your organization.	1 2 3 4 5
SPL2	To what extent is costing specialized by product or factory in your organization.	1 2 3 4 5

Complexity of workflow.
Please select the number from the scale below.
1—Very low, 2—Low, 3—Moderate, 4—High, 5—Very high.

COMP1	In your organization how frequently are interdepartmental committees set up, to allow departments to engage in joint decision making.	1 2 3 4 5
COMP2	In your organization how frequently are task forces and/or temporary bodies set up to facilitate interdepartmental collaboration on a specific project.	1 2 3 4 5
COMP3	In your organization the use of liaison personnel, whose job is to coordinate the efforts of several departments for the purpose of a specific project is.	1 2 3 4 5
COMP4	In your organization the inter departmental interactions on most decisions are.	1 2 3 4 5
COMP5	As new situation presents itself on the whole, capability of your organization to come up with a matching new response.	1 2 3 4 5

Table A3. Cyber Security Infrastructure (CSI) parameters.

Please rate the following statements at 5 points Likert-scale where:
1—Strongly disagree, 2—Disagree, 3—Neither agree nor disagree, 4—Agree, 5—Strongly agree.

Item	Statement	Response
	Modularity	
Mod1	New algorithms have to be implemented each time.	1 2 3 4 5
Mod2	Reusable subsystems or modules are never used in system development.	1 2 3 4 5
	Compatibility	
COM1	CSI can be used across multiple operating systems.	1 2 3 4 5
COM2	Data can be shared across applications and operating systems.	1 2 3 4 5
COM3	All CSI (hardware and software) is compatible	1 2 3 4 5
	Rapidity	
RAP1	CSI components (*i.e.*, hardware, software database) are	1 2 3 4 5
RAP2	Compared to rivals within the industry, the organization has the foremost CSI networks.	1 2 3 4 5
RAP3	CSI can be easily upgraded on existing IT infrastructure.	1 2 3 4 5
RAP4	CSI can be easily and quickly adapted for changing needs and standards.	1 2 3 4 5
	Modernity	
MON1	Cyber Security Infrastructure (CSI) is based on well-known products.	1 2 3 4 5
MON2	Cyber Security infrastructure (CSI) is based on current technological trends.	1 2 3 4 5
	Technological Uncertainty	
TU1	We have sufficient information about new technological requirements for our organization.	1 2 3 4 5
TU1	We can predict the new technological requirement for our organization.	1 2 3 4 5
TU3	The product/services technologies change very quickly.	1 2 3 4 5

Table A4. Cyber Security Overview.

Rate the following factors if you agree, which inhibit your organization from adequately defending against cyber threats. 1—Strongly disagree, 2—Disagree, 3—Neither agree nor disagree, 4—Agree, 5—Strongly agree.

Item	Statement	Response
CT1	Lack of budget.	1 2 3 4 5
CT2	Inability to justify additional investment.	1 2 3 4 5
CSB1	Your organization provides incentives for cyber security training and certification.	1 2 3 4 5
CSB2	Your organization makes financial investments for procuring scalable Cyber Security Infrastructure (CSI) to fulfill the strategic requirements.	1 2 3 4 5

Appendix B

Table B1. Data Setup for H5.a, b.

Responses	Strategy Cluster	Cyber Security Budget Cluster
1	Cost Leader	Low Budget
2	Cost Leader	Low Budget
3	Cost Leader	Low Budget
4	Cost Leader	Low Budget
5	Differentiator	Low Budget
6	Cost Leader	Low Budget
7	Cost Leader	Low Budget
8	Cost Leader	Low Budget
9	Cost Leader	Low Budget
10	Differentiator	Low Budget
11	Cost Leader	Low Budget
12	Cost Leader	Low Budget
13	Cost Leader	Low Budget
14	Cost Leader	Low Budget
15	Differentiator	Low Budget
16	Cost Leader	Low Budget
17	Cost Leader	High Budget
18	Cost Leader	Low Budget
19	Cost Leader	Low Budget
20	Cost Leader	Low Budget
21	Cost Leader	High Budget
22	Cost Leader	Low Budget
23	Differentiator	Low Budget
24	Cost Leader	Low Budget
25	Cost Leader	Low Budget

Continued

26	Cost Leader	Low Budget
27	Cost Leader	Low Budget
28	Cost Leader	Low Budget
29	Cost Leader	Low Budget
30	Cost Leader	Low Budget
31	Cost Leader	Low Budget
32	Cost Leader	Low Budget
33	Differentiator	High Budget
34	Differentiator	High Budget
35	Differentiator	High Budget
36	Differentiator	High Budget
37	Differentiator	High Budget
38	Differentiator	High Budget
39	Differentiator	High Budget
40	Differentiator	High Budget
41	Differentiator	High Budget
42	Differentiator	High Budget
43	Differentiator	High Budget
44	Differentiator	High Budget
45	Differentiator	High Budget
46	Differentiator	High Budget
47	Differentiator	High Budget
48	Differentiator	High Budget
49	Differentiator	High Budget
50	Cost Leader	Low Budget
51	Cost Leader	Low Budget
52	Cost Leader	Low Budget
53	Cost Leader	Low Budget
54	Cost Leader	Low Budget
55	Cost Leader	Low Budget
56	Cost Leader	Low Budget
57	Cost Leader	Low Budget
58	Cost Leader	Low Budget
59	Differentiator	High Budget
60	Differentiator	High Budget
61	Differentiator	High Budget
62	Differentiator	High Budget

Continued

63	Differentiator	High Budget
64	Differentiator	High Budget
65	Differentiator	High Budget
66	Differentiator	High Budget
67	Cost Leader	Low Budget
68	Cost Leader	Low Budget
69	Differentiator	High Budget
70	Differentiator	High Budget
71	Cost Leader	Low Budget
72	Cost Leader	High Budget
73	Cost Leader	Low Budget
74	Cost Leader	Low Budget
75	Cost Leader	Low Budget
76	Differentiator	High Budget

Table B2. Data setup for H6.a, b.

Responses	Strategy Cluster	Cyber Security Infrastructure Cluster
1	Cost Leader	Basic minimal
2	Cost Leader	Basic minimal
3	Cost Leader	Basic minimal
4	Cost Leader	Basic minimal
5	Differentiator	Basic minimal
6	Cost Leader	Highly involved
7	Cost Leader	Basic minimal
8	Cost Leader	Basic minimal
9	Cost Leader	Basic minimal
10	Differentiator	Basic minimal
11	Cost Leader	Highly involved
12	Cost Leader	Basic minimal
13	Cost Leader	Basic minimal
14	Cost Leader	Basic minimal
15	Differentiator	Basic minimal
16	Cost Leader	Highly involved
17	Cost Leader	Basic minimal
18	Cost Leader	Basic minimal
19	Cost Leader	Basic minimal
20	Cost Leader	Basic minimal

Continued

21	Cost Leader	Basic minimal
22	Cost Leader	Basic minimal
23	Differentiator	Basic minimal
24	Cost Leader	Basic minimal
25	Cost Leader	Basic minimal
26	Cost Leader	Basic minimal
27	Cost Leader	Basic minimal
28	Cost Leader	Basic minimal
29	Cost Leader	Basic minimal
30	Cost Leader	Basic minimal
31	Cost Leader	Basic minimal
32	Cost Leader	Basic minimal
33	Differentiator	Highly involved
34	Differentiator	Highly involved
35	Differentiator	Highly involved
36	Differentiator	Highly involved
37	Differentiator	Highly involved
38	Differentiator	Highly involved
39	Differentiator	Highly involved
40	Differentiator	Highly involved
41	Differentiator	Highly involved
42	Differentiator	Highly involved
43	Differentiator	Highly involved
44	Differentiator	Highly involved
45	Differentiator	Highly involved
46	Differentiator	Highly involved
47	Differentiator	Highly involved
48	Differentiator	Highly involved
49	Differentiator	Highly involved
50	Cost Leader	Basic minimal
51	Cost Leader	Basic minimal
52	Cost Leader	Basic minimal
53	Cost Leader	Basic minimal
54	Cost Leader	Basic minimal
55	Cost Leader	Basic minimal
56	Cost Leader	Basic minimal
57	Cost Leader	Basic minimal

Continued

58	Cost Leader	Basic minimal
59	Differentiator	Highly involved
60	Differentiator	Highly involved
61	Differentiator	Highly involved
62	Differentiator	Highly involved
63	Differentiator	Highly involved
64	Differentiator	Highly involved
65	Differentiator	Highly involved
66	Differentiator	Highly involved
67	Cost Leader	Basic minimal
68	Cost Leader	Basic minimal
69	Differentiator	Highly involved
70	Differentiator	Highly involved
71	Cost Leader	Basic minimal
72	Cost Leader	Basic minimal
73	Cost Leader	Basic minimal
74	Cost Leader	Basic minimal
75	Cost Leader	Basic minimal
76	Differentiator	Highly involved

Biographies

R. R. K. Sharma: He is B.E. (mechanical engineering) from VNIT Nagpur India, and PhD in management from I.I.M., Ahmedabad, INDIA. He has nearly three years of experience in automotive companies in India (Tata Motors and TVS-Suzuki). He has 32 years of teaching and research experience at the Department of Industrial and Management Engineering, I.I.T., Kanpur, 208016 INDIA. To date he has written 1230 papers (peer-reviewed (416)/under review (33)/working papers 781 (not referred)). He has developed over ten software products. To date, he has guided 69 M TECH and 25 Ph D theses at I.I.T. Kanpur. He has been Sanjay Mittal Chair Professor at IIT KANPUR (15.09.2015 to 14.09.2018) and is currently a H.A.G. scale professor at I.I.T. Kanpur. In 2015, he received "Membership Award" given by IABE USA (International Academy of Business and Economics). In 2016 he received the "Distinguished Educator Award" from IEOM (Industrial Engineering and Operations Management) Society, U.S.A. In 2021, he received IEOM Distinguished Service Award. In 2019, 2020, 2021 and 2022 he was invited by MHRD Govt. of India to participate in NIRF rankings survey for management schools in India. In 2019, 2020, 2022, 2023, 2024 and 2025 he was invited to participate in QS ranking exercise for management schools in Asia. He was invited to participate in THE (Times Higher Education) World University Ranking Exercise

2023, 2024 and 2025. He is Fellow of IEOM Society USA 2024.

Niraj K. Vishavkarma: Dr. Vishvakarma is a faculty of IT and Systems. He has more than two years of teaching experience in the reputed institutions like IIM Jammu, International Management Institute Bhubaneswar and Symbiosis Institute of Operations Management Nashik. He has pursued his Ph.D. from IIT Kanpur in the area of information systems. He has also obtained B.Tech (IT) and MBA both from ABV-Indian Institute of Information Technology &Management Gwalior. His current areas of research interests are management of technologies, diffusion of innovation, information system implementation, business process reengineering, big-data analytics, and supply chain strategies. He has a number of publications in ABDC ranked and Scopus indexed journals. He is also a reviewer in various international journals.

Avirag Bajpai: He is Associate Professor with L&T IPM Vadodra India. He has 15 publications to his credit.

Vimal Kumar: He has over 200 publications. His name appeared in 2% intellectiual list of Stanford University.

Shivam Sharma has earned his M. Tech degree from the department of IME IIT Kanpur.