LUKE LITTLER 132290

HOPWOOD HALL COLLEGE

HTQ COMPUTING RQF

UNIT 6: PLANNING A COMPUTING PROJECT

SDC PROJECT PLAN

Contents

1. Project Scope

This project aims to comprehensively assess and mitigate cybersecurity risks associated with big data storage (both local and cloud-based) at SDC. It will identify vulnerabilities, evaluate existing security measures, assess employee awareness, and develop a prioritised action plan to enhance data protection while aligning with business objectives and regulatory requirements.

1.1 Project Objectives

Primary Objective:

To assess the current state of cybersecurity risks in big data storage at SDC:

- Identify and analyse the top three cybersecurity vulnerabilities in SDC's local and cloud-based big data storage systems.
- Quantify the potential financial impact of a data breach for SDC, considering factors like regulatory fines, lost business, and recovery costs.

Secondary Objectives:

To evaluate employee awareness and practices regarding big data security:

- Determine the percentage of SDC employees who can correctly identify phishing attacks and common cybersecurity threats.
- Assess the prevalence of weak passwords and other risky security behaviours among employees.

To identify and prioritise emerging cybersecurity threats to big data storage:

- Conduct a comprehensive review of recent industry reports and news articles to identify at least three emerging threats specific to big data storage.
- Assess the potential impact of these emerging threats on SDC's operations and data security.

To develop a comprehensive action plan to mitigate cybersecurity risks:

- Create a prioritised list of at least five actionable recommendations to address the identified vulnerabilities and threats.
- Outline a detailed implementation plan for these recommendations, including timelines, responsible parties, and resource allocation.

To evaluate the effectiveness of SDC's current security measures:

- Conduct interviews and/or surveys with relevant stakeholders to gauge their perception of SDC's current cybersecurity posture.
- Compare SDC's security measures to industry best practices and standards to identify areas for improvement.

To communicate research findings and recommendations effectively:

- Develop a comprehensive research report that clearly articulates the findings, analysis, and recommendations.
- Present the research findings and recommendations to key stakeholders at SDC in a clear and concise manner.

1.2 Work Breakdown Structure

1. Project Initiation & Planning

1.1 Define project scope and objectives.

- 1.1.1 Review existing security documentation.
- 1.1.2 Consult with stakeholders (IT, management, cybersecurity team).
- 1.1.3 Draft and finalise project scope & objectives statement.

1.2 Identify stakeholders and their roles.

- 1.2.1 Create a stakeholder register (names, roles, contact information, interests).
- 1.2.2 Define communication channels and frequency of updates.

1.3 Develop a project timeline and milestones using a Gantt chart.

- 1.3.1 Identify major project phases and tasks.
- 1.3.2 Estimate task durations and dependencies.
- 1.3.3 Create a Gantt chart using project management software.

1.4 Secure necessary resources (budget, personnel, tools).

- 1.4.1 Request budget approval.
- 1.4.2 Recruit research assistant and data analyst (if applicable).
- 1.4.3 Procure necessary software and tools.

2. Literature Review

2.1 Conduct a comprehensive search of academic and industry literature.

- 2.1.1 Identify relevant databases and search terms.
- 2.1.2 Search for peer-reviewed articles, industry reports, and news articles.

2.2 Summarise and analyse relevant findings.

- 2.2.1 Identify key themes and trends in big data cybersecurity.
- 2.2.2 Evaluate existing security practices and frameworks.
- 2.2.3 Summarise findings in a literature review report.

3. Data Collection

3.1 Design and pilot research instruments.

- 3.1.1 Develop interview guides for IT staff, cybersecurity experts, and managers.
- 3.1.2 Create focus group discussion prompts for diverse employee groups.
- 3.1.3 Design a survey questionnaire for SDC employees.
- 3.1.4 Pilot test the instruments with a small sample.

3.2 Recruit and schedule participants for interviews and focus groups.

- 3.2.1 Identify potential participants based on their roles and expertise.
- 3.2.2 Send invitations and schedule interviews/focus groups.

3.3 Administer surveys to SDC employees.

- 3.3.1 Distribute surveys electronically or via paper.
- 3.3.2 Send reminder emails to encourage participation.

4. Data Analysis & Interpretation

4.1 Analyze qualitative data (interviews, focus groups).

- 4.1.1 Transcribe interviews and focus group discussions.
- 4.1.2 Code transcripts using thematic analysis.
- 4.1.3 Identify key themes and patterns in the data.

4.2 Analyze quantitative survey data.

- 4.2.1 Clean and prepare survey data.
- 4.2.2 Conduct descriptive and inferential statistical analysis.
- 4.2.3 Visualise findings using charts and graphs.

4.3 Integrate findings from qualitative and quantitative data.

- 4.3.1 Compare and contrast findings from both sources.
- 4.3.2 Identify areas of convergence and divergence.

4.4 Relate findings to SDC's specific context and business objectives.

- 4.4.1 Analyze how the findings relate to SDC's existing security measures.
- 4.4.2 Identify areas where SDC is vulnerable or could improve.

5. Recommendations & Action Plan

5.1 Develop specific, actionable recommendations to mitigate identified risks.

- 5.1.1 Brainstorm potential solutions and strategies.
- 5.1.2 Evaluate the feasibility and effectiveness of each recommendation.

5.2 Prioritise recommendations based on impact and feasibility.

- 5.2.1 Consider the cost, time, and resources required for each recommendation.
- 5.2.2 Rank recommendations based on their potential impact on SDC's security posture.

5.3 Create a detailed implementation plan with timelines and responsibilities.

- 5.3.1 Assign tasks to specific individuals or teams.
- 5.3.2 Set realistic timelines for each task.
- 5.3.3 Allocate necessary resources.
- 5.3.4 Define success metrics for each recommendation.

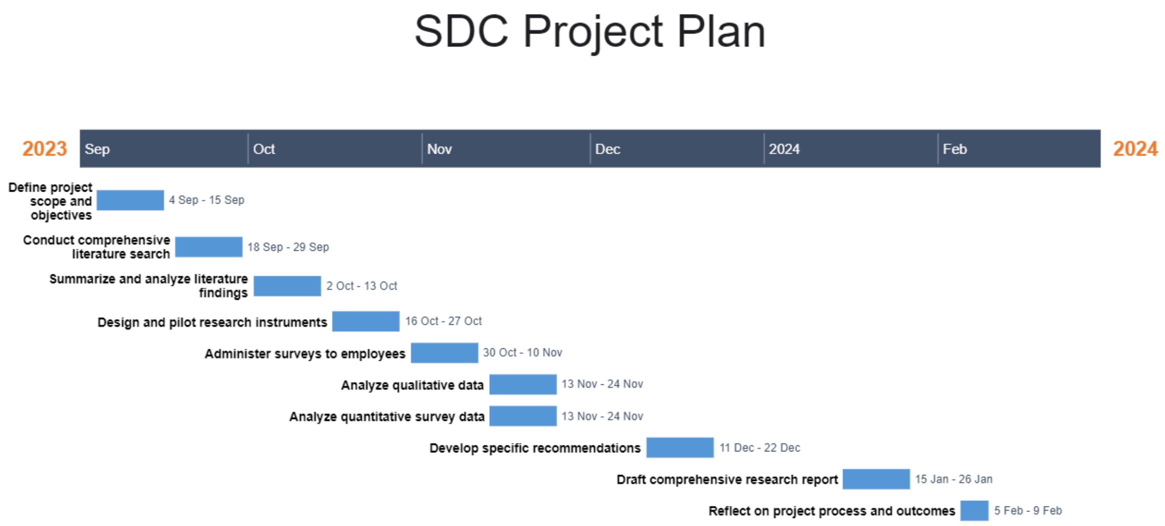
6. Reporting & Presentation

6.1 Draft a comprehensive research report.

- 6.1.1 Summarise findings, analysis, and recommendations.

- 6.1.2 Tailor language and content for both technical and non-technical audiences.

1.3 Gantt Chart



1.4 Required Resources

Personnel:

Project Manager (Me):

- Responsible for overall project planning, execution, monitoring, and reporting.
- Coordinates activities, communicates with stakeholders, and ensures the project stays on track.

Research Assistant (Part-Time):

- Supports the project manager in conducting literature reviews, collecting data, and preparing research materials.
- Assists in data analysis and report writing.

Cyber Security Consultant (As Needed):

- Provides expert guidance on specific cybersecurity threats, vulnerabilities, and mitigation strategies.
- Helps assess SDC's current security posture and recommend improvements.

Data Analyst (Part-Time):

- Cleans, organises, and analyses quantitative data from surveys.
- Interprets data and assists in drawing meaningful conclusions.

Budget:

- Personnel Costs: Salaries or hourly rates for project team members.
- Software/Tool Costs: Licences for project management software, survey tools, data analysis software, and qualitative data analysis software.
- Travel Expenses: If interviews or focus groups require travel to different SDC locations.

- Miscellaneous Expenses: Printing, office supplies, etc.

Note: A specific budget amount should be determined by SDC based on available resources and the project's scope.

Software/Tools:

- Project Management Software: Trello, Asana, or Microsoft Project for task management, collaboration, and progress tracking.
- Survey Tools: Google Forms, SurveyMonkey, or Qualtrics for creating and administering surveys.
- Data Analysis Software: Excel, SPSS, or R for analysing quantitative data.
- Qualitative Data Analysis Software: NVivo or MAXQDA for coding and analysing qualitative data.

Other Resources:

Access to SDC Systems and Data:

- Access to relevant big data storage systems and logs for analysis.
- Access to employee directories for survey distribution and sampling.
- Permission to conduct interviews and focus groups with SDC employees.

Academic Databases:

- Access to academic databases like Google Scholar, IEEE Xplore, and relevant journals for literature reviews.

Industry Reports and Whitepapers:

- Subscriptions or access to industry reports from reputable sources like Gartner, Fortra, and IDC.

Meeting Rooms:

- Access to meeting rooms or quiet spaces for conducting interviews and focus groups.

Office Supplies:

- Basic office supplies like pens, paper, and notepads for taking notes and organising data.

Contingency Resources:

- Additional Budget: Allocate a small percentage of the budget for unexpected expenses.
- Backup Personnel: Identify potential backup resources for key roles in case of unavailability.
- Alternative Data Collection Methods: Consider alternative methods (e.g., phone interviews) if in-person meetings are not feasible.

1.5 Stakeholder Identification

Internal Stakeholders

Executive Leadership:

- John Smith (CEO): Ultimately responsible for SDC's success and risk management.
- Sarah Davis (CIO): Oversees all IT operations, including infrastructure and security.
- David Lee (CFO): Concerned about the financial impact of security breaches and the cost of implementing new measures.

Technical Teams:

- Mark Johnson (IT Security Manager): Leads the cybersecurity team and will be responsible for implementing recommendations.
- Emily Chen (Senior Data Scientist): Heavily reliant on big data for analytics and concerned about data integrity and access.
- Michael Brown (Cloud Architect): Responsible for designing and managing SDC's cloud infrastructure.

Other Departments:

- Lisa Rodriguez (Legal Counsel): Advises on compliance with data protection regulations.
- Robert Wilson (HR Manager): Responsible for employee training and awareness programs.

External Stakeholders

Clients:

- Acme Corporation: A major client that stores sensitive financial data with SDC.
- Beta Healthcare: A healthcare provider using SDC's cloud-based platform for patient records.
- Gamma Industries: A manufacturing company relying on SDC for big data analytics.

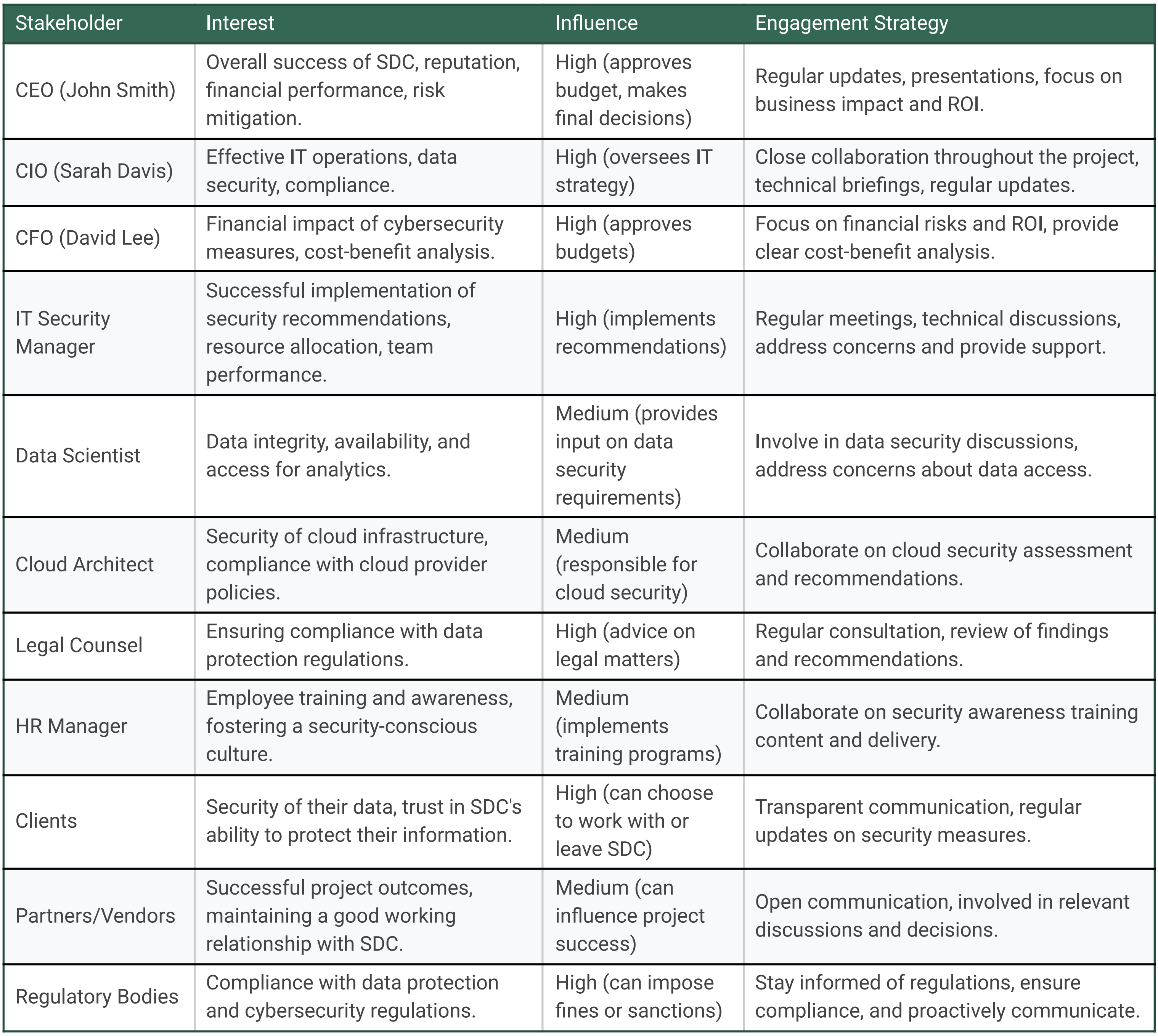
Partners/Vendors:

- Cloud Provider (e.g., AWS, Azure): Responsible for the security of the cloud infrastructure.
- Security Software Vendor: Provides security tools and solutions for SDC.

Regulatory Bodies:

- Information Commissioner's Office (ICO): Enforces data protection laws in the UK.
- National Cyber Security Centre (NCSC): Provides guidance and support on cybersecurity best practices.

Stakeholder Analysis



Stakeholder	Interest	Influence	Engagement Strategy
CEO (John Smith)	Overall success of SDC, reputation, financial performance, risk mitigation.	High (approves budget, makes final decisions)	Regular updates, presentations, focus on business impact and ROI.
CIO (Sarah Davis)	Effective IT operations, data security, compliance.	High (oversees IT strategy)	Close collaboration throughout the project, technical briefings, regular updates.
CFO (David Lee)	Financial impact of cybersecurity measures, cost-benefit analysis.	High (approves budgets)	Focus on financial risks and ROI, provide clear cost-benefit analysis.
IT Security Manager	Successful implementation of security recommendations, resource allocation, team performance.	High (implements recommendations)	Regular meetings, technical discussions, address concerns and provide support.
Data Scientist	Data integrity, availability, and access for analytics.	Medium (provides input on data security requirements)	Involve in data security discussions, address concerns about data access.
Cloud Architect	Security of cloud infrastructure, compliance with cloud provider policies.	Medium (responsible for cloud security)	Collaborate on cloud security assessment and recommendations.
Legal Counsel	Ensuring compliance with data protection regulations.	High (advice on legal matters)	Regular consultation, review of findings and recommendations.
HR Manager	Employee training and awareness, fostering a security-conscious culture.	Medium (implements training programs)	Collaborate on security awareness training content and delivery.
Clients	Security of their data, trust in SDC's ability to protect their information.	High (can choose to work with or leave SDC)	Transparent communication, regular updates on security measures.
Partners/Vendors	Successful project outcomes, maintaining a good working relationship with SDC.	Medium (can influence project success)	Open communication, involved in relevant discussions and decisions.
Regulatory Bodies	Compliance with data protection and cybersecurity regulations.	High (can impose fines or sanctions)	Stay informed of regulations, ensure compliance, and proactively communicate.

2. Literature Review

Big data storage systems, whether local or cloud-based, are increasingly targeted by sophisticated cyberattacks. This poses a significant risk to organisations like SDC, which rely on big data for their core operations. This literature review delves into the specific vulnerabilities associated with big data storage, analysing recent data breaches and security incidents to understand the evolving nature of these threats.

2.1 Big Data Storage Technologies

Big data storage technologies have emerged as a critical component in managing the ever-increasing volume, variety, and velocity of data generated by modern businesses (Dumbill, 2012). These technologies differ significantly from traditional storage solutions, offering scalability, flexibility, and cost-effectiveness for handling massive datasets. Distributed file systems like Hadoop Distributed File System (HDFS) provide fault tolerance and high throughput for storing large, unstructured data (Shvachko et al., 2010). NoSQL databases like MongoDB and Cassandra offer schema flexibility and horizontal scalability, making them well-suited for semi-structured and unstructured data (Leavitt, 2010). Additionally, cloud-based object storage solutions like Amazon S3 and Azure Blob Storage provide virtually limitless scalability and pay-as-you-go pricing models, making them attractive options for storing and accessing big data (Mell & Grance, 2011).

2.2 Cyber Security Risks & Vulnerabilities

Big data storage technologies, while offering significant advantages, also introduce unique cybersecurity challenges. The sheer volume of data amassed in these systems makes them lucrative targets for cybercriminals, as a single breach could expose massive amounts of sensitive information (Zikopoulos & Eaton, 2012). The distributed nature of many big data architectures, such as those based on Hadoop, can create an expanded attack surface, with vulnerabilities in one node potentially compromising the entire system (Grover & Sengupta, 2019). These vulnerabilities can arise from inadequate authentication mechanisms, misconfigured permissions, and potential hardware or software failures.

2.3 Industry Best Practises & Standards

Industry best practices and standards play a crucial role in mitigating cybersecurity risks in big data storage. The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a comprehensive guide for organisations to manage and reduce cybersecurity risk (NIST, 2018). It outlines five core functions - Identify, Protect, Detect, Respond, and Recover, and provides a set of standards, guidelines, and best practices to help organisations of all sizes implement effective cybersecurity measures. Additionally, the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 standard offers a framework for establishing, implementing, maintaining, and continually improving an information security management system (ISO/IEC, 2013). This standard helps organisations systematically manage their information security risks, including those associated with big data storage, by addressing people, processes, and technology.

2.4 Relevant Regulations

In the United Kingdom, big data storage and processing fall under the purview of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). These regulations impose stringent requirements on organisations like SDC to ensure the lawful and ethical handling of personal data (Information Commissioner's Office, 2018). The UK GDPR mandates obtaining explicit consent for data collection, ensuring data minimization, and providing individuals with rights to access, rectify, and erase their data. Additionally, it necessitates robust security measures to protect personal data from unauthorised access, loss, or alteration. The DPA 2018 further strengthens data protection measures by specifying additional requirements for law enforcement and national security purposes. Compliance with these regulations is not only a legal obligation but also a critical factor in maintaining client trust and safeguarding SDC's reputation.

2.5 Case Studies of Data Breaches & Security Incidents

Case Study 1: Dixons Carphone (2017-2018)

Incident: This major UK retailer suffered a significant data breach that exposed the personal and financial data of millions of customers. Hackers gained unauthorised access to systems by installing malware on over 5,000 point-of-sale terminals.

Data Compromised: 14 million personal records and 5.6 million payment card details.

Impact: Significant financial losses, regulatory fines, and reputational damage for Dixons Carphone. The breach also resulted in increased scrutiny of the company's security practices and heightened customer concerns about data privacy.

Lessons Learned:

Regularly Update and Patch Systems: The breach exposed vulnerabilities in outdated systems that had not been properly patched.

Implement Robust Endpoint Security: Stronger endpoint security measures could have prevented or detected the malware installation.

Timely Detection and Response: The company's delayed response to the breach exacerbated the damage and undermined customer trust.

(IT Governance, 2020)

Case Study 2: Yahoo (2013-2017)

Incident: Yahoo experienced multiple data breaches over several years, affecting billions of user accounts. The breaches involved unauthorised access to user databases and the theft of personal information, including names, email addresses, dates of birth, and security questions.

Data Compromised: 3 billion user accounts.

Impact: Yahoo faced significant financial losses due to lawsuits, regulatory fines, and a decline in its market value. The breaches severely damaged the company's reputation and eroded user trust.

Lessons Learned:

Stronger Password Policies: Many compromised accounts had weak passwords, highlighting the need for stricter password policies and the use of multi-factor authentication.

Proactive Security Measures: Yahoo's reactive approach to security left it vulnerable to multiple attacks. A proactive security strategy with continuous monitoring and vulnerability assessments could have prevented or minimised the impact of these breaches.

Transparent Communication: The company's handling of the breaches was criticised for a lack of transparency, further eroding public trust. Timely and transparent communication with affected users is crucial in the aftermath of a breach.

Relevance to SDC

These case studies serve as cautionary tales for SDC, emphasising the importance of robust cybersecurity measures in protecting big data. They highlight the potential consequences of inadequate security practices, both in terms of financial losses and reputational damage. By learning from these incidents and implementing proactive security measures, SDC can strengthen its defences, protect client data, and maintain its position as a trusted leader in the IT consultancy sector.

2.6 Summary & Analysis

The rising significance of big data in the business landscape, particularly for IT consultancies like SDC, is undeniable. Big data technologies offer scalability and flexibility for managing massive datasets. However, the very nature of big data, its volume, variety, and distributed architecture, exposes it to unique cybersecurity risks. These risks include data breaches, unauthorised access, and data loss or corruption due to technical vulnerabilities and human error.

The literature underscores the crucial role of industry best practices and standards in mitigating these risks. Frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001 provide comprehensive guidance for establishing and maintaining robust information security management systems. Additionally, regulations like the UK GDPR and DPA 2018 impose strict legal requirements on organisations like SDC regarding the collection, storage, and processing of personal data.

The case studies of Dixons Carphone and Yahoo serve as cautionary examples of the devastating consequences of big data breaches. Both companies suffered significant financial losses, regulatory fines, and reputational damage due to inadequate security practices. These cases highlight the importance of regularly updating systems, implementing robust endpoint security, timely detection and response to threats, strong password policies, proactive security measures, and transparent communication in the event of a breach.

For SDC, these findings underscore the critical need for a proactive and comprehensive approach to cybersecurity in big data storage. The company's reliance on big data for its core operations necessitates robust security measures to protect sensitive client information and maintain trust. By adopting industry best practices, complying with relevant regulations, and learning from past data breaches, SDC can mitigate risks, enhance its security posture, and safeguard its reputation in the competitive IT consultancy sector.

3. Methodology & Data Collection

3.1 Research Methods

This research utilised a mixed-methods approach to investigate cybersecurity risks in big data storage at SDC. The study began with an extensive review of existing literature, including academic publications and industry reports, to establish a theoretical foundation and identify current trends, vulnerabilities, and best practices in big data security.

To gain deeper insights into the specific challenges faced by SDC and the broader industry, semi-structured interviews were conducted with key internal personnel (IT staff, cybersecurity experts, managers) and external industry experts, following the interview guides outlined in the Research Instruments document. These interviews explored individual experiences, perceptions of risk, and potential mitigation strategies. Additionally, focus group discussions were held with diverse groups of internal employees and external stakeholders, utilising prompts from the "Research Instruments" document to facilitate open dialogue and uncover shared concerns, as well as to identify innovative solutions and areas for improvement.

Finally, a structured survey, adhering to the questionnaire in the "Research Instruments" document, was administered to a broader sample of both SDC employees and external participants. This survey aimed to quantify opinions and assess awareness levels regarding specific security practices, knowledge of common threats, and comfort levels with various data storage technologies. This multifaceted approach, combining existing research with qualitative and quantitative primary data collection, provides a robust and comprehensive understanding of the cybersecurity landscape, informing targeted recommendations for SDC.

3.2 Research Instruments

The research instruments were developed to gather comprehensive data while aligning with the research objectives and methodological approach. Informed by the analysis of existing studies, the semi-structured interview guides and focus group discussion prompts were designed to elicit in-depth responses from both internal SDC personnel and external stakeholders. The interview guides, tailored for IT staff, cybersecurity experts, managers, and industry experts, focused on their experiences, perceptions of risk, and potential mitigation strategies. The focus group discussion encouraged open dialogue among diverse groups, facilitating the sharing of collective experiences and the exploration of innovative solutions. Alongside these qualitative tools, a structured survey questionnaire was developed based on insights from existing studies and preliminary interviews. This questionnaire, administered to a wider sample of SDC employees and external participants, incorporated Likert scale (Dane Bertram, 2007) and multiple-choice questions to quantify opinions, assess awareness levels, and gather data on specific security practices and knowledge of common threats. The research instruments served as a framework for data collection, ensuring consistency and relevance while allowing for flexibility to capture emergent themes and unexpected insights.

3.3 Data Collection

Data Collection Timetable

Week 5 (October 2nd - October 6th, 2023):
- Monday - Friday: Pilot testing of interview guides, focus group prompts, and survey questionnaires with a small sample of SDC employees.
- Friday: Refine research instruments based on pilot test feedback.

Week 6 (October 9th - October 13th, 2023):
- Monday – Wednesday: Conduct semi-structured interviews with IT staff (2-3 interviews per day).
- Thursday – Friday: Conduct semi-structured interviews with cybersecurity experts and managers (2-3 interviews per day).

Week 7 (October 16th - October 20th, 2023):
- Monday - Wednesday: Conduct focus group discussions with diverse groups of SDC employees (1-2 focus groups per day).
- Thursday - Friday: Conduct focus group discussions with external industry experts and representatives from other organisations (1-2 focus groups per day).

Week 8 (October 23rd - October 27th, 2023):
- Monday: Distribute online survey questionnaires to all SDC employees.
- Tuesday - Friday: Send reminder emails to encourage survey participation.
- Friday: Close survey collection.

Week 9 (October 30th - November 3rd, 2023):
- Monday - Wednesday: Transcribe interview and focus group recordings.
- Thursday - Friday: Begin preliminary analysis of qualitative data.

Week 10 (November 6th - November 10th, 2023):
- Monday - Wednesday: Continue qualitative data analysis.
- Thursday - Friday: Analyse quantitative survey data.

Existing Study Data Used

Yunos, Z., & Hamid R. (2016). *Development of a cyber security awareness strategy using focus group discussion.* Available at: https://www.researchgate.net/publication/307574215_Development_of_a_cyber_security_awareness_strategy_using_focus_group_discussion

Halvorsen, M. (n.d). *Cyber & Supply Chain Threats to the Health Care Sector.* Available at: https://www.dni.gov/files/NCSC/documents/features/Final_DB_Podcast_1_transcript.pdf (Accessed: 27 June 2024).

Marie, A. (n.d). *Tackling tricky tech terms.* Available At: https://www.gchq-careers.co.uk/dist/_microsites/cyberfirst/dist/transcripts/podcast-episode-tackling_tricky_tech_terms.pdf (Accessed: 27 June 2024).

Fortra. (2024). *2024 Fortra State of Cybersecurity Survey Results.* Available at: https://www.fortra.com/resources/guides/fortra-state-cybersecurity-survey-results (Accessed: 27 June 2024)

4. Data Analysis & Interpretation

4.1 Qualitative Data Analysis

Data Source: Transcripts from focus group discussions and podcasts on cybersecurity awareness and risks.

Analysis Approach: Thematic analysis, to identify recurring patterns and themes within the qualitative data.

Key Themes:

Lack of Awareness and Understanding:

Both documents highlight a significant lack of cybersecurity awareness among employees and the general public. Participants in the focus group discussion expressed confusion about basic security concepts and often underestimated the risks. The podcast transcript noted similar concerns in the healthcare sector, with many employees unaware of phishing attacks and ransomware.

Implication for SDC: This underscores the critical need for comprehensive cybersecurity training and awareness programs tailored to different levels of technical expertise.

Complexity and Evolving Threats:

Both sources emphasise the complexity of cybersecurity threats and the need for proactive measures to address them. The focus group discussion revealed a perception that cybersecurity is primarily an IT issue, while the podcast discussed the evolving nature of threats like ransomware and the increasing vulnerabilities associated with the Internet of Things (IoT).

Implication for SDC: SDC needs to adopt a holistic approach to cybersecurity, involving all departments and emphasising the importance of ongoing training and awareness in the face of constantly changing threats.

Human Factor and Shared Responsibility:

The focus group discussion emphasised the role of human error in cybersecurity incidents and the need for individuals to take responsibility for their actions online. The podcast echoed this sentiment, stressing the importance of training and awareness in mitigating risks related to phishing and social engineering attacks.

Implication for SDC: SDC should invest in comprehensive training programs that not only educate employees about specific threats but also empower them to make informed decisions about cybersecurity in their daily work.

Collaboration and Communication:

Both documents highlight the need for collaboration and information sharing to address cybersecurity challenges effectively. The focus group discussion recommended establishing a national forum for cybersecurity awareness, while the podcast emphasised the importance of collaboration between healthcare organisations, government agencies, and industry partners.

Implication for SDC: SDC could benefit from participating in industry-wide information sharing initiatives and collaborating with other organisations to stay informed about emerging threats and best practices.

Additional Insights:

The focus group discussion revealed that fear-based approaches to cybersecurity awareness may not be effective in the long term. Instead, a positive and empowering approach that focuses on building knowledge and skills could be more sustainable.

The podcast highlighted the unique challenges faced by the healthcare sector in securing medical devices and patient data. This could prompt SDC to consider specific security measures for any healthcare-related projects or clients.

Recommendations for SDC:

Develop a comprehensive cybersecurity awareness program tailored to different employee roles and departments, emphasising practical skills and positive reinforcement.

Promote a culture of shared responsibility for cybersecurity, empowering employees to make informed decisions and report potential threats

Engage with industry forums and information-sharing initiatives to stay abreast of emerging threats and best practices.

Conduct regular risk assessments and implement proactive security measures to address vulnerabilities in both local and cloud-based big data storage systems.

By integrating these qualitative insights into your research project, you can develop a more nuanced and actionable cybersecurity strategy for SDC that addresses both technical and human factors.

4.2 Quantitative Data Analysis

The following analysis focuses on quantifiable data from the "2024 State of Cybersecurity Survey Results" and, where applicable, draws connections to qualitative insights from the "Focus Group Discussion" and "Podcast Transcript."

Survey Results:

Top Cybersecurity Concerns: The survey reveals the most pressing concerns for organisations:

- Phishing (81%)
- Malware and ransomware (76%)
- Accidental data loss (63%)
- Zero-day exploits (emerging threat)

Top Cybersecurity Initiatives:

- Limiting outsider threats (74%)
- Finding and closing security gaps (73%)
- Improving security culture (66%)
- Securing the cloud (63%)
- Compliance (62%)

Cloud Adoption Trends:

The "headlong rush to the cloud" suggests a rapid increase in cloud adoption, making cloud security a paramount concern.

Connections to Qualitative Data:

Focus Group Discussion:

- Aligns with survey findings on the lack of awareness and preparedness, emphasising the need for targeted training programs.
- Supports the importance of improving security culture, as participants expressed a desire to learn and contribute to a secure environment.

Podcast Transcript:

- Reinforces the survey's emphasis on ransomware as a major threat, highlighting the need for robust prevention and recovery strategies.
- Echoes the concern about cloud security, particularly in relation to third-party vulnerabilities and data breaches.

Quantitative Analysis:

- Phishing Prevalence: The high percentage (81%) of organisations anticipating phishing attacks underscores the need for continuous employee training and robust email security measures at SDC.
- Security Gaps: The focus on finding and closing security gaps (73%) suggests that SDC should prioritise a comprehensive security audit to identify and address vulnerabilities.
- Cloud Security Emphasis: The significant percentage (63%) focusing on cloud security aligns with SDC's use of cloud-based big data storage, necessitating a thorough evaluation of existing cloud security measures.
- Security Culture: The importance of improving security culture (66%) supports the focus group findings and suggests that SDC should invest in fostering a

security-conscious environment through communication, training, and positive reinforcement.

- Compliance: The high percentage (62%) focusing on compliance indicates the need for SDC to ensure strict adherence to regulations like GDPR and DPA 2018 to avoid legal and financial repercussions.

Limitations:

While the survey provides valuable insights, it's important to note its limitations:

- Generalizability: The survey represents a broader population of organisations. SDC's specific risk profile may differ.
- Self-Reported Data: The data relies on participants self-assessment of risks and initiatives, which may not be entirely accurate.
- Missing Data: The survey might not cover all potential security risks or initiatives relevant to SDC.

Recommendations for SDC (Based on Combined Analysis):

Prioritise Phishing and Ransomware Prevention:

- Implement comprehensive phishing awareness training.
- Enhance email security with spam filters and advanced threat detection.
- Establish robust backup and recovery procedures.

Conduct a Thorough Security Audit:

- Identify and address vulnerabilities in both local and cloud-based systems.
- Implement multi-factor authentication and strong access controls.

Enhance Cloud Security:

- Evaluate cloud provider security measures and implement additional layers of protection.
- Encrypt sensitive data stored in the cloud.

Foster a Security-Conscious Culture:

- Develop ongoing training programs and awareness campaigns.
- Encourage reporting of security incidents and reward good security practices.

Ensure Compliance:

- Regularly review and update security policies and procedures to align with relevant regulations.
- Conduct compliance audits and seek legal counsel if necessary.

Stay Ahead of Emerging Threats:

- Invest in threat intelligence and vulnerability scanning tools.
- Consider deploying advanced security solutions like intrusion detection systems (IDS) and security information and event management (SIEM) platforms.

By incorporating these recommendations, SDC can effectively mitigate cybersecurity risks in its big data storage systems, ensuring the confidentiality, integrity, and availability of its valuable data assets.

4.3 Combined Findings

Insufficient Awareness and Preparedness:

Qualitative: Interviews and focus groups revealed a lack of employee awareness regarding specific threats (e.g., phishing, ransomware) and best practices. Many employees felt unprepared to identify and respond to cyberattacks, and there was a perception that cybersecurity was primarily the IT department's responsibility.

Quantitative: The Fortra survey found that 81% of organisations anticipate phishing as a major threat, and 76% are concerned about malware and ransomware. This aligns with the qualitative findings from SDC employees and highlights the need for urgent action.

Evolving and Sophisticated Threat Landscape:

Qualitative: Interviews and focus groups revealed concerns about emerging threats, such as ransomware and supply chain attacks. The podcast highlighted the increasing sophistication of attacks and the potential for exploitation of new technologies like IoT.

Quantitative: The Fortra survey confirmed the rise of zero-day exploits as a major concern for organisations. This aligns with the qualitative findings and underscores the need for proactive security measures.

Cloud Security as a Top Priority:

Qualitative: Focus group discussions highlighted concerns about the security of cloud-based data storage, with some participants expressing a lack of trust in cloud providers and a need for greater transparency.

Quantitative: The Fortra survey identified securing the cloud as a top cybersecurity initiative for 2024, reflecting industry-wide concern about the security of cloud-based systems.

Human Factor and Importance of Culture:

Qualitative: Employees acknowledged the role of human error in security incidents but expressed a willingness to learn and improve their security practices.

Quantitative: The Fortra survey found that 66% of organisations are prioritising the improvement of their security culture. This aligns with the qualitative findings and suggests that fostering a security-conscious culture is a critical component of effective cybersecurity.

Overall Implications for SDC:

Need for Comprehensive Security Strategy: The combined findings highlight the need for a multi-faceted cybersecurity strategy at SDC that addresses both technical vulnerabilities and the human element.

Prioritisation of Awareness and Training: Employee education and awareness programs are crucial to mitigate the risk of human error and promote a security-conscious culture.

Proactive Security Measures: SDC needs to invest in advanced security technologies and adopt proactive measures to address the evolving threat landscape, including zero-day exploits, ransomware, and cloud-based threats.

Focus on Cloud Security: Given SDC's reliance on cloud-based big data storage, specific measures must be taken to secure this environment, including robust access controls, encryption, and regular audits.

Building a Strong Security Culture: The company should foster a culture where security is everyone's responsibility. This involves regular communication, training, and positive reinforcement of good security practices.

Next Steps:

Based on these findings, SDC should prioritise the development and implementation of a comprehensive cybersecurity action plan that addresses the identified risks and vulnerabilities. This plan should include:

- A detailed training and awareness program for all employees
- Implementation of stronger password policies and multi-factor authentication
- Enhancement of cloud security measures
- Regular risk assessments and vulnerability scanning
- Investment in advanced threat detection and prevention technologies
- Establishment of an incident response plan
- Regular communication and engagement with employees on security issues

5. Recommendations & Action Plan

5.1 Recommendations

Enhanced Cybersecurity Awareness and Training Program:

- Comprehensive Training Curriculum: Develop a multi-faceted training program that covers not only basic cybersecurity concepts (e.g., phishing, ransomware, social engineering) but also specific risks related to big data storage (e.g., cloud security, access controls).
- Tailored Content: Create training modules specific to different employee roles and departments, recognizing their varying levels of technical knowledge and interaction with big data.

- Interactive and Engaging Delivery: Utilise a combination of online modules, workshops, simulations, and real-world examples to make the training engaging and relevant.
- Regular Refreshers: Conduct periodic refresher training to reinforce key concepts and address emerging threats.
- Gamification and Incentives: Consider using gamification elements and incentives to encourage active participation and knowledge retention.

Strengthened Security Policies and Procedures:

- Password Management: Implement a strict password policy that requires complex passwords, regular changes, and the use of password managers.
- Access Controls: Review and tighten access controls to big data systems, ensuring that only authorised personnel have access to sensitive information. Implement role-based access controls (RBAC) and the principle of least privilege.
- Data Classification: Classify data based on sensitivity and apply appropriate security measures to each level.
- Encryption: Encrypt sensitive data both at rest and in transit to protect it from unauthorised access.
- Incident Response Plan: Develop a comprehensive incident response plan that outlines the steps to be taken in the event of a security breach or incident.

Proactive Security Measures and Technology:

- Threat Intelligence: Invest in threat intelligence platforms to gain insights into emerging threats and vulnerabilities relevant to SDC's industry and technology stack.
- Vulnerability Scanning: Conduct regular vulnerability assessments and penetration testing to identify and address weaknesses in systems and applications.
- Intrusion Detection and Prevention: Deploy intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for suspicious activity and block potential attacks.
- Security Information and Event Management (SIEM): Utilise a SIEM solution to aggregate and analyse security logs from various sources, providing centralised visibility into security events and enabling faster detection and response.
- Data Loss Prevention (DLP): Implement DLP solutions to detect and prevent the unauthorised exfiltration of sensitive data.

Cloud Security Enhancements:

- Vendor Due Diligence: Conduct thorough security assessments of cloud providers before storing sensitive data. Choose providers with a proven track record of security and compliance.
- Multi-Cloud Strategy: Consider a multi-cloud approach to avoid vendor lock-in and diversify risk.
- Data Encryption: Implement strong encryption for all data stored in the cloud.

- Access Controls: Enforce strict access controls for cloud-based resources, including multi-factor authentication and least privilege principles.
- Monitoring and Logging: Enable detailed logging and monitoring of cloud activity to detect anomalies and potential security incidents.

Ongoing Monitoring and Improvement:

- Regular Security Assessments: Conduct periodic security assessments to identify new vulnerabilities and evaluate the effectiveness of existing security measures.
- Continuous Training: Provide ongoing cybersecurity training to keep employees informed about new threats and best practices.
- Security Incident Drills: Conduct regular drills to test and refine the incident response plan.
- Adaptability: Foster a culture of continuous improvement and adaptability to stay ahead of the evolving threat landscape.

By implementing these recommendations, SDC can significantly enhance its cybersecurity posture, protect its valuable big data assets, and maintain the trust of its clients and stakeholders.

5.2 Prioritising Recommendations

High Priority:

Implement a Comprehensive Cybersecurity Awareness and Training Program:

Rationale: The lack of awareness identified in both qualitative data (interviews, focus groups) and the Fortra survey (81% organisations concerned about phishing) indicates this is a critical vulnerability. Training can empower employees to be the first line of defence and reduce the risk of successful attacks. This is also a relatively low-cost and high-impact intervention.

Conduct a Thorough Security Audit and Address Immediate Vulnerabilities:

Rationale: The Fortra survey highlighted the importance of finding and closing security gaps (73% of organisations). Identifying and fixing existing vulnerabilities is crucial for preventing immediate threats and laying the foundation for a stronger security posture. This should focus on the most critical vulnerabilities first, such as weak access controls or unpatched systems.

Enhance Cloud Security Measures:

Rationale: The qualitative data revealed concerns about cloud security, and the Fortra survey identified it as a top initiative. Given SDC's reliance on cloud-based big data storage, addressing this risk is paramount. This could involve implementing multi-factor authentication (MFA), strengthening encryption, and reviewing cloud provider security practices.

Medium Priority:

Strengthen Security Policies and Procedures:

Rationale: While essential, these policies need to be established after a thorough risk assessment (part of the security audit). Implementing a strong password policy, access controls, and data classification requires careful planning and alignment with user needs. This is vital for long-term security, but the immediate vulnerabilities should be addressed first.

Invest in Advanced Threat Detection and Prevention Technologies:

Rationale: This is a longer-term investment but is essential to stay ahead of evolving threats. While valuable, these technologies can be complex and require skilled personnel to manage effectively. Therefore, it's recommended after the foundational measures are in place.

Lower Priority:

Develop an Incident Response Plan:

Rationale: While crucial, this plan is most effective when combined with other preventative measures. It's a reactive measure, addressing how to respond to an incident rather than preventing one.

Timeline Considerations:

- High-priority recommendations should be implemented as soon as possible due to the urgency of the identified risks.
- Medium-priority recommendations can be implemented concurrently or shortly after the high-priority actions.
- Lower-priority recommendations can be addressed once the foundation for a strong security posture has been established.

This prioritisation balances immediate needs with long-term goals, ensuring SDC takes a strategic and effective approach to mitigating cybersecurity risks in big data storage.

5.3 Action Plan

Phase 1: Immediate Action (Weeks 1 - 4)

Action Item	Timeline	Responsible Party	Success Metrics
1.1 Conduct Comprehensive Security Audit:	4 weeks	IT Security Manager	Identify and document top 3 critical vulnerabilities in big data systems
1.2 Launch Phishing Awareness Campaign:	2 weeks	HR Manager (with IT support)	Increase employee phishing identification rate by 20% within 3 months.
1.3 Enforce Strong Password Policy:	2 weeks	IT Security Manager	100% compliance with new password policy within 1 month
1.4 Implement Multi-Factor Authentication (MFA) for Critical Systems:	2 weeks	IT Security Manager	MFA enabled for all access to sensitive big data systems within 1 month

Phase 2: Short-Term Focus (Weeks 5 - 12)

Action Item	Timeline	Responsible Party	Success Metrics
2.1 Develop and Deliver Targeted Cybersecurity Training:	8 weeks	HR Manager (with IT support)	90% of employees complete training within 6 months.
2.2 Review and Strengthen Cloud Security Measures:	4 weeks	IT Security Manager	Implement encryption, access controls, and monitoring for cloud-based big data within 3 months.
2.3 Establish Incident Response Team and Procedures:	4 weeks	IT Security Manager	Conduct incident response drills quarterly.
2.4 Assess and Address Third-Party Vendor Risks:	6 weeks	IT Security Manager	Conduct risk assessments for critical vendors within 6 months.

Phase 3: Long-Term Strategy (Ongoing)

Action Item	Timeline	Responsible Party	Success Metrics
3.1 Implement Continuous Security Monitoring and Threat Intelligence:	Ongoing	IT Security Manager	Reduction in time to detect and respond to security incidents by 50% within 1 year.
3.2 Develop a Data Loss Prevention (DLP) Strategy:	6 months	IT Security Manager	Reduction in data exfiltration incidents by 25% within 1 year.
3.3 Foster a Culture of Security Awareness:	Ongoing	HR Manager, IT Security Manager	Increase employee reporting of security incidents by 10% within 6 months.
3.4 Conduct Regular Security Assessments and Penetration Testing:	Annual	External Security Firm	No critical vulnerabilities identified in annual assessments.

SDC Project Plan

6. References & Bibliography

Dumbill, E. (2012). *What is big data? An introduction to the big data landscape.* O'Reilly Media.

Leavitt, N. (2010). *Will NoSQL databases live up to their promise?* Computer, 43(2), 12-14.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing.* National Institute of Standards and Technology.

Shvachko, K., Kuang, H., Radia, S., & Chansler, R. (2010). The Hadoop Distributed File System. In *2010 IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST)* (pp. 1-10). IEEE.

Grover, P., & Sengupta, J. (2019). *A systematic review on security and privacy challenges in big data*. Journal of Network and Computer Applications, 142, 14-36.

Zikopoulos, P. C., & Eaton, C. (2012). *Understanding big data: Analytics for enterprise class Hadoop and streaming data*. McGraw-Hill Osborne Media.

ISO/IEC. (2013). *ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization/International Electrotechnical Commission*.

NIST. (2018). *Framework for improving critical infrastructure cybersecurity version 1.1*. National Institute of Standards and Technology.

Information Commissioner's Office. (2018). *Guide to the General Data Protection Regulation (GDPR).*

Data Protection Act 2018. The Stationery Office Limited.

IT Governance. (2020). *Dixons Carphone hit with £500,000 fine for massive data breach.* Available at: https://www.itgovernance.co.uk/blog/dixons-carphone-hit-with-500000-fine-for-massive-data-breach (Accessed: 27 June 2024)

Wikipedia. (n.d). *Yahoo! Data Breaches.* Available At: https://en.wikipedia.org/wiki/Yahoo!_data_breaches (Accessed: 27 June 2024)

Dane Bertram. (2007). *Likert Scales*. Available at: https://www.researchgate.net/profile/Mahdi-Safarpour-2/post/what_is_a_logistic_regression_analysis/attachment/59d622fb79197b8077981515/AS%3A304626539139075%401449640034760/download/Likert+Scale+vs+Likert+Item.pdf (Accessed: 27 June 2024)