Security Fundamentals (H9SFND)

Security Fundamentals (H9SFND)

Turnitin

Document Details

Submission ID

trn:oid:::2945:318533574

Submission Date

Oct 14, 2025, 2:08 PM GMT+5

Download Date

Oct 14, 2025, 2:09 PM GMT+5

File Name

unknown_filename

File Size

62.0 KB

8 Pages

2,493 Words

15,269 Characters

0% detected as AI

The percentage indicates the combined amount of likely AI-generated text as well as likely AI-generated text that was also likely AI-paraphrased.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Detection Groups

0 AI-generated only 0%
Likely AI-generated text from a large-language model.

0 AI-generated text that was AI-paraphrased 0%
Likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

Disclaimer
Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

National College of Ireland

Project Submission Sheet

Student Name: ………

Student ID: ………

Programme: ……………………………………………………………… **Year:** ……………………………

Module: ………

Lecturer: ………

Submission Due Date: ………

Project Title: ………

Word Count: ………………………………………………………………………………… 1258……………………………………

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: ………

Date: ………

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.

3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgment Supplement

Security Fundamentals (H9SFND)

Continuous Assessment (CA) Type:

Open-book Assignment

Your Name/Student Number	Course	Date

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

[Insert Tool Name]	
[Insert Description of use]	
[Insert Sample prompt]	[Insert Sample response]

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Continuous Assessment (40%)
Security Fundamentals

[Student Name]
[Student ID]
[Group (Charity)]

Q1 Answer: Cybersecurity Report: PeopleCare Charity

Cyber Attacks within the Charity Industry

Charitable organisations like PeopleCare are becoming a target of cybercriminals because they store confidential information of their donors, beneficiaries, and applicants. Such organisations are sometimes viewed as an easy target because they have fewer IT systems, weaker IT defences than organisations with more money and government agencies. 2 recent cases illustrate the weaknesses in the charity sector:

First Incident: Ransomware service access: Save the children Breach (2023)

In November 2023, the BianLian gang was accused of a ransomware attack against Save the Children International (Powell, 2023). The initial access was obtained by attackers with the help of a phishing email addressed to employees. Having entered the network, they installed ransomware, stole the data, and provided them with a price. Financial reports and donor-related information, as well as 7TB of sensitive files, were compromised. The attack interfered with the operations as staff were not allowed to access the important case management and fundraising systems.

The breach of personal identifiable information, with an opportunity to be perpetrated against innocent people as a result of it, was a serious blow to the confidence of the donors. In addition, the incident raised a risk of regulatory compliance in the context of GDPR that could put the organisation at risk of a penalty (Greig, 2023). The case demonstrates that charities are very profitable targets because of the use of digital solutions and their international scope of donors, and how one successful phishing attack can grow into a mass crisis when there are not sufficient preventive mechanisms in place and donor training.

Compromise & Impact:

- Data of staff and donors is at risk.
- Temporary failure of systems to process the donations.
- Tarnished image with donor trust.
- Possible violation of GDPR specifications.

Table 1: Attack Vector & Timeline of first incident

Day 1: Phishing Email	A malicious email that appeared in the form of an internal financial update was received by an employee.
Day 3: Deployment of malware	A Trojan was deployed that was a remote access trojan (RAT).
Day 7: Privilege Escalation	Hackers transferred laterally, obtaining admin credentials.
Day 12: Data Exfiltration	Huge volumes of data on donors and beneficiaries were captured.

Day 15: Ransom Note Fulfilled	Files had been encrypted, and a ransom was demanded by the attackers.
Day 20: Response to the Incident	The IT department switched off the affected servers and called in the specialists on cybersecurity.

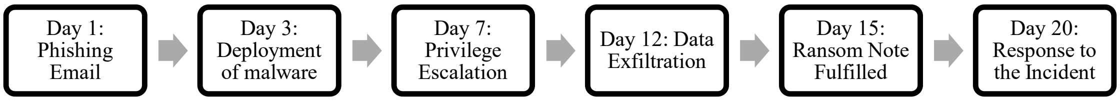
Day 1: Phishing Email
Day 3: Deployment of malware
Day 7: Privilege Escalation
Day 12: Data Exfiltration
Day 15: Ransom Note Fulfilled
Day 20: Response to the Incident

Figure 1: Diagram of the Attack Vector and timeline of the first incident

Second Incident: British Council Data Leak (2022)

In 2022, the British Council, a charity and training organisation, leaked more than 144,000 documents made up of sensitive files in a Microsoft Azure cloud server that was not secured (Elsayed, 2022). These files contained student files, passport scans, emails and log-ins exposing beneficiaries and applicants to a high risk of identity theft and fraud. The attack location was not a penetration attempt, but an incorrect setup that resulted in open cloud storage.

The reputational effects were tremendous as the stakeholders doubted the capability of the organisation to be responsible with sensitive information. This error also brought out the compliance issues under GDPR and illustrated the impact of human and policy vulnerabilities in cloud management, as potentially harmful as external intrusions (Zurier, 2022). It established the fact that charities that heavily depend on cloud services should ensure that there are strict access regimes, auditing, and frequent security tests to mitigate the wrongful exposure of highly confidential information.

Compromise & Impact:

- Including student records, email addresses, and passport scans were revealed.
- There was a vulnerability of beneficiaries to identity theft and fraud.
- Reputational danger, especially in relation to the inability to gain access to cloud resources.

Table 2: Attack Vector & Timeline of the second incident

Day 1: Config error	One of the cloud storage buckets remained with public access.
Day 5: Discovery by Security Researchers	The flaw was discovered by a cybersecurity company, SafetyDetectives.
Day 10: Exploitation Window	Unprotected files might be compromised by potential attackers.
Day 12: Responsible Disclosure	Having learned about it, researchers notified the British Council.
Day 15: Remediation	Trained access was limited, and an internal audit emerged.
Day 30: Public Awareness	Publicity on the incident took place, resulting in reputational examination.

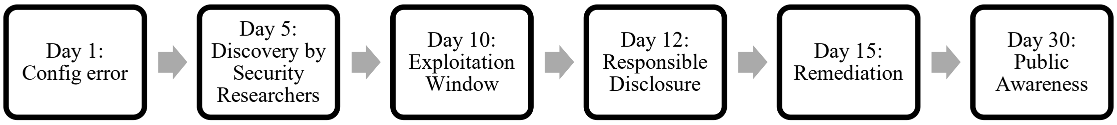

Figure 2: Diagram of the Attack Vector and timeline of the second incident

Comparative Analysis

The two incidents show various yet similar vectors of attack, such as ransomware, phishing, and cloud misconfiguration. The operations and financial impacts of the ransomware incident, and the weakness in governance and compliance exposed by the cloud leak, highlighted the vulnerabilities of the healthcare systems. In the case of PeopleCare, the two cases are an example that charities are not only susceptible to external attacks by criminals but also to their mismanagement.

Q2 Answer: Application of the CNSS Security Model (McCumber Cube)

The CNSS model takes into account three dimensions, namely information states (storage, transmission, processing), security objectives (confidentiality, integrity, availability), and security measures (technology, policy, human factors) (Rafique, 2023). There are four main intersections which are explored in the case of the charity sector, and for PeopleCare, this framework is very useful since security recommendations are not viewed as a standalone but as an element of a multidimensional approach.

Charities tend to be multi-jurisdictional, receive donation transactions via the internet, store beneficiary data on the cloud, and work with sensitive health, financial or personal data. By using the CNSS cube, PeopleCare have the ability to maintain the priority in both the technical measures and the organisational operations and cover the weaknesses identified in the most recent incidents in the sector, including ransomware and cloud misconfigurations.

Mapping resilience measures to particular intersections can assist the charity in building its resilience, operational compliance, and the willingness of people to trust the charity and its activities (Cordery and Yates, 2024). This is also a systematic way of ensuring that the technological solutions are strengthened by the policies and awareness among the employees creating a comprehensive defence mechanism that suits the dynamic environment that PeopleCare operates in.

a) Technology × Confidentiality × Transmission

Control: Engage in end-to-end encryption of donor and beneficiary emails (emails, payment advertisements, applications).

- Plucks off the interception of crucial information during communication.
- Data protection and compliance with the standards of GDPR.
- Secures the credit card information of the donors when making online donations.

b) Policy × Integrity × Storage

Control: Enforcing the data classification and access control.

- All records of the beneficiaries and the donor in databases ought to be labelled in terms of sensitivity.
- RBAC (Role-based access control) allows records to be edited or accessed by authorised staff.
- Integrity is ensured because unwarranted changes or corruption of data are avoided.

c) Human Factors × Availability × Processing.

Control: Train all charity staff and volunteers by means of cybersecurity awareness training.

- Lowers phishing results of phishing attacks, such as the Save the Children campaign.
- Employees are taught how to identify the red flags, report the cases, and proceed with the recommendations.
- Guarantees the consistency of donation-processing and case management systems.

d) Technology × Integrity × Storage

Control: Have automatic backup and security check systems.

- The use of hash-based verification to verify files that are authentic and not altered is done daily.
- Ransomware attacks are also recoverable in unaffected backups without paying ransom.
- Increases business continuity recovery through restoration of donor systems within recovery time boundaries.

These CNSS intersections offer comprehensive protection of PeopleCare with the amalgamation of the technology, tech-powered policies, and human resilience. It will be in line with best practices such as ISO/IEC 27001 and guidance on digital resilience by the UK Charity Commission.

Q3 Answer: Key Security Roles in PeopleCare

To ensure a strong security posture, PeopleCare needs to be willing to formulate specific and distinct positions which respond to the special risks charities are exposed to. Charities have restricted budgets and a huge number of volunteers, unlike commercial firms, and sensitive information about beneficiaries, so it is necessary to have good governance and accountability. Distinct security roles of responsibilities seek to ensure that the duties are not divided and that the processes, technology, and people systematically address cyber risks (Admass *et al.*, 2024). PeopleCare can offer ownership of certain positions and thereby address the threats in advance, the legal requirements, and counteract the occurrences in a well-coordinated manner, which will save the donor confidence and the well-being of the beneficiaries.

1. Chief Information Security Officer (CISO)

- Strategises and manages the cybersecurity of the organisation.
- Guarantees the adherence to regulations (GDPR, PCI-DSS for the donations).
- Risk and incident response reports straight to the Board.

2. Data Protection Officer (DPO)

- Deals with privacy and compliance requirements.
- Fulfils data processing based on the donor and beneficiary consent.
- Provides an interface between the data subjects and the regulators.

3. The Security Operations Centre (SOC) Analysts

- Surveillance networks on suspicious activity.
- React to events promptly.
- Identify the anomalies in the systems of donation and CRM with the assistance of SIEM tools.

4. Cloud Security Engineer

- Administers setups of online giving websites and beneficiary databases.
- Provides identity and access management (IAM) with proper management.
- Eliminates improper administration, such as the case of the British Council.

5. Cybersecurity Awareness Trainer.

- Plans and conducts security awareness programs for employees and volunteers.
- Lessens the human factor by creating awareness.
- Strengthens the organisational culture of security.

6. Incident Response Manager

- Manages coordination activities of IT response, legal, and communications teams.
- Ensures containment of incidents to limit the damage is limited.
- Manages after-death reviews and enhancements.

Discussion and Conclusion

PeopleCare has a high vulnerability to cyberattacks because their custodianship of sensitive data of donors and beneficiaries, and their comparatively low levels of defence, place them at a disadvantage. The case of the Save the Children ransomware hack and the misconfigured cloud of the British Council reveals costs borne (financial, operational, and reputational costs) related to a lack of effective cybersecurity.

Using the CNSS model, one can emphasise the encryption, policy of access control, staff training, and backup to ensure integrity (Doyle, 2025). Moreover, a well-structured defence and conformity to regulations through the presence of well-defined positions like CISO, DPO, SOC Analysts, and Cloud Engineers ensure that the defence is in layers (Abagale, 2025). Finally, improving the cybersecurity situation in charity is not merely a technological matter, but a culture of safety and the ability to establish a stable relationship with the donor and to guarantee the continuous provision of humanitarian assistance. The long-term vision of the introduction of cybersecurity at PeopleCare needs to be aimed at integrating it into all its operational decisions, periodic audits, and contributing to donor transparency.

References

Abagale, G. (2025) *Welcome To Zscaler Directory Authentication*. *Medium.com*. Available at: https://medium.com/@gertrude.kaneah.abagale/defence-in-depth-to-a-soc-analyst-d40903d8e362 (Accessed: 1 January 2025).

Admass, W.S., Munaye, Y.Y. and Diro, A.A. (2024) ‘Cyber Security: State of the Art, Challenges and Future Directions’. *Cyber Security and Applications*, 2(2). DOI: 10.1016/j.csa.2023.100031.

Cordery, C. and Yates, D. (2024) ‘Regulatory Responses to Build Charity Financial Resilience: “Tow Truck” or “Guardian Angel”?’ *Financial Accountability & Management*. DOI: 10.1111/faam.12392.

Doyle, K. (2025) *CNSS Instruction: Why It’s Critical for National Security and Your Organization | Tripwire*. *Tripwire.com*. Available at: https://www.tripwire.com/state-of-security/cnss-instruction-why-its-critical-national-security-and-your-organization.

Elsayed, J.H. (2022) *British Council Data Breach Leaks 10,000 Student Records*. *The Daily Swig | Cybersecurity news and views*. Available at: https://portswigger.net/daily-swig/british-council-data-breach-leaks-10-000-student-records.

Greig, J. (2023) *Save the Children International Hit with Cyberattack, but Says Operations Weren’t Impacted*. *therecord.media*. Available at: https://therecord.media/save-the-children-charity-cyberattack.

Powell, O. (2023) *Ransomware Gang Steals 6.8TB of Data from Save The Children*. *Cyber Security Hub*. Available at: https://www.cshub.com/attacks/news/ransomware-gang-steals-68tb-of-data-from-save-the-children.

Rafique, K. (2023) *Demystifying Cybersecurity and Information Security: Exploring the CNSS Security Model and More*. *Medium*. Available at: https://medium.com/@kashafrafique5/demystifying-cybersecurity-and-information-security-exploring-the-cnss-security-model-and-more-44420e2667f3.

Zurier, S. (2022) *Personal Data on British Council Students Exposed on Open Microsoft Azure Blob*. *SC Media*. Available at: https://www.scworld.com/news/personal-data-on-british-council-students-exposed-on-open-microsoft-azure-blob (Accessed: 1 January 2025).