

APPENDIX GA36a

LEVEL 4 ASSESSMENT SPECIFICATION

Student name:	Maisie Evans	Student number:	ID 2512230
Programme:	DA Program - BSC in Supply Chain and Logistics		
Module:	Data Analytics Principles		
Module code:	ACMA 4016	Contribution to Overall Module Assessment (%):	100%
Lecturer:	Dr Moutushi Tanha	Internal Verifier:	Dr Irina Neaga
Assignment Title:	Developing a Data-Based Report	Word count (or equivalent):	1500 words
Submission deadline:	01/03/2026	Return date of provisional marks & written feedback:	20 working days after submission
Submission method:	All written assessments, where practical and possible, must be submitted via Turnitin unless otherwise instructed by the Lecturer. (Please DO NOT put this assessment specification into Turnitin or it will match many similarities with other students' submissions.) Alternative submission method (if applicable): Late submission of the assessment will result in a late penalty mark: Work which is submitted up to 1 week late will be capped at 40% for the first attempt and will be awarded a mark of 0% for re-assessment. Late submission penalties may be lifted only if there is an approved extenuating circumstances claim. Work submitted more than 1 week late will be considered as a non-submission and will not be marked. The work may be considered as a submission for reassessment if offered by an Examining Board or if there is an approved extenuating circumstances claim.		

Academic honesty / referencing:	Academic honesty is required. In the main body of your submission you must give credit to authors on whose research and ideas your work is based. Append to your submission a reference list that indicates the books, articles, etc. that you have used, cited or quoted in order to complete this assessment.
--	---

Module Learning Outcomes (from module syllabus)
Upon the successful completion of this module, the student should be able to: understand the fundamental concepts and principles of data analysis, management systems and will be developing practical skills in using data analysis tools and systems in logistics and supply chains.

TASK DESCRIPTION

Use of Generative AI in Assessment

(Lecturer to indicate Yes or Not against each element)

RESEARCH	For this assessment, you can use Generative AI to support you in research, including searching for bibliography, using tools to summarise, compare and interrogate materials.	Yes ☒ No ☐
STRUCTURE	For this assessment, you can use Generative AI to support you in structuring your submission, including creating a draft argument structure, identifying parts and headings, etc.	Yes ☒ No ☐
PROOFREADING	For this assessment, you can use Generative AI to check your own text/creation for grammatical and syntactical mistakes, including rephrasing of your own work within specific standards.	Yes ☒ No ☐
WRITING	For this assessment, you can use Generative AI to create text for submission.	Yes ☐ No ☒
CREATIVE	For this assessment, you can use Generative AI to create creative materials, such as images.	Yes ☐

		No ☒
PROGRAMMING	For this assessment, you can use Generative AI to create and check code.	Yes ☐ No ☒
NONE	For this assessment, you are not allowed to use any type of Generative AI support. This includes research support, structure support, writing/proofreading support and creative support.	Yes ☐ No ☒

AI Acknowledgement

I confirm that I have not present any AI-generated materials as my own work in this portfolio.

However, I acknowledge that I have used or may have used the AI in the research and proofreading of my portfolio.

Name: Maisie Evans

Student ID: 2512230

Part A

Table of Contents

1.0 Executive Summary

2.0 Introduction

3.0 Background of Problem

4.0 Resolution Strategy

5.0 Data Collection / Preparation

6.0 Data Analysis

7.0 Discussion

8.0 Conclusion

Appendix

References

1.0 Executive Summary

Aumovio System UK Ltd is a worldwide company founded in Germany, established from the spin-off of former company Continental AG. Aumovio specialises in developing technology for future mobility, automated driving systems and software defined vehicles. The site in Ebbw Vale specialises in the manufacture of brake callipers and air suspension components for the global market, along with vehicle safety dynamics and technologies. Aumovio supplies major OEMs and companies within the automotive industry, such as Porsche, Mercedes-Benz, Bentley and many more. "We started from a strong position in the growth segments for the mobility of the future. We have a clear strategy for increasing value and are well equipped to take on the market challenges that lie ahead." (Aumovio, 2026).

2.0 Introduction

This report will cover a recent issue that occurred within the Aumovio plant in Ebbw Vale, looking into the data analytics and data reports. This occurrence was an incident involving one of the main customers of Aumovio, Jaguar Land Rover (JLR). Jaguar Land Rover is a major automotive company based in the UK, owned by Tata motors. This problem happened in late 2025, which resulted in Aumovio having numerous production issues and dispatching issues due to JLR not being able to access their systems correctly. JLR experienced a severe cyber-attack, terminating production for over five weeks across all UK plants. “A Cyber-attack is a deliberate attempt to gain unauthorised access to a computer network, computer system or digital device. The goal is to steal, expose, alter, disable or destroy data, applications or other assets.” (IBM, 2025).

3.0 Background of Problem

JLR fell victim to an extreme cyber-attack within the later months of 2025. This attack targeted their systems which caused considerable delays with production and stammered their stock intakes as all systems were harshly affected. As a result, this also caused substantial problems for their suppliers and customers. As Aumovio is one of JLRs suppliers, they took a mighty hit to both their production, and distributions to JLR. As JLR is one of Aumovio’s main customers, with goods being dispatched to them daily, it impacted sales by an excessive percentage. JLR had a £398m profit in 2024, however this cyber-attack resulted in a £485m pre-tax loss and a £196m in direct costs within the third quarter of 2025. The hack forced IT networks to completely shut down, impacting many processes such as, vehicle wholesaling and the Global Parts Logistics Centre. “The hack of Jaguar Land Rover has cost the UK economy an estimated £1.9bn, potentially, making it the costliest cyber-attack in British history.” (The Guardian, 2025). The HELLCAT ransomware group declared responsibility for the cyber-attack against JLR, where gigabytes of confidential information were exposed. The hack was assigned to a threat called “Ray” through a dark forum on March 10, 2025. The breach was conducted through stolen Jira credentials via Malware, one of HELLCAT’s signature trademarks. One of the many leaked sources of information was employee's information, such as email addresses, names, time zones and usernames. This raised massive workforce concerns about identity theft

and targeted phishing campaigns. “Emerging in mid-2024, HELLCAT has rapidly developed into a sophisticated ransomware group, using spear-phishing or public-facing application exploits for internal access, followed by PowerShell-based persistence, AMSI bypasses, and reflective code loading.” (Cyfirma, 2025).

4.0 Resolution Strategy

During the Cyber-attack, Aumovio had to intensely identify if their systems were affected by the hack. Aumovio had to quantify the impact on production, so that they were able to work alongside JLR, to provide support towards their pending recovery. Aumovio had regular meetings, twice a week to maintain communication with JLR and ensure it was up to date. This aided both JLR and Aumovio to try resolve the situation and develop strategies to support. Aumovio had to access logs and credential reviews to investigate whether any unauthorised access had been gained through third party points, such as VPNs, customer portals, ERP Systems or any servers that connected them to JLR. There were assessments on Identity Theft to recognise if any credentials were stolen through the malware, obtaining unauthorised access and confidential data or documents. Suppliers of JLR had to prove that their systems were secure before being able to reconnect with JLR. Aumovio scrutinized their network connections to determine whether there were any vulnerabilities that could have been a gateway for the cyber-attack. By mid-October 2025, the attack was coming to an end, Aumovio coordinated their return to usual. They prioritised shipping components to other plants, such as JLR’s Electric Population Manufacturing Centre and JLR’s Battery Assembly Centre initially as these were the first to recover from the attack. Aumovio’s logistics team gave persistent effort to clear all backlog shipments that had rapidly accumulated over the five-week period.

5.0 Data Collection / Preparation

JLR Data

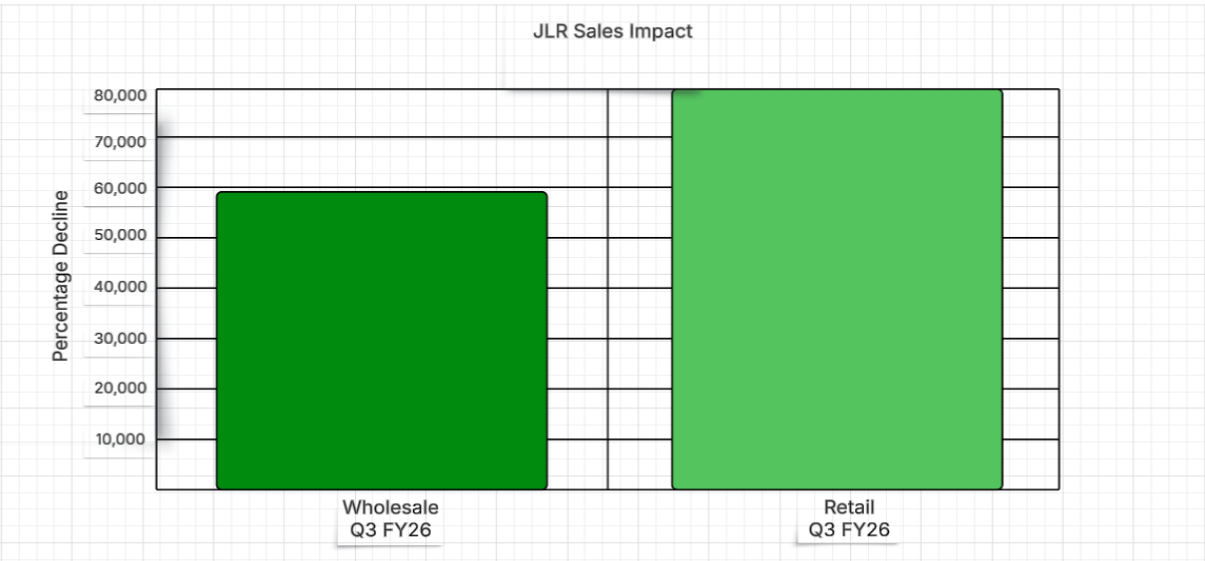


Figure 1: Financial Sales decrease during cyber-attack.

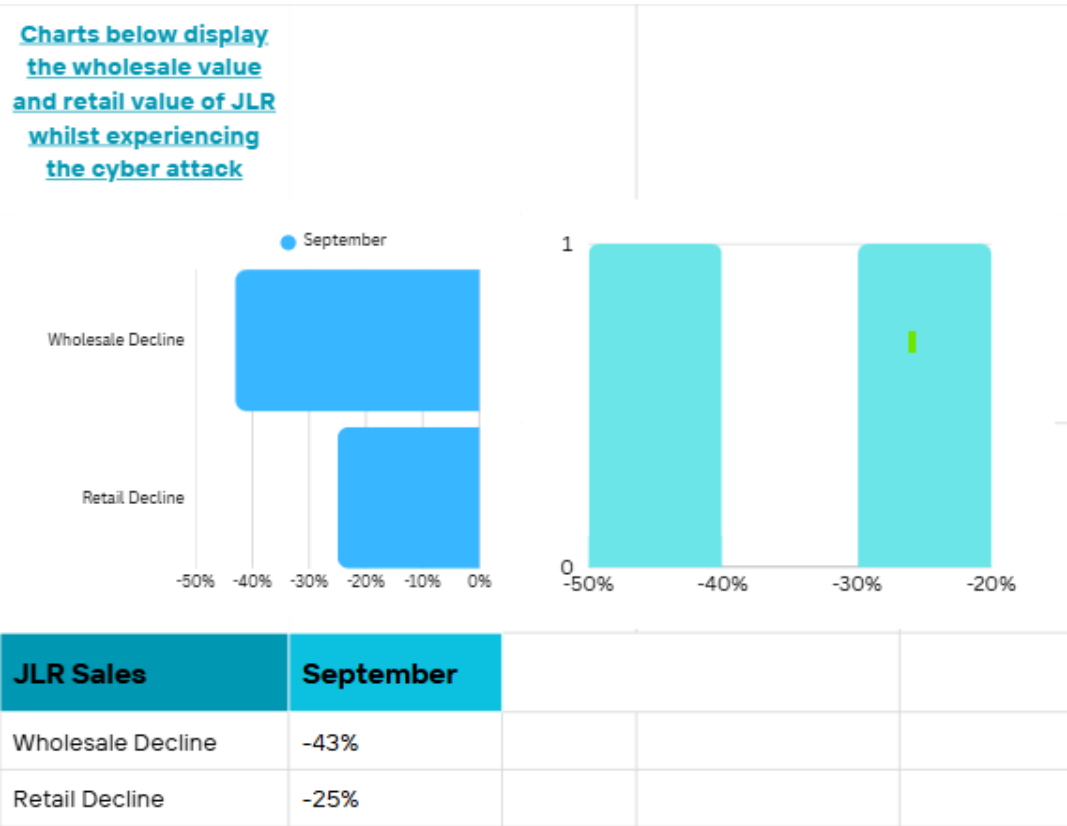


Figure 2: JLR wholesale value and retail percentage value drops during the cyber-attack.

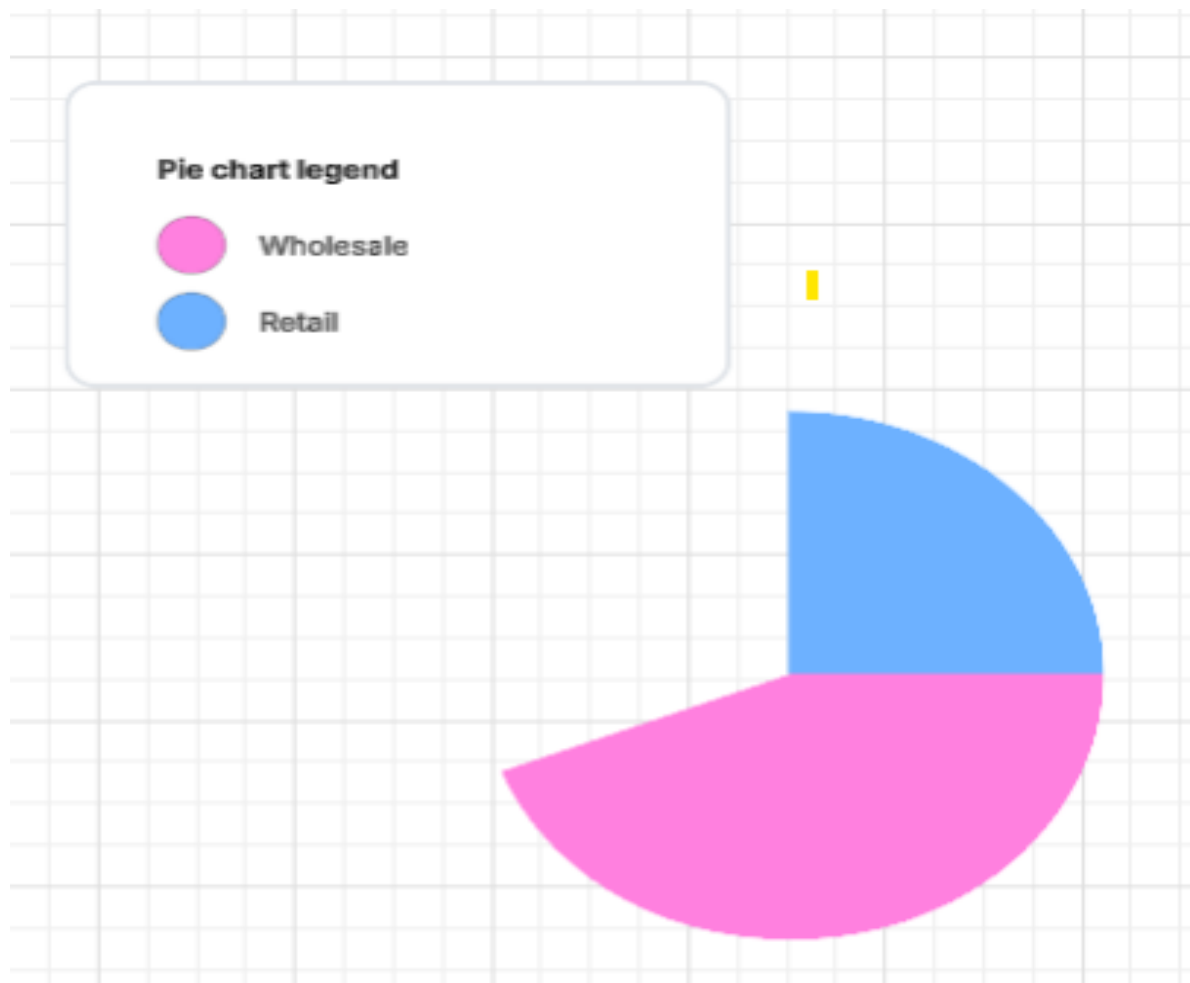


Figure 3: Declined percentage of units sold in Q3:

Wholesale – 44%

Retail – 25%

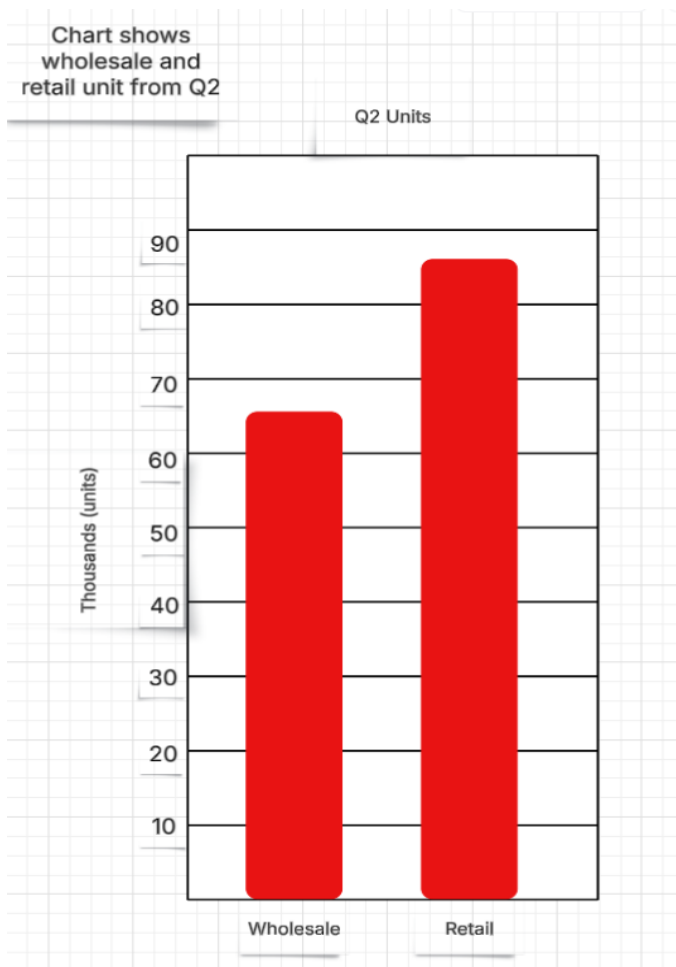


Figure 4: Wholesale and retail units sold in Q2, prior to the cyber-attack.

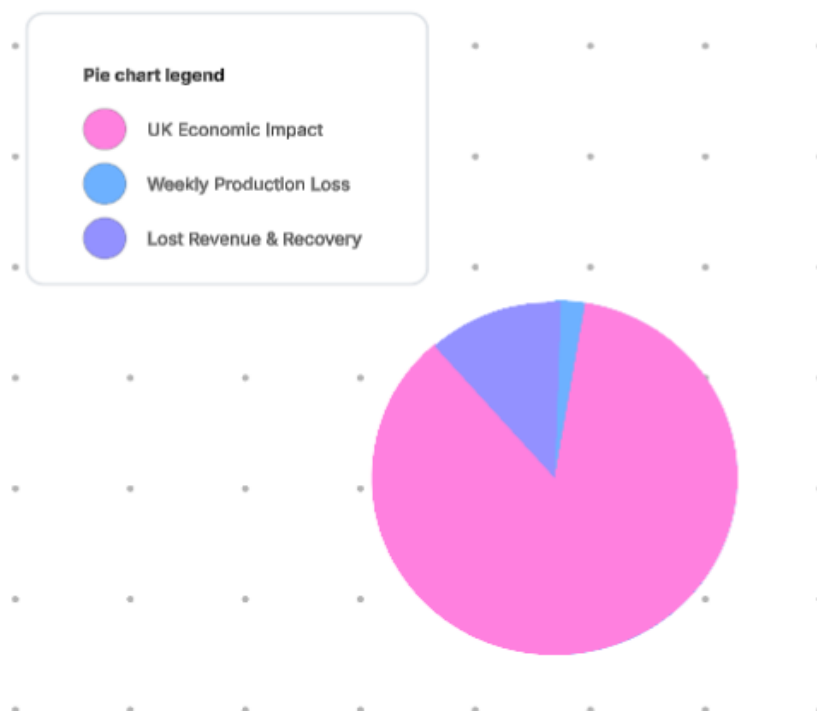


Figure 5: Distribution of cyber-attack related costs.

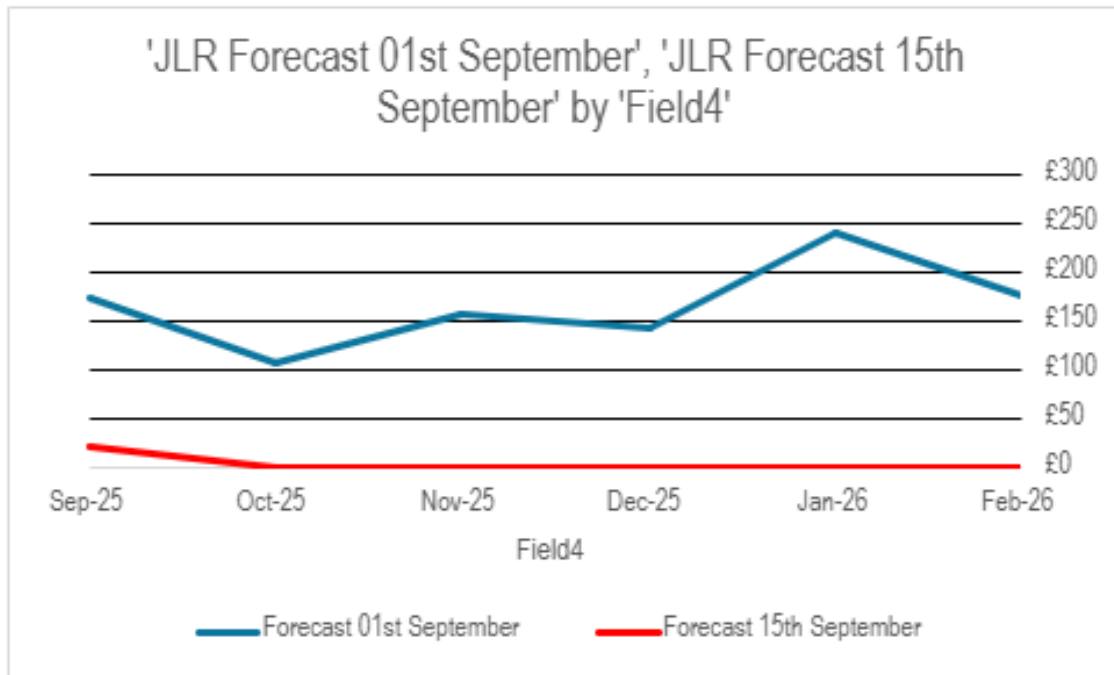


Figure 6: Aumovio's Forecasted Sales from JLR.

Sales Impact							
Customer Forecast Fortnightly Comparison		AUMOVIO					
		Sep-25	Oct-25	Nov-25	Dec-25	Jan-26	Feb-26
JLR	Forecast 01st Septem	£173,860	£108,967	£157,375	£144,418	£242,066	£176,467
	Forecast 15th Septem	£22,760	£0	£0	£0	£0	£0
	Forecast Dif +/-	-£151,100	-£108,967	-£157,375	-£144,418	-£242,066	-£176,467

Figure 7: Aumovio's impacted sales during JLRs cyber-attack.

Head Count Impact							
Customer Forecast Fortnightly Comparison		AUMOVIO					
		Sep-25	Oct-25	Nov-25	Dec-25	Jan-26	Feb-26
JLR	Forecast 01st Septem	37	37	36	34	34	33
	Forecast 15th Septem	33	35	33	31	29	29
	Forecast Dif +/-	-4	-2	-3	-3	-5	-4

Figure 8: Aumovio's Head Count impact during JLRs cyber-attack.

Directed Communications				
Receive email alerts when bulletins are published. Get started » View Help				
View Bulletins Subscriptions Alerts				
Archived Bulletins				
Search: Go				
Viewing 21-40 of 10102 « previouspage: 1 2 3 4 5 6 7 8 9 10 next » 20 ▼ per page				
ID	Status	Subject	From	Publish Date
280420	!	SUPPLIER COMMUNICATION: UPCOMING DEACTIVATION OF YOUR SUPPLIER JLR ACCOUNT - CDSID AUTHENTICATION	Jaguar Land Rover	October 03, 2025 05:15 PM GMT
280381	!	SUPPLIER COMMUNICATION: UK MANUFACTURING PRODUCTION UPDATE	Jaguar Land Rover	October 01, 2025 10:06 AM GMT
280380		SUPPLIER COMMUNICATION - WERS ALERTS INTERIM CONTAINMENT IN JIRA	Jaguar Land Rover	October 01, 2025 01:11 PM GMT
280341	!	SUPPLIER COMMUNICATION: WE WILL BUILD BACK EVEN BETTER TOGETHER	Jaguar Land Rover	September 29, 2025 09:30 AM GMT
280321	!	SUPPLIER COMMUNICATION - THE FOUNDATIONAL WORK OF OUR RECOVERY IS UNDERWAY	Jaguar Land Rover	September 25, 2025 01:29 PM GMT
280302	!	SUPPLIER COMMUNICATION - PRODUCTION UPDATE FROM CHIEF PROCUREMENT OFFICER	Jaguar Land Rover	September 23, 2025 06:46 AM GMT
280260	!	SUPPLIER COMMUNICATION - PRODUCTION UPDATE	Jaguar Land Rover	September 16, 2025 06:25 AM GMT
280240	!	SUPPLIER COMMUNICATION - UPDATE REGARDING OUR CYBER INCIDENT	Jaguar Land Rover	September 10, 2025 09:59 AM GMT
280200	!	SUPPLIER COMMUNICATION - UPDATE ON JLR CYBER INCIDENT	Jaguar Land Rover	September 04, 2025 07:58 PM GMT
280160	!	SUPPLIER COMMUNICATION - JLR GLOBAL IT SYSTEM ISSUES UPDATE	Jaguar Land Rover	September 02, 2025 11:29 AM GMT
280180	!	SUPPLIER COMMUNICATION: JLR CYBER INCIDENT UPDATE	Jaguar Land Rover	September 02, 2025 08:58 PM GMT
280140	!	SUPPLIER COMMUNICATION - JLR GLOBAL IT SYSTEM ISSUES	Jaguar Land Rover	September 01, 2025 12:29 PM GMT

Figure 9: Weekly meetings between Aumovio and JLR.

6.0 Data analysis

Internal

JLR Sales Performance Impact Analysis

Wholesale volume in Q3: measures vehicles shipped from JLR to dealerships
59,200 units – down 44%.

Retail volume in Q3: vehicles sold to actual customers
79,600 units – down 25%.

Figure 1 - As shown in Figure 1, this visual chart is displaying the financial sales decrease during the cyber-attack throughout the third quarter of JLRs financial year, 2026 (Q3 FY26).

Figure 2 - JLR wholesale value and retail percentage value drops during the cyber-attack.

Figure 3 - Declined percentage of units sold in Q3:
Wholesale – 44%
Retail – 25%

Figure 4 - Wholesale and retail units sold in Q2, prior to the cyber-attack.

Figure 5 - Distribution of cyber-attack related costs. Figure 6 Illustrates substantial expenses arising from the attack.

- UK Economic Impact - The production halt was so significant that it contributed majorly to the UK's economic contraction in September 2025.
- Weekly Production Loss – JLR analysis estimated a weekly deficit of £50million per week amidst idle production lines.
- Lost Revenue and Recovery – The company recorded an expense of £196million related to the cyber-attack, revenue fell by 39% at this time.

Aumovio Data Impact Analysis

Figure 6: Aumovio's Forecasted Sales from JLR. As shown in Figure 6, Aumovio's forecasted sales significantly dropped due to the complete shutdown of JLR. Their forecasted sales, concluded on 1st September were extensively greater than their forecasted sales following their discovery of the cyber-attack on the 15th of September. The forecasted sales were at £0 for the upcoming months, after regeneration mid-October the actual sales started to ascend gradually.

Figure 7 - As shown in Figure 7, Aumovio's forecasted sales significantly dropped due to the complete shutdown of JLR. Their forecasted sales, concluded on 1st September were extensively greater than their forecasted sales following their discovery of the cyber-attack on the 15th of September. The forecasted sales were at £0 for the upcoming months, after regeneration mid-October the actual sales started to ascend gradually.

Figure 8 - As displayed in Figure 8, Aumovio had a decrease in the number of employees working in production through the cyber-attack. For example, in September 2025, there were 37 heads expected to be on the shop floor working production. As a result of the stoppage, there were only 33 heads, which means 4 less heads at this time. This resulted in employees receiving less shifts, and less working hours which would have unfortunately affected their pay throughout the upcoming months.

Figure 9 - As presented in Figure 9, Aumovio and JLR were conducting meetings between once and twice a week. This implies that the issues between Aumovio's production and JLR were severe and had a crucial impact up on sales volumes. Aumovio was also receiving daily updates during this time via email from JLR. More in depth information regarding the meetings between JLR and Aumovio cannot be provided due to the confidential nature of these.

7.0 Discussion

Jaguar Land Rover is a major automotive company based in the UK, owned by Tata motors. JLR experienced a cyber-attack in September 2025, leading to immense

issues. This effected supply chains not only in the UK but globally. All automotive companies rely on JIT (Just-in-time) manufacturing, intending that even the smallest interruption, could be critical to suppliers and customers of JLR.

During the cyber-attack on JLR, it is evident that it wasn't only JLR affected substantially, it was also all their suppliers. With over 5,000 suppliers impacted, through line stoppages and production decreases, there was also a direct impact to the employers within these organisations with employees receiving less work and therefore, effects their pay. The cyber-attack also effected their customers, such as dealerships and retail customers. No one was able to receive any cars or parts distributed by JLR at this time.

Supply chains were exposed to many risks if there were systems linking them to JLR. Aumovio are connected to JLR through interconnected systems such as ERP and EDI and this made Aumovio vulnerable to third-party cyber risks. Consequently, Aumovio had to run in-depth system checks and data reviews to ensure no unauthorised access was gained through the interconnected systems. We can compare this to previous cyber-attacks that other companies have suffered from. Nissan faced a cyber related operational issue in the past; this proves that cyber risks within automotive industries are certainly not isolated.

It is critical that all companies ensure they implement cyber security improvements, thus making it more difficult for hackers to gain unauthorised access into systems. These improvements could be achieved through stronger third-party risk managements, regular penetration testing, increased cybersecurity investments, shared cybersecurity regulations and more pressure on mandatory compliance requirements. "As the nation's cyber defence agency and national coordinator for critical infrastructure security, the Cybersecurity and Infrastructure Security Agency lead the national effort to understand, manage, and reduce risk to the digital and physical infrastructure Americans rely on every hour of every day." (CISA, 2024).

Within the JLR data sheets above, we see more of a decrease in wholesale due to production stoppages. This is because no vehicles were manufactured or distributed. Once distribution started again, shipping still faced delays, not only from the excessive amount of backlog but the whole attack. There was limited availability as dealerships couldn't replenish stock for weeks, even months. Retail sales benefited from cars

already being with dealers before the attack, with an existing pipeline inventory for customers. This is a reason as to why retail wasn't as affected as wholesale. "The shutdown has disrupted both manufacturing and retail operations, with dealerships unable to register new vehicles". (Cyber Magazine, 2025).

Aumovio data shows significant decrease in sales within the third quarter of 2025. Forecasted sales were considerably greater before the attack, than they were during the attack. This presents to us, the immense decline Aumovio's sales had taken. Head counts also declined as Aumovio couldn't produce parts for JLR anymore, due to having no demands whilst their systems were completely shut down for weeks.

8.0 Conclusion

In conclusion, the Jaguar Land Rover cyber-attack demonstrates how supply chains are exposed to the risk of cyber-crimes. For suppliers such as Aumovio, the hack had implemented substantial issues within companies interconnected to JLR. The disruption didn't only reduce orders for a short period but exposed numerous vulnerabilities in just-in-time manufacturing. The temporary disruption resulted in inventory imbalances, pressure within cash flows, and huge sales decreases.

With a major OEM such as JLR, they would have advanced systems to prevent issues like this, with greater financial resilience. Whereas smaller OEMs often operate with thinner margins, therefore they are more vulnerable to cyber-crimes.

Furthermore, this illustrates that companies need to approach cyber resilience collaboratively. Greater investments need to be made towards cyber security in order to prevent future attacks, as you can never know the potential extent of damages caused whilst experiencing a cyber-attack.

References

Aumovio. (2026). How are we Shaping the Future of Mobility? (Accessed on 24th February 2026).

Available at: <https://www.aumovio.com/en/company/about-us.html>

CISA. (2025). CISA Launches New Platform to Strengthen Industry Engagement and Collaboration. (Accessed on 25th February 2026).

Available at: <https://www.cisa.gov/news-events/news/cisa-launches-new-platform-strengthen-industry-engagement-and-collaboration>

Cyber Magazine. (2025). An Overview of the JLR cyberattack. (Accessed on 27th February 2026).

Available at: [The Impact of Major Cyber Attack on JLR's Production Lines | Cyber Magazine](#)

Cyfirma, Decoding Threats. (2025). Investigation on Jaguar Land Rover Cyberattack. (Accessed on 18th February 2026).

Available at: <https://www.cyfirma.com/research/investigation-report-on-jaguar-land-rover-cyberattack/>

Jonker, A. Krantz T. IBM. (2025). Cyberattacks. What is a cyberattack? (Accessed on 27th February 2026).

Available at: [What Is a Cyberattack? | IBM](#)

The Guardian. (2025). Jaguar Land Rover hack has cost UK economy £1.9bn, experts say. (Accessed on 4th February 2026).

Available at: <https://www.theguardian.com/business/2025/oct/22/jaguar-land-rover-hack-has-cost-uk-economy-19bn-most-costly-cyber-attack-britain>

Part B

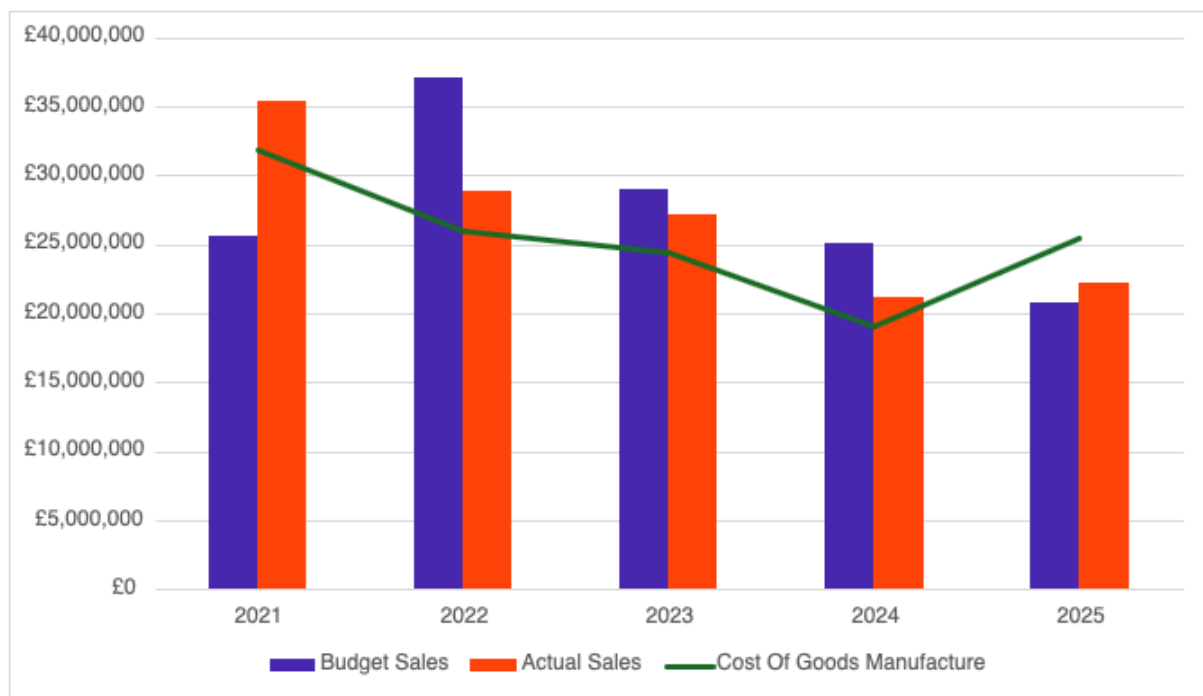


Figure 1: Sales for 2025.

As displayed in Figure 1, there is a comparison between Budget sales, Actual sales, and Cost of Goods Manufacture (COGM). This is analysed over a five-year period, from 2021-2025. We can see that in the years 2021 and 2025, Aumovio's actual sales exceeded the forecasted sales. This indicated that a higher volume of goods was sold in those years. Whereas in the years 2022, 2023 and 2024, Aumovio's budget sales were greater than their actual sales, displaying that there were less goods sold than expected. We can also see a pattern through the COGM where it shows a general downward trend, lower than budget and actual sales through 2021 to 2024. The COGM experienced a rise in the year of 2025, this is indicating that roughly £3million was spent on COGM. Performance falls below expectation as an excessive amount was overspent on COGM, compared to budget and actual sales.

COGM includes factors such as the cost of goods, cost of labour and employees, cost of transport, cost of manufacturing and utilities. So many expenses are included in this category.

Field1	Sum of Actual Sales	Sum of Budget Sales
2021	£35,361,875	£25,638,266
2022	£28,877,092	£37,109,523
2023	£27,187,309	£28,996,242
2024	£21,241,543	£25,084,847
2025	£22,177,770	£20,751,111
Grand Total	£134,845,589	£137,579,990

Figure 2: Table of Budget and Actual Sales from 2021 – 2025.

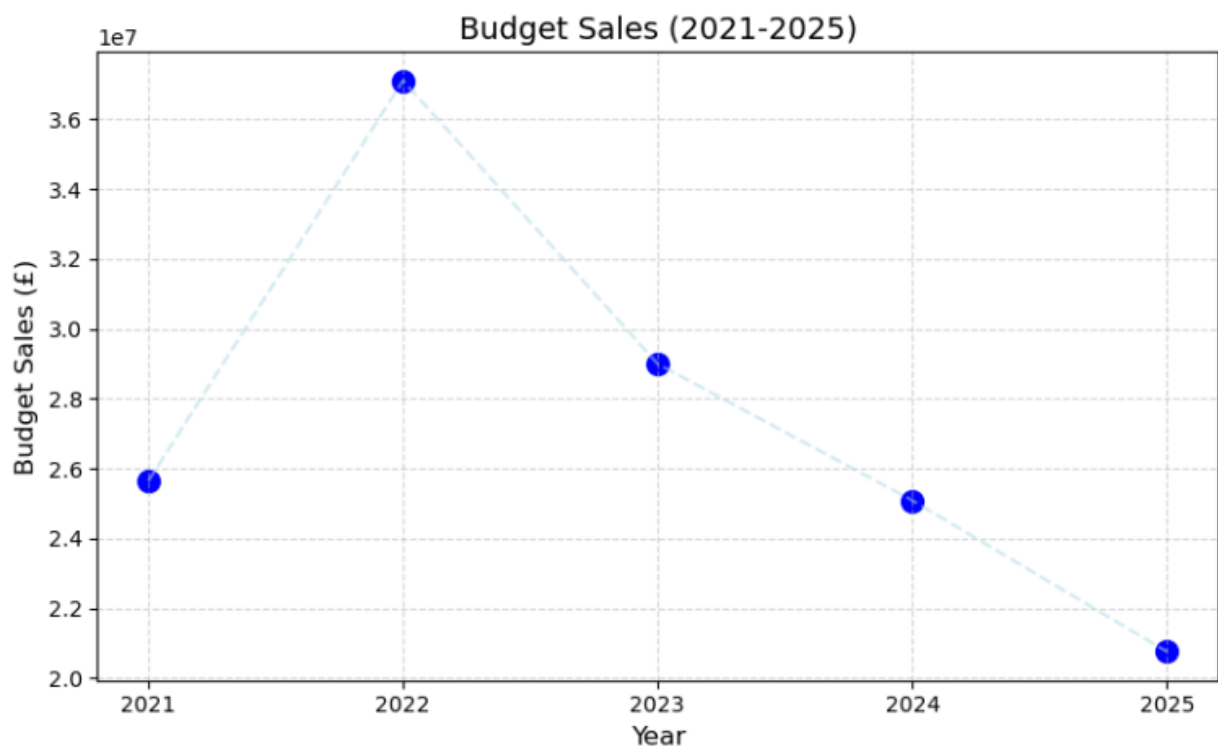


Figure 3: Budget sales comparison through years 2021 – 2025.

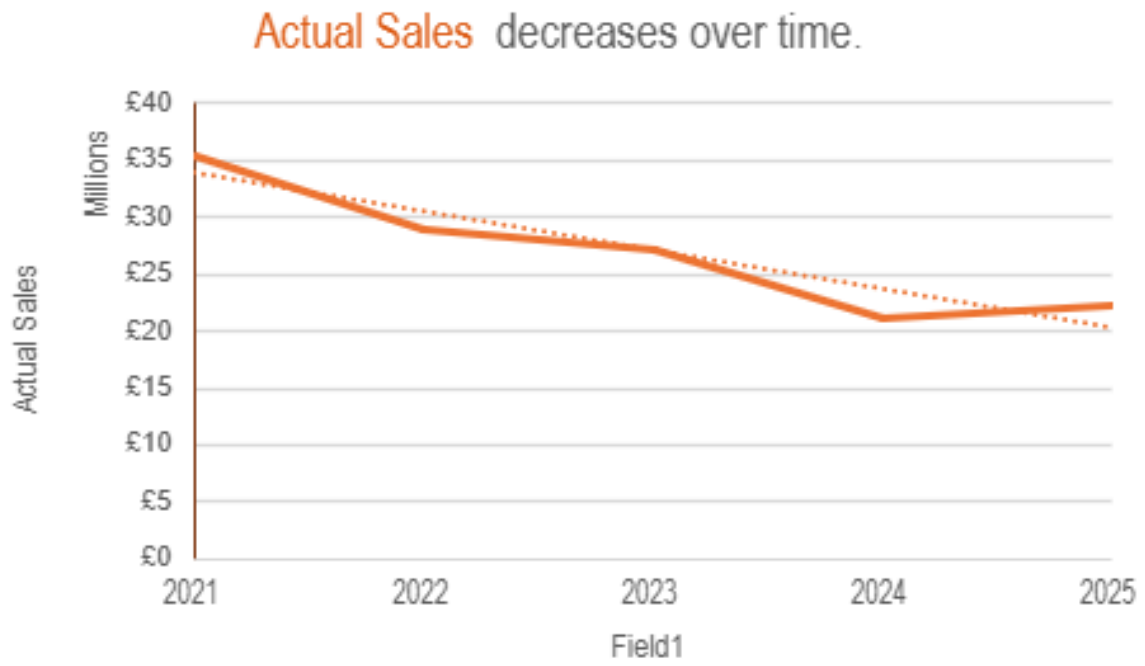


Figure 4: Actual Sales Decrease Over The 5-Year Period (Negative Correlation).

Sample

2021-2025 Sales	Mean	Median	Mode	Variance	Standard Deviation
Budget Sales	£27,515,998	£25,638,266		£38,150,000,000,000	£6,180,000
Actual Sales	£26,969,118	£27,187,309		£34,580,000,000,000	£5,881,000
COGM	£25,381,095	£25,504,436		£20,390,000,000,000	£4,516,000

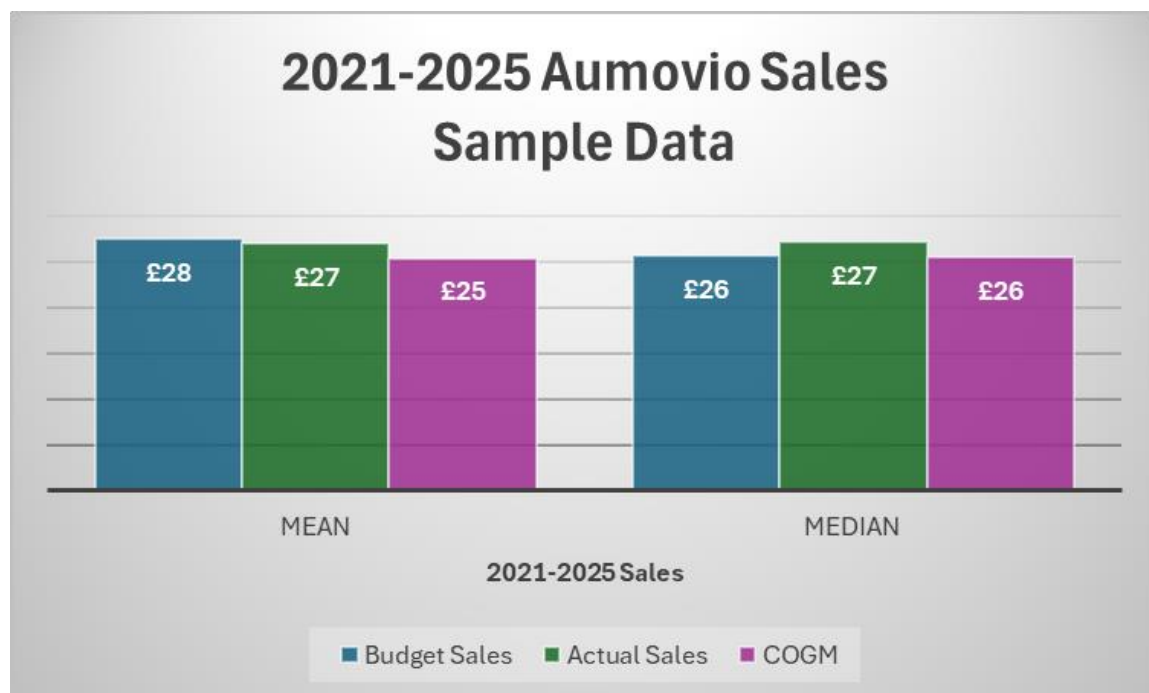


Figure 5: Sample Data from Aumovio's sales.

2021-2025 Sales	Standard Deviation
Budget Sales	£6,180,000
Actual Sales	£5,881,000
COGM	£4,516,000

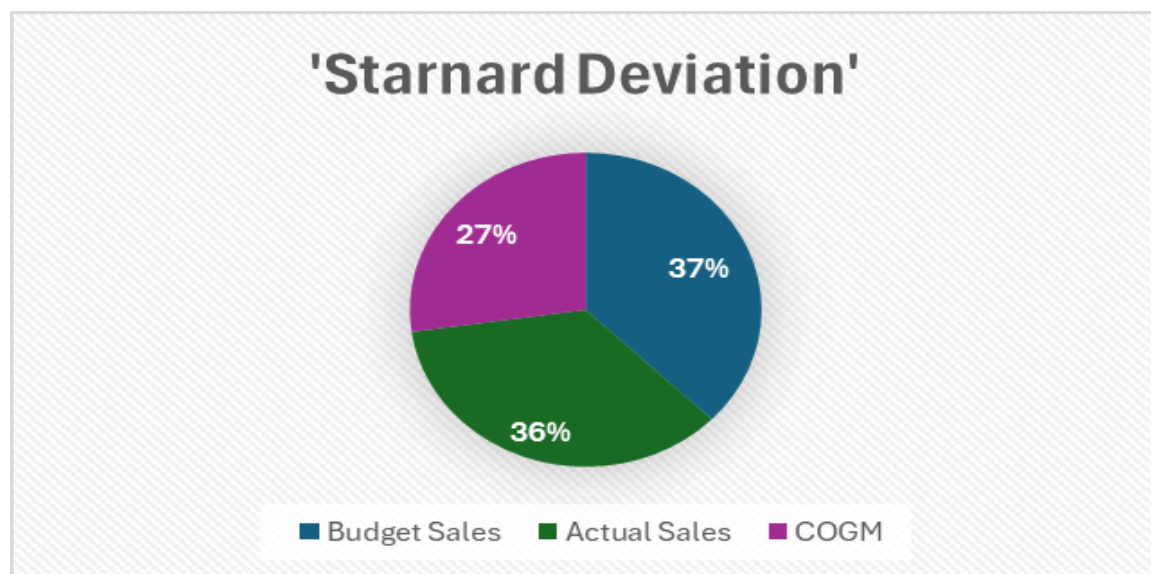


Figure 6: Standard Deviation from Aumovio's Sales (Sample Data).

Population

2021-2025 Sales	Mean	Median	Mode	Variance	Standard Deviation
Budget Sales	£27,515,998	£25,638,266		£30,520,000,000,000	£5,525,000
Actual Sales	£26,969,118	£27,187,309		£27,660,000,000,000	£5,260,000
COGM	£25,381,095	£25,504,436		£16,310,000,000,000	£4,033,000



Figure 7: Population Data from Aumovio's sales.

2021-2025 Sales	Standard Deviation
Budget Sales	£5,525,000
Actual Sales	£5,260,000
COGM	£4,033,000

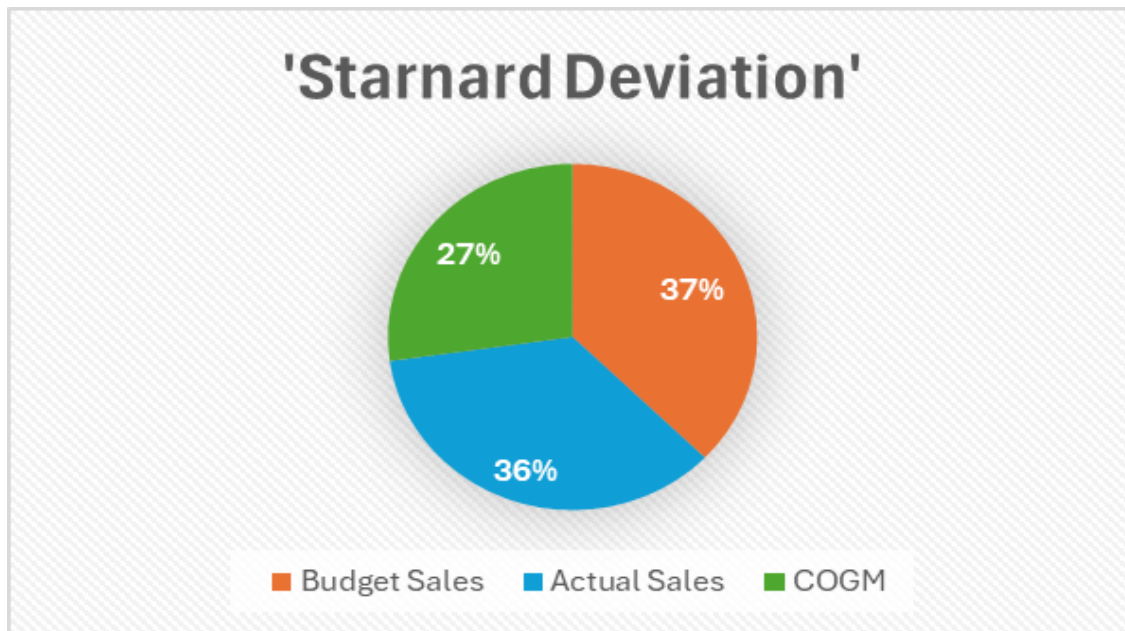


Figure 8: Standard Deviation from Aumovio's Sales Data (Population Data).

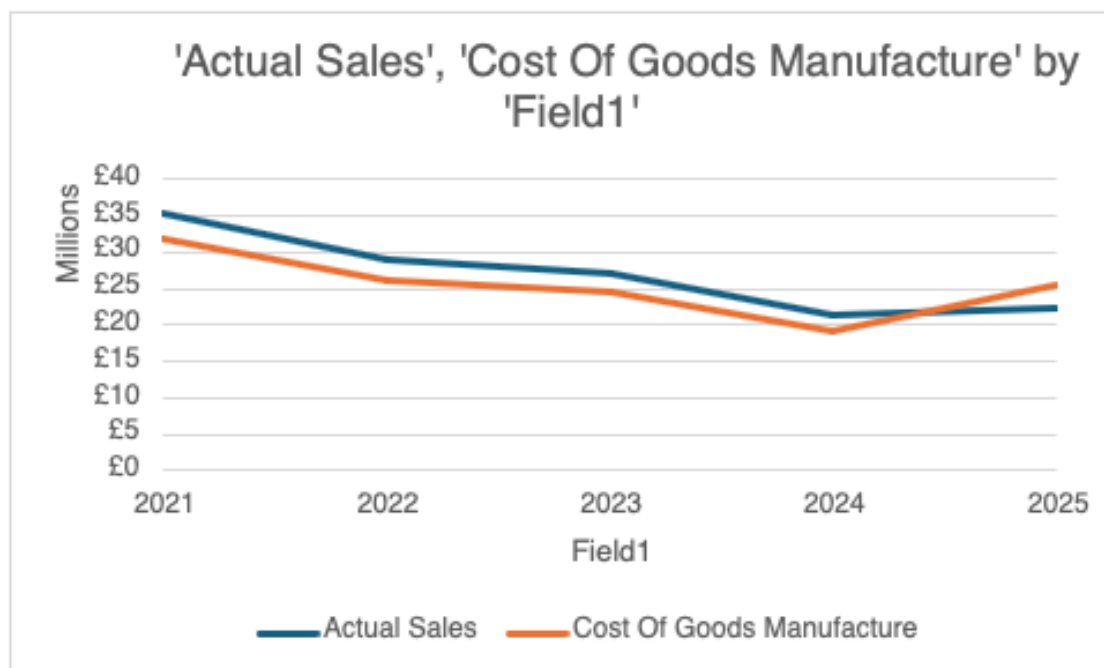


Figure 9: Negative correlation between sales and COGM.

Management Level	Structured	Semi-Structured	Unstructured
Operational	Inventory Management: Automatic Systems to reorder parts.	Production Scheduling: Balancing workloads to meet deadlines.	Incident Response: Controlling unexpected accidents or problems.
Managerial	Sales Analysis: Weekly reports of stock intake.	Budget Allocations: Specifying expenses over a period of time.	Talent Retention: Strategic efforts to keep skilled employees engaged.
Strategic	Warehouse Location: Optimising locations to minimize supply chain expenses.	Product Roadmap: Visual summary that outlines vision and priority.	Market Expansion: Expanding resources and global sales.

Figure 10: 3 by-3 Management Level matrix for Aumovio.