

TM - Cybersecurity and Computer Systems Design Report

by Tamsin McKerrow

Submission date: 11-Apr-2025 02:14PM (UTC+0100)

Submission ID: 255505083

File name: 58656_Tamsin_McKerrow_TM_-
_Cybersecurity_and_Computer_Systems_Design_Report_659655_253176904.docx (3.25M)

Word count: 2992

Character count: 20491

APRIL 11, 2025

CYBERSECURITY AND COMPUTER SYSTEM DESIGN

COMPUTER SYSTEMS FUNDAMENTALS – ACCA4028

TAMSIN MCKERROW (2415958)
BEng Embedded Electronic Systems

Table of Contents

Table of Figures	2
Introduction	3
1: Computer System Design Specification	4
Requirements	4
Technical Specification	5
1.0. Motherboard	5
2.0.	5
3.0. RAM	5
4.0. Storage	5
5.0. I/O Ports	6
6.0. Graphics Card	6
7.0. Case	6
8.0. Power Supply	6
9.0. Network Connectivity	6
10.0. Peripheral Devices	6
11.0. Required Software	7
Shopping List	7
2: Cyber Security – Risks and Strategies	10
Cybersecurity Risks and Their Impact	10
Cybersecurity Mitigation Strategy	11
Incident Response Plan	12
Preparation	12
Threat Identification	12
Threat Containment	12
Threat Elimination	12
Recovery and Restoration	12
Feedback and Refinement	12
Conclusion	13
References	14

Table of Figures



Figure 1: Ryzen 7 7800X3D [7]	7
Figure 2: CPU Cooler [8]	7
Figure 3: ASUS PRIME B650M-A [9]	7
Figure 4: Crucial 64GB [10]	7
Figure 5: Kingston 1TB [11]	7
Figure 6: Asus DUAL EVO GeForce RTX4060 [12]	7
Figure 7: be quiet! Case [13]	8
Figure 8: 120mm Fan [14]	8
Figure 9: 140mm Fan [15]	8
Figure 10: Corsair RM750e [16]	8
Figure 11: VX2418C 24.0" [17]	8
Figure 12: Logitech MK345 [18]	8
Figure 13: JBL Headset [19]	8
Figure 14: Asus Webcam [20]	9
Figure 15: Ergonomic Mat [21]	9
Figure 16: Windows 11 Pro [22]	9

Introduction

This report details the setup of a custom-built desktop computer for a work-from-home environment. It is capable of running design and simulation software and other general business applications.

The second section examines cybersecurity risks and develops mitigation strategies and an incident response plan.

1: Computer System Design Specification

Requirements

An electrical engineer is transitioning to a work-from-home environment, and they require a robust desktop computer capable of handling the following engineering (e.g. design and simulation) tasks efficiently:

- **SolidWorks Electrical**
 - o x86_64 Processor
 - o >16GB RAM
 - o SSD Drive Recommended [1].
- **Pspice (integrated into OrCAD X)**
 - o 64-bit capable CPU chip.
 - o 8GB RAM
 - o Recommended 500GB free disk space.
 - o 1024x768 resolution
 - o Dedicated graphics card [2].
- **LabVIEW Software**
 - o Pentium 4G1 or later/equivalent (64-bit).
 - o 1024x768 resolution
 - o 5GB disk space
 - o 16-bit colour graphics [3].
- **MS365** (covering report writing, presentations, budget preparation, online video conference meetings and security software)
 - o Windows 10/11
 - o 4GB RAM
 - o 4GB free disk space
 - o 1280x768 resolution
 - o Graphics – Direct X9 or later, with WDDM [4].

Technical Specification

1.0. Motherboard

1.1. Asus PRIME B650M-A WIFI II

- 1.1.1. AM5 Socket – compatible with selected CPU, ensure to update BIOS with BIOS flashback button.
- 1.1.2. 4xDIMM max – 2 spare slots allowing for future memory upgrades.
- 1.1.3. 128GB Max Memory Supported – allowing for upgrades.
- 1.1.4. PCIe Graphics Card Interface – meets specs required for modern graphics card.

2.0. CPU

2.1. AMD Ryzen 7 7800X3D – compatible with selected motherboard

- 2.1.1. X3D ideal for CAD as helps with memory access.
- 2.1.2. Cheaper option compared to the latest AMD CPU as did not need this capability.

2.2. be quiet! Pure Rock Pro 3 59.6CFM CPU Cooler

- 2.2.1. 14-34.8dB

3.0. RAM

3.1. 16GB+8GB+4GB+4GB=32GB= RAM Requirement from Software

3.2. Roughly 30-40% of RAM is used to run just the Windows OS and other background processes [5].

3.3. Minimum 64GB of RAM needed.

- 3.3.1. $64\text{GB} \times 40\% = 25.6\text{GB}$ + $32\text{GB} = 57.6\text{GB}$ used if everything was running.

3.4. Crucial Pro Overclocking 64 GB (2x32 GB) DDR5-6400 CL40 Memory

- 3.4.1. Dual channel configuration uses both memory channels and doubles the bandwidth [6].
- 3.4.2. Alter the mega transfers from the JEDEC specification of 4800(MT) to the RAMs XMP profile (6400).

4.0. Storage

4.1. 500GB+5GB+4GB=509GB minimum free disk space.

4.2. Kingston NV3 1 TB SSD x2

- 4.2.1. To run in RAID1 as a backup in case one drive fails [7].

5.0. I/O Ports

5.1. Motherboard has:

5.1.1. 1xVGA, 1xHDMI, 1xDisplayPort, 1xPS/2, 4xUSB2.0, 4xUSB3.2, 1x2.5GB Ethernet, 3xAudioJacks

6.0. Graphics Card

6.1. Asus DUAL EVO OC GeForce RTX 4060 8 GB

- 6.1.1. Run wires directly to monitors using HDMI.
- 6.1.2. Supports up to 4 displays.
- 6.1.3. Ray tracing provides higher quality rendering.

7.0. Case

7.1. be quiet! PURE BASE 501 Airflow Window

- 7.1.1. Fits all components and is on the cheaper side.
- 7.1.2. Airflow for extra dissipation of heat.

7.2. 3x Case Fans to ensure components don't overheat.

- 7.2.1. Low decibels

8.0. Power Supply

8.1. 450W estimated.

8.2. Corsair RM750e 750W 80+ Gold Certified Fully Modular ATX

9.0. Network Connectivity

9.1. Motherboard has 2.5Gb Ethernet, WiFi6 – allowing for no network card.

10.0. Peripheral Devices

10.1. ViewSonic VX2418C 24.0" 1920x1080 Monitor.

- 10.1.1. x2 for ease-of-use.

10.2. Logitech MK345 Wireless Keyboard and Mouse & GOJI Mouse Mat

- 10.2.1. Ergonomic

10.3. JBL Quantum 100 – cheapest for comfort in long conference calls.

10.4. Asus Webcam C3

11.0. Required Software

11.1. CD Key for Windows 11 Pro Retail

11.1.1. Key more cost effective than download.

11.1.2. Pro version has more capabilities for business uses.

Shopping List

Component	Component Name	Specification	Price	Image
CPU	AMD Ryzen 7 7800X3D	4.2GHz, 8-Core	£369.00	 Figure 1: Ryzen 7 7800X3D [8]
CPU Cooler	be quiet! Pure Rock Pro 3	59.6CFM	£37.99	 Figure 2: CPU Cooler [9]
Motherboard	Asus PRIME B650M-A WIFI II	AM5	£129.98	 Figure 3: ASUS PRIME B650M-A [10]
Memory (RAM)	Crucial Pro Overclocking 64GB	2x32GB, DDR5-6400 CL40	£169.98	 Figure 4: Crucial 64GB [11]
Storage	Kingston NV3 1TB	M.2-2280 PCIe 4.0 X4 NVME SSD	£51.95 x2	 Figure 5: Kingston 1TB [12]
Graphics/Video Card	Asus DUAL EVO GeForce RTX 4060	8GB	£279.00	 Figure 6: Asus DUAL EVO GeForce RTX4060 [13]

Case	be quiet! Pure Base 501 Airflow	ATX Mid Tower Case	£89.99		Figure 7: be quiet! Case [14]
Case Fan	be quiet! Pure Wings 3	49.9CFM 120mm	£9.95 x3		Figure 8: 120mm Fan [15]
Case Fan	be quiet! Pure Wings 3	57.4CFM 140mm	£9.95		Figure 9: 140mm Fan [16]
Power Supply	Corsair RM750e (2023)	750W 80+ Gold Certified Fully Modular ATX	£89.99		Figure 10: Corsair RM750e [17]
Peripheral Devices	ViewSonic VX2418C 24.0"	1920x1080 165Hz	£89.97 x2		Figure 11: VX2418C 24.0" [18]
Peripheral Devices	Logitech MK345	Wireless	£29.99		Figure 12: Logitech MK345 [19]
Peripheral Devices	JBL Quantum 100	Headset	£18.74		Figure 13: JBL Headset [20]

Peripheral Devices	Asus Webcam C3	1080p 30fps	£32.04	 Figure 14: Asus Webcam [21]
Peripheral Devices	GOJI Ergonomic Mouse Mat	Non-Slip	£8.99	 Figure 15: Ergonomic Mat [22]
Software (Operating System)	Windows 11 Pro	Cd Key Retail	£8.63	 Figure 16: Windows 11 Pro [23]
TOTAL:			£1587.96	

PCPartpicker was used to determine compatibility between all components of the desktop computer [24]. A cheaper headset was picked than the one in the link and a Cd Key was found for Windows 11 Pro Retail as this is more cost-effective.

2: Cyber Security – Risks and Strategies

Cybersecurity Risks and Their Impact

Recent audits have identified several risks (and their impact) across areas of the company. These risks are prioritised based on their potential impact and likelihood before any mitigation steps are implemented (1=most impact):

1. Limited cyber security training among employees.

Having already resulted in occasional instances of phishing and social engineering attacks, it could lead to unauthorised access to sensitive information and systems.

Without proper training, employees pose a serious threat to the company as human error remains the weakest link in cybersecurity, 98% of cyber-attacks rely on social engineering, with phishing accounting for 70% all social engineering attacks [25]. This issue has a high likelihood and can have a serious impact on the company's operations and customer data.

2. Some devices used in the company have outdated firmware and default passwords.

Outdated firmware can have security gaps and can make the company susceptible to cyber-attacks and other risks including ransomware, data breaches, data loss, malware and IoT vulnerabilities [26]. Issues may also arise with new security technologies not being compatible, and regulations not being met [26].

This risk would have a significant impact on the company if exploited. Cyber-criminals can actively scan for vulnerable devices and exploit them using known vulnerabilities [27]. Default passwords are also easier for hackers to guess, meaning that it is more likely they will gain access to sensitive information they can use for ransom or to disrupt the system.

3. Company's network is vulnerable due to outdated firewall configurations.

This allows unauthorised access to the network and systems therefore increasing the risk of ransomware attacks and data theft, which could lead to loss of customer confidence. Outdated firewalls may be more likely to crash and need rebooting, leading to periods of decreased security [28].

Outdated firewall configurations still pose a huge risk to the company – e.g. Denial-of-Service and Distributed-Denial-of-Service attacks could lead to downtime and are very common.

4. Company sources components from international suppliers, some of which lack robust cyber security practices.

Increases the risk of introducing vulnerabilities into the manufacturing process, it could lead to supply chain threats such as ransomware attacks, security breaches, malware infection, process disruptions and intellectual property theft. Cybercriminals can also claim to be a

known retailer and request a change to the payment process – also known as supplier fraud [29].

Although this risk could halt manufacturing processes and possibly grant access to cybercriminals, when comparing it to the other risks identified, it is less likely to happen if nothing has been implemented to mitigate the above-mentioned risks.

Cybersecurity Mitigation Strategy

After security measures have been implemented the risks have been re-prioritised based on their potential impact and likelihood:

1. Company's network is vulnerable due to outdated firewall configurations.

- 1.1. Schedule Regular Updates and Patches – when firewalls reach their end-of-life ensure to upgrade to keep up-to-date with the latest security features [30].
- 1.2. Conduct Regular Security Audits – These can reveal any vulnerabilities, meaning the company can address these quickly [30].
- 1.3. Implement Network Segmentation – If a breach has occurred, it can contain the impact as it will limit how far the cybercriminal can penetrate [30].

Denial-of-Service and DDOS attacks are increasingly popular, on average, Microsoft mitigates 1700 DDOS attacks daily [31].

2. Limited cyber security training among employees.

- 2.1. Regular Cyber-Security Training – Including social engineering and phishing examples. Also, encourage employees to not write passwords down or share them.
- 2.2. Blocking Unsecured Websites.

Organisations with regular cyber-security training reduce phishing success by 60%, however human error is still responsible for 82% of data breaches [25].

3. Company sources components from international suppliers, some of which lack robust cyber security practices.

- 3.1. Third-Party Risk Assessments – Implement a regular third-party risk assessment schedule which will uncover third-party security risks before cyber criminals exploit them [29].
- 3.2. Data Encryption – This can be used to minimise the value of sensitive data in the event of a third-party breach [29].
- 3.3. Incident Response Planning – Responses should be designed for specific scenarios to minimise the impact on the company if an attack occurs. These responses should be updated and tested routinely [29].

4. Some devices used in the company have outdated firmware and default passwords.

- 4.1. Update All Firmware and Software – as soon as updates are released.
- 4.2. Install Anti-Virus Software – to constantly watch over and scan all devices and alert when there is a vulnerability [26]. And update the license yearly.
- 4.3. Reset All Default Passwords – to stronger ones and implement multi-factor authentication for employee sign-ins.

Incident Response Plan

Preparation

Recent audits have determined the risks and mitigation steps have been implemented for each of these. The risks have been re-prioritised based on their potential impact and likelihood, so the company's security team can monitor the weaknesses.

The company should also keep a backup copy of all data on a network attached storage that makes a backup once a day, so in the case of a ransomware or malware attack, they can restore data easily.

This stage of the response plan should regularly be visited to make improvements to policies, procedures, and systems as well as conduct updates when technologies change [32].

Threat Identification

Once an incident is identified the security team must investigate and document findings regarding the type of attack, the source of the breach, and the cybercriminals goals. The team must also inform any stakeholders/customers of the attack and communicate their planned next steps [32].

Threat Containment

The security team must then contain the threat swiftly, possibly by using the companies network segmentation, where it can limit how far the cybercriminal can penetrate. The team should isolate applications/systems that are under attack from the rest of the company's networks [32].

Threat Elimination

Once the attacker has been contained, the security team must remove the attacker and any malware or viruses from the affected systems and files. The team must also keep stakeholders/customers informed of the progress and if any information has been leaked [32].

Recovery and Restoration

Once the threat has been removed, the security team must restore systems, recover data from backup, and monitor the affected network/system/application to ensure the cybercriminal doesn't return – this step could take several hours.

Feedback and Refinement

Once the incident is concluded, the security team and other parties (privacy experts, lawyers and business decision makers) should review what happened, record ant lessons that have been learnt and identify any improvements that can be made to the company's defences [32].

Conclusion

The desktop computer setup could have been a little cheaper, but the components chosen allow for future upgrades and smooth running of all design, simulation, and other business applications. MS365 professional was a beneficial choice as it includes professional tools for report writing, presentations, budget preparation, as well as Microsoft Defender to protect against cybersecurity threats.

Following this, the risks to the company were evaluated and mitigation steps were executed. The risks were then reranked into which could be a weakness even with mitigation strategies in place. The incident response plan was very brief, and the company and security team should review this and create responses based on the company's weaknesses and for different types of attacks that may occur.

References

- [1] SOLIDWORKS, “SOLIDWORKS and SW Data Management System Requirements,” SolidWorks, [Online]. Available: <https://www.solidworks.com/support/system-requirements>. [Accessed 17 March 2025].
- [2] “Cadence Community,” CADENCE, 14 May 2013. [Online]. Available: https://community.cadence.com/cadence_technology_forums/pcb-design/f/pcb-design/26214/minimum-pc-requirements. [Accessed 07 04 2025].
- [3] NI, “LabVIEW 2022 Q3 and Drivers Readme,” July 2022. [Online]. Available: <https://www.ni.com/pdf/manuals/labview-2022-q3-and-drivers.html>. [Accessed 07 May 2025].
- [4] Microsoft, “Microsoft 365 Personal,” [Online]. Available: <https://www.microsoft.com/en-gb/microsoft-365/p/microsoft-365-personal/cfq7tte0k5bf#tab-requirements>. [Accessed 07 April 2025].
- [5] A. Khanse, “Why is my RAM usage so high when nothing is running?,” TheWindowsClub, 14 December 2022. [Online]. Available: <https://www.thewindowsclub.com/why-is-my-ram-usage-so-high-when-nothing-is-running>. [Accessed 10 April 2025].
- [6] A. Glawion, “How Much RAM (Memory) Do You Need? Different Workloads explored,” CGDIRECTOR, 22 November 2022. [Online]. Available: <https://www.cgdirector.com/how-much-ram-do-you-need/>. [Accessed 10 April 2025].
- [7] Prepressure, “RAID,” [Online]. Available: <https://www.prepressure.com/library/technology/raid>. [Accessed 11 April 2025].
- [8] Amazon, “AMD Ryzensets 7 7800X3D Processor with 3D V Cache technology (integrated Radeon Graphics, 8 cores/16 threads, 120W TDP, AM5 Socket, 104MB cache, up to 5.0 GHz max boost, no cooler),” [Online]. Available: <https://www.amazon.co.uk/dp/B0BTZB7F88?tag=pcp0f-21&linkCode=ogi&th=1>. [Accessed 11 April 2025].
- [9] OverClockersUK, “be quiet Pure Rock 3 PRO CPU Cooler - 120mm,” [Online]. Available: https://www.overclockers.co.uk/be-quiet-pure-rock-3-pro-cpu-cooler-120mm-coo-beq-04689.html?sv1=affiliate&sv_campaign_id=127079&awc=28821_1744216909_8156a4470c4bfd10dc8ca920ebb19e9e&utm_medium=affiliate&utm_source=PCPartPicker%20_127079_Communities+%26+UG. [Accessed 09 April 2025].
- [10] Amazon, “ASUS Prime B650M-A WiFi II AMD AM5 Micro-ATX Motherboard (DDR5, PCIe 5.0 M.2 support, 2.5Gb Ethernet, WiFi 6, DisplayPort, VGA, HDMI,

SATA 6 Gbps, USB 3.2 Gen 2 ports, BIOS FlashBack, Arua Sync),” [Online]. Available: <https://www.amazon.co.uk/dp/B0BSVDKRKN?tag=pcp0f-21&linkCode=ogi&th=1>. [Accessed 09 April 2025].

- [11] Amazon, “Crucial Pro DDR5 RAM 64GB Kit (2x32GB) 6400MHz CL40, Overclocking Gaming Memory, Intel XMP 3.0 / AMD EXPO, Computer Memory (PC), Black - CP2K32G64C40U5B,” [Online]. Available: <https://www.amazon.co.uk/dp/B0DSR14511?tag=pcp0f-21&linkCode=ogi&th=1>. [Accessed 09 April 2025].
- [12] OverClockersUK, “Kingston NV3 1TB PCI-e 4.0 NVMe M.2 Solid State Drive (SNV3S/1000G),” [Online]. Available: https://www.overclockers.co.uk/kingston-nv3-1tb-pcie-4.0-nvme-m.2-solid-state-drive-snv3s-1000g-sto-kng-02942.html?sv1=affiliate&sv_campaign_id=127079&awc=28821_1744217462_fea5c210d4cce98208351faca73675a8&utm_medium=affiliate&utm_source=PCPartPicker%20_12. [Accessed 09 April 2025].
- [13] Currys, “ASUS GeForce RTX 4060 8 GB Dual Evo OC Graphics Card - Black,” [Online]. Available: https://www.currys.co.uk/products/asus-geforce-rtx-4060-8-gb-dual-evo-oc-graphics-card-black-10268412.html?istCompanyId=bec25c7e-cbcd-460d-81d5-a25372d2e3d7&istFeedId=2f489429-2329-4fcd-941a-a6a497a10e1d&istItemId=qxprlrixr&istBid=t&sv1=affiliate&sv_campa. [Accessed 09 April 2025].
- [14] OverClockersUK, “be quiet! PURE BASE 501 Airflow Window Black,” [Online]. Available: https://www.overclockers.co.uk/be-quiet-pure-base-501-airflow-window-black-cas-beq-03816.html?sv1=affiliate&sv_campaign_id=127079&awc=28821_1744225794_05ee87b4d9855187978cd49aa54f02eb&utm_medium=affiliate&utm_source=PCPartPicker%20_127079_Communities+%26+. [Accessed 09 April 2025].
- [15] OverClockersUK, “be quiet Pure Wings 3 120mm PWM Fan,” [Online]. Available: https://www.overclockers.co.uk/be-quiet-pure-wings-3-120mm-pwm-fan-coo-beq-01128.html?sv1=affiliate&sv_campaign_id=127079&awc=28821_1744226832_fe4d526b3f597c8f6f1297bbc9365dcf&utm_medium=affiliate&utm_source=PCPartPicker%20_127079_Communities+%26+UGC. [Accessed 09 April 2025].
- [16] OverClockersUK, “be quiet Pure Wings 3 140mm PWM Fan,” [Online]. Available: https://www.overclockers.co.uk/be-quiet-pure-wings-3-140mm-pwm-fan-coo-beq-01131.html?sv1=affiliate&sv_campaign_id=127079&awc=28821_1744227027_1effa82e2ce431001d7f208b7b24874c&utm_medium=affiliate&utm_source=PCPartPicker%20_127079_Communities+%26+UGC. [Accessed 09 April 2025].
- [17] SCANs, “Corsair RMe Series 750 Watt Compact Fully Modular 80+ Gold PCIe5 PSU/Power Supply ATX3.0,” [Online]. Available:

- https://www.scan.co.uk/products/750w-corsair-rm750e-pcie-50-fully-modular-80plus-gold-single-rail-625a-120mm-rifle-bearing-fan-atx30?utm_source=pc%20part%20picker&utm_medium=referral. [Accessed 10 April 2025].
- [18] Laptops Direct, "ViewSonic VX2418C 24" VA Full HD 165Hz 1ms FreeSync Curved Gaming Monitor," [Online]. Available: https://www.laptopsdirect.co.uk/-/vx2418c/version.asp?utm_campaign=127079_PCPartPicker&utm_medium=affiliate&refsource=awin&sv1=affiliate&sv_campaign_id=127079&awc=74730_1744273165_dad68c13dd4ee72f045b7154cc8ffb66. [Accessed 10 April 2025].
- [19] Currys, "LOGITECH MK345 Wireless Keyboard & Mouse Set," [Online]. Available: <https://www.currys.co.uk/products/logitech-mk345-wireless-keyboard-and-mouse-set-10101117.html?istCompanyId=bec25c7e-cbcd-460d-81d5-a25372d2e3d7&istFeedId=2f489429-2329-4fcd-941a->. [Accessed 10 April 2025].
- [20] Currys, "JBL Quantum 100 Gaming Headset - Black," [Online]. Available: <https://www.currys.co.uk/products/jbl-quantum-100-gaming-headset-black-10214762.html>. [Accessed 10 April 2025].
- [21] Amazon, "ASUS Webcam C3 USB camera with 1080p 30 fps recording, beamforming microphone for better live-streaming video and audio quality, and adjustable clip that fits various devices," [Online]. Available: <https://www.amazon.co.uk/dp/B08QSMNM7N?tag=pcp0f-21&linkCode=ogi&th=1>. [Accessed 10 April 2025].
- [22] Currys, "GOJI Ergonomic Mouse Mat - Black," [Online]. Available: <https://www.currys.co.uk/products/goji-ergonomic-mouse-mat-black-10257706.html>. [Accessed 10 April 2025].
- [23] Gamers Outlet, "Windows 11 Pro Cd Key Retail Microsoft Global," [Online]. Available: <https://www.gamers-outlet.net/en/buy-windows-11-pro-cd-key-oem-microsoft-global>. [Accessed 10 April 2025].
- [24] PCPARTPICKER, "Part List," 08 April 2025. [Online]. Available: <https://uk.pcpartpicker.com/list/bWpkRV>. [Accessed 10 April 2025].
- [25] A. Belyh, "51 Social Engineering Statistics for 2025," Keevee, 10 February 2025. [Online]. Available: <https://www.kevee.com/social-engineering-statistics>. [Accessed 10 April 2025].
- [26] EASY2PATCH, "What are the Cybersecurity Risks Associated with Outdated Software and Operating Systems?," 24 May 2024. [Online]. Available: <https://www.easy2patch.com/blog/cybersecurity-risks-outdated-software-systems>. [Accessed 10 April 2025].

- [27] A. Barhate, "The Importance of Firmware Security and How Hackers Exploit Outdated Devices," 26 March 2025. [Online]. Available: <https://www.linkedin.com/pulse/importance-firmware-security-how-hackers-exploit-outdated-atish-b-v1a3f/>. [Accessed 10 April 2025].
- [28] OAC Technology , "What Are The Dangers of an Outdated Firewall?," 12 June 2024. [Online]. Available: <https://www.oactechnology.com/blog/dangers-outdated-firewall/>. [Accessed 10 April 2025].
- [29] E. Kost, "The Biggest Security Risks in Your Supply Chain in 2025," UpGuard, 08 January 2025. [Online]. Available: <https://www.upguard.com/blog/biggest-supply-chain-security-risks>. [Accessed 10 April 2025].
- [30] Kyber Security, "The Hidden Dangers of Outdated Firewalls: A Wake-Up Call for Small Businesses," 07 August 2024. [Online]. Available: <https://kybersecure.com/the-hidden-dangers-of-outdated-firewalls-a-wake-up-call-for-small-businesses/>. [Accessed 11 April 2025].
- [31] M. St.John, "Cybersecurity Stats: Facts And Figures You Should Know," Forbes, 28 August 2024. [Online]. Available: <https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/>. [Accessed 11 April 2025].
- [32] Microsoft, "What is incident response?," [Online]. Available: https://www.microsoft.com/en-gb/security/business/security-101/what-is-incident-response?ef_id=_k_54232516252f14cec55842eecfe88f51_k_&OCID=AIDcmmao55x8o7_SEM__k_54232516252f14cec55842eecfe88f51_k_&msslkid=54232516252f14cec55842eecfe88f51. [Accessed 11 April 2025].
- [33] Amazon, "AMD Ryzenets 7 7700X Processor (integrated Radeon Graphics, 8 cores/16 threads, 105W DTP, AM5 Socket, 40MB cache, up to 5.4 GHz max boost, no cooler)," [Online]. Available: <https://www.amazon.co.uk/dp/B0BBHHT8LY?tag=pcp0f-21&linkCode=ogi&th=1>. [Accessed 09 April 2025].

TM - Cybersecurity and Computer Systems Design Report

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

83/100

PAGE 1



Comment 1

Good work

PAGE 2



Comment 2

Good Work



Comment 3

It is better to number as 1.1, 1.2, 1.3 etc



Comment 4

it is better to number each heading

PAGE 3



Comment 5

Good Work

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

GRADING FORM: GRADING

TAMSIN MCKERROW

82.50

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, with consistently accurate referencing throughout. A wide range of recent and reliable sources has been used. However, the work would be further strengthened by incorporating more peer-reviewed journals

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.



Excellent knowledge and understanding of the basic underlying concepts and principles of cybersecurity and computer systems. The report

25.2

demonstrates a detailed understanding of hardware compatibility and alignment with the core principles of confidentiality, integrity, and availability. The work would be further improved by referencing specific cybersecurity standards

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. Risk prioritisation is logical and well-justified, with clear cost-justification and a thoughtful rationale for selecting 64GB of RAM. The work could be further strengthened by providing more detailed comparisons for components and including a risk matrix or visual summary of mitigation strategies. A good approach to mitigating security risks is demonstrated.

20

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. Practical skill is evident through the selection of computer components. The incident response plan is structured, but it could be further strengthened by including a simple workflow diagram or timeline to enhance clarity and visual impact.

21

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 exhibits a high level of structure and coherence. Presentation is clear, contributing to a very good overall quality. Demonstrates strong transferable skills for life and professional practice. Minor grammar and phrasing could be polished

8.3