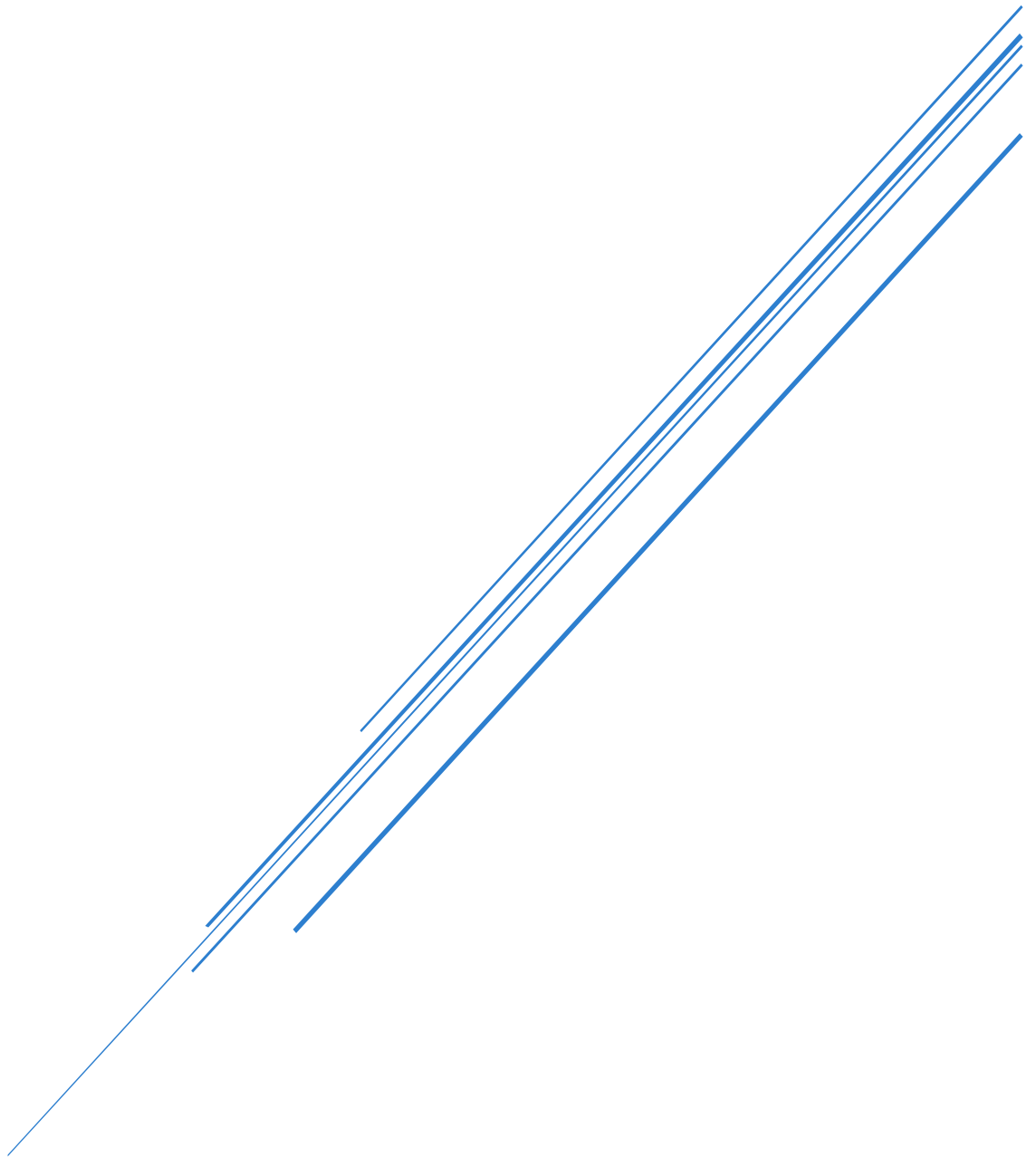


COMPUTER SYSTEMS & FUNDAMENTALS

Cyber Security and Computer System Design



Jacob C – 2420842 – Embedded Electronics
2420842@student.uwtsd.ac.uk

Contents

Task 1	2
Introduction	2
Components	2
Software	5
Task 2	5
Introduction	5
Vulnerabilities and Risks.....	5
Prevention and Mitigation Strategy	6
Incident Response	7
References	8

Task 1

Introduction

Task 1 details the components required to fit the requirements detailed in the scenario provided in the assignment brief, wherein an electrical engineer is required to work from home and requires a computer capable of running design and simulation software such as, SolidWorks, Pspice and LabVIEW, as well as generic word/spreadsheet processing for budget preparation.

In addition to this, the system should also be ready and capable for video conferencing and should also include a security system to protect against any potential cyber threats.

Components

The below table details the components utilised in the proposed system based on the requirements for SolidWorks 2025 [1]. This was used as the basis for the component list as SolidWorks was software with the greatest hardware requirements out of the specified software, and as such the other required programs would be able to run without issue.

Component, Product & Price (£) (Correct as of 04/2025)	Spec
CPU: Ryzen 7 7700x £299.04	8 core CPU, 16 Threads, base clock speed of 4.5Ghz, 32MB L3 Cache, x86-x64 architecture compatible.
CPU Cooler: Noctua NH-D15S Chromax Black CPU cooler £104.99	
GPU: Nvidia Quadro RTX 6000 £4569.99	24GB GDDR6 memory, up to 672GB/s Memory Bandwidth, PCI-E 3.0 x 16 connectivity, 4x Display port Output.
RAM: 2 x 32GB DDR5 Crucial Memory £224.99	64GB DDR5 memory clocked at 6000MHz
Motherboard: ROG STRIX B650E-F £209.99	Wi-Fi and Ethernet Enabled, Supports up to 128GB memory at 6400MHz, AM5 Motherboard, PCI-e 4.0 Expansion Slots, NVME and SATA Compatible
Power Supply: CORSAIR RM1000x 1000-Watt Gold PSU £179.99	1000W PSU rated at Gold Efficiency
Storage: Corsair MP700 1TB PCI-e 5.0 NVMe £125.99 Kingston FURY Renegade 4TB PCI-e 4.0 NVMe £359.99	Corsair Specs: Up to 10000MB/s read/write speeds, PCI-e 5.0 compatibility, 1,600,000 Hours mean time between failures, 1TB Capacity. Kingston Specs: Up to 7000MB/s read/write speeds, PCI-e 4.0 Compatibility, 2,000,000 Hours mean time between failures

I/O Devices: 7-Port PCI-Ex USB 3.0 Card £57.62	Supports an additional 7 USB Devices using USB 3.0
Network	Included with motherboard
Case: Silent ES Midi PC Tower Case with Sound Dampening, Black £40.72	Compatible with all current components, with space for cable routing and management, includes front I/O Ports
Peripherals: Mouse: Logitech MX Master 3S £79.99 Keyboard: Dell 091A682 KB216 USB QWERTY Keyboard £18.50 Webcam: Logitech C920s £69.99 Microphone: Hyper X Quadcast £79.99 Speakers: Logitech Z150 PC Speaker £26.99	
Monitor: LG Ultra-Wide Curved Monitor, 49 Inch, 5120 x 1440, 144Hz. £1,191.82	Ultrawide display to allow for a large screen real estate, featuring a high resolution and refresh rate.

Overall Total cost: £7,640.59

Due to the vagueness of the SolidWorks requirements, regarding the CPU Requirements, Pspice was used to establish a baseline requirement for the CPU required for the build [2]. These requirements identified a minimum requirement of a Ryzen 7 chipset with 4 cores, as such the 7700x was an ideal choice, surpassing the minimum requirements, ensuring a smooth user experience.

The CPU was then also paired with a large cooling unit, ensuring the CPU will remain cool and will continue to function under stress without worry of potential thermal throttling, due to the multitude of features provided by the unit [3].

The Ryzen CPU also benefits from faster and larger RAM units, as such 64GB of DDR5 RAM, clocked at 6000MHz was selected to be the ideal choice, as this quantity also fits within the required specifications outlined by the required software, whilst also providing a larger overhead for any larger simulations the user may perform. The GPU is a professional unit, featuring dedicated raytracing processors and many processing cores, enabling for faster rendering, shading processing and faster simulation than the previous units in the Quadro range [4].

Following this, a suitable motherboard is required, in which the Asus B650e-F satisfied the necessary requirements, providing suitable compatibility with the other components such as, providing the correct form factor for the RAM modules whilst also supporting the clock speeds of the modules, whilst also supporting the CPU form factor and providing the suitable base for the NVMe storage options to be installed. This motherboard also comes with both a built in Wi-Fi module and an Ethernet Port, saving the need for a network card [5].

Following this was the need for storage solutions, and such two NVMe modules were selected, the Corsair MP700 1TB, and the Kingston FURY Renegade 4TB, both of which providing a large amount of storage for the user whilst also providing fast read/write speeds, allowing for the user to maintain a rapid working environment without having to wait for hangups surrounding data speeds. The faster of the two being the Corsair MP700, boasting a read/write of 9500MB/s and 8500MB/s respectively [6], this module would typically used as a boot drive, allowing for a rapid start up process on boot, whilst also maintaining plenty of space for any updates and programs to be ran off of the main drive. The smaller drive, the Kingston FURY Renegade, boasts a much larger capacity, but at a lower read/write speed of 7300MB/s and 7000MB/s respectively, and is intended for the storage of any files and projects.

It is also necessary to source a power supply for the system, as such the Corsair RM1000x was selected. This unit is a 1000W supply, providing plenty of power for the system, whilst also providing plenty of an overhead for the system in the event of a future upgrade, saving costs in the future. The power supply is also rated at gold, meaning that PSU is capable of supplying more than 85% of the power taken from the mains supply to the system, without losing as much power to other elements such as noise and heat [7].

Suitable video conferencing equipment was also necessary, as such the Hyper X Quadcast was selected as a microphone, due to the microphone featuring a cardioid microphone pickup pattern, allowing for all noise from outside of the direction of the user in relation to the microphone to be cancelled out [8]. Logitech Z150 Speakers were chosen due to them being a cheap device with complimentary reviews, and the Logitech c920 was chosen due to the webcam being a high quality/low-cost webcam.

Finally, the monitor was chosen due to the size of the screen, providing a large working space for the user whilst also providing a sharp and high-quality image with a high response rate of 144Hz.

Software

The required software is as follows:

Software, and Cost (£)	Spec
OS: Windows 11 £119.99	
Antivirus: Malwarebytes Free or £285.20 p/y	An antivirus software providing a large suite of protection, including virus scanning, and incident response.
Microsoft Office Suite: £9.60 p/m	Includes Word, Excel, PowerPoint, Outlook
SolidWorks £2177.45 (after conversion from USD)	CAD Software
Pspice	Electronics Simulation and design Software

Task 2

Introduction

Task 2 details the evaluation of potential cybersecurity risks within an electronics manufacturing company and focuses on the strategies that could potentially be deployed in order to prevent a cyber-attack, or in the event of a breach, mitigate any potential damages to the company.

Vulnerabilities and Risks

Following an audit, the company has been identified to be lacking in several areas wherein a breach could occur.

One of the biggest vulnerabilities found within the company is that the company uses outdated firmware and firewall configurations, potentially leaving the company open to cyberattacks. These attacks could come in the form of phishing emails, network hacking, malware, or potentially through an internal threat.

An outdated firewall leaves a system vulnerable to any new threats that could have arisen since the last time the system was updated, leaving the system unable to recognise and flag up the threat [9].

The company has also found a number of devices to be using outdated firmware and using default passwords. Practices such as these could lead to breaches within the company, as using default passwords could lead to anyone gaining access to a user's account by guessing, or by having insider knowledge of how the company's password reset structure is handled. From these user accounts it would potentially be possible to gain access to confidential documentation, such as manufacturing processes or even prototype documents for products that have yet to be patented. Breaches such as these could also lead to the leaking of personnel data, which is covered under GDPR and could potentially lead to fines for the company [10].

The company has also been found to be lacking in regard to sufficient cyber security training, which has led to breaches within the company through both phishing and social engineering attacks. With proper training the frequency of these attacks being successful can be reduced, as the users will be made aware of the tricks and practices used by the cyber attackers, and as such can prevent any future attacks.

Finally, the most insignificant of the found security concerns was the companies use of international suppliers, some of which were found to be lacking in robust cyber security practices. This is less of a problem due to the fact that the external companies are only suppliers and would not be privy to the inner working of the company. These companies would be responsible for their own cyber security structures, however in cases such as this, it would be best to keep any information shared with external companies to a minimum.

Prevention and Mitigation Strategy

One of the best ways to prevent a cyber-attack is through training [11], as this can raise employee awareness of any potential threats, as the employees will be aware of the signs of a potential attack, such as the methods used in a social engineering attack or a phishing attack. And in the event of a breach, can be flagged to the necessary authorities within the company and handled in order to mitigate any potential damages that could have been incurred by the attack. Training should be carried out on a regular basis to ensure that all members of staff remain up to date on the procedures and practices to be carried out.

It is also important to maintain that all systems are kept up to date with the latest firmware in order to ensure the system is has countermeasures against as many known methods of attack as possible. Another method that can be deployed in this case is the use of an antivirus, such as Malwarebytes, as these antivirus software's can come packaged with countermeasures such as VPNs to encrypt browser traffic [12], preventing a hack from an insecure internet connection. These anti-virus software's also sometimes come packaged with virus scanning utilities, enabling users to ensure that they do not have a virus on their computer already which could potentially have gotten past the firewall.

Incident Response

Prior to an incident a series of steps can be taken in order to ensure that in the event, the necessary procedures can be followed to handle everything smoothly and promptly, whilst also mitigating any damages to the company. These steps are as follows:

- Ensure proper communication channels are present, and ensure all staff remain trained on the escalation procedures and protocol, and regular system backups are kept.
- Verify the threat, assess whether the attack was a cyber attack or not and evaluate the severity of the situation.
- Contain the impact of the incident and isolate the affected systems from the network to prevent further breaches.
- Investigate the threat and clean it from the system, ensuring no trace of the attack remains.
- Roll back any affected systems to a previous backup to get business operating.
- Learn from the incident and ensure that in the event that staff were responsible for the incident that they are properly educated on the preventative procedures.
- Reevaluate the security systems currently in place and strengthen the existing system to prevent a similar attack from taking place.

By following these steps, a proper cyber security system can be put in place and maintained, ensuring that all data remains secure.

References

- [1] SolidWorks, "Solidworks and SW Data Management System Requirements," 2025. [Online]. Available: <https://www.solidworks.com/support/system-requirements#hwhyper>.
- [2] Cadence Design, "ORCAD X System Requirements," Cadence Design, 2025. [Online]. Available: <https://resources.pcb.cadence.com/blog/2024-orkad-x-software-requirements>. [Accessed 10 04 2025].
- [3] Noctua, "Noctua NH-D15s chromax.black," noctua, 2025. [Online]. Available: <https://noctua.at/en/nh-d15s-chromax-black>. [Accessed 10 04 2025].
- [4] NVIDIA, "The worlds first ray tracing gpu - NVIDIA Quadro RTX 6000," NVIDIA, 2025. [Online]. Available: <https://www.nvidia.com/content/dam/en-zz/Solutions/design-visualization/quadro-product-literature/quadro-rtx-6000-us-nvidia-704093-r4-web.pdf>. [Accessed 10 04 2025].
- [5] ASUS, "ROG STRIX B650E-F GAMING WIFI," ASUSTek, Taipei City, 2022.
- [6] Corsair, "MP700 1TB PCIe 5.0 (Gen 5) x4 NVMe M.2 SSD," Corsair, [Online]. Available: https://www.corsair.com/uk/en/p/data-storage/cssd-f1000gbmp700r2/mp700-1tb-pcie-5-0-gen-5-x4-nvme-m-2-ssd-cssd-f1000gbmp700r2?srsltid=AfmBOop08vAPGf8_HuZc3siTFtmg-HOPShRfAD_nxcPSxuE-ySmHYZF3#tab-techspecs. [Accessed 10 04 2025].
- [7] Corsair, "PSU: Efficiency Ratings Explained," Corsair, [Online]. Available: <https://help.corsair.com/hc/en-us/articles/14641912717453-PSU-Efficiency-Ratings-Explained>. [Accessed 10 04 2025].
- [8] Kingston, "HyperX QuadCast Microphone Manual," Kingston.
- [9] OAC Technology, "What are the dangers of an outdated firewall," OAC Technology, 12 06 2024. [Online]. Available: <https://www.oactechnology.com/blog/dangers-outdated-firewall/#:~:text=Outdated%20firewalls%20can%20allow%20various,that%20should%20have%20been%20blocked..> [Accessed 10 04 2025].
- [10] European Union, "Regulations," *Official Journal of the European Union*, 2018.
]
- [11] T. Murray, "Why training is the best defence against cybersecurity and data threats," Thomas Murray, [Online]. Available: <https://thomasmurray.com/training-employees-cyber-security>. [Accessed 10 04 2025].
- [12] Malwarebytes, "Malwarebytes," Malwarebytes, [Online]. Available: <https://www.malwarebytes.com>. [Accessed 10 04 2025].