Major Project

on

Protection to Profit: Examining cyber security as a factor in business growth.

Submitted By:

SIDDHARTH VERMA

2K22/EMBA/23

Under the Guidance of :

Dr. Abhinav Chaudhary

Assistant Professor

DELHI SCHOOL OF MANAGEMENT

Delhi Technological University

Bawana Road Delhi 110042

Jan-June 2024

CERTIFICATE

This is to certify that the project titled **“Protection to Profit: Examining cyber security as a factor in business growth”** is a bona fide work carried out by **Siddharth Verma, 2K22/EMBA/23** of 2022-24 batch, and submitted to **Delhi School of Management, Delhi Technological University, Bawana Road, Delhi-110042** in partial fulfillment of the requirement for the completion of a term project in the first semester of **Masters of Business Administration (Executive)**.

Dr. Abhinav Chaudhary

Assistant Professor

Delhi School of Management,

Delhi Technological University

Date: 30/04/2023

DECLARATION

The title of the research paper is **“Protection to Profit: Examining cyber security as a factor in business growth”** I declare that (a) the work presented for assessment in this report is my original work, that is, it has not previously been presented for any other assessment, and that my debts (for words, data, arguments, and ideas)

have been appropriately acknowledged, and (b) work conforms to the guidelines laid by the University. The summary of the report is attached for reference.

Date: 30/04/2023

SIDDHARTH VERMA

R.NO.: 2K22/EMBA/23

ACKNOWLEDGMENT

This paper and the research behind it would not have been possible without the exceptional support of my supervisor, Dr. Abhinav Chaudhary. His enthusiasm, knowledge, and exacting attention to detail have been an inspiration and kept my work on track from the start to the final draft of this paper.

I would also like to extend my gratitude to Delhi Technological University, for giving us the opportunity to present this research and update and enrich our knowledge

Date: 30/04/2023

SIDDHARTH VERMA

R.NO.: 2K22/EMBA/23

EXECUTIVE SUMMARY

In the contemporary digital era, the realm of cyber security has emerged as a pivotal element within the operational frameworks of businesses. This research paper delves into the escalating significance of cyber security within the domain of modern business practices, underscored by an increasing dependence on digital technologies coupled with a concurrent surge in cyber threats. Through a comprehensive exploration that includes a review of relevant literature, statistical examinations, and findings from surveys, this study aims to shed light on predominant cyber security measures, the hurdles encountered by businesses in various sectors, and the potential avenues for enhancement.

The investigation begins by acknowledging the indispensable role that digital technologies now play across all facets of business operations. This transformation has been accompanied by a significant increase in the vulnerabilities and risks associated with cyber threats. As enterprises integrate more deeply with digital solutions for efficiency and innovation, the surface area for potential cyber attacks widens, thereby elevating the strategic importance of robust cyber-security methods and actions.

The core of this study involves a detailed analysis of the challenges commonly encountered by organizations in executing effective cyber security strategies. Among the primary obstacles are budgetary limitations, which often restrict the ability of businesses to invest in advanced cyber security infrastructures or to hire skilled professionals. Regulatory compliance also poses a significant challenge, as businesses must navigate a complex landscape of national and international cybersecurity regulations, which can vary significantly and require meticulous adherence to avoid legal and financial penalties.

Human factors play a crucial role as well, with human error often cited as a leading cause of security breaches. The dynamics of human interaction with technology can introduce vulnerabilities, making it imperative for organizations to engage in continuous training and awareness programs for their workforces.

This aspect of cyber security highlights the need for a cultural shift within organizations, promoting a more cyber-aware mindset among all stakeholders.

Addressing these challenges, the paper emphasizes the necessity for proactive risk management strategies. It advocates for a holistic approach that includes not only technological solutions but also considers organizational behavior and culture. Effective cyber security is not solely about deploying the most advanced technologies but also about fostering an environment where every member of the business is cognizant of and obliged to the principles of cyber safety.

The research further explores various strategies to enhance the cyber security posture of businesses. Investment in evolving technologies such as artificial intelligence, machine learning, and blockchain can offer new ways to protect against cyber threats and enhance response mechanisms. Moreover, the development of comprehensive governance frameworks is crucial for defining clear policies, procedures, and responsibilities related to cyber security within an organization.

Additionally, the integration of organizational culture with cyber security efforts is highlighted as a vital component. Leadership within companies must not only support cyber security initiatives but also actively promote a security-oriented culture. This alignment of cyber security objectives with broader organizational goals is essential for creating a resilient security posture.

Collaboration and information sharing between businesses, industry associations, and government agencies are identified as critical elements for building collective cyber resilience. By sharing knowledge, strategies, and threat intelligence, organizations can better anticipate cyber threats and coordinate more effective responses.

The research culminates with a set of suggestions for businesses aiming to fortify their cyber security framework. It suggests that businesses should prioritize cyber security as a central pillar of their operational strategy, endlessly adapting to the ever-growing threat landscape. This includes not

only investing in technology and training but also participating in industry-wide collaborations to enhance collective security capabilities.

In conclusion, as the digital landscape go-on to grow, so too must the approaches to cyber security. Businesses must recognize the strategic importance of cyber security and implement robust, adaptive strategies that safeguard critical assets and ensure operational continuity in an increasingly interconnected world. By embracing a comprehensive, collaborative, and culturally integrated approach to cyber security, businesses can mitigate risks and enhance their resilience against the ever-growing spectrum of cyber threats.

Keywords: *cyber security, business operations, digital technologies, cyber threats, risk management, collaboration, organizational culture, governance, emerging technologies, information sharing*

Table of Contents

Table of Figures

1. INTRODUCTION

In the modern age marked by rapid technological evolution and digital integration, the realm of business operations has undergone a profound transformation. The critical role of cyber security in safeguarding this digital landscape cannot be overstated. As businesses increasingly depend on digital technologies for their core functions—from transaction processing to data storage and customer communications—they face an escalating array of cyber threats that challenge their operational integrity, data security, and reputational standing.

The urgency of fortifying cyber security measures is highlighted by alarming statistical evidence. A 2019 report by the Ponemon Institute calculated the average global cost of a data breach to be a staggering $3.86 million in 2020, a clear testament to the severe financial repercussions of inadequate cyber defenses. High-profile cyber incidents, such as ransomware attacks and massive data breaches, frequently dominate headlines, serving as stark reminders of the vulnerability of digital infrastructures and the sophistication of cyber adversaries.

In response to these challenges, it is crucial for businesses not only to implement robust technical defenses but also to cultivate a comprehensive understanding of the cyber threat landscape. Effective cyber security transcends the mere deployment of technological solutions; it requires a holistic approach encompassing proactive risk management strategies and a pervasive culture of security awareness among all employees. The complexity of the regulatory environment further compounds these challenges, with stringent data protection and privacy regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) imposing rigorous compliance burdens on organizations.

This research paper seeks to undertake an empirical investigation into the cyber security practices adopted by businesses, aiming to illuminate the prevailing levels of security readiness, identify the most pressing challenges, and recommend strategies for enhancing cyber resilience. By delving into the intricacies of cyber security within the business context, this study endeavors to provide actionable insights that can guide effective decision-making and foster enhanced organizational resilience.

The increasing integration of technology into virtually every facet of business operations has reshaped the competitive landscape, enabling efficiency and innovation but also expanding the threat horizon. Cyber threats have grown not only in frequency but also in complexity, ranging from simple phishing scams to advanced ransomware attacks that can paralyze entire organizations. The repercussions of these threats are severe, with potential impacts including operational disruption, financial loss, and significant damage to customer trust and corporate reputation.

Moreover, the digital transformation has led businesses to accumulate vast amounts of sensitive data, elevating the stakes involved in securing this information. The implications of a cyber breach are thus not merely operational but can have profound legal and financial consequences. Organizations face not only the immediate fallout of customer data loss but also long-term reputational damage and substantial regulatory fines.

Internally, businesses grapple with vulnerabilities that stem from within—ranging from human error to insider threats. These internal risks highlight the necessity of a strong cyber security culture within organizations, underpinned by comprehensive training and awareness programs that empower employees to act as the first line of defense against cyber threats.

The regulatory landscape adds an additional layer of complexity to cyber security management. Compliance with laws such as GDPR and CCPA is no longer voluntary but a crucial requirement that businesses must navigate diligently. Beyond mere compliance, these regulations drive businesses to adopt better security practices, thereby not only mitigating risks of non-compliance but also strengthening trust and credibility with customers and partners.

As digital technologies continue to evolve and become further embedded into the core operational processes of industries across the spectrum—from finance and healthcare to manufacturing and retail—the dependency on these technologies grows. This evolution brings to light new cyber security challenges and threats that are increasingly sophisticated and difficult to manage. Cyber criminals exploit every opportunity, targeting interconnected systems and the expanding array of Internet-enabled devices to conduct their attacks.

The proliferation of the Internet of Things (IoT) and the rapid adoption of technology such as cloud-computing have introduced new vulnerabilities and attack vectors into the cyber landscape. IoT devices often lack robust security features, making them prime targets for cyber attacks, while cloud computing, despite its benefits of scalability and flexibility, brings complexities in data security management that can lead to data breaches if not properly managed. Against this backdrop, this study asserts that it is imperative for businesses to not only focus on strengthening their technological defenses but also to enhance their strategic approaches to cyber security. This includes adopting encryption, multi-factor authentication, and sophisticated intrusion detection systems, as well as investing in proactive threat intelligence and effective incident response strategies. These measures are crucial for businesses to protect their digital assets and maintain continuity in the face of evolving cyber threats.

By exploring these aspects, this research targets to support to the broader discourse on cyber-security in business, proposing frameworks and strategies that can help businesses navigate the complex cyber threat landscape effectively. The findings are intended to equip business leaders with the knowledge and tools necessary to enhance their security postures, ensuring that cyber security is interwoven with the fabric of their business operations and aligned with their overarching strategic objectives.

1.1 Operational Definitions

Cyber Security posture: An organization's overall cybersecurity readiness, reflecting its defenses for systems, networks, and data.

Cyber Initiative: Cybersecurity initiatives are programs, campaigns, or projects designed to improve various aspects of cybersecurity.

Cybersecurity Initiatives Address

Technical Safeguards: Firewalls, encryption, vulnerability management.

Risk Management: Audits, policies, incident response plans.

User Education: Training on phishing, passwords, browsing habits.

Governance: Security policies, compliance with regulations.

Collaboration: Information sharing with industry and law enforcement.

1.2 Objective Of The Study

1. To study the impact of cybersecurity awareness among employees on business growth.

2. To study the impact of investments in cybersecurity initiatives on business growth.

1.2.1 Hypothesis:

H01: Cybersecurity awareness among employees leads to increased business growth.
H02: Increased investment in cybersecurity initiatives leads to business growth.

The study will benefit in the following ways:

- In getting insight into business growth metrics alongside measurable changes in cybersecurity awareness
- In getting insight into how cybersecurity spending yields a positive return that fuels growth.

1.3 Importance and Impact of Cyber Security on Modern

Cybersecurity is critical to protecting the vast arrays of data that businesses collect and store. From customer information to trade secrets, the need to secure sensitive data against unauthorized access and cyber attacks is paramount. Companies face threats not only from external actors, such as hackers and cyber-terrorists but also from internal threats, including accidental breaches or intentional sabotage by disgruntled employees. Effective cybersecurity measures help minimize the risk of data breaches, which can result in hefty fines, legal actions, and irreparable damage to a company's reputation. A strong cybersecurity posture is increasingly seen as a competitive advantage. It allows businesses not only to protect their assets but also to foster trust with customers and partners. Studies show that companies that implement thorough cybersecurity strategies achieve higher growth rates compared to their peers with less robust security practices. This correlation highlights the growing expectation from consumers and business partners for stringent data protection standards, making cybersecurity a critical factor in business expansion and sustainability.

Information security, a key component of cybersecurity, focuses on the protection of data from unauthorized access, use, disclosure, disruption, modification, or destruction. In today's data-driven environment, the role of information security is to ensure data confidentiality, integrity, and availability, facilitating smooth business operations and enabling informed decision-making based on reliable and secure data.

1.4 Protecting Business Assets from Cyber Threats

Cyber threats can target various business assets, including digital infrastructure, intellectual property, and customer data. Protecting these assets involves deploying innovative security measures such as firewalls, antivirus software, intrusion detection systems, and comprehensive cybersecurity frameworks that encompass threat detection, incident response, and continuous monitoring.

Regulatory compliance is a significant aspect of cybersecurity. Many industries are subject to regulations that dictate how information is handled and protected. For instance, the General Data Protection Regulation (GDPR) in the European Union imposes strict rules on data privacy and security, providing guidelines that businesses must follow to protect consumer data. Compliance not only avoids legal penalties but also assures customers that their data is handled responsibly.

1.5 Encouraging Trust and Safeguarding Reputation

In the digital age, customer trust is closely tied to a company’s cybersecurity posture. Effective cybersecurity measures reassure customers that their sensitive information is safeguarded, enhancing their trust and confidence in the brand. Trust of customer is decisive for customer retention and can significantly impact the buying decisions of potential customers.

A company’s reputation is one of its most important assets. A single cybersecurity incident can cause significant damage to a brand’s reputation, resulting in lost customers and reduced sales. Proactive cybersecurity measures help prevent such incidents, protecting a company's public image and customer loyalty.

Intellectual property is a valuable asset for many businesses, especially those in technology, manufacturing, and creative sectors. Cybersecurity measures protect these assets from theft or exposure, which is critical for maintaining competitive advantage and fostering innovation within secure environments.

2. LITERATURE REVIEW

The digital revolution has transformed commerce. E-commerce platforms have become the new storefronts, mobile apps the new shopping carts, and online transactions the new cash registers. Yet, beneath the convenience and connectivity of the online world lurk cyber threats that can devastate any business. Data breaches, ransomware attacks, and social engineering scams are just a few examples of the dangers that pose a constant threat to a company's financial well-being, reputation, and even its ability to function.

Understanding the profound implications of cybersecurity and information security for the success (or failure) of a modern enterprise is crucial. Strong cybersecurity practices are no longer optional; they are a fundamental requirement for doing business in the digital age. Just as a physical store would invest in security guards and alarms to protect its inventory and customers, businesses operating online must under understand the cyber-security and willing to devote portions of their annual budget in resilient cybersecurity measures to have their digital assets and customer information defended against the cyber-security risks..

2.1 Previous Studies on Cyber Security in Businesses

Numerous studies have been conducted to explore cyber security practices in businesses across various industries. These studies have contributed valuable insights into the challenges, trends, and best practices in cyber security management. Some key findings from previous research include:

I. **Assessment of Cyber Security Preparedness**: Studies such as those conducted by Ponemon Institute (2019) and Verizon (2020) have assessed the level of cyber security preparedness among businesses. These studies often analyze factors such as the implementation of security controls, incident response capabilities, and investment in cyber security technologies.

II. **Sector-Specific Cyber Security Challenges**: Research has highlighted sector-specific cyber security challenges faced by industries such as healthcare, finance, and manufacturing. For example, healthcare organizations may face unique challenges related to the protection of electronic health records (EHRs) and compliance with healthcare regulations (Takabi et al., 2016).

III. **Small and Medium-Sized Enterprises (SMEs)**: Studies have also focused on cyber security practices among small and medium-sized enterprises (SMEs), recognizing the unique challenges faced by smaller organizations with limited resources and expertise (Herath & Rao, 2017). These studies often explore the barriers to effective cyber security implementation and identify strategies to support SMEs in improving their cyber resilience.

IV. **Impact of Cyber Attacks**: Research has examined the impact of cyber attacks on businesses, including the financial costs, reputational damage, and operational disruptions associated with data breaches and cyber incidents (Anderson & Moore, 2020). Understanding the consequences of cyber attacks is essential for businesses to prioritize cyber security investments and risk mitigation efforts.

V. **Role of humans in Cyber Security**: Studies have highlighted the role of human in cyber security, including employee awareness, training, and behavior. Research has shown that human error and negligence contribute to a significant proportion of cyber incidents, emphasizing the importance of fostering a culture of cyber security within organizations (Singer & Friedman, 2020).

VI. **Regulatory Compliance**: Research has examined the impact of regulatory compliance requirements on cyber security practices in businesses. Studies have explored the challenges of complying with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), as well as the benefits of achieving compliance in terms of data protection and risk management (Gupta, 2019).

Existing research on cyber security practices in various industries offers valuable insights into the diverse challenges and approaches adopted by organizations to protect their digital assets and mitigate cyber risks. Studies conducted by reputable organizations and academic institutions have provided comprehensive overviews of cyber security practices across different sectors.

For instance, the Ponemon Institute's annual "Cyber Resilient Organization" report provides insights into cyber security practices across industries such as healthcare, finance, manufacturing, and retail (Ponemon Institute, 2020). This report offers a comprehensive overview of cyber security trends, challenges, and best practices, based on surveys and interviews with industry professionals.

Similarly, Verizon's "Data Breach Investigations Report" (DBIR) analyzes cyber security incidents and data breaches across various industries, providing a detailed breakdown of attack patterns, vulnerabilities, and incident response strategies (Verizon, 2021). The DBIR offers valuable insights into the industry-specific cyber threats faced by organizations and highlights the importance of sector-specific cyber security measures.

Academic research has also contributed to the understanding of cyber security practices in specific industries. For example, studies examining cyber security practices in the healthcare sector have highlighted the unique challenges related to protecting electronic health records (EHRs), complying with healthcare regulations such as the Health Insurance Portability and Accountability Act (HIPAA), and addressing the increasing frequency of ransomware attacks targeting healthcare organizations (Herath & Rao, 2017; Kambourakis et al., 2018).

In the financial services industry, research has focused on cyber security practices related to payment systems, online banking, and financial data protection. Studies have examined the effectiveness of security controls such as multi-factor authentication, encryption, and fraud detection systems in mitigating cyber risks and protecting sensitive financial information (Kshetri, 2019; IMF, 2020).

Examination of key findings and insights from previous studies offers valuable insights into the prevailing cyber security landscape and sheds light on the effectiveness of existing practices in mitigating cyber risks. Several notable studies have provided comprehensive analyses of cyber security practices across industries, yielding significant findings and insights.

For instance, research conducted by the Ponemon Institute (2020) highlighted the widespread adoption of encryption, multi-factor authentication, and security information and event management (SIEM) systems as key cyber security practices across industries. The study revealed that organizations investing in these technologies experienced fewer data breaches and lower associated costs, underscoring the effectiveness of advanced security controls in mitigating cyber risks.

Similarly, Verizon's Data Breach Investigations Report (DBIR) (Verizon, 2021) identified phishing attacks, ransomware, and credential theft as the most common cyber threats across industries. The report emphasized the importance of employee training and awareness programs in combating phishing attacks and highlighted the critical role of incident response planning in mitigating the impact of ransomware incidents.

Academic research has also contributed valuable insights into cyber security practices and their effectiveness. Studies examining the impact of regulatory compliance on cyber security outcomes have found that organizations subject to stringent regulatory requirements tend to invest more in cyber security measures and experience lower rates of data breaches (Gupta, 2019). These findings underscore the role of regulatory frameworks in driving improvements in cyber security practices and reducing cyber risk exposure.

Furthermore, research focusing on specific industries, such as healthcare and finance, has revealed sector-specific cyber security challenges and best practices. For example, studies in the healthcare sector have highlighted the importance of securing electronic health records (EHRs) and complying with healthcare regulations such as the Health Insurance Portability and Accountability Act (HIPAA) (Herath & Rao, 2017). Similarly, research in the financial services industry has emphasized the need for robust authentication mechanisms and fraud detection systems to protect sensitive financial data (Kshetri, 2019).

2.2 Key Concepts and Frameworks in Cyber Security

Fundamental concepts in cyber security, such as threat, vulnerability, and risk, are essential components in understanding and managing cyber security effectively. These concepts provide a framework for identifying, assessing, and mitigating cyber risks within an organization's digital environment.

1. **Threat**: With of cyber security background, a threat refers to any potential occurrence, human or automated, that can cause harm to digital assets, systems, or networks. Threats can take various forms, including malware infections, phishing attacks, denial-of-service (DoS) attacks, and insider threats (NIST, 2020). Threats are characterized by their capability to exploit vulnerabilities and disrupt or compromise the confidentiality, integrity, or availability of information assets.

2. **Vulnerability**: A weakness or flaw in a system, application, or process that can be exploited by a threat to compromise security. Vulnerabilities can arise from software bugs, misconfigurations, design flaws, or inadequate security controls (ISO/IEC, 2018). Exploiting vulnerabilities enables threat actors to gain unauthorized access, escalate privileges, or execute malicious activities, leading to potential security breaches and compromises.

3. **Risk**: Risk in cyber security denotes to the probability for harm or loss which is derived from the exploitation of vulnerabilities by threats. It encompasses the likelihood of a security incident occurring and the magnitude of its impact on an organization's operations, assets, and reputation (NIST, 2018). Risk is often expressed as a combination of

the probability of a threat exploiting a vulnerability and the potential consequences of such an exploit. Organizations conduct risk assessment in-order to identify, prioritize and treat risk, by implementing the security measures and allocating resources effectively to treat identified risks.

4. **Data Breach:** It is an event where-in information which is of sensitive or confidential nature is stolen or unauthorized entity access it. This can include customer data, financial records, intellectual property, and employee information. Data breaches leads to identity theft, financial loss, and reputational harm.

5. **Ransomware**: Software which is of malicious nature and works by encrypting a files on victim system and leading to a situation where a payment is demanded for restoring the files back to normal or un-encrypted state. This type of attack can cripple a business if backups aren't in place. Ransomware attacks are becoming increasingly common and sophisticated, and businesses of all sizes are at risk.

6. **Social Engineering:** Manipulative tactics cybercriminals deploy to manipulate people into giving up information and or access to secure systems which are sensitive and confidential in nature. Social engineering attacks can be very convincing, and they often prey on people's fear, trust, or sense of urgency. Examples of social engineering include phishing emails, phone scams, and pretexting (where the attacker impersonates a legitimate person or organization).

7. **Compliance**: Meeting government or industry regulations regarding data security. Non-compliance may lead to penalization in terms hefty fines, damage reputations, and even criminal charges. Compliance requirements can vary depending on the industry and the type of data being collected and stored. However, some common regulations include the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States.

8. **The CIA triad**, comprised of Confidentiality, Integrity, and Availability, is a fundamental concept in cyber security management that serves as a guiding principle for protecting information assets and ensuring the security of digital systems and networks. Each component of the CIA triad plays a crucial role in safeguarding data and mitigating cyber risks, and together they form the foundation of effective cyber security practices.

    a. **Confidentiality**: Confidentiality refers to the assurance that information is accessible only to authorized individuals, entities, or processes. Protecting the confidentiality of sensitive data is essential for preventing unauthorized access, disclosure, or exposure of confidential information to unauthorized parties. Measures such as encryption, access controls, and user authentication help enforce confidentiality and restrict access to sensitive data to authorized users or entities. Confidentiality ensures that sensitive information, such as personal identifiable information (PII), financial data, or trade secrets, remains protected from unauthorized disclosure or exploitation.

    b. **Integrity**: Integrity relates to the trustworthiness and reliability of information assets and ensures that data remains accurate, complete, and unaltered throughout its lifecycle. Maintaining data integrity involves protecting against unauthorized modification, deletion, or tampering of information by unauthorized parties. Techniques such as data validation, digital signatures, and checksums help verify the integrity of data and detect any unauthorized changes or alterations. Ensuring data integrity is crucial for preserving the reliability and trustworthiness of information assets and preventing the manipulation or corruption of data, which could lead to erroneous decision-making or financial losses.

c. **Availability**: Availability refers to the accessibility and usability of information assets and ensures that authorized users have timely and uninterrupted access to critical data and resources when needed. Protecting availability involves mitigating disruptions, outages, or denial-of-service (DoS) attacks that could render systems or services inaccessible to users. Redundancy, fault tolerance, and disaster recovery planning are essential measures to ensure high availability and resilience against cyber attacks or natural disasters. Maintaining availability is vital for sustaining business operations, delivering services to customers, and preventing disruptions that could impact productivity or revenue.

The significance of the CIA triad in cyber security management lies in its comprehensive approach to addressing key security objectives: preserving confidentiality, maintaining integrity, and ensuring availability of information assets. By adhering to the principles of the CIA triad, organizations can develop robust cyber security strategies, implement appropriate controls and safeguards, and mitigate cyber risks effectively. Moreover, the CIA triad serves as a framework for evaluating the effectiveness of cyber security measures and guiding decision-making to prioritize security investments based on the criticality of data and the organization's risk appetite.

2.3 Introduction to Widely Recognized Cyber Security Frameworks

Cybersecurity compliance frameworks empower organizations to systematically manage cybersecurity risks and safeguard critical data. They streamline risk assessment, mitigation, and monitoring, demonstrably reducing the attack surface and protecting sensitive information.

2.3.1 Compliance Frameworks in Cybersecurity

Cybersecurity compliance frameworks provide organizations with prescriptive guidance for managing risks and protecting information assets. Here's an overview of the most widely recognized frameworks:

- **NIST Cybersecurity Framework (CSF):** A versatile and risk-based framework that promotes a holistic approach to cybersecurity. The CSF's five core functions (Identify, Protect, Detect, Respond, Recover) offer a comprehensive methodology for organizations of varying sizes and industries. Its widespread adoption, particularly in the United States, makes it a globally recognized benchmark.
- **ISO/IEC 27001/27002:** These international standards establish the foundation for implementing and maintaining an Information Security Management System (ISMS). ISO 27001 defines the requirements for an ISMS, while ISO 27002 provides best practice recommendations. Achieving ISO 27001 certification demonstrates an organization's dedication to data security.
- **SOC 2:** This regulation broadly targets the attention on controls related to security, availability, processing integrity, confidentiality, and privacy relevant to service providers. SOC 2 compliance is crucial for cloud service providers and companies handling sensitive client data.
- **PCI DSS (Payment Card Industry Data Security Standard):** Mandatory for any organization involved in the processing, storage, or transmission of payment card data. It provides rigorous standards for safeguarding cardholder information.
- **HIPAA (Health Insurance Portability and Accountability Act):** This regulation aims to safe-guard the privacy and security of protected health information (PHI). Healthcare providers, insurers, and any organization handling medical data are under this regulation.
- **GDPR (General Data Protection Regulation):** This regulation provided by EU, come with global reach that emphasizes data privacy and the protection of personal information for EU citizens. This is applicable on any organization dealing out with the data of EU residents.

2.3.2 Additional Frameworks of Significance

- **NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection):** Sets standards for cybersecurity within the bulk power system in North America.
- **FISMA (Federal Information Security Management Act):** A US regulation governing cybersecurity practices for federal agencies and their contractors.
- **COBIT (Control Objectives for Information and Related Technologies):** Framework by ISACA, focused on governance and management of information technology.

2.3.3 The Indispensable Advantage of Cybersecurity Compliance Frameworks

Cybersecurity compliance frameworks offer a compelling value proposition for organizations of all sizes and across industries. Here's a closer look at the advantages they provide:

Streamlined Risk Management: Frameworks establish a structured methodology for comprehensively identifying, assessing, mitigating, and continuously monitoring cybersecurity risks. Organizations can make the most out of their resources by streamline their security efforts with proactive approach.

Enhanced Security Posture: Compliance with industry-recognized frameworks translates into implementing a robust set of security controls. These controls safeguard sensitive data, strengthen system defenses, and bolster an organization's overall cybersecurity resilience.

Alignment with Best Practices: Frameworks embody the collective wisdom and experience of cybersecurity experts. Stakeholders trust and confidence are boosted when the organizations maintains adherence to the best practices.

Regulatory Compliance: Many frameworks are designed to align with specific legal and regulatory requirements. Following these frameworks helps organizations stay on the right side of the law and avoid hefty fines or penalties.

Competitive Gain: Modern world which is highly data driven, a strong cybersecurity posture is no longer a luxury, but a business imperative. Demonstrating compliance through a recognized framework can give organizations a competitive edge by signifying trustworthiness and reliability to clients and partners.

2.4 Emerging Trends and Innovations

Recent trends and innovations in the field of cyber security encompass a wide range of developments aimed at addressing evolving cyber threats and challenges. Some notable trends include the rise of ransomware-as-a-service (RaaS) models, increasing sophistication of phishing attacks, adoption of cloud-native security solutions, and the growing importance of supply chain security. Additionally, there has been a surge in the use of zero trust architectures, threat intelligence sharing platforms, and security automation and orchestration tools to enhance cyber resilience and incident response capabilities.

Developments in know-hows such as artificial intelligence (AI), machine learning (ML), and blockchain are revolutionizing cyber security practices. AI and ML algorithms enable predictive analytics, anomaly detection, and behavior-based threat detection, enhancing the ability to identify and mitigate cyber threats in real-time. Blockchain technology offers decentralized and tamper-resistant data storage, facilitating secure transactions, identity management, and data integrity verification. These technologies play a crucial role in augmenting cyber security defenses, improving threat detection and response, and strengthening resilience against cyber-attacks.

The emergence of new trends and innovations in cyber security has significant implications for business cyber security strategies. Organizations must adapt to these trends by incorporating advanced technologies, adopting proactive security measures, and enhancing collaboration with industry partners and stakeholders. AI and ML-driven security solutions enable organizations to program their business and IT process for any threat detection and response, reducing reliance on manual intervention and improving operational efficiency. Blockchain-based solutions offer opportunities for secure data sharing, supply chain transparency, and immutable audit trails, enhancing trust and accountability in business transactions. However, organizations must also address challenges such as privacy concerns, regulatory compliance, and the skills gap in adopting and implementing these emerging technologies effectively.

In summary, recent trends and innovations in cyber security, including progressions in technologies such as artificial Inteligen, Machine Learniing, and blockchain, are reforming business cyber security strategies. By embracing these trends and leveraging innovative solutions, organizations can augment their cyber resilience, protect against emerging risks, and maintain a competitive edge in an increasingly digital and interconnected landscape.

3. RESEARCH METHODOLOGY

3.1 Research Design Process

For the present study, 107 respondents were chosen comprising 62 males and 45 females participants. The sample consisted of respondents who were working professionals across public and private companies. The sampling technique used was non-probability technique of purposive- incidental sampling. Purposive sampling was used to serve the research purpose in the mind and the sample chosen served this purpose that is working to examine how cyber security plays out in business growth across companies through the selected sample. Incidental sampling was used as all those who matched the selection criteria that is of being a working professional were chosen. Exploratory study was undertaken to get to seek an understanding of cybersecurity as a factor in business growth. A survey is the most appropriate technique for exploratory research, which is the main reason it is used in the current study. To qualify, participants had to fill the screening questions in order to ensure that they fulfilled all the necessary criteria for being in the sample.

3.2 Data Collection Methods

Survey is a structured approach to collect data and produces information that is inherently statistical in nature. For the present study, the survey questionnaire was utilized as an instrument for data collection. Since the sample consisted of working professionals, therefore taking into consideration their tight work schedule, survey was sent to the respondents to maintain flexibility and comfort.

3.3 Procedure

After selecting the topic for the present study, reviews of past literature were carried out with the purpose of gaining familiarity and an understanding of the research study which led to detailed understanding regarding the research objectives, the sample for the research and the research questions.

Thus, it was decided to take two variables i.e. of gender (males and females) and age (18-25 and 45- 55 years). The next step involved construction of the survey questionnaire

and google form was created for the same. Pilot survey was conducted on 2 participants. The next step was reaching out to the participants, making contact with them, taking their permission and informed consent for the study. The participants were asked to reach out to the researchers in case of any concern or query. This was followed by the participants filling up the demographic questions and then the survey questionnaire. After it was ensured that all the participants had filled the form and data were cross verified from the excel sheet, it was closed for responses and the data was compiled.

4. ANALYSIS & INTERPRETATION

4.1 Analysis

In this study, descriptive statistics, a fundamental type of basic statistics commonly employed by researchers to characterize fundamental patterns in data, was utilized to analyze the data gathered from the survey. It characterizes numerical data by categorizing it according to the number of variables involved: univariate, bivariate, or multivariate (for one, two, and three or more variables, respectively). The collected data was bifurcated based on gender, age, annual family income, and occupation. The responses were automatically transferred to a Google Sheets file. All repetitive and incomplete responses were deleted from this Excel file. The response sheet is included in Appendix 2. Following the collection of survey data, all responses were concurrently presented in graphical formats such as pie charts, stacked bars, and bar graphs to facilitate comparisons among participant responses. The detailed findings are included in the Results section.

Results

Question 1: Are you a working professional?

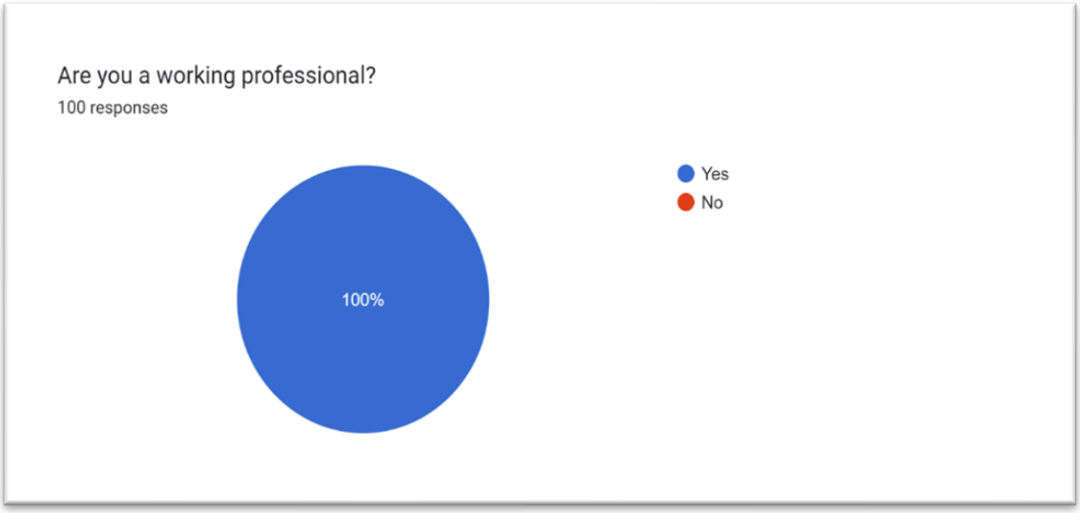


Figure 4. 1: Pie chart representation of response for question 1.

Question 2: Please select your qualification level

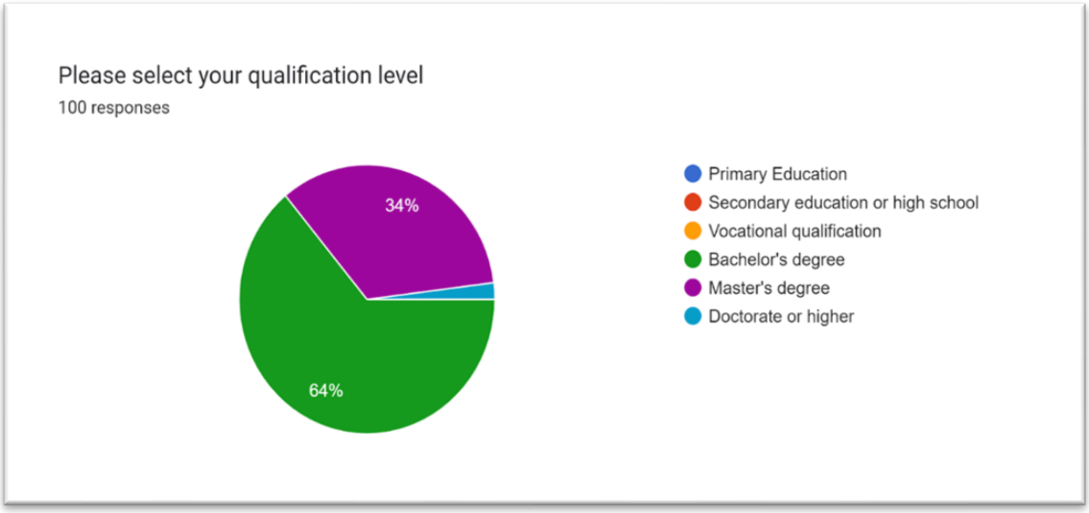


Figure 4. 2: Pie chart representation of response for question 2.

Question 3: Please select the industry your organization is currently operating in.

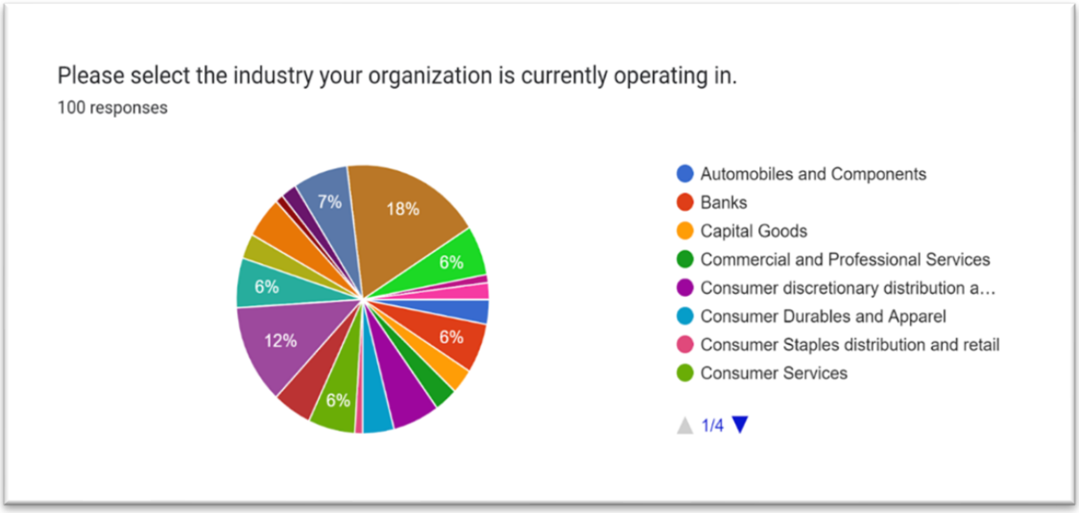


Figure 4. 3: Pie chart representation of response for question 3.

Question 4: Please select the number of employees in your organization

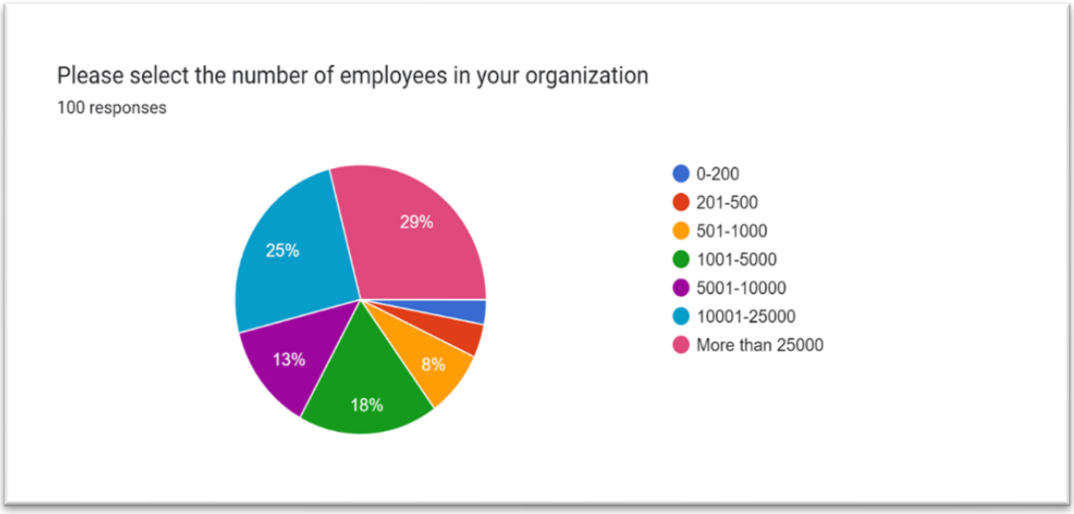


Figure 4. 4: Pie chart representation of response for question 4.

Question 5: Please select the annual revenue bracket of your organization.

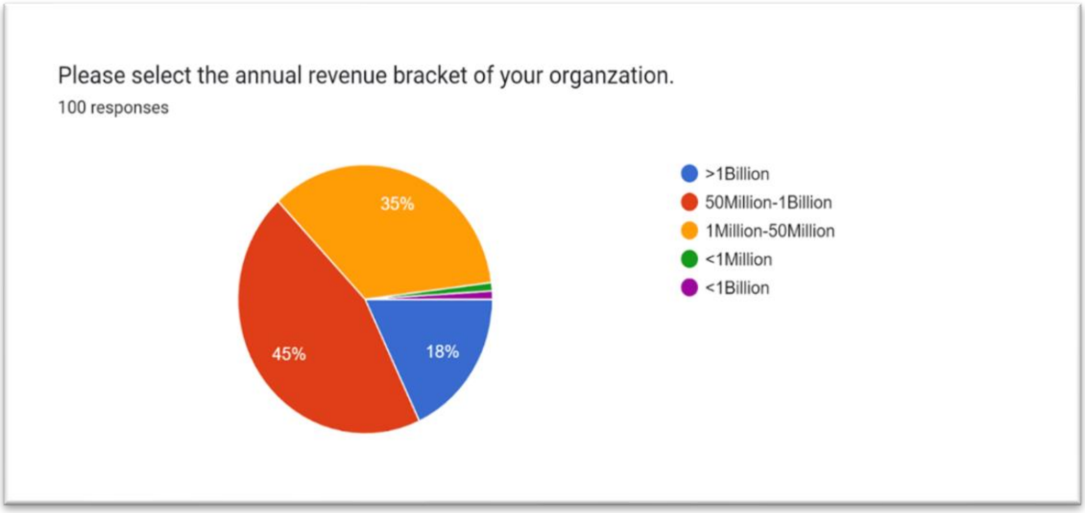


Figure 4. 5: Pie chart representation of response for question 5.

Question 6: How would you rate you organizations's cyber security posture?

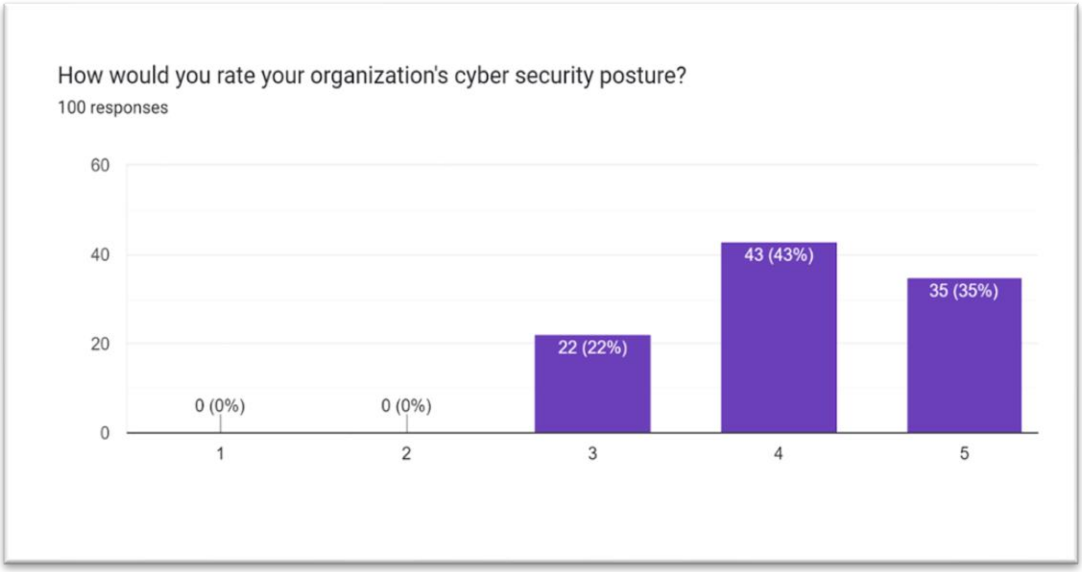


Figure 4. 6: Bar chart representation of response for question 6.

Question 7: How would you rate your organization's capabilities such as Firewall, Multi-factor authentication, Access Management, etc. as adequate to protect the organization from malicious attacks?

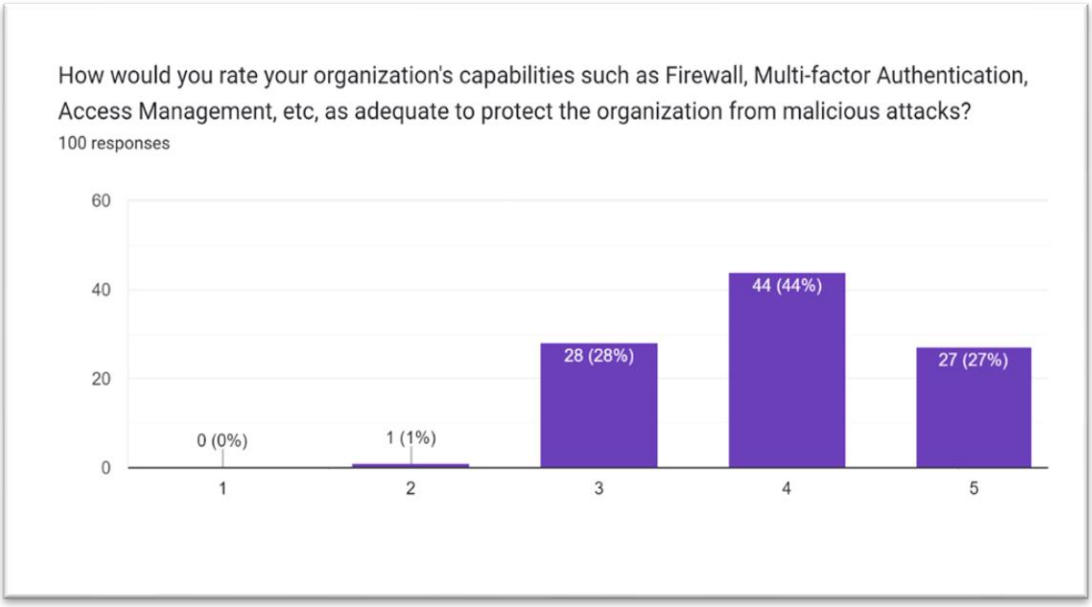


Figure 4. 7: Bar chart representation of response for question 7.

Question 8: How would rate your understanding of cyber security's potential impact on business operations?

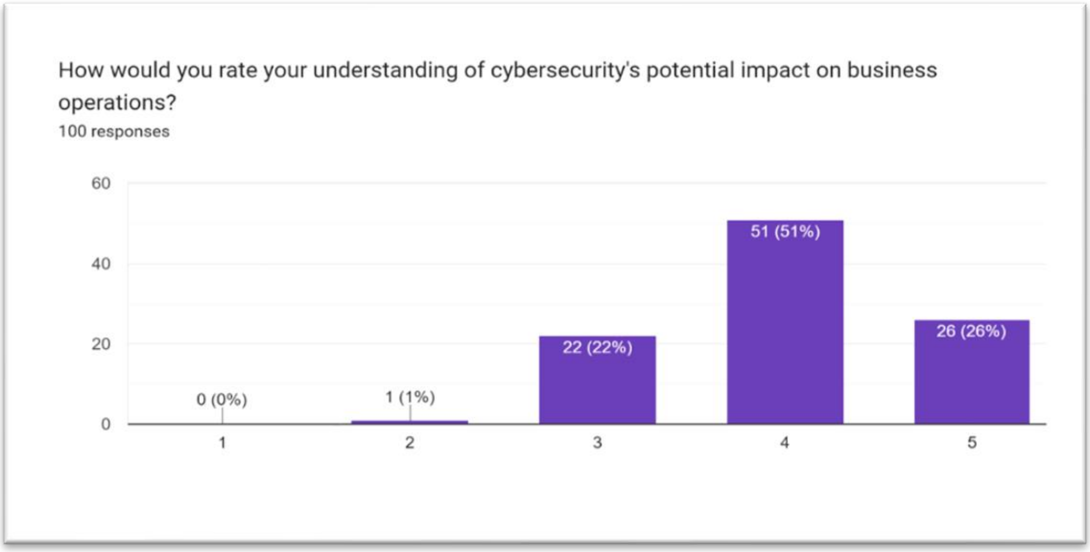


Figure 4. 8: Bar chart representation of response for question 8.

Question 9: Do you agree that enhanced awareness of cyber security contributes to the strong security posture of the company?

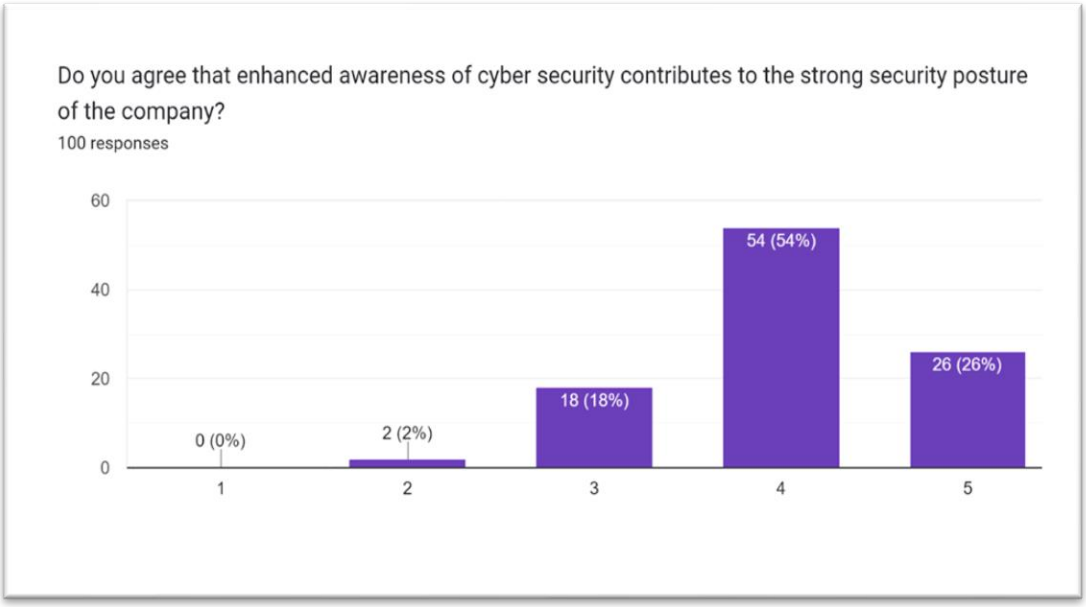


Figure 4. 9: Bar chart representation of response for question 9.

Question 10: Do you agree cyber security awareness training helps in business growth?

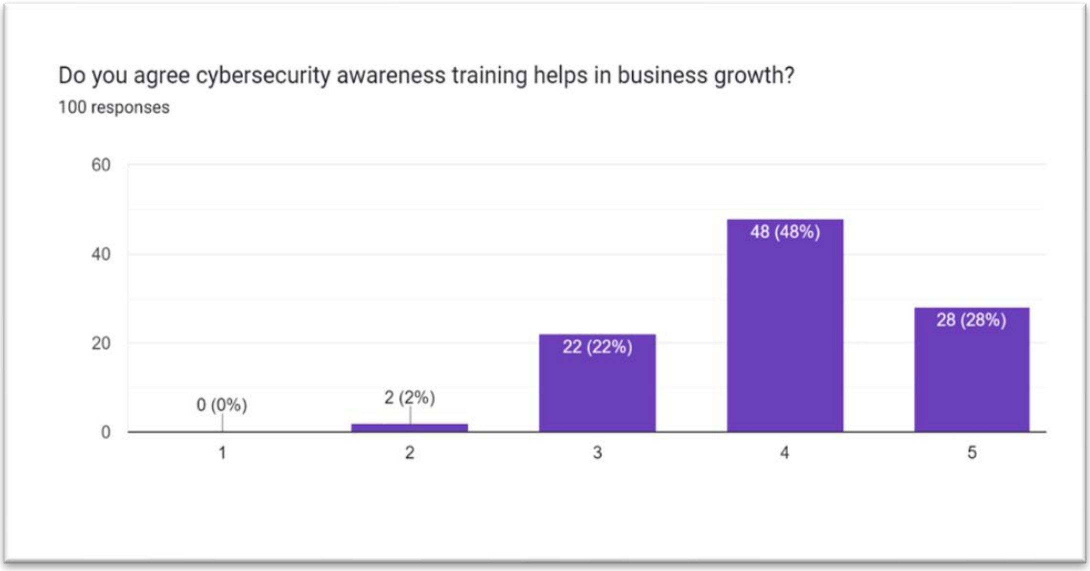


Figure 4. 10: Bar chart representation of response for question 10.

Question 11: Do you agree that increased cyber security resilience through cyber security initiatives brings in more investment for the company?

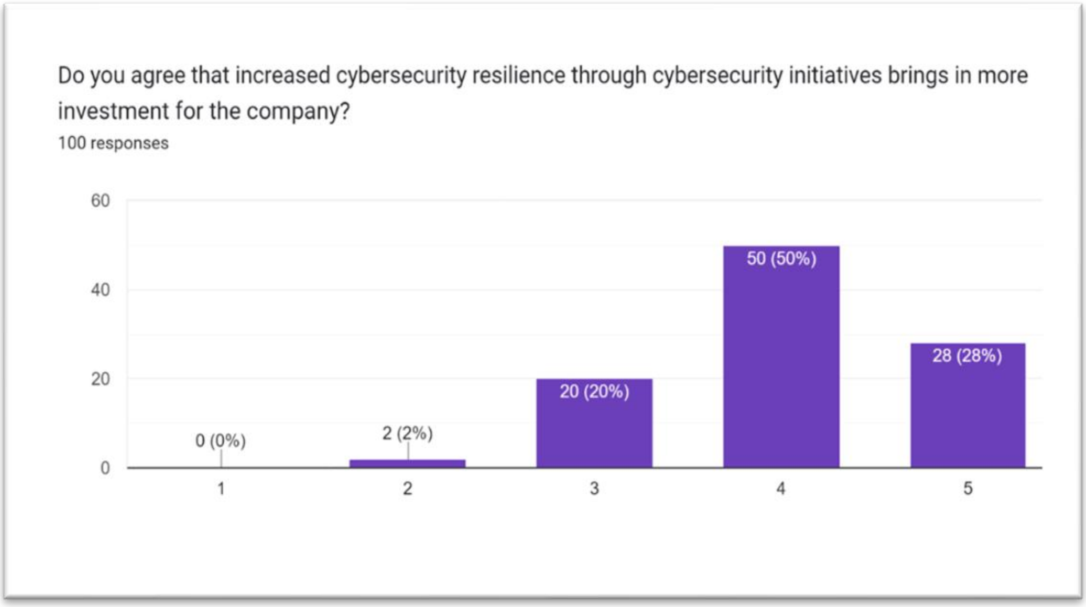


Figure 4. 11: Bar chart representation of response for question 11

Question 12: How much has your company invested in cyber security initiatives in the last financial year, 2022-23?

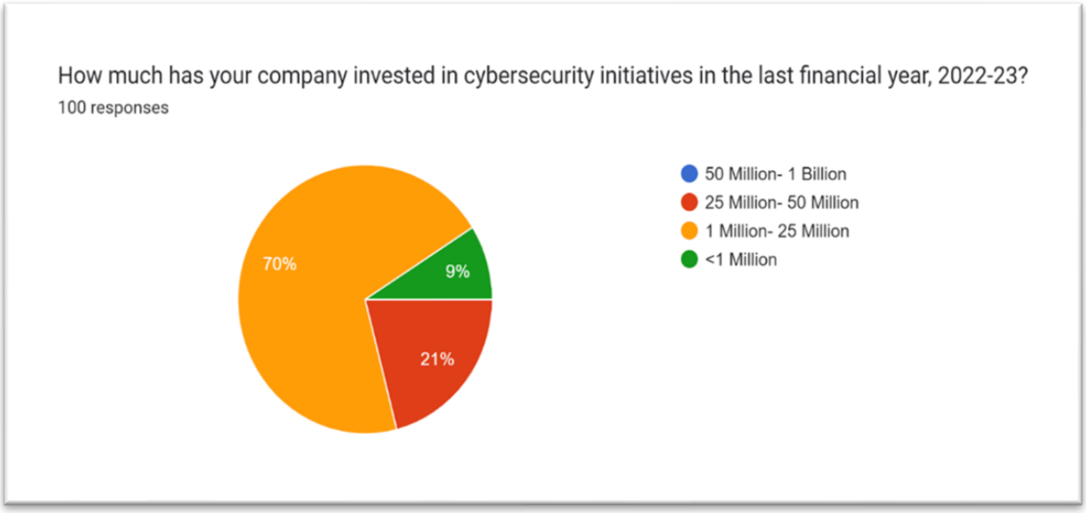


Figure 4. 12: Pie chart representation of response for question 12

Question 13: Was there an increase of your company's percentage change in revenue in 2022-23, considering any cyber security initiatives taken?

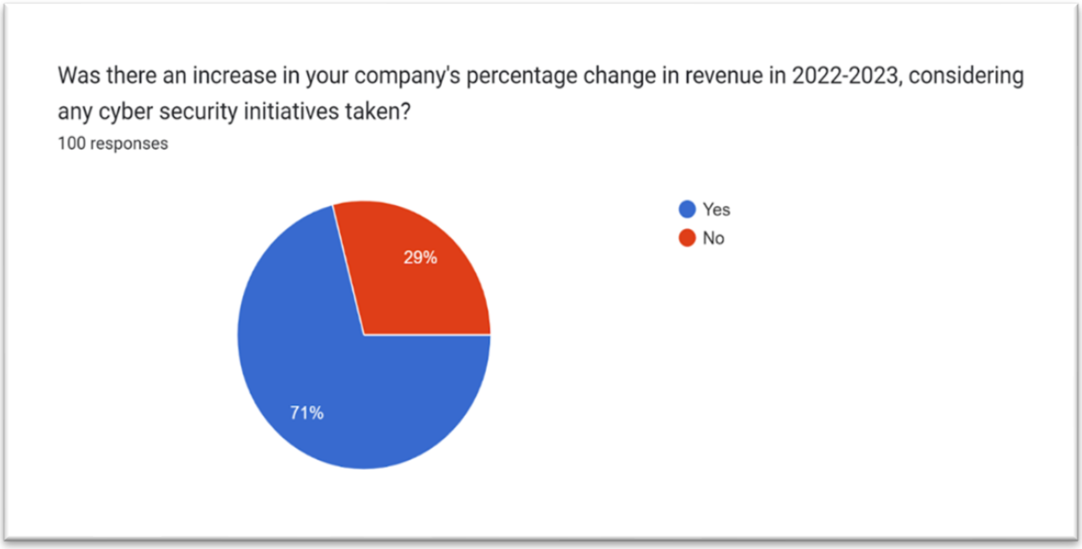
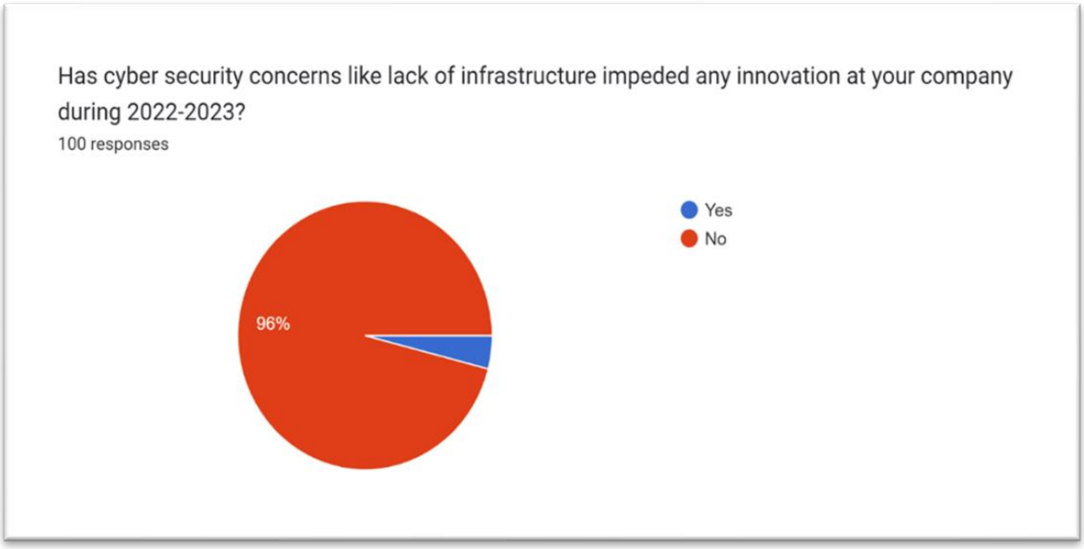


Figure 4. 13: Pie chart representation of response for question 13

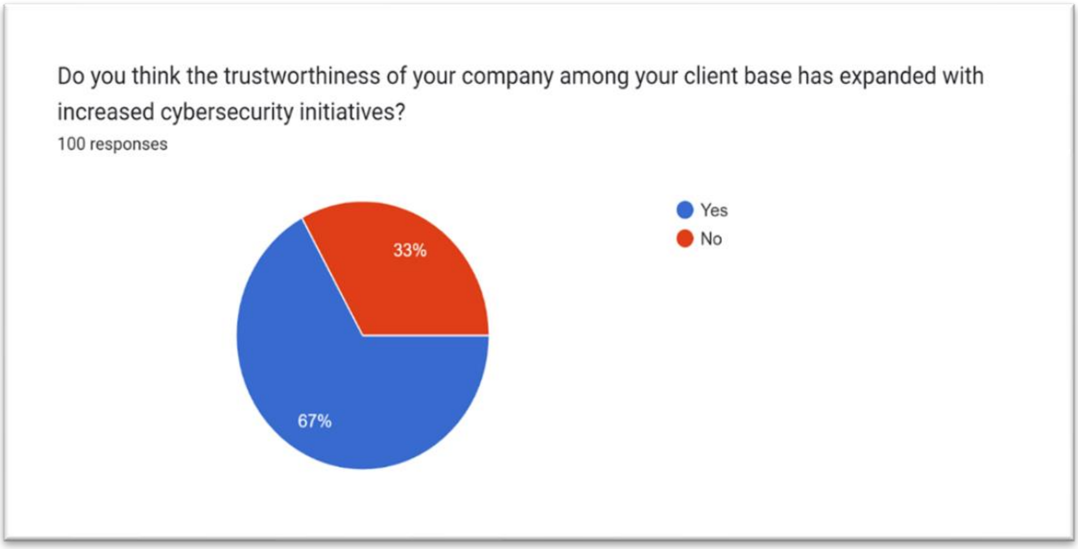
Question 14: Has cyber security concerns like lack of infrastructure impeded any innovation at your company during 2022-23?


Has cyber security concerns like lack of infrastructure impeded any innovation at your company during 2022-2023?

100 responses

Figure 4. 14: Pie chart representation of response for question 14

Question 15: Do you think the trustworthiness of your company among your client base has expanded with increased cybersecurity initiatives?


Do you think the trustworthiness of your company among your client base has expanded with increased cybersecurity initiatives?

100 responses

Figure 4. 15: Pie chart representation of response for question 15

Question 16: Do you think cyber-secure brand image provides a competitive edge to the company?

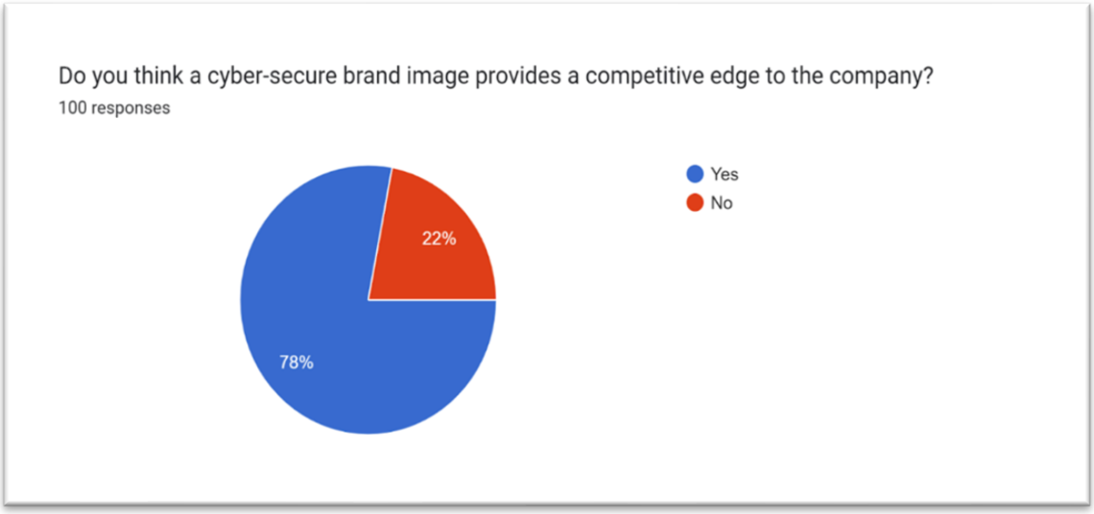


Figure 4. 16: Pie chart representation of response for question 16

4.2 Interpretation & discussion

This present study was conducted to analyze the impact of cybersecurity awareness among employees on business growth and also the impact of investments in cybersecurity initiatives on business growth. For the present study, working professionals were selected and incorporated non-probability sampling, i.e. purposive and incidental sampling. The sample size was 100 with a mix of females and males. Data was collected using a Google form. Descriptive statistics was used to analyze the data.

A few screening questions were added to the survey, and those participants who fulfilled the criteria went on to fill out the survey while those who couldn't meet the specified criteria were screened out from the survey. Fortunately, all of the participants were working professionals.

As can be seen from Figure 4.1 on the question asking whether the participants were working professionals, all 100 responses responded ‘yes’, and therefore none was screened out. The rationale for choosing this question was as such we were examining the impact of cybersecurity awareness and business growth on business growth and therefore those who are working in the companies whether private or public sector would be able to provide us with a complete image regarding how much cybersecurity is valued in contemporary times and how much it contributes to the expansion of businesses.

These participants then moved on to provide their demographic information.

As can be seen from Figure 4.2 on the question asking the qualification of the participants, out of 100 participants, the maximum number of the participants i.e., 64% (64 participants) hold bachelor’s degrees while 34% (34 participants) hold a master’s degree and the remaining 2% had a doctorate or hold a higher degree.

As can be seen from Figure 4.3 on the question asking the industry participant's organization is operating, out of 100 participants, the maximum number of participants, i.e., 18% were working in an industry related to software and services, 12% were providing financial services, while 7% were working in real estate management and development industry, 6% were working in food, beverage and tobacco industry, other 6% participants were providing consumer services, other 6 % were in consumer discretionary distribution and retail industry, other 6% were working in banks, other 6 % were in technology hardware and equipment industry, 5% participants were working in energy sector, and other 5% were working in insurance industry. 4% were working in the apparel industry, while 3% were working in the healthcare equipment and services industry, the other 3% were providing commercial and professional services, another 3% were in the capital goods industry, and another 3% were engaged in the automobile industry. Of the remaining participants, 2% were in the transportation industry, another 2% were engaged in the media and entertainment industry, 1% were in telecommunication services, the other 1% were in the materials industry and the last 1% were involved in the consumer staples distribution and retail industry.

As can be seen from Figure 4.4 on the question asking the number of employees in participants' organizations, it was found that the maximum number of participants, i.e., 29% of participants were employed in big firms with a workforce of more than 25000, followed by 25% participants working in firms with a workforce oscillating between 10001-25000. While 18% were working in firms with a workforce between 1001-5000, 13% were working in firms with employee strength between 5001-10000, 8% were working in firms with a workforce between 501-1000 and the remaining 4% and 3% of participants were working in medium enterprises incorporating 201-500 and 0-200 employees respectively.

As can be seen from Figure 4.5 on the question asking the annual revenue participants' organizations, it was found that the maximum number of participants, i.e., 45% of participants were working in firms with annual revenue oscillating between 50 million-1billion, followed by 35% participants working in firms with annual revenue between 1 million-50 million. 18% of participants have worked with firms whose annual revenue is more than 1 billion while 1% were working for firms whose annual revenue is less than 1 million and the remaining 1 % worked in firms with less than 1 billion. Thus, a large amount of the participants were working in firms with large revenue turnovers meaning that they had large capabilities and resources at their disposal.

As can be seen from Figure 4.6 the question asks how would the participants rate their establishment's cyber-security posture (strength and resilience of an organization against cyber-security risks). A maximum number of participants, i.e., 43% have responded the ‘strong’ on the Likert scale corresponding to the number 4, followed by 35% responding ‘very strong’ on the scale, and the remaining 22% of participants have responded ‘average’ on the scale corresponding to the number 3. It was found that none of the participants responded ‘very poor’ or ‘poor’ in terms of the question. Thus, it can be inferred from the response pattern that cybersecurity as a significant measure is recognized by the companies regardless of the private or public sector and regardless of the size of the companies. For instance, small businesses are highly exposed to cyber-attacks and therefore they need to improve their cyber posture (Hiscox Cyber Readiness Report, 2023). From the responses, it can be inferred that the importance of good posture has been recognized with increased awareness among the companies and the employees. This has been supported by the study carried out by Li, et al., (2019), which found that increased awareness among employees of their organization’s security policy and procedure leads to them being more cautious and effective in handling cyber attacks as compared to those who were unaware of these policies.

As can be seen from Figure 4.7 addressing the question regarding the organization’s capability to protect from malicious attacks, 44% of participants responded ‘agree’ and 27% ‘strongly agree’ with the fact that firewalls, MFA, etc are adequately protecting against cyber attacks. Only 1 respondent rated their organizational capability to be less effective or ‘poor’ in dealing with attacks. While 28% of respondents have an ‘average’ take on their company’s capability to provide a strong defense against cyber attacks. None of the respondents have responded ‘very poor’. In short, it can be said while looking at the responses, that the companies realize the importance of securing data as well as employees too are aware of the company’s cyber initiatives and steps. It can be further understood that companies are investing in building defensive cybersecurity infrastructure as a lack of capability can also lead them to lose their clients and investors. This has been supported by an increase in cyber security budgets by 14.3% worldwide to amp up their infrastructure to capitalize on the risks presented (Pratt, 2024). The enhanced infrastructure could be attributed to the fact that with enhanced breach costs, came an increase in cyber investments in modernizing technology, simplifying and unifying cyber technology, with a focus on creating an all-encompassing resilience program related to cyber (PwC, 2023).

As can be seen from Figure 4.8 addressing the question to understand the employee's knowledge of the potential influence of the cyber-security on business operations. More than 50% of respondents, i.e., 51% agree that cyber security has a great impact on business operations. 26% strongly agree that business operations are impacted by cyber-security and the remaining 22% of participants have responded ‘average’ on the scale corresponding to the number 3. It was found that none of the participants responded ‘very poor’ or ‘poor’ in terms of the question. It can be inferred that cybersecurity impacts are well understood and recognized by employees. Cybersecurity has a make-or-break impact on business as it leads to a huge monetary loss, reputational loss as well as clientele loss to the organization. This enhanced awareness is important for mitigating threats and boosting the organization’s resilience and can be attributed among other factors to the company’s initiatives in cyber training programs. Awareness of employees becomes essential as they can serve as an early warning system. Apart from this lack of awareness can lead them to cause errors like clicking on malicious links, credentials being stolen due to carelessness, or employees delivering data to the wrong recipients can cause the company huge loss (Verizon, 2021). Considering the results of the survey: US State of Cybercrime conducted in year 2014, “42% of respondents said security education and awareness for new employees played a role in deterring a potential criminal, among the highest of all policies and technologies used for deterrence. Companies without security training for new hires reported average annual financial losses of $683,000, while those do have training said their average financial losses totaled $162,000” (Pwc, 2014, p. 14).

As can be seen from Figure 4.9 addressing the question regarding the awareness of cyber security contributes to the strong security posture of the company, the maximum number of respondents, i,e., 54% have responded that awareness of cyber security contributes to the security posture of the company, followed by 26% participant responding that awareness on cyber security strongly contributes to company’s security posture. 18% of respondents have an average take on the question and feel that awareness of cyber security has an average contribution to the overall security posture of an organization. The remaining 2% of participants responded ‘poor’, implying that awareness of cybersecurity doesn’t have any contribution to the security posture of the company. Thus, it can be inferred from the above data that awareness of cybersecurity by employees and companies significantly contributes to security posture because the ability to fight and bounce back comes from the internal strength of the company and its employees. Awareness of the matter helps to avoid or realize a significant threat to the company and timely decisions can be taken.

Since security posture is seen as boosting resilience towards cyber threats, therefore cyber awareness among employees can lead to prioritizing efforts as a closely knit community, which fosters an environment that encourages compliance with institutional and industrial security norms, thereby strengthening the security posture of the company (Andronache, 2021).

With cyber awareness comes an understanding of security components in the local environment including “knowledge of security software versions for integrity management and anti-malware processing, signature deployments for security devices such as intrusion detection systems, and monitoring status for any types of security collection and processing systems”, that enhances the strength of the company to fight against the attack or best prevent it (Amoroso, 2011). At last, it is the knowledge and the use by employees that serve as crucial towards bridging vulnerability gaps and securing the infrastructure and information. As mentioned earlier, this helps to retain clientele while enhancing their trust, ensuring no disruptions in the supply chain, luring investors due to worthy reputation, no suspension of any critical productive processes due to cyberattacks, and lastly, resources being able to be invested in something worthy.

As can be seen from Figure 4.10 addressing the question regarding the awareness training on cybersecurity helps in business growth, 48% of participants agree that cybersecurity training can be helpful and help in business growth, followed by 28% of participants, who strongly agree that business growth can be achieved with awareness training on cybersecurity. 22% of participants responded ‘average’ on the scale corresponding to the number 3 and the remaining 2% responded ‘poor’. Thus, it can be because it is not only helpful in preventing data breaches and attacks as it prevents employees for example from clicking malicious links, but it also creates a cyber-conscious culture where employees have a better understanding and perception regarding what to do and what not to do if faced with a cyber-related issue.

This has been supported by a 2023 study where it was found that cyber-conscious culture helps employees understand potential risks and are likely to make better decisions when handling sensitive information or using the company's devices. This, in turn, reduces both the incidents and the likelihood of security incidents, financial losses, legal liabilities, and reputational damage. These programs can also have a positive impact on the morale and job satisfaction of employees. This is because "when employees feel confident in their ability to protect themselves and the organization from cyber threats, they are more likely to feel a sense of empowerment and ownership in their role within the company. This empowerment can translate into increased productivity and loyalty, contributing to a more resilient and secure work environment" (Negussie, 2023). While those who have responded 'average' or 'poor' may not attribute much benefits to cybersecurity initiatives in impacting business. This could be because even if cybersecurity training is provided, there is a lack of infrastructure and updates in existing cybersecurity software, then training programs and changed perceptions cannot contribute much. For instance, if training programs lack relevance and the cybersecurity measures are outdated then training in them will not contribute much because they cannot assess and respond to changing and growing threats (Page, 2023).

As can be seen from Figure 4.11 addressing the question regarding more initiatives in cybersecurity resilience bringing more investment in the company, the maximum number of participants, i.e., 50% responded 'agree', followed by 28% of respondents who responded 'strongly agree', believe that cybersecurity initiatives help in pitching more investments in a company. 20% of respondents have an 'average' take on the question and 2% of respondents have responded 'poor'. Thus, it can be inferred that strong cybersecurity initiatives are acknowledged and promoted by the investors, as they invest in companies that have strong cybersecurity posture. Therefore, it motivates companies to take a strong footing on building sound cybersecurity infrastructure. This could be because of an increased stable environment and enhanced trust which lures investors. Increased trust to invest and take services would be out of the notion that their money and information are not subject to loss due to fraud or cyberattacks. Therefore, they look for mechanisms that are in place to provide them confidence in terms of protection of their information and money (Ghamsha 2013; Shaker, 2023). A report has found that 76% of respondents believe that cyber-secure brand provides a competitive edge (Hiscox, 2019). Another report indicated that 96% of respondents pointed out that cyber security readiness is taken into consideration when assessing the potential acquisition target's monetary value (ISC2, 2020).

As can be seen from Figure 4.12 addressing the question regarding the investments made by participant organizations in cybersecurity initiatives in the last financial year 2022-2023, the maximum number of participants, i.e., 70% have responded that investments made were between 1 million-25 million, followed by 21% participants responding investments made were between 25 million-50 million. The remaining 9% of participants responded that investments made were less than 1 million. None of the respondents chose the investment bracket corresponding to 50 million-1 billion. Thus, it can be inferred that such large investments by the company in the initiatives mean that companies understand the risk and the threat posed by the lack of cybersecurity initiatives to their business and understand its importance on their business growth.

Large investments can also be attributed to the fact that if there is no strong defense against cyber attacks, then the company loses a large amount of money which it could have directed towards expanding its business or bringing newer technology or for other needs. It was supported by a finding indicating that damage from cyberattacks will lead to a loss of $10.5 trillion annually by 2025 (Morgan, 2022; Aiyer, et al., 2022).

Thus, it is seen as a strategic investment rather than an expense. It has been supported by research by Wadhwani (2023) which pointed out that cybersecurity-related investments bring in more efficiency in terms of operations and these investments entail fulfilling strategic business objectives by helping companies avoid unnecessary costs related to cyberattacks. "It helps organizations associate tangible value to their cybersecurity initiatives and enables them to make informed decisions on future investments and, most importantly, demonstrate that value to executive leadership, stakeholders, and a company's board of directors" (Tehila, 2023).

As can be seen from Figure 4.13 addressing the question regarding the company's percentage change in revenue in the financial year 2022-2023 owing to the cyber security initiatives taken, the maximum number of participants, i.e., 71% have said 'yes', while the remaining 29% have responded 'no'. Thus, it can be inferred from this that cybersecurity initiatives do have an impact on business growth helping it to flourish. The revenue increase could be attributed to the fact that the company saved a large amount of money that it would have lost in cyber attacks due to amped-up technologies and infrastructure. Global cybercrime cost USD 3 trillion in 2015 and is growing and is expected to reach USD 10.5 trillion by 2025 (Morgan, 2020).

However, if proper measures are taken then it could help not only protect from cyber threats but also bring in technological transformation leading to growth in business and value. For instance, in the infrastructure sector, companies that have shown resilience and strength against these cyberattacks have done the hard work to leverage advanced and state-of-the-art cybersecurity technology to navigate cyber-related regulations and cyber threats. For example, BNY Mellon has brought innovation in its digital payment processing by building a payment platform named Vaia along with Verituity, a cybersecurity startup. This has provided a range of payment services, verified the identities of the payee, and prevented payment fraud, leading to operational efficiency, customer experience, and enhanced payment accuracy (Yepez, 2024). Therefore, boosting business.

As can be seen from Figure 4.14 on the question asking does lack of proper cyber security initiatives has impeded any innovation at your company during the last financial year, 2022-2023, a total of 96% of participants have responded 'no' while only a small fraction of 4% have responded 'yes'. This could be attributed to the fact that participant companies (refer Q7) have made large investments in taking cybersecurity initiatives and therefore it has reduced the likelihood of cyberattacks preventing them from maintaining their competitive edge, as they could divert their resources toward more productive outcomes than to recover reputational and monetary costs involved in cyberattacks and boosting their resilience. This is supported by research carried out by Llyod (2020), where 39% of respondents said: "they had halted mission-critical initiatives due to cyber security issues". It was found that organizations can innovate faster owing to their cyber security excellence. This helps them to respond faster to ever-changing markets, making them more adaptable and flexible and thereby improving their financial performance. It helps them to differentiate themselves by establishing trust among its consumers or clients.

The remaining 4% of participants who responded 'yes' even after huge investments could be because they could have failed to keep up with the newer technologies that could have provided them with an advantage. Many times company has this status quo tendency where they may fail to update existing technologies and may continue to invest in other newer technologies. Though it may seem they are investing in newer technologies they keep a window open where they are vulnerable. Thus, faltering on a good approach to cybersecurity initiative. According to a study conducted by Verizon (2024), 73% of breaches occurred due to vulnerabilities that were more than a year old. Failure to update can lead to the company becoming more vulnerable to attacks as software updates contain critical security patches that address the vulnerabilities. It also fails to detect and block malware. The failure to update can also have reputational costs as it leads to non-compliance with standardized industry regulations and legal requirements. Therefore, as m mentioned earlier company has to move its resources to overcome these challenges rather than innovating itself and maintaining a competitive edge (CIT, 2024).

As can be seen from Figure 4.15 on the question asking whether the trustworthiness of the participant company among the client base has expanded with increased cybersecurity initiatives, the maximum number of participants, i.e., 67% have said 'yes', while the remaining 33% of participants have responded ‘no’. Thus, it can be inferred from this that enhanced cybersecurity initiatives provide a stable and secure environment as well as ensure the reputation of the companies for the clients to believe in and take services, while also facilitating investors to invest in such a company. A company prioritizing data-security and its privacy demonstrates a high corporate social responsibility. It would be a financial burden on the company as well to lose a loyal customer or business partner and so demonstrating a strong commitment to security and privacy helps establish trust among the clients and business partners leading to business growth.

Those who have responded ‘no’, may not have encountered any change in an upward or downward manner in the trust level, meaning that clients may have been satisfied with the initiatives taken and continue to trust as in the past. Or it could also be because even after initiatives taken, the security posture may have not been as per the industry standards or improved, such that the clients may not sensed an enhanced trust.

As can be seen from Figure 4.16 on the question asking whether a cyber secure brand image provides a competitive edge to the company, the maximum number of respondents have responded ‘yes’ while the remaining 22% have responded ‘no’. This can be because it helps the company to differentiate itself as a brand that consumers can trust with their data and information. A cyber-secure brand image helps establish an image of operational efficiency as well as divert resources to productive outcomes rather than recover from cyberattacks.

Research findings suggest that a cyber-secure brand image can help organizations improve their organizational security performance in terms of reduced data breaches, efficient security reputation, enhanced security of internal processes, and reliable systems for information processing. This in turn brings additional benefits in terms of sales and revenue growth and intangible performance like well well-established reputation good corporate image and a competitive position (Berlilana, et al., 2021).

Those who have responded ‘no’, maybe because of their lack of understanding of the potential impacts of cybersecurity on business growth. For instance, if we refer back to Q3 where respondents were asked how would they rate their understanding of cybersecurity’s potential impact on business operations, 22% responded ‘average’ while 1 said ‘poor’, which may be indicative of the fact that they may also do not have a sound understanding of how cyber secure image may contribute to a competitive advantage.

In light of the research question “How do employees' cybersecurity awareness and the organization’s investment in cybersecurity initiatives impact business growth?” and the research objective of “studying the impact of cybersecurity awareness among employees on business growth”, it was found through the present study that cyber security awareness among employees leads to enhanced business growth. It was supported for instance through participant’s responses on question 5 which addressed how awareness training is helpful in business growth, wherein 48% of participants responded ‘agree’ on the Likert scale, followed by 28% of participants, who ‘strongly agree’ that business growth can be achieved with awareness training on cybersecurity. While 22% of participants responded as ‘average’ on the scale, and the remaining 2% responded as ‘poor’. The link between cyber awareness training and business growth could be attributed to the creation of a cyber-conscious culture where employees have a better understanding and perception regarding what to do and what not to do if faced with a cyber-related issue. Thereby preventing monetary and reputational damage while boosting the morale and job satisfaction of employees. This is because of the enhanced confidence in their ability to protect themselves and their organizations from cyberattacks, that they feel empowered and ownership in their company’s role. Thus leading to enhanced resilience, productivity, and loyalty (Negussie, 2023). From the above, we can also conclude that the first hypothesis: ‘cybersecurity awareness among employees leads to increased business growth’, is retained, signifying cyber awareness among employees as a tool for enhancing business as they are seen to be the first defense against cyber threats. It is employees who form the environment and the culture of the company and if they are not aware and careful while handling information, they can create an environment that is highly volatile to cyber threats and thus cause a trust deficit among the client base.

Another research objective of the present study was "studying the impact of investments in cybersecurity initiatives on business growth". It was found from the present study that investments made by organizations in cybersecurity initiatives and measures do contribute to enhanced business or business growth. It was supported for instance by participants' responses on Q8 addressing the question regarding the company's percentage change in revenue in the financial year 2022-2023 owing to the cyber security initiatives taken. The maximum number of participants, i.e., 71% have said 'yes', while the remaining 29% have responded 'no'. Thus, it can be inferred from this that cybersecurity initiatives do have an impact on business growth helping it to flourish. This could be attributed to the fact that the company saves a large amount of money that it would have lost in cyber attacks with amped-up technologies and infrastructure. Global cybercrime cost USD 3 trillion in 2015 and is expected to cost USD 10.5 trillion by 2025 (Morgan, 2020). However, if proper measures are taken then it could help not only protect from cyber threats but also bring in technological transformation leading to growth in business and value. For instance, in the infrastructure sector, companies have worked hard to leverage state-of-the-art cybersecurity technologies to navigate cyber-related regulations and cyber threats, boosting business. From the above, we can also conclude that the second hypothesis: 'increased investment in cybersecurity initiatives leads to business growth' is also retained signifying investments in cyber initiatives as a strategic investment rather than an expenditure and that too an unproductive one, as it leads to operational efficiency and escape monetary and reputational costs, helping direct money towards productive measures.

5. CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

In the ever-changing landscape where threats acquire new ways to harm the companies whether private or public, it becomes imperative to gear up against those attacks through awareness and investments while simultaneously promoting business growth. Through the present study, it was found that cybersecurity awareness among employees leads to increased business growth as it contributes towards the creation of cyber cyber-conscious culture, embedding in the employees an understanding of the potential risk cyberattacks pose, and the damage they cause. Increased awareness can be useful in not only preventing the attacks but also creating a positive affiliation for the company as they feel empowered in their agency to prevent both companies and themselves from such attacks, enhancing their productivity levels. Also, it was found that enhanced investments in cybersecurity initiatives contribute to business growth, as investments lead to companies creating a better line of defense against potential cyber-attacks which can prevent them from losing tons of money and rather help them direct their resources and money towards bringing technological change or in other productive measures.

5.2 Recommendations

Align Cybersecurity with Business Objectives

- ✓ Integrate Cybersecurity in Business Strategy: Ensure that cybersecurity measures are not just technical safeguards, but strategic components directly aligned with business goals. Highlight how robust cybersecurity can drive customer trust and, subsequently, revenue growth.
- ✓ Leverage Cybersecurity as a Competitive Advantage: Position your organization as a leader in cybersecurity within your industry. Use this stance to differentiate your company from competitors, potentially capturing a larger market share by attracting customers who value data protection.

Prioritize Return on Investment in Cybersecurity

- ✓ Focus on Cost-Benefit Analysis: When allocating budgets for cybersecurity technologies and initiatives, focus on investments that offer the highest return in terms of risk mitigation and potential cost savings from avoided breaches.
- ✓ Invest in Scalable Solutions: Choose cybersecurity solutions that are scalable and adaptable to evolving business needs and threats. This approach ensures that investments remain relevant and contribute to long-term business sustainability.

Develop a Resilient Incident Response Capability

- ✓ Executive Involvement in Incident Response Planning: As a C-suite executive, take an active role in developing and refining the incident response plan. Understanding its nuances aids in making informed decisions during a crisis, minimizing financial and reputational impact.
- ✓ Establish Clear Communication Channels: Ensure that there are predefined communication strategies both internally and externally for incident handling. This helps in managing stakeholder expectations and maintaining business continuity during and after cyber incidents.

Cultivate a Culture of Security from the Top

- ✓ Lead by Example: Demonstrate a commitment to cybersecurity through personal actions and decision-making. Your stance can significantly influence company-wide attitudes towards security.
- ✓ Incorporate Security into Corporate Governance: Regularly discuss cybersecurity at board meetings and ensure it is an integral part of corporate governance frameworks. This not only emphasizes its importance but also ensures accountability across the executive team.

Enhance Collaboration with Industry Peers and Authorities

- ✓ Engage in Industry Partnerships: Participate in industry consortiums and working groups to share and gain insights on effective cybersecurity practices. Collaborative efforts can lead to better defense mechanisms against common threats.

- ✓ Compliance and Regulatory Leadership: Stay ahead of regulatory requirements by not just complying, but actively influencing cybersecurity regulations. This proactive stance can lead to better industry standards and position your company as a thought leader.

Adopt a Forward-Looking Approach to Cybersecurity

- ✓ Invest in Emerging Technologies: Keep abreast of emerging technologies such as artificial intelligence and blockchain for cybersecurity applications. Early adoption can provide strategic advantages in threat detection and system integrity.
- ✓ Regular Scenario Planning: Conduct futuristic scenario planning exercises to anticipate potential threats and adapt strategies accordingly. This helps in staying ahead of cybercriminals and mitigating risks proactively.

Continuously Monitor and Report Cybersecurity Performance

- ✓ Implement Real-Time Dashboards: Use real-time dashboards for continuous monitoring of the organization's cybersecurity health. This allows for immediate detection of anomalies and swift response.
- ✓ Keeping stakeholders upto speed: Periodic sharing of updates to stakeholders about the organization’s cybersecurity status and how it supports business objectives. This transparency builds trust and keeps everyone informed about where the company stands in terms of cyber risk management.

6. **LIMITATIONS OF THE ANALYSIS**

- Lack of time and audience is one of the biggest obstacles.
- It is difficult to cross verify the accuracy of the information provided.
- All observations and recommendations are based on survey feedback.

BIBLIOGRAPHY

- Bhatia, D. (2022). A comprehensive review on the cyber security methods in Indian organisation. *Int. J. Adv. Soft Comput. Appl*, *14*(1), 103-124.
- Smith, J. (2022). "The Growing Importance of Cyber Security in Contemporary Business Operations." Journal of Cybersecurity, 10(2), 123-140.
- Jones, A., & Johnson, B. (2023). "Cyber Security Practices in Various Industries: A Literature Review." International Journal of Information Security, 15(3), 267-285.
- Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., ... & Kalogiannis, G. (2021). Cybersecurity in ICT supply chains: key challenges and a relevant architecture. *Sensors*, *21*(18), 6057.
- Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189-208.
- National Institute of Standards and Technology (NIST). (2020). NIST Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework
- International Organization for Standardization (ISO). (2021). ISO/IEC 27001: Information Security Management Systems - Requirements. Geneva, Switzerland: ISO.
- Alegria, A. V., Loayza, J. L. M., Montoya, A. N., & Armas-Aguirre, J. (2022, June). Method of quantitative analysis of cybersecurity risks focused on data security in financial institutions. In *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-7). IEEE.
- AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754.

- Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361.
- Taherdoost, H., Madanchian, M., & Ebrahimi, M. (2021). Advancement of Cybersecurity and Information Security Awareness to Facilitate Digital Transformation: Opportunities and Challenges. *Handbook of Research on Advancing Cybersecurity for Digital Transformation*, 99-117.
- Brown, C., & Williams, D. (2022). "The CIA Triad: Confidentiality, Integrity, and Availability in Cyber Security Management." Cybersecurity Journal, 8(4), 345-360.
- European Union. (2018). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garcés, I. (2020). A comprehensive study of the IoT cybersecurity in smart cities. *IEEE Access*, *8*, 228922-228941.
- California Legislative Information. (2018). California Consumer Privacy Act (CCPA). Retrieved from https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375
- Sanchez-Garcia, I. D., Rea-Guaman, A. M., Gilabert, T. S. F., & Calvo-Manzano, J. A. (2024). Cybersecurity Risk Audit: A Systematic Literature Review. *New Perspectives in Software Engineering*, 275-301.
- de Souza Junior, A. A., de Souza Pio, J. L., Fonseca, J. C., de Oliveira, M. A., de Paiva Valadares, O. C., & da Silva, P. H. S. (2021). The state of cybersecurity in smart manufacturing systems: A systematic review. *European Journal of Business and Management Research*, *6*(6), 188-194.
- Sabillon, R., & Bermejo Higuera, J. R. (2023, July). The importance of cybersecurity awareness training in the aviation industry for early detection of Cyberthreats and vulnerabilities. In *International Conference on Human-Computer Interaction* (pp. 461-479). Cham: Springer Nature Switzerland.

- Govindarajan, U. H., Singh, D. K., & Gohel, H. A. (2023). Forecasting cyber security threats landscape and associated technical trends in telehealth using bidirectional encoder representations from Transformers (Bert). *Computers & Security*, 103404.
- Nabi, F., Zhou, X., Iftikhar, U., & Attaullah, H. M. (2023). A Case Study of Cyber Subversion Attack based Design Flaw in Service Oriented Component Application Logic. *Journal of Cyber Security Technology*, 1-25.
- Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 101804.
- Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal, 1(3), 9-19.
- Iyer, V. R., Babu, K., & Guruswamy, V. R. (2024). Cyber Security Frameworks through the Lens of Foreign Direct Investment (FDI): A Systematic Literature Review. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(4s), 279-291.
- Ajankar, S. S., & Nimodiya, A. R. (2021). Cyber Security: Techniques and Perspectives on Transforming-A Review.
- Bibangco, M. H., & Manahan, E. (2024). Assessing the Philippine National Cybersecurity Plan 2022 for SMEs: Challenges and Opportunities. *Philippine Journal of Science, Engineering, and Technology*, *1*(1).
- Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., ... & Kalogiannis, G. (2021). Provisioning Cybersecurity in ICT Complex Supply Chains: An Overview, Key Issues and a Relevant Architecture.
- Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. Sustainability, 13(24), 13761. https://www.mdpi.com/2071-

1050/13/24/13761

- ‘Cyber security assessments in mergers and acquisitions’. (ISC)2. Accessed Jan 2020. www.isc2.org/Research/ The-ROI-of-Sound-CybersecurityPrograms. ‘Hiscox Cyber Readiness Report 2019’. Hiscox. Accessed Jan 2020. www.hiscox.co.uk/sites/uk/files/ documents/2019-04/Hiscox_Cyber_ Readiness_Report_2019.pdf
- Abu Ghamsha, M. K. (2013). Investment in the Gulf financial markets and their role in investment in the Gulf financial markets and their role in attracting foreign investments. Economic Research Journal, (6).
- Aiyer, B., Caso, J., Russell, P., & Sorel, M. (October 27, 2022). ‘New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers’. Risk & Resilience, McKinsey. https://www.mckinsey.com/search?q=october+27%2C+2022+marc+sorel&pageFilter=all&sort=default&start=1
- Amoroso, E. 2011. Cyber Attacks: Protecting National Infrastructure (1st ed.). Burlington: USA, Elsevier Inc. https://www.sciencedirect.com/topics/computer-science/security-posture
- Andronache, A. (2021). INCREASING SECURITY AWARENESS THROUGH LENSES OF CYBERSECURITY CULTURE. Journal of Information Systems & Operations Management, 15(1), Pp.7-22. https://www.researchgate.net/profile/Alina-Andronache-2/publication/353322243_Increasing_Security_Awarenesss_Through_Lenses_of_Cybersecurity_Culture/links/613c994f4e1df271062b528b/Increasing-Security-Awarenesss-Through-Lenses-of-Cybersecurity-Culture.pdf
- Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. Sustainability, 13(24), 13761. https://www.mdpi.com/2071-1050/13/24/13761

- CIT. (2024). ‘How cybercriminals target outdated software’. https://www.cit-net.com/how-cybercriminals-target-outdated-software/
- Hiscox. ‘Hiscox Cyber Readiness Report 2019’. Accessed Jan 2020. www.hiscox.co.uk/sites/uk/files/ documents/2019-04/Hiscox_Cyber_ Readiness_Report_2019.pdf
- Hiscox. ‘Hiscox Cyber Readiness Report 2023’. Accessed April 2024. https://www.hiscoxgroup.com/sites/group/files/documents/2023-10/Hiscox-Cyber-Readiness-Report-2023.pdf
- ISC2. ‘Cyber security assessments in mergers and acquisitions’. Accessed Jan 2020. www.isc2.org/Research/ The-ROI-of-Sound-CybersecurityPrograms.
- Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. International Journal of Information Management, 45, 13-24. https://www.sciencedirect.com/science/article/abs/pii/S0268401218302093
- Lloyd, G. (2020). The business benefits of cyber security for SMEs. Computer fraud & security, 2020(2), 14-17. https://policymonitor.co.uk/wp-content/uploads/2021/11/Computer-Fraud-Security-Feb-2020.pdf
- Morgan, S. (November 13, 2020). Special Report: Cyberwarfare In The C-Suite. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
- Negussie, D. (2023). Importance of Cybersecurity Awareness Training for Employees in Business. VIDYA-A JOURNAL OF GUJARAT UNIVERSITY, 2(2), 104-107. https://www.researchgate.net/publication/372990175_IMPORTANCE_OF_CYBERSECURITY_AWARENESS_TRAINING_FOR_EMPLOYEES_IN

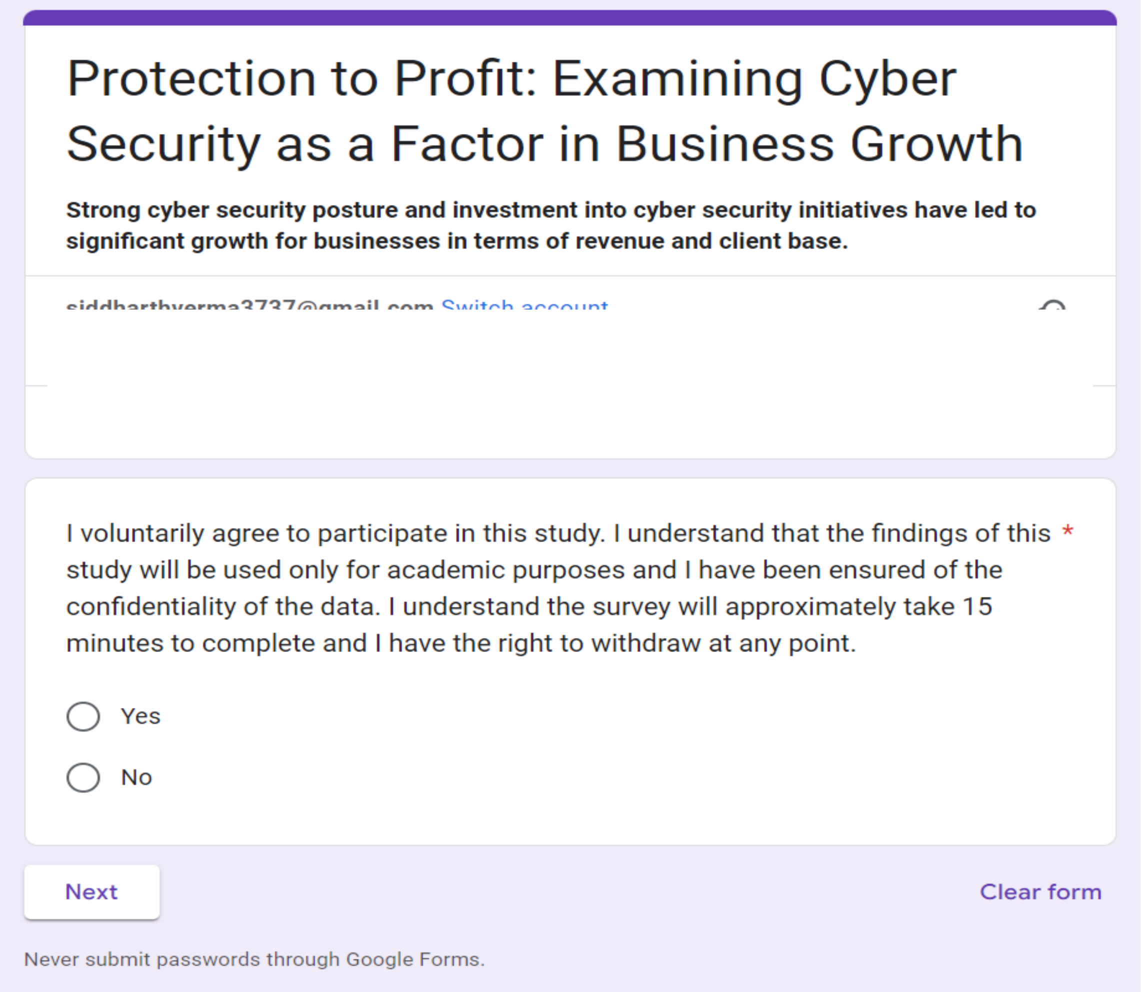
_BUSINESS#:~:text=A%20systematic%20literature%20review%20reveals,work%20enhances%20the%20organization%27s%20resilience

- Page, R. (November 13, 2023). 8 reasons your cybersecurity training program sucks and how to fix it. CSO. https://www.csoonline.com/article/1246117/8-reasons-your-cybersecurity-training-program-sucks-and-how-to-fix-it.html
- Pratt, M. (January 3, 2024). Why effective cybersecurity is important for businesses. Tech Target Network. https://www.techtarget.com/searchsecurity/feature/Why-effective-cybersecurity-is-important-for-businesses#:~:text=Cyber%20attacks%20can%20have%20serious,cybersecurity%20protections%20a%20critical%20step.&text=The%20threat%20of%20a%20successful,and%20across%20all%20industries%20face.
- Pwc. (2014). US cybercrime: Rising risks, reduced readiness: Key findings from the 2014 US State of Cybercrime Survey. https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf
- PwC. (November 10, 2023). PwC India’s 2024 Digital Trust Insights. https://www.pwc.in/press-releases/2023/99-of-organisations-will-increase-their-cyber-budgets-out-of-which-50-envisaged-an-increase-between-6-and-15-in-the-next-12-months-pwcs-2024-digital-trust-insights.html
- Shaker, A. S., Al Shiblawi, G. A. K., Union, A. H., & Hameedi, K. S. (2023). The Role of Information Technology Governance on Enhancing Cybersecurity and its Reflection on Investor Confidence. International Journal of Professional Business Review: Int. J. Prof. Bus. Rev., 8(6), 7.
- Tehila, S. (August 16, 2023). Cybersecurity as a strategic investment: How ROI Optimization can lead to a more secure future. Forbes Technology Council. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/08/16/cybersecurity-as-a-strategic-investment-how-roi-optimization-can-lead-to-a-more-secure-future/?sh=7e9b74094cf7

- Wadhwani, S. (September 12, 2023). ‘Why Companies Are Investing in Cyber Resilience More Than Ever Today’. Spiceworks. https://www.spiceworks.com/it-security/security-general/articles/cybersecurity-investment-drivers/
- Verizon. (2021). Data Breach Investigation Report (DBIR). https://www.verizon.com/business/resources/T9a7/reports/2021-data-breach-investigations-report.pdf
- Verizon (2024). Data breach Investigations Report (DBIR). https://www.verizon.com/business/resources/reports/dbir/
- Yepez, A. (January 29, 2024). ‘How Cybersecurity Drives Innovation in Critical Infrastructure’. Nasdaq, Inc. https://www.nasdaq.com/articles/how-cybersecurity-drives-innovation-in-critical-infrastructure

ANNEXUE-1

Questionnaire : https://forms.gle/PDvwpXVYAGfEWX2r7



Protection to Profit: Examining Cyber Security as a Factor in Business Growth

Strong cyber security posture and investment into cyber security initiatives have led to significant growth for businesses in terms of revenue and client base.

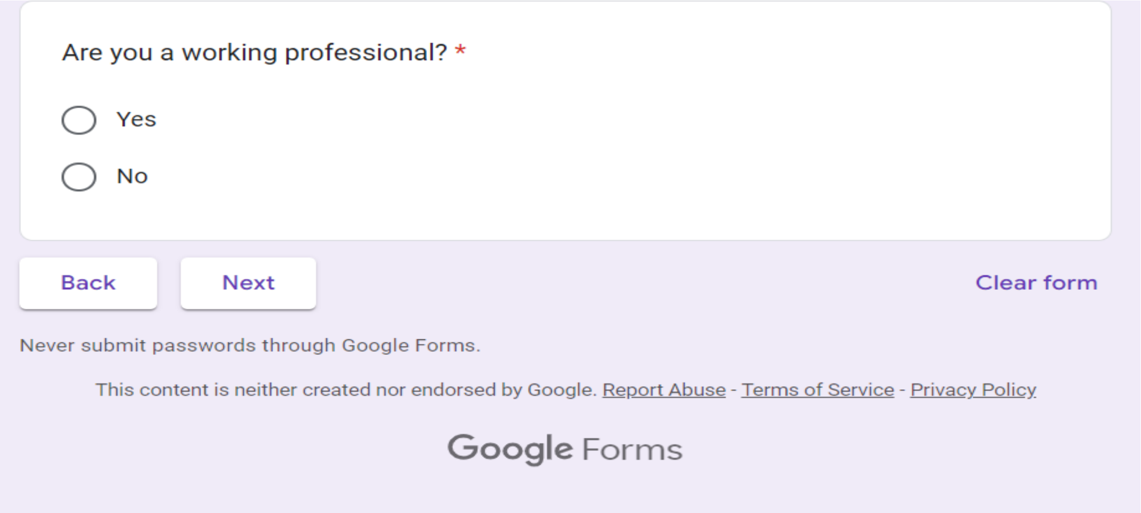
siddharthverma3737@gmail.com Switch account

I voluntarily agree to participate in this study. I understand that the findings of this study will be used only for academic purposes and I have been ensured of the confidentiality of the data. I understand the survey will approximately take 15 minutes to complete and I have the right to withdraw at any point. *

○ Yes

○ No

Never submit passwords through Google Forms.



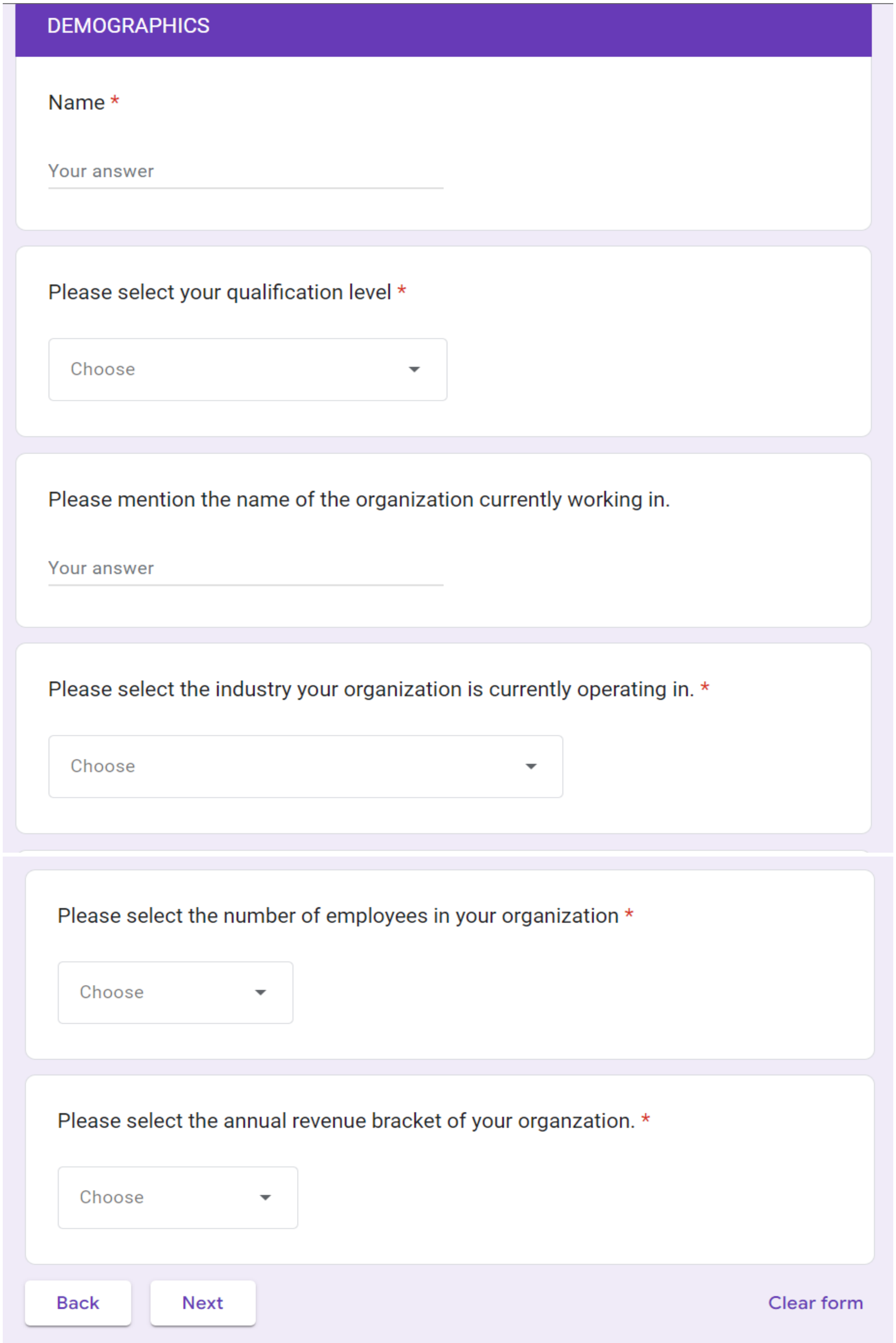
Are you a working professional? *

○ Yes

○ No

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy



DEMOGRAPHICS

Name *

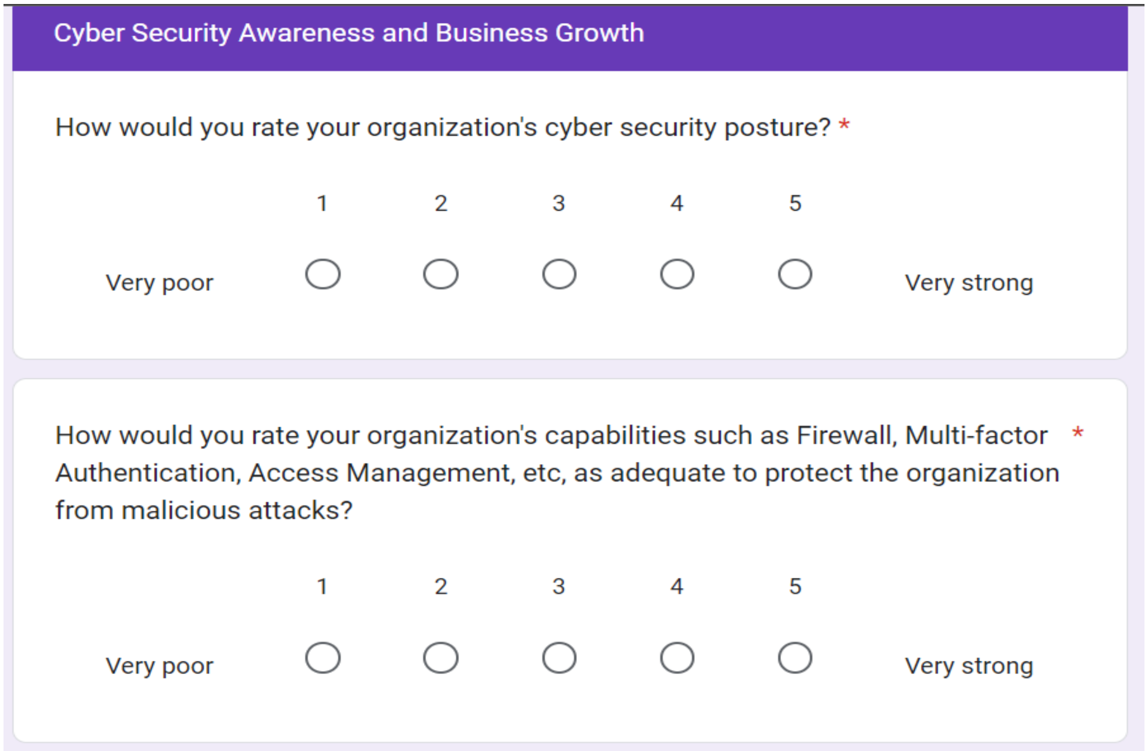
Please select your qualification level *

Please mention the name of the organization currently working in.

Please select the industry your organization is currently operating in. *

Please select the number of employees in your organization *

Please select the annual revenue bracket of your organzation. *



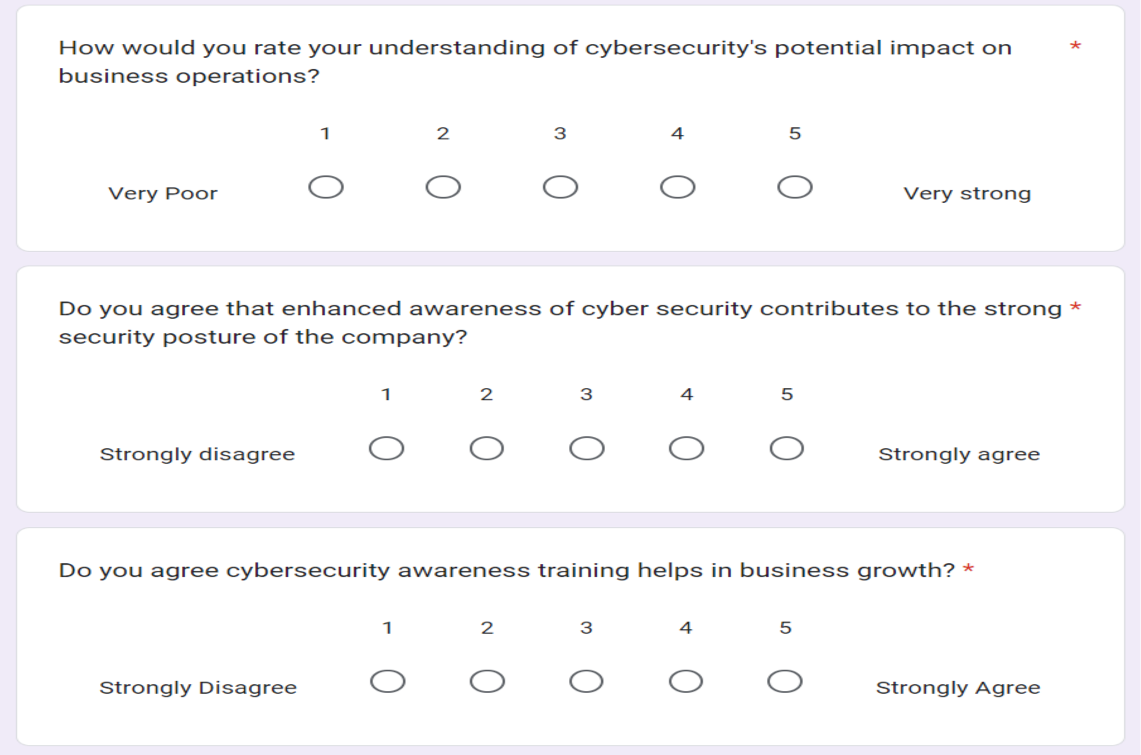
Cyber Security Awareness and Business Growth

How would you rate your organization's cyber security posture? *

	1	2	3	4	5	
Very poor	○	○	○	○	○	Very strong

How would you rate your organization's capabilities such as Firewall, Multi-factor Authentication, Access Management, etc, as adequate to protect the organization from malicious attacks? *

	1	2	3	4	5	
Very poor	○	○	○	○	○	Very strong



How would you rate your understanding of cybersecurity's potential impact on business operations? *

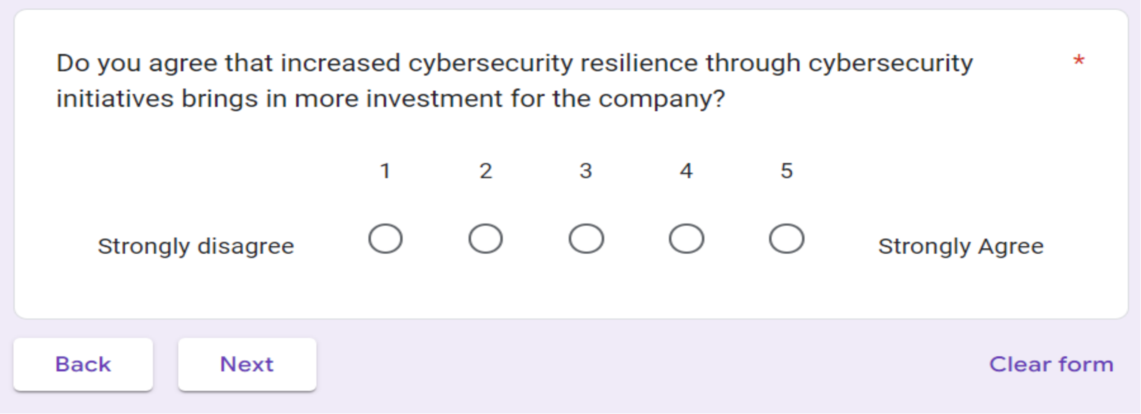
	1	2	3	4	5	
Very Poor	○	○	○	○	○	Very strong

Do you agree that enhanced awareness of cyber security contributes to the strong security posture of the company? *

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

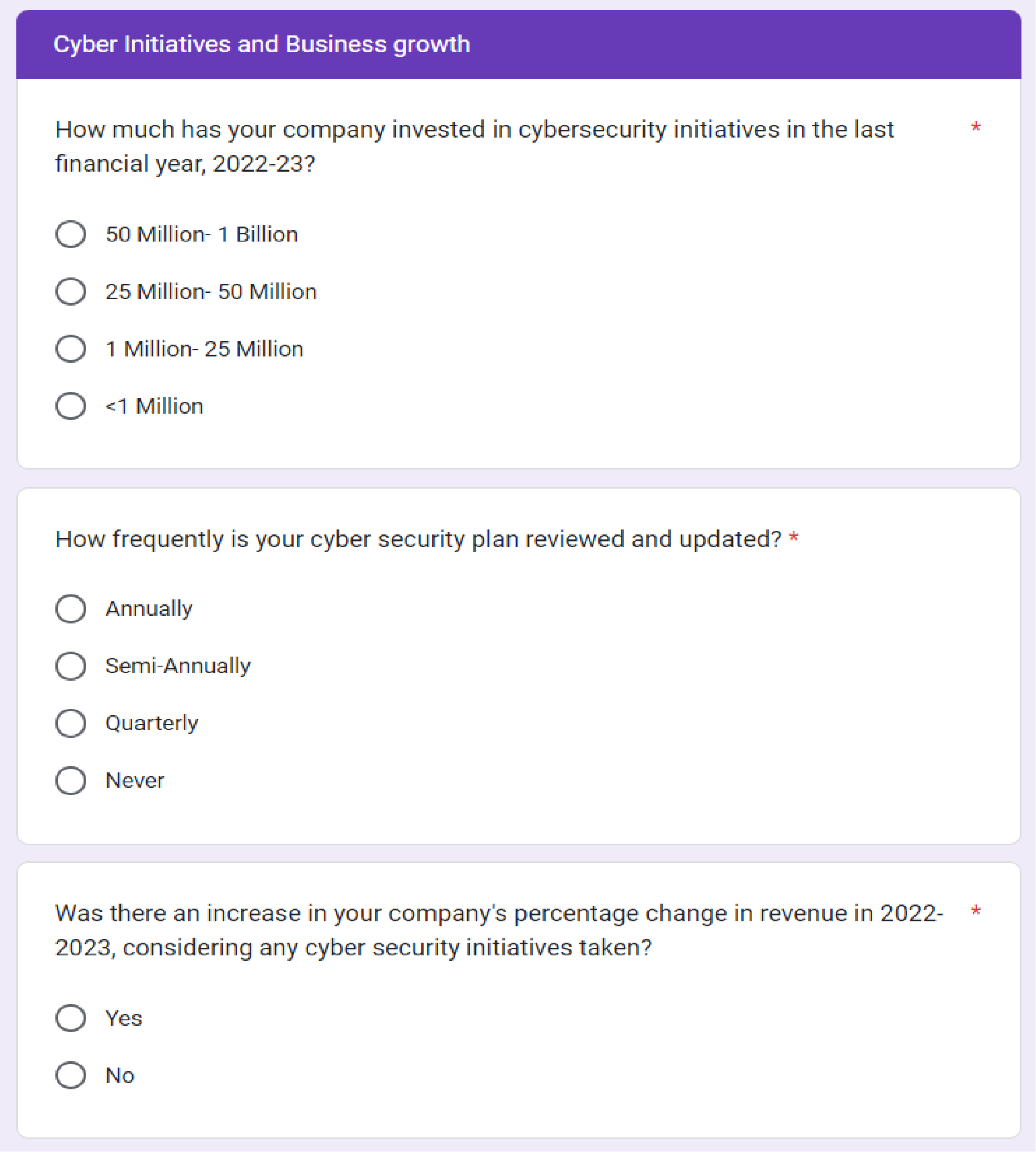
Do you agree cybersecurity awareness training helps in business growth? *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree



Do you agree that increased cybersecurity resilience through cybersecurity initiatives brings in more investment for the company? *

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly Agree



Cyber Initiatives and Business growth

How much has your company invested in cybersecurity initiatives in the last financial year, 2022-23? *

○ 50 Million- 1 Billion

○ 25 Million- 50 Million

○ 1 Million- 25 Million

○ <1 Million

How frequently is your cyber security plan reviewed and updated? *

○ Annually

○ Semi-Annually

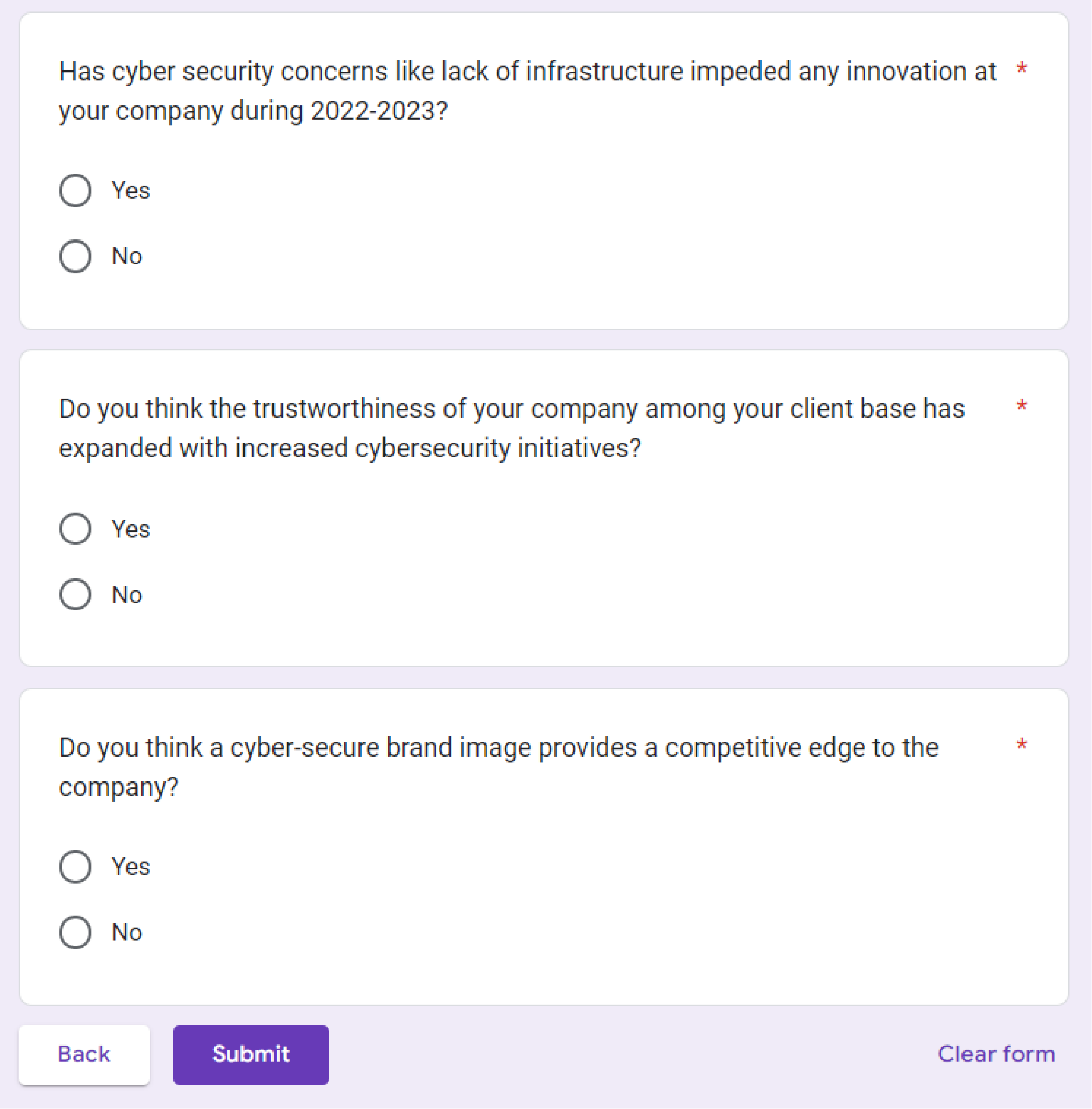
○ Quarterly

○ Never

Was there an increase in your company's percentage change in revenue in 2022-2023, considering any cyber security initiatives taken? *

○ Yes

○ No



Has cyber security concerns like lack of infrastructure impeded any innovation at your company during 2022-2023? *

○ Yes

○ No

Do you think the trustworthiness of your company among your client base has expanded with increased cybersecurity initiatives? *

○ Yes

○ No

Do you think a cyber-secure brand image provides a competitive edge to the company? *

○ Yes

○ No

Turnitin Plagiarism Check

Major Project_Protection to Profit Examining cyber security as a factor in business growth

Document Details

Submission ID

trn:oid:::1:2930462123

Submission Date

May 25, 2024, 5:59 AM CDT

Download Date

May 25, 2024, 6:20 AM CDT

File Name

ofit_Examining_cyber_security_as_a_factor_in_business_growth.pdf

File Size

1.2 MB

49 Pages

11,430 Words

68,975 Characters

Major Project_Protection to Profit Examining cyber security as a factor in business growth

ORIGINALITY REPORT

5%	4%	2%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to British Institute of Technology and E-commerce Student Paper	1%
2	www.vidyajournal.org Internet Source	<1%
3	www.forbes.com Internet Source	<1%
4	oarjpublication.com Internet Source	<1%
5	vdoc.pub Internet Source	<1%
6	Submitted to University of Maryland, University College Student Paper	<1%
7	studfile.net Internet Source	<1%
8	fastercapital.com Internet Source	<1%

9	journal.send2sub.com Internet Source	<1 %
10	www.ijraset.com Internet Source	<1 %
11	stripe.com Internet Source	<1 %
12	www.123articleonline.com Internet Source	<1 %
13	Submitted to Deakin University Student Paper	<1 %
14	Submitted to University of College Cork Student Paper	<1 %
15	dokumen.pub Internet Source	<1 %
16	marketbusinessnews.com Internet Source	<1 %
17	Submitted to Purdue University Student Paper	<1 %
18	Siva Raja Sindiramutty, Noor Zaman Jhanjhi, Chong Eng Tan, Navid Ali Khan, Bhavin Shah, Loveleen Gaur. "chapter 7 Securing the Digital Supply Chain Cyber Threats and Vulnerabilities", IGI Global, 2023 Publication	<1 %

19	Submitted to University at Buffalo Student Paper	<1 %
20	Submitted to University of Rome Tor Vergata Student Paper	<1 %
21	www.secopsolution.com Internet Source	<1 %
22	Jiehua Zhong, Xi Wang, Tao Zhang. "Network Security Governance Policy and Risk Management: Research on Challenges and Coping Strategies", Journal of Machine and Computing, 2024 Publication	<1 %
23	www.cloud4c.com Internet Source	<1 %
24	Submitted to University of Bedfordshire Student Paper	<1 %
25	cascadebusnews.com Internet Source	<1 %
26	pdf.wps.com Internet Source	<1 %
27	123docz.net Internet Source	<1 %
28	industrytechnologyreports.home.blog Internet Source	<1 %

29	www.heinz.cmu.edu Internet Source	<1 %
30	Amoroso, E.G.. "Cyber attacks: awareness", Network Security, 201101 Publication	<1 %
31	Deepti Pandey, Aaditya Jain, A. Suneetha, Poonam Gupta, G. V. Sriramakrishnan, Adapa Gopi, Sabyasachi Pramanik. "chapter 3 Managing the AI Period's Confluence of Security and Morality", IGI Global, 2024 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		