LUKE LITTLER 132290

HOPWOOD HALL COLLEGE

HTQ COMPUTING RQF

UNIT 6: PLANNING A COMPUTING PROJECT

SDC CYBER SECURITY RESEARCH REPORT

Executive Summary

Big data is a cornerstone of SDC's success, driving innovation and providing valuable insights for both the company and its clients. However, the storage and processing of vast amounts of data expose SDC to significant cybersecurity risks that, if left unaddressed, could severely impact the company's operations, reputation, and financial standing.

This comprehensive research project investigated the specific cybersecurity vulnerabilities faced by SDC in its local and cloud-based big data storage systems. A mixed-methods approach was employed, encompassing in-depth interviews with key personnel, focus group discussions with diverse employee groups, and a survey administered to a broader sample of SDC employees and external stakeholders. This multi-faceted approach allowed for a holistic assessment of the current security landscape, uncovering both technical vulnerabilities and gaps in employee awareness and practices.

Key findings reveal a concerning lack of cybersecurity awareness among employees, with many unaware of specific threats like phishing and ransomware, and a tendency to engage in risky behaviours such as using weak passwords. Additionally, concerns were raised about the security of cloud-based data storage, highlighting a need for enhanced transparency and stricter security measures. The research also identified emerging threats like ransomware and supply chain attacks as growing concerns for SDC.

These findings underscore the urgent need for a comprehensive cybersecurity strategy at SDC. The company's reliance on big data, coupled with evolving threats and vulnerabilities, necessitates proactive measures to protect its valuable data assets.

To address these challenges, this report proposes a multi-pronged approach, focusing on:

- Enhancing Employee Awareness and Training: Implementing a comprehensive, ongoing training program tailored to different roles, covering basic security concepts, big data-specific risks, and best practices.
- Strengthening Security Policies and Procedures: Enforcing strong password policies, implementing strict access controls, and regularly reviewing and updating security procedures.
- Enhancing Cloud Security Measures: Conducting thorough security assessments of cloud providers, implementing additional security layers like encryption and multi-factor authentication, and monitoring cloud activity for anomalies.

- Proactive Security Measures: Investing in threat intelligence, conducting regular vulnerability scans and penetration testing, and deploying advanced security solutions like intrusion detection and prevention systems (IDS/IPS).
- Incident Response Planning: Developing a comprehensive plan outlining the steps to be taken in the event of a security breach or incident, establishing an incident response team, and conducting regular drills to test and refine the plan.

- Fostering a Security Culture: Promoting a security-conscious culture through regular communication, employee engagement, and recognition of good security practices.

The accompanying action plan outlines a detailed timeline, responsibilities, and resource allocation for implementing these recommendations. By prioritising immediate actions, focusing on short-term goals, and establishing a long-term strategy, SDC can significantly enhance its cybersecurity posture, protect its valuable data assets, and maintain its reputation as a trusted leader in the IT consultancy sector.

Contents

1. Introduction

Big data has revolutionised the modern business landscape, offering unprecedented opportunities for data-driven decision-making, enhanced customer experiences, and streamlined operations. Organisations across industries are leveraging the power of big data to gain valuable insights, improve efficiency, and drive innovation. IT consultancies and software development firms like SDC are at the forefront of this revolution, providing expertise and solutions to help clients harness the potential of big data.

However, the exponential growth of big data also poses significant challenges, particularly in the realm of cybersecurity. The sheer volume, variety, and velocity of data generated and stored by organisations create an expanded attack surface and a lucrative target for cybercriminals. Data breaches, ransomware attacks, unauthorised access, and data loss can have devastating consequences for businesses, leading to financial losses, reputational damage, and regulatory penalties.

SDC, as a leading IT consultancy, recognizes the critical importance of safeguarding its big data assets. This research project aims to address the complex and evolving cybersecurity landscape associated with big data storage, both local and cloud-based. By understanding the specific vulnerabilities and threats faced by SDC, we can develop a comprehensive and proactive cybersecurity strategy that aligns with the company's business objectives and ensures the confidentiality, integrity, and availability of its valuable data.

This report presents a thorough examination of cybersecurity risks in big data storage, drawing on a comprehensive literature review, in-depth interviews with key personnel, focus group discussions with diverse employee groups, and a survey of both internal and external stakeholders. The research findings shed light on the current state of cybersecurity awareness and practices at SDC, identify areas for improvement, and inform the development of actionable recommendations. By implementing these recommendations, SDC can strengthen its security posture, protect its data assets, and maintain its position as a trusted leader in the IT consultancy sector.

In the following sections, we will delve into the specific cybersecurity challenges faced by SDC, analyse the root causes of these vulnerabilities, and propose a comprehensive action plan to mitigate risks. This plan will encompass employee training and awareness initiatives, technical solutions, and proactive measures to address emerging threats. The goal is to create a robust and adaptive cybersecurity strategy that ensures the long-term security and resilience of SDC's big data infrastructure.

2. Literature Review

The rise of big data has transformed the business landscape, particularly for IT consultancies and software development firms. The vast volumes of data generated and stored offer unparalleled opportunities for data-driven insights, improved decision-making, and innovation. However, the storage and processing of big data also introduces significant cybersecurity risks, necessitating a comprehensive understanding of these challenges and the development of effective mitigation strategies.

2.1 Big Data Storage Technologies

The proliferation of big data has spurred the development of specialised storage technologies to handle its unique characteristics: volume, variety, and velocity (Dumbill, 2012). Distributed file systems like Hadoop Distributed File System (HDFS) excel at storing large, unstructured data, offering fault tolerance and high throughput (Shvachko et al., 2010). NoSQL databases like MongoDB and Cassandra provide schema flexibility and horizontal scalability, making them ideal for handling semi-structured and unstructured data (Leavitt, 2010). Additionally, cloud-based object storage solutions like Amazon S3 and Azure Blob Storage offer virtually limitless scalability and attractive pay-as-you-go pricing models (Mell & Grance, 2011). While these technologies offer significant advantages, they also introduce new security challenges that traditional storage solutions may not address adequately.

2.2 Cybersecurity Risks & Vulnerabilities

The very nature of big data makes it an attractive target for cyberattacks. The sheer volume of data stored in these systems can yield vast amounts of sensitive information if compromised (Zikopoulos & Eaton, 2012). The distributed nature of big data architectures further expands the attack surface, with vulnerabilities in one node potentially compromising the entire system (Grover & Sengupta, 2019). These vulnerabilities can arise from inadequate authentication mechanisms, misconfigured access controls, and software or hardware failures. Moreover, the complexity of big data environments makes it difficult to detect and respond to security incidents in a timely manner, potentially exacerbating the damage caused by a breach (Jin et al., 2015).

Specific cybersecurity risks include:

- Data Breaches: Unauthorised access to sensitive data, leading to financial loss, reputational damage, and potential legal liabilities.
- Ransomware Attacks: Malicious software that encrypts data and demands payment for its release, causing significant disruption to operations.
- Insider Threats: Malicious or accidental actions by employees or contractors with authorised access to sensitive data.
- Supply Chain Attacks: Vulnerabilities in third-party software or services used in big data environments can be exploited by attackers.
- Social Engineering: Manipulation of employees to gain unauthorised access to systems or data.

2.3 Industry Best Practices & 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 offers a set of standards, guidelines, and best practices to help organisations 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, organisations that collect, store, or process personal data must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) (Information Commissioner's Office, 2018). These regulations impose stringent requirements on organisations like SDC to ensure the lawful and ethical handling of personal data. Compliance 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

Recent high-profile data breaches, such as those experienced by Dixons Carphone and Yahoo, serve as cautionary tales, highlighting the potential consequences of inadequate security practices in big data environments. These incidents emphasise the need for robust security measures, proactive risk management, and transparent communication in the event of a breach. They also underscore the importance of continuous employee training and awareness programs to mitigate the risk of human error and social engineering attacks.

3. Methodology

This research employed a mixed-methods approach, incorporating both qualitative and quantitative data collection and analysis techniques to gain a comprehensive understanding of cybersecurity risks in big data storage at SDC. This approach allowed for triangulation of data, enhancing the validity and reliability of the findings.

Qualitative Data Collection

Semi-structured Interviews: In-depth interviews were conducted with key internal stakeholders at SDC, including IT staff (e.g., system administrators,

network engineers), cybersecurity experts, and managers. These interviews aimed to elicit detailed insights into their experiences, perceptions of risk, challenges faced, and potential solutions related to big data security. Interviews also included external industry experts to gain a broader perspective on industry trends and best practices.

Focus Group Discussions: Focus group discussions were held with diverse groups of SDC employees from different departments, including IT, data science, business, and legal. This facilitated open dialogue and the sharing of collective experiences and concerns, enabling the identification of common themes and the exploration of potential solutions.

Interview and Focus Group Guides: The interview and focus group discussion guides, as detailed in the accompanying "Research Instruments" document, were designed to address specific research questions related to:

- Current big data storage practices at SDC.
- Perceived cybersecurity risks and vulnerabilities.
- The effectiveness of existing security measures.
- Employee awareness and training needs.
- Emerging threats and industry trends.
- Recommendations for improvement.

Quantitative Data Collection

Survey Questionnaire: A structured survey questionnaire, developed based on insights from the literature review and preliminary interviews, was administered to a broader sample of SDC employees and external participants. The survey included both Likert scale and multiple-choice questions to quantify opinions, assess awareness levels, and gather data on specific security practices and knowledge of common threats.

Data Analysis

Qualitative Data Analysis: Interview and focus group transcripts were analysed using thematic analysis. This involved coding the data to identify recurring patterns, themes, and key concepts related to big data security risks, challenges, and potential solutions. Thematic maps were created to visualise the relationships between themes.

Quantitative Data Analysis: Survey responses were analysed using descriptive and inferential statistics. Descriptive statistics (e.g., frequencies, percentages, means) were used to summarise responses and identify trends. Inferential statistics (e.g., t-tests, ANOVA, chi-square tests) were used to test hypotheses and examine relationships between variables, such as the relationship between employee role and cybersecurity awareness.

Ethical Considerations:

- Informed Consent: All participants were informed about the purpose of the research and their right to withdraw at any time.
- Confidentiality: All data collected was anonymized to protect the privacy of participants.
- Data Security: Data was stored securely in accordance with SDC's data protection policies.

Limitations:

- Sample Size: The sample size for interviews and focus groups was relatively small, which may limit the generalizability of the findings.
- Self-Reported Data: The survey data relies on self-reported information, which may be subject to biases and inaccuracies.
- Limited Timeframe: The research was conducted within a limited timeframe, which may have precluded a more in-depth exploration of certain issues.

Despite these limitations, the mixed-methods approach and the use of multiple data sources allowed for a comprehensive and nuanced understanding of cybersecurity risks in big data storage at SDC. The findings are robust and provide a solid foundation for developing effective recommendations to enhance the company's security posture.

4. Findings

1. Awareness and Preparedness Gap

Knowledge Deficits: Focus group discussions revealed that employees often lack a clear understanding of key cybersecurity threats. For instance, many participants confused phishing with general spam emails, and there was a misconception that ransomware only affects personal devices, not enterprise systems. This lack of awareness was corroborated by the internal SDC survey, where only 45% of employees reported completing cybersecurity training in the past year.

Risky Behaviours: The survey data revealed that 65% of SDC employees reuse passwords across multiple accounts, a practice that significantly increases vulnerability to breaches. Furthermore, 28% admitted to clicking on suspicious links or attachments, and 42% indicated they had never reported a potential security incident, suggesting a culture of complacency.

Misplaced Responsibility: Focus group discussions highlighted a common sentiment among employees that "cybersecurity is ITs job." This belief indicates a need to foster a culture of shared responsibility, where every employee understands their role in protecting company data.

2. Evolving and Sophisticated Threat Landscape

Ransomware Concerns: Both the podcast and interviews emphasised the growing sophistication of ransomware attacks, with attackers now targeting

backups and critical systems to maximise disruption. SDC employees also expressed concerns about ransomware, particularly its potential impact on project deadlines and client data.

Zero-Day Exploits and Supply Chain Risks: The Fortra survey highlighted the rise of zero-day exploits and third-party vulnerabilities as major concerns for organisations. This aligns with discussions in the podcast, which emphasised the need for proactive security measures and vigilance against unknown vulnerabilities that can be exploited before patches are available.

Overconfidence in Security: Focus group participants expressed a general belief that SDC was "probably safe" from cyberattacks, indicating a potential overconfidence in the company's security measures. This complacency could make employees more susceptible to social engineering attacks and less likely to report suspicious activity.

3. Cloud Security as a Top Priority AND Distrust:

Lack of Trust and Understanding: Focus group discussions revealed a significant lack of trust in cloud providers' security measures among some SDC employees. Many were unsure of who was responsible for what in the shared responsibility model, leading to confusion and a feeling of decreased control over data security.

Desire for Transparency: Employees expressed a desire for more transparency from SDC regarding the security measures in place for cloud-based big data storage. They wanted reassurance that their data was adequately protected and that SDC had taken steps to mitigate potential risks.

4. Human Factor and the Importance of Culture:

Acknowledging Human Error: Both the focus group and survey data highlighted the role of human error in security incidents. Participants acknowledged making mistakes like clicking on phishing links or reusing passwords. However, they also expressed a willingness to learn and improve their security practices.

Cultural Barriers: The low score on feeling empowered to report incidents in the SDC survey (2.8/5) suggests a cultural barrier to reporting potential threats. Employees may fear blame or repercussions for reporting mistakes, hindering early detection and response to security incidents.

Leadership and Communication: The need for strong leadership commitment to cybersecurity and clear communication of security policies and procedures was emphasised in both the focus group and interviews.

Conclusion:

These findings paint a comprehensive picture of the cybersecurity risks and challenges faced by SDC. They highlight the need for a multi-faceted approach that addresses technical vulnerabilities, enhances employee awareness, and fosters a culture of shared responsibility for security. The detailed evidence provided in this analysis will serve as a strong foundation for developing targeted and effective recommendations to improve SDC's overall cybersecurity posture.

5. Discussion

Awareness and Preparedness Gap: A Critical Vulnerability

The research paints a concerning picture of employee awareness and preparedness at SDC. While most employees have received some form of cybersecurity training, it has not translated into a deep understanding of specific threats like phishing and ransomware. Many employees lack confidence in identifying these threats and are unaware of the potential impact a successful attack could have on the company.

This lack of awareness is further compounded by risky behaviours such as password reuse and a reluctance to report suspicious activity. These behaviours, often stemming from a sense of complacency or a belief that "it won't happen to me" create significant vulnerabilities that could be easily exploited by cybercriminals.

The case studies of Dixons Carphone and Yahoo serve as stark reminders of the devastating consequences that can result from inadequate employee awareness and training. In both instances, human error played a significant role in the breaches, highlighting the importance of investing in comprehensive and ongoing training programs.

SDC must prioritise bridging this awareness gap by implementing a robust cybersecurity training program that goes beyond the basics. The training should be tailored to different roles and departments, focusing on the specific threats and risks relevant to each employee's responsibilities. It should also emphasise the importance of individual responsibility in maintaining a secure environment, empowering employees to become active participants in protecting company data.

Evolving Threat Landscape: The Need for Proactive Security

The research findings, coupled with insights from the Fortra survey and podcast, reveal a constantly evolving threat landscape that requires a proactive and adaptive approach to cybersecurity. Ransomware attacks are becoming increasingly sophisticated, targeting backups and critical systems to maximise disruption. Zero-day exploits, which take advantage of vulnerabilities unknown to software vendors, are on the rise, highlighting the need for continuous monitoring and rapid response capabilities.

The overconfidence expressed by some SDC employees regarding the company's security is a cause for concern. This complacency can lead to lax security practices and a delayed response to potential threats. SDC must foster a culture of vigilance and create a sense of urgency around cybersecurity.

To address the evolving threat landscape, SDC needs to invest in threat intelligence to stay informed about the latest attack vectors and techniques. Regular vulnerability assessments and penetration testing can help identify and address weaknesses before they are exploited. Additionally, SDC should consider adopting advanced security technologies, such as intrusion detection systems (IDS) and security information and event management (SIEM) solutions, to detect and respond to threats in real time.

Cloud Security: Addressing Concerns and Building Trust

The research revealed significant concerns among SDC employees regarding the security of cloud-based big data storage. Many lacked trust in cloud providers security measures and were unsure of their own responsibilities in the shared responsibility model. This lack of trust can hinder the effective utilisation of cloud resources and create a perceived security risk, even if the actual risk is low.

To address these concerns, SDC needs to prioritise transparency and communication regarding its cloud security practices. Clearly articulating the shared responsibility model, outlining the specific security measures implemented by both SDC and the cloud provider, and addressing employee questions and concerns can help build trust and confidence in the cloud environment. Additionally, implementing additional security layers, such as encryption and data loss prevention (DLP) solutions, can further enhance the security of SDC's cloud-based data.

Human Factor and the Importance of Culture:

The research consistently highlighted the crucial role of the human factor in cybersecurity. Employee behaviours, such as password reuse and failure to report suspicious activity, can create significant vulnerabilities. However, the findings also indicate that employees are willing to learn and improve their security practices when provided with the right tools and support.

This emphasises the need for SDC to foster a culture of security awareness and shared responsibility. This involves not only providing comprehensive training but also creating a supportive environment where employees feel empowered to report potential threats without fear of reprisal. Clear communication from leadership, regular reminders about security policies, and recognition of good security practices can all contribute to building a strong security culture.

Conclusion

The findings of this research project provide a comprehensive understanding of the cybersecurity risks and challenges faced by SDC in its big data storage operations. By addressing the identified vulnerabilities and implementing the recommended actions, SDC can significantly enhance its security posture, protect its valuable data assets, and maintain the trust of its clients and stakeholders. A multi-faceted approach that combines technical solutions with employee education and a strong security culture is essential for effectively mitigating risks in the ever-evolving landscape of cybersecurity.

6. Recommendations

1. Comprehensive Cybersecurity Awareness and Training Program

Tailored Content: Develop a modular training program with content specific to different roles (e.g., IT staff, data analysts, executives). Cover topics like:

- Basic Cybersecurity Hygiene: Password management, phishing recognition, social engineering awareness, software updates, and secure browsing habits.
- Data Handling and Classification: Understanding SDC's data classification system and proper procedures for handling sensitive information.
- Cloud Security Awareness: Educating employees on the shared responsibility model, cloud-specific risks, and best practices for secure cloud usage.
- Incident Reporting Protocols: Clear instructions on how and when to report suspected security incidents.

Engaging Delivery Methods:

- Interactive online modules with quizzes and simulations.
- Hands-on workshops for technical staff.
- Simulated phishing campaigns to test employee awareness.
- Regular newsletters and briefings on emerging threats and security tips.

Positive Reinforcement:

- Reward employees for completing training and demonstrating good security practices.
- Recognize and celebrate security champions within the organisation.

Ongoing Training:

- Schedule regular refresher training sessions to maintain awareness and address new threats.
- Make training resources easily accessible through an online portal or intranet.

2. Strengthened Security Policies and Procedures

Password Management:
- Require strong, unique passwords for all accounts.
- Enforce regular password changes (e.g., every 90 days).
- Mandate the use of password managers for storing and generating complex passwords.
- Consider implementing multi-factor authentication (MFA) for added security.

Access Controls:
- Implement role-based access controls (RBAC) to restrict access to sensitive data based on job responsibilities.
- Enforce the principle of least privilege, granting users only the minimum necessary permissions to perform their tasks.
- Regularly review and update access permissions to ensure they are appropriate.
- Implement strong authentication mechanisms, including MFA for privileged accounts.

Data Classification and Handling:
- Develop a comprehensive data classification scheme that categorises data based on its sensitivity (e.g., confidential, restricted, public).
- Establish clear policies and procedures for handling each data classification level, including storage, transmission, and disposal.
- Train employees on data classification and handling procedures.

Patch Management and System Updates:
- Develop a standardised patch management process to ensure timely application of security patches and software updates.
- Utilize automated tools to scan for vulnerabilities and prioritise patching.
- Monitor vendor security advisories and apply patches promptly.

3. Enhanced Cloud Security Measures

Vendor Due Diligence:
- Thoroughly assess the security practices of cloud providers before storing sensitive data.
- Ensure that cloud providers comply with relevant regulations (e.g., GDPR) and industry standards (e.g., ISO 27001).
- Negotiate strong contractual agreements that address data ownership, security responsibilities, and breach notification requirements.

Multi-Cloud Strategy:
- Consider using multiple cloud providers to diversify risk and avoid vendor lock-in.
- Evaluate the pros and cons of different cloud service models (e.g., Infrastructure as a Service, Platform as a Service, Software as a Service) to determine the best fit for SDC's needs.

Data Encryption:
- Encrypt sensitive data both at rest and in transit using strong encryption algorithms.
- Manage encryption keys securely and consider using hardware security modules (HSMs) for added protection.

Access Controls:
- Enforce strict access controls for cloud-based resources, including role-based access controls (RBAC), multi-factor authentication (MFA), and least privilege principles.
- Regularly review and update access permissions to ensure they are appropriate.

Monitoring and Logging:
- Enable detailed logging and monitoring of cloud activity to detect anomalies or suspicious behaviour.
- Implement real-time alerting for potential security incidents.

4. Proactive Security Measures and Technology

Threat Intelligence:
- Subscribe to threat intelligence feeds to stay informed about the latest cyber threats and vulnerabilities.
- Participate in information-sharing initiatives with other organisations in the industry.
- Vulnerability Scanning and Penetration Testing:
- Conduct regular vulnerability scans and penetration testing to proactively identify and address weaknesses in systems and applications.
- Use automated tools to scan for vulnerabilities and prioritise patching.

Intrusion Detection and Prevention Systems (IDS/IPS):
- Deploy IDS and IPS to monitor network traffic for suspicious activity and block potential attacks.
- Configure IDS/IPS to alert security personnel of potential threats in real-time.

Security Information and Event Management (SIEM):
- Implement a SIEM solution to aggregate and analyse security logs from various sources, providing centralised visibility into security events.
- Use SIEM to correlate events and identify patterns that may indicate a potential attack.

Data Loss Prevention (DLP):
- Implement DLP solutions to detect and prevent the unauthorised exfiltration of sensitive data.
- Configure DLP policies based on data classification and risk profiles.

5. Incident Response Plan

Establish an Incident Response Team:

- Identify and train a team of individuals responsible for responding to security incidents.
- Define roles and responsibilities for each team member.
- Develop Incident Response Procedures:
- Create detailed procedures for incident identification, containment, eradication, recovery, and lessons learned.
- Test the procedures regularly through tabletop exercises and simulations.

These comprehensive recommendations, when implemented effectively, will significantly enhance SDC's cybersecurity posture, protect its valuable data assets, and mitigate the risks associated with big data storage.

7. 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.

8. Conclusion

This comprehensive research project has illuminated the complex and evolving cybersecurity landscape that SDC faces in the realm of big data storage. Through a mixed-methods approach, the study has revealed critical vulnerabilities, including a significant gap in employee awareness and preparedness, concerns surrounding cloud security, and the ever-present threat of sophisticated attacks like ransomware.

While SDC has made strides in implementing some security measures, the findings underscore the urgent need for a more proactive, comprehensive, and employee-centric approach to cybersecurity. The prevalence of risky behaviours, such as password reuse and a reluctance to report potential threats, coupled with the rapid evolution of cyberattacks, necessitates immediate action.

The recommendations outlined in this report provide a roadmap for SDC to strengthen its security posture. Prioritising employee education and awareness, implementing robust technical controls (especially in the cloud), and fostering a culture of shared responsibility for security are paramount. Investing in advanced threat detection technologies and establishing a well-defined incident response plan are also crucial steps towards mitigating the risks associated with big data storage.

The successful implementation of these recommendations will not only enhance the protection of SDC's valuable data assets but also bolster the company's reputation as a trusted leader in the IT consultancy sector. A strong security posture will instil confidence in clients, attract new business opportunities, and ensure compliance with increasingly stringent regulations.

Moreover, by empowering employees with the knowledge and tools to make informed security decisions, SDC can create a more resilient and agile organisation, better equipped to adapt to the ever-changing threat landscape. This shift towards a security-conscious culture will not only protect SDC's bottom line but also contribute to its long-term success and sustainability.

In conclusion, this research project serves as a call to action for SDC. By embracing a proactive, comprehensive, and employee-centric approach to cybersecurity, the company can navigate the complexities of the digital age, safeguard its valuable data, and maintain its position as a trusted partner in the IT consultancy industry. The road ahead may be challenging, but with a committed and informed approach, SDC can successfully mitigate risks and capitalise on the vast opportunities presented by big data.

9. References & Bibliography

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)

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)