An empirical study to analyze the impact of Enterprise Collaborative Strategies for Cyber Security Solution Adoption on their Business ROI

Sanjay Navin, Research Scholar, IFIM Business School, VTU

Abstract

Today's distributive business environment, the success or failure of enterprise business depends on adopting the correct business strategy. Enterprises are adopting digital transformation to optimize the business ROI. Digital transformation has increased the cyber threat landscape and cyber-attack are increasing at the exponential rate impacting Business Return on Investment (ROI). The enterprises are adopting different types of strategies to meet the business objectives for adoption of cyber security solutions. This paper analyzes the impact of enterprise collaborative strategy for adopting Cyber Security Solution on their business ROI.

In this paper, the research conceptual framework has been divided into three parts – Firstly, the enterprise collaborative strategies are broadly classified into three levels – Corporate Level Collaborative Strategy, Business Level Collaborative Strategies and Functional level collaborative strategies. Secondly, The Business ROI is classified in three parts – Financial ROI, Marketing ROI and Ethical ROI. Thirdly, questionnaires developed from the comprehensive Cyber Security Solutions are analyzed based on five steps of NIST CyberSecurity Framework 1.1 - Identify, Protect, Detect, Respond, and Recover. Finally the data are collected from telecom sector enterprises.

An empirical research methodology adopted to derive the findings and recommendation. The identified hypothesis is verified based on secondary data. The data is collected from various Webinars, Interviews

[1]***Acknowledgement:***

Dr. S. Baskaran

Reviewer

of Strategic leaders, Corporate's Press release notes. These collected data are used to quantify on Linkert Scale for statistical correlation and regression analysis.

The results suggest that a collaborative strategy at corporate, business and functional level improves Financial, Market and Ethical business ROI.

Key words:

Cyber Security, Digital Transformation, Collaborative Strategies, NIST, Disruptive Business Environment.

I. INTRODUCTION

In today's dynamic business environment, the enterprise needs to adopt the right strategy for the growth and growth and sustainability of a business. In the recent past, the enterprise was adopting either cost leadership, product differential strategy, but innovation of technology has completely transformed enterprise structure and element of business growth and profits margins. Enterprises are adopting digital transformation to adapt to a disruptive business environment. This has increased the cyber threat landscape and impact of cyber-attacks. Cyber security solutions have been considered as a continuous process to integrate defense mechanisms for protecting critical infrastructure and information. The Cybersecurity challenges have forced enterprises to define strategies at corporate, business and functional level. Considering the complexity and cost of continuous adoption of cyber security solutions, this paper recommends the adoption of collaborative strategies for Cybersecurity Risk assessment and mitigation strategies. This paper also analyzes the impact of enterprise collaborative strategy for adopting Cyber Security Solution on their business ROI.

In this paper, the research conceptual framework have been divided into three parts – Firstly, the enterprise collaborative strategies are broadly classified into three levels – Corporate Level Collaborative Strategy, Business Level Collaborative Strategies and Functional level collaborative strategies. Secondly, The Business ROI is classified in three parts – Financial ROI, Marketing ROI and Ethical ROI. Thirdly, questionnaires developed from the comprehensive Cyber Security Solutions are analyzed based on five steps of NIST CyberSecurity Framework 1.1 - Identify, Protect, Detect, Respond, and Recover. Finally the data are collected from telecom sector enterprises.

This paper is organized in multiple chapters - the chapter 2 details the literature review on cyber security challenges, threats and adoption strategies used by various enterprises. Chapter 3 details the significance of this research study. The chapter 4 details the statement of problem for Cybersecurity threats and solution adoptions strategy. Chapter 5 details the objectives of this research study. Chapter 6 details the research methodology used for this research study. Chapter 7 details the results and key finding. The chapter 8 details the key recommendation from the key findings. The chapter 9 details the conclusion and final chapter details the overall limitation of this research study.

II. Review of Literature

In today's dynamic business environment, the adoption of the right type of strategy is mandatory for an enterprise to meet the business objective. In the current digital era, one of the key challenges for an enterprise is to develop a secure business environment by adopting effective cyber security solutions. The literature review for this research is divided into four themes – a) Strategy management for disruptive technology and business environment, b) Components of business ROI, c) Cyber security threats and solution adoption, and, d) Collaborative strategy for adopting cyber security solutions. Each literature review theme is presented in chronological order. This chapter is divided into four sections. The first sections details literatures surveys of strategic management analysis, formulation, execution and monitoring approach for disruptive

A. Strategic Management for disruptive technology and business environment

The business environments are broadly classified as Internal, External and Global. The distributive technology innovation also disrupting business scenarios and industrial evolution 4.0 and consequently industry 5.0 are adopting digital transformation and fully automated using Artificial Intelligence and Machine Learning technology. This has created new challenges for enterprise strategic leaders – cyber security. It is difficult to analyze the impact of cyber-attack due to the incase attack surface. The Cyber Security Solution got placed in the Vision Statement for enterprise. Thus the cyber security solution needs to be included in corporate level, Business Level and functional level Strategic plan management. Enterprise strategic leader's need to trade off among various strategies approaches like Competitive, Differential, Low Cost, Focus, innovation and collaborative strategies. Porters' recommends relationships between Market Scope and Competitive advantages for selecting effective strategies to manage their enterprise objective.

Michael E. Porter's Five Generic Strategy Model

Source: Michael E. Porter, Competitive Strategy: Techniques for Analyzing Industries and Competitors (New York: Free Press, 1980)

B. Components of business ROI

The key objectives of any enterprise are maximizing revenue and optimizing profits. This can be measured

The total business objectives are classified into three parts

- Financial ROI (FROI) - This dependent variable measures the actual final gain and loss due for adoption of collaborative strategy for cyber security solution.
- Market ROI (MROI) – This dependent variable measures the brand value, long terms market share gain or loss for adoption of collaborative strategy for cyber security solution
- Ethical ROI (EROI) – This dependent variable measures regulatory compliance and social contribution in contributing to providing a secure environment.

C. Cyber security threats and solution adoption

This paper evaluates the impact of collaborative strategies for Cybersecurity solution adoptions to optimize the business objective which is measured as ROI. Cyber Security is integrated functions that require effective collaboration throughout the organization. It is imperative for security strategists to have everyone required on board, so that they know the value of the assets being protected and the real cost of breaches which can then help determine current and future security requirements.

"The enterprise security program must address all of the infrastructure elements in order to provide true protection of information assets. Failure to address even one element of the enterprise security infrastructure leaves large holes in protection and results in little security improvement." (Vance, slide 10). Cyber Security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information." (The National Cyber Security Strategy 2011, Dutch Ministry of Security and Justice)

Cyber-attacks can happen from any loopholes the attacker finds, the enterprise strategic leader needs to identify threats and risk of all components for enterprise organizational structure.

A joint study by McKinsey and the World Economic Forum in 2014 revealed that 71 percent of global banking IT executives believe that attackers will continue to move faster than banks in modifying their skill sets and spotting potential vulnerabilities. Additionally, 80 percent of respondents believe that the risk of cyberattacks and compromised data will have major strategic implications for their businesses over the next five years.

D. Collaborative Strategic Management for Cyber Security Solution Adoption

Developing a security strategy is a detailed process that involves initial assessment, planning, implementation and constant monitoring. It also include a combination of actions that counter imaginable threats and vulnerabilities: policies and procedures, access management measures, communications systems, technologies and systems integration practices

E. Literature review findings and conclusion

III. SIGNIFICANCE OF THE STUDY

Collaboration Strategies

- Digitization of data, products, and processes is an increasingly important driver of economic growth, but it also creates a host of cybersecurity challenges and vulnerabilities. The push toward greater multichannel integration, for instance, adds significantly to the customer experience but introduces many more interfaces that intruders can exploit.
- Enterprise collaboration with business partners, customers, advisers, and other third parties can enrich everything from product development to recruiting but can also result in more complex, conjoined supply chains and information flows.
- Hybrid delivery models, in which some business services and processes are moved to the cloud and managed by external providers, extend the security perimeter and add to the sweep of activities that companies must monitor to detect attacks on their environments.
- Not only does digitization introduce more openings for hackers and others to exploit, but it also increases the value of an organization's data assets. Within the banking sector, for instance, the use of big data and analytics may greatly increase a bank's ability to target and serve high-value clients with specific cross-selling offers. The value of the data rises as customer information is aggregated and cross-referenced—allowing companies to track names, demographics, and purchase histories (with due regard for customer privacy)—but so does the attendant risk. A breach can expose the bank and its clients to severe financial and reputational harm.
- Many organizations have invested heavily in IT security, but because of budget and time pressures, most have ended up layering new security infrastructure on top of their existing IT architecture. That creates a heterogeneous architectural landscape in which individual systems are haphazardly ring-fenced
- The rush to roll out automated, end-to-end process work flows through the cloud can sometimes result in poorly planned pilots that are coded without considering how they will be integrated into

the existing landscape. Companies that proceed without first creating a safe testing area, or "sandbox," can end up putting their entire IT landscape at risk.

IV. Statements of the problem

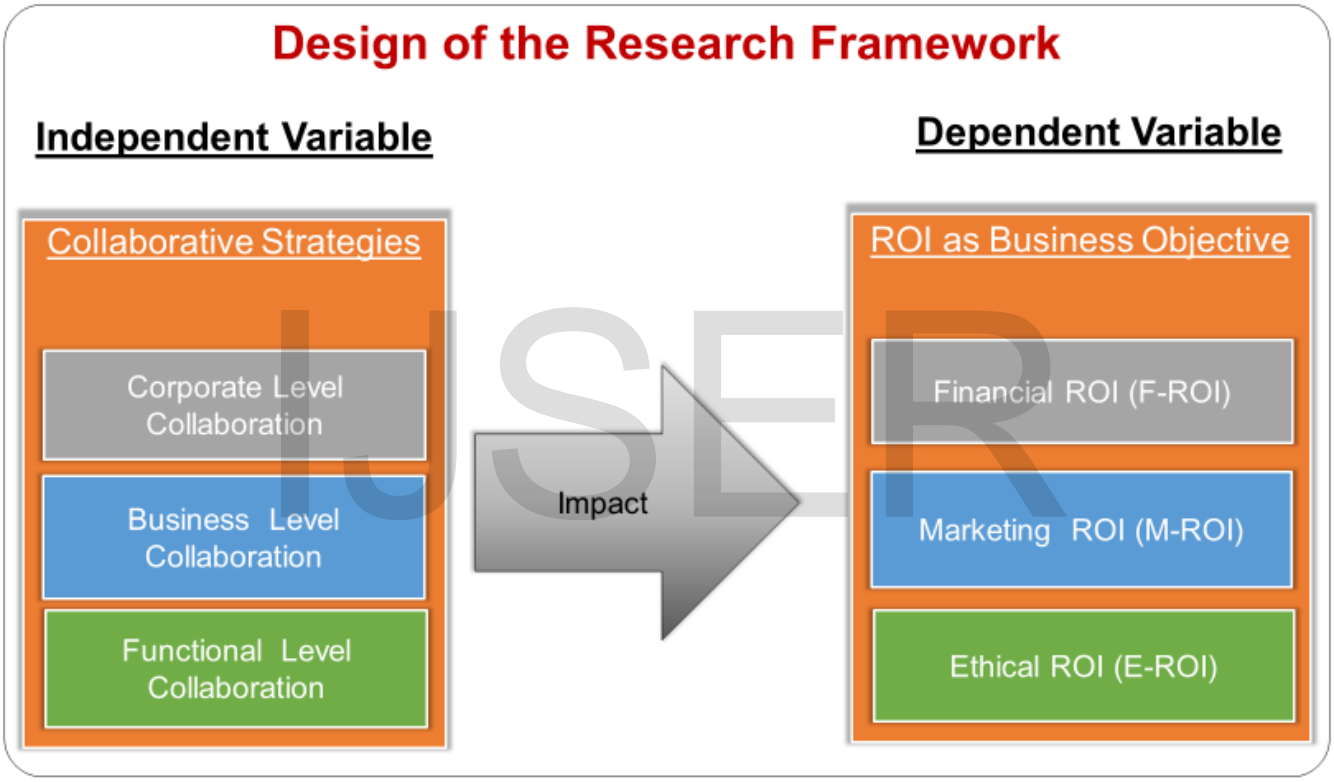
The selection and adoption of the right strategy is mandatory for an enterprise to protect its critical infrastructure and information from cyber-attacks.

Objectives

- To create the awareness for Cyber Security Challenge among entrepreneurs and enterprise leaders
- To evaluate the impact of Cyber Security threats on Business Objectives
- How to manage and Formulate Strategic Plan for Cyber Security Solution adoptions
- Cyber security Threats and Solutions
- Formulating Right Strategy - Analysis, Plan, Execute and Evaluate
- Evaluating the impacts on Business Objectives
- Key Recommendation for Cyber Security Strategic Plan Management

V. Research Methodology

The objective of this paper is to analyze the impact of Enterprise Collaborative Strategies for Cyber Security Solution Adoption on their Business ROI. Based on the literature review, the research study is planned to study the independent variables Corporate Level Collaboration, Business Level Collaboration and Functional Collaboration and dependent variables Financial ROI, Market ROI and Ethical ROI as mentioned in Figure below.



A. Independent Variable

Corporate Level Collaboration (CLC) – The corporate strategy for Cyber Security Solution adoption means the Cyber security adoption in the vision and mission statement of the enterprise organization. The impact of cyber security risk and impact needs to be sponsored by the CXO level.

Business Level Collaboration (BLC) - Each business unit in an enterprise identifies threat landscape, vulnerability and risk. Business Heads adopt the appropriate cyber security solution to protect

information. Business Heads need to collaborate with other businesses within and outside enterprise to have effective cyber security solutions. This variable will impact ROI of the enterprise

Functional Level Collaboration (FLC) – This independent variable evaluates the implementation and integration of cyber solutions to protect enterprise information and data. The adoption of collaborative strategies at functional level impacts enterprise ROI.

B. Dependent Variable

One of the most effective approaches to evaluate enterprise performance is Return of Investment. In this study ROI has been used to measure the overall business performance. This is divided into three parts and considered as a dependent variable for this research study.

Financial ROI (FROI) - This dependent variable measures the actual final gain and loss due for adoption of collaborative strategy for cyber security solution.

Market ROI (MROI) – This dependent variable measures the brand value, long terms market share gain or loss for adoption of collaborative strategy for cyber security solution

Ethical ROI (EROI) – This dependent variable measures regulatory compliance and social contribution in contributing to providing a secure environment.

C. Research Proposition

This study identified three independent variables and three dependent variables for evaluating the impact of collaborative strategies. The following research proposition has been defined

[1.] Is there any significant relationship between CLC and FROI?

[2.] Is there any significant relationship exist between CLC and MROI

[3.] Is there any significant relationship exist between CLC and EROI

[4.] Is there any significant relationship exist between BLC and FROI

[5.] Is there any significant relationship exist between BLC and MROI

[6.] Is there any significant relationship exist between BLC and EROI

[7.] Is there any significant relationship exist between FLC and FROI

[8.] Is there any significant relationship exist between FLC and MROI

[9.] Is there any significant relationship exist between FLC and EROI

D. Research Method

The research proposition is verified based on secondary data. The enterprise data for collaborative strategy for adoption of cybersecurity solutions is selected based on Judgmental analysis. The data is collected from various Webinars, Interviews of Strategic leaders, Corporate's Press release notes. These collected data are used to quantify on Linkert Scale for statistical correlation and regression analysis.

❖ Research Approach

Empirical Methods with Secondary Data collected from Blogs, Webinar, Social Media. These collected data are used to quantify on Linkert Scale for statistical correlation and regression analysis

❖ Sample Design

Sample Universe is selected as Cyber Security Ecosystem. Based on Literature review and Secondary data, the Cyber Security is divided in three Strata.

- Enterprise Looking for Digital Transformation, Cyber Security Solution Providers, Cyber Security Analyst, Regularity and Standardization Bodies

Each Strata are again classified into three level - Responder Classification

- Corporate Level Strategic leaders, Business Level Strategic Leaders and Functional Level Strategic leaders for collection of data

- Questionnaires, Data Collection and Analysis

  Developed total 11 questions, 9 questions as mentioned in research postulates, 1 Question on Responder Profile, 1 Question on Enterprise Product Domain

  Classified the Blogs writers based on the enterprise Working and Experience Label – CXO, Business Heads and Managers

  Read and Collected more 1000 Blogs, 100 Webinar Presenter, attended 20 Security and Network Solution Workshop, 500 Enterprise Vision and Mission statements to create a sample for 70 respondents for detailed analysis and generating recommendations and final conclusion

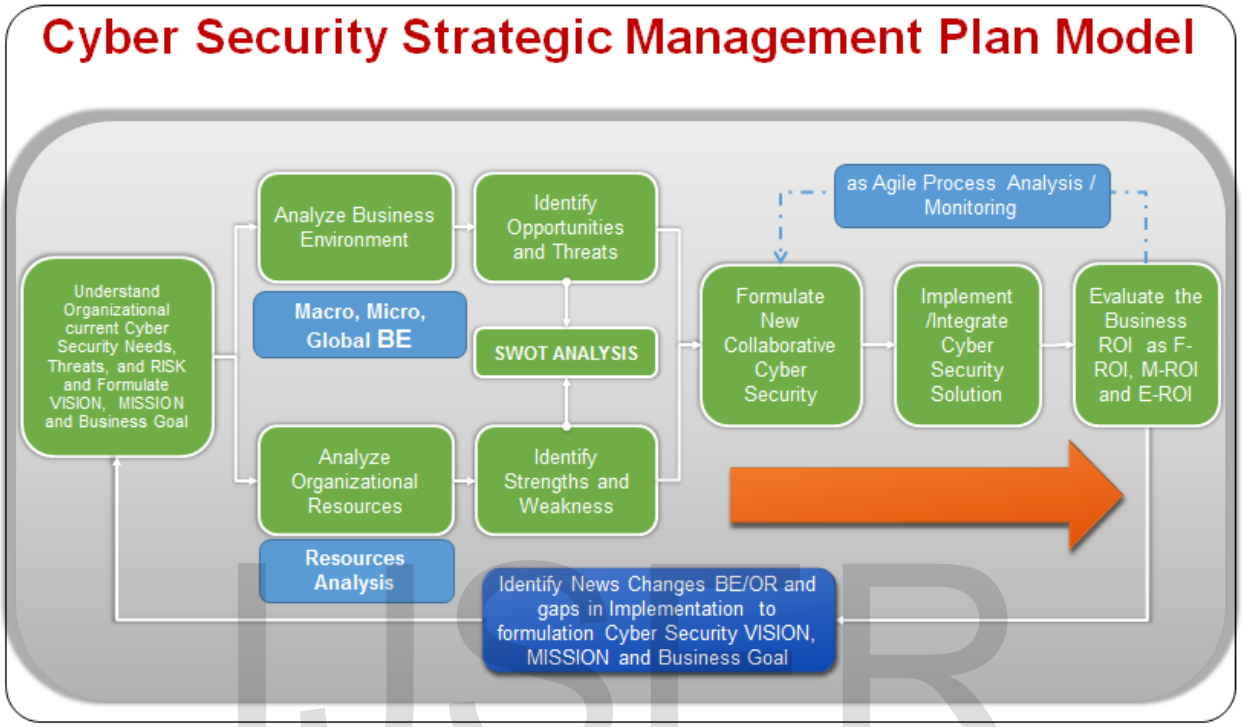
VI. Results and Key Finding

Cyber Security strategy in any enterprise starts with an in-depth analysis of their business. A cyber security strategy is thus an important document which details out a series of steps necessary for an organization to identify, remediate and manage risks while staying compliant. An effective cyber security strategy is comprehensive and dynamic, with the elasticity to respond to any type of security threats.

- As digitization creates new cyber threats, businesses should make security an integrated part of their IT infrastructure.

VII. Recommendation and Conclusion

Collaborative Strategies formulation for Cyber Security



Key recommendations are

- Collaboration Strategy at Corporate, Business and Functional Level to manage zero day vulnerability, attack and defense.
- The Cyber Security Strategic Management Plan document defines and prioritizes information assurance and security initiatives that the enterprise must commence to enhance the protection of information and related technology.
- Theft of information is not only costly, but can also jeopardize valuable customer relationships and brand reputation.
- More than half (54%) of telecom respondents said they have purchased cybersecurity coverage.

- [Evaluation] An Enterprise should consolidate previously identified and executed projects (where practical), provide scope and definition for each of the identified efforts, detail the general risks addressed by the initiative and provide a foundation that can later be refined by senior management.
- Additionally, to support higher-level evaluation of initiatives that can be undertaken when required, the security strategy planning process needs to identify any significant dependencies associated with the initiative
- Enterprise should help the business take advantage of robust analytics capabilities while also ensuring that the information and application architecture adequately protects sensitive data.

VIII. Conclusion

To stay ahead of attackers, companies need to design processes, platforms, and IT infrastructures with security in mind and incorporate secure architecture principles into their security programs.

- A collaborative strategy at corporate, business and functional level improves Financial, Market and Ethical business ROI

Limitation and Scope of Further Research

The conclusion and finding are drawn based on secondary data only.

References

[1] J.M. Bryson, J.M. (2018). Strategic planning for public and nonprofit organizations: A guide to strengthening and sustaining organizational achievement. John Wiley & Sons.

[2] NIST, April, 2018, Framework for Improving Critical Infrastructure Cyber Security, version 1.1, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[3] Vance, Bill. “Employees are your greatest assets… in security too!” March 2001. www.techxans.org/resources/techxans.ppt

[4] Erica Olsen (2012). Strategic Planning Kit for Dummies, 2nd Edition. John Wiley & Sons, Inc.

[5] Max Mckeown (2012), The Strategy Book, FT Prentice Hall.

[6] Rumelt, Richard P. (2011). Good Strategy / Bad Strategy. Crown Business. ISBN 978-0-307-88623-1.

[7] Adner, R., Zemsky, P., 2005. Disruptive technologies and the emergence of competition.RAND Journal of Economics, 36(2), 229-254.

[8] Stephen G. Haines (2004). ABCs of strategic management : an executive briefing and plan-to-plan day on strategic management in the 21st century

[9] Anthony SD (2004). A diagnostic for Disruptive Innovation. Boston. Harvard Business School Press. Harvard Business School Press.

[10] Afuah, A., Tucci, C. A., 2001. Internet Business Models and Strategies. McGraw Hill, New York.

[11] Bradford and Duncan (2000). Simplified Strategic Planning. Chandler House.