Research Report

Research report: Part A 3
1. Research objectives 3
2. Strategies/methods used 3
3. Sources of information 4
4. Securely store research information 4
5. Nature of issue 5
6. Cyber security vulnerabilities 6
7. Conclusion 6
Project Plan: Part B 7
1. Background to the project 7
2. Project scope 7
3. Project objectives 7
4. Key project deliverables 8
5. Process of implementation 8
6. Structure of the project team 10
7. Criteria to evaluate team performance 11
8. Methodology and sources of data 11
9. Risk management plan 11
Security systems: Part C 12
1. Risks and vulnerabilities 12
2. Stored securely 12
3. Research methods 12
4. Implications 12
5. Organisational assets 13
6. Risks and vulnerabilities 13
7. Conclusions 13
Appendix A – Name 13

Research report: Part A

1. Research objectives

The research aims to evaluate Gelos Enterprises' cyber security environment, focusing on policies, controls, and operational practices to determine the nature and causes of identified vulnerabilities. Specifically, the objectives are to:

- Assess the effectiveness of Gelos' **cyber security, data protection, and backup policies** in protecting sensitive customer data.
- Investigate potential causes of the suspected **data breach**, including outdated systems, weak security controls, and poor compliance practices.
- Identify cyber security vulnerabilities and risks that expose Gelos to potential exploitation and regulatory non-compliance.
- Provide evidence-based findings to guide DataTrust in recommending mitigation strategies and improved practices.

These objectives ensure the research addresses both **technical risks** and **compliance obligations**, including those under the **Privacy Act 1988** and the **Notifiable Data Breaches (NDB) scheme**.

2. Strategies/methods used

The research was conducted through a structured, evidence-based approach:

- **Document review**: Analysed Gelos' internal policies — Cyber Security Policy & Procedure, Data Protection Policy, and Data Backup Policy — to identify stated controls and standards.
- **Initial incident report analysis**: Reviewed the CI_CyberSecProject_AE_Pro2of2_Appx_InitialReport for details of the suspected breach, staff observations, and security weaknesses.
- **Comparative benchmarking**: Compared Gelos' practices with **NIST Cybersecurity Framework** and **Australian Government ISM** guidelines.
- **Risk analysis**: Examined how weaknesses in current procedures could lead to exposure of sensitive customer data.

These strategies directly align with the research objectives by identifying gaps between **current practice** and **required standards**, ensuring findings are based on both organisational evidence and external best practices.

3. Sources of information

The following sources were accessed and reviewed:

a. Gelos policies and procedures

- **Cyber Security Policy & Procedure**: Covers system access, password use, malware protection, and remote access requirements.
- **Data Protection Policy**: Outlines responsibilities for managing personal information, privacy protection, and secure storage.
- **Data Backup Policy**: Establishes backup schedules, responsibilities, and recovery planning.

b. Existing risk controls and monitoring strategies

- Antivirus and malware detection controls in place but inconsistently updated.
- Backup processes exist but restoration testing is limited.
- Access controls defined but weak enforcement of password complexity and multi-factor authentication.

c. Privacy protection and storage policies/procedures

- Data Protection Policy sets obligations for lawful collection and secure storage of customer information, consistent with the **Australian Privacy Principles (APPs)**.
- However, no evidence of regular compliance audits or incident response planning aligned with the **NDB scheme**.

d. Information and security policy

- Cyber Security Policy mandates secure remote access, use of VPNs, and user responsibility for safeguarding credentials.
- Weak implementation was evident, with outdated software and delayed patching.

4. Securely store research information

All research materials, including reports and policy documents, were stored in compliance with Gelos' **Data Protection Policy** and **Cyber Security Policy** by:

- Saving files in **encrypted company-approved storage** with access restricted to authorised DataTrust team members.

- Applying **role-based access controls** to prevent unauthorised data sharing.
- Backing up research data in accordance with the **Data Backup Policy**, ensuring recovery in the event of system failure.
- Avoiding the use of personal devices or third-party cloud storage systems not authorised by Gelos.

This ensured that sensitive customer and organisational information was safeguarded throughout the research process.

5. Nature of issue

Analysis of Gelos' policies, the incident report, and security environment identified several critical issues:

a. Outdated software and insufficient patch management

- Systems and applications were not updated regularly, leaving known vulnerabilities unpatched.
- This increased the likelihood of malware infection and system compromise.

b. Weak access controls and authentication mechanisms

- Employees were allowed to use default or weak passwords, with no clear enforcement of strong credential policies.
- Multi-factor authentication (MFA) was not mandated for remote access.
- These weaknesses increased the risk of unauthorised access.

c. Gaps in backup and recovery assurance

- While backup processes exist, there was little evidence of regular testing to confirm data restoration integrity.
- This exposes Gelos to prolonged outages or data loss if backups fail during a breach incident.

6. Cyber security vulnerabilities

Table 1: Cyber security vulnerabilities

Conclusions	Evidence
Outdated software and insufficient patching	*Initial report confirmed outdated applications and missing security patches; Cyber Security Policy does not mandate automated patch management (CI_CyberSecProject_AE_Pro2of2_Appx_InitialReport; GE_Cyber-security-policy-and-procedure).*
Weak access controls and authentication	*Cyber Security Policy references password use but lacks clear enforcement of strong passwords and MFA; Incident report highlighted login failures and system compromise (GE_Cyber-security-policy-and-procedure; CI_CyberSecProject_AE_Pro2of2_Appx_InitialReport).*
Gaps in backup and recovery assurance	*Data Backup Policy mandates scheduled backups but lacks mandatory recovery testing and monitoring of backup integrity (GE_Data-backup-policy).*

7. Conclusion

The research demonstrates that Gelos' cyber security vulnerabilities stem from both technical weaknesses and inadequate enforcement of policies. Outdated software and poor patch management expose systems to malware and exploitation. Weak access controls and the absence of MFA increase the likelihood of unauthorised access, particularly in remote working contexts. Backup processes exist but without routine validation, they cannot be relied upon during incidents.

These conclusions are justified by clear evidence from Gelos' own policies, the incident report, and industry standards. The assumption that existing policies alone provide adequate protection is flawed — policies require **enforcement, regular audits, and alignment with evolving security frameworks**. Without urgent improvements, Gelos remains at high risk of further data breaches, identity theft, and regulatory penalties under the **Privacy Act 1988** and the **Notifiable Data Breaches scheme**.

Project Plan: Part B

1. Background to the project

Gelos Enterprises has recently experienced a suspected **data breach** that may have exposed the personal information of up to 3.4 million customers, including sensitive identifiers such as driver's licence and passport numbers. Investigations revealed outdated software, weak access controls, and limited assurance of backup reliability. These weaknesses have left the organisation vulnerable to malware, unauthorised access, and data loss. The project has been initiated to address these vulnerabilities and ensure compliance with the **Privacy Act 1988** and the **Notifiable Data Breaches (NDB) scheme** while restoring trust in Gelos' cyber security practices.

2. Project scope

The scope of the project covers all **ICT systems, applications, and customer data environments** within Gelos Enterprises.

- **In scope:** patch management, authentication mechanisms, backup and disaster recovery, penetration testing, and compliance alignment.
- **Out of scope:** physical security audits, non-ICT business processes, and unrelated IT system upgrades.

Problem-solving methodology: The project will use the **NIST Cybersecurity Framework** and **OWASP Security Testing Guide**. It will follow a structured cycle of identifying vulnerabilities, assessing risk, implementing remediation, testing effectiveness, and establishing continuous monitoring.

3. Project objectives

a. Objectives:

1. Deploy automated patch management to ensure timely updates and eliminate known vulnerabilities.
2. Implement multi-factor authentication (MFA) and enforce stronger credential policies to mitigate unauthorised access.
3. Validate and strengthen backup and disaster recovery processes to ensure reliable data restoration.

b. Questions to be answered:

1. How can patch management be automated to reduce vulnerability exposure?
2. What authentication and access control mechanisms best protect sensitive customer information?
3. How can backup testing be standardised to ensure business continuity during a breach?

4. Key project deliverables

Deliverable	Expected Outcome
Cyber security research and vulnerability analysis	Evidence-based understanding of risks and best practices for mitigation.
Automated patch management deployment	All systems regularly updated with security patches.
MFA rollout across remote and internal systems	Reduced risk of unauthorised access.
Backup validation and disaster recovery testing	Verified ability to restore data and maintain continuity.
Final audit and project report	Comprehensive evaluation of project outcomes and compliance status.

5. Process of implementation

a. Statement of Work: Deliver a secure ICT environment by implementing patching automation, stronger authentication, and reliable backup testing, with minimal business disruption.

b. Key Tasks and Subtasks:

1. Research vulnerabilities and solutions (DataTrust Analyst).
2. Deploy automated patch management system (ICT).
3. Roll out MFA to all employees (Security Admin).
4. Conduct and validate backup restoration tests (Operations + ICT).

5. Final project audit and reporting (DataTrust).

c. Resource Allocation: ICT staff, project analysts, patch automation tools, MFA licences, backup servers, penetration testing software.

d. Milestones and Timelines:

- Week 1–2: Vulnerability research completed.
- Week 3–5: Patch management system deployed.
- Week 4–6: MFA rollout completed.
- Week 6–7: Backup testing conducted.
- Week 8: Final audit and reporting.

e. Estimated Costs:

- Research & reporting: $15,000
- Patch management deployment: $25,000
- MFA rollout & training: $30,000
- Backup testing & validation: $10,000
- Final audit & compliance reporting: $20,000
  Total Estimated Budget: $100,000

6. Structure of the project team

Outline the structure of the project team, including:

a. Selection of team members, including their roles and functions, allocated to the project.

b. Determination of team member roles and responsibilities, including tasks and subtasks to which they are assigned, and the resources required to complete them.

Table 2-Internal contacts

Role	Name	Contact details	Responsible for:
Project Sponsor	Tejas Aarush	Tejas.Aarush@gelosmail.com.au	Executive oversight and approvals
Project Manager	Md Salam	md.salam@dmail.com	Manage project execution
Project Lead / ICT	Lucas Isaaks	Lucas.Isaaks@gelosmail.com.au	Patch management deployment
Security Administrator	Lee Dowling	Lee.Dowling@gelosmail.com.au	MFA rollout, monitoring
Operations / Pen Tester	Chris Smith	Chris.Smith@gelosmail.com.au	Backup testing, penetration testing
Incident Handler	Andrew Negapatan	andrew.negapatan@dmail.com	Lead on incident response & privacy
Desktop	ICT Support Team	ict.support@gelosmail.com.au	Communications, note taking, team coordination

7. Criteria to evaluate team performance

- Completion of tasks within allocated timelines and budget.
- Quality of deliverables, measured against project objectives.
- Compliance with Gelos' policies and relevant legislation.
- Effective collaboration and communication between team members.
- Minimal disruption to business operations during implementation.

8. Methodology and sources of data

Performance will be evaluated using:

- Project documentation (status reports, meeting minutes).
- Milestone tracking via Gantt charts and project dashboards.
- Incident response and penetration testing reports.
- Feedback from stakeholders and project sponsor.
- Compliance checks against **Privacy Act 1988**, **NDB scheme**, and **ISM controls**.

9. Risk management plan

#	Risk / Unexpected Event	Likelihood	Consequence	Risk Rating	Mitigation Strategy	Resources Required
1	Malware infection due to outdated systems	High	High	Extreme	Automated patch management	ICT staff, patching tools
2	Credential theft due to weak authentication	High	High	Extreme	MFA rollout, password policy enforcement	Security Admin, MFA licences
3	Backup failure during recovery	Medium	High	High	Regular restoration testing	ICT, backup servers
4	End-user disruption during MFA rollout	Medium	Medium	Medium	Phased rollout with training	ICT staff, trainers

#	Risk / Unexpected Event	Likelihood	Consequence	Risk Rating	Mitigation Strategy	Resources Required
5	Budget overruns	Medium	Medium	Medium	Strict tracking and approvals	Project Manager, Finance
6	Non-compliance penalties under Privacy Act	Medium	High	High	Regular audits, compliance checks	DataTrust consultants

Security systems: Part C

1. Risks and vulnerabilities

[Identify, outline, and document the risks and vulnerabilities associated to the research objectives.]

2. Stored securely

[Explains how research information will be stored securely.]

3. Research methods

[Outlines the research methods to be used and explains the reliability of each method.]

4. Implications

[Identifies, evaluates, and outlines the implications of:

1. current levels of employee awareness, strategies to promote awareness, habits, and compliance with cyber-security policies.
2. existing cyber security configuration and change management capability.
3. existing security clearance levels relating to organisational data.
4. existing security infrastructure baseline including physical security assets.
5. Gelos are using Nessus and Splunk as part of the organisation security infrastructure,

provide an audit review of these two tools. Using minimum of 100 to maximum of 200 words for each tool.]

5. Organisational assets

[Outlines a valuation of the organisations assets impacted by cyber security policies.

6. Risks and vulnerabilities

Identify, outline, and document the risks and vulnerabilities associated with:

1. Categorisation of risks based on their likelihood and consequence.
2. Controls to effectively manage identified risks, including those associated with human interaction.
3. Resources required by risk category which minimise business disruption.

7. Conclusions

Outlines conclusions relating to:

a. cyber information and security policy and procedure documents.

b. employee work habits and their impact on cyber security.

c. cyber security configuration and change management capability.

d. Strategies for raising employee awareness cyber security practices, policies and procedures.

Explains how the conclusions are justified.

Details a security recovery plan.

Appendix A – Name

Table 3: Give the table a title or brief description

Table header		
