LUKE LITTLER 132290

HOPWOOD HALL COLLEGE

HTQ COMPUTING RQF

UNIT 6: PLANNING A COMPUTING PROJECT

RESEARCH INSTRUMENTS

Research Instruments

Contents

Research Instruments

1. Interview Guides

   1.1 Interview Guide for IT Staff

   Introduction and Background

   - Introduce yourself and the purpose of the interview.
   - Explain the importance of big data to SDC's operations.
   - Assure confidentiality and anonymity of responses.

   Current Big Data Storage Practices
   - Describe your role in managing and interacting with SDC's big data storage systems (both local and cloud-based).
   - What are the primary technologies used for big data storage at SDC (e.g., Hadoop, NoSQL databases, cloud storage)?
   - How do you access and utilise big data in your daily work?

   Perceived Cybersecurity Risks
   - What do you consider to be the most significant cybersecurity risks associated with big data storage at SDC?
   - Have you personally encountered any security incidents or breaches related to big data?
   - How have you seen these risks evolve over time?

   Current Security Measures
   - What security measures are currently in place to protect SDC's big data?
   - How effective do you believe these measures are in addressing the identified risks?
   - What are the main challenges you face in implementing or maintaining security measures?

   Awareness and Training
   - How confident are you in your ability to identify and respond to cybersecurity threats, such as phishing attacks or malware?
   - What kind of cybersecurity training have you received at SDC?
   - What additional training or resources would you find beneficial?

   Recommendations for Improvement
   - What specific actions do you think SDC should take to improve its big data security posture?
   - What new technologies or tools would you recommend for enhancing security?
   - How can we better raise awareness and promote security best practices among employees?

Research Instruments

1.2 Interview Guide for Cybersecurity Experts

Introduction and Background
- Introduce yourself and the purpose of the interview.
- Briefly describe SDC's big data environment and technology stack.
- Assure confidentiality and anonymity of responses.

Industry Trends and Emerging Threats
- What are the most significant cybersecurity trends and emerging threats you see in the big data landscape?
- How do these trends affect IT consultancies like SDC?
- What specific threats should SDC be particularly concerned about?

Risk Assessment
- How would you assess SDC's current cybersecurity posture regarding big data storage?
- What are the most critical vulnerabilities that you see in SDC's systems or processes?
- What are the potential consequences of a successful cyberattack on SDC's big data?

Best Practices and Recommendations
- What are the industry best practices for securing big data storage?
- What specific security measures and technologies would you recommend for SDC?
- How can SDC balance the need for security with the need for data accessibility and usability?

Compliance and Regulations
- What are the key regulatory requirements (e.g., GDPR, HIPAA) that SDC must comply with regarding big data storage?
- How can SDC ensure compliance while maintaining efficient operations?
- What are the potential consequences of non-compliance?

1.3 Interview Guide for Managers

Introduction and Background
- Introduce yourself and the purpose of the interview.
- Explain the importance of big data to your department's operations.
- Assure confidentiality and anonymity of responses.

Departmental Big Data Usage
- How does your department utilise big data in its day-to-day operations?
- What types of data do you collect, store, and analyse?
- How do you access and share big data within your department and with other teams?

Research Instruments

Security Concerns and Experiences
- What are your main concerns regarding the security of big data in your department?
- Have you or your team members experienced any security incidents related to big data?
- How does your department currently address these security concerns?

Impact of Security Incidents
- What would be the potential impact on your department if SDC suffered a big data breach or security incident?
- How would this impact your operations, productivity, and client relationships?
- What steps would you take to mitigate these impacts?

Resource Allocation
- How are resources (budget, personnel, time) allocated to cybersecurity in your department?
- Do you feel that these resources are sufficient to address the current risks?
- What additional resources would you require to improve your department's cybersecurity posture?

2. Focus Group Prompts

2.1 General Prompts

Perception of Cybersecurity:
- How would you describe your overall understanding of cybersecurity?
- What do you think are the biggest cybersecurity risks that SDC faces as a whole?
- How important is cybersecurity to you personally, and why?

Big Data Awareness and Usage:
- How familiar are you with the concept of "big data"?
- In what ways does your department or team use big data?
- What types of information are you storing or accessing within SDC's big data systems?

Security Concerns and Experiences:
- What are your main concerns regarding the security of big data at SDC?
- Have you personally encountered any security incidents or issues related to big data?
- How comfortable do you feel sharing sensitive information within SDC's systems?

Research Instruments

Current Security Practices:
- What security measures are you aware of that SDC currently has in place to protect big data?
- How effective do you think these measures are?
- What are the most frustrating or inconvenient aspects of SDC's current security practices?

Desired Improvements:
- What actions do you think SDC should take to improve its big data security?
- What specific security measures would you like to see implemented?
- How can we better raise awareness and promote security best practices among employees?

2.2 Targeted Prompts

IT Staff:
- What are the specific technical vulnerabilities you see in SDC's big data infrastructure?
- How could we improve our current security tools and technologies?
- What challenges do you face in managing and securing big data systems?

Cybersecurity Experts:
- What are the emerging threats specific to big data that you think SDC should be most concerned about?
- How can we proactively identify and address vulnerabilities in our big data environment?
- What industry best practices or standards should SDC adopt?

Managers:
- How does big data security impact your department's operations and productivity?
- What are the potential consequences of a data breach for your department?
- How can we better integrate security practices into your department's workflow?

3. Survey Questionnaire

Your participation in this survey is crucial to help us understand how we can improve cybersecurity measures for big data storage. Your responses will be kept confidential and used solely for research purposes.

Section 1: Demographics

Department/Team:
Job Title:
Years of Experience at SDC:

Research Instruments

Section 2: Cybersecurity Awareness

How would you rate your overall understanding of cybersecurity?
- Very poor
- Poor
- Fair
- Good
- Very good

Which of the following cybersecurity threats are you familiar with? (Check all that apply)
- Phishing attacks
- Malware
- Ransomware
- Social engineering
- Denial-of-service (DoS) attacks
- Other (please specify)

How often do you receive cybersecurity training at SDC?
- Never
- Rarely (once a year or less)
- Sometimes (a few times a year)
- Often (monthly or quarterly)
- Regularly (weekly)

How confident are you in your ability to identify a phishing email?
- Not at all confident
- Slightly confident
- Moderately confident
- Very confident
- Extremely confident

How would you rate the effectiveness of SDC's current cybersecurity communication and awareness efforts?
- Very ineffective
- Ineffective
- Neutral
- Effective
- Very effective

Section 3: Big Data Security Practices

How often do you work with sensitive or confidential data in your role?
- Never
- Rarely
- Sometimes
- Often
- Always

Research Instruments

How would you rate the security of SDC's big data storage systems?
- Very insecure
- Insecure
- Neutral
- Secure
- Very secure

Do you feel comfortable storing sensitive data in SDC's cloud-based storage systems?
- Yes, very comfortable
- Somewhat comfortable
- Neutral
- Somewhat uncomfortable
- No, very uncomfortable

How often do you change your passwords for work-related accounts?
- Never
- Rarely
- Every few months
- Every month
- More frequently than every month

Do you use a password manager to store and manage your passwords?
- Yes
- No

Section 4: Additional Feedback
- What are your main concerns regarding big data security at SDC?
- What specific actions would you recommend for SDC to improve its big data security?

Thank you for your participation!

Research Instruments