

Computer Systems Report

by Lucy Henson

Submission date: 10-Apr-2025 02:02PM (UTC+0100)

Submission ID: 255358029

File name: 59290_Lucy_Henson_Computer_Systems_Report_659655_573233473.docx (42.63K)

Word count: 1955

Character count: 10248

Computer systems fundamental

Lucy Henson
Student No: 2418593

L4 – Computer systems
fundamental

ACDA4022

Embedded Electronic systems
Engineering Degree Apprenticeship

Contents

Introduction	3
Task 1	3
Overview	3
PC parts	3
Task	5
Security Assessment	5
Response Plan and cybersecurity fixes	6
Conclusion.....	7
Reference.....	7
Bibliography	7

Introduction

This report is split into two parts the first part tackles the company's hardware requirements for being able to design run engineering software's like SolidWorks and It spice. It also tackles the operating system used Aswell  second part focuses on the companies cyber security vulnerabilities which were highlighted in a recent audit. The second part will go into detail about the severity and likelihood of each vulnerability and will provide solutions to all the cyber security problems. The second part will also show a response action plan which will show the company how to deal with a breach in their system and which areas are more vital to running the company.

Task 1

Overview

The company would like a PC which can run both engineering software's SolidWorks, Spice and LabVIEW while also being able to operate as a normal desktop being able to run teams meeting software and other profession tools for presenting, report writing and budgeting. The list of parts needed can be seen below

- CPU and Motherboard
- RAM
- Storage
- Input and output ports
- Graphics card
- Case and power supply
- Monitor
- Webcam
- Keyboard
- Mouse
- Required software
- Network connectivity

PC parts

Component	Selection	Specification	Price
CPU	Intel Core Ultra 9 285K	24 cores, 24 threads, 4.6-5.7GHz	£539.99
CPU Cooler	Noctua NH-D15	300-1500RPM 19.2- 24.6 dB	£99.98

Motherboard	Gigabyte Z890 Aorus Elite Wifi7	1 x PCIe 5.0 M.2 Slot 3 x PCIe 4.0 M.2 Slots x PCIe 5.0 x16 2 x PCIe 4.0 x4 4 x USB 2.0 2 x USB 3.2 Gen 2,3 x USB 3.2 Gen 1 ,2.5 GbE LAN, Wi-Fi 7, 1 x Front USB-C 10Gb/s 4 x SATA 6Gb/s, 2 x PCIe 4.0	£241.90
Memory	Kingston fury beast 128 GB (4x32GB) DDR5 memory	DDR5 – 5200MT/s 128GB total	£244.80
Storage	Crucial P3 Plus SSD 2TB M.2 NVMe PCIe Gen4 Internal SSD	2TB read speed 7,400MB/s	£97.99
Graphics card	MSI Venture GeForce rtx 3050	2x8GB 1550MHz GDDR6 HDMI	£184.99
Case	Lian Li O11 Dynamic XL	8x USB 3.0 Type A 2x USB 3.1 Type C 2x HDD cages	£194.99
Power supply	TUF 1000W 80+ Gold certified fully modular power supply	Fully modular 1000W ATX 3.0	£151.97
Operating system	Windows 11	Runs SolidWorks	£119.99
Monitor	Dell C3422WE 34Inch WQHD	Built in webcam curved 34-inch monitor 60Hz	£494.00
Mouse and keyboard combo	HP 230 Wireless Keyboard and mouse combo	2.4GHz 16-month battery life Wireless 1600dpi	£19.96

In the table above you can see the chosen parts for the companies PC build. The main task was for it to run SolidWorks and other engineering applications without any issues therefore I used the recommended hardware selection on SolidWorks site to choose the CPU as the developers will know exactly what hardware will work the most optimal for the company. The intel core ultra 9 285K CPU was chosen as not only was it recommended by the SolidWorks hardware part of their website [1], but the CPU has 24 cores to run allowing for more performance. The motherboard was used as its compatible with the CPU and can be overclocked to allow for more performance. It also has Wi-Fi 7 built in and lots of ports to connect different devices to. The 1000-watt power supply was chosen as it allows the engineer to upgrade parts of the pc in the future without having to get a new power supply as the power consumption of the pc now is 671watts. A large case was chosen to house all the components with room to upgrade in the future. The 128 Gb memory DDR5 as it has more

bandwidth per CPU core which should allow for better performance across the cores. Windows 11 was chosen as the operating system due to the easier nature of the operating system compared to others like Linux which windows is more restrictive the user will not be able to notice and their experience using SolidWorks and teams will not be hampered.

Task

Security Assessment

The companies cyber security issues have been listed below.

- Outdated firewall configurations cause vulnerable network
- Outdated firmware on devices and default passwords
- International supplier has no cybersecurity practices
- Limited cyber security training amongst staff has led to phishing and social engineering attacks

The issues will all be ranked for their severity and likelihood. The most vulnerable part is the outdated firewall due to the risk of an attack being able to eavesdrop on the network and potential gain access to not only the company's data but also customer data Aswell. The most common form of attack against a company is the DDOS denial of service attack which would render customers and clients unable to access the website. With the DDOS attacks being more common the severity and likelihood of an attack is high. [2]. The outdated firewall could lead the company susceptible to many forms of attack including drive by attacks where hackers embed malicious scripts into various websites which when users interact with cause there data to be accessible to hackers another form of attack would be adware attacks which allows hackers to pop up adverts on a victims computer or mobile device which can cause them to slow down the device or try and install a virus or spyware. The firewall would block users from being able to go onto dangerous websites and block adverts the second most vulnerable area would be the outdated firmware and default passwords. The default passwords can easily be cracked by hackers as in the 2014 Trustwave analysis out of 691 data breaches a third were caused by default passwords. [3]The default passwords also mean that once the attack is inside they could potential have access to all data forms including customers and clients. The outdated firmware leaves the devices open to SQL injection attacks which involve a malicious SQL code being injecting into an application allowing attackers to view and modify the database. These forms of attack are usually counteracted by developers releasing security patches in the firmware. The default passwords being cracked would be very likely to happen however the outdated firmware is less likely to happen due to it being harder for an attacker to accomplish compared to other forms of attack. The lack of cybersecurity training is third in the most vulnerable but still very severe due to untrained staff not being able to identify breaches when they happen. The lack of cybersecurity training means the staff would not have the knowledge to identify a potential breach in the system it would also make them more susceptible to social engineering attacks like the phishing attacks which have already caused problems for the company. The main

two phishing attacks which the company is vulnerable to are spear and whale attacks which involve the hacker posing as either an important businessperson like a chairman or head of an organisation or sending fraudulent emails and phone calls to gather unauthorised information. The lack of training is the most likely to cause an issue due to untrained staff being a target for phishing attacks. The international supplies not having robust cybersecurity practices is an issue but is less serious compared to the others as its not in house and there is always the option of switching supplies. The lack of cybersecurity practices means that any of these devices could be susceptible to zero-day attacks which might take months for the developers to fix.

Response Plan and cybersecurity fixes

A plan to tackle all the major cybersecurity risks in the company would first be setup proper network firewalls and to have a dedicated network engineer who can routinely check and update the firewalls, if necessary, against new types of attacks. The second part of the plan would be to implement proper cybersecurity training for all staff and to have an annual refresher for all employees. The company could also implement fake phishing emails every so often to ensure that all employees are able to correctly identify and report any attempts at breaches. The next part of the plan would be to change all default passwords and update all firmware on factory devices. The passwords should be changed to something between 8-16 characters with a mixture of numbers and special characters to make it more secure. The same password should also not be used for multiple devices and passwords should not be written down somewhere in plain sight like on a desk next to a PC. A recommendation would be to enable 2FA on devices which are able to support it as it brings an extra layer of protection against brute force attacks. The companies' issue with the international manufacturer is more difficult to fix as they are a different company. The advice would be to either change manufacturers to one which is more cybersecurity aware or to provide feedback to the manufacturer around concerns that their product may be vulnerable to firmware attacks.

The steps taken to ensure a company is protected against any cybersecurity threats can be seen below

1. Identify key and critical assets within the company and then categorise them based on their function. This will give the company an idea on which areas they need to focus their resources, and which are the most essential.
2. Identify potential threats and vulnerabilities through risk assessments and threat analysis to understand the evolving landscape of cybersecurity threats. This step allows the company to see any other points of failure in their system before it's too late.
3. Create an incident response team of trained professionals who have a clear view of their roles and responsibilities and clear communication channels. These people should be able to detect, contain and investigate any breaches in security quickly and efficiently.
4. Create an incident response plan. The steps in the incident response plan would be to

- 1.Preparation create an incident response team with clear understanding of their roles, responsibilities and knowledge of any potential threats.
- 2.Detect and identity any breaches in the company related to cybersecurity.
- 3.contain the incident and limit damage to the company.
- 4.Removal of the threat from company systems
- 5.Recover any data or affected systems to normal
- 6.Review and analyse the incident to see key areas for improvement like weak points in the system and response time to threat.

Conclusion

In conclusion this report demonstrates the necessary parts needed to build a functional PC for the companies engineering needs and has given the company a clear understanding and plan of what's needed to upgrade their cybersecurity system to mitigate threats from attackers. The report has also given the company a response plan on what to do if the have had a cybersecurity breach. The key takeaways for the company on their cybersecurity policy is to always make sure all firmware and firewalls are up to date with the latest updates against any threats. The company should also annually have cybersecurity training updates for the employees and to change all default passwords to more secure ones which should not all be related or the same. If devices can have 2FA on, then they should as it provides another layer of security. The PC built has been designed around the requirements of SolidWorks and the other engineering software so there it should run optimally on those software and any normal professional office tools.

Reference

Bibliography

- [1] "Solidworks solutions hardware recommendations," [Online]. Available: <https://www.solidolutions.co.uk/solidworks-support/hardware-advice.aspx>. [Accessed 10 04 2025].
- [2] "Checkpoint main threats against firewalls," [Online]. Available: <https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/6-main-firewall-threats-vulnerabilities-and-how-to-mitigate-them/>. [Accessed 09 04 2025].

Lucy Henson 2418593
University Wales Trinity St David
Computer system fundamentals

- [3] "advania 5 common network vulnerabilities," [Online]. Available:
https://www.advania.co.uk/insights/blog/top-5-common-network-vulnerabilities-default-login-credentials/?lai_vid=OXgk0nqXaflax&lai_sr=35-39&lai_sl=m. [Accessed 09 04 2025].

Computer Systems Report

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

64/100

PAGE 1

PAGE 2

PAGE 3



Comment 1

aswell



Comment 2

Good use of table



Comment 3

caption
should be added for the table, so the reader will get an idea about the table

Caption for the table should be
positioned at the top of the table

PAGE 4



Comment 4

Compose
the report from a third-person perspective.

**Comment 5**

Its Reference, as you have cited this in the description.

GRADING FORM: GRADING

LUCY HENSON**64****ENGAGEMENT WITH LITERATURE**

The report should be supported by credible sources relevant to cybersecurity and computer systems design in engineering. Sources may include academic journal articles, textbooks, government and industry guidelines, and reputable websites. Recent materials (within the last five years) on cybersecurity, and hardware specifications are encouraged. Proper referencing with in-text citations and a reference list is essential to show the breadth and relevance of research.



Engagement with a limited range of mostly relevant and credible sources. However, only three references were included. The work would have been stronger with a greater number of references from reliable sources.

4.8**KNOWLEDGE AND UNDERSTANDING**

The report should demonstrate knowledge of key cybersecurity principles and hardware specifications relevant to the scenario. Understanding should be shown through explanations of how these

principles apply to real-world scenarios, supporting a balanced approach to risk mitigation by protecting data integrity, confidentiality, and availability.



Competent knowledge of the basic underlying concepts and principles of computing fundamentals and cybersecurity is evident through the description. There is a good understanding of the PC components required for engineering tasks, and an awareness of key cybersecurity concepts is also demonstrated. However, the work would have been stronger with a deeper explanation of the PC component and more detailed demonstration of threat mitigation methods would enhance the cybersecurity analysis.

20.4

COGNITIVE AND INTELLECTUAL

The report must include evaluation of the cybersecurity risks and hardware specifications relevant to the scenario. This involves comparing alternatives and assessing cost-effectiveness. Logical reasoning and clear arguments should illustrate why each decision is suitable, ensuring a proportionate response to security risks.



Sound evaluation of the underlying concepts and principles of computer systems. The logical reasoning behind the hardware selection is strong, and the comparison and prioritisation of vulnerabilities based on severity and likelihood is well executed. However, the report would have been stronger if at least one alternative PC component had been compared, with justification for why the chosen option was more suitable. Using reasoning techniques such as risk versus impact assessment would further enhance the justifications provided. The report demonstrates a thoughtful and generally well-balanced approach

15.55

to mitigating security risks, incorporating both technical controls and organisational considerations.

PRACTICAL SKILLS

Practical application of theoretical knowledge is expected, with clear demonstrations of how hardware choices are suited to the given scenarios. Solutions should be realistic, feasible, and contextually appropriate, showing a direct link between theory and practical implementation.



Good application of a range of basic methods, materials, tools, and techniques, with very good consideration of the context of the application. The PC specification is strong and would realistically support the mentioned software. Additionally, the proposed cybersecurity solutions are practical and reflect realistic organisational practices. However, a total cost for the PC was not provided, which would be expected in real-world recommendations.

17.25

TRANSFERABLE SKILLS FOR LIFE

The report should display clear and professional communication, with high presentation quality, including well-organised sections, diagrams, and tables to convey technical information effectively. It should demonstrate the ability to complete tasks, reflecting readiness for professional practice, and emphasise clarity, accuracy, and fluency in technical writing.



The report is well-structured with good coherence, contributing to a solid overall presentation. The quality is commendable and demonstrates effective transferable skills. However, minor refinements could enhance the polish of the work.

6

Spelling and grammar require attention, and some sentences are overly long or confusing. Careful proofreading is recommended. Use of headings and bullet points should be more consistent to improve readability. Additionally, work on improving sentence structure, transitions between paragraphs, and alignment of text