

ACCA4028 Aaron Bell

Assignment FINAL

by Aaron Bell

Submission date: 09-Apr-2025 03:39PM (UTC+0100)

Submission ID: 255247090

File name: 59334_Aaron_Bell_ACCA4028_Aaron_Bell_Assignment_FINAL_659655_1161505397.docx (36.56K)

Word count: 2318

Character count: 13455

ACCA4028 – Computer systems fundamentals

Level 6 Embedded Electronics Apprenticeship

By Aaron Bell (2410529)



Table of Contents

PC Build Table	 2	3
1.0 Introduction		4
2.0 Identification and evaluation of risks		4
2.1 Outdated Firewall Configurations		4
2.2 Outdated firmware and default passwords		5
2.3 Insecure supply chain		5
2.4 Limited security awareness training		5
3.0 Prioritisation of risks		6
4.0 Mitigation of risks		7
4.1 Outdated Firewall configurations:		7
4.2 Outdated firmware and default passwords:		7
4.3 Insecure supply chain:		7
4.4 Limited security awareness training:		7
5.0 Computer Incident Response Plan (CIRT)		7
5.1 Purpose and Scope		7
5.2 Roles and Responsibilities		7
5.3 Incident Identification and Reporting		7
5.4 Response Workflow		8
5.4.1 Preparation		8
5.4.2 Detection and Analysis		8
5.4.3 Containment, Eradication, and Recovery		8
5.4.4 Post-Incident Activity		8
5.5 Communication Plan		8
5.6 Documentation and Evidence Collection		8
5.7 Review and Testing		8
References		9

PC Build Table



Component	Section	Specification	Price
CPU	Intel Core i7-14700K 3.4 GHz 20-Core Processor	20-core, 28 threads, 3.4GHz base, upto 5.6GHz	£ 306.97
CPU Cooler	Noctua NH-D9L 46.44 CFM CPU Cooler	400-2000 RPM, 16.3-22.8 dB	£ 49.95
Motherboard	Asus PRIME B760-PLUS ATX LGA1700 Motherboard	2x PCIe x16, 2x PCIe 1x, 4x M.2 Slots, 4x SATA 6Gb/s, 1x 2.5Gb/s Ethernet, 2x USB 2.0 and 2x USB 3.2	£ 125.99
Memory	Kingston FURY Beast 128 GB (4 x 32 GB) DDR5-5600 CL40 Memory	DDR5-5600, 128GB total	£ 356.15
Storage	Crucial P3 Plus 2 TB M.2-2280 PCIe 4.0 X4 NVME Solid State Drive	2TB SSD Storage	£ 114.98
Graphics Card	MSI VENTUS 2X XS OC GeForce RTX 3050 8GB 8 GB Video Card	1550MHz core clock, 8GB GDDR6. DisplayPort, HDMI and DVI-D	£ 197.20
Case	Lian Li Lancool II Mesh C Performance ATX Mid Tower Case	2x USB 3.2 and 9x Drive Bays	£ 92.94
Power Supply	be quiet! Straight Power 12 1000 W 80+ Platinum Certified Fully Modular ATX Power Supply	1000W, Fully modular, 9x SATA connectors	£ 156.66
Operating System	RHEL	It's not windows	£ 255.36
			£ 1,656.20

1.0 Introduction

Based on a recent security audit, potential issues have been identified within an electronics manufacturing company producing IoT (Internet of Things) devices, sensors and industrial electronics. Given the industry of the company is producing devices that may be used in the role of Operational Technology (OT), it is essential to assess the threat landscape against this sector before conducting a risk analysis.

Nation-state threat actors remain the primary threat to OT, responsible for the active exploitation of internet-accessible OT and industrial control systems (ICS) devices [1]. Therefore, securing the production line is crucial to ensure these devices are secure by design. By developing products that are secure by design, it enables engineers to implement these devices securely and at pace; ensuring uptime of critical infrastructure. By taking steps to secure the production environment, peace of mind can be provided to customers that these devices meet secure by design principles.

2.0 Identification and evaluation of risks

Whilst the audit has successfully picked up 4 key risks, it is important to understand the criteria by which these need to be evaluated.

- Quantitative risk analysis considers the financial impact of incidents or attacks. Quantitative risk analysis uses relevant, verifiable data to predict the probability of certain risk outcomes and their estimated monetary cost. [2] However, without numbers and accurate statistics, this type of risk analysis is outside the scope of this document.
- Qualitative risk analysis differs in the sense that it does not assign direct monetary values to risks and instead ranks threats on a scale to evaluate their risks, costs and effects. [3] As this latter approach **doesn't** directly require prior data, it will be the approach used for this document. The standard  approach of using Severity, Likelihood and Impact will be adopted henceforth.

2.1 Outdated Firewall Configurations

Before properly addressing this risk, it would be advised to ask the auditor for clarification, as "outdated firewall configuration" is a somewhat vague statement. For the purpose of this analysis, it is assumed to refer to a misconfigured firewall. One plausible scenario is that access-control lists (ACLs) are setup for an outdated IP schema. The scenario analysed will be IP addresses once based in a demilitarized zone (DMZ) have become reused in the enterprise local area network (LAN) and bring potential security implications, particularly if the firewall is a stateless one.

Generically, misconfigured firewalls can lead to a high chance of external attackers being able to penetrate the edge of the enterprise network, potentially resulting in access to sensitive data. A misconfigured firewall may also allow easier exfiltration of stolen data. The aforementioned example of DMZ addresses being re-used in the enterprise LAN would be a critical problem requiring immediate remediation. Such a scenario could allow traffic through the DMZ firewall and flow straight to the internal network without triggering alerts or being dropped.

Severity	Likelihood	Impact
4.5/5	4/5	Data loss and reputational damage. Compliance violations.

2.2 Outdated firmware and default passwords

Outdated firmware and default passwords are common vulnerabilities, but provide high value to attackers. With vulnerabilities being well documented and proof of concepts (PoCs) readily available on the web, it is incredibly important to keep devices up to date to avoid them being vulnerable to known exploits [4]. In addition to this, default passwords are often well known and easily brute forced, whether from knowing the device in question or a random brute-force attack.

This vulnerability in the company's infrastructure would allow for external attacks to scan for these devices, whether from within or targeting internet-exposed system specifically. Attackers can take advantage of search engines like Shodan to find internet-exposed devices running outdated versions of firmware. Therefore this is a severe security risk and should be addressed immediately by enforcing authentication, network segmentation, device provisioning and ensuring updates are carried out regularly.

Severity	Likelihood	Impact
4.5/5	4/5	Data loss and reputational damage. Direct impact to production line and compliance violations.

2.3 Insecure supply chain

The term "insecure supply chain" is broad and encompasses many factors that would need to be considered. It's possible that in this context, the risk being referred to is the sourcing of components from suppliers, alternatively the threats posed by OT devices used on the production line. The integrity and security of these components is critical, especially if they are programmed externally. This role usually lies with the organisations Governance, Risk and Compliance (GRC) analysts.

Risks can range from insecure practices at the companies, to firmware that is compromised with backdoors. To mitigate the potential damage this can cause, suppliers that the company use should be checked to ensure compliance with established security standards such as ISO 27001 [5] and/or Cyber Essentials depending on jurisdiction. This will provide peace of mind that third-party vendors take security of their devices seriously, with commitments to identify and assess information security risks, implement controls to mitigate those risks and monitor and review these controls on an ongoing basis [5].

Severity	Likelihood	Impact
3/5	3/5	Data loss, unauthorised access, reputational damage and espionage.

2.4 Limited security awareness training

End users are often considered the weakest link according to common practices. Direct attacks such as phishing and social engineering remain common vectors for initial compromise. From technical threats such as malicious attachments, to physical threats such as tailgating and trespassing.

Severity	Likelihood	Impact
2/5	3/5	Initial compromise, unauthorised access, loss of personal devices, theft.

3.0 Prioritisation of risks

Before discussing prioritisation of risks, first the formulas for calculating quantitative risk are detailed below. However in the given scenario they are unable to be used, but would be an important factor when considering risks in an organisational context.

$$\text{Single Loss Expectancy (SLE)} = \text{Asset Value (AV)} \times \text{Exposure Factor (EF)}$$

$$\text{Annual Loss Expectancy (ALE)} = \text{SLE} \times \text{Annual Rate of Occurrence (ARO)}$$

Based on the evaluation of each individual, the table below lists these risks in descending order. From highest priority to lowest priority

Priority	Risk	Reasoning
Critical	Outdated firewall configurations	The proposed misconfigurations represent a significant risk, being easily exploitable and allowing network traffic into the enterprise LAN that should be stopped at the DMZ.  13
High	Outdated firmware and default passwords	Known vulnerable versions of firmware and default passwords are easy to exploit, with the internet being a readily available source of this information and search engines allowing attackers to easily scan lots of devices.
Medium	Insecure supply chain	The risk is relative to the above, however this takes more time to sort out and will involve GRC and legal. Hence, it should be treated as a medium risk, giving a realistic timeframe to have it amended.
Medium	Limited security awareness training	Whilst the impact that may arise from successful phishing and social engineering attacks, implementing a security awareness programme is simple and can be quite hands off. The priority doesn't suggest it shouldn't be actioned immediately, but that the process isn't as critical as the risks above.

4.0 Mitigation of risks

4.1 Outdated Firewall configurations:

- Keeping network documentation up to date and conducting red team exercises will help catch misconfigurations early and allow action to be taken. In addition to this, having network segmentation in place for different systems will help mitigate the damage an attacker can do if one part of the network is compromised.

4.2 Outdated firmware and default passwords:

- Implementation of a proper asset management lifecycle and provisioning policy for new devices will help prevent outdated firmware and default passwords, provided firmware is updated as soon as reasonably possible in a production environment.

4.3 Insecure supply chain:

- GRC specialists will need to investigate third-party vendors and their sources before agreeing contracts, ensuring third parties in the supply chain are compliant with industry recognised information security standards. Helping verify the minimum additional risk is added by the introduction of these components and products.

4.4 Limited security awareness training:

- Implementation of regular security awareness training either in house or through a third party will meet requirements, in addition to this the carrying out of phishing tests and physical penetration tests will help boost security culture and identify staff who need further training.

5.0 Computer Incident Response Plan (CIRT)

Please note this is a very brief plan, a real incident response plan would be a document of 10s of pages with multiple pieces of supporting documentation, but I only have ~700 words.

14

5.1 Purpose and Scope

This plan outlines the procedures in place for the detection, response and recovery from security incidents affecting IT and OT infrastructure.

5.2 Roles and Responsibilities

This section cannot be completed fully without detail about the companies' personnel but here is an example table that is a good start:

Role	Responsibility
Incident Response (IR) Lead	Coordination of the overall response effort.
IT/OT Analysts	Work under the lead to detect and identify incidents, and with engineers to contain them.
Security/Network Engineers	Work with analysts to contain incidents, and responsible for eradication of the cause.
Communications Officer	Handling internal and external communications.
GRC & Legal teams	Ensure compliance with regulations.
HR	Handle any employee related aspects.

15

5.3 Incident Identification and Reporting

An incident shall henceforth be defined as an action that may result, or has resulted in an impact on the confidentiality, integrity or availability of the companies systems and/or information. Examples include but are not limited to:

- Any attempted network intrusion

- Any detection of malware
- Any unauthorized access to information/data
- Violation of security policies
- Any attempted denial-of-service attack

Reported incidents will come in either via the ticketing process from end-users or as a result of analysts and continuous monitoring or flagged alerts from Security Information & Event Management (SIEM) systems and shall be processed under a levels 1-3 ticketing system.

5.4 Response Workflow

5.4.1 Preparation

Development of supporting documentation based on lessons learned from table top exercises or live incidents. Ensuring staff are properly trained to identify and respond to incidents, or seek third party IR teams. Ensure plans are up to date and ready, with staff comfortable with the tools and resources.

5.4.2 Detection and Analysis

Analysts are responsible for responding to tickets and triage of potential incidents, determining their scope and provide insight into indicators or compromise to assist in the containment and eradication.

5.4.3 Containment, Eradication, and Recovery

Engineers take action based on the triage of incidents by analysts, with the aim to limit the damage of an active incident, eliminate any malware or adversary presence and restore systems back to their usual operational state.

5.4.4 Post-Incident Activity

Phase where lessons learned are drawn up, so that a full review of what happened, how the response was handled, to ensure continuous improvement ahead of future incidents and exercises.

5.5 Communication Plan

IR lead shall distribute information internally, with communications officer responsible for external and stakeholder communications.

5.6 Documentation and Evidence Collection

Actions taken to triage and decisions made to contain incidents must be documented and timestamped, the same applies to mitigations put in place by engineers. This allows for better analysis in the post incident phase and can help convert temporary solutions into permanent blocks.

5.7 Review and Testing

Incident response plans shall be reviewed quarterly, allowing for updates based on the latest trends and best practices. In addition to this, table top exercises and red team simulations should be conducted every 6 months, to ensure staff are up to date and can respond in way that's prompt, effective and in-line with procedures.

References

- [1] CISA, "Threat Actors Continue to Exploit OT/ICS through Unsophisticated Means," 25 Sept 2024. [Online]. Available: <https://www.cisa.gov/news-events/alerts/2024/09/25/threat-actors-continue-exploit-otics-through-unsophisticated-means>. [Accessed 02 Apr 2025].
- [2] M. Tierney, "Quantitative Risk Analysis: Annual Loss Expectancy," Netwrix, 24 Jul 2020. [Online]. Available: <https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/>. [Accessed 02 Apr 2025].
- [3] C. Mike Chapple, "Chapter 2, Personnel Security and Risk Management Concepts," in *Certified Information Systems Security Professional Study Guide, Eighth Edition*, Indianapolis, Sybex, 2018, p. 74.
- [4] NCSC, "Device Security Guidance," NCSC, 29 Jun 2021. [Online]. Available: <https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date>. [Accessed 03 Apr 2025].
- [5] ISO, "ISO/IEC 27001:2022," Oct 2022. [Online]. Available: <https://www.iso.org/standard/27001>. [Accessed 08 Apr 2025].

ACCA4028 Aaron Bell Assignment FINAL

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

69/100

PAGE 1



Comment 1

Good Work,
the first page or the tile page of the report should have the name, student ID,
Module Name, Module code, Title of the Coursework, programme of study. Most of
these are in the title page, but however few are missing.

PAGE 2



Comment 2

Good Work

PAGE 3



Comment 3

It is better to start with a introduction proceed with explanation for each component, justifying
the reason for choosing.



Comment 4

Good Work



Comment 5

It is
better to provide a numbered title for the table, as it clearly indicates the
table's content and purpose, making it easier for readers to understand its
context and relevance.

PAGE 4



Comment 6

Recommended
to avoid contractions like "doesn't." Instead, use the full form of the
phrase, which in this case is "does not."



Comment 7

Use of severity and likelihood to assess the risk is appropriate. However, this section would be stronger with a supporting citation



Comment 8

It is better to include page number

PAGE 5



Comment 9

Good Background work



Comment 10

Use of severity and likelihood to assess the risk is appropriate. However, this section would be stronger with a supporting citation



Comment 11

Use of severity and likelihood to assess the risk is appropriate. However, this section would be stronger with a supporting citation



Comment 12

Use of severity and likelihood to assess the risk is appropriate. However, this section would be stronger with a supporting citation

PAGE 6



Comment 13

It is
better to provide a numbered title for the table, as it clearly indicates the
table's content and purpose, making it easier for readers to understand its
context and relevance.

PAGE 7



Comment 14

It is better to write as, Due to word count constraints, the plan is summarised briefly



Comment 15

It is
better to provide a numbered title for the table, as it clearly indicates the
table's content and purpose, making it easier for readers to understand its
context and relevance.

**Comment 16**

It is better to have a conclusion, that would have enhanced the overall quality of the report.

GRADING FORM: GRADING

AARON BELL**69.10****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.



Wide and appropriate reading demonstrated, with strong selection of sources. Referencing is consistent. Include more peer-reviewed or technical publications to enhance depth. Consider expanding to a broader range of literature types.

6.55**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 cyber security and Computer Systems which is evident through the description. It would have been better with a description about components used in task 1.

22

COGNITIVE AND INTELLECTUAL

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



Sound evaluation of the underlying concepts and principles of Computer Systems and cyber security. Ability to devise arguments using evidence to make mostly appropriate and valid judgements is evident from the description. The report would be improved by providing clearer justification for the selection of each component. The report clearly demonstrates the adoption of a holistic and proportionate approach to mitigating security risks by addressing technical, organisational, and human factors, aligned with the severity and likelihood of each risk.

18

PRACTICAL SKILLS

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



Good application of a range of hardware tools and techniques. Very good consideration of the context of the application. Good evidence of different approaches to problem-solving in Computer and link between theory and practice. It would have been better with the a clear justification of the choice of component.

16.25

TRANSFERABLE SKILLS FOR LIFE

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



The report is well-structured with good coherence, contributing to a strong presentation. Overall quality is commendable, demonstrating effective transferable skills. Consider Minor refinements such as ensuring proper text alignment would further enhance the polish of the report. It would also benefit from the inclusion of an introduction for Task 1 and a conclusion to effectively close the report.

6.3