

2420823 Charles H Cybersecurity and Computer System Design

by Charles H

Submission date: 10-Apr-2025 08:33PM (UTC+0100)

Submission ID: 255403663

File name:

59347_Charles_H_2420823_Charles_H_Cybersecurity_and_Computer_System_Design_659655_141485650.docx
(45.44K)

Word count: 3265

Character count: 18791

Cybersecurity and Computer System Design

By Charles H, 2420823

For **L4 – Computer System
Fundamentals (ACCA4028)**

Embedded Electronic Systems

Contents page:



Section/ Task 1: Planning a computer.

1.1: The use case of PC	Page 3
1.2: Table of PC components	Page 3
1.3: Choice behind components	Page 4

Section/ Task 2: Cybersecurity risk and strategy development

2.1: Scenario and identified risks.	Page 8
2.2: Employee cybersecurity training	Page 8
2.3: Firewalls	Page 8
2.4: Outdated firmware	Page 9
2.5: Default passwords	Page 9
2.6: External partners	Page 9
2.7: Incident response plan	Page 9

Section 1: Task 1: Building a computer.

Section 1.1: Use case for PC.



The computer below is designed for an electrical engineer who will be working from home. The system keeps a proficient level of cyber security and will be capable of running SolidWorks, Pspice and LabVIEW in a productive environment. The user will also be to enter video conferences. Every environment is different, and it should be considered whether there are other intentions of the system which may change the requirements and therefor components purchased before using the guide below.

When comparing the engineering software, SolidWorks was the most demanding for all aspects [1] [2] [3], so the system below meets the requirements for all listed software by meeting the requirements SolidWorks.

The SolidWorks website mentions that windows home edition is not supported [4], so the recommended OS is Windows 11 Professional, since Windows 10 is not supported from November 2025 [1] and other OS tend to have general compatibility issues.

The system used current generation components (as of March 2025) for more modern hardware utilising new features and longer lasting software support improving the cybersecurity of the system in later years when older hardware is unsupported.

Section 1.2: The System:



Component, Product and Prices (as of March 2025)	Specification
GPU: RTX 4000 Ada [5] [6] £1200	Connection: PCIe 4x16 Additional power connector: 12VHPWR Power draw: 130W Length: 245mm. Width: 112mm. Single slot card. Onboard memory: 20GB ECC GDDR6. 160-bit bus width. Display ports: 4x DisplayPort 1.4a
CPU: 9950x3d [7] £700	Socket: AM5. Power draw: 170W 16 cores, 32 Threads. Clock speeds: 4.3GHz base, 5.7GHz Turbo. Cache: 1280KB L1, 16MB L2, 128MB L3 cache. Supported memory: Up to 192GB and 5.6GHz without overclocking
Motherboard: ASRock Gaming x870 Riptide [8] [9] £250	Form factor: ATX. Socket: AM5. Chipset: X870 Memory: 4 channel DDR5 up to 256GB at 5.6GHz (8GHz with overclocking) PCIe Sockets: 1 PCIe 5x16, 1PCIe 4x16 operating in 4x4. 1 M.2 PCIe Gen 5x4 (2280)



	1 M.2 PCIe Gen 4x4 (2260/2280). 1 M.2 PCIe Gen 4x4 (2230/2260/2280). Header connections: 2x USB 2, 2x USB 3.2 Gen 1, 1x USB 3.2 Gen 2. Fan connections (4 pin with speed control): 1x AIO, 3x chassis, 2x CPU. Additional connectivity: 4x SATA 3 connections. Rear IO: 2x USB4 Type C, 2x USB 3.2 Gen 2, 3x USB 3.2 Gen 1, 4x USB 2, 1x RJ-45,
Memory: 2x Kingston Fury DDR5 6400 CL32. £200	Socket: DDR5 Capacity: 32GB CAS Latency: 32 cycles Supported frequency: 5.2/5.6/6/6.4/6.8 GHz
Storage: Samsung 9100 PRO 2TB [10] £250	Connection: M.2 PCIe 5x4 Onboard cache: 2GB Maximum read speed: 14.8GB/s Maximum write speed: 13.4 GB/s
CPU cooler: ARCTIC Liquid Freezer III [11] £75	360mm Radiator AM5 socket mounting bracket included. Connector: 4pin all in one or 3x 4pin (pump, VRM, Fans) Pump speed (PWM): 800-2800RPM Radiator Size: 398mm Length. 120mm Width. 38mm Height. Radiator fan speed: 200-1800RPM VRM fan speed (PWM): 400-2500RPM
PSU: SeaSonic VERTEX PX-1000. Invalid source specified. Invalid source specified. £250	ATX 160mm deep. Available power connections: 1x 16 pin / 12V-6X2. (Compatible with 12VHPWR) 1 x 24 pin – Motherboard. 2 x (4 +4) pin – CPU. 3 x 6+2 pin connectors. 4 x 4 SATA connections cables. 1 x 2 SATA 3.3V connections. 1 x 3 MOLEX connections.
Case: NZXT H5 Flow £100 [12]	Full ATX case. Mesh front panel. 225mm x 430mm x 465mm ATX PSU up to 200mm GPU max length: 410mm Fan Support: Front: 2x140mm / 360mm radiator support. Top: 2x 120/140mm Bottom: 2x120mm Rear: 1x120mm 2 120mm fans included Drive bays: 2x 2.5", 1x 3.5" Front IO: 1x USB C 20gbps, 1x USB 3.2, audio jack.
Monitor: Dell U2723QE [13] £300	27" Screen size. 3840 x 2160 Pixels (4K). 60Hz refresh rate. IPS Panel.

	1x HDMI, 1x Display port, 1x Display Port over USB-C with 90W Power delivery, 2x USB C 3.2, 5x USB A 3.2 gen 2, Audio line-out.
Keyboard and Mouse: Any USB mouse or keyboard ≈ £10 for basic set.	Connection: USB
Webcam: Adesso Cybertrack H5 [14] £35	Resolution: 1920 x 1080p at 30Hz. Connection: USB Auto-focus Privacy cover.
Microphone and speakers: ≈ £10	Pair of earphones using AUX which can be plugged in to the monitor chosen.
Total Cost: £3580 +	

Section 1.3: Choice behind components.

CPU:

Workstation CPUs were originally chosen for the system; however, SolidWorks mention that consumer level CPUs are just as effective. AMD was chosen over Intel because they support sockets for longer, allowing more modern upgrade choices later. Their x3d chips include more L3 cache which provides better multi-core performance.

GPU:

For reliable system stability the GPU should be on the certified list by SolidWorks [2]. A Nvidia GPU was chosen from their advantage in productivity over AMD as well as better support for hardware acceleration and AI. The RTX 4000 Ada [15] was chosen because of the 20GB of VRAM as 24GB or more is rarely going to be fully utilised by the software and the system RAM can also be used in exceptional circumstances.

AIO Cooler (All in one):

The AIO cooler was chosen as it takes heat directly away from the CPU to the edge of the case, which reduces the internal temperature of the case and reduces the temperature of the air cooling the GPU. By being a 360mm radiator it will ensure that the CPU will always be cooled sufficiently when running at its maximum.

Motherboard:

The motherboard needs to have the right CPU socket and have a good chipset for connectivity. The x870 chipset [9] has fewer PCIe lanes and USB ports than the flagship x870e chipset but still more than adequate. The chosen board [8] supports ECC memory if it was wanted in the future. The PCIe5x16 slot connects directly to the CPU. The board has both a 2.5Gb ethernet port and onboard WiFi 7 providing

options for the end user. There are 2 M.2 slots available with a third if the PCIe 4 slot is not used.

RAM:

SolidWorks recommends 64GB of RAM for heavy use. A professional engineer is likely to use more than 32GB and this also provides extra RAM that the GPU can use. The ram sticks chosen can operate at the maximum 5.6GHz without overclocking any components. The 32GBx2 configuration allows expansion if needed, while having the benefits of 2 sticks over one. The RAM is not ECC as it isn't in any recommended specs.

Storage:

M.2 SSDs was chosen for its better Read/Write speeds over SATA SSD's and HDD's. A large storage requirement is unlikely so 2TB should be plenty. There is the ability to expand it using the other M.2 slots and SATA ports. PCIe gen 5 read write speeds might not be utilised now over gen 4 however the latency improvement could be used in the future.

PSU:

A PSU should have an added 25% maximum power draw over the expected system rating to prevent overdemanding the component in power spikes. The VERTEX PX was selected as it is power efficient across a wide range and is good at keeping the voltage supplied within relatively small tolerances [16]. The expected power rating for the computer is 500W (+25% = 625W). If the GPU was swapped out the power draw could increase by 250W (750+25% = 925W). The series has a couple of different power ratings, 750, 850, 1000 and 1200W. If the system is unlikely to be upgraded, then a 750W PSU would be sufficient. The 1000W PSU is recommended as this provides the flexibility of upgrading the GPU and CPU without changing any other components for a small upfront cost.

Case:

The H5 flow has a mesh front for sufficient airflow to cool the system, with enough room for the rest of the components. It has cable routing options while not being too difficult to work in and not overly sized while giving 2.5" and 3.5" drive bay options.

Monitor:

An electrical engineer is unlikely to need great colour accuracy, local dimming or fast refresh rates from their monitor. Having a screen which can be seen in a wide range of environments and viewing angles will be more important, so an IPS [17] panel is preferred. The monitor chosen also has a broad range of connectivity, which can be more accessible on the monitor to users and allow the PC to be in awkward or suboptimal positions.

Keyboard and Mouse:

The keyboard and mouse chosen are basic ones which connect through USB and utilise the easy connection. The best options for end users are those which feel like an extension of the user and fit their personal use case increasing their productivity.

Webcam:

The webcam offers a USB connection, auto focus so it doesn't function as a distraction during meetings. The privacy filter gives the option for the user to use if preferred and can protect others within the user's environment. A 1080p and 30Hz camera was chosen as greater quality is likely not needed. Any presenting will likely be screen sharing.

Speaker/microphone:

The system does not include a microphone or speaker built in so a pair of earphones were chosen as a basic option which can be plugged into the monitor and provide privacy. It may be worth considering a better pair of headphones if meetings are more common, or separate speakers and microphones.

Task 2: Cybersecurity risk and strategy development

2.1: Overview

This section of the report is about the cybersecurity of a company which works in electronics manufacturing, where a recent audit found problems with their cybersecurity. Some of those include outdated firewalls, default passwords and outdated firmware, components sourced from international suppliers lacking their own cybersecurity, and employee cybersecurity training.

The risks are evaluated below detailing what they are, why they are a risk to the cybersecurity and possible mitigations to reduce the effect. Information on how common some types of attacks are can be found through the cyber security breaches survey, conducted yearly and published on the gov.uk website [18], which could be used as a guide to which defences should be prioritised when reviewing or creating cybersecurity measures. The risks are analysed in an order of priority based of the likelihood of an occurrence, and the damage that could be caused, however it may be different for other organisations if they operate differently.

2.2: Employee cybersecurity training

The strength of a systems security is up to as strong as the weakest point of vulnerability. People are very often one of the weakest points, and affect all types of organisations, including YouTube tech tip channels [19]. When they become comfortable and familiar with an environment where threats are not persistently visible, mistakes may happen. It could be opening files which are infected, bypassing security features previously installed, or leaving information in places they shouldn't be stored. It may also be providing physical access in person. A common reason is because it's easier for the user, where a 2024 survey found 65% of people bypass cybersecurity features [20]. If an effect is not swiftly realised of the action, it may become common occurrence. These incidents are likely to be very common and a high risk. Regular, up to date staff training on security processes and the reasons for them should decrease the chances of accidental weaknesses occurring within the organisation from human error.

2.3: Firewalls

Firewalls are a level of protection for incoming internet traffic into the system [21]. They control what information can pass, both incoming and outgoing, depending on rules determined by the administrator. Firewalls scan all data and decide whether it should be able to pass through or not. They can also prevent data from leaving a system, protecting data from being transferred outside of the system, acting as a preventative measure for data leaks. Firewalls also prevent other systems which do not meet its requirements to pass from communicating with the internal system. Harmful software is commonly transferred over the internet, through both untrusted

sources, but also compromised sources like emails from partners. A firewall forms one layer of a barrier to malicious files which are regularly encountered. It is important to regularly update them as malicious files are constantly changing to avoid detection.

2.4: Outdated firmware

Firmware is low level control of a system which act as an intermediate level between an operating system and the hardware [22] and is the first thing to start when a computer boots. Compromised firmware can be used to run harmful software first before the OS begins, going unnoticed by the rest of the computer. It can be used to introduce other vulnerabilities for different malware to utilise, bypassing other security features [23]. Although relatively uncommon, they pose an extremely large risk.

2.5: Default passwords

Default passwords often follow patterns, if not the same password when mass produced. That makes it much easier for hackers to gain access as they already have information required to narrow down the possibilities in a forced entry attempt by trying all possible combinations by brute force. By changing a set password, it prevents patterns from being used to gain access, massively increasing the possible combinations and helps limit control to only those who should have access to the system, especially if it's written on the access point. Password attacks are common, but this risk is also open to those who should not have access in person.

2.6: External partners

Sourcing components from external partners means they will hold data with regular communication between organisations. They may also have easier access to internal systems depending on whether access has been provided to them. If their cybersecurity is weak, they could provide an easier path for malicious actors into your system reducing your own cybersecurity, but also your data that they hold is vulnerable. Limiting their access to your system and any data shared reduces the possible effects of an attack via the external partners. These are unlikely, and if data management and access control is used, should have a small effect on the organisation.

2.7: Incident response plan (IRP):

An incident response plan is a pre-prepared decisions or actions which can be used to determine the next steps after an incident, while minimising the effect by acting swiftly. The stages of an IRP are the preparation, threat identification, containment and elimination, recovery, and improvements. [24]

The preparation of an IRP is not a make once and leave. It needs to be regularly reviewed and adapted if needed as an organisation grows and changes. A system change may mean that previously planned actions may no longer work as intended or activated in a unique way. Staff being familiar with the environment they need to work in increases confidence and in turn speed reducing knock on effects. If an attack is likely, it may be effective to increase the frequency of review periods and training.

The identification of a threat is required, because otherwise incidents would go unnoticed. Having network traffic monitoring software is one method of identification. Over time the network usage should follow regularly repeating patterns, and any major differences can trigger an alert to be investigated further.

Containment of a threat is needed to prevent the spread but also begin the elimination of it. If not contained, threats could continue to spread, and systems may not be able to eliminate them fast enough. They may also cause irreparable damage causing long lasting damaging effects. A method of containment is isolating systems to prevent further spread. This has a drawback of reducing the connectivity of the working system if applied too widely. Having a response plan which has separations already defined and how serious an incident needs to be before certain separations are triggered can help avoid shutting a system down too much.

After an incident has been eliminated. The event should be analysed, including how the threat originated, when it was identified and the effect of the current IRP in containment and elimination. All events should be analysed, no matter how small, as they can expose weaknesses which need improving, especially if they could be used again. It may also show that current review periods are not as often as they should if the organisation is in a period of rapid change.

A good response could also include informing staff with a brief overview of the event, and how it was managed. It could help staff identify possible threats in the future, helping to reduce the identification period, but also remind them about their role in keeping the organisation safe and improve the effectiveness of future staff training.

References

- [NI, "LabVIEW and Microsoft Windows Compatibility," NI, 27 01 2025. [Online].
1 Available: [https://www.ni.com/en/support/documentation/compatibility/17/labview-](https://www.ni.com/en/support/documentation/compatibility/17/labview-and-microsoft-windows-compatibility.html)
] [and-microsoft-windows-compatibility.html](https://www.ni.com/en/support/documentation/compatibility/17/labview-and-microsoft-windows-compatibility.html). [Accessed 31 01 2025].
- [Solidworks, "System Requirements," Solidworks, [Online]. Available:
2 <https://www.solidworks.com/support/system-requirements>. [Accessed 31 01
] 2025].
- [Cadence, "OrCAD X Installation Guide," Cadence, 2025. [Online]. Available:
3 <https://resources.pcb.cadence.com/blog/2025-client-orcad-x-installation>.
] [Accessed 10 04 2025].
- [Solidworks, "Solidworks Hardware Recommendations," Solidworks, 12 12 2023.
4 [Online]. Available: [https://www.solidx.co.uk/resources/post/solidworks-hardware-](https://www.solidx.co.uk/resources/post/solidworks-hardware-recommendations/)
] [recommendations/](https://www.solidx.co.uk/resources/post/solidworks-hardware-recommendations/). [Accessed 31 01 2025].
- [NVIDIA, "NVIDIA RTX 4000 SFF," NVIDIA, 2023. [Online]. Available:
5 [https://www.nvidia.com/content/dam/en-zz/Solutions/rtx-4000-sff/proviz-rtx-4000-](https://www.nvidia.com/content/dam/en-zz/Solutions/rtx-4000-sff/proviz-rtx-4000-sff-ada-datasheet-2616456-web.pdf)
] [sff-ada-datasheet-2616456-web.pdf](https://www.nvidia.com/content/dam/en-zz/Solutions/rtx-4000-sff/proviz-rtx-4000-sff-ada-datasheet-2616456-web.pdf). [Accessed 13 03 2025].
- ["NVIDIA RTX 4000 Ada Generation," Tech Power up, [Online]. Available:
6 <https://www.techpowerup.com/gpu-specs/rtx-4000-ada-generation.c4171>.
] [Accessed 13 03 2025].
- [AMD, "AMD Ryzen™ 9 9950X3D Gaming and Content Creation Processor,"
7 AMD, [Online]. Available:
] [https://www.amd.com/en/products/processors/desktops/ryzen/9000-series/amd-](https://www.amd.com/en/products/processors/desktops/ryzen/9000-series/amd-ryzen-9-9950x3d.html)
] [ryzen-9-9950x3d.html](https://www.amd.com/en/products/processors/desktops/ryzen/9000-series/amd-ryzen-9-9950x3d.html). [Accessed 13 03 2025].
- [Asrock, "PHANTOM GAMING X870 Riptide WiFi," Asrock, [Online]. Available:
8 [https://pg.asrock.com/MB/AMD/X870%20Riptide%20WiFi/index.asp#Specificatio](https://pg.asrock.com/MB/AMD/X870%20Riptide%20WiFi/index.asp#Specification)
] [n](https://pg.asrock.com/MB/AMD/X870%20Riptide%20WiFi/index.asp#Specification). [Accessed 10 02 2025].
- [AMD, "AMD Socket AM5 Chipsets," AMD, [Online]. Available:
9 <https://www.amd.com/en/products/processors/chipsets/am5.html>. [Accessed 10
] 02 2025].
- [Samsung, "Samsung Announces the 9100 PRO Series SSDs," Samsung, 25 02
1 2025. [Online]. Available: [https://news.samsung.com/us/samsung-announces-](https://news.samsung.com/us/samsung-announces-9100-pro-series-ssds-with-breakthrough-pcie-5-0-performance/)
0 [9100-pro-series-ssds-with-breakthrough-pcie-5-0-performance/](https://news.samsung.com/us/samsung-announces-9100-pro-series-ssds-with-breakthrough-pcie-5-0-performance/). [Accessed 10 03
] 2025].

- [Arctic, "Liquid Freezer III 360," Arctic, [Online]. Available:
1 <https://www.arctic.de/en/Liquid-Freezer-III-360/ACFRE00136A>. [Accessed 7 4
1 2025].
]
- ["H5 Flow," NZXT, [Online]. Available: Full ATX case. Mesh front panel.. [Accessed
1 10 04 2025].
2
]
- [Dell, "Dell UltraSharp 27 4K USB-C Hub Monitor - U2723QE," Dell, [Online].
1 Available: [https://www.dell.com/en-uk/shop/dell-ultrasharp-27-4k-usb-c-hub-
3 monitor-u2723qe/apd/210-bcxc/monitors-monitor-
\] accessories?msocid=339a177a212667ed248b025a202066b3](https://www.dell.com/en-uk/shop/dell-ultrasharp-27-4k-usb-c-hub-monitor-u2723qe/apd/210-bcxc/monitors-monitor-accessories?msocid=339a177a212667ed248b025a202066b3). [Accessed 12 03
2025].
- [Adesso, "CyberTrack H5," Adesso, [Online]. Available:
1 [https://www.adesso.com/products/1080p-hd-auto-focus-webcam-with-built-in-
4 dual-microphones-tripod-ready-clip-and-privacy-shutter/](https://www.adesso.com/products/1080p-hd-auto-focus-webcam-with-built-in-4-dual-microphones-tripod-ready-clip-and-privacy-shutter/). [Accessed 10 03 2025].
]
- [Nvidia, "RTX 4000 ada generation datasheet," Nvidia, 2023. [Online]. Available:
1 [https://resources.nvidia.com/en-us-briefcase-for-datasheets/rtx-4000-ada-
5 datasheet-1](https://resources.nvidia.com/en-us-briefcase-for-datasheets/rtx-4000-ada-datasheet-1). [Accessed 06 02 2025].
]
- ["Seasonic Vertex PX-1000," Cybenetics, 10 06 2024. [Online]. Available:
1 <https://www.cybenetics.com/evaluations/psus/2495/>. [Accessed 10 03 2025].
6
]
- [T. Singh, "IPS vs. VA vs. TN vs. OLED: Which gaming monitor to buy?," XDA, 23
1 11 2024. [Online]. Available: [https://www.xda-developers.com/ips-va-tn-oled-
7 gaming-monitor/](https://www.xda-developers.com/ips-va-tn-oled-gaming-monitor/). [Accessed 07 02 2025].
]
- ["Official Statistics: Cyber security breaches survey 2024," UK Government, 09 04
1 2024. [Online]. Available: [https://www.gov.uk/government/statistics/cyber-security-
8 breaches-survey-2024/cyber-security-breaches-survey-2024](https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024). [Accessed 09 04
] 2025].
- [J. Peters, "How hackers took over Linus Tech Tips," The Verge, 24 03 2023.
1 [Online]. Available: [https://www.theverge.com/2023/3/24/23654996/linus-tech-tips-
9 channel-hack-session-token-elon-musk-crypto-scam](https://www.theverge.com/2023/3/24/23654996/linus-tech-tips-9-channel-hack-session-token-elon-musk-crypto-scam). [Accessed 10 04 2025].
]

[Help Security, "65% of office workers bypass cybersecurity to boost productivity,"
2 Help Security, 4 12 2024. [Online]. Available:
0 [https://www.helpnetsecurity.com/2024/12/04/employees-privileged-access-](https://www.helpnetsecurity.com/2024/12/04/employees-privileged-access-security-risk/)
] [security-risk/](https://www.helpnetsecurity.com/2024/12/04/employees-privileged-access-security-risk/). [Accessed 09 04 2025].

[Cisco, "What is a firewall," Cisco, [Online]. Available:
2 <https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html>.
1 [Accessed 09 04 2025].
]

["Firmware," Wikipedia, 28 03 2025. [Online]. Available:
2 <https://en.wikipedia.org/wiki/Firmware>. [Accessed 04 09 2025].
2
]

[Keffer, "Firmware Attacks: How Do They Work and How to Protect Yourself,"
2 Techwalls, [Online]. Available: [https://www.techwalls.com/firmware-attacks-how-](https://www.techwalls.com/firmware-attacks-how-do-they-work-protect-yourself/)
3 [do-they-work-protect-yourself/](https://www.techwalls.com/firmware-attacks-how-do-they-work-protect-yourself/). [Accessed 04 09 2025].
]

[Microsoft, "What is incident response?," Microsoft, [Online]. Available:
2 [https://www.microsoft.com/en-gb/security/business/security-101/what-is-incident-](https://www.microsoft.com/en-gb/security/business/security-101/what-is-incident-response?ef_id=_k_683e4505bed51878fb3c22f0f53260d6_k_&OCID=AIDcmmao55x8o7_SEM__k_683e4505bed51878fb3c22f0f53260d6_k_&msclkid=683e4505bed51878fb3c22f0f53260d6)
4 [response?ef_id=_k_683e4505bed51878fb3c22f0f53260d6_k_&OCID=AIDcmmao](https://www.microsoft.com/en-gb/security/business/security-101/what-is-incident-response?ef_id=_k_683e4505bed51878fb3c22f0f53260d6_k_&OCID=AIDcmmao55x8o7_SEM__k_683e4505bed51878fb3c22f0f53260d6_k_&msclkid=683e4505bed51878fb3c22f0f53260d6)
] [55x8o7_SEM__k_683e4505bed51878fb3c22f0f53260d6_k_&msclkid=683e4505](https://www.microsoft.com/en-gb/security/business/security-101/what-is-incident-response?ef_id=_k_683e4505bed51878fb3c22f0f53260d6_k_&OCID=AIDcmmao55x8o7_SEM__k_683e4505bed51878fb3c22f0f53260d6_k_&msclkid=683e4505bed51878fb3c22f0f53260d6)
bed51878fb3c22f0f53260d6. [Accessed 08 04 2025].

["VERTEX PX ATX 3.1," Seasonic, [Online]. Available: [https://seasonic.com/vertex-](https://seasonic.com/vertex-2-px/)
2 [px/](https://seasonic.com/vertex-2-px/). [Accessed 10 03 2025].
5
]

2420823 Charles H Cybersecurity and Computer System Design

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

75/100

PAGE 1

PAGE 2



Comment 1

Good Work

PAGE 3



Comment 2

It is better to start with an introduction



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



Comment 4

It would have been better if a column is included for the cost

PAGE 4

PAGE 5



Comment 5

It would have been if the sub-headings are numbered

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10



Comment 6

It would have been better with a conclusion

PAGE 11

PAGE 12

PAGE 13

GRADING FORM: GRADING

CHARLES H

75

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 an extensive range of relevant and credible literature, and referencing is consistently accurate. In-text citations are generally well-integrated. However, some sources, like Wikipedia, are not suitable for academic work. It is recommended to refer to peer-reviewed journals instead.

7

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.



Excellent knowledge and understanding of the basic underlying concepts and principles of computer systems and cybersecurity. The report demonstrates a strong understanding of both PC component selection and cybersecurity principles. Hardware justification is detailed, and cybersecurity risks are clearly explained with

24

relevant examples. However, the work could be further improved by linking the analysis to specific cybersecurity frameworks.

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.



Excellent evaluation of the underlying concepts and principles of computer systems. Risks are logically prioritised based on likelihood and severity, and there is good reasoning behind the choice of hardware components. Evidence of critical thinking is shown in the discussion on risk reduction strategies. The work would be even better with the inclusion of a table or matrix to rank risks, and briefly discuss alternative components (e.g., Intel vs. AMD) to support the final selection. A good approach to mitigating security risks is demonstrated.

18.75

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.



A very good application of a range of taught, basic methods, materials, tools and techniques. The context of the application is well considered, and insightful. The practical skill is evident through the selection of components for the computer. The response would benefit from a clearer explanation of how component compatibility, The design would be better with potential future upgrades or system scalability, which is important for long-term usability.

19.45

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 displays a reasonable level of structure and coherence. The presentation is generally clear, contributing to a satisfactory overall quality. However, some areas would benefit from improved organisation and clarity. The report would be stronger with the inclusion of an introduction, a conclusion, adherence to the word count limit, and proper text alignment. Proofread carefully and tighten phrasing to stay within the word count. consider using bullet points or tables where appropriate.

5.8