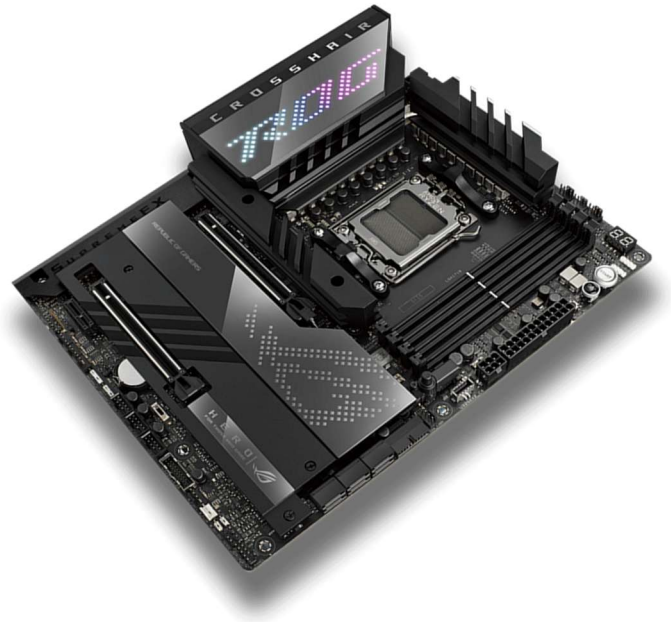

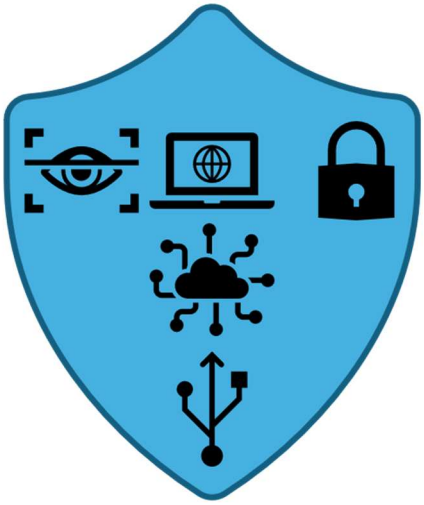

COMPUTER SYSTEM FUNDEMENTALS

ACCA4028

Jamie Hamilton-Swingewood
2308342@student.uwtsd.ac.uk

Table of Contents

Task 1: Custom Desktop 2

Robust Setup for an Electrical Engineer 2

The Big Three: CPU, Motherboard, and GPU 3

CPU: AMD Ryzen 9 7950X 3

Motherboard: ASUS ROG Strix X670E-F. 4

GPU: RTX 5080 5

Completing the Setup 5

Task 2: Bespoke Cybersecurity solution. 7

Risks and Assessment of Impact 7

Risk 1: The company's network is vulnerable due to outdated firewall configurations. 7

Risk 2: Devices used in the production facility have outdated firmware and default passwords. 7

Risk 3: Insecure Supply Chain 8

Risk 4: Limited cybersecurity training among employees 8

Required Steps for Cybersecurity Hardening 9

Risk 1 Mitigation: General Network Overhaul 9

Risk 2 Mitigation: Password and Patch Management 9

Risk 3 Mitigation: Establishing Robust Supplier Checks 9

Risk 4 Mitigation: Personnel and Training 9

Risk Matrix After Mitigation 10

Conclusion 10

Bibliography 11

Task 1: Custom Desktop

Robust Setup for an Electrical Engineer

Building and collecting the required components for a high-performance custom workstation computer has become much easier than it once was, gone are the days of few available components, hard to work with cases, and forests of the now antiquated "ketchup and mustard" cables. The decade of the 2010s to 2020s saw monumental leaps in digital technology with AI and "big data" taking off, industries and individuals spending more time on social media and significant advancements in hardware enabling greater efficiency in the workforce.[1] For an electrical engineer this means that a high performance workstation can be neatly tucked under a desk at home. In this exercise specifications for such a machine and the reasons for choosing each part will be detailed.

The big three parts that determine the performance of a modern ATX style PCs are the CPU (or central processing), the GPU (graphics processing unit) and the motherboard (to a lesser extent RAM above 16GB) influence the overall performance. Settling on a CPU is the most important as it will then in turn limit what motherboards that will be available. Each manufacturer generally having, budget, mid-range, and performance/enthusiast level equipment to suit an individual's or company's specific needs. From the top an electrical engineering company would generally buy enterprise or professional grade workstations from the likes of Dell, HP, or similar instead of buying the individual parts, often for uniformity, warranties and simplicity. A quick analysis of typical workstations these companies have to offer will be a good starting point to comparably spec the custom PC for the required task.[2]

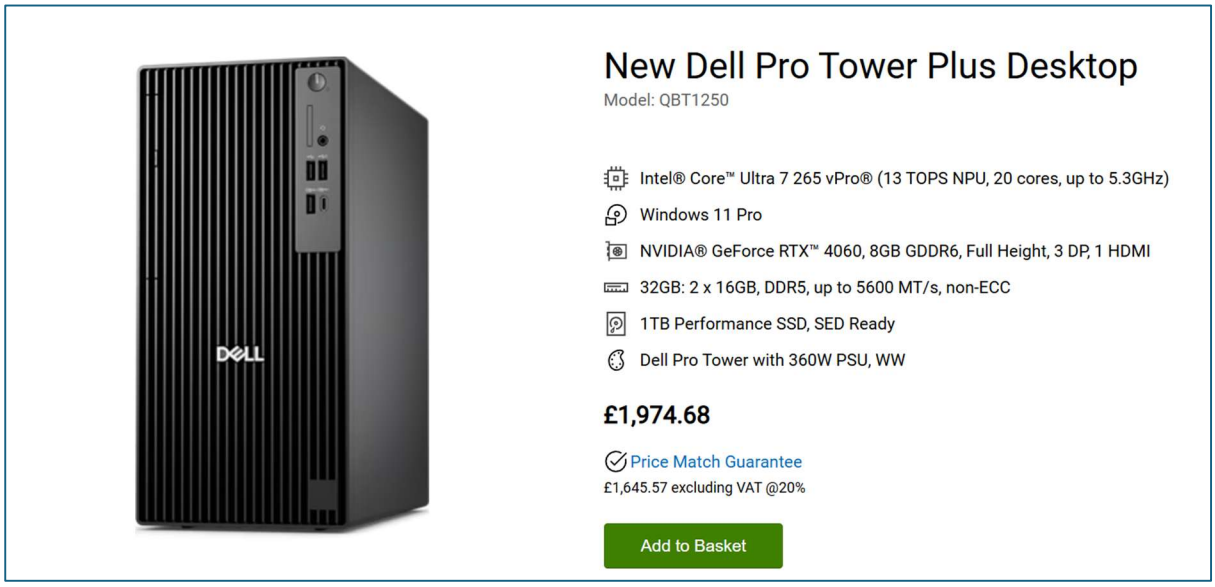

Figure 1: A professional grade workstation desktop taken from the DELL website, from this the specifications and budget are used as a guide.[2]

From the Dell website a comfortable system costs around £2000, So that will be the rough upper limit for the parts of the PC with another £2000 allotted for peripherals like a keyboard, monitor and so on, with an all in work from home set up price of approximately £4000.

The Big Three: CPU, Motherboard, and GPU

CPU: AMD Ryzen 9 7950X

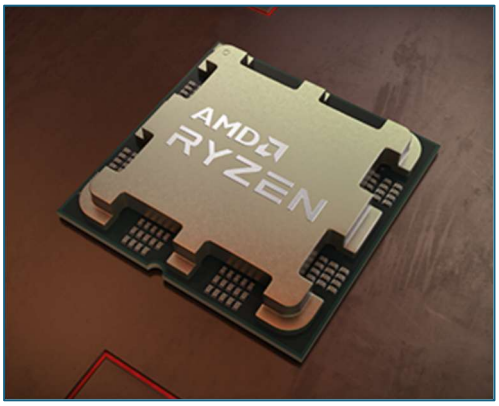

Figure 2: AMD Ryzen 9 7950X [4]

Being literally the centre of processing tasks it is crucial for engineering applications typical of what an electrical engineer will require namely running commercial software, simulations, calculations, and compiling code, robust high core count CPU is required and the 7950X delivers.

Key Features:

- On AMDs latest AM5 platform with ZEN4 Architecture supporting PCIe gen 5.0.
- 16 Cores and 32 Threads, Ideal headroom for continuing normal use while working with situations that are demanding multithreaded workloads such as parallel simulations in Pspice.
- High base and boost clock performance of 4.5GHz to 5.7 GHz respectively. The high base clock and greater boost clock frequencies available to the 7950X can handle single-thread demanding tasks like simulating in Proteus, ABAQUS or SolidWorks Electrical. With fast single threaded performance being conducive to a fast and responsive system as a whole.[3]
- Overall, the 7950X provides the speed and raw computational power required for running complex simulations or specialist software expected to be used by an electrical engineer. Whilst not sacrificing functionality for a more general PC use such as word processing or conferencing, albeit at a premium price point exceeding £400[4].

With runner up:

- Intel Core i9- 13900K or 14900K
    - With intel not being chosen due to the 13th/14th generation CPUs being plagued with system destroying stability issues. Causing industry wide loss of faith in intel's products, recalls and billions of USD lost, resulting in a 70% drop in share price from all-time high in 2021.[5]

Motherboard: ASUS ROG Strix X670E-F.

Figure 3: ASUS ROG Strix X670E-F [6]

This is a high-end motherboard supporting the AM5 platform, with expanded slots for greater compatibility and flexibility in terms of components that can be hosted on any single device. Supporting the AM5 platform means there is scope for upgradeability down the line as AMD is famous for releasing new CPUs across multiple generations as seen with new AM4 CPUs. This in effect means that a new lease of life could be brought to this machine in a couple of generations time without having the expense of having to replace the entire computer.

Key factors:

- PCIe Gen 5 support, as of 2025 this is the latest standard of PCI Express and represents a doubling of speed over its predecessor allowing for bandwidth speed per lane to be 4GB/s with an aggregate bandwidth of 64GB/s on typical x16 lane devices. With two of the four M.2 SSD x4 and both PCIe x16 expansion slots supporting the Gen 5 standard.
- Requiring DDR5 RAM with an upper limit of 128GB and support for extreme memory profiles (XMP). XMP being motherboard specific and enabling the default 4800MT/s to be overclocked beyond 6000MT/s.
- Lage number of I/O, multiple USB A, USB C, HDMI, Network RJ45, PCIe and SSD ports, in addition to inbuilt Bluetooth and Wi-Fi 6E. Enabling the connection of a large array of peripherals in addition to future upgrades and storage with ease.
- Price: £314.99[6]

With similar products being around the same £300-350 price range from comparable manufactures such as ASRock, MSI and Gigabyte offering much the same features and functionality at this price point. Slightly newer X870 chipset motherboards are now available but come with potential instability issues due to being brand new to market.

GPU: RTX 5080

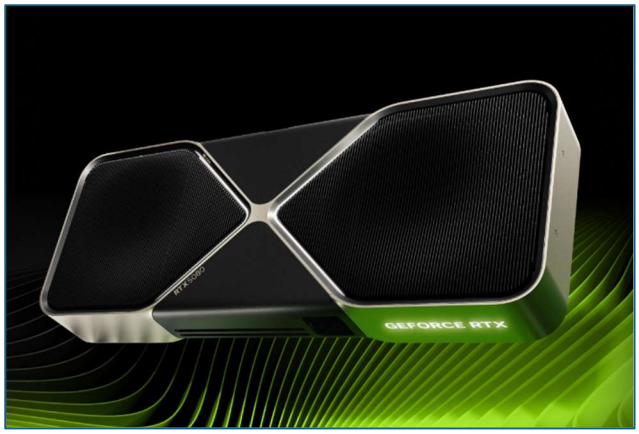

Figure 4: Nvidia GeForce RTX 5080 [7]

The Nvidia RTX 5080 was released in January 2025 for $999, it is built on the new Blackwell architecture and has 10752 CUDA cores and 16GB of DDR7 memory. Whilst definitely high end, the 5080 is a compromise in price for performance against ISV certified parts like the Quadro or RTX Pro series of GPUs offered, with the Quadro RTX 6000 24GB coming in at around £3000 for a single unit.

- Performance for 3D CAD and simulations will be excellent, being a gaming class GPU the 5080 will make light work of demanding 3D rendering tasks. The 10,000 CUDA cores and high 960GB/s bandwidth means the 5080 can take advantage of GPU hardware acceleration in high computational workloads found in simulation software. With many software produces such as Ansys and solid work providing direct support for this.
- Good driver support, within NVidia's ecosystem on windows. Wrapped into a single desktop application it is easy to stay on top of stability and security updates for the hardware. This support includes the ability to build GPU-accelerated simulations and even small AI or machine learning models through NVidia's CUDA support.
- Support for Display port 2.1 (and HDMI 2.1) which enables the GPU to output to multiple 4K resolution monitors, essential for multitasking a workflow such as reporting on a simulation.

The RTX 5080 offers very good high-end performance, efficient power usage, within a reasonable cost of less than half the price of the RTX5090 or QRTX6000. AMD have a very strong gaming GPUs at less than $800 however NVidia's CUDA cores and hardware acceleration make them the more suitable pick for use in a workstation/productivity setting.[7]

Completing the Setup

Given the CPU, Motherboard and GPU have been chosen the rest of the parts fall into place. In a modern system running windows 11, the minimum recommended amount of system RAM is 16GB. This is generally found in budget to midrange laptops, the task requires a system for performance and productivity, thus a sensible amount is 64GB of DDR5 RAM. This will allow for smooth running of the operating system with a large headroom for running multiple programmes or processes in parallel without affecting performance.

Whilst manufacturer and style of RAM is less of a pressing issue than it would be for a GPU or CPU going with reputable, well-established brands is best. For this system Corsair Vengeance DDR5 64GB (2x32GB) DRAM 5600MT/s CL40, will be used, costing £162.99.[8]

The remainder of the parts are as below:

Component	Selection	Price
CPU	AMD Ryzen 9 7950X 4.5 GHz 16-Core Processor	£408.26
CPU Cooler	Thermalright Peerless Assassin 120 SE 66.17 CFM CPU Cooler	£29.99
Motherboard	Asus ROG STRIX X670E-F GAMING WIFI ATX AM5 Motherboard	£297.52
Memory	Corsair Vengeance 64 GB (2 x 32 GB) DDR5-5200 CL40 Memory	£136.97
Storage	Crucial T705 2 TB M.2-2280 PCIe 5.0 X4 NVME Solid State Drive	£186.95
Storage	PNY CS2150 1 TB M.2-2280 PCIe 5.0 X4 NVME Solid State Drive	£103.29
Video Card	Zotac GAMING SOLID CORE GeForce RTX 5080 16 GB Video Card	£985.47
Case	Fractal Design Pop XL Silent ATX Full Tower Case	£89.99
Power Supply	Silverstone Strider Titanium 1300 W 80+ Titanium Certified Fully Modular ATX Power Supply	£299.99
Operating System	Microsoft Windows 11 Pro Retail - Download 64-bit	£181.97
Case Fan	Thermalright TL-C12C X3 66.17 CFM 120 mm Fans 3-Pack	£12.00
Monitor	Samsung Odyssey OLED G8 32.0" 3840 x 2160 240 Hz Monitor	£898.99
Monitor	Samsung Odyssey G55C 32.0" 2560 x 1440 165 Hz Curved Monitor	£178.77
Keyboard	Logitech MK540 ADVANCED Wireless/Wired Standard Keyboard With Optical Mouse	£34.99
Headphones	JVC HARX900 Headphones	£50.37
Webcam	Anker PowerConf C200 Webcam	£59.99
Base Total:		£3,944.54
Shipping:		£10.97
Total:		£3,955.51

Figure 5: Table of full parts list, power budget and price, with images and compatibility charts available at https://uk.pcpartpicker.com/list/hgWpWc . For the most part peripherals like keyboard, mouse, camera; components like power supplies, RAM, SSDs, fans and cases are relatively interchangeable providing they are suitably rated for the required size and power requirements. Here the sensible Logitech keyboard and mouse combo will be easy to use while the 4k and 2K Samsung monitors make use of the systems high graphical performance with the Anker webcam able to stream video at 2K resolution. Some stated prices may vary due to availability and demand.

Last but not least is security software, for this build going with specialist business software is to be expected. So going with ESET Small Business Security enables proactive security features against common online threats with the addition of enterprise grade aftercare for any required support, costing £164.99 for a year on 5 devices. This brings the total cost to £4120.50.

Task 2: Bespoke Cybersecurity solution.

The following is a report for the company outlining the cybersecurity risks found, a risk assessment, the negative impact these risks could cause and finally an action plan for a holistic cybersecurity overhaul to be implemented. Due to the complex and connected production and supply chains involving business sensitive intellectual property, with the goal of this report to ensure operational continuity of the business by hardening the physical, software and personnel cybersecurity defences.

Risks and Assessment of Impact

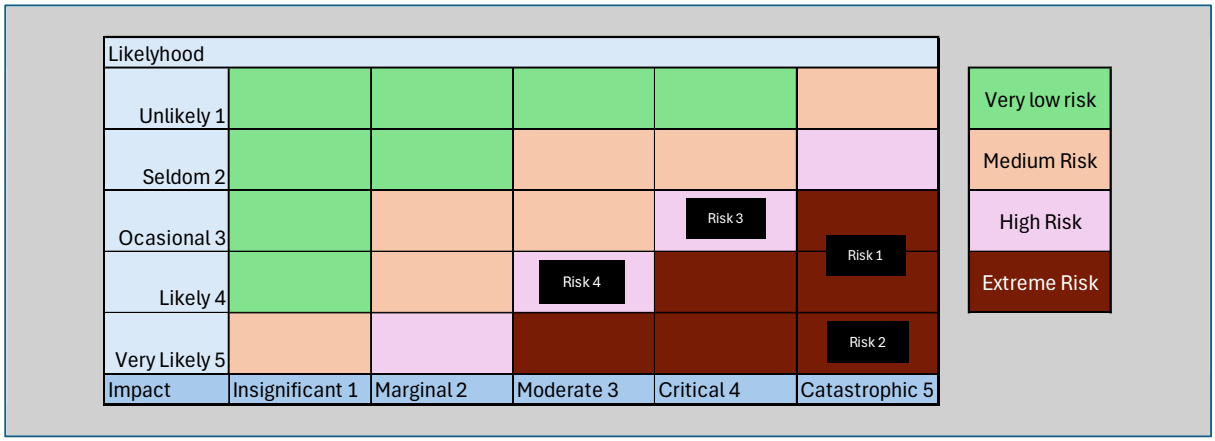

Figure 6: Risk assessment matrix for risks 1-4, detailed breakdown to follow but anything in the pink or red is totally unacceptable to remain unaddressed. With correct mitigation protocols in place the risk will be reduced to acceptable levels, the four pillars to manage cybersecurity risks are, Avoidance, Acceptance, Transfer and Treatment of risk.[9]

Risk 1: The company's network is vulnerable due to outdated firewall configurations.

Outdated firewall configurations and open ports propose a real threat with unauthorised access to the company's internal systems. This is compounded by the risk of lateral movement of a threat actor once the network is penetrated allowing for further access to sensitive business information such as intellectual property, schematics/designs, staff and customer data. The exfiltration of this data will cause reputational damage and open the company up to legal and potentially criminal proceedings particularly with the mismanagement of GDPR/protected information in the -Data Protection Act 2018.[10,11]

Evaluation of risk 1, the impact is catastrophic 5 and the likelihood is occasional/high, 3-4. Overall Risk = Extreme Risk, steps must be taken to mitigate immediately.

Risk 2: Devices used in the production facility have outdated firmware and default passwords.

Outdated firmware and default passwords leave the company open to sabotage either through intentional actions or through the propagation of malware throughout the production system. Criminal actors could readily hold the production line hostage in lieu of payment or other types

of malware could cause downtime in production as engineering systems go offline with the potential risk to staff as automatic safety measures could be overwritten, or entire production systems could be taken over by remote accesses tools. Lost production through downtime in any meaningful volume will economically cripple the organisation with the average cost per ransomware attack being in the region of £1.5Million per incident compounded by the reputational harm and loss of customer trust that would be caused.[12]

Evaluation of risk 2 = Catastrophic impact and highly likely.
Overall Risk = Extreme Risk, steps must be taken to mitigate immediately.

Risk 3: Insecure Supply Chain

An insecure supply chain poses as a unique threat due to the unavoidability of sourcing certain components and the lack of control one has over such items before they arrive at the company. This means that measures can be taken from the point of integration to the company network, but as these suppliers may lack stringent cybersecurity measures or infrastructure potential vulnerabilities can be introduced. Common weak points are through counterfeit components, outdated and or compromised firmware or hostile embedded backdoors. These weak points can undermine the integrity of the security of the entire manufacturing process and once embedded in a production system are difficult to rectify. Supply chain vulnerabilities can occur digitally or physically, such as malicious code incorporated into software or malicious software embedded on trusted hardware like microchips respectively. [13] An interesting case study into compromised supply lines are the pager explosion of 2024 and highlight the difficulty of counteracting a threat, physical or cyber once a supply line is compromised.[14]

Evaluation of risk = Critical impact and occasional likelihood.
Overall risk = High Risk, steps must be taken to mitigate.

Risk 4: Limited cybersecurity training among employees

Personnel training and security is often overlooked as a large number of major cybersecurity breaches are able to take place as threat actors have social engineered their way onto privileged accounts or systems. Without sufficient training employees will be less resilient to human based exploits such as, phishing or the classic confidence man (con man) social engineering techniques. Left under skilled a workforce is easy prey for manipulation attacks that lead to the compromise of sensitive systems, credential theft and accidental installation of malicious software.[15] Employees have privileged accesses to systems at all levels of an organisation compared to an outsider, even a non-technical member of staff with access to only a surface level intranet or company email could have that bit of privilege taken advantage of. A threat actor could hijack an internal email account via a phishing attack as all members of staff will be more trusting of an email coming from within the organisation this could easily be exploited to further penetrate into the company's more sensitive assets.

Evaluation of Risk= moderate impact, Likely occurrence.
Overall Risk= High Risk, steps must be taken to mitigate.

Required Steps for Cybersecurity Hardening.

Risk 1 Mitigation: General Network Overhaul

To strengthen firewalls and network security the company must:

- Update existing firewalls and close unnecessary ports.
- Implement a zero-trust model enforcing strict access controls to systems and information.
- integrate an intrusion detection and prevention system alongside firewalls to help detect anomalous and suspicious network activity.
- Ring fence areas of the network that host different business environments. By separating the networks a breach in the administrative network for example will not compromise the entire infrastructure, at least not immediately, giving much needed triage and reaction time.

Risk 2 Mitigation: Password and Patch Management

To secure devices on the production line the company should implement a structured internal process to manage the regular rollout of updates to machinery and a password manager.
- Default passwords must be changed with strong passwords and managed through a password manager.
- If and where possible implement multi-factor authentication not just on production devises but throughout the company.
- Have a system for patch management of production machinery with multiple responsible personnel to ensure continuity.
- Deploy continuous monitoring tools for a real time overview of production devices and allow threat monitoring.

These actions will help prevent exploitation of easily preventable vulnerabilities and more generally protect the operational and production continuity of the company.

Risk 3 Mitigation: Establishing Robust Supplier Checks

The company should implement a robust supplier risk mitigation program essentially vetting the background and general compliance with carious protocols as a prerequisite for business to start.
- Conduct business with companies that adhere to internationally recognised cybersecurity standards such as ISO/IEC 27001.
- have a secure environment to validate hardware and software before it goes into the production line.
- implement a process for efficiently keeping track of physical components and deployments of software to make traceability easy should a compromise occur.

With these steps cybersecurity risks in the supply chain are greatly reduced.

Risk 4 Mitigation: Personnel and Training

People are unfortunately always an inherent risk in security and cybersecurity in any industry, from disgruntled employees posing an insider threat or criminals targeting the company for financial gain, employees are an often-used attack vector.
- Comprehensive training regiment for cybersecurity within the company, with more in depth training and certification depending on the level of privilege an individual role requires.

-Training should be updated to reflect new developments and trends.
- Engage with employees and foster a security conscious work culture, highlighting individual ownership of and responsible actions with privileged information.
- Have a security helpdesk built into the IT system with an anonymous hotline so staff can highlight concerns discretely.
- Conduct simulated attacks such as phishing and social engineering scenarios so staff can have familiarity with these common methods in a controlled environment.

Risk Matrix After Mitigation

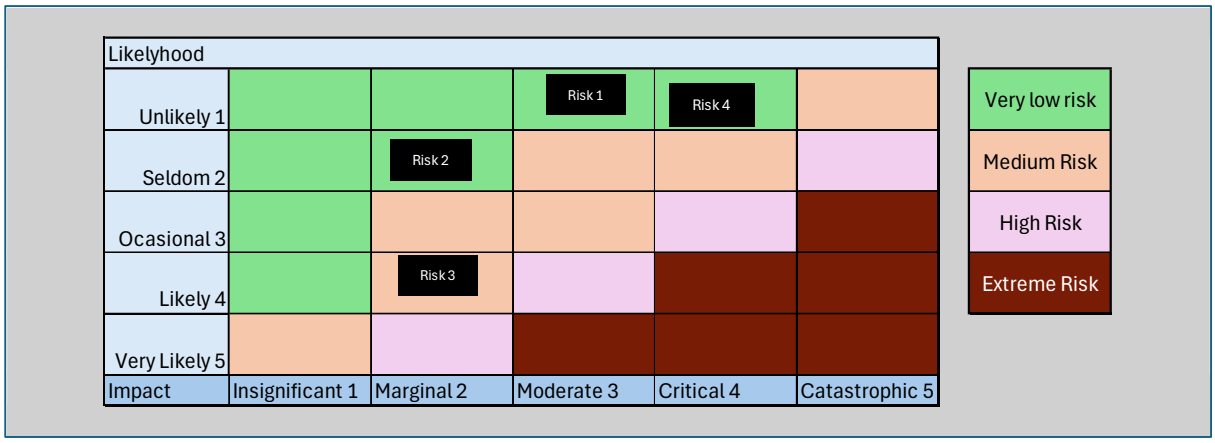

Figure 7: New acceptable levels of risk with mitigation measures in place.

Conclusion

In this document a custom-built desktop workstation was outlined in task 1 to meet the needs of an electrical engineer. With relatively high-end components the system is reasonably equipped to handle complex simulations, coding, CAD, and data processing tasks. With a good range of peripherals, expansion and upgrade options to remain useful for many years to come.

In task 2 cybersecurity threats were identified and assessed based on the potential impact and likelihood of occurrence. A mitigation action plan was outlined broadly modernising the network, securing production equipment, strengthening the supply chain and upskilling members of staff. Through this the company will greatly reduce its risk of falling foul of threats in the cyber space. Cybersecurity is an evolving ongoing procedure with mitigation strategy and security culture needing to be embedded into a company from the ground up. Investment in training and new technology is critical to maintaining the organisations security posture in the long term.

Bibliography

Bibliography

[1]

P. Palandrani, “A Decade of Change: How Tech Evolved in the 2010s and What’s In Store for the 2020s,” *Global X ETFs*, Feb. 10, 2020. https://www.globalxetfs.com/a-decade-of-change-how-tech-evolved-in-the-2010s-and-whats-in-store-for-the-2020s/ (accessed Apr. 02, 2025).

[2]

Dell Inc., “Dell Pro Tower | Dell UK,” *Dell*, 2018. https://www.dell.com/en-uk/shop/desktop-computers/dell-pro-tower-plus-desktop/spd/dell-pro-qbt1250-plus-desktop/gcto_qbt1250_emea?redirectto=SOC&configurationid=89a3a8e7-5b72-4ed9-a86e-c040d4334ac9 (accessed Apr. 02, 2025).

[3]

J. Potter, “CPU Cores Vs. Threads - Everything You Need To Know,” *NameHero® Blog*, Jul. 03, 2023. https://www.namehero.com/blog/cpu-cores-vs-threads-everything-you-need-to-know/ (accessed Apr. 02, 2025).

[4]

Scan Computers International Ltd, “AMD Ryzen 9 7950X 16 Core AM5 CPU/Processor,” *Scan.co.uk*, 2022. https://www.scan.co.uk/products/amd-ryzen-9-7950x-am5-zen-4-16-core-32-thread-45ghz-57ghz-turbo-64mb-cache-pcie-50-170w-cpu (accessed Apr. 03, 2025).

[5]

Dell Inc., “Industry-wide Issue with Intel Core 13th and 14th Generation i5, i7, and i9 Processors,” *Dell.com*, Jan. 30, 2025. https://www.dell.com/support/kbdoc/en-uk/000227933/industry-wide-issue-with-intel-core-13th-and-14th-generation-i5-i7-and-i9-processors (accessed Apr. 03, 2025).

[6]

ADMI LIMITED, “ASUS ROG STRIX X670E-F GAMING WIFI AMD Ryzen DDR5 ATX Motherboard - Socket AM5,” *Awd-it.co.uk*, 2025. https://www.awd-it.co.uk/asus-rog-strix-x670e-f-gaming-wifi-amd-ryzen-ddr5-atx-motherboard-socket-am5.html?gad_source=4 (accessed Apr. 03, 2025).

[7]

NVIDIA Corporation, “NVIDIA GeForce RTX 5080 Graphics Cards,” *NVIDIA*, 2025. https://www.nvidia.com/en-gb/geforce/graphics-cards/50-series/rtx-5080/ (accessed Apr. 08, 2025).

[8]

Corsair Gaming, Inc., “VENGEANCE® 64GB (2x32GB) DDR5 DRAM 5600MT/s CL40 AMD EXPO & Intel XMP Memory Kit,” *CORSAIR*, 2025. https://www.corsair.com/uk/en/p/memory/cmk64gx5m2b5600z40/vengeance-64gb-2x32gb-ddr5-dram-5600mt-s-c40-amd-expo-memory-kit-cmk64gx5m2b5600z40 (accessed Apr. 08, 2025).

[9]

National Cyber Security Centre UK Gov, “Cyber security risk management framework,” *Ncsc.gov.uk*, 2025. https://www.ncsc.gov.uk/collection/risk-management/cyber-security-risk-management-framework (accessed Apr. 09, 2025).

[10]

Information Commissioner's Office, “The UK GDPR,” *Ico.org.uk*, Nov. 19, 2024. https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/#:~:text=Yes.,and%20obligations%20remain%20the%20same. (accessed Apr. 10, 2025).

[11]

UK Gov, “Data Protection Act 2018,” *Legislation.gov.uk*, 2018. https://www.legislation.gov.uk/ukpga/2018/12/section/170 (accessed Apr. 10, 2025).

[12]

D. Gilmore, “The Rising Threat of Ransomware in Manufacturing,” *Threatintelligence.com*, Sep. 03, 2024. https://www.threatintelligence.com/blog/manufacturing-ransomware#:~:text=Cyber%20attacks%20often%20lead%20to,to%20delays%20and%20increased%20costs. (accessed Apr. 10, 2025).

[13]

Information Commissioner's Office, “Supply chain attacks,” *Ico.org.uk*, Feb. 06, 2025. https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/learning-from-the-mistakes-of-others-a-retrospective-review/supply-chain-attacks/#:~:text=The%20threat%20from%20a%20supply,supply%20chain%2C%20open%20to%20attack. (accessed Apr. 10, 2025).

[14]

C. Demarest, “Supply chain terror: Explosions in Lebanon raise new security alarms,” *Axios*, Sep. 18, 2024. https://www.axios.com/2024/09/18/hezbollah-pager-explosions-supply-chain-terror (accessed Apr. 10, 2025).

[15]

IBM, “Social Engineering,” *Ibm.com*, Jun. 14, 2022. https://www.ibm.com/think/topics/social-engineering (accessed Apr. 10, 2025).

[16]

BlueVoyant, “8 Devastating Phishing Attack Examples (and Prevention Tips),” *BlueVoyant*, 2015. https://www.bluevoyant.com/knowledge-center/8-devastating-phishing-attack-examples-and-prevention-tips (accessed Apr. 10, 2025).