**ASSIGNMENT 1 FRONT SHEET**



|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | Unit 13:Computing Research Project | | |
| **Submission date** |  | **Date Received 1st submission** |  |
| **Re-submission Date** |  | **Date Received 2nd submission** |  |
| **Student Name** | Nguyen Van Tung | **Student ID** | BH00299 |
| **Class** | IT0503 | **Assessor name** | Nguyen Thanh Trieu |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice. | | | |
|  | | **Student’s signature** | Tung |

**Grading grid**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P1 | P2 | P3 | P4 | P5 | M1 | M2 | M3 | D1 | D2 |
|  |  |  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  **Summative Feedback:**  **Resubmission Feedback:** | | |
| **Grade:** | **Assessor Signature:** | **Date:** |
| **Internal Verifier’s Comments:** | | |
| **Signature & Date:** | | |

Contents

[**A.** **Introduction** 5](#_Toc43999)

[**B.** **Content** 6](#_Toc44000)

[I. Produce a research proposal that clearly defines a research question or hypothesis supported by a literature review (P1) 6](#_Toc44001)

[**1.** **Abstracts** 6](#_Toc44002)

[**2.** **Situation** 6](#_Toc44003)

[**3.** **Project Type:** 6](#_Toc44004)

[**4.** **Define the main aims and objectives of the project:** 6](#_Toc44005)

[**5.** **Aim** 6](#_Toc44006)

[**6.** **Objectives** 7](#_Toc44007)

[II. Examine appropriate research methods and approaches to primary and secondary research (P2) 10](#_Toc44008)

[**1.** **Primary research** 10](#_Toc44009)

[**2.** **Secondary research** 13](#_Toc44010)

[**3.** **Pros and Cons of Primary Research and Secondary Research** 15](#_Toc44011)

[**4.** **Qualitative Method** 16](#_Toc44012)

[**5.** **Quantitative Method** 18](#_Toc44013)

[**6.** **Compare Qualitative With Quantitative** 20](#_Toc44014)

[**7.** **Research process** 21](#_Toc44015)

[III. Conduct primary and secondary research using appropriate methods for a computing research project that consider costs, access and ethical issues (P3) 24](#_Toc44016)

[**1.** **Primary Research** 24](#_Toc44017)

[**2.** **Secondary Research** 25](#_Toc44018)

[**3.** **Data collected** 26](#_Toc44019)

[**4.** **Interview** 27](#_Toc44020)

[**5.** **Questions** 27](#_Toc44021)

[**6.** **Survey** 28](#_Toc44022)

[IV. Apply appropriate analytical tools, analyze research findings and data (P4) 28](#_Toc44023)

[**1.** **Survey** 28](#_Toc44024)

[**2.** **Interview** 36](#_Toc44025)

[**3.** **Survey summary** 41](#_Toc44026)

[**4.** **Analyze the results of the primary research** 41](#_Toc44027)

[V. Communicate research outcomes in an appropriate manner for the intended audience (P5) 42](#_Toc44028)

[**C.** **Conclusion** 43](#_Toc44029)

[**D.** **References** 43](#_Toc44030)

**Table Of Figures**

[Figure 1: Project Plan 9](#_Toc160737250)

[Figure 2: Primary research 10](#_Toc160737251)

[Figure 3: Secondary research 13](#_Toc160737252)

[Figure 4: Qualitative Method 16](#_Toc160737253)

[Figure 5: Quantitative Method 18](#_Toc160737254)

[Figure 6: Research process 21](#_Toc160737255)

[Figure 7: Survey 28](#_Toc160737256)

[Figure 8: Survey 29](#_Toc160737257)

[Figure 9: Survey 29](#_Toc160737258)

[Figure 10: Survey 30](#_Toc160737259)

[Figure 11: Survey 31](#_Toc160737260)

[Figure 12: Survey 32](#_Toc160737261)

[Figure 13: Survey 33](#_Toc160737262)

[Figure 14: Survey 34](#_Toc160737263)

[Figure 15: Survey 34](#_Toc160737264)

[Figure 16: Survey 35](#_Toc160737265)

# A. Introduction

This time, I've decided to write about the study topic for this project, which is "The most common cyber threats and vulnerabilities associated with big data environments and how organizations can effectively mitigate them." "The most common cyber threats and vulnerabilities associated with big data environments and how organizations can effectively mitigate them" is an important question in the contemporary digital world. It is critical to comprehend and counter these cyberthreats in order to protect big data's availability, confidentiality, and integrity. This investigation explores the most common cyberthreats and vulnerabilities linked to big data environments and clarifies practical mitigation techniques that businesses can use to strengthen their data ecosystems against possible assaults. Organizations may traverse the data-driven world with resilience and confidence by proactively strengthening their defenses, which will also ensure the safety and purity of their priceless data assets.

# B. Content

## I. Produce a research proposal that clearly defines a research question or hypothesis supported by a literature review (P1)

### 1. Abstracts

Due to their massive volume, velocity, and diversity of data, big data sets are susceptible to a wide range of cyberthreats. It's essential to identify and reduce these risks for the sake of organizational integrity and data security. The main cyberthreats and vulnerabilities that big data environments face are covered in this article, including malware assaults, insider threats, unauthorized access, and data breaches. It examines mitigating strategies such encryption, periodic security assessments, staff training, safe access controls, and using sophisticated analytics to find anomalies. By adopting a thorough and proactive approach, organizations may prevent cyberattacks and minimize potential damage to their big data ecosystems.

### 2. Situation

In the quickly evolving field of information technology, organizations are depending more and more on big data environments to handle, examine, and derive actionable insights from massive and diverse datasets. These settings include intricate infrastructures and linked systems, which pose significant cybersecurity issues. Businesses need to prioritize protecting their big data assets since cyber risks, such as sophisticated attacks and vulnerabilities, are on the rise. The reputation and overall operations of a business can be severely harmed by threats such as cyber attacks, illegal access, data breaches, insider threats, and unstable finances. Thus, proactively implementing efficient mitigation techniques and maintaining a complete understanding of the risks are necessary for safeguarding large data settings as well as data integrity and confidentiality. This situation highlights how crucial it is for companies to have comprehensive cybersecurity plans to lessen possible risks and ensure the security of their big data ecosystems.

### 3. Project Type:

Research and Analysis

### 4. Define the main aims and objectives of the project:

"Learn about dangers and weaknesses that affect big data environments and how to counter them" is the project's primary goal.

### 5. Aim

* **Comprehensive Understanding:** To have a thorough understanding of the special risks and weaknesses related to large data situations.
* **Risk Assessment:** must carry out a comprehensive risk analysis in order to pinpoint any possible vulnerabilities in the big data operations and infrastructure.
* **Best Practices Analysis:** To examine industry standards and best practices for protecting big data settings.
* **Mitigation Strategies:** To create practical mitigation techniques that can greatly lower the dangers that cyberthreats pose in large data settings.
* **Integration of Technologies:** To investigate and suggest appropriate cybersecurity solutions that may be included into big data platforms to improve security.

### 6. Objectives

* **Threat Identification:** Determine and classify the main cyberthreats and vulnerabilities that are common in big data settings, such as malware attacks, illegal access, insider threats, and data breaches.
* **Risk Analysis:** To evaluate possible hazards and their possible effects on organizational operations and data integrity, do a thorough risk analysis of the big data infrastructure.
* **Current Security Measures Assessment:** Examine the big data infrastructure of the company to determine its security measures' strengths, weaknesses, gaps, and opportunities for development.
* **Compliance and Standards Review:** Examine and evaluate if the company complies with all applicable cybersecurity laws and guidelines that apply to big data settings.
* **Mitigation Strategy Development:** Create a customized, proactive set of cybersecurity policies and procedures to successfully address threats and vulnerabilities that have been discovered.
* **Technology Recommendations:** Provide suitable cybersecurity strategies, methods, and technologies that can be incorporated into the big data ecosystem to improve security.
* **Implementation Roadmap:** Provide a staged implementation plan including the procedures, schedule, distribution of resources, and roles necessary to successfully execute the suggested cybersecurity tactics and technology.
* **Training and Awareness**: To inform staff members and other interested parties about cybersecurity best practices and their part in upholding a safe big data environment, suggest a program for training and awareness raising.

**7. Project Plan**

**Week 1:** Launch of the Project and Literature Review

**Day 1-2: Project Kickoff**

* Specify the goals and research question.
* Assemble the research team and assign roles.

**Day 3-7: Literature Review**

* Conduct an extensive literature review on cyber threats and vulnerabilities in big data environments.
* Identify the most common threats and vulnerabilities.

**Week 2: Data Collection and Analysis**

**Day 8-14: Data Collection and Analysis**

* Collect data from reputable sources, including case studies, academic papers, and industry reports.
* Analyze the collected data to identify patterns, commonalities, and notable findings regarding cyber threats and vulnerabilities in big data environments.

**Week 3: Mitigation Strategies and Framework Development**

**Day 15-21: Mitigation Strategies**

* Research and compile effective mitigation strategies for the identified threats and vulnerabilities.
* Develop a comprehensive framework outlining best practices and recommendations for mitigating cyber threats in big data environments.

**Week 4: Report Writing and Presentation Preparation**

**Day 22-28: Report Writing and Presentation**

* Draft the research report, including an introduction, methodology, findings, discussion, conclusions, and recommendations.
* Create visuals (charts, graphs) to represent the data and findings effectively.
* Practice and prepare for the final research presentation.

**Day 29-30: Final Revisions and Presentation**

* Review and revise the research report based on feedback and insights.
* Finalize the presentation and ensure it effectively communicates the research findings and recommendations.

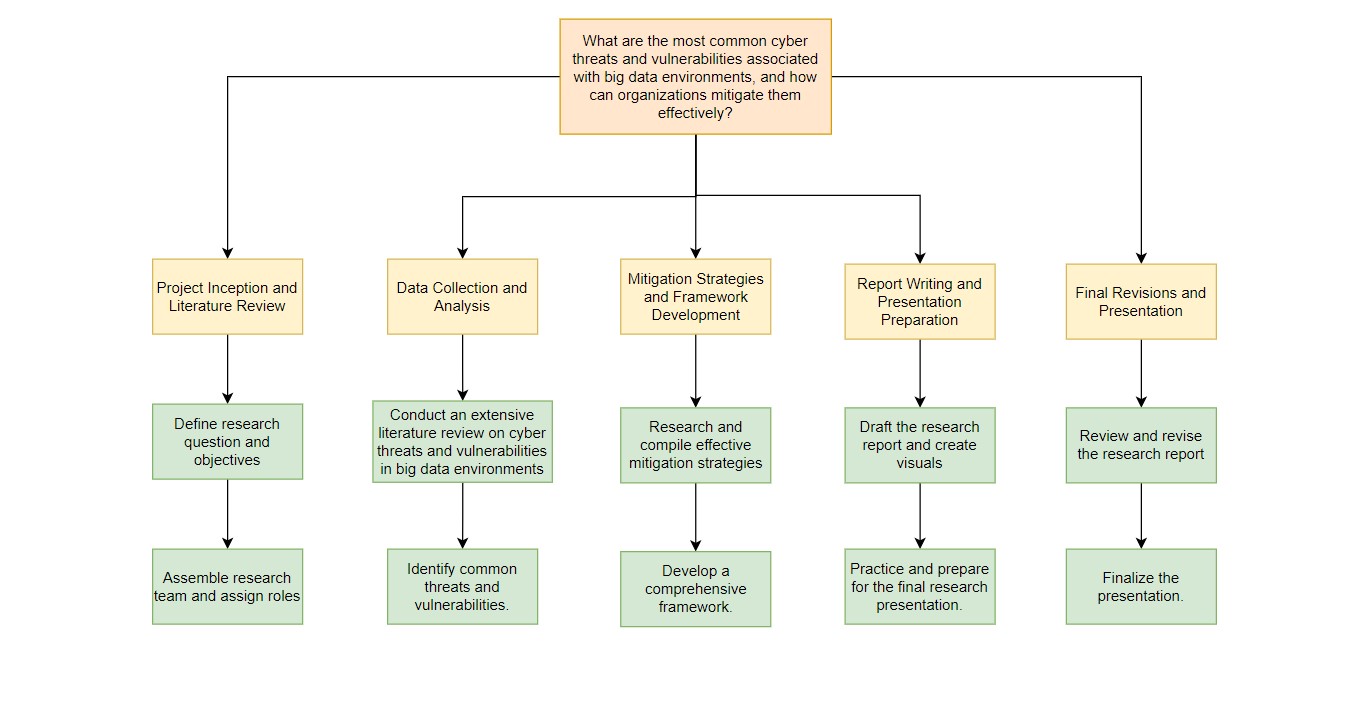


Figure : Project Plan

## II. Examine appropriate research methods and approaches to primary and secondary research (P2)

Research techniques and approaches are a general term that may be used to describe both primary and secondary research. Every technique has pros and cons as well as suitable use cases, contingent on the goals of the research and available resources. Below is a review of appropriate research methods and approaches for primary and secondary research:

### 1. Primary research

Primary research, often known as first-hand or original research, involves obtaining new and original information directly from sources. Researchers design and execute studies, experiments, surveys, or observations to gather information relevant to their research objectives.

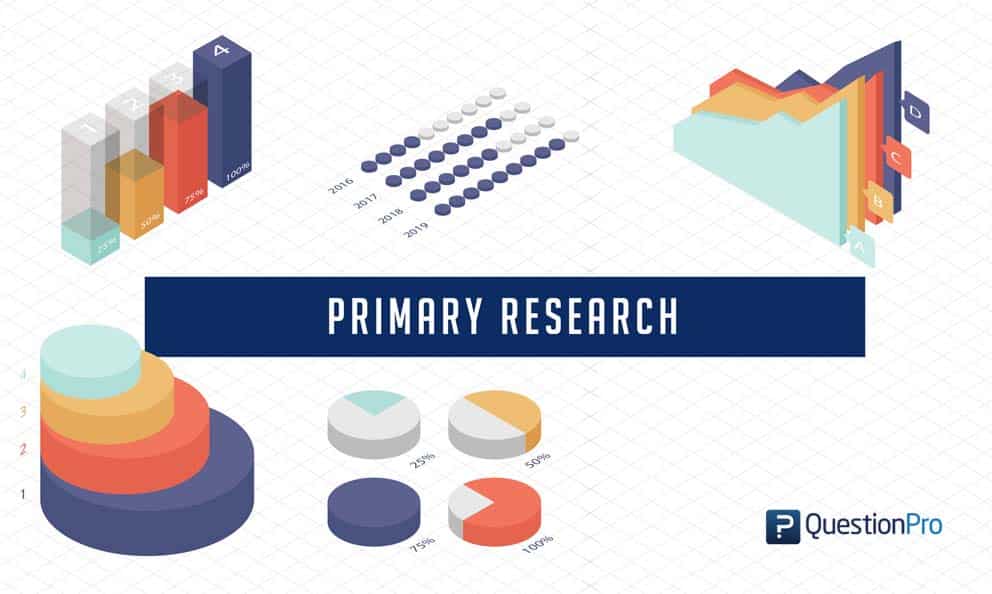


Figure : Primary research

|  |  |
| --- | --- |
| **PROS** | **CONS** |
| Primary research ensures that the study fulfills its intended goals and needs by enabling customized data gathering that is directly associated with the objectives. | Planning, data collecting, analysis, and interpretation are all time-consuming aspects of primary research that can cause delays in the entire study process. |
| Since primary research gathers data directly from the source, it offers the most recent insights and trends and is therefore the most current and up-to-date. | Due to costs associated with participant recruiting, data collecting instruments, incentives, and other logistics, primary research can be expensive. |
| Scholars possess authority over the research design, methodology, and data collection procedures, therefore permitting modification and optimization to meet the specific requirements of the study. | It is difficult for smaller research groups or organizations with low resources since it necessitates a large commitment of staff, knowledge, and infrastructure. |
| Original data from primary research adds to the study's distinctiveness and worth, offers new insights, and advances knowledge in academia or business. | When primary research is done in an unreliable manner or when the researcher's viewpoints affect the way the data is gathered or interpreted, it may create researcher bias. |
| During the study, researchers might make adjustments to the research design and methodology to better handle any unanticipated problems or improve the strategy and yield better findings. | It might be difficult to contact the intended participant pool, especially if the target population is hard to reach. This can lead to constraints in the amount of data that can be collected. |
| Primary research frequently enables in-depth investigation and comprehension of the study issue, offering a thorough analysis and subtle insights. | Primary research data can be complicated, requiring sophisticated analytical techniques and instruments for in-depth analysis and significant findings. |
| Direct interaction between researchers and participants allows for greater knowledge of their viewpoints, deeper investigation of ideas, and clarification of replies. | The ethical aspects of primary research might include more complicated decisions, such as getting informed permission and protecting data privacy, which calls for cautious handling in order to uphold moral principles. |

1. **Surveys and Questionnaires:**

* **Approach**: Make structured surveys and questionnaires to get information directly from consumers, businesses, and data privacy experts.
* **Methodology**: Use multiple-choice, open-ended, and Likert scales to gather quantitative and qualitative data about user experiences, issues, and attitudes surrounding data privacy. Find out if they are utilizing any data protection measures or are aware of any.
* **Example**: Make an online poll with 500 digital service consumers as a sample. Ask them about their experiences with data breaches, privacy concerns, and their comprehension of data protection procedures. Use Likert scales to gauge how serious their issues are.

1. **Interviews:**

* **Approach**: Interview key informants in a semi-structured manner, including cybersecurity professionals, data privacy specialists, and victims of data breaches.
* **Method**: To get their thoughts, insights, and recommendations, use open-ended inquiries. Give folks the opportunity to share their thoughts and elaborate on certain incidents.
* **Example**: Get the opinions of three cybersecurity experts and five victims of data breaches. Speak with individuals affected by data breaches and get professional advice on effective data protection measures in order to comprehend the psychological and practical ramifications of such incidents.

**c. Focus Groups:**

* **Approach**: Hold focus groups with smaller user groups to find out more about their views and data protection habits.
* **Method**: Facilitate conversations in groups to identify common challenges, experiences, and points of view. Allow participants to engage with one another in order to generate a collection of insights.
* **Example**: Organize two focus groups: one for youth and one for elderly people. Look into their internet behavior, views on privacy, and understanding of data security protocols.

### 2. Secondary research

Secondary research, sometimes called desk research, is the act of employing data and information that has already been obtained for another purpose. Researchers synthesize, evaluate, and interpret preexisting data to arrive at conclusions or address research problems.



Figure : Secondary research

|  |  |
| --- | --- |
| **PROS** | **CONS** |
| Because secondary research makes use of already-existing data, it is typically less expensive because it eliminates the need for considerable data collecting and related costs. | Secondary data can range widely in quality and dependability, thus researchers need to assess the sources' veracity and correctness carefully. |
| Compared to original research, secondary research saves time because the data is already available and can be analyzed quickly. | Because of their limited control over the data gathering process, researchers may encounter problems with data completeness, relevance, or fit for their particular study aims. |
| Research may be greatly aided by the abundance of data and information provided in secondary sources, which can span a wide range of subjects and historical periods. | Findings from secondary data may not be as accurate or applicable in the present study environment since they are out-of-date. |
| By comparing historical data, secondary research makes it possible to look at patterns, trends, and changes across time. | There may be situations where important data is not readily available to the public, making it difficult to find thorough and pertinent information. |
| Researchers don't need to physically be there or make attempts to collect data because they can obtain data from different geographic places. | Using secondary sources requires careful citation to ensure full credit is given to the original authors and to prevent plagiarism. |
| Before beginning primary research, researchers can improve their research questions and find knowledge gaps with the aid of secondary research. | In order to obtain significant insights, researchers must synthesis information from several sources because secondary data may not be detailed enough for the study aims. |
|  | The initial intent and prejudice of the source that provided the secondary data may have an impact on the data's objectivity and impartiality, which may have an impact on the study's conclusions. |

**a. Steps involved in conducting secondary research:**

* **Define Research Objectives**: Outline your research's objectives and questions in clear terms. What specific information or viewpoints are you seeking in secondary research?
* **Identify Sources and Databases**: Select the ones that have the greatest bearing on your study. These might include books, corporate reports, academic journals, government papers, novels, internet databases, and reliable webpages.
* **Data Synthesis and Analysis**: summarize the key findings, trends, and conclusions drawn from a variety of sources. Examine the data to look for any trends, inconsistencies, or knowledge gaps.
* **Citations and references**: List and properly credit every source you utilized for your research. Utilize a recognized citation format (APA, MLA, or Chicago, for example) to maintain academic integrity.

### 3. Pros and Cons of Primary Research and Secondary Research

|  |  |  |
| --- | --- | --- |
| **BASIS FOR**  **COMPARISON** | **Primary Research** | **Secondary Research** |
| **Data Source** | **Source**: Data is directly gathered by surveys, interviews, experiments, observations, and other methods from original sources.  **Nature:** firsthand, particular to the goals of the research | **Source:** Existing sources such as books, papers, databases, government reports, and so on are used to gather data.  **Nature:** Previously gathered and already accessible for other uses |
| **Time and Cost** | **Time:** usually takes a lot of time since it requires planning, gathering, analyzing, and interpreting data.  **Cost:** often more costly since data gathering and resource requirements must be met | **Time:** Faster in general because the data is already there and reasonably accessible.  **Cost:** more economical since it makes use of already-existing sources and data |
| **Control** | **Control:** The methods, data gathering procedures, and research design are all largely under the researchers' control. **Flexibility:** able to modify strategies and tactics while conducting study | **Control:** Because the data is obtained from outside sources, there is little control over its relevancy and quality. **Flexibility:** Less freedom to change the data because it already exists |
| **Data Relevance and Accuracy** | **Accuracy:** good accuracy in general since the data is gathered with certain study goals in mind.  **Relevance:** extremely pertinent to the inquiry being studied. | **Accuracy:** Depending on the caliber and dependability of the references consulted.  **Relevance:** Depending on how well-suited the available data is to the study question, relevance varies. |
| **Bias and Objectivity** | **Bias:** Possibility of bias in the study team when gathering and analyzing data. **Objectivity:** requires deliberate effort to be impartial. | **Bias:** less researcher bias because other people have already gathered the data.  **Objectivity:** The original data source's quality determines the objectivity. |
| **Sample Size** | **Sample Size:** Based on the goals and design of the study, researchers can decide on the sample size. | **Sample Size:** restricted by the data's availability and current state. |
| **Applicability** | **Applicability:** Extremely relevant for tackling particular research questions and goals. | **Applicability:** helpful in giving background data, historical trends, and a larger perspective. |

### 4. Qualitative Method

Understanding and researching complex phenomena by concentrating on people's unique experiences, behaviors, and attitudes is the aim of qualitative research. It aims to clarify context, patterns, and meaning by carefully examining and analyzing qualitative data.

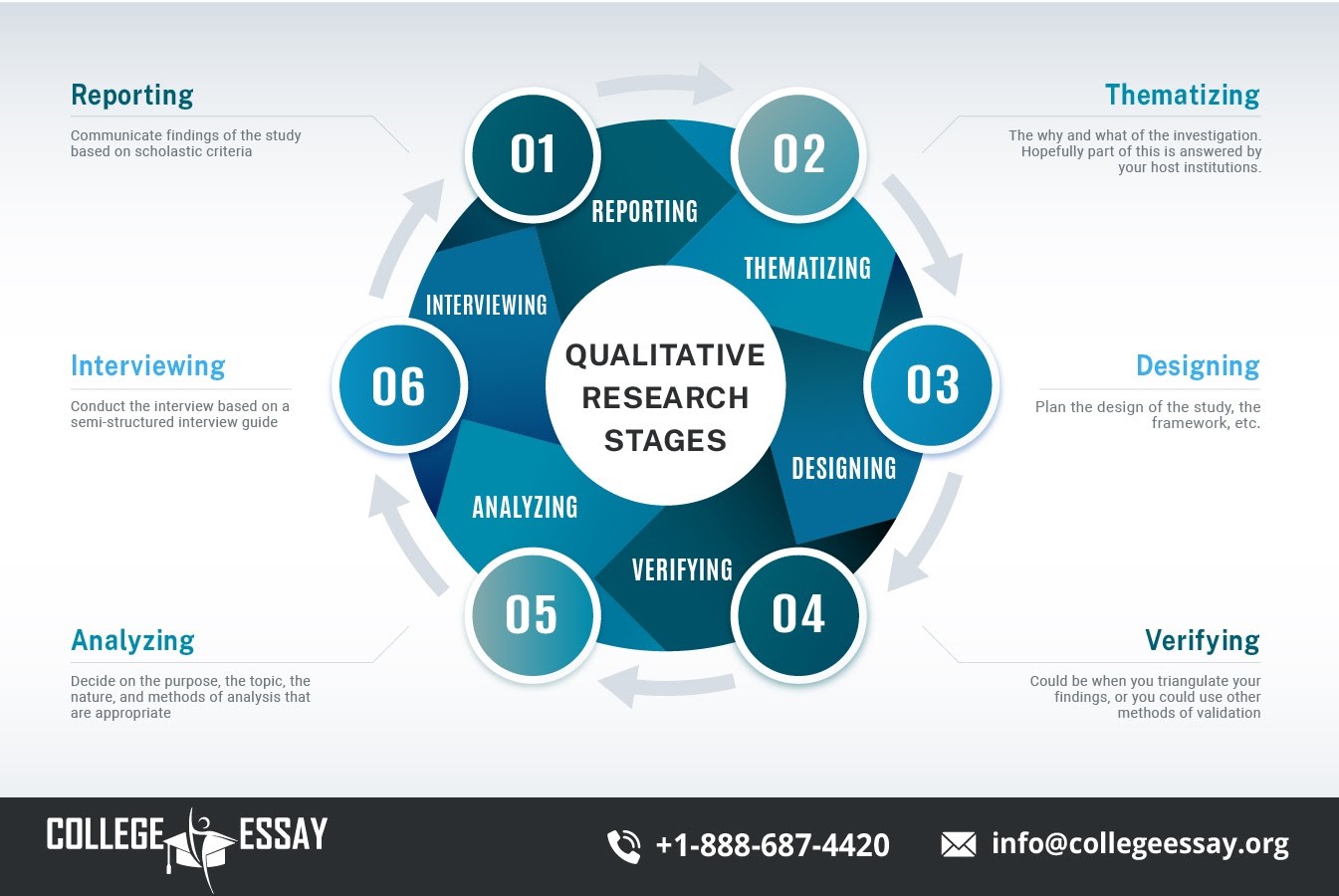


Figure : Qualitative Method

**a. Qualitative data analysis**

* **Data Preparation:** Sort and organize qualitative data (such as audio files, field notes, and transcripts of interviews) as needed.
* **Data coding:** The practice of classifying important data elements (sentences, phrases, and paragraphs) into distinct categories is known as coding. These are often referred to as "codes."
* **Continuous Comparison:** Researchers continuously compare newly collected data with pre-existing codes and themes in order to make improvements and get a deeper understanding. The data-based basis of the analysis is maintained with the help of this iterative process.
* **Triangulation:** Consider employing a variety of researchers or data sources to increase the analysis's validity and reliability. The technique of triangulation involves cross-referencing conclusions from several sources or points of view.
* **Data Visualization:** Create graphic representations of the data, such as idea maps, matrices, or diagrams, to aid in the organization and presentation of the results.
* **Report Writing:** Write a narrative report that summarizes the data analysis, findings, and themes. Provide examples or assertions that support your points of view and conclusions.

**b. Pros and cons**

|  |  |
| --- | --- |
| **Pros** | **Cons** |
| **Exploratory Research:** When there is minimal information available about a topic, it is especially helpful for theory creation, hypothesis generating, and exploratory study. | **Subjectivity:** The trustworthiness of the results of qualitative research might be impacted by the bias and interpretation of the researchers. |
| **Rich Data:** Nuanced interpretations might result from the rich and extensive information that qualitative data frequently give, including context and human histories. | **Time-Consuming:** Because in-depth interviews, coding, and theme analysis are required for qualitative data analysis, it might take a while to gather and process the data. |
| **Contextual Insights:** When it comes to revealing underlying meanings and social dynamics, qualitative research is particularly good at capturing the environment in which actions or events occur. | **Limited Generalizability:** Qualitative research often yields context-specific findings that might be difficult to generalize to wider groups. |
| **In-Depth Understanding:** Through qualitative inquiry, complex phenomena may be fully understood holistically. | **Difficulty in Data Management:** Large amounts of qualitative data can be difficult to manage and analyze, necessitating the use of efficient data management techniques. |
| **Flexibility:** Because qualitative approaches are adaptive and flexible, researchers may change their strategy when new information comes to light while doing their study. | **Resource-Intensive:** More resources, such as experienced researchers and transcribing services, are frequently needed for qualitative research, which might |

### 5. Quantitative Method

The goal of quantitative research is to characterize, elucidate, and forecast correlations between variables via the methodical collecting and analysis of numerical data. It aims to measure things and get statistically meaningful conclusions.



Figure : Quantitative Method

**a. Quantitative data analysis**

* **Data Preparation and Cleaning:** Sorting and cleansing your data should come first. To do this, check the dataset for mistakes, anomalies, and missing values.
* **Descriptive Statistics:** To summarize the data, compute basic descriptive statistics such as mean, median, mode, standard deviation, and range. Graphical tools like as scatterplots, box plots, and histograms can be used to visualize data distributions and correlations.
* **Inferential Statistics:** Inferential statistics can be used to make inferences about populations based on the analysis of sample data. In this case, confidence intervals are calculated and parameters are approximated.
* **Regression analysis:** is a technique for modeling the relationship that exists between one or more independent variables and a dependent variable. This aids in forecasting results.
* **Data Visualization:** Bar charts, line graphs, scatterplots, and heatmaps are examples of data visualizations that may be used to communicate results and help audiences comprehend data.
* **Interpretation of Results:** Think about the connections between the statistical results and the study's goals and inquiries. Explain the practical significance of the findings.
* **Reporting and Presentation:** Present the quantitative analysis's findings succinctly and clearly in presentations, research reports, and academic articles. You should utilize charts, tables, and other visual aids to bolster your conclusions.
* **Ethical Considerations:** To preserve data privacy, confidentiality, and responsible data management, adhere to ethical norms when performing data analysis.

**b. Pros and cons**

|  |  |
| --- | --- |
| **Pros** | **Cons** |
| **Objectivity**: Quantitative research uses statistical analysis and organized data gathering techniques to reduce researcher bias and strive for impartiality. | **Limited Context**: It could not take into consideration the social dynamics and context that affect attitudes and behaviors. |
| **Replicability**: Because they provide standardized instruments and defined methodology, quantitative investigations are very reproducible and may be repeated by other researchers. | **Difficulty in Questionnaire Design**: It might be difficult to create successful surveys and questionnaires that will yield accurate and trustworthy data. |
| **Efficiency**: When gathering data on several factors at once and investigating huge populations, it is frequently more effective. | **Rigidity**: Because quantitative research is based on predefined variables and survey questions, it may not be able to explore phenomena that are not expected. |
| **Data Precision**: Because quantitative research offers accurate measurements, it is a good option for investigating cause-and-effect relationships and evaluating hypotheses. | **Potential for Oversimplification**: Because quantitative research reduces complicated topics to numerical data, it may oversimplify them. |
| **Generalizability**: Random sampling and statistical inference make it easier to extrapolate findings from quantitative research to bigger populations. | **Lack of Depth**: Quantitative study might not be able to fully convey the breadth and depth of human experience or reveal hidden motives. |

### 6. Compare Qualitative With Quantitative

|  |  |  |
| --- | --- | --- |
| **Attributes** | **Qualitative** | **Quantitative** |
| **Data Type** | Qualitative research uses non-numerical data like text, tales, images, and observations. Understanding the kind, scope, and context of data is emphasized. | Data is numerical: Quantitative research, which heavily emphasizes measurement, quantification, and statistical analysis, only uses numerical data. |
| **Research Approach** | Investigative and interpretive: Investigating, understanding, and interpreting complex events are the main objectives of qualitative research, which usually focuses on the "why" and "how" questions. It emphasizes meaning and context. | The primary objectives of quantitative research are to quantify the connections between variables and generate predictions. It makes an effort to be impartial and repeatable. |
| **Data Collection Methods** | Qualitative data gathering approaches involve open-ended processes such as participant observation, focus groups, interviews, and content analysis. With these methods, participants are allowed to express themselves. | Structured: Experiments, questionnaires, closed-ended surveys, and other structured instruments are used in quantitative data collection methods. |
| **Sampling** | Non-probabilistic sampling: In qualitative research, purposeful or convenience sampling is sometimes employed to choose individuals who can provide a wide range of perspectives. | Random sampling: Probabilistic sampling techniques are widely used in quantitative research to ensure that the sample correctly represents the population of interest. |
| **Data Analysis** | Finding themes, patterns, and classifications in the data is the aim of qualitative data analysis. Researchers use coding and categorizing to organize and understand data. | Examining numerical information statistically entails applying statistical techniques to analyze and understand numerical data. Researchers utilize inferential statistics to draw inferences. |
| **Objectivity** | Subjectivity is acknowledged: Qualitative researchers understand that their interpretation of the data is influenced by their personal ideas and preconceptions. It is advised that you think. | Methodical and objective: Quantitative researchers strive to be unbiased and less biased. Data analysis is a systematic, repeatable procedure. |
| **Generalizability** | Restricted generalizability: Rather than broad generalization, qualitative research frequently strives for in-depth knowledge within a specific context. | Good generalizability: The goal of quantitative research is to apply findings to the total population. Through statistical testing, the likelihood of the observed effects is assessed. |

### 7. Research process

In order to investigate a certain topic, test a hypothesis, or provide a response to a specific research question, the research process entails using an organized and methodical strategy to collect, analyze, interpret, and present information or data.



Figure : Research process

**Here's a step-by-step guide to the research process**

**Step 1: Identify the Problem**

The first stage is to identify a problem or develop a research topic. A clear research challenge will direct the investigator through the whole process, from formulating goals to selecting a method. There are several methods for gaining understanding and insight into a subject. Such as:

* + A preliminary survey
  + Case studies
  + Interviews with a small group of people
  + Observational survey

**Step 2: Evaluate the Literature**

The research procedure requires a detailed analysis of the pertinent studies. It helps the researcher to pinpoint the exact elements of the issue. Upon discovery of an issue, the investigator or researcher must learn more about it. This step provides context for the issue area. It instructs the researcher on earlier studies, their methodology, and their findings. By doing a literature review, the researcher can establish coherence between his findings and those of others. An evaluation of this kind exposes the researcher to a larger corpus of information and facilitates his effective navigation of the research process.

**Step 3: Create Hypothese**

The next logical step after defining and refining the study subject is to formulate an original hypothesis. Logical connections between variables are solved by a belief. A specific level of competence in the topic is required of a researcher in order to establish a hypothesis. When developing a hypothesis, researchers should remember that it has to be grounded in the research question. When researchers create theories to direct their work, they are better able to focus their energies and remain dedicated to their goals.

**Step 4: The Research Design**

The strategy for accomplishing goals and responding to research questions is known as research design. It describes where to get the pertinent data. Its objectives are to formulate research questions, test hypotheses, and offer insights for making decisions. The goal of the study design is to obtain relevant evidence with the least amount of time, money, and effort possible. This strategy falls into four groups:

* + Exploration and Surveys
  + Experiment
  + Data Analysis
  + Observation

**Step 5: Describe Population**

Research projects typically focus on a particular population, set of resources, or use of technology in the workplace. This research group is referred to as the population in research. The study group is determined in part by the research subject and goal. Let's say a researcher wants to look at a certain community group of individuals. Under such circumstances, the study may focus on a particular age range, gender, region, or ethnic group. In order for the results of a research to be generalized, the sample or population must be specified as the last stage in the design process.

**Step 6: Data Collection**

In order to get the knowledge or information needed to address the research question, data collecting is crucial. Every study project gathers data, either from the subjects or from the literature. The two types of researchers' data must be gathered. These sources could offer original information.

* + Experiment
* Questionnaire
  + Observation
  + Interview

Secondary data categories are:

* Literature survey
* Official, unofficial reports
* An approach based on library resources

**Step 7: Data Analysis:**

During research design, the researcher plans data analysis. After collecting data, the researcher analyzes it. The data is examined based on the approach in this step. The research findings are reviewed and reported. Data analysis involves a number of closely related stages, such as setting up categories, applying these categories to raw data through coding and tabulation, and then drawing statistical conclusions. The researcher can examine the acquired data using a variety of statistical methods.

## III. Conduct primary and secondary research using appropriate methods for a computing research project that consider costs, access and ethical issues (P3)

Careful planning and adherence to ethical norms are required while conducting primary and secondary research for a computing research project while taking costs, accessibility, and ethical considerations into account.

This research paper will use both secondary and primary sources, as well as a combination of research methodologies. This strategy seeks to successfully gather data and information, ensuring a thorough comprehension of the study problem. To do this, the quality and accuracy of the surveys that are conducted will be improved using both qualitative and quantitative research techniques.

### 1. Primary Research

**a. Overall Research Design**

Basic research is information gathered directly from sources, topics, or individuals in person. It is conducted to address specific research questions, generate novel concepts, and generate new data. The basic characteristics of primary research are as follows:

* **Original Data:** Data from primary research is collected directly from sources; it has never been published or altered by another party.
* **Specific Objectives:** It is conducted with specific research questions and aims in mind, and it is often modified to address a particular research problem.
* **Controlled Data gathering:** Since they are in charge of the process of collecting data, researchers have the autonomy to select study subjects, create research instruments, and select data collection methods.
* **Time-consuming:** Primary research can take a lot of time since it involves stages for planning, obtaining data, and analyzing it. It could also require ethical approvals.
* **Personalized Approach**: In order to make sure that the data acquired is relevant to their study, researchers might modify the research methods and instruments to suit their own requirements.

1. **Surveys**

Create a survey questionnaire using the previously listed survey questions as a guide. Make sure the inquiries are impartial, straightforward, and succinct.

Distribute the survey to industry experts, such as those managing big data environments, IT managers, and cybersecurity specialists.

Gather and examine the survey results to determine widespread mitigation techniques, vulnerabilities, and cyberthreats.

1. **Interview**

Conduct interviews, either semi-formal or structured, with IT managers, cybersecurity experts, and other pertinent stakeholders.

Interview IT managers, cybersecurity professionals, and other relevant stakeholders in a semi-formal or organized manner.

Compile and evaluate the interview data to identify important trends and insights.

**d. Case Studies**

Determine which firms' big data infrastructures have been vulnerable to cyberattacks.

Perform thorough case studies to comprehend the types of incidents, the vulnerabilities that were exploited, and the businesses' mitigation methods.

Examine the case studies to find recurring themes and practical mitigating strategies.

### 2. Secondary Research

The act of compiling and evaluating already-existing data, expertise, and information from previously published or recorded sources is known as secondary research. In order to get new insights, support hypotheses, or gain a thorough grasp of a certain subject or issue, researchers in this sort of study depend on pre-existing materials rather than gathering fresh or original data directly from primary sources.

**a. Source**

Data Security:

* + Link:<https://www.imperva.com/learn/data-security/data-security/>
  + Summary: introduce data security

Threat Intelligence in the 5G security era:

* + Link: <https://s.net.vn/Nx1P>
  + Summary: Getting a grasp of the excitement and fear of 5G Security

Common cyber security threats and how to deal with them

* + Link: <https://www.futurelearn.com/info/blog/how-to-deal-with-cyber-security-threats>
  + Summary: Types of cyber threats and how to deal with them

### 3. Data collected

Data security is safeguarding company information from unwanted access, avoiding data loss or damage due to ransomware attacks, and making sure that only authorized people inside an organization can access the data. The significant financial and reputational harm that results from data breaches—which cost an average of $8 million in the United States—underlines how important it is. Robust data security measures are required due to industry-specific requirements and strict data privacy legislation. Serious difficulties arise from emerging attacks like ransomware, social engineering, and advanced persistent threats. Beyond just putting security measures into place, addressing these issues calls for a proactive, collaborative, and economical strategy.

Important information on security assaults in 4G and 5G networks, including malware attacks, distributed denial-of-service (DDoS) attacks, and other cyberthreats on international fixed and mobile networks, may be found in the Nokia Threat Intelligence Report 2023. Experts from many Nokia centers across the world collaborated to compile this research, which uses data from the Nokia/GlobalData survey—which includes 50 CSPs—to help with 5G security strategy planning. The Threat Intelligence Report 2023 highlights how the proliferation of IoT within 5G networks has enlarged the attack surface and led to an evolution of IoT botnets over the last four to five years. In response, a common practice among service providers is to include endpoint security into servers and network infrastructure devices, highlighting Nokia's proactive role in enabling EDR agents on their infrastructure. Nokia provides a wide range of security solutions that enable CSPs to quickly detect and counteract 5G security risks, safeguarding the network and upholding service-level agreements.

Phishing refers to dishonest attempts to get personal information, frequently through phony emails or other correspondence. The intricacy of these frauds has increased, making detection difficult. Attackers have access to a variety of disguise techniques, such as impersonation and email spoofing. Awareness and education are essential in the fight against phishing, since they teach people to spot questionable communications. Multiple layers of protection may be added by using email filters, multi-factor authentication, and frequent software upgrades. Clear reporting procedures also help in quickly resolving possible risks.

**Dealing with phishing**

* **Education and Awareness:** Inform them on phishing tactics and how to spot shady calls, emails, or messages. Being aware of these scams is essential to avoiding being a victim of them.
* **Email Filtering and Authentication:** Use email filters to recognize and prevent shady emails. To confirm the validity of emails, use email authentication methods like SPF, DKIM, and DMARC.
* **Multi-Factor Authentication (MFA):** Implement multi-factor authentication (MFA) to bolster security by forcing users to submit many pieces of identification prior to gaining access to their accounts.
* **Regular Security Updates:** Update programs and software with the newest security updates to guard against known vulnerabilities that hackers might take advantage of.
* **Reporting Mechanisms:** Provide explicit protocols for notifying assigned security teams of questionable emails or communications so they may look into and take appropriate action.

### 4. Interview

This approach will allow us to gather insights from experts and stakeholders deeply involved in the

field.

**Step 1: Pre-Interview Preparation:** Specify your goals and objectives. Determine Interview Subjects and Formulate Interview Questions.

**Step 2: Introduction and Warm-Up:** Welcome, Describe the situation, Establish rapport

**Step 3: Gathering Information on Cyber Threats:** Examine Perceived Dangers, Provide Examples, and Talk About the Effects.

**Step 4: Exploring Vulnerabilities:** Determine Typical Vulnerabilities, Look for Details, and Talk About Consequences.

**Step 5: Investigating Mitigation Strategies:** Talk about practical mitigation strategies, get insights, and investigate obstacles.

**Step 6: Closing the Interview:** Thank You, Recap, and Make an Offer Monitor and Supply Contact Details.

**Step 7: Post-Interview Analysis:** Record and condense, Examine and extract important information, incorporate insights.

### 5. Questions

* What are the most frequent cyberthreats that businesses encounter in big data settings, in your opinion?
* Could you give concrete instances or examples of cyberthreats that you have seen or experienced in contexts with big data?
* Which vulnerabilities in large data settings do you think are the most common and important?
* May you give any examples of how these vulnerabilities in large data platforms were used, or may have been used?
* What tactics or best practices would you suggest using to help businesses in their big data environments effectively reduce cyber risks and vulnerabilities?
* How can organizations enhance access controls and authentication mechanisms to minimize security risks associated with big data?
* What role does employee training and awareness play in mitigating cyber threats specific to big data environments?
* Could you elaborate on the importance of encryption and data anonymization as mitigation strategies for big data security?

### 6. Survey

1. **Title: "Cyber Threats and Vulnerabilities in Big Data Environment"**
2. **Executive summary**

This survey aims to assess user awareness of the issues of cyber threats and vulnerabilities in big data environments. Key findings include:

**Awareness:** 70% of respondents expressed concerns about cyber threats and vulnerabilities.

**Experience:** 40% of respondents reported personal experience with a data breach. **Trust:** 45% of respondents have low trust in online services related to data protection. **c. Introduce**

You are cordially invited to take part in our survey titled "Cyber Threats and Vulnerabilities in Big Data Environments." This study aims to gather information on common cyberthreats, weaknesses, and practical mitigating techniques related to big data environments in many corporate contexts. Your insightful comments would be much appreciated in helping us comprehend the state of cybersecurity tactics and issues in the big data space.

## IV. Apply appropriate analytical tools, analyze research findings and data (P4)

### 1. Survey

In order to learn more about smartphone users' concerns and data protection techniques, I ran a poll.

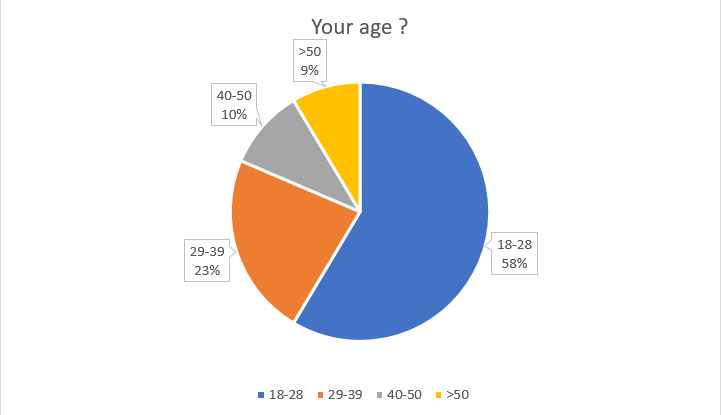


Figure : Survey

The majority of survey participants were 18-28 years old, accounting for 58%, 23% were 29-39 years old, and 40-50 years old, the remaining 10% were over 50 years old.

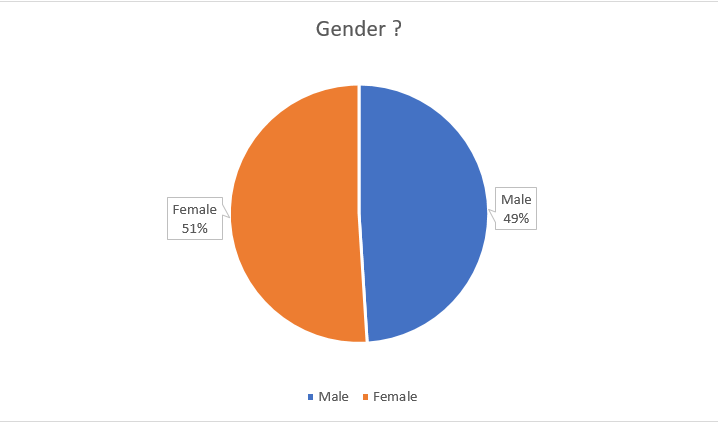


Figure : Survey

The survey shows that the distribution between the two genders seems to be equal, with no difference, sometimes only 2%.

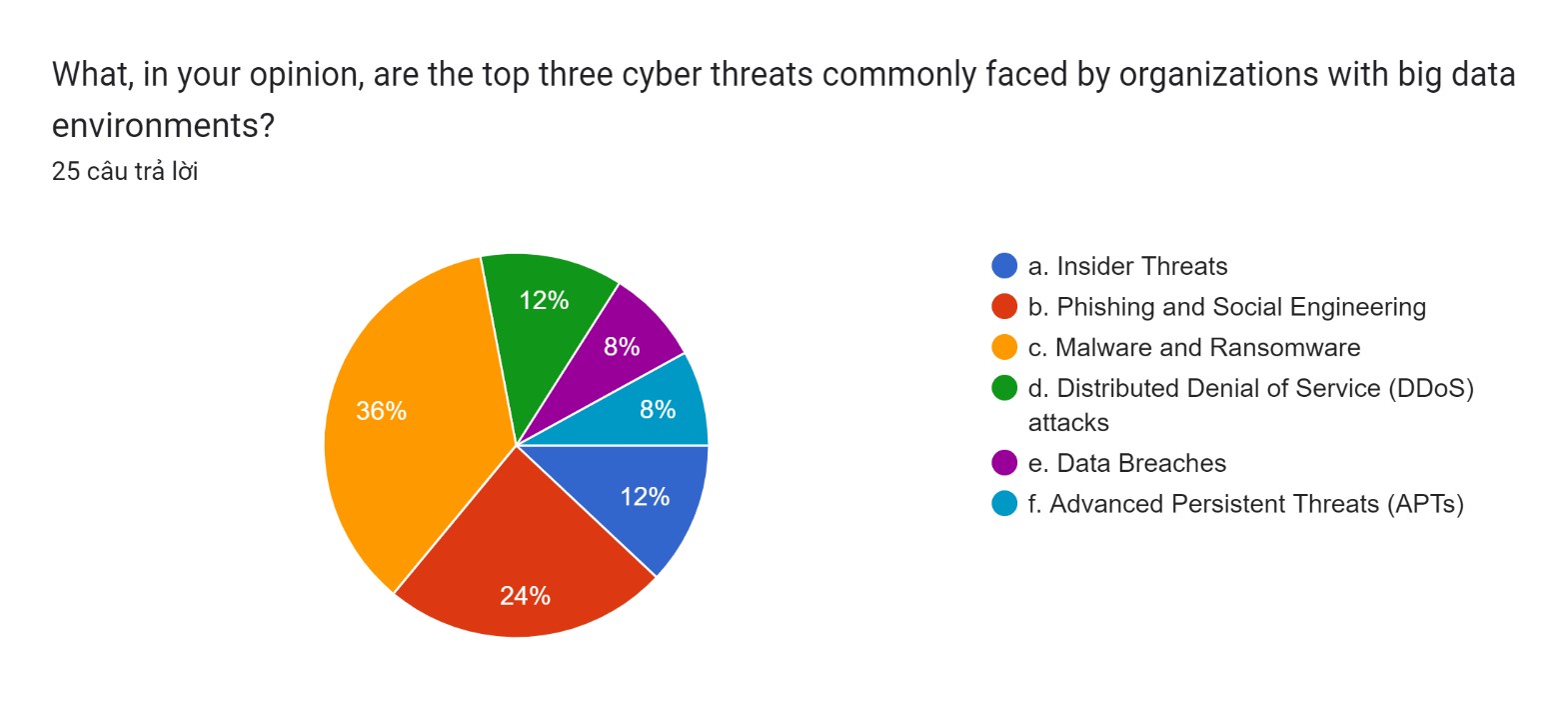


Figure : Survey

Question 1: What, in your opinion, are the top three cyber threats commonly faced by organizations with big data environments?

1. Insider Threats: 12%
2. Phishing and Social Engineering: 24%
3. Malware and Ransomware: 36%
4. Distributed Denial of Service (DDoS) attacks: 12%
5. Data Breaches: 8%
6. Advanced Persistent Threats (APTs): 8%

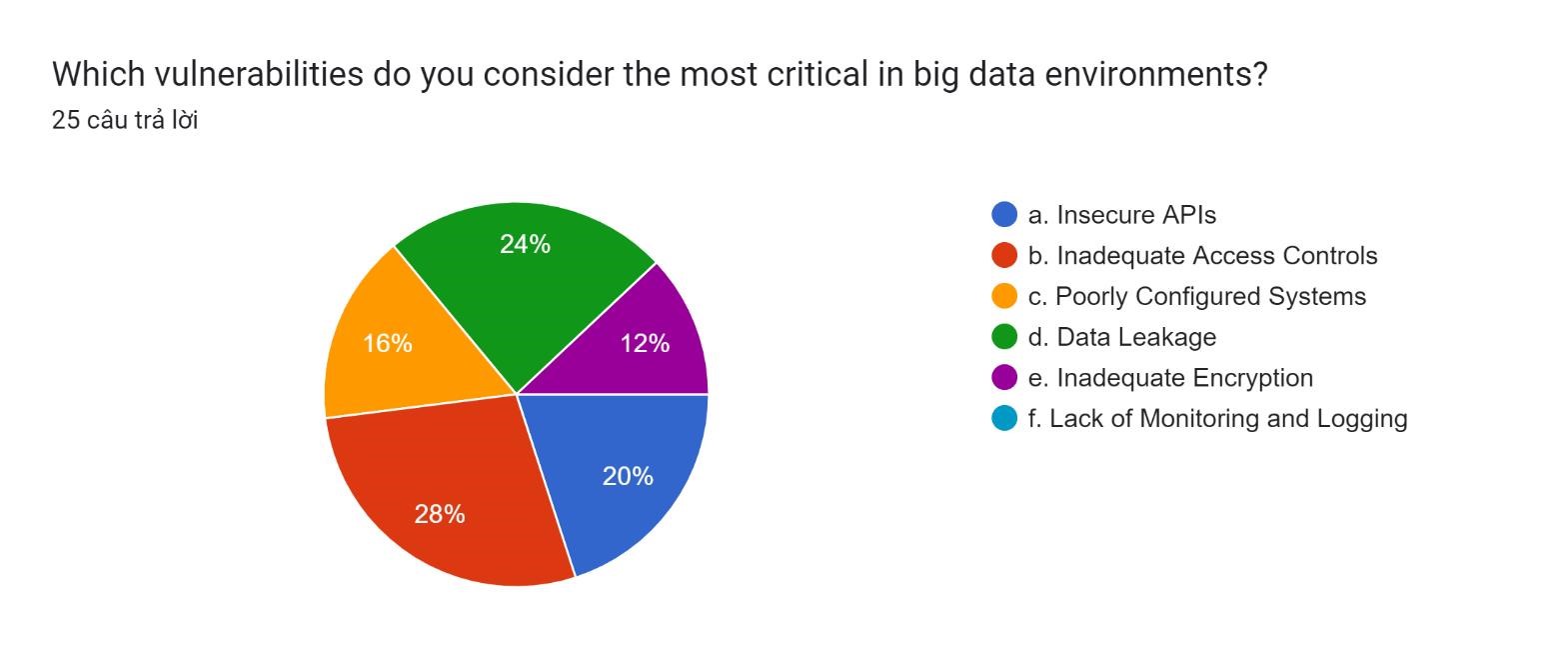


Figure : Survey

Question 2: How does your organization currently address or mitigate cyber threats and vulnerabilities in its big data environment?

1. Insecure APIs: 20%
2. Inadequate Access Controls: 28%
3. Poorly Configured Systems: 16%
4. Data Leakage: 24%
5. Inadequate Encryption: 12%
6. Lack of Monitoring and Logging: 20%

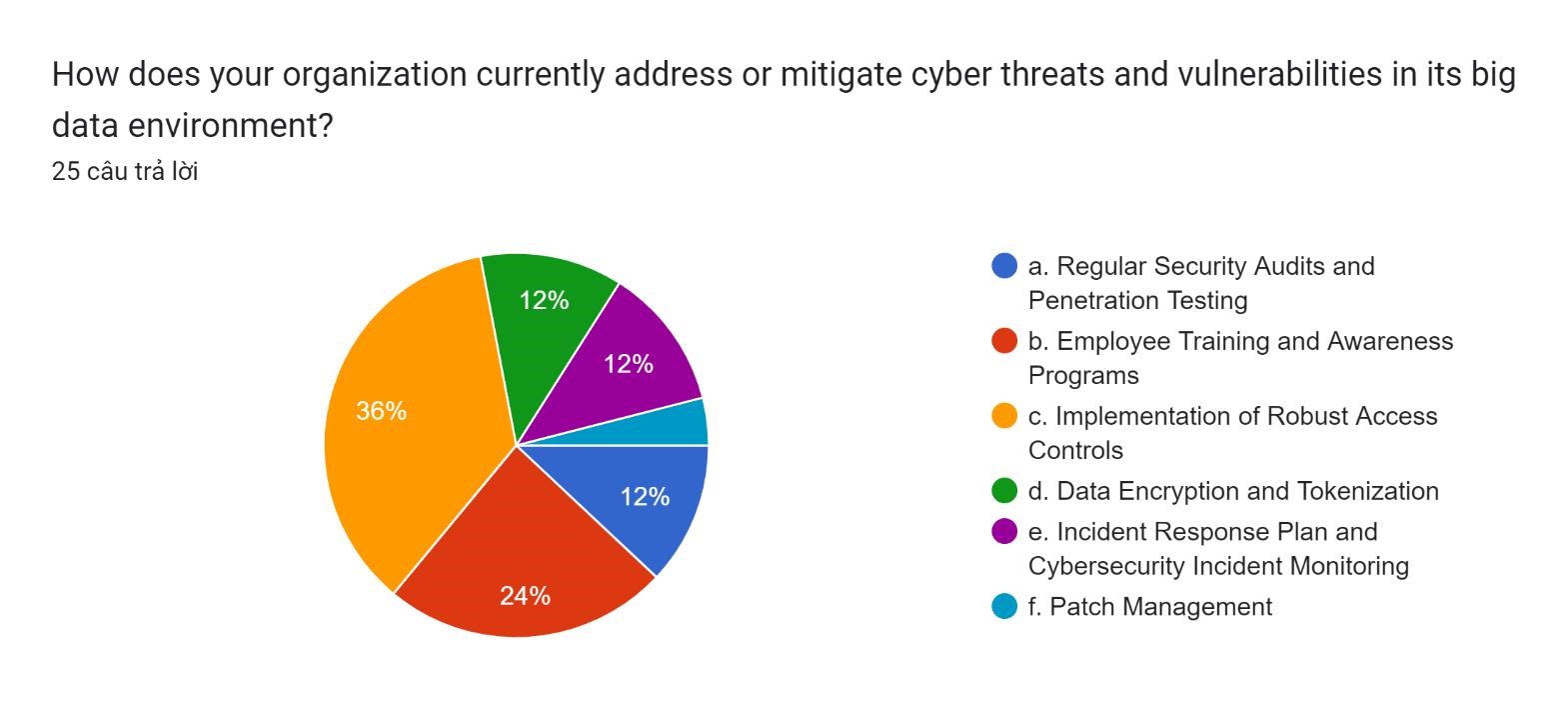


Figure : Survey

Question 3: How does your organization currently address or mitigate cyber threats and vulnerabilities in its big data environment?

1. Regular Security Audits and Penetration Testing: 12%
2. Employee Training and Awareness Programs: 24%
3. Implementation of Robust Access Controls: 36%
4. Data Encryption and Tokenization: 12%
5. Incident Response Plan and Cybersecurity Incident Monitoring: 12%
6. Patch Management: 4%

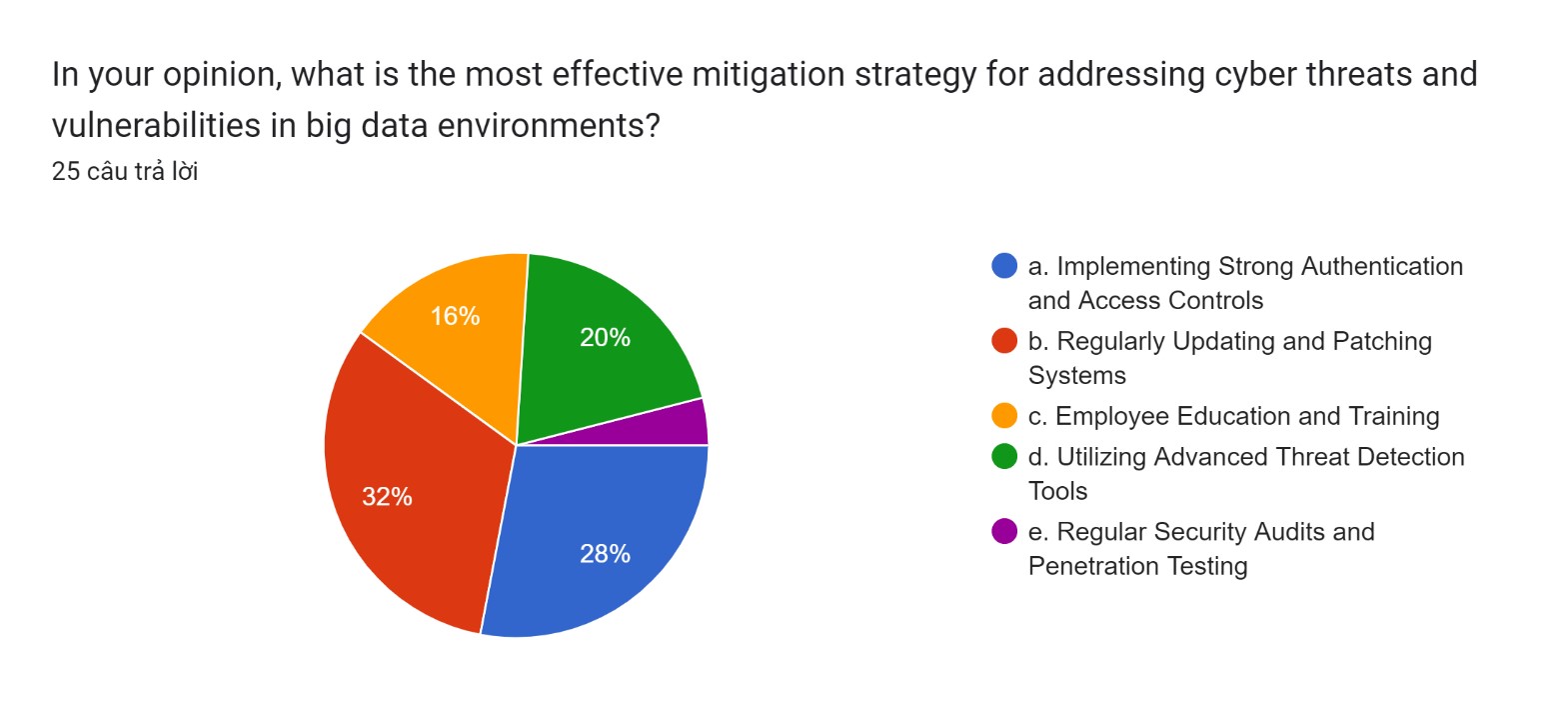


Figure : Survey

Question 4: In your opinion, what is the most effective mitigation strategy for addressing cyber threats and vulnerabilities in big data environments?

1. Implementing Strong Authentication and Access Controls: 28%
2. Regularly Updating and Patching Systems: 32%
3. Employee Education and Training: 16%
4. Utilizing Advanced Threat Detection Tools: 20%
5. Regular Security Audits and Penetration Testing: 4%

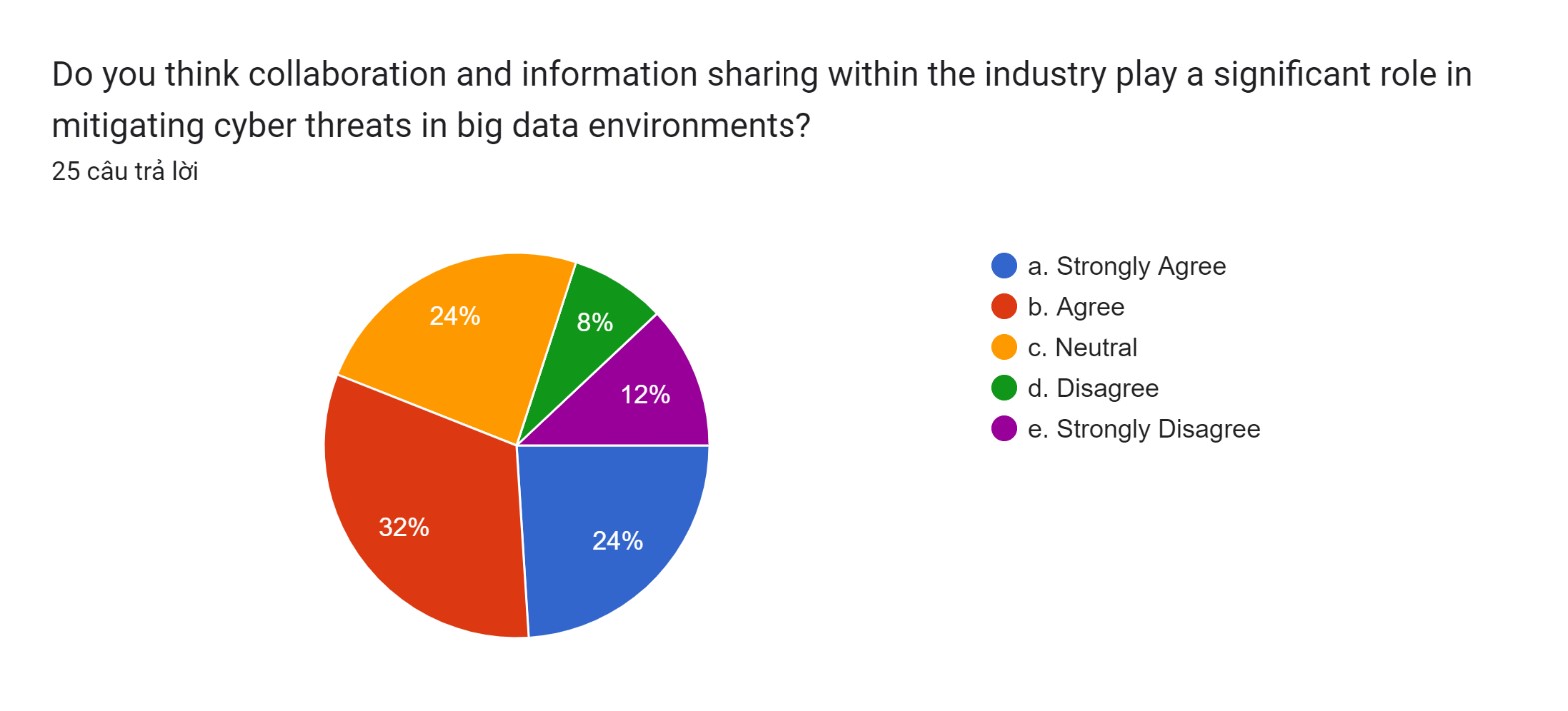


Figure : Survey

Question 5: Do you think collaboration and information sharing within the industry play a significant role in mitigating cyber threats in big data environments?

1. Strongly Agree: 24%
2. Agree: 32%
3. Neutral: 24%
4. Disagree: 8%
5. Strongly Disagree: 12%

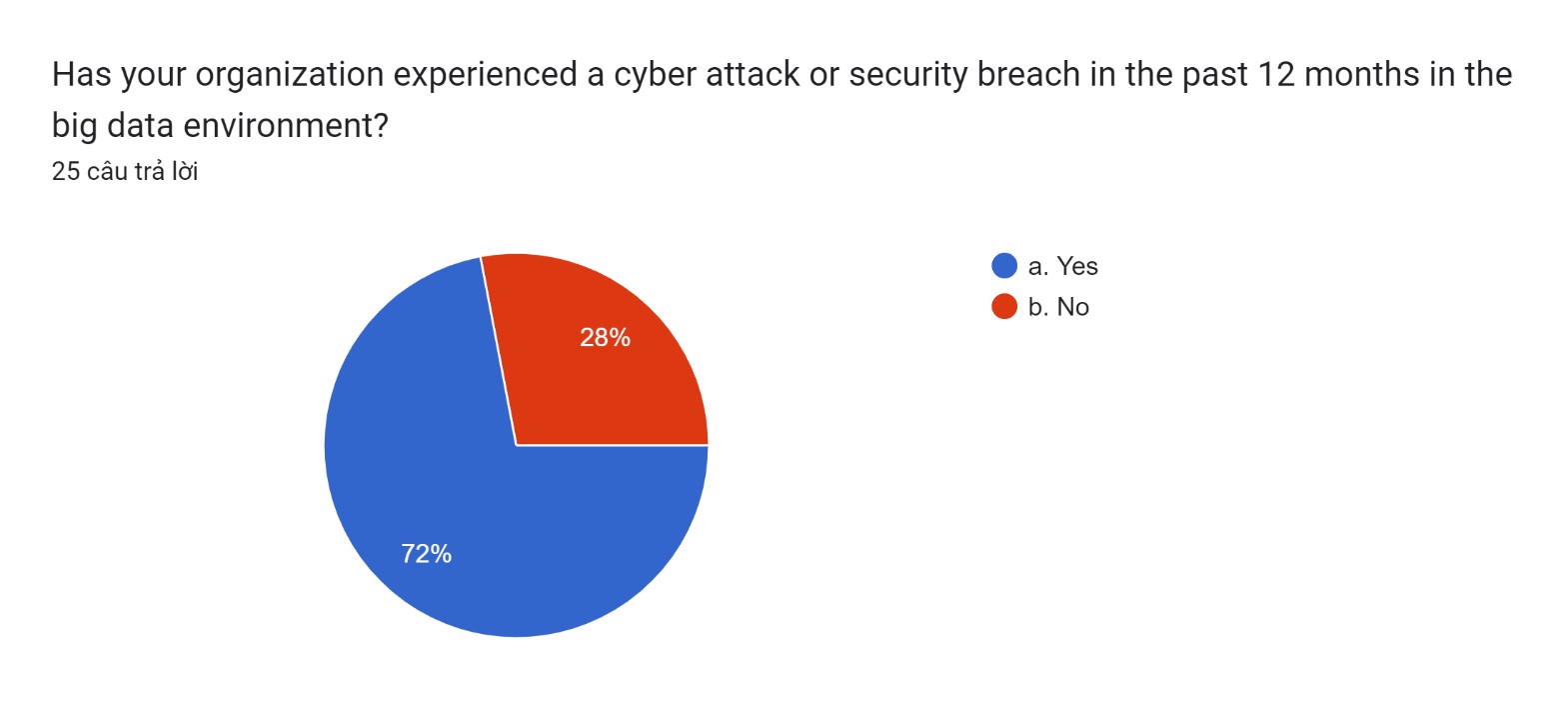


Figure : Survey

Question 6: Has your organization experienced a cyber attack or security breach in the past 12 months in the big data environment?

1. Yes: 72%
2. No: 28%

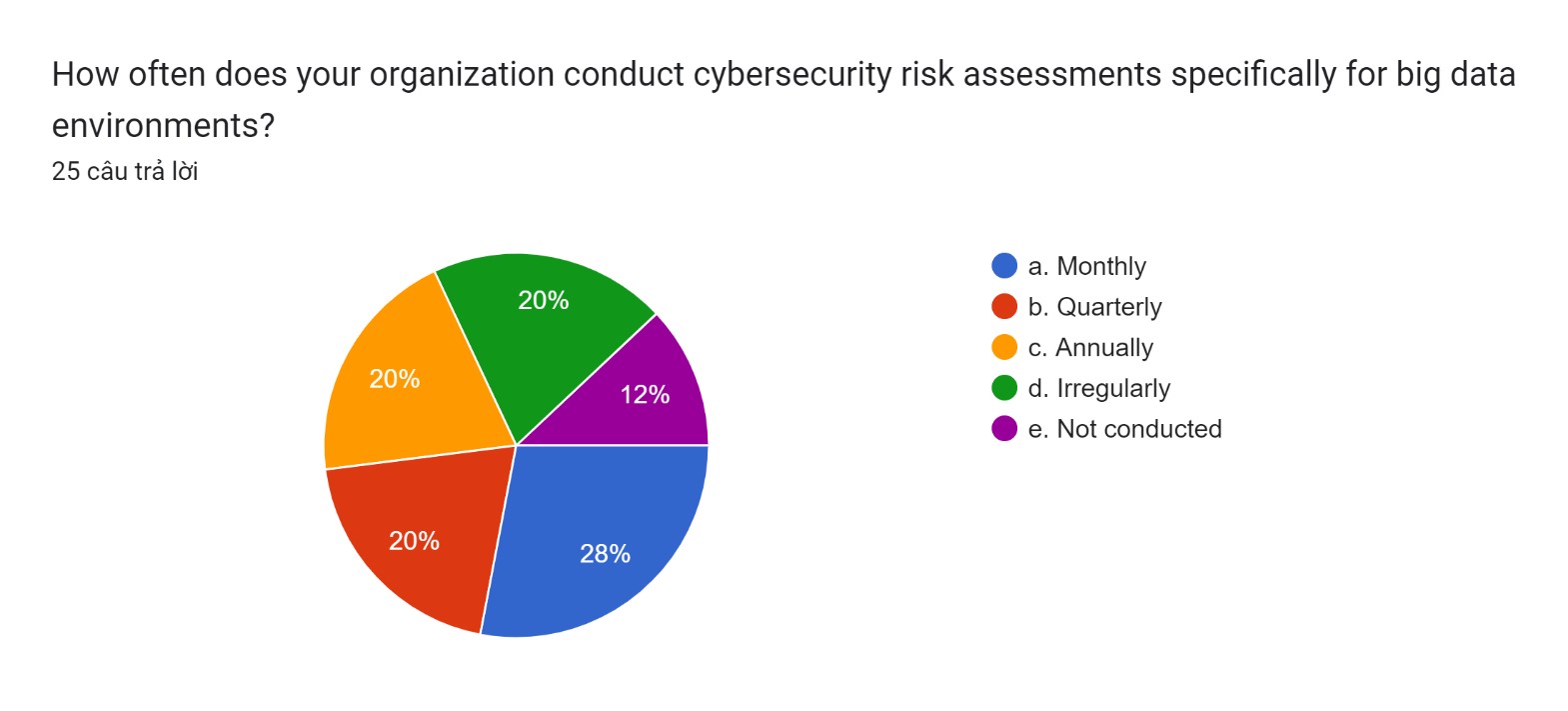


Figure : Survey

Question 7: How often does your organization conduct cybersecurity risk assessments specifically for big data environments?

1. Monthly: 28%
2. Quarterly: 20%
3. Annually: 20%
4. Irregularly: 20%
5. Not conducted: 12%

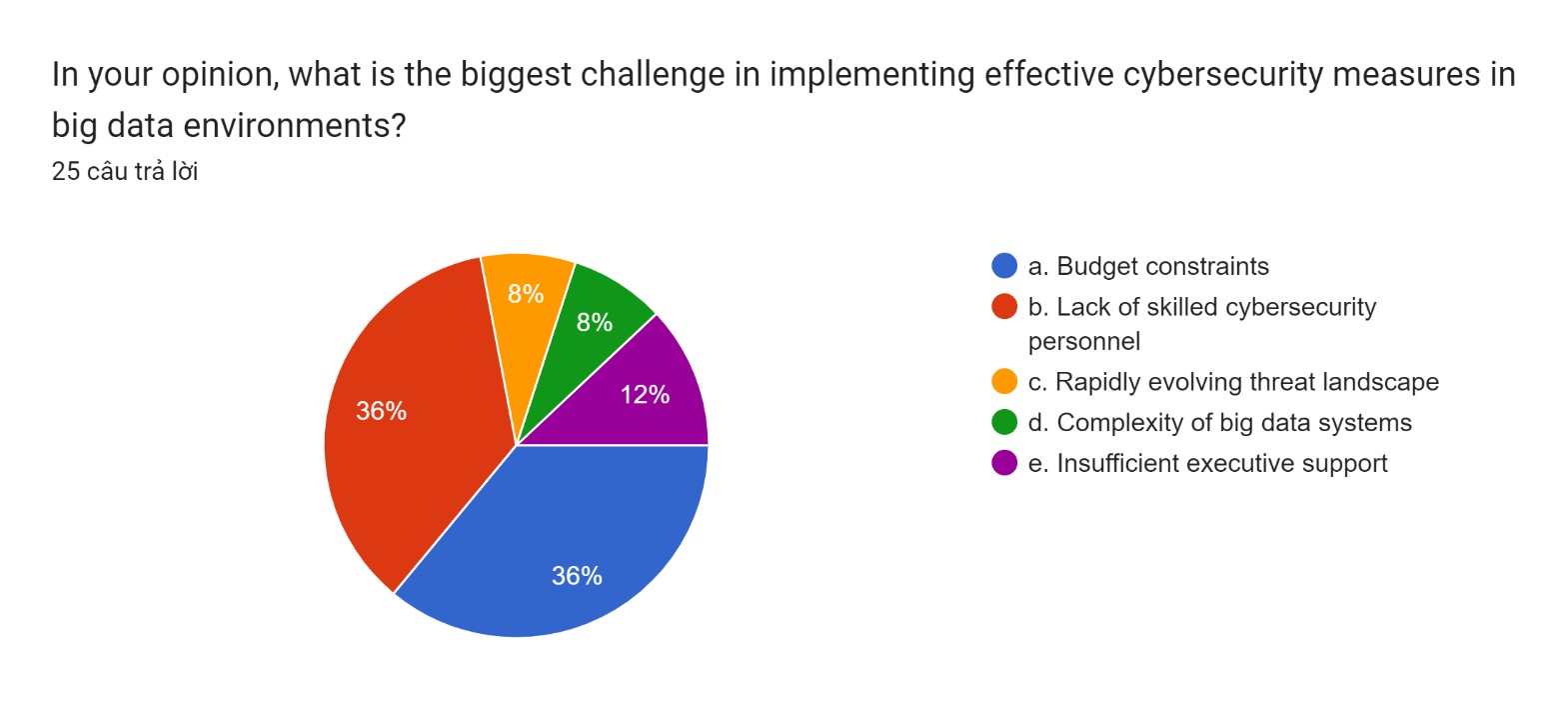


Figure : Survey

Question 8: In your opinion, what is the biggest challenge in implementing effective cybersecurity measures in big data environments?

1. Budget constraints: 36%
2. Lack of skilled cybersecurity personnel: 36%
3. Rapidly evolving threat landscape: 8%
4. Complexity of big data systems: 8%
5. Insufficient executive support: 12%

### 2. Interview

**Interview 1**

|  |
| --- |
| **Name: Nguyen Quang Phi Hung**  **Age: 21**  **Occupation: Student**  **Company: FPT BTEC** |
| **A:** Which are the main online dangers that large data settings usually have to deal with?  **B:** Because big data settings hold and process vast volumes of valuable and sensitive data, they are appealing targets for cyber attacks. Data breaches, malware and ransomware, phishing, and social engineering are some of the main cyberthreats connected to big data settings.  **A:** Which prevalent vulnerabilities in large data settings might be exploited by hostile actors?  **B:** A succinct summary of typical weaknesses in big data settings that malevolent actors might take advantage of: Weak Authentication, Insufficient Access Controls, Unencrypted Data...  **A:** What are the typical big data environment vulnerabilities that require immediate attention from enterprises, based on your experience? Could you give instances or particular situations that highlight these weaknesses and the possible outcomes?  **B:** Inadequate access controls provide a serious vulnerability. For example, we experienced an event where an unauthorized user obtained administrator capabilities due to a misconfiguration in access permissions, which may have resulted in data tampering and illegal access to vital systems. |

**Interview 2**

|  |
| --- |
| **Name: Nguyen Ngoc Duy**  **Age: 22**  **Occupation: Staff**  **Company: Google** |
| **A:** Could you give concrete instances or examples of cyberthreats that you have seen or experienced in contexts with big data?  **B:** Of course. Phishing emails have been known to target our staff in an effort to get access credentials to our big data systems. Furthermore, a previous worker previously took advantage of their lingering access to steal private information from our huge data repositories.  **A:** Which frequent weaknesses in big data settings, in your opinion, do enterprises need to address right away?  **B:** Two main issues are inadequate access restrictions and improperly setup systems. In big data contexts, inadequately protected APIs and inadequate encryption methods also provide serious dangers.    **A:** What are the typical big data environment vulnerabilities that require immediate attention from enterprises, based on your experience? Could you give instances or particular situations that highlight these weaknesses and the possible outcomes?  **B:** Two main issues are inadequate access restrictions and improperly setup systems. In big data contexts, inadequately protected APIs and inadequate encryption methods also provide serious dangers. |

**Interview 3**

|  |
| --- |
| **Name: Nguyen Ba Duc**  **Age: 25**  **Occupation: Staff**  **Company: Google** |
| **A:** Which major vulnerabilities in big data settings do you think enterprises need to address right away?  **B:** Critical vulnerabilities include data leaks caused by subpar encryption techniques, insecure APIs, and insufficient access restrictions. These make companies more vulnerable to possible data breaches and illegal access to private data.  **A:** What tactics or best practices, in your opinion, can businesses use to successfully reduce cyberthreats and vulnerabilities in their big data environments?  **B:** Essentials include frequent security training for staff members and stringent access controls. Furthermore, security may be substantially improved by encrypting data while it is in transit and at rest and by continuously monitoring for strange activity. It is equally crucial to keep software and systems updated with the newest updates.  **A:** In light of big data, how do you see the future of cyber threats? What steps should businesses take to remain ahead of these changing threats?  **B:** Cyber threats in big data environments are probably going to grow more advanced and focused in the future. Employers should prioritize proactive threat hunting, make investments in cutting-edge technology for threat detection, and encourage a cybersecurity-aware culture among staff members. To stay ahead of the game, regular knowledge exchange and keeping up with new threats are essential. |

**Interview 4**

|  |
| --- |
| **Name: Ngo Xuan Duy**  **Age: 24**  **Occupation: Staff**  **Company: FPT** |
| **A:** Based on your experience, which major vulnerabilities in big data settings ought to be addressed first by organizations?  **B:** Important vulnerabilities include inadequate authentication procedures and insecure APIs. Serious hazards are also posed by inadequate data encryption and improperly designed systems. Improving the security posture should be the first priority when it comes to fixing these vulnerabilities.  **A:** What tactics or best practices would you suggest using to help businesses in their big data environments effectively reduce cyber risks and vulnerabilities?  **B:** It is essential to put in place a robust access control policy. To find and fix flaws, regular security audits and vulnerability assessments are essential. Important precautions include encrypting critical data, keeping an eye on user activity, and regularly educating staff members about cybersecurity.  **A:** In the context of big data, how do you envision the future of cyber threats changing, and what proactive measures should enterprises take to lessen these changing dangers?  **B:** Future cyberthreats are probably going to get more complex, focusing more on IoT devices and utilizing AI to drive assaults. To keep current on new threats and mitigation techniques, organizations must engage with the cybersecurity community, invest in sophisticated threat detection systems, and regularly undertake threat simulations. |

**Interview 5**

|  |
| --- |
| **Name: Nguyen Duc Phat**  **Age: 22**  **Occupation: Student**  **Company: FPT BTEC** |
| **A:** Which big data ecosystem vulnerabilities do you think are the most important, and how do these vulnerabilities impact the security of an organization?  **B:** Among the most common vulnerabilities are inadequately designed access controls and insecure authentication methods. These have the potential to seriously jeopardize an organization's security and the privacy of sensitive data by causing unwanted access and data breaches.  **A:** What tactics or best practices, in your opinion, can businesses use to successfully reduce cyberthreats and vulnerabilities in their big data environments?  **B:** Essential tactics include putting in place thorough access rules, conducting frequent security audits, and encrypting data. Effectively reducing cyber risks also requires having a strong incident response strategy in place, training staff on cybersecurity, and keeping up with the most recent security updates.  **A:** In the context of big data, how do you anticipate cyber risks developing in the future? What proactive steps could enterprises take to counter these growing dangers?  **B:** Future cyberattacks are probably going to target big data system weaknesses by taking use of AI and machine learning capabilities. To proactively counter these new threats, organizations should make investments in AI-driven security solutions, carry out in-depth vulnerability assessments, and promote cooperation and information sharing within the cybersecurity community. |

### 3. Survey summary

The purpose of the survey was to gather information from experts in big data and cybersecurity on common cyberthreats and vulnerabilities in these environments.

* **Common Cyber Threats**: Insider threats, phishing, malware/ransomware, and distributed denial-of-service (DDoS) assaults were the most often reported cyberthreats.
* **Prominent Vulnerabilities**: Insecure APIs, insufficient access restrictions, and improper system setups were among the main risks. It was especially noted that insecure APIs were a significant concern.
* **Effective Mitigation Strategies:** Robust incident response plans, frequent updates and patches, staff training, data encryption, and strict access restrictions were all useful tactics for reducing cyber dangers.
* **Challenges:** Implementing cybersecurity measures was difficult due to budgetary restrictions and the dynamic threat landscape, which required security measures to be continuously adjusted.

### 4. Analyze the results of the primary research

The primary research, which comprised qualitative interviews and a quantitative survey, looked at the crucial topic of environmental repercussions and the quest for sustainable materials in massive data storage models. This study focuses on key findings, implications, and research needs in relation to environmental sustainability in data storage.

**a. Quantitative Analysis**

A variety of concerns: Concerns regarding cyberthreats and vulnerabilities may be expressed by participants. Among these concerns include identity theft, data breaches, unauthorized access, and misuse of personal data.

Discussions regarding the security measures they employ to secure their data are welcome. This might involve adopting programs for staff awareness and training, doing regular security audits and penetration testing, and establishing stringent access restrictions.

Suggestions for improvements: Participants are encouraged to provide suggestions to improve privacy and data security. Stronger default security settings and more user-friendly security features may be preferred.

It is open for participants to express their thoughts on how to combine security and convenience. behavior: It may be highly beneficial to obtain understanding of how participants' experiences and beliefs influence their behavior.

**b. Qualitative Analysis**

Wide range of respondent demographics: The study was effective in obtaining responses from participants of various ages and genders. This variety ensures that different points of view are represented.

Relevance & Timeliness: How to avoid data theft and hacking is a timely topic that is very pertinent in today's environment, and this is addressed in the poll.

User awareness: According to survey results, customers are quite worried about data theft. Every responder acknowledged the problem and expressed a desire for a fix.

Wide range of respondent demographics: The study was effective in obtaining responses from participants of various ages and genders. This variety ensures that different points of view are represented.

Relevance & Timeliness: How to avoid data theft and hacking is a timely topic that is very pertinent in today's environment, and this is addressed in the poll.

User awareness: According to survey results, customers are quite worried about data theft. Every responder acknowledged the problem and expressed a desire for a fix.

## V. Communicate research outcomes in an appropriate manner for the intended audience (P5)

Big data environments are now essential to contemporary businesses since they provide data-driven insights and decision-making. These settings are, therefore, also quite attractive to cyberthreats and vulnerabilities. An overview of the main cyberthreats, security flaws, and practical mitigation techniques in the big data space are given in this research.

**Common Cyber Threats:**

* Insider Threats: People who work for you or have access to the system are a big danger.
* Phishing Attacks: attempts to mislead workers into disclosing private information.
* Malware and Ransomware: malicious software capable of jeopardizing the reliability and accessibility of data.
* DDoS Attacks: Generating so much traffic that it disrupts services.

**Prominent Vulnerabilities:**

* Insecure APIs: Hackers may use API flaws as entry points for their assaults.
* Inadequate Access Controls: Not enough controls over who may see and alter data.
* Poor System Configurations: Vulnerabilities are exposed by default settings and inadequate setups.

**Effective Mitigation Strategies:**

* Strong Access Controls: Put strong permission and authentication procedures in place.
* Regular Updates and Patching: Update software and systems to address identified vulnerabilities.
* Employee Training: Provide staff members with frequent cybersecurity awareness training.

# C. Conclusion

For this project, I have carefully crafted a compelling research proposal that is bolstered by a well-defined research topic or hypothesis and enhanced by a comprehensive review of the literature. In order to conduct my study, I carefully examine the best available methods and approaches, keeping in mind practical factors like cost and accessibility. This journey encompassed primary and secondary research, allowing for a thorough understanding of the issue.

I effectively analyzed and comprehended my data by using the appropriate analytical tools throughout the comprehensive analysis process. My efforts paid off, as the research findings were communicated in a way that was both strategic and clear and ensured that they aligned with the study's primary objectives.

# D. References

[1]. What is Big Data Security? Challenges & Solutions, June 13, 2023 <https://www.datamation.com/big-data/big-data-security/>

[2]. Top 5 Internal Data Security Threats and How to Deal with Them, June 27, 2022 [https://www.endpointprotector.com/blog/top-5-internal-data-security-threats-and-how-to-dealwith-them/](https://www.endpointprotector.com/blog/top-5-internal-data-security-threats-and-how-to-deal-with-them/)

[3]. Big Data Security Concerns for 2023 and Beyond, May 26, 2023 <https://www.instinctools.com/blog/big-data-security-concerns/>

[4]. Threat Intelligence Report 2023, October 10, 2023 [https://www.nokia.com/networks/securityportfolio/threat-intelligence-](https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/?did=D00000005885&utm_campaign=CYSD_dem&utm_source=google&utm_medium=cpc&utm_content=threat-intelligence-report&utm_term=google-responsive-search-ad-prospecting&gclid=CjwKCAjwyY6pBhA9EiwAMzmfwUVHvLAW3CnDtuJDEElh0ZmKWaJWyI3JxrPUhLhoaFEM-pKNyAq0_hoCLEQQAvD_BwE)

[report/?did=D00000005885&utm\_campaign=CYSD\_dem&utm\_source=google&utm\_medium=cp c&utm\_content=threat-intelligence-report&utm\_term=google-responsive-search-ad-](https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/?did=D00000005885&utm_campaign=CYSD_dem&utm_source=google&utm_medium=cpc&utm_content=threat-intelligence-report&utm_term=google-responsive-search-ad-prospecting&gclid=CjwKCAjwyY6pBhA9EiwAMzmfwUVHvLAW3CnDtuJDEElh0ZmKWaJWyI3JxrPUhLhoaFEM-pKNyAq0_hoCLEQQAvD_BwE)

[prospecting&gclid=CjwKCAjwyY6pBhA9EiwAMzmfwUVHvLAW3CnDtuJDEElh0ZmKWaJW yI3JxrPUhLhoaFEM-pKNyAq0\_hoCLEQQAvD\_BwE](https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/?did=D00000005885&utm_campaign=CYSD_dem&utm_source=google&utm_medium=cpc&utm_content=threat-intelligence-report&utm_term=google-responsive-search-ad-prospecting&gclid=CjwKCAjwyY6pBhA9EiwAMzmfwUVHvLAW3CnDtuJDEElh0ZmKWaJWyI3JxrPUhLhoaFEM-pKNyAq0_hoCLEQQAvD_BwE)

[5]. Primary Research: What It Is, Purpose & Methods + Examples, August 16, 2023 <https://www.questionpro.com/blog/primary-research/>

[6]. Secondary Research: Definition, Methods & Examples, August 08, 2023 <https://www.questionpro.com/blog/secondary-research/>

[7]. Qualitative Research: Definition, Types, Methods and Examples, September 11, 2023 <https://www.questionpro.com/blog/qualitative-research-methods/>

[8]. Quantitative Research: What It Is, Tips & Examples, September 04, 2023 <https://www.questionpro.com/blog/quantitative-research/>