HUMAN FACTORS IN SECURITY

Donna Naadu Botchway (2415778)

Word Count: 2990

Robert Gordon University
28th November,2024

Table of Contents

Table of Figures

1.0. Executive Summary

This report analyses Buzzle Inc.'s security posture and culture, focusing on stakeholder interactions and system usage. Buzzle Inc. is a global leader in electronic component manufacturing. Manufactured components include buzzers, switches, and sensors. The data used is based on the company brief and interview scripts with employees. As shown in **Figure 1**, the analysis shows two risks: unauthorized access and privilege abuse, primarily caused by inadequate access controls and overly complex security measures. Most employees expressed concerns about the complexity of current security protocols and stressed the need for job-specific security training. These challenges showed Buzzle's need for human-centred security solutions. By focusing on the interactions of the production manager, J. Crowder, I identified vulnerabilities and recommend implementing job-specific training, Single Sign-On (SSO), multifactor authentication, a streamlined VPN for remote access, and secure portable hotspots for offsite workers to improve usability and security.

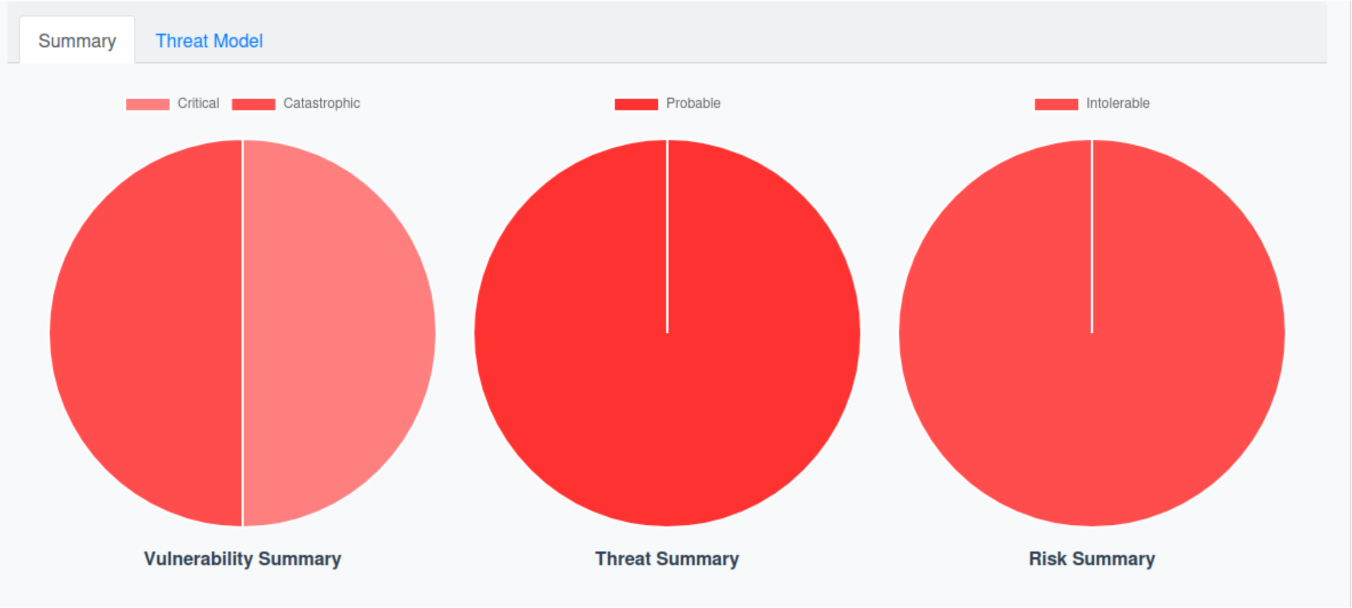


Figure 1: Risk Summary

2.0. System Modelling

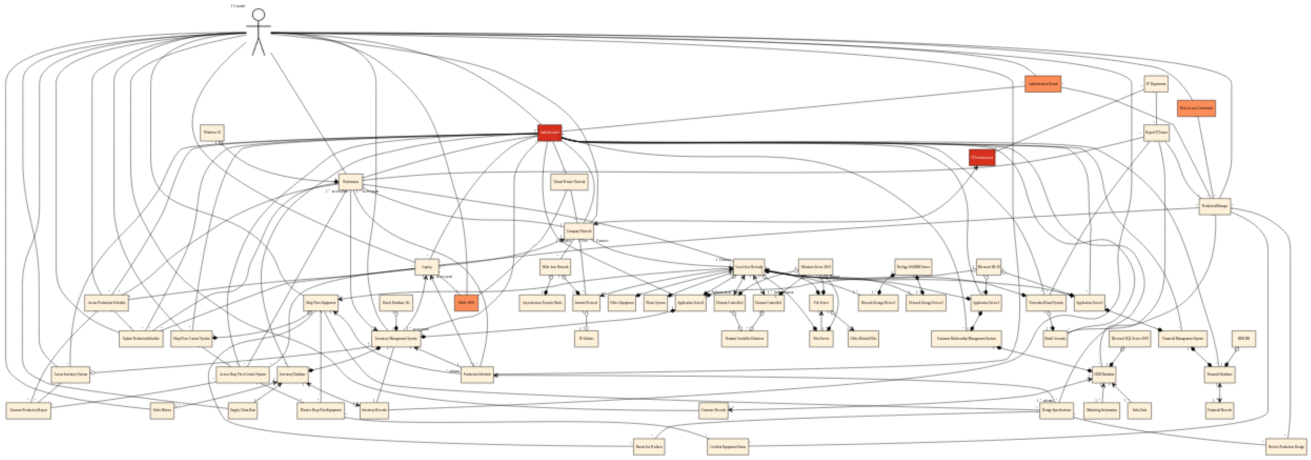


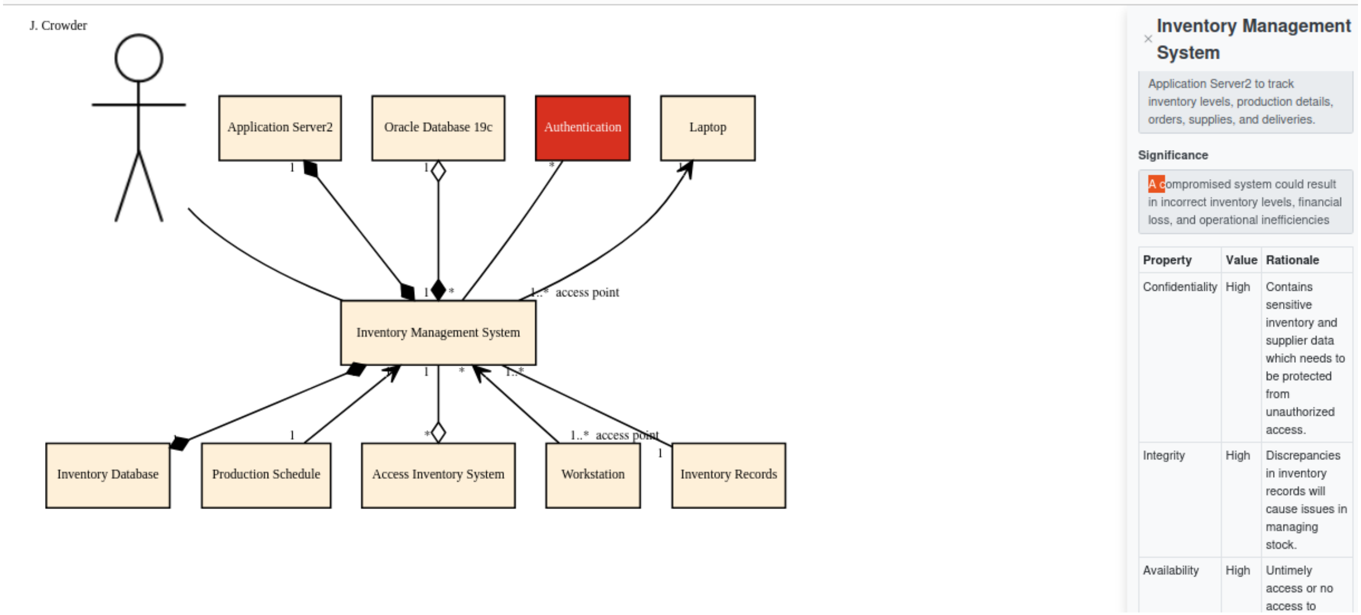
Figure 2: Complete Asset Model

Here I modelled the systems and assets, identifying their security properties and asset relationships. The full asset model is shown in **Figure 2**, but some details may not be clear. For more information, please refer to Appendix 1 for the parts and association tables.

The assets that the production manager interacts with includes:

2.1. Inventory Management System (IMS)

The Inventory Management System (IMS), as shown in **Figure 3**, is needed in resource allocation and production planning. The integrity of the IMS must be protected to prevent production errors and supply chain disruptions. It's availability and confidentiality also play important roles. The IMS has a composition relationship with the Microsoft IIS 10 Application Server, which hosts the system, and the Oracle Database 19c, which functions as the inventory database, storing data on inventory, orders, and supply chain. It also shares an association relationship with the production schedule, as it provides the data needed for creating schedules. Also, the IMS is associated with laptops and workstations which act as access points. IMS requires authentication to preserve its integrity and functionality.



Inventory Management System

Application Server2 to track inventory levels, production details, orders, supplies, and deliveries.

Significance

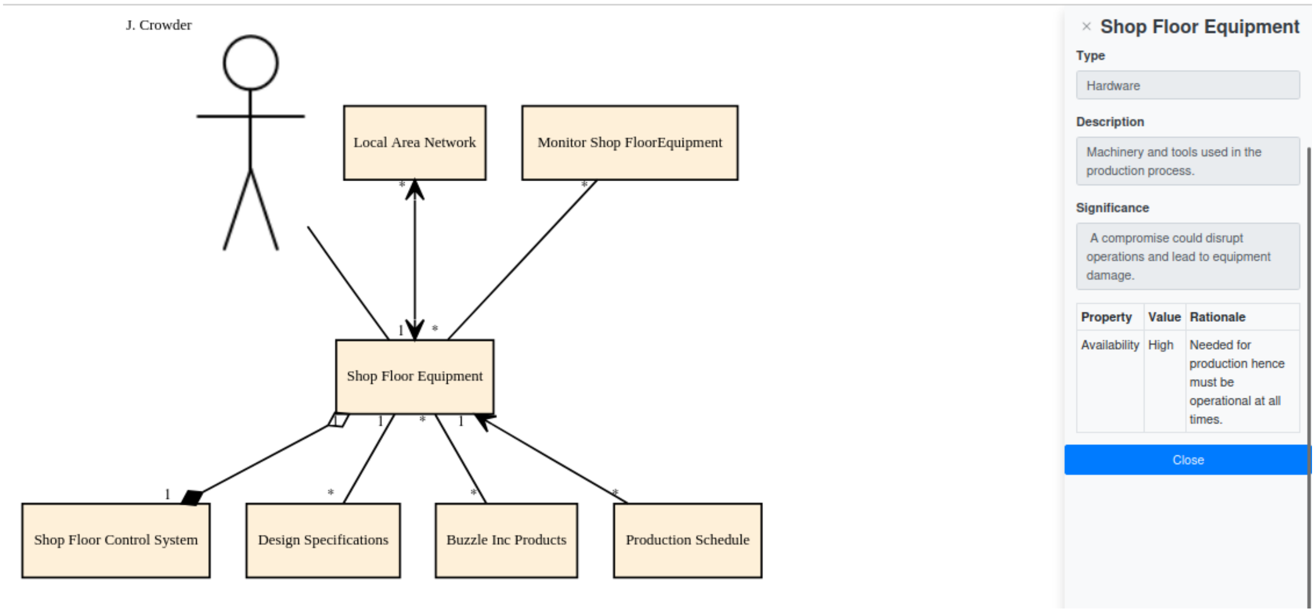
A compromised system could result in incorrect inventory levels, financial loss, and operational inefficiencies

Property	Value	Rationale
Confidentiality	High	Contains sensitive inventory and supplier data which needs to be protected from unauthorized access.
Integrity	High	Discrepancies in inventory records will cause issues in managing stock.
Availability	High	Untimely access or no access to

Figure 3:The Inventory Management System (IMS)

2.2. Shop Floor Equipment (SFE)

The Shop Floor Equipment (SFE), as shown in **Figure4**, is a needed hardware for manufacturing. The equipment's availability must be protected to minimize disruptions and delays that could result in financial losses. It has an aggregation relationship with the Shop Floor Equipment Control, which monitors and manages its operations while remaining functionally independent. The equipment shares an association with the Production Schedule, which relies on it to execute tasks, and with the network. This allows the production manager to remotely manage it to ensure continuous operations. Also, the equipment is associated with Buzzle Inc.'s products, as it produces them according to the design specifications to reach the desired outcome.



Shop Floor Equipment

Type

Hardware

Description

Machinery and tools used in the production process.

Significance

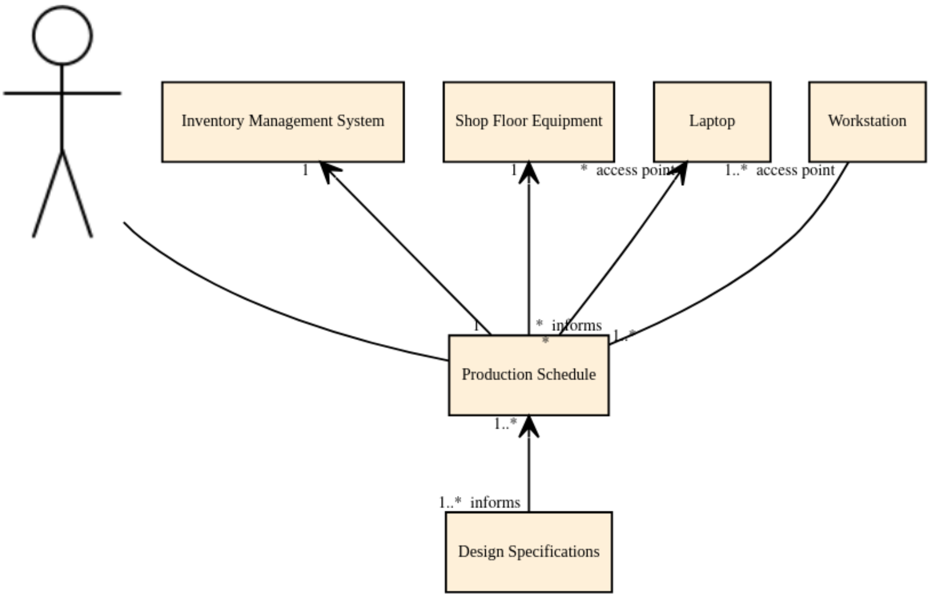
A compromise could disrupt operations and lead to equipment damage.

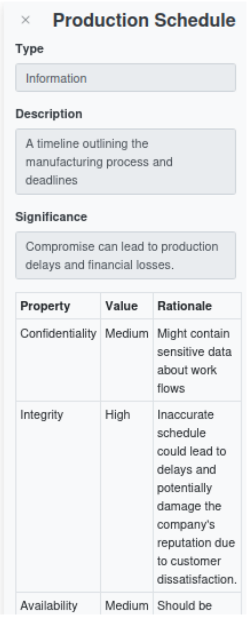
Property	Value	Rationale
Availability	High	Needed for production hence must be operational at all times.

Figure4:The Shop Floor Equipment

2.3. Production Schedule (PS)

The production schedule, as shown in **figure5**, is an information asset that contains the timeline that drives manufacturing. Its integrity must be protected as inaccuracies can lead to delays and damage Buzzle Inc's reputation. Its confidentiality and availability must also be protected as it contains data. The schedule is associated to assets including shop floor equipment that follows the schedule, laptops or workstations as access points, the inventory system that provides data on inventory and customer orders, and design specifications to ensure accurate production.




× Production Schedule

Type

Information

Description

A timeline outlining the manufacturing process and deadlines

Significance

Compromise can lead to production delays and financial losses.

Property	Value	Rationale
Confidentiality	Medium	Might contain sensitive data about work flows
Integrity	High	Inaccurate schedule could lead to delays and potentially damage the company's reputation due to customer dissatisfaction.
Availability	Medium	Should be

Figure 5: The Production Schedule (PS)

Refer to **Appendix1** for Buzzle Inc.'s assets and their associations.

3.0. Persona

3.1. Overview

I chose to model a persona based on the production manager, J. Crowder. He interacts directly with the Shop Floor Equipment, Inventory Management System (IMS), and Production Schedule. I used data from interview scripts and the company brief, along with online blogs about a day in the life of a production manager, to better understand his role. This gave me a better context on his daily workflows.

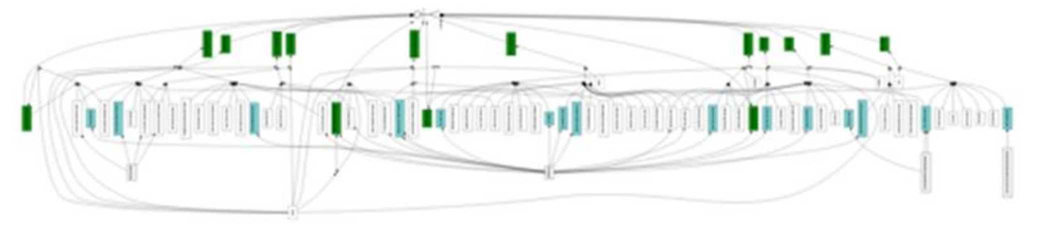
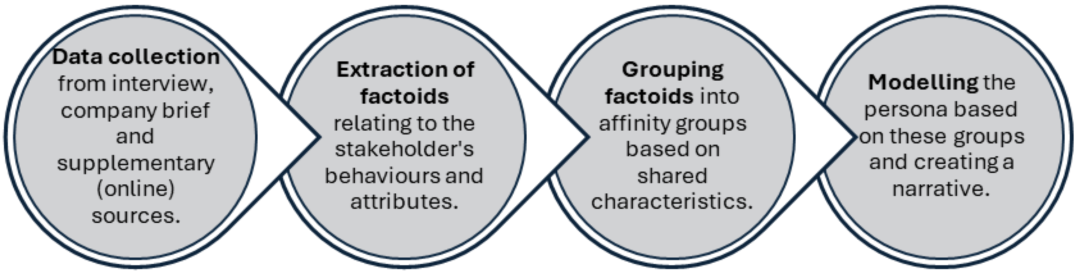


Figure6: Complete Persona Model

3.2. Methodology

I analysed and grouped factoids by shared attributes to form affinity groups. I identified characteristics such as a fast work tempo, little concern for security, works remotely, offsite security frustrations, and a focus on production tasks. I used theories like value-based and consequence-based to inform the persona development. From these, I modelled a persona for J. Crowder. I also included a persona narrative to clearly represent his needs and challenges.



Data collection from interview, company brief and supplementary (online) sources.

Extraction of factoids relating to the stakeholder's behaviours and attributes.

Grouping factoids into affinity groups based on shared characteristics.

Modelling the persona based on these groups and creating a narrative.

Figure7: Methodology

3.3. Characteristics

To better understand J. Crowder's role and challenges, I identified several key characteristics that influence his behaviour and interactions within the system, including:

3.3.1. *Works Remotely*

Crowder frequently works remotely. Production managers travel a lot for work to oversee operations and ensure efficiency. In his interview, he stated, “I spend a lot of time offsite, so I remotely manage some of the shop floor equipment to make sure everything’s running as it should.” He explained that his biggest challenge is the time it takes to get through security protocols, especially when working remotely. Crowder also revealed that, because he is often on the go, he connects to the company network using any available Wi-Fi and relies on his laptop for most tasks. “But most of the time, I’m working remotely, so I access the systems through my laptop,” he added.

Crowder connects to the company network from offsite locations using public Wi-Fi. He admitted, “Sometimes the security measures we have in place slow me down, especially when I’m in a hurry to fix something remotely.”

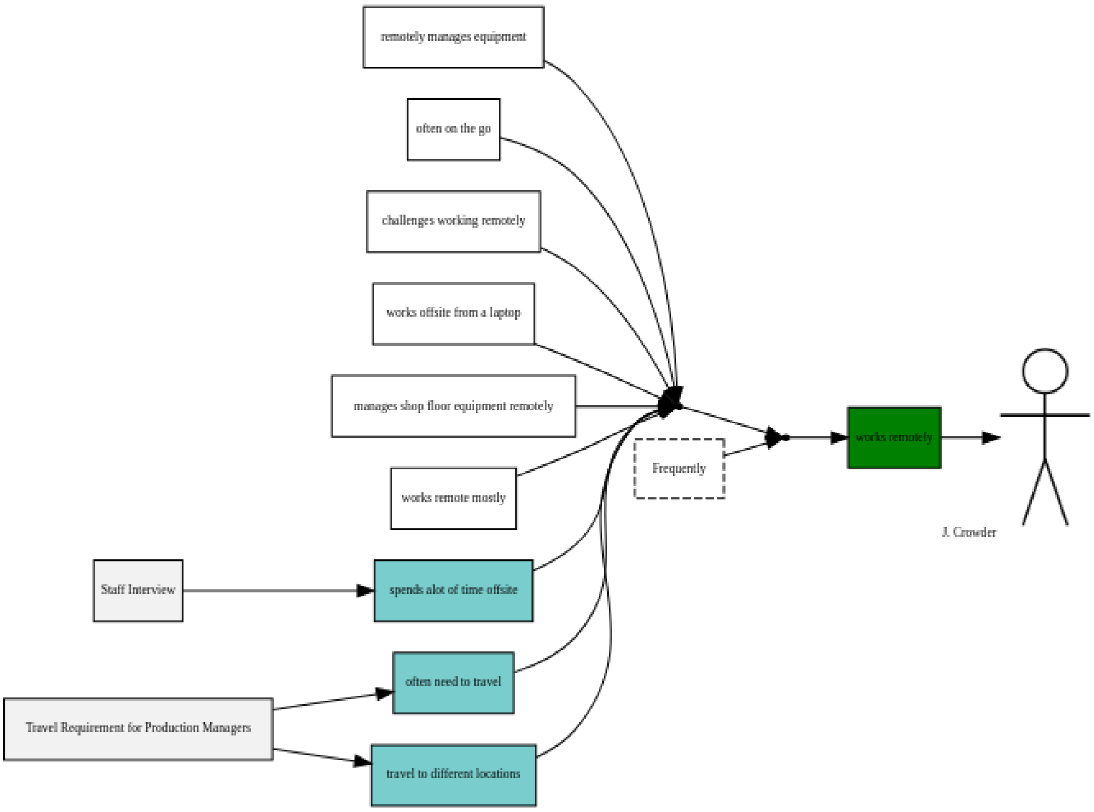
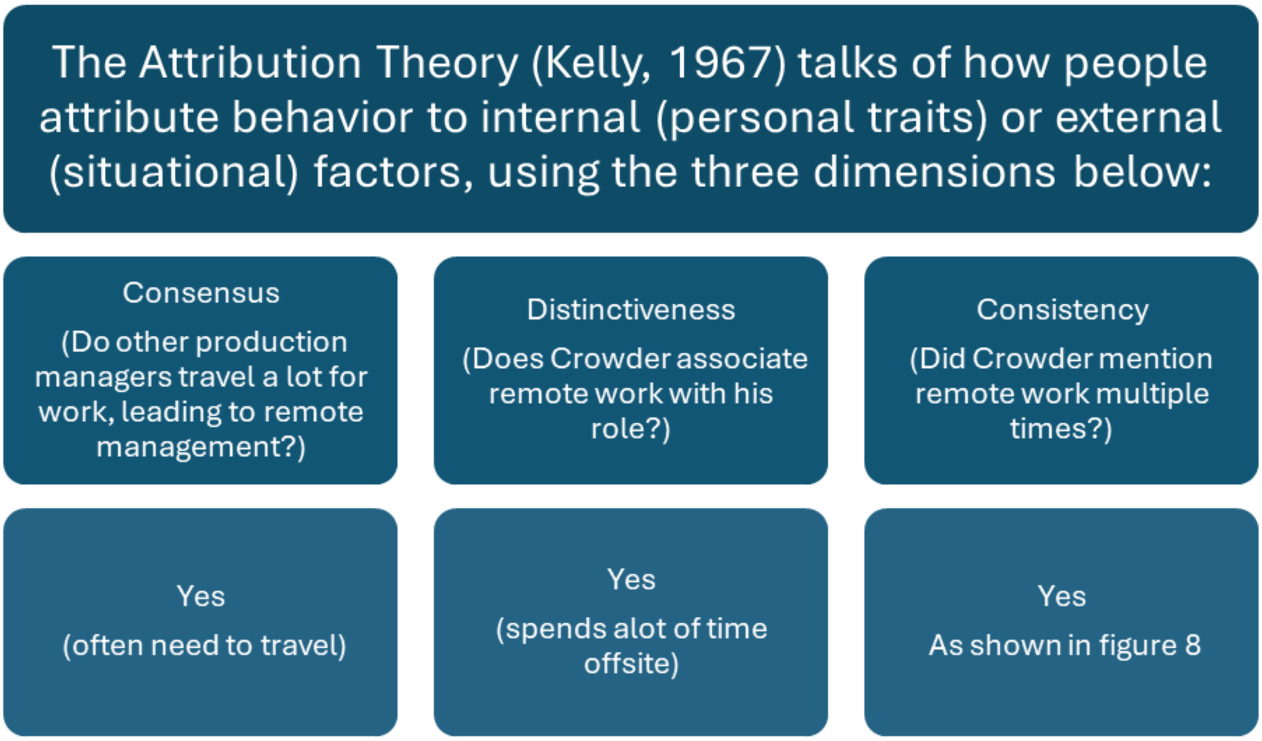

remotely manages equipment
often on the go
challenges working remotely
works offsite from a laptop
manages shop floor equipment remotely
works remote mostly
Frequently
works remotely
J. Crowder
Staff Interview
spends alot of time offsite
often need to travel
Travel Requirement for Production Managers
travel to different locations

Figure 8: Frequently Works Remotely

As shown in **figure9**, I used the attribution theory to analyse Crowder’s remote work habits to understand how the demands of his role, which often require meeting with clients or suppliers, quick responses, and flexibility, influence his need to work offsite.



The Attribution Theory (Kelly, 1967) talks of how people attribute behavior to internal (personal traits) or external (situational) factors, using the three dimensions below:

Consensus (Do other production managers travel a lot for work, leading to remote management?)	Distinctiveness (Does Crowder associate remote work with his role?)	Consistency (Did Crowder mention remote work multiple times?)
Yes (often need to travel)	Yes (spends alot of time offsite)	Yes As shown in figure 8

Figure 9: The Attribution Theory Explaining Crowder's Remote Work

However, working remotely exposes Crowder and the company to potential threats, such as man-in-the-middle attacks and data compromise. Crowder must use the available VPN, and the company must implement encryption and Multi-Factor Authentication (MFA), to minimize risks.

3.3.2. Little Concern for Security

Crowder shows little concern for security. He prioritizes efficiently managing production. Crowder believes security is less relevant to him, saying, “I don’t deal with a lot of sensitive information directly.” He also stated, “I’m not someone who’s going to dive deep into the details,” indicating a disinterest in security. When asked about encountering suspicious situations, he admitted, “I might just ignore it and keep working.” Crowder also, stated that security protocols like multiple logins are obstacles and that he’s been tempted to bypass them while admitting “I get why we have these measure”. He finds current security measures "not always practical" and admits that security checks slow him down.

When under pressure to keep production running smoothly, he values convenience over security. Crowder openly admits to using any available Wi-Fi to connect to the company network offsite, despite knowing the risks. As he stated, “I know it’s not ideal from a security standpoint, but it’s the most convenient option for me.” Crowder even acknowledged the insecurity of public Wi-Fi, saying, “… I’ve had to connect to the network over public Wi-Fi, and I couldn’t help but wonder how secure that connection really was… I needed to get the job done, so I just went ahead with it.”

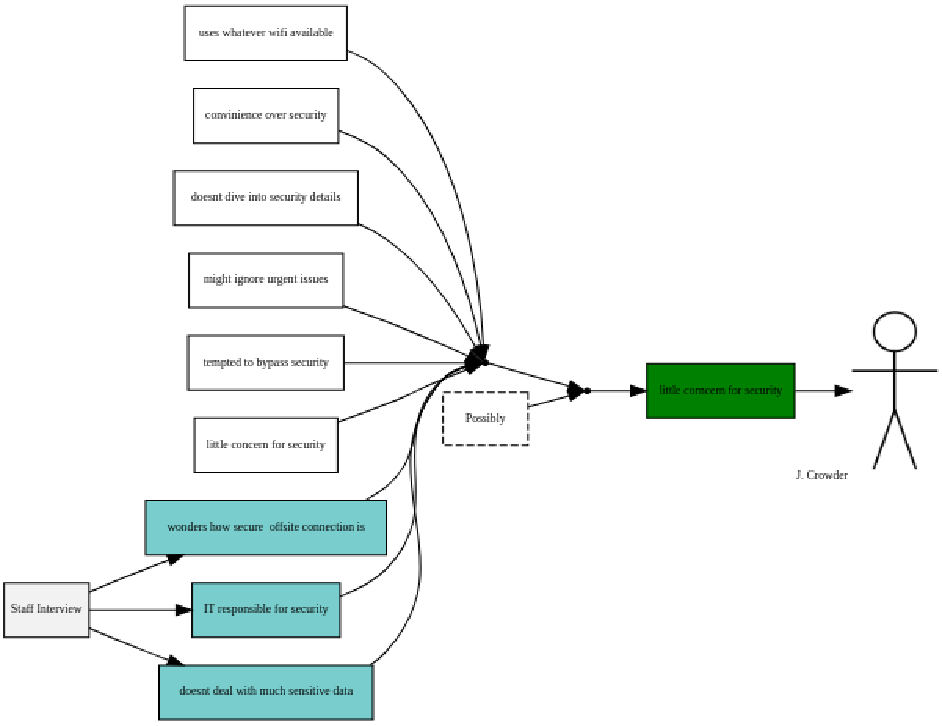
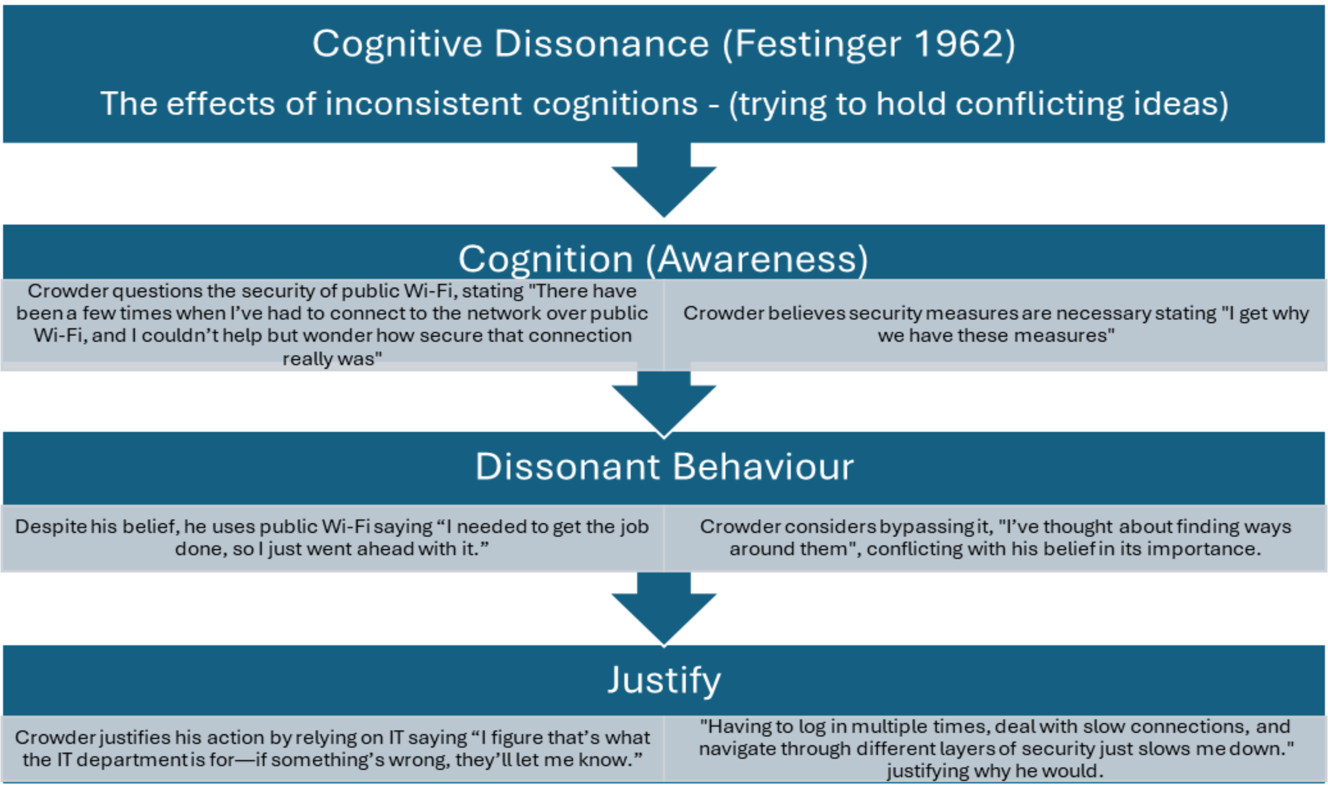

uses whatever wifi available
convinience over security
doesnt dive into security details
might ignore urgent issues
tempted to bypass security
little concern for security
wonders how secure offsite connection is
Staff Interview
IT responsible for security
doesnt deal with much sensitive data
Possibly
little concern for security
J. Crowder

Figure10:Possibly Little concerns for security

Figure11 identifies Crowder's cognitive dissonance. He understands the need for security and possible risks of using public Wi-Fi but chooses convenience due to his workload. This attitude poses a significant risk, especially with root access credentials over insecure networks.



Cognitive Dissonance (Festinger 1962)

The effects of inconsistent cognitions - (trying to hold conflicting ideas)

Cognition (Awareness)

Crowder questions the security of public Wi-Fi, stating "There have been a few times when I've had to connect to the network over public Wi-Fi, and I couldn't help but wonder how secure that connection really was"

Crowder believes security measures are necessary stating "I get why we have these measures"

Dissonant Behaviour

Despite his belief, he uses public Wi-Fi saying "I needed to get the job done, so I just went ahead with it."

Crowder considers bypassing it, "I've thought about finding ways around them", conflicting with his belief in its importance.

Justify

Crowder justifies his action by relying on IT saying "I figure that's what the IT department is for—if something's wrong, they'll let me know."

"Having to log in multiple times, deal with slow connections, and navigate through different layers of security just slows me down." justifying why he would.

Figure11: The Cognitive Dissonance Theory Explaining Crowder's Little Concerns for Security

Rather than enforcing rigid security protocols, the company could implement single sign-on (SSO) and job specific training to reduce friction without compromising security. This would make security measures more practical and acceptable to Crowder while mitigating the risks introduced by his current approach.

3.4. Persona Narrative

J. Crowder is a production manager who is often on the go, so he frequently works remotely, managing shop floor equipment and overseeing production schedules. His focus on production tasks is driven by the need to ensure smooth operations, but this often overshadows security concerns. His little concern for security, reliance on public Wi-Fi and tendency to bypass security protocols when they slow down production reflect a tension between efficiency and security. This behaviour emphasizes the importance of introducing practical, role-specific security measures that align with his fast-paced work environment while addressing offsite vulnerabilities.

For detailed information on persona, refer to **Appendix2**.

4.0. Human Behaviour and Usability

4.1. Overview

I modelled two scenarios reflecting J. Crowder's primary tasks: monitoring shop floor and creating or updating production schedule, to understand how he interacts with the system. Also, I included a Misusability scenario focused on inaccurate updates to the production schedule. These scenarios analyse task demands, system usability, and risks, with proposed antidotes to address errors and violations.

4.2. Task

4.2.1. Monitoring Shop Floor Equipment

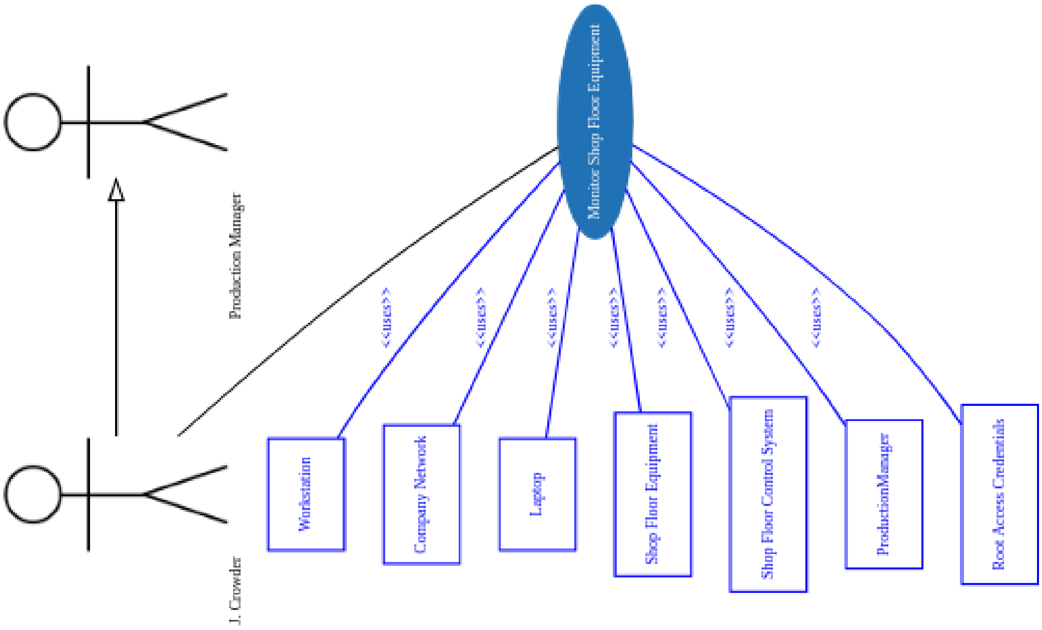


Figure12: Monitoring Shop Floor Equipment

Crowder's primary task involves monitoring shop floor equipment to ensure operational efficiency and prevent production delays or equipment damage. As a production manager, he must be vigilant, make quick decisions, and solve problems to meet delivery demands. The task demands technical access and immediate responsiveness, especially during critical production runs. It takes minutes, occurring hourly or more, especially during peak times.

Crowder stated, "My main job is to oversee the production schedule and make sure everything on the shop floor runs smoothly," highlighting his responsibility for equipment functionality. He added, "I remotely manage some of the shop floor equipment to make sure everything's running as it should," emphasizing the need for constant monitoring, even when on the go.

Crowder shared, *"Honestly, the biggest challenge is staying connected to the company's network when I'm off-site."* emphasizing the need for reliable network access. The company brief confirms that Crowder's depends on remote access, stating he manages equipment connected to the network off-site and has root access to most systems, reinforcing his expertise.

The online insights used from “day in the life of a production manager” describe their environment as one characterized by urgency, driven by customer demands and manufacturing constraints. Crowder’s task fits this high-pressure scenario, requiring real-time visibility to avoid disruptions (Ike, 2024).

This task requires a laptop, shop floor control system, root access, and network connection. Crowder explained, “I use my workstation like everyone else, but most of the time, I’m working remotely, so I access the systems through my laptop.”

Using a consequence-based approach, I highlight the criticality of this task. Effective monitoring mitigates risks like production delays and equipment damage, which could lead to missed deliveries and financial losses. The shop floor control system provides real-time visibility, enabling Crowder to make proactive decisions and maintain operational efficiency (Ike, 2024).

4.2.1.1. Task Narrative

Crowder’s role as a production manager requires him to prioritize the operation of shop floor equipment. This ensures that production targets are met, and downtime is minimized. He relies on the shop floor control, network access, and real-time data to carry out this task. If this task fails, there will be delays, equipment malfunctions, and reduced production efficiency. Considering Crowder’s role and expertise, assigning this task to Crowder is justified. Buzzle Inc. can further support Crowder’s ability to perform this task effectively by implement enhanced monitoring tools with automated reports. This would alert him to issues and keep him updated on the equipment status reducing manual checks and increasing response time.

4.3. Misusability

4.3.1. Inaccurate Update of Production Schedule

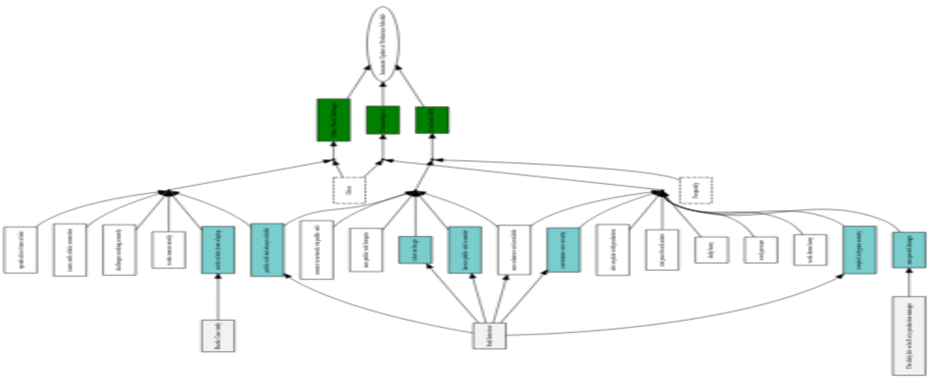
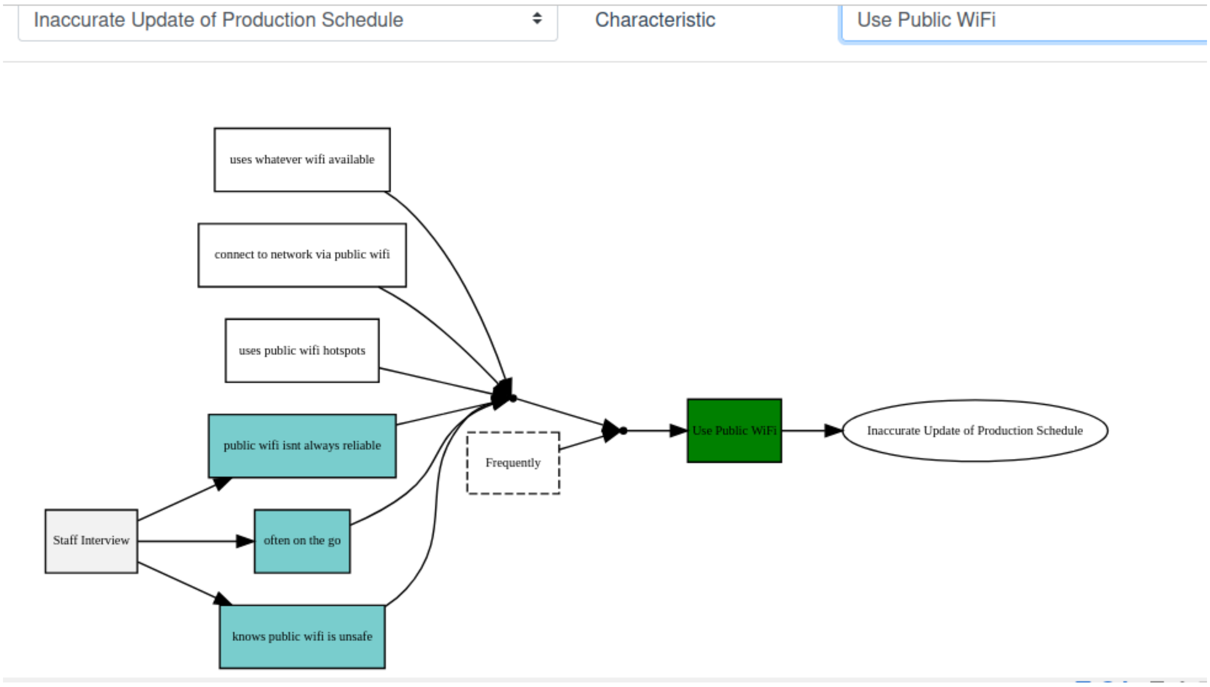


Figure 13: Full Model on Inaccurate Update of Production Schedule

Crowder updates the production schedule hourly throughout the day, and remotely when on the go, based on customer orders and inventory levels. These updates, typically taking minutes, can extend during peak periods with frequent changes. Accuracy and access to real time data is vital, which makes it a high-demand task.


Inaccurate Update of Production Schedule ⬍ Characteristic Use Public WiFi

uses whatever wifi available
connect to network via public wifi
uses public wifi hotspots
public wifi isnt always reliable
Staff Interview
often on the go
knows public wifi is unsafe
Frequently
Use Public WiFi
Inaccurate Update of Production Schedule

Figure14: Use Public Wi-Fi Characteristic Model on Inaccurate Update of Production Schedule

However, Crowder's reliance on public Wi-Fi and focus on speed over security increases error risks. Crowder admits, "Public Wi-Fi isn't always reliable, and it can be a pain to deal with connection issues." Despite knowing the potential security risks, he prioritizes convenience, stating, "I connect to whatever Wi-Fi is available... it's the most convenient option for me." He further justified his actions, explaining, *"When you're under pressure to keep production running smoothly, the last thing you want is to be slowed down by security checks."* These frustrations with network instability and fast work pace results in high risk of errors.

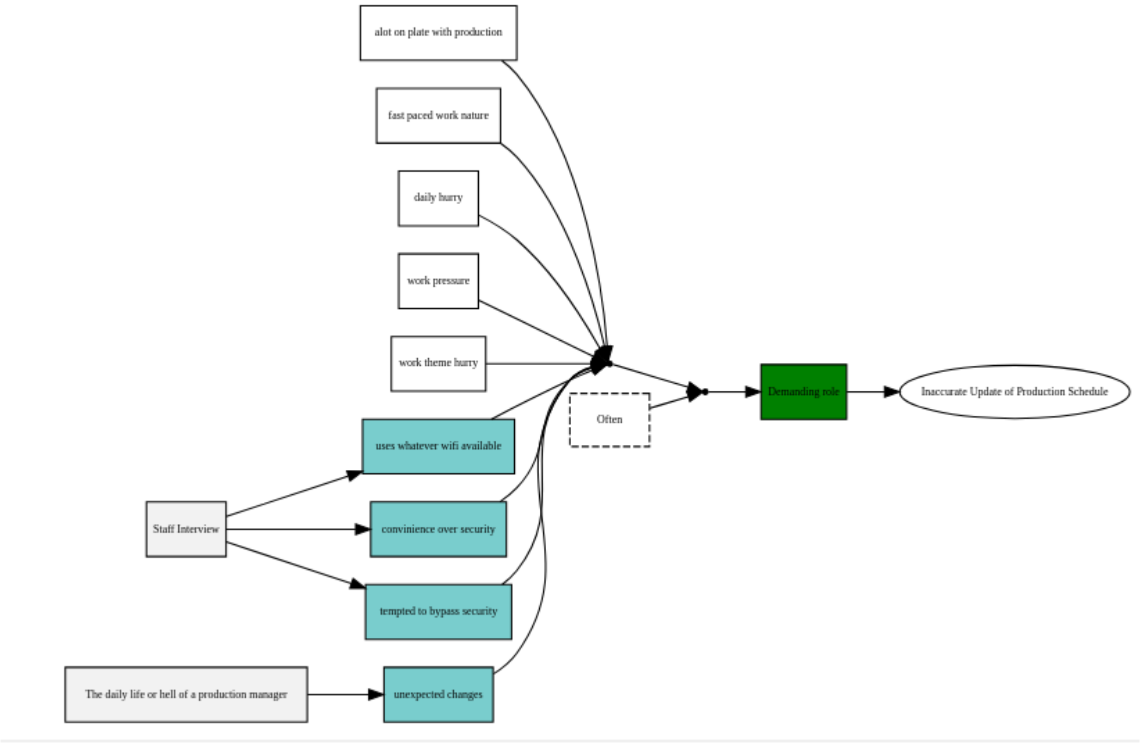
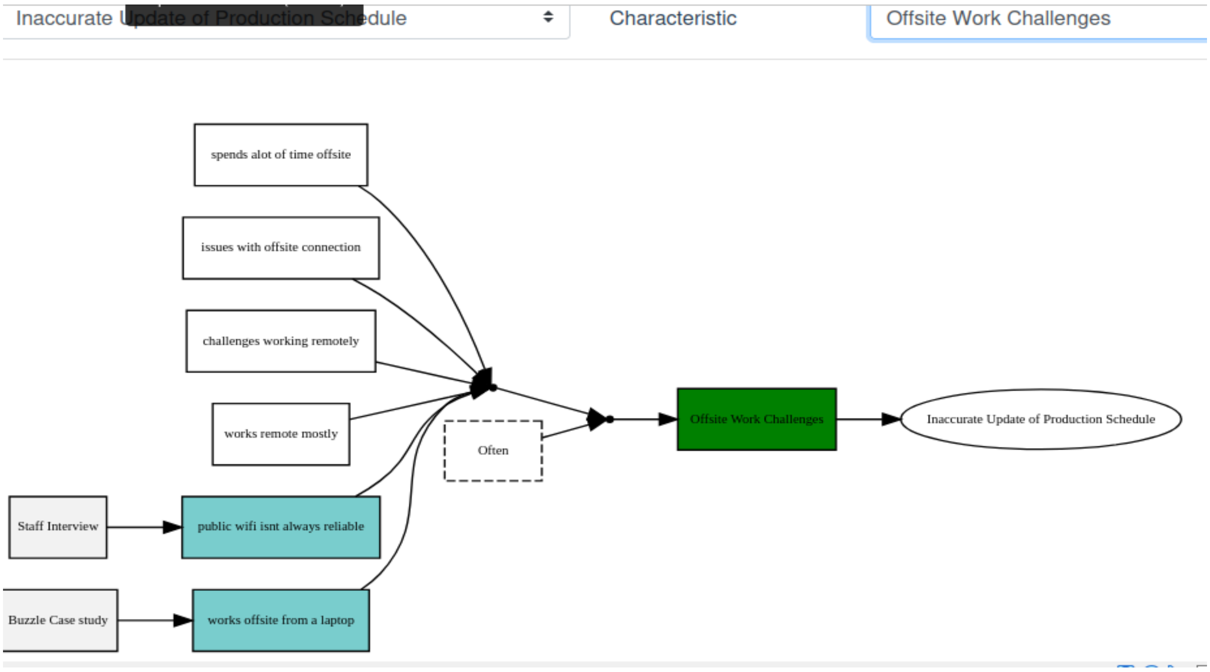

alot on plate with production
fast paced work nature
daily hurry
work pressure
work theme hurry
uses whatever wifi available
Staff Interview
convinience over security
tempted to bypass security
The daily life or hell of a production manager
unexpected changes
Often
Demanding role
Inaccurate Update of Production Schedule

Figure15:" Demanding Role" Model on Inaccurate Update of Production Schedule

Crowder’s decisions reflect his high-pressure environment. From the secondary data sources, production managers face urgency driven by customer demands and manufacturing constraints. The logic behind Crowder’s decisions can be better understood through a value-based approach. His decisions stem from a value-driven choice between speed and security. As a production manager, he faces immense pressure to meet customer demands and ensure smooth operations, making speed needed. He perceives the time spent on security checks as a costly trade-off, especially when tasks must be completed quickly.



Inaccurate [redacted]edule ⬍ Characteristic Offsite Work Challenges

spends alot of time offsite
issues with offsite connection
challenges working remotely
works remote mostly
Often
Offsite Work Challenges
Inaccurate Update of Production Schedule
Staff Interview
public wifi isnt always reliable
Buzzle Case study
works offsite from a laptop

Figure16: "Offsite Work Challenges" Model on Inaccurate Update of Production Schedule

Crowder also complains about logging in multiple times, slow connections, and navigating layers of security, which he feels slow him down. He suggests, "We need to find a better balance between security and usability to streamline security measures." This system flaw compromises security and increases the likelihood of human error.

Given the frequency of these updates, which occur throughout the day, Buzzle Inc. must address the usability challenges in Crowder’s workflow. Set up VPN auto-connect for secure remote connections and provide secure mobile hotspots to eliminate reliance on public Wi-Fi. Also, incorporating system features that flag inventory discrepancies before updates are finalized would help reduce manual checks and improve accuracy. By addressing usability challenges, the company can balance security and efficiency, reducing the likelihood of errors and system violations.

Please refer to [Appendix3](#) for information on the other task.

5.0. Threat Modelling

5.1. Overview

As shown in **figure17**, I modelled the data flow between entities, processes, and datastores, focusing on the production management assets. The data flow showed how data moves between different levels and trust boundaries where possible vulnerabilities exist. This helped me identify the vulnerabilities. I also used the STRIDE framework to identify threats explained in the risk model. I then referred to CAPEC to find real world attack scenarios that could use the threats to exploit the identified vulnerabilities.
For details, please refer to Appendix4.

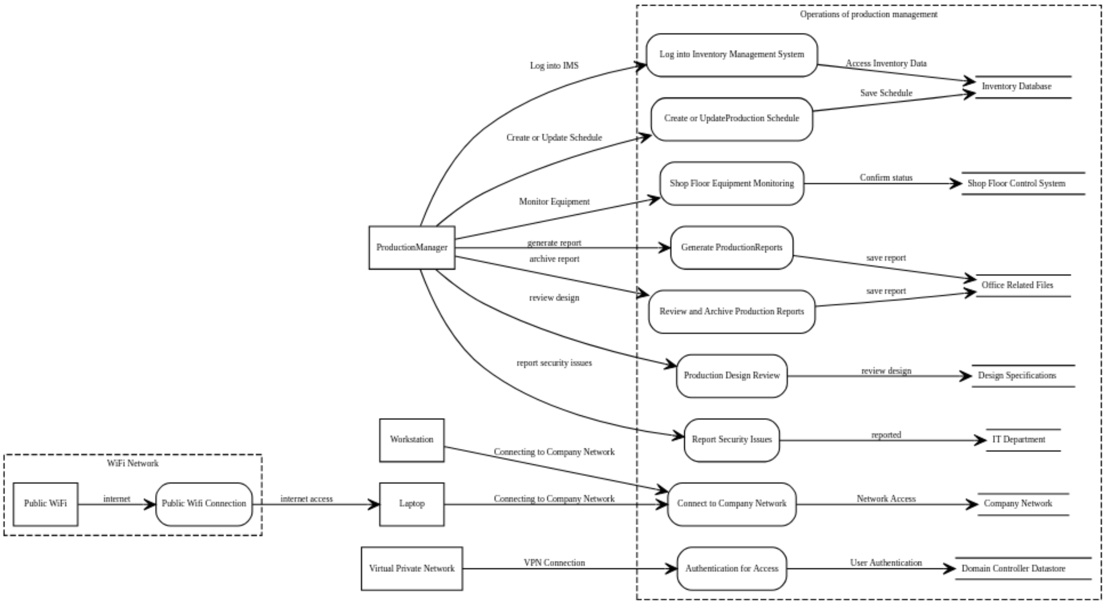


Figure 17: The Production Management Data Flow

5.2. Risk

For each risk, I analysed its threat and vulnerability, impact on assets, and the validity of its execution.

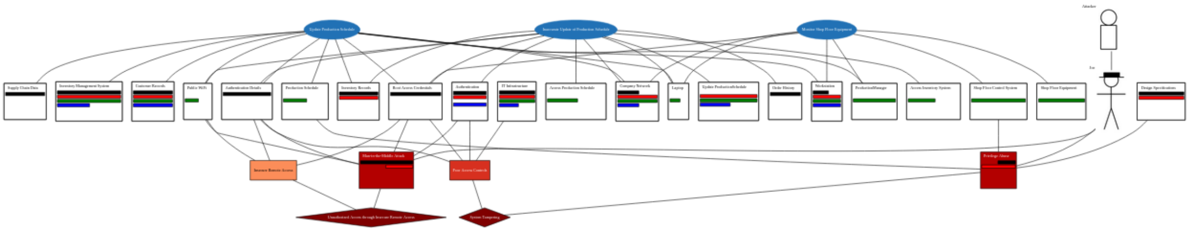


Figure 18: The Complete Risk Model

5.2.1. *Unauthorized Access through MITM Attack*

Joe, the attacker, gains unauthorized access to Buzzle Inc.'s internal systems by exploiting insecure remote access through a Man-in-the-Middle (MITM) attack. This exposes the authentication process including authentication details and root access credentials. A MITM attack (CAPEC-94) occurs when an attacker intercepts unencrypted data transmitted over public Wi-Fi.

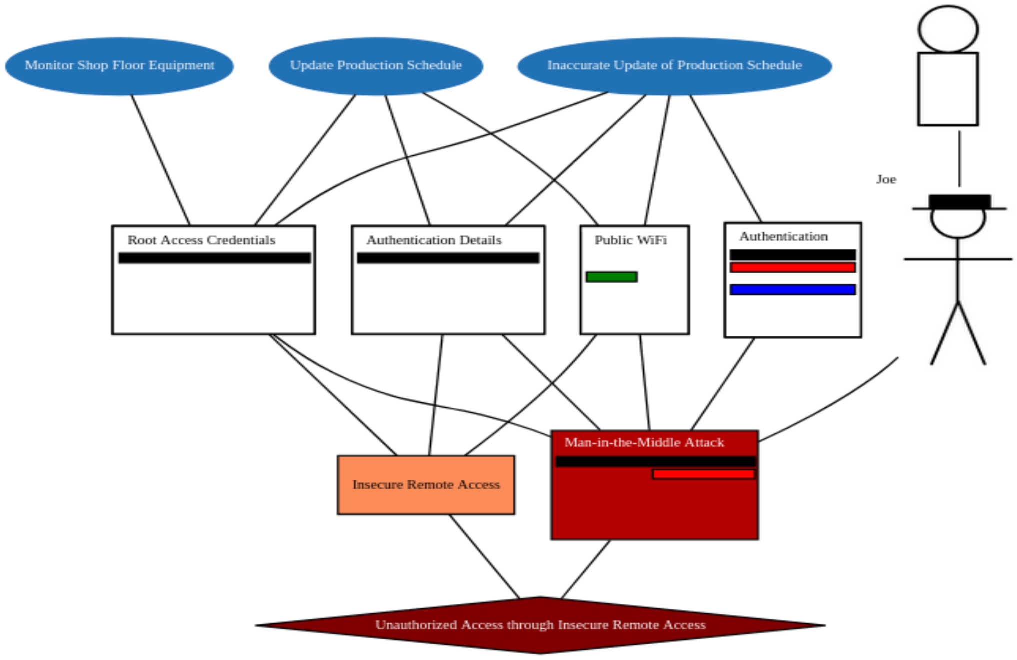

Monitor Shop Floor Equipment
Update Production Schedule
Inaccurate Update of Production Schedule
Joe
Root Access Credentials
Authentication Details
Public WiFi
Authentication
Man-in-the-Middle Attack
Insecure Remote Access
Unauthorized Access through Insecure Remote Access

Figure19: Unauthorized Access through MITM

In this scenario, Joe sets up a rogue Wi-Fi access point, and Crowder connects to public Wi-Fi without using a VPN. This exposes his login credentials to interception. Joe using Wireshark captures these details including Crowder's root access, granting him unauthorized access to the company network. This breaches confidentiality and exposes sensitive systems and data, as shown in ***Figure19***.

The trust boundary is breached when Crowder connects to the company system via public Wi-Fi network, without using a VPN. This attack is highly plausible because public Wi-Fi is often unencrypted, making them vulnerable to interception via packet sniffers and rogue access points (Buxton,2024). MITM tools like Wireshark are readily available and easy to use. Furthermore, Crowder's frequent use of public networks, and prioritizing convenience over security, makes him an ideal target. As Crowder himself confesses, "I connect to the company network using whatever Wi-Fi is available… but it's the most convenient option for me." His disregard for security protocols highlights the risks of insecure remote access, allowing this exploit to succeed. This risk has severity score of 9 and is intolerable.

5.2.2. *System Tampering through Privilege Abuse*

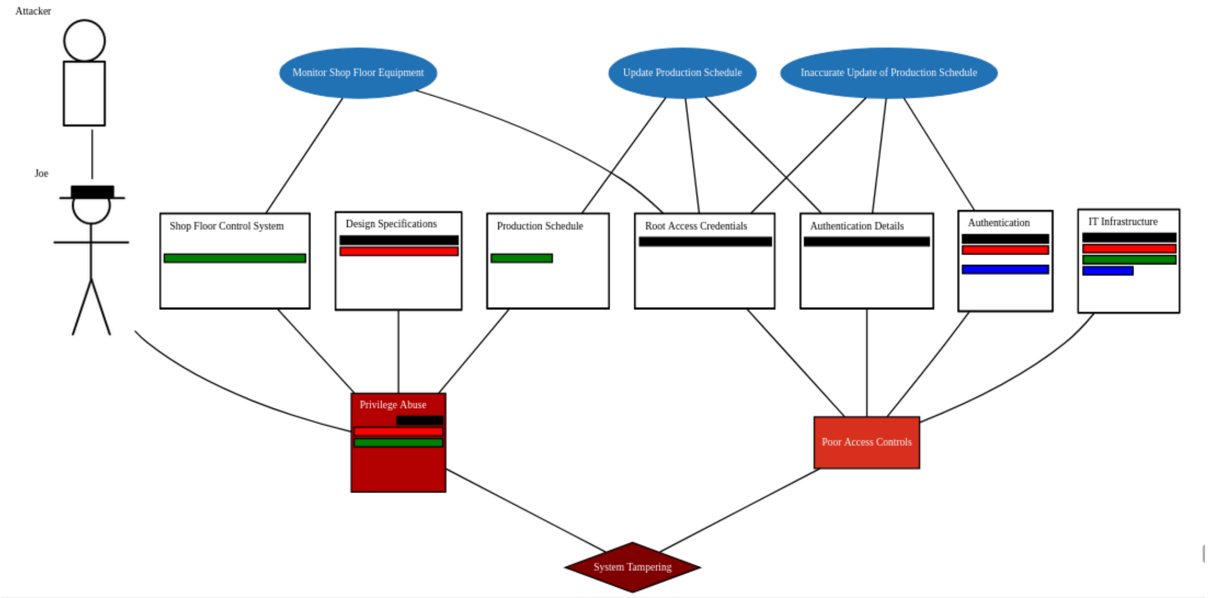


Figure20: System Tampering Through Privilege Abuse

Joe exploits Crowder's admin privileges to tamper with production schedules and shop floor configurations. This compromises data integrity and disrupts Buzzle Inc's operations. A Privilege Abuse attack (CAPEC-122) takes advantage of excessive permissions, enabling the attacker to alter system, such as production schedules or quality control settings.

The trust boundary between Crowder's role and company systems is breached when the system assumes Crowder's authentication credentials are sufficient. The system trusts that once Crowder is authenticated, he has the authority to perform any action. However, weak access controls allow the attacker to exploit this to gain unrestricted system access.

Crowder's admin-level access, which exceeds his role, increases the risk of both accidental and malicious misuse. This attack scenario involves the "Elevation of Privilege" and "Tampering" components of STRIDE. Once an attacker gains access to Crowder's credentials, like through MITM attack, they can modify critical systems without escalating privilege, leading to tampered data. As shown in **Figure 20**, the attack affects the integrity of altered systems like the shop floor control system. This results to delays, defects, and financial and reputational damage.

The attack is highly plausible due to Crowder's unrestricted admin access, and his attitude towards security. Privilege misuse is a common attack method (Redmond, 2023), and the lack of role-based access control makes it easy for Joe to exploit Crowder's privileges without triggering alerts. As the company brief notes, "He has little concern for security, much to the annoyance of Trafford, given his root access to the majority of systems." Crowder's dismissive attitude is highlighted when he says, "I might just ignore it and keep working,". This attitude exposes the system to exploitation and reinforces the need for access control measures like least privilege and multifactor authentication. This risk is intolerable and scores 9.

See Appendix4 for more on data flows, and risk breakdown.

6.0. References

1. MITRE (2018) 'CAPEC-94: Adversary in the Middle (AiTM)'. Available at: https://capec.mitre.org/data/definitions/94.html (Accessed: 11 November 2024).
2. MITRE (2018) 'CAPEC-122: Privilege Abuse'. Available at: https://capec.mitre.org/data/definitions/122.html (Accessed: 11 November 2024).
3. Clooper (2024) 'Travel Requirement for Production Managers: [Checklist + Guide]', Clooper Blog, 24 July. Available at: https://clooper.com/blog/travel-requirement-for-production-managers-checklist-guide (Accessed: 11 November 2024).
4. Fastems (2024) 'The daily life (or hell) of a production manager', Fastems Blog, 4 May. Available at: https://www.fastems.com/blog/the-daily-life-or-hell-of-a-production-manager/ (Accessed: 11 November 2024).
5. Alpha Manufacturing (2024) 'A day in the life of a manufacturing production manager', Alpha Manufacturing News, 11 November. Available at: https://www.alphamanufacturing.co.uk/news/a-day-in-the-life-of-a-manufacturing-production-manager (Accessed: 11 November 2024).
6. Ike, C. (2024) 'What is Shop Floor Control Management and Why Is It Important?', Uphance Blog, 9 September. Available at: https://www.uphance.com/blog/shop-floor-control-management/ (Accessed: 11 November 2024).
7. Buxton, O. (2024) 'Public Wi-Fi: A guide to the risks and how to stay safe', Norton Blog, 16 September. Available at: https://us.norton.com/blog/privacy/public-wifi (Accessed: 24 November 2024).
8. Melnick, J. (2017) 'Privilege Abuse: Threat Alert', Netwrix Blog, 24 October. Available at: https://blog.netwrix.com/2017/10/24/privilege-abuse-threat-alert/ (Accessed: 24 November 2024).
9. Redmond, M. C. (2023) 'Exploring Privilege Abuse in Cyber Security: Uncovering the Impact and Strategies to Prevent Unauthorized Access and Misuse of Data', CDOMagazine, 11 April. Available at: https://www.cdomagazine.tech/opinion-analysis/article_94796266-d85c-11ed-b27b-f7a62e3cf746.html (Accessed: 24 November 2024).
10. PrivacySavvy (2024) 'Insider Threats in 2024: 30 Eye-opening Statistics', PrivacySavvy, 30 July. Available at: https://privacysavvy.com/security/business/insider-threats-statistics/ (Accessed: 24 November 2024).

7.0. Appendices

7.1. Appendix 1: Asset Analysis

7.1.1. Asset Property

7.1.1.1. Inventory Database

Table 6-57. Inventory Database attributes

Attribute	Description
Type	Information
Description	Oracle Database 19c dedicated to monitor inventory levels, order history, and supply chain data
Significance	Provides data needed for supply chain management and operational efficiency. Compromise could result in inaccurate inventory records and financial losses.

Table 6-58. Inventory Database environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Contains data required for supply chain management and order fulfilment considered as sensitive.) Integrity : High (For effective operations both in supply chain and order fulfilment, accurate in data is required.) Availability : Medium (Needed for day to day activities but scheduled maintenance which would cause downtime is understandable) Accountability : High (For proper management of inventory data, actions by users need to be monitored and tracked.)

7.1.1.2. Inventory Management System

Table 6-59. Inventory Management System attributes

Attribute	Description
Type	Systems

Attribute	Description
Description	Hosted on a Microsoft IIS 10 Application Server2 to track inventory levels, production details, orders, supplies, and deliveries.
Significance	A compromised system could result in incorrect inventory levels, financial loss, and operational inefficiencies

Table 6-60. Inventory Management System environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Contains sensitive inventory and supplier data which needs to be protected from unauthorized access.) Integrity : High (Discrepancies in inventory records will cause issues in managing stock.) Availability : High (Untimely access or no access to inventory records will cause issues in fulfilling orders leading to operational inefficiency) Accountability : Low (A need to track who updates inventory data.)

7.1.1.3. Inventory Records

Table 6-61. Inventory Records attributes

Attribute	Description
Type	Information
Description	Information on inventory levels and movements.
Significance	Unauthorized access could result in inventory discrepancies and financial losses.

Table 6-62. Inventory Records environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Contains sensitive inventory data) Integrity : High (Accurate inventory levels requires changes made to be authorized)

7.1.1.4. Laptop

Table 6-69. Laptop attributes

Attribute	Description
Type	Hardware
Description	Portable computers used by employees for work especially offsite.
Significance	If compromised, they can serve as entry points for attackers to access corporate networks.

Table 6-70. Laptop environmental attributes

Environment	Security Property (Rationale)
Default	Availability : Medium (Must be operational as it is important for employee productivity during offsite work)

7.1.1.5. Microsoft IIS 10

Table 6-77. Microsoft IIS 10 attributes

Attribute	Description
Type	Software
Description	A web server that hosts applications.
Significance	A possibility of unauthorized access and change to sensitive data when there is a breach.

Table 6-78. Microsoft IIS 10 environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Contains sensitive data that must be protected to prevent breaches.) Integrity : High (Data accuracy in the applications hosted by this software is key for day to day task hence tampering must be prevented.) Availability : High (Downtime affects access and day to day activities)

Environment	Security Property (Rationale)
	Accountability : Medium (Track access to deter unauthorized changes.)

7.1.1.6. Microsoft SQL Server 2019

Table 6-79. Microsoft SQL Server 2019 attributes

Attribute	Description
Type	Software
Description	Hosts the CRM DB enabling storing and retrieving data as requested by other software applications.
Significance	Compromising can lead to data corruption, unauthorized access, data loss and loss of reputation.

Table 6-80. Microsoft SQL Server 2019 environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Contains sensitive customer data which when leaked could cause reputational loss to the company and financial loss) Integrity : High (Unauthorized changes made to configurations could compromise data) Availability : High (Should be operational for the use of the CRM DB)

7.1.1.7. Monitor Shop FloorEquipment

Table 6-81. Monitor Shop FloorEquipment attributes

Attribute	Description
Type	Process
Description	An authorized user via the control system monitors the performance of equipment on the shop floor.
Significance	Monitoring systems help to identify issues, which could lead to equipment failure and resolve early

Table 6-82. Monitor Shop FloorEquipment environmental attributes

Environment	Security Property (Rationale)
Default	Availability : High (Not monitoring systems would mean that operators may miss issues which could lead to equipment failure)

7.1.1.8. Access Inventory System

Table 6-3. Access Inventory System attributes

Attribute	Description
Type	Process
Description	Users have the ability to access the inventory management system.
Significance	If unauthorized access occurs, an attacker could tamper with inventory levels, steal inventory data, or cause disruptions in order processing

Table 6-4. Access Inventory System environmental attributes

Environment	Security Property (Rationale)
Default	Availability : Medium (Unavailability of this can disrupt inventory management)

7.1.1.9. Access Production Schedule

Table 6-5. Access Production Schedule attributes

Attribute	Description
Type	Process
Description	Users have the ability to access the production schedule.
Significance	If compromised, attackers could modify production timelines, causing delays or mismanagement in manufacturing processes

Table 6-6. Access Production Schedule environmental attributes

Environment	Security Property (Rationale)
Default	Availability : Medium (Unavailability of this would negatively impact production and operational planning)

7.1.1.10. Access Shop Floor Control System

Table 6-7. Access Shop Floor Control System attributes

Attribute	Description
Type	Process
Description	Authorized users have access to the shop floor control system, which monitors production and the shop floor equipment
Significance	Access to the control system is access to the shop floor operations

Table 6-8. Access Shop Floor Control System environmental attributes

Environment	Security Property (Rationale)
Default	Availability : High (Access to this is needed to manage and monitor shop floor operations)

7.1.1.11. Application Server1

Table 6-9. Application Server1 attributes

Attribute	Description
Type	Hardware
Description	Runs a Microsoft IIS 10 that hosts Customer Relationship Management System.
Significance	There is a possibility of application downtime and unauthorized access when the system is compromised

Table 6-10. Application Server1 environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : Medium (Protect sensitive application data.) Integrity : Medium (Application data must be reliable and unaltered to achieve operational efficiency) Availability : High (Needed for maintaining application uptime.) Accountability : Low (Monitor application access and usage.)

7.1.1.12. Application Server2

Table 6-11. Application Server2 attributes

Attribute	**Description**
Type	Hardware
Description	Runs a Microsoft IIS 10 that hosts Inventory management system.
Significance	There is a possibility of application downtime and unauthorized access when the system is compromised

Table 6-12. Application Server2 environmental attributes

Environment	**Security Property (Rationale)**
Default	Confidentiality : Medium (Protect sensitive application data.) Integrity : Medium (Application data must be reliable and unaltered to achieve operational efficiency) Availability : High (Needed for maintaining application uptime.) Accountability : Low (Monitor application access and usage.)

7.1.1.13. Application Server3

Table 6-13. Application Server3 attributes

Attribute	**Description**
Type	Hardware
Description	Runs a Microsoft IIS 10 that hosts Financial Management System.
Significance	There is a possibility of application downtime and unauthorized access when the system is compromised

Table 6-14. Application Server3 environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : Medium (Protect sensitive application data.) Integrity : Medium (Application data must be reliable and unaltered to achieve operational efficiency) Availability : High (Needed for maintaining application uptime.) Accountability : Low (Monitor application access and usage.)

7.1.1.14. Asynchronous Transfer Mode

Table 6-15. Asynchronous Transfer Mode attributes

Attribute	Description
Type	Systems
Description	A technology that transmits data in fixed-size packets for high-speed transfer.
Significance	If compromised, can lead to poor network performance and unauthorized access.

Table 6-16. Asynchronous Transfer Mode environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : Medium (Data must be encrypted to prevent unauthorized access) Integrity : High (Data must be transmitted correctly without modifications) Availability : High (Needed for network communication)

7.1.1.15. Authentication

Table 6-17. Authentication attributes

Attribute	Description
Type	Process

Attribute	Description
Description	Verifies the identity of a user or system to grant access to resources.
Significance	If compromised, attackers could gain unauthorized access to sensitive systems, leading to data theft or system manipulation.

Table 6-18. Authentication environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Needed to control access to sensitive information) Integrity : High (Tampering with this could allow unauthorized access or prevent legitimate users from accessing systems) Accountability : High (For monitoring user activity and detecting malicious actions)

7.1.1.16. Authentication Details

Table 6-19. Authentication Details attributes

Attribute	Description
Type	Information
Description	Needed to verify identity and manage access rights
Significance	If compromise, could lead to unauthorized access, posing significant risks to system integrity, confidentiality, and availability.

Table 6-20. Authentication Details environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Must be kept from disclosure)

7.1.1.17. Buzzle Inc Products

Table 6-21. Buzzle Inc Products attributes

Attribute	Description
Type	Hardware

Attribute	Description
Description	Buzzers, switches, sensors, and any other electronic components or devices manufactured by the company
Significance	The main source of revenue for the company which directly impacts customer satisfaction and brand reputation

Table 6-22. Buzzle Inc Products environmental attributes

Environment	Security Property (Rationale)
Default	Integrity : High (Products must meet design specifications)

7.1.1.18. Company Network

Table 6-23. Company Network attributes

Attribute	Description
Type	Information
Description	Connects all devices and systems within Buzzle Inc.
Significance	Compromise can lead to unauthorized access to all connected systems, risking a data breach.

Table 6-24. Company Network environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : Medium (Handles sensitive data across all systems.) Integrity : High (Must ensure accurate data flows across the network.) Availability : High (Critical for ensuring continuous access to resources.) Accountability : Medium (Track user access to maintain security.)

7.1.1.19. Confirm Equipment Status

Table 6-25. Confirm Equipment Status attributes

Attribute	Description
Type	Process
Description	The regular checking and validation of the operational status of the shop floor equipment
Significance	It ensures that equipment is properly maintained and functioning

Table 6-26. Confirm Equipment Status environmental attributes

Environment	Security Property (Rationale)
Default	Integrity : High (Status reports must be accurate)

7.1.1.20. CRM Database

Table 6-27. CRM Database attributes

Attribute	Description
Type	Information
Description	A Microsoft SQL Server 2019 dedicated to store customer records, sales data, and marketing information.
Significance	Unauthorized access can lead to loss of customer data and damage to company reputation as it is the central hub that has the information needed in managing customer relationships and sales strategies.

Table 6-28. CRM Database environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Contains customer data which is sensitive hence must be protected from unauthorized access.) Integrity : High (To achieve effective customer management, accurate data is required.)

Environment	Security Property (Rationale)
	Availability : Medium (Timely and reliable access is needed but there is room for scheduled maintenance) Accountability : High (To be certain of data security, user activities must be tracked.)

7.1.1.21. Customer Records

Table 6-29. Customer Records attributes

Attribute	Description
Type	Information
Description	Information about customers, including contact details and transaction history
Significance	Compromise may lead to identity theft and loss of customer trust.

Table 6-30. Customer Records environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Customer data is sensitive data) Integrity : High (Unauthorized changes must be avoided as it must be accurate for good customer relationship) Availability : High (Needed for customer interactions) Accountability : High (Access and modifications must be monitored to prevent unauthorized actions.)

7.1.1.22. Customer Relationship Management System

Table 6-31. Customer Relationship Management System attributes

Attribute	Description
Type	Systems
Description	Hosted on a Microsoft IIS10 Application Server1 which manages customer interactions, records, sales, and support.

Attribute	Description
Significance	The system handles sensitive customer data and is needed in managing customer relationships, so protecting it from unauthorized access and change is vital in maintaining customer trust.

Table 6-32. Customer Relationship Management System environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (The system handles sensitive customer data, so protecting this information from unauthorized access is vital for privacy and compliance as well as preventing financial loss.) Integrity : High (Accurate customer data is needed for effective relationship management and reliable decision-making like identifying core customers and investors.) Availability : High (The CRM is needed to maintain contact with core customers and investors making availaibilty a need for business success) Accountability : Medium (There is a need to track who accesses and makes changes to customer data)

7.1.1.23. Design Specifications

Table 6-33. Design Specifications attributes

Attribute	Description
Type	Information
Description	Documents that outline the technical and functional requirements for Buzzle Inc.'s products
Significance	Needed for the accurate and efficient production of Buzzle Inc.'s products

Table 6-34. Design Specifications environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Contain proprietary information that should be kept from unauthorized disclosure) Integrity : High (Must be protected from unauthorized modifications)

7.1.1.24. Domain Controller Datastore

Table 6-35. Domain Controller Datastore attributes

Attribute	Description
Type	Information
Description	Saves authentication and validation of user access to the network.
Significance	Compromise could provide unauthorized access to the entire network and further access to all systems.

Table 6-36. Domain Controller Datastore environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Need to safeguard user credentials) Integrity : High (Authentication data must be accurate and complete) Availability : Medium (Failure of would affect domain controller, causing network problems) Accountability : High (All authentication attempts must be tracked for security.)

7.1.1.25. Domain Controller1

Table 6-37. Domain Controller1 attributes

Attribute	Description
Type	Hardware
Description	With a Windows Server 2019, authenticates and validates user access to the network.
Significance	Compromise could provide unauthorized access to the entire network and further access to all systems.

Table 6-38. Domain Controller1 environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Need to safeguard user credentials) Integrity : High (Authentication data must be accurate and complete) Availability : Medium (Failure of domain controller will cause network problems) Accountability : High (All authentication attempts must be tracked for security.)

7.1.1.26. Email Accounts

Table 6-41. Email Accounts attributes

Attribute	Description
Type	Information
Description	Used for internal and external communications via the email system.
Significance	When compromised can lead to phishing attacks and unauthorized access to sensitive information.

Table 6-42. Email Accounts environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Access to communications)

Environment	Security Property (Rationale)
	Integrity : Medium (Needed for daily communication)

7.1.1.27. File Server

Table 6-43. File Server attributes

Attribute	Description
Type	Hardware
Description	A Windows Server 2019 that centralizes file storage and management for employee access
Significance	Compromise may result in data loss, unauthorized access, and also operational disruptions.

Table 6-44. File Server environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Protecting sensitive company data is crucial to prevent unauthorized access and data breaches which could lead to reputation damage and financial loss.) Integrity : Medium (Accurate and unaltered data will help maintain trust in information used.) Availability : High (Employees need reliable access to files for day to day tasks hence availability is needed to maintain productivity.) Accountability : Medium (Itâ□□s important to know who accesses and changes files since there is a lot of work collaboration.)

7.1.1.28. Financial Database

Table 6-45. Financial Database attributes

Attribute	Description
Type	Information
Description	A IBM DB2 11.1 database dedicated to manage financial transactions, accounts payable/receivable,and budgeting data
Significance	Provides data needed for financial management, decision making , compliance and operational efficiency. A breach could result in financial mismanagement and legal consequences.

Table 6-46. Financial Database environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Contains sensitive financial data that must be protected from unauthorized disclosure.) Integrity : High (To make good information based decisions, financial data needs to be accurate and free from unauthorized modifications.) Availability : Medium (Needed for financial operations but some downtime due to maintenance is allowed.) Accountability : High (To ensure the security of the data , users actions must be tracked.)

7.1.1.29. Financial Management System

Table 6-47. Financial Management System attributes

Attribute	Description
Type	Software
Description	Hosted on a Microsoft IIS 10 Application Server3 dedicated to managing financial records, handling payroll, processing invoices, overseeing budgets, and generating financial reports.
Significance	Unauthorized access to sensitive financial data would negatively affect the company's reputation and finance.

Table 6-48. Financial Management System environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Unauthorized access to sensitive financial data which includes personal information would negatively affect the company's reputation and finance.) Integrity : High (It is important to have accurate financial records for compliance and in making right decisions.) Availability : High (Timely reporting and decision making needed for operations can be possible when financial data is available.) Accountability : High (Track who accesses and modifies financial data)

7.1.1.30. Financial Records

Table 6-49. Financial Records attributes

Attribute	Description
Type	Information
Description	financial transactions, accounts payable/receivable, and budgeting data
Significance	Unauthorized access can lead to fraud and regulatory penalties.

Table 6-50. Financial Records environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Unauthorized access can lead to fraud and regulatory penalties.) Integrity : High (Must be accurate for report generation and decision making hence unauthorized changes must be avoided.) Accountability : Medium (User actions must be monitored and tracked)

7.1.1.31. Generate Production Report

Table 6-51. Generate Production Report attributes

Attribute	Description
Type	Process
Description	Generate reports that summarize production progress
Significance	Helps in strategic decision-making

Table 6-52. Generate Production Report environmental attributes

Environment	Security Property (Rationale)
Default	Integrity : High (Reports generated must be accurate)

7.1.1.32. IBM DB

Table 6-53. IBM DB attributes

Attribute	Description
Type	Software
Description	IBM DB2 11.1, a relational database managing the Financial Database
Significance	Compromise can lead to data breaches and operational disruptions.

Table 6-54. IBM DB environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Manages financial data and must be protected from breaches.)

7.1.1.33. Internet Protocol

Table 6-55. Internet Protocol attributes

Attribute	Description
Type	Systems
Description	Technology for transmitting data packets over the network.
Significance	For accurate and efficient data delivery.

Table 6-56. Internet Protocol environmental attributes

Environment	Security Property (Rationale)
Default	Integrity : High (Data is transmitted without modification) Availability : High (Needed for routing traffic which aids in communication in the network) Accountability : Medium (Track IP address and associated activities)

7.1.1.34. IP Address

Table 6-63. IP Address attributes

Attribute	Description
Type	Information
Description	A unique address assigned to each device connected to the network.
Significance	Compromise can lead to unauthorized access to the network.

Table 6-64. IP Address environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : Medium (Disclosure could lead to network access as it contains network configuration data.)

7.1.1.35. IT Department

Table 6-65. IT Department attributes

Attribute	Description
Type	Information
Description	Responsible for managing and responding to security incidents and inquiries.
Significance	Needed for addressing security concerns and maintaining overall security posture.

Table 6-66. IT Department environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (They manage sensitive company data, user credentials, including systems and network access.) Integrity : High (They ensure the integrity of the systems) Availability : High (They ensure the availability of systems and networks)

7.1.1.36. IT Infrastructure

Table 6-67. IT Infrastructure attributes

Attribute	Description
Type	System of Systems
Description	The composite hardware, software, and network resources used for IT services.
Significance	A breach could disrupt all IT services, leading to operational downtime.

Table 6-68. IT Infrastructure environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (IT assets must be safeguarded from unauthorized access.) Integrity : High (Ensures accurate operation of IT services hence unauthorized changes to configurations must be avoided.) Availability : High (Needed for daily task so must be consistently operational.) Accountability : Medium (All access must be logged to monitor compliance)

7.1.1.37. Local Area Network

Table 6-73. Local Area Network attributes

Attribute	Description
Type	Systems

Attribute	Description
Description	Connects employees' workstations, servers, and other devices in each Buzzle Inc site.
Significance	If compromised, may allow unauthorized access to internal communications and possibly sensitive data.

Table 6-74. Local Area Network environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : Medium (Data within internal communications must be protected from unauthorized access) Integrity : High (Accurate data is required in collaboration and communication) Availability : High (Must be always available for daily operations.)

7.1.1.38. Marketing Information

Table 6-75. Marketing Information attributes

Attribute	Description
Type	Information
Description	Data related to marketing strategies and campaigns.
Significance	Compromise can lead to loss of competitive advantage and ineffective marketing strategies.

Table 6-76. Marketing Information environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : Medium (Contains strategic information and must be safeguarded from unauthorized disclosure.) Integrity : High (Accuracy in strategies is key and tampering must be prevented.) Availability : Medium (Access to current data is important to avoid delays.)

7.1.1.39. NetApp FAS8000 Series

Table 6.83: NetApp FAS8000 Series attributes

Attribute	Description
Type	Software
Description	A series of networked storage device.
Significance	Compromise may result in data loss and hinder operational efficiency.

Table 6.84: NetApp FAS8000 Series environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Contains sensitive data and must be protected from breaches.) Integrity : High (Stored data must be accurate hence unauthorized changes must be avoided.)

7.1.1.40. Network Storage Device1

Table 6.85: Network Storage Device1 attributes

Attribute	Description
Type	Hardware
Description	NetApp FAS8000 series device that provide additional storage capacity and redundancy.
Significance	Provides data availability and backup solutions. Compromise may result in data loss and hinder operational efficiency.

Table 6.86: Network Storage Device1 environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : Medium (May handle sensitive data but do not store it) Integrity : Medium (Data transmitted must not be corrupted or altered without authorization, this could happen when the device is faulty.) Availability : High (Needed for network connectivity)

7.1.1.41. Networked Email System

Table 6.89: Networked Email System attributes

Attribute	Description
Type	Systems
Description	Email systems connected to the network for communication
Significance	A breach could result in phishing attacks and unauthorized data access.

Table 6.90: Networked Email System environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Contains communication data that must be protected.)

7.1.1.42. Office Equipment

Table 6.91: Office Equipment attributes

Attribute	Description
Type	Hardware

Attribute	Description
Description	Tools and devices used in the office, such as printers, copiers, and phones.
Significance	Compromise may lead to data exposure and operational disruptions.

Table 6.92: Office Equipment environmental attributes

Environment	Security Property (Rationale)
Default	Availability : Medium (Needed for daily operations hence should be operational)

7.1.1.43. Office Related Files

Table 6.93: Office Related Files attributes

Attribute	Description
Type	Information
Description	Documents related to day-to-day office operations and any other files
Significance	Compromise could disrupt operations and lead to loss of sensitive information.

Table 6.94: Office Related Files environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : Medium (Information needs to be safe from unauthorized disclosure or access) Integrity : Medium (Protect accuracy)

7.1.1.44. Oracle Database 19c

Table 6.95: Oracle Database 19c attributes

Attribute	Description
Type	Software
Description	Hosts inventory database.

Attribute	Description
Significance	Compromise can lead to data breaches and operational disruptions.

Table 6.96: Oracle Database 19c environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Unauthorized access can lead to data breaches and operational disruptions.)

7.1.1.45. Order History

Table 6.97: Order History attributes

Attribute	Description
Type	Information
Description	A record of customer orders and transactions.
Significance	Unauthorized access can lead to fraudulent transactions and loss of customer trust.

Table 6.98: Order History environmental attributes

Environment	Security Property (Rationale)

Default	Confidentiality : High (Unauthorized disclosure or access can lead to fraudulent transactions and loss of customer trust.)

7.1.1.46. Phone System

Table 6.99: Phone System attributes

Attribute	**Description**
Type	Hardware
Description	Telecommunication systems used for internal and external communication.
Significance	A breach could disrupt communications and lead to data leaks.

Table 6.100: Phone System environmental attributes

Environment	Security Property (Rationale)
Default	Availability : High (Needed for communication)

7.1.1.47. Print Server

Table 6.101: Print Server attributes

Attribute	Description
Type	Hardware
Description	A Windows Server 2019 that manages print jobs across the company.
Significance	Facilitates printing across the network. Compromise could lead to unauthorized access to sensitive documents.

Table 6.102: Print Server environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : Medium (May handle sensitive data but not as high compared to database) Integrity : Medium (Documents must be printed correctly) Availability : High (Needed for daily tasks that involve printing services) Accountability : Medium (Keeps track of print jobs)

7.1.1.48. Production Schedule

Table 6.103: Production Schedule attributes

Attribute	Description

Type	Information
Description	A timeline outlining the manufacturing process and deadlines
Significance	Compromise can lead to production delays and financial losses.

Table 6.104: Production Schedule environmental attributes

Environment	**Security Property (Rationale)**
Default	Availability : Medium (Should be accessible as it is Important for production flow)

7.1.1.49. ProductionManager

Table 6.105: ProductionManager attributes

Attribute	**Description**
Type	People
Description	Creates the master production schedule based on customer orders and inventory, Works with the Chief Technology Officer to ensure new designs are feasible.
Significance	Leads production management

Table 6.106: ProductionManager environmental attributes

Environment	**Security Property (Rationale)**
Default	Availability : High (Manages production)

7.1.1.50. Public WiFi

Table 6.107: Public WiFi attributes

Attribute	Description
Type	Systems
Description	A network that provides internet access
Significance	If not managed properly, attackers can exploit the network to access sensitive data or launch attacks like man-in-the-middle

Table 6.108: Public WiFi environmental attributes

Environment	Security Property (Rationale)
Default	Availability : Low (Only needed when working offsite or on the move)

7.1.1.51. Report IT Issues

Table 6.109: Report IT Issues attributes

Attribute	Description
Type	Process
Description	A user reports identified security issues, or suspicions to the IT department for resolution
Significance	Early reporting and resolution could prevent or minimize the impact of security attacks

Table 6.110: Report IT Issues environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Security issues often involve sensitive system vulnerabilities or data, so disclosure should be limited to authorized personnel)

7.1.1.52. Review Production Design

Table 6.111: Review Production Design attributes

Attribute	**Description**
Type	Process
Description	The production manager and the Chief Technology Officer review and approve production designs.
Significance	The review ensures new designs are feasible

Table 6.112: Review Production Design environmental attributes

Environment	**Security Property (Rationale)**
Default	Integrity : High (It ensures new designs are feasible, so must be accurate)

7.1.1.53. Root Access Credentials

Table 6.113: Root Access Credentials attributes

Attribute	Description
Type	Information
Description	The highest level of authority within a system, allowing a user or process to have complete control.
Significance	If compromised , can lead to severe breaches, data loss, or system corruption

Table 6.114: Root Access Credentials environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Must be kept from unauthorized access and disclosure)

7.1.1.54. Sales Data

Table 6.115: Sales Data attributes

Attribute	Description
Type	Information
Description	Information on sales and customer purchases
Significance	Breach could result in competitive disadvantage and financial loss.

Table 6.116: Sales Data environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Contains sensitive data which must be protected from unauthorized disclosure.) Integrity : High (Tampering will lead to inaccurate data and reports.)

	Availability : High (Must be accessible for operational insights) Accountability : Medium (Track access for compliance)

7.1.1.55. Shop Floor Control System

Table 6.117: Shop Floor Control System attributes

Attribute	**Description**
Type	Information
Description	Monitors and controls shop floor operations
Significance	Compromise can disrupt production and lead to financial losses

Table 6.118: Shop Floor Control System environmental attributes

Environment	**Security Property (Rationale)**
Default	Availability : High (Has to be always operational as it is needed for production)

7.1.1.56. Shop Floor Equipment

Table 6.119: Shop Floor Equipment attributes

Attribute	**Description**
Type	Hardware
Description	Machinery and tools used in the production process.
Significance	A compromise could disrupt operations and lead to equipment damage.

Table 6.120: Shop Floor Equipment environmental attributes

Environment	Security Property (Rationale)
Default	Availability : High (Needed for production hence must be operational at all times.)

7.1.1.57. Supply Chain Data

Table 6.121: Supply Chain Data attributes

Attribute	Description
Type	Information
Description	Information related to the supply chain process, including suppliers, inventory, and delivery schedules
Significance	Unauthorized access or change could disrupt supply chain operations and lead to financial losses.

Table 6.122: Supply Chain Data environmental attributes

Environment	**Security Property (Rationale)**
Default	Confidentiality : High (Unauthorized access could disrupt supply chain operations and lead to financial losses.)

7.1.1.58. Update ProductionSchedule

Table 6.123: Update ProductionSchedule attributes

Attribute	**Description**
Type	Process
Description	Authorized users make changes to the production schedule
Significance	Inaccurate modifications could lead to production delays or inefficiencies

Table 6.124: Update ProductionSchedule environmental attributes

Environment	**Security Property (Rationale)**
Default	Integrity : High (The accuracy of this is needed for a smooth production flow) Availability : High (Production cannot proceed without a current schedule) Accountability : Medium (Tracking changes made to the schedule is needed)

7.1.1.59. Virtual Private Network

Table 6.125: Virtual Private Network attributes

Attribute	Description
Type	Systems
Description	It enables secure and encrypted communication over a public network, such as the internet
Significance	It ensures that data is encrypted and protected from interception

Table 6.126: Virtual Private Network environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Data transmitted is encrypted) Availability : High (Needed for secure, remote access to company resources when offsite)

7.1.1.60. Wide Area Network

Table 6.127: Wide Area Network attributes

Attribute	Description
Type	Systems
Description	Connects Buzzle Inc.'s multiple sites over large areas and allows for remote work.
Significance	A malicious attack could disrupt communication, impacting global business operations and collaboration.

Table 6.128: Wide Area Network environmental attributes

Environment	Security Property (Rationale)

Default	Confidentiality : Medium (Data must be encrypted to prevent unauthorized disclosure) Integrity : High (During transmission it is key to ensure data is not modified.) Availability : High (To support the company's global operations, it must be operational at all times)

7.1.1.61. Windows 10

Table 6.129: Windows 10 attributes

Attribute	**Description**
Type	Software
Description	The operating system of workstations.
Significance	An improper configuration could lead to data loss or system compromise due to security controls bypass.

Table 6.130: Windows 10 environmental attributes

Environment	Security Property (Rationale)
Default	Integrity : Medium (Configurations must be protected from tampering.) Availability : High (Needed for workstation function.) Accountability : Medium (Monitor system use)

7.1.1.62. Windows Server 2019

Table 6.131: Windows Server 2019 attributes

Attribute	Description
Type	Software
Description	An operating system that manages and operates server infrastructure.
Significance	A compromised could lead to the exposure of confidential information and disruption of services.

Table 6.132: Windows Server 2019 environmental attributes

Environment	Security Property (Rationale)
Default	Confidentiality : High (Protect sensitive data managed by the server to prevent unauthorized disclosure of data) Integrity : High (Data must be accurate and unaltered.) Availability : High (Necessary for uninterrupted access to services) Accountability : Medium (Track and monitor user actions to easily identify malicious activities)

7.1.1.63. Workstation

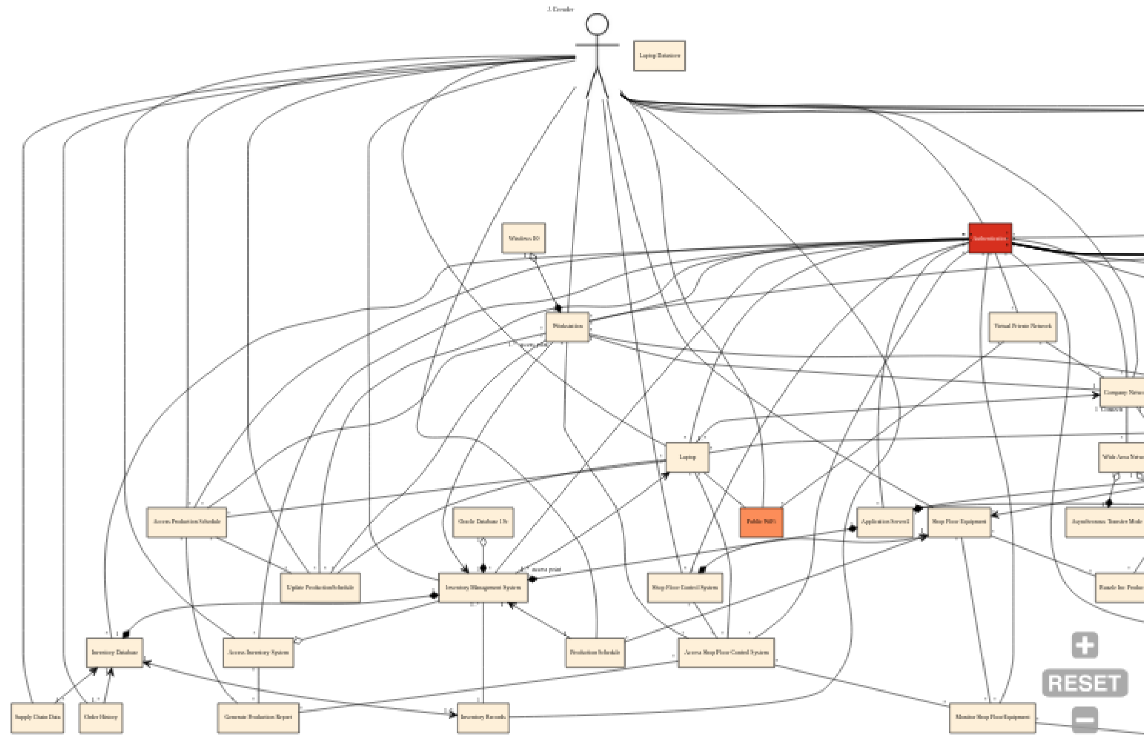
Table 6.133: Workstation attributes

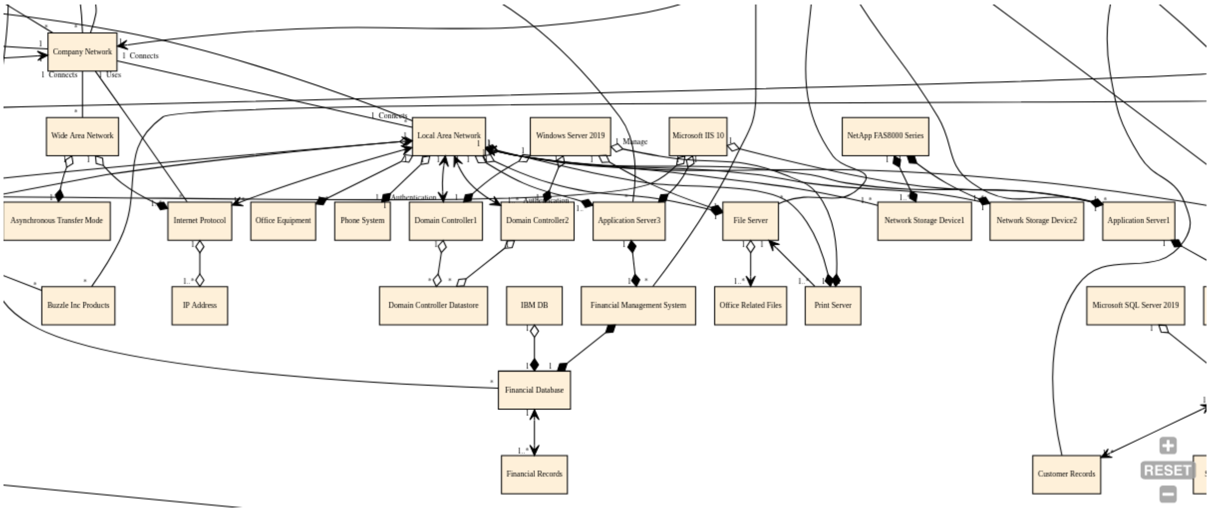
Attribute	**Description**
Type	Hardware
Description	A windows 10 used by employees to access all systems, retrieve and store documents, perform daily tasks, as well as communicate within the organization.
Significance	As a primary tool for employee’s daily tasks and data entry, a compromise would lead to unauthorized data access, resulting in intellectual property theft and reduced competitive advantage.

Table 6.134: Workstation environmental attributes

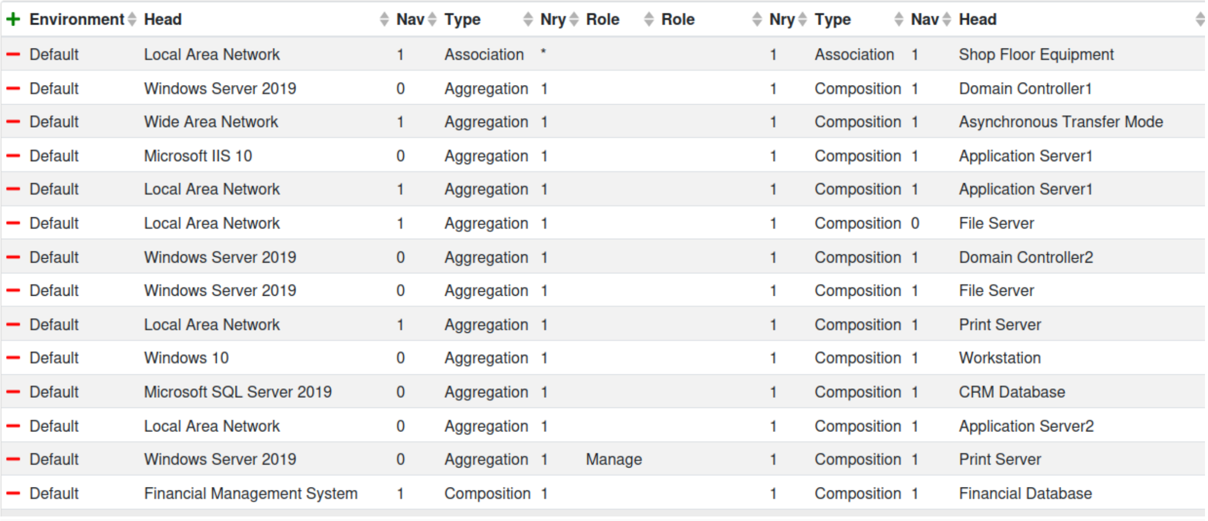
Environment	**Security Property (Rationale)**
Default	Confidentiality : Medium (The employees make use of the PC in their tasks however its not the main repository for sensitive data.) Integrity : High (Data must be safeguarded against tampering.) Availability : High (Employees rely on PCs to carry out their daily tasks hence if not available productivity will be negatively impacted.) Accountability : High (Track usage and prevent unauthorized access as it is the key access to all systems)

7.1.2. Asset Model

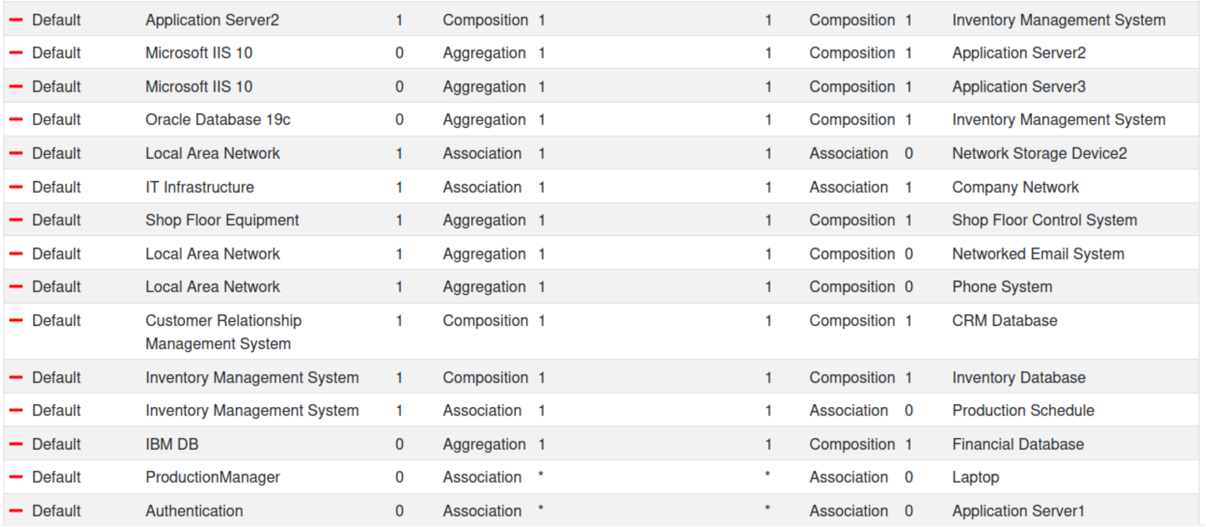




7.1.3. Asset Association



+	Environment	Head	Nav	Type	Nry	Role	Role	Nry	Type	Nav	Head
−	Default	Local Area Network	1	Association	*			1	Association	1	Shop Floor Equipment
−	Default	Windows Server 2019	0	Aggregation	1			1	Composition	1	Domain Controller1
−	Default	Wide Area Network	1	Aggregation	1			1	Composition	1	Asynchronous Transfer Mode
−	Default	Microsoft IIS 10	0	Aggregation	1			1	Composition	1	Application Server1
−	Default	Local Area Network	1	Aggregation	1			1	Composition	1	Application Server1
−	Default	Local Area Network	1	Aggregation	1			1	Composition	0	File Server
−	Default	Windows Server 2019	0	Aggregation	1			1	Composition	1	Domain Controller2
−	Default	Windows Server 2019	0	Aggregation	1			1	Composition	1	File Server
−	Default	Local Area Network	1	Aggregation	1			1	Composition	1	Print Server
−	Default	Windows 10	0	Aggregation	1			1	Composition	1	Workstation
−	Default	Microsoft SQL Server 2019	0	Aggregation	1			1	Composition	1	CRM Database
−	Default	Local Area Network	0	Aggregation	1			1	Composition	1	Application Server2
−	Default	Windows Server 2019	0	Aggregation	1	Manage		1	Composition	1	Print Server
−	Default	Financial Management System	1	Composition	1			1	Composition	1	Financial Database



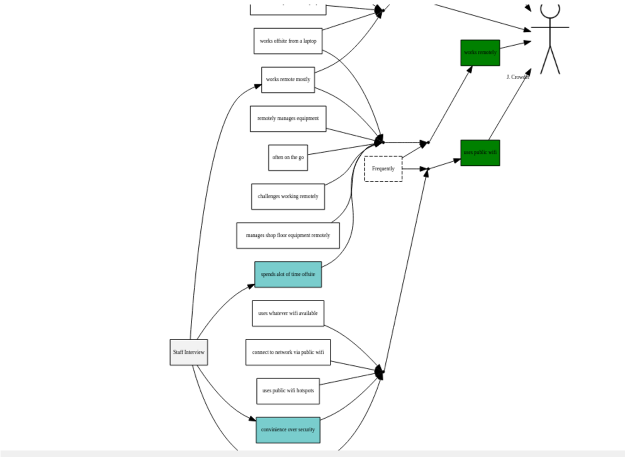
−	Default	Application Server2	1	Composition	1			1	Composition	1	Inventory Management System
−	Default	Microsoft IIS 10	0	Aggregation	1			1	Composition	1	Application Server2
−	Default	Microsoft IIS 10	0	Aggregation	1			1	Composition	1	Application Server3
−	Default	Oracle Database 19c	0	Aggregation	1			1	Composition	1	Inventory Management System
−	Default	Local Area Network	1	Association	1			1	Association	0	Network Storage Device2
−	Default	IT Infrastructure	1	Association	1			1	Association	1	Company Network
−	Default	Shop Floor Equipment	1	Aggregation	1			1	Composition	1	Shop Floor Control System
−	Default	Local Area Network	1	Aggregation	1			1	Composition	0	Networked Email System
−	Default	Local Area Network	1	Aggregation	1			1	Composition	0	Phone System
−	Default	Customer Relationship Management System	1	Composition	1			1	Composition	1	CRM Database
−	Default	Inventory Management System	1	Composition	1			1	Composition	1	Inventory Database
−	Default	Inventory Management System	1	Association	1			1	Association	0	Production Schedule
−	Default	IBM DB	0	Aggregation	1			1	Composition	1	Financial Database
−	Default	ProductionManager	0	Association	*			*	Association	0	Laptop
−	Default	Authentication	0	Association	*			*	Association	0	Application Server1

−	Default	Workstation	0	Association	*		*	Association	0	Access Shop Floor Control System
−	Default	Access Shop Floor Control System	0	Association	*		*	Association	0	Monitor Shop FloorEquipment
−	Default	Authentication	0	Association	*		*	Association	0	Monitor Shop FloorEquipment
−	Default	Monitor Shop FloorEquipment	0	Association	*		*	Association	0	Shop Floor Equipment
−	Default	ProductionManager	0	Association	*		*	Association	0	Review Production Design
−	Default	Access Inventory System	0	Association	*		*	Association	0	Generate Production Report
−	Default	Access Production Schedule	0	Association	*		*	Association	0	Generate Production Report
−	Default	Access Shop Floor Control System	0	Association	*		*	Association	0	Generate Production Report
−	Default	Authentication	0	Association	*		*	Association	0	Virtual Private Network
−	Default	Virtual Private Network	0	Association	*		*	Association	0	Public WiFi
−	Default	Virtual Private Network	0	Association	*		*	Association	0	Company Network
−	Default	Report IT Issues	0	Association	*		*	Association	0	Networked Email System
−	Default	Report IT Issues	0	Association	*		*	Association	0	Workstation
−	Default	Report IT Issues	0	Association	*		*	Association	0	ProductionManager
−	Default	Report IT Issues	0	Association	*		*	Association	0	Email Accounts
−	Default	ProductionManager	0	Association	*		*	Association	0	Design Specifications
−	Default	Local Area Network	1	Association	1		1..*	Association	0	Network Storage Device1
−	Default	NetApp FAS8000 Series	1	Composition	1		1..*	Composition	1	Network Storage Device2
−	Default	NetApp FAS8000 Series	1	Composition	1		1..*	Composition	1	Network Storage Device1
−	Default	Inventory Database	1	Association	1		1..*	Association	1	Inventory Records
−	Default	Inventory Database	1	Association	1		1..*	Association	0	Supply Chain Data
−	Default	Inventory Database	1	Association	1		1..*	Association	0	Order History
−	Default	Financial Database	1	Association	1		1..*	Association	1	Financial Records
−	Default	Local Area Network	1	Association	1		1..*	Association	1	Internet Protocol
−	Default	Local Area Network	1	Aggregation	1		1..*	Composition	0	Application Server3
−	Default	File Server	1	Aggregation	1		1..*	Association	1	Office Related Files
−	Default	Networked Email System	1	Aggregation	1		1..*	Composition	1	Email Accounts
−	Default	Internet Protocol	1	Aggregation	1		1..*	Aggregation	0	IP Address
−	Default	Company Network	1	Association	1		1..*	Association	0	Laptop
−	Default	Laptop	1	Association	1	access point	1..*	Association	0	Inventory Management System

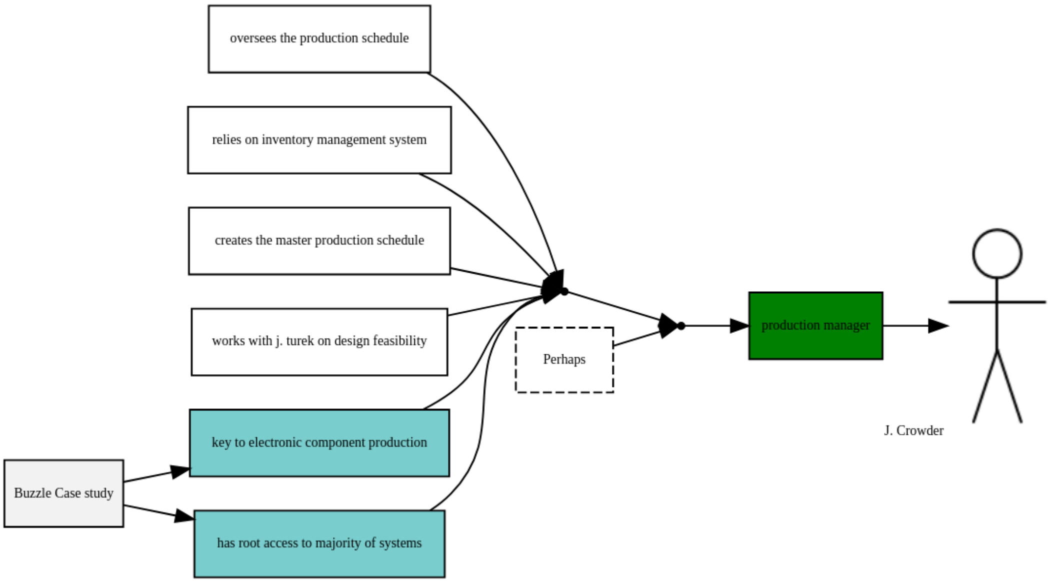
7.2. Appendix 2: Persona Data Analysis

7.2.1. *Persona Narrative*: J. Crowder

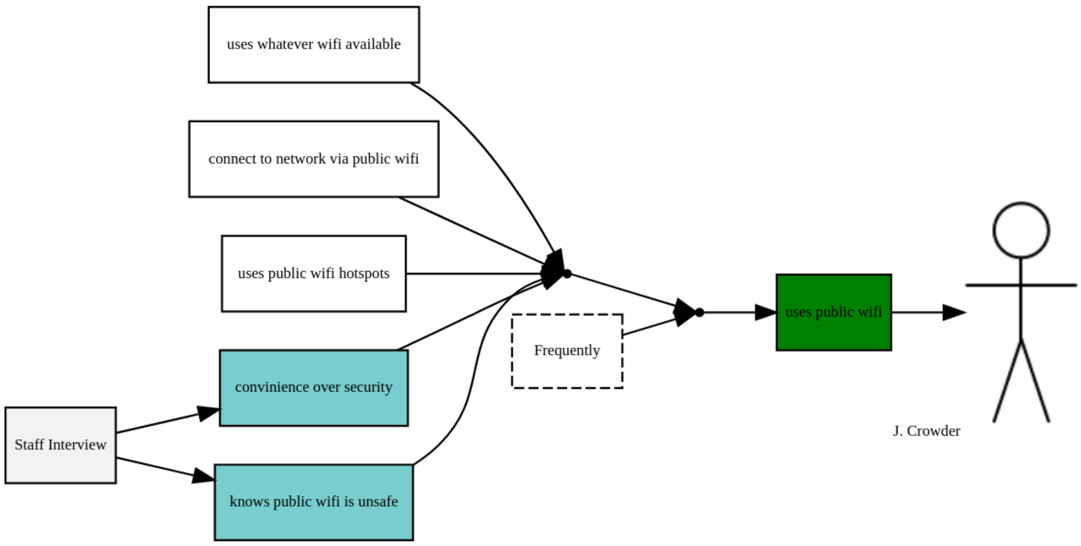
7.2.1.1. Activities


works offsite from a laptop
works remote mostly
remotely manages equipment
often on the go
challenges working remotely
manages shop floor equipment remotely
spends alot of time offsite
uses whatever wifi available
Staff Interview
connect to network via public wifi
uses public wifi hotspots
convinience over security
Frequently
works remotely
uses public wifi
J. Crowder

J. Crowder often works offsite from a laptop because he is always on the move. He oversees the production schedule, relying on the inventory management system to create and manage the schedule. His work is fast paced themed with frequent unexpected changes.

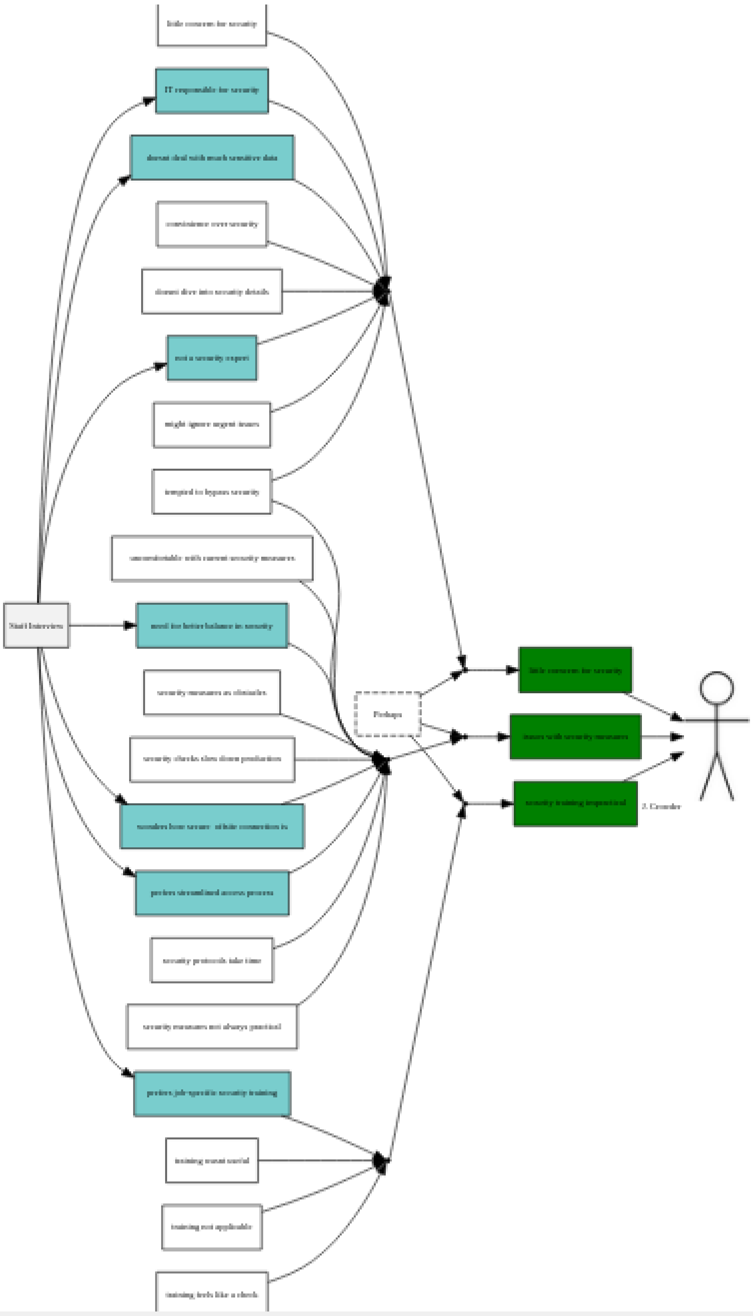

oversees the production schedule
relies on inventory management system
creates the master production schedule
works with j. turek on design feasibility
key to electronic component production
has root access to majority of systems
Buzzle Case study
Perhaps
production manager
J. Crowder

J. Crowder ensures that the shop floor equipment is functioning properly so when offsite, he connects to the company network via Public Wi-Fi to manage the equipment remotely. He also works with J. Turek on design feasibility.

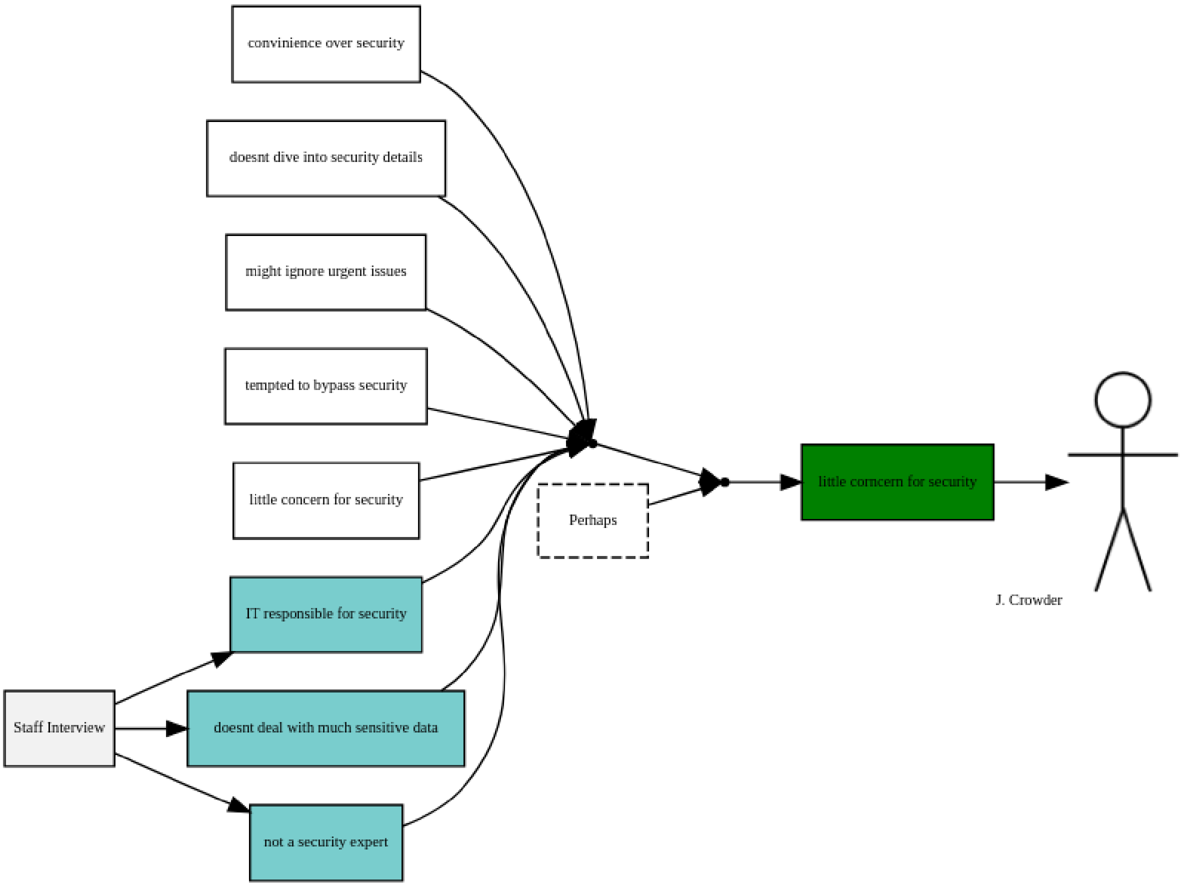

uses whatever wifi available
connect to network via public wifi
uses public wifi hotspots
convinience over security
Staff Interview
knows public wifi is unsafe
Frequently
uses public wifi
J. Crowder

Crowder faces connectivity issues when working offsite hence his reliance on public Wi-Fi. His use of Public Wi-Fi raises security concerns.

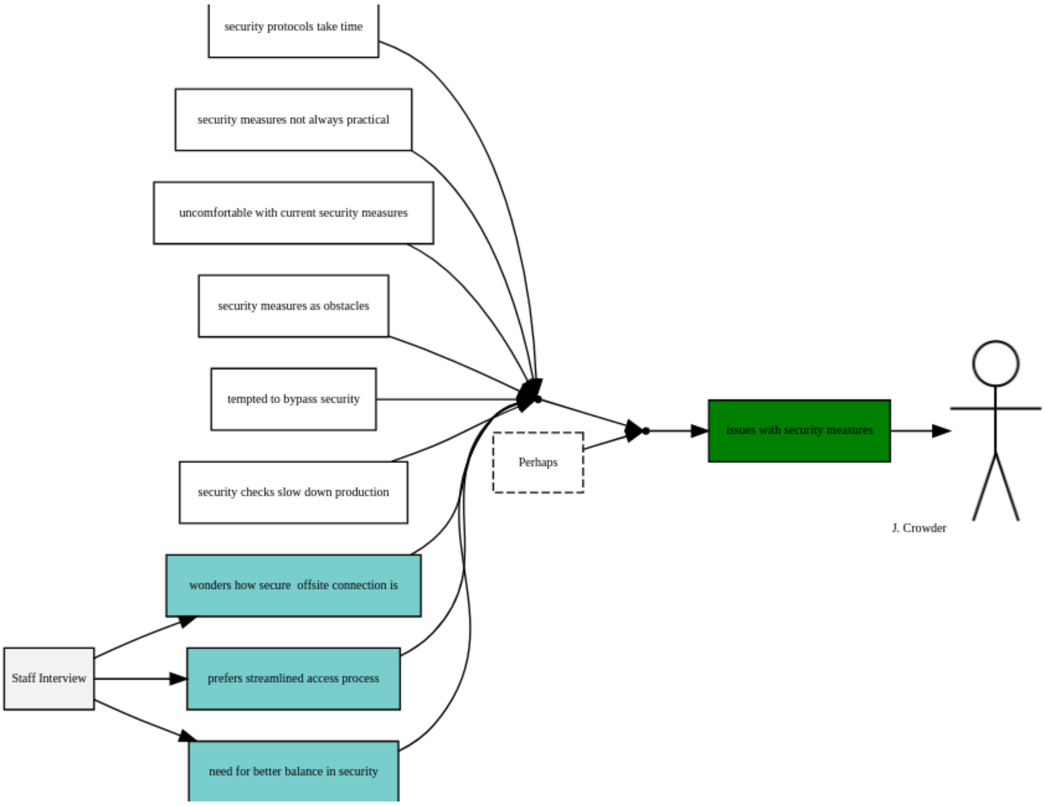
7.2.1.2. Attitudes


little concern for security
IT responsible for security
doesnt deal with much sensitive data
convenience over security
doesnt dive into security details
not a security expert
might ignore urgent issues
tempted to bypass security
uncomfortable with current security measures
Staff Interview
need for better balance in security
security measures as obstacles
security checks slow down production
wonders how secure offsite connection is
prefers streamlined access process
security protocols take time
security measures not always practical
prefers job-specific security training
training wasnt useful
training not applicable
training feels like a check
Perhaps
little concern for security
issues with security measures
security training impractical
J. Crowder

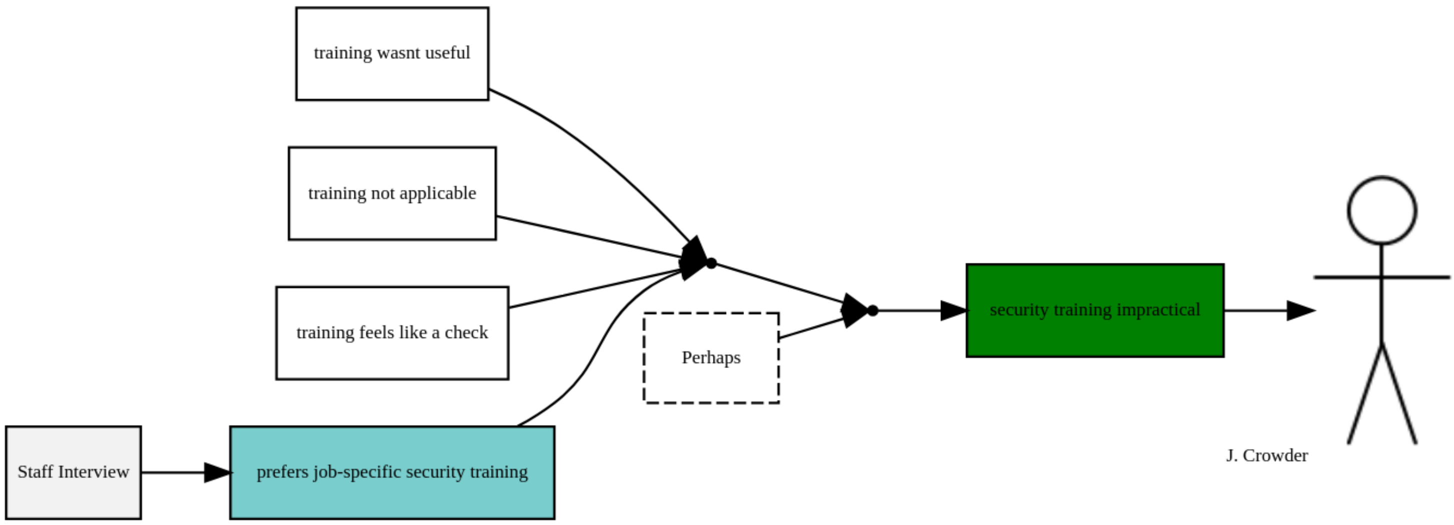
J. Crowder shows little concern for security, preferring convenience and focusing on completing production tasks efficiently. He relies on the IT department for security, as he does not deal with much sensitive data.


convinience over security
doesnt dive into security details
might ignore urgent issues
tempted to bypass security
little concern for security
IT responsible for security
doesnt deal with much sensitive data
not a security expert
Staff Interview
Perhaps
little corncern for security
J. Crowder

Crowder sees the current security measures as a hindrance that slows down productivity.


security protocols take time
security measures not always practical
uncomfortable with current security measures
security measures as obstacles
tempted to bypass security
security checks slow down production
wonders how secure offsite connection is
prefers streamlined access process
need for better balance in security
Staff Interview
Perhaps
issues with security measures
J. Crowder

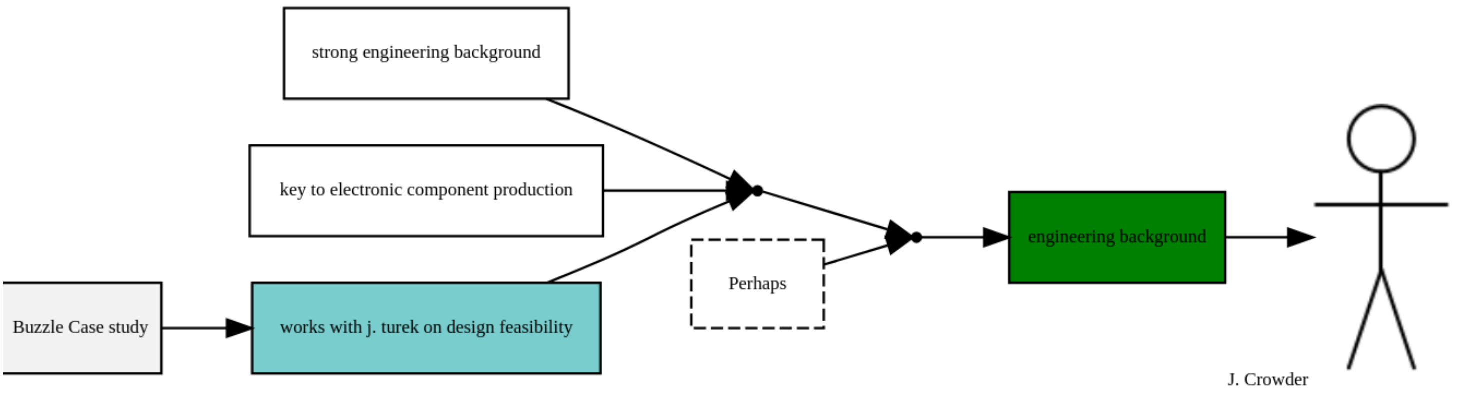
Also, he views the security training offered as impractical and a box checking activity as it is of no relevance to his job.


training wasnt useful
training not applicable
training feels like a check
Staff Interview
prefers job-specific security training
Perhaps
security training impractical
J. Crowder

His lack of concern for security poses a high risk as he has root access credentials.

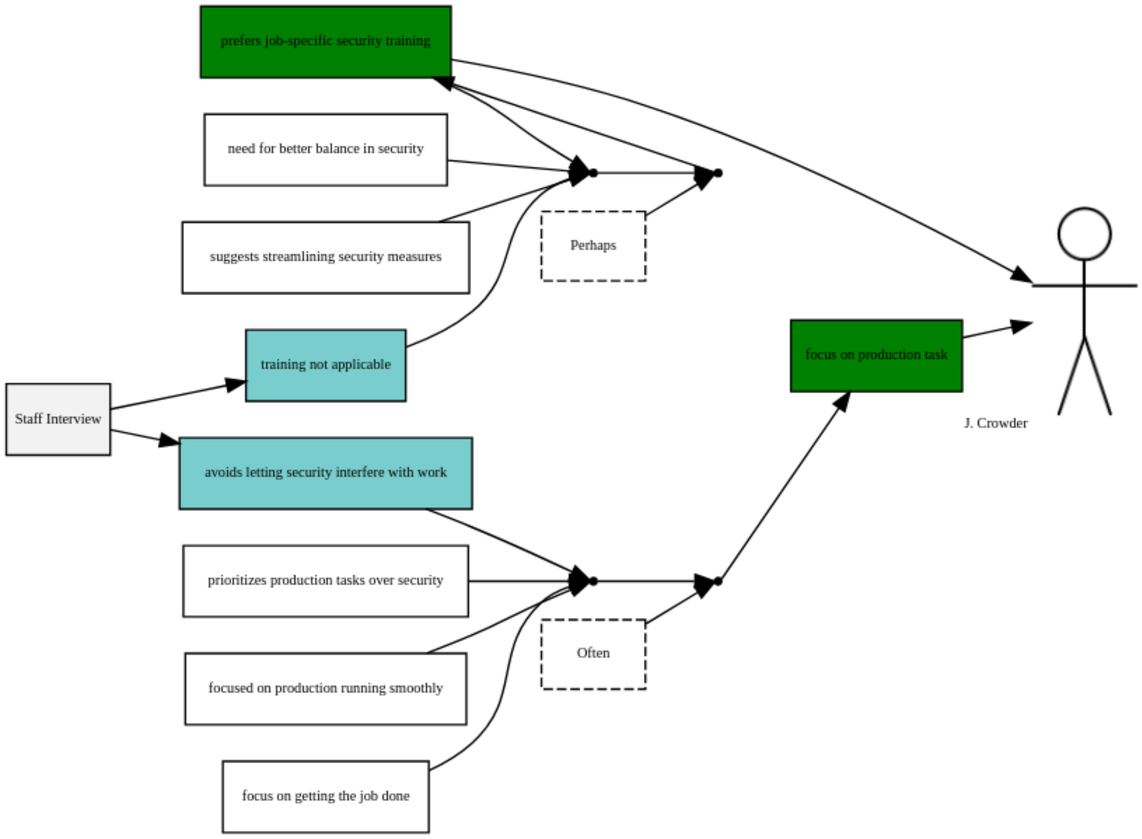
7.2.1.3. Aptitudes

J. Crowder is key to the company's electronic component production utilizing his strong engineering background. His root access credentials and collaboration with the Chief Technology Officer J. Turek in design feasibility, further shows his technical responsibilities and influence over key production systems.

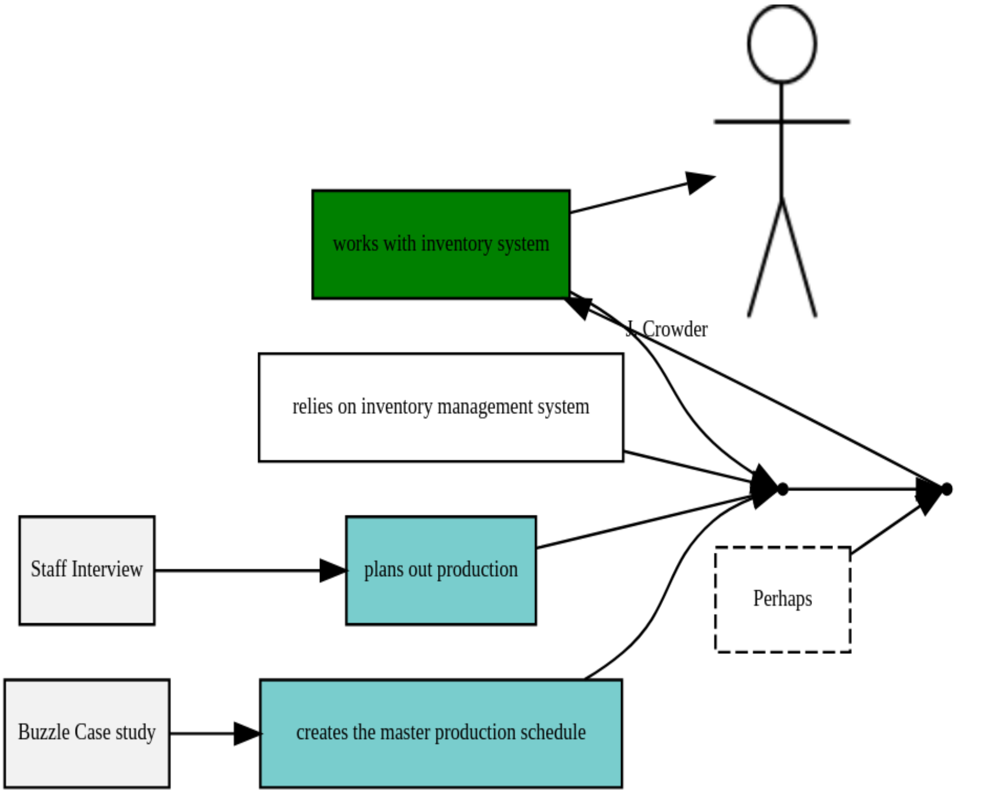

strong engineering background
key to electronic component production
Buzzle Case study
works with j. turek on design feasibility
Perhaps
engineering background
J. Crowder

7.2.1.4. Motivations

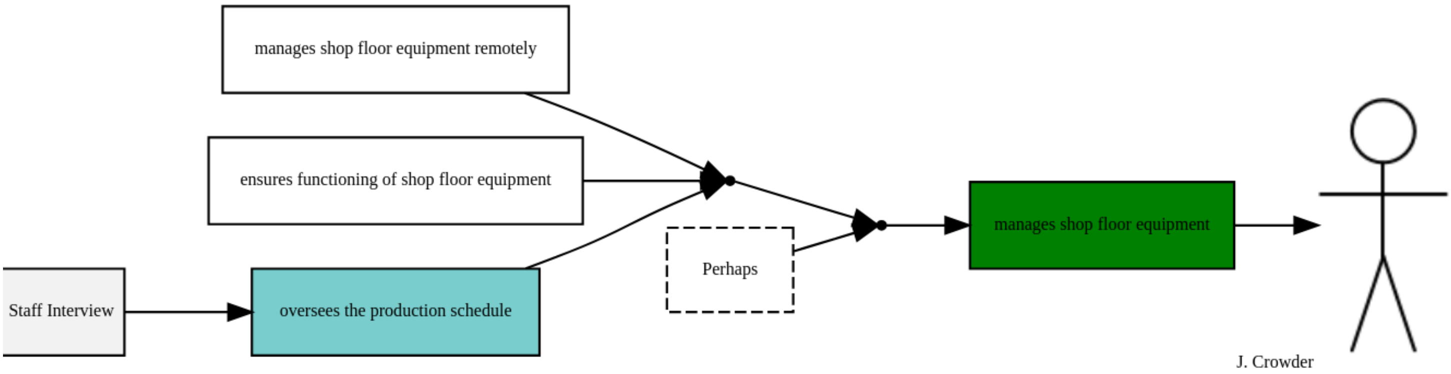
J. Crowder's focus is on production running smoothly. He also prefers job specific security training and streamlined security measures to provide a balance between security and productivity.

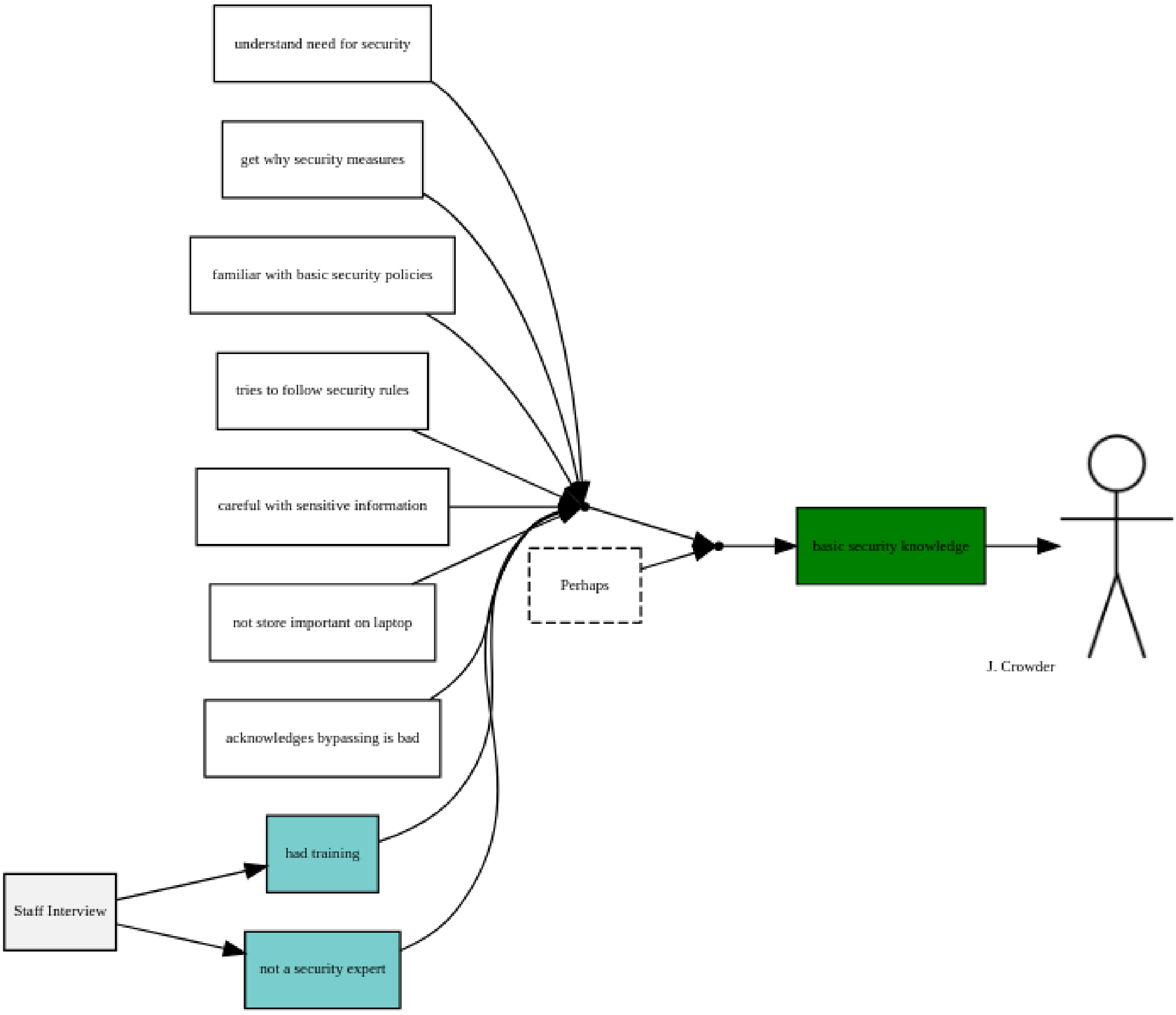

prefers job-specific security training
need for better balance in security
suggests streamlining security measures
Perhaps
training not applicable
Staff Interview
avoids letting security interfere with work
focus on production task
J. Crowder
prioritizes production tasks over security
Often
focused on production running smoothly
focus on getting the job done

7.2.1.5. Skills


works with inventory system
J. Crowder
relies on inventory management system
Staff Interview
plans out production
Perhaps
Buzzle Case study
creates the master production schedule

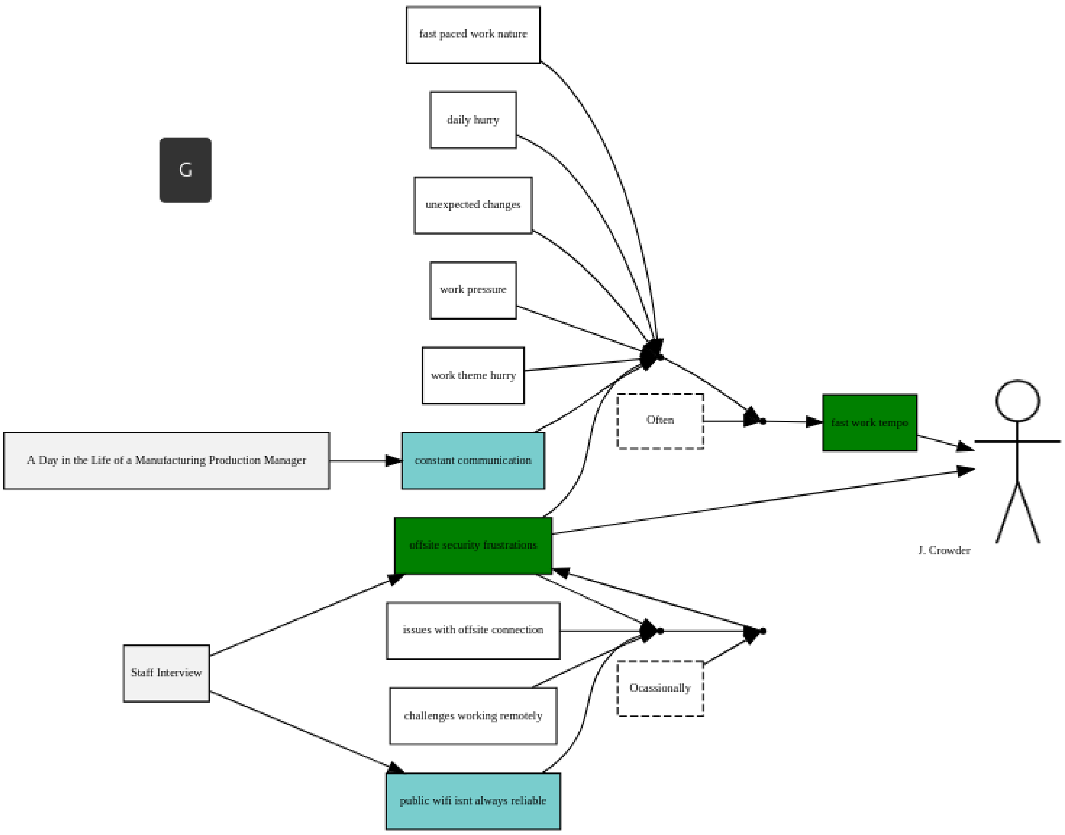
J. Crowder uses the inventory management system to create the master production schedule and plan production effectively. He remotely manages shop floor equipment, ensuring its proper functioning and overseeing the overall production schedule.


manages shop floor equipment remotely
ensures functioning of shop floor equipment
Staff Interview
oversees the production schedule
Perhaps
manages shop floor equipment
J. Crowder


understand need for security
get why security measures
familiar with basic security policies
tries to follow security rules
careful with sensitive information
not store important on laptop
acknowledges bypassing is bad
had training
Staff Interview
not a security expert
Perhaps
basic security knowledge
J. Crowder

J. Crowder is not a security expert but has basic security awareness, understanding the need for security measures. He makes an effort to follow the company's security policies like being careful with sensitive information.

As Crowder often works offsite from his laptop, he does not store sensitive data on his laptop and acknowledges the risks of bypassing security. His awareness shows his understanding of possible vulnerabilities although his priority on convenience can sometimes outweigh security practices.


fast paced work nature
daily hurry
G
unexpected changes
work pressure
work theme hurry
Often
fast work tempo
A Day in the Life of a Manufacturing Production Manager
constant communication
offsite security frustrations
J. Crowder
issues with offsite connection
Staff Interview
Ocassionally
challenges working remotely
public wifi isnt always reliable

7.2.2. External Reference

Document	Version	Authors	Date	Description
A Day in the Life of a Manufacturing Production Manager	1	Alpha Manufacturing	26 March 2021	https://www.alphamanufacturing.co.uk/news/a-day-in-the-life-of-a-manufacturing-production-manager
Buzzle Case study	1	Donna Naadu Botchway	2024-09-02 00:00:00	Staff Information
Staff Interview	1	Donna Naadu Botchway	2024-09-01 00:00:00	Interview between CTO J. Turek and Production Manager J. Crowder
The daily life or hell of a production manager	1	Podcast, FasTALKS	5 May 2020	https://www.fastems.com/blog/the-daily-life-or-hell-of-a-production-manager/

7.2.3. Factoids

Characteristic	Persona	Variable	Modal Qualifier	Grounds	Warrant
personal laptop use	J. Crowder	Activities	Perhaps	not store important on laptop, personal laptop use, works offsite from a laptop	works remote mostly
production manager	J. Crowder	Activities	Perhaps	creates the master production schedule, oversees the production schedule,relies on inventory management system,works with j. turek on design feasibility	has root access to majority of systems,key to electronic component production
works remotely	J. Crowder	Activities	Frequently	challenges working remotely,manages shop floor equipment remotely,often on the go,remotely manages equipment,works offsite from a laptop,works remote mostly	spends alot of time offsite
uses public wifi	J. Crowder	Activities	Frequently	connect to network via public wifi,uses public wifi hotspots,uses whatever wifi available	convinience over security,knows public wifi is unsafe
engineering background	J. Crowder	Aptitudes	Perhaps	key to electronic component production,strong engineering background	works with j. turek on design feasibility
little corncern for security	J. Crowder	Attitudes	Perhaps	convinience over security,doesnt dive into security details,little concern for security,might ignore urgent issues,tempted to bypass security	IT responsible for security,doesnt deal with much sensitive data,not a security expert
issues with security measures	J. Crowder	Attitudes	Perhaps	security checks slow down production,security measures as obstacles,security measures not always practical,security protocols take time,tempted to bypass security,uncomfortable	need for better balance in security,prefers streamlined access process,wonders how secure offsite connection is

				with current security measures	
security training impractical	J. Crowder	Attitudes	Perhaps	training feels like a check,training not applicable,training wasnt useful	prefers job-specific security training
offsite security frustrations	J. Crowder	Environment Narrative	Ocassionally	challenges working remotely,issues with offsite connection,offsite security frustrations	public wifi isnt always reliable
fast work tempo	J. Crowder	Environment Narrative	Often	daily hurry,fast paced work nature,unexpected changes,work pressure,work theme hurry	constant communication,offsite security frustrations
focus on production task	J. Crowder	Motivations	Often	focus on getting the job done,focused on production running smoothly,prioritizes production tasks over security	avoids letting security interfere with work
prefers job-specific security training	J. Crowder	Motivations	Perhaps	need for better balance in security,prefers job-specific security training,suggests streamlining security measures	training not applicable
works with inventory system	J. Crowder	Skills	Perhaps	relies on inventory management system,works with inventory system	creates the master production schedule,plans out production
manages shop floor equipment	J. Crowder	Skills	Perhaps	ensures functioning of shop floor equipment,manages shop floor equipment remotely	oversees the production schedule
basic security knowledge	J. Crowder	Skills	Perhaps	acknowledges bypassing is bad,careful with sensitive information,familiar with basic security policies,get why security measures,not store important on laptop,tries to follow security rules,understand need for security	had training,not a security expert

7.2.4. Document References

Name	External Document	Contributor	Excerpt
oversees the production schedule	Staff Interview	Donna Naadu Botchway	Sure, J. My main job is to oversee the production schedule and make sure everything on the shop floor runs smoothly
works with inventory system	Staff Interview	Donna Naadu Botchway	I work closely with the inventory management system to plan out production based on customer orders and ensure we have the necessary materials on hand.
plans out production	Staff Interview	Donna Naadu Botchway	I work closely with the inventory management system to plan out production based on customer orders and ensure we have the necessary materials on hand.
spends alot of time offsite	Staff Interview	Donna Naadu Botchway	I also spend a lot of time off site, so I remotely manage some of the shop floor equipment to make sure everything's running as it should
remotely manages equipment	Staff Interview	Donna Naadu Botchway	I also spend a lot of time off site, so I remotely manage some of the shop floor equipment to make sure everything's running as it should
issues with offsite connection	Staff Interview	Donna Naadu Botchway	Honestly, the biggest challenge is staying connected to the company's network when I'm off site
public wifi isnt always reliable	Staff Interview	Donna Naadu Botchway	Public Wi Fi isn't always reliable, and it can be a pain to deal with connection issues
offsite security frustrations	Staff Interview	Donna Naadu Botchway	Also, sometimes the security measures we have in place slow me down, especially when I'm in a hurry to fix something remotely
understand need for security	Staff Interview	Donna Naadu Botchway	I understand the need for security, but it does get frustrating at times
works remotely mostly	Staff Interview	Donna Naadu Botchway	But most of the time, I'm working remotely, so I access the systems through my laptop
personal laptop use	Staff Interview	Donna Naadu Botchway	But most of the time, I'm working remotely, so I access the systems through my laptop
workstation use	Staff Interview	Donna Naadu Botchway	When I'm in the office, I use my workstation like everyone else.
often on the go	Staff Interview	Donna Naadu Botchway	I connect to the company net work using whatever Wi Fi is available—usually public Wi Fi since I'm often on the go

uses whatever wifi available	Staff Interview	Donna Naadu Botchway	I connect to the company net work using whatever Wi Fi is available—usually public Wi Fi since I'm often on the go
convinience over security	Staff Interview	Donna Naadu Botchway	I know it's not ideal from a security standpoint, but it's the most convenient option for me.
knows public wifi is unsafe	Staff Interview	Donna Naadu Botchway	I know it's not ideal from a security standpoint, but it's the most convenient option for me.
security protocols take time	Staff Interview	Donna Naadu Botchway	The biggest challenge for me is the amount of time it takes to get through the security protocols, especially when I'm working remotely
challenges working remotely	Staff Interview	Donna Naadu Botchway	The biggest challenge for me is the amount of time it takes to get through the security protocols, especially when I'm working remotely
get why security measures	Staff Interview	Donna Naadu Botchway	I get why we have these measures, but they're not always practical when you're trying to get things done quickly
security measures not always practical	Staff Interview	Donna Naadu Botchway	I get why we have these measures, but they're not always practical when you're trying to get things done quickly
familiar with basic security policies	Staff Interview	Donna Naadu Botchway	I'm familiar with them on a basic level—I know the do's and don'ts, like not sharing passwords and being cautious with emails.
doesnt dive into security details	Staff Interview	Donna Naadu Botchway	But I'm not someone who's going to dive deep into the details.
prioritizes production tasks over security	Staff Interview	Donna Naadu Botchway	I've got a lot on my plate with production, so I just try to follow the rules as best I can without letting them interfere with my work
tries to follow security rules	Staff Interview	Donna Naadu Botchway	I've got a lot on my plate with production, so I just try to follow the rules as best I can without letting them interfere with my work
avoids letting security interfere with work	Staff Interview	Donna Naadu Botchway	I've got a lot on my plate with production, so I just try to follow the rules as best I can without letting them interfere with my work

had training	Staff Interview	Donna Naadu Botchway	Yeah, I've had the training, but to be honest, I didn't find it all that useful.
training wasnt useful	Staff Interview	Donna Naadu Botchway	Yeah, I've had the training, but to be honest, I didn't find it all that useful.
training not applicable	Staff Interview	Donna Naadu Botchway	A lot of it felt like common sense, and some of the scenarios they talked about didn't really apply to what I do.
focused on production running smoothly	Staff Interview	Donna Naadu Botchway	I'm more focused on making sure production is running smoothly, so the training sometimes feels like just another thing to check off the list
training feels like a check	Staff Interview	Donna Naadu Botchway	I'm more focused on making sure production is running smoothly, so the training sometimes feels like just another thing to check off the list
connect to network via public wifi	Staff Interview	Donna Naadu Botchway	There have been a few times when I've had to connect to the network over public Wi Fi, and I couldn't help but wonder how secure that connection really was.
wonders how secure offsite connection is	Staff Interview	Donna Naadu Botchway	There have been a few times when I've had to connect to the network over public Wi Fi, and I couldn't help but wonder how secure that connection really was.
focus on getting the job done	Staff Interview	Donna Naadu Botchway	But at the end of the day, I needed to get the job done, so I just went ahead with it.
IT responsible for security	Staff Interview	Donna Naadu Botchway	I figure that's what the IT department is for—if something's wrong, they'll let me know.
doesnt deal with much sensitive data	Staff Interview	Donna Naadu Botchway	I don't deal with a lot of sensitive information directly—that's more the finance team's area.
careful with sensitive information	Staff Interview	Donna Naadu Botchway	But when I do have to handle something sensitive, I try to be careful.
use secure network	Staff Interview	Donna Naadu Botchway	I make sure to use the secure network and not leave anything important on my laptop.
not store important on laptop	Staff Interview	Donna Naadu Botchway	I make sure to use the secure network and not leave anything important on my laptop.
finds security checks a hassle	Staff Interview	Donna Naadu Botchway	That said, I do find it a bit of a hassle to constantly double

			check that everything is secure, so I don't always go as far as I probably should
forwards issues to IT department	Staff Interview	Donna Naadu Botchway	I'd probably forward it to the IT department and let them handle it
not a security expert	Staff Interview	Donna Naadu Botchway	I'm not an expert in this stuff, so I'd rather leave it to the professionals
might ignore urgent issues	Staff Interview	Donna Naadu Botchway	But if it was something that seemed really urgent, I might just ignore it and keep working, especially if I'm in the middle of something import ant
uncomfortable with current security measures	Staff Interview	Donna Naadu Botchway	To be honest, I'm not entirely comfortable with them.
security measures as obstacles	Staff Interview	Donna Naadu Botchway	They seem like more of an obstacle than a help, especially when I'm trying to access the system quickly while off site.
prefers streamlined access process	Staff Interview	Donna Naadu Botchway	If I had my way, I'd prefer a more streamlined process, even if it meant a bit less security
tempted to bypass security	Staff Interview	Donna Naadu Botchway	I wouldn't say I've bypassed them, but I've definitely been tempted.
security checks slow down production	Staff Interview	Donna Naadu Botchway	When you're under pressure to keep production running smoothly, the last thing you want is to be slowed down by security checks.
acknowledges bypassing is bad	Staff Interview	Donna Naadu Botchway	I've thought about finding ways around them, but I know that's not a good idea in the long run
need for better balance in security	Staff Interview	Donna Naadu Botchway	I think we need to find a better balance between security and usability
suggests streamlining security measures	Staff Interview	Donna Naadu Botchway	Maybe there's a way to streamline some of the security measures so they don't slow us down as much
prefers job-specific security training	Staff Interview	Donna Naadu Botchway	Also, more practical, job specific training could be helpful—something that's really relevant to what we do every day, instead of just general security guidelines.
works remote mostly	Staff Interview	Donna Naadu Botchway	But most of the time, I'm working remotely, so I access the systems through my laptop
alot on plate with production	Staff Interview	Donna Naadu Botchway	I've got a lot on my plate with production, so I just try to follow

			the rules as best I can without letting them interfere with my work
strong engineering background	Buzzle Case study	Donna Naadu Botchway	Crowder has a strong background in engineering and is key to the company's electronic component production.
key to electronic component production	Buzzle Case study	Donna Naadu Botchway	Crowder has a strong background in engineering and is key to the company's electronic component production.
works offsite from a laptop	Buzzle Case study	Donna Naadu Botchway	Crowder often works off site from a laptop using public wifi hotspots to connect back to the company network.
uses public wifi hotspots	Buzzle Case study	Donna Naadu Botchway	Crowder often works off site from a laptop using public wifi hotspots to connect back to the company network.
little concern for security	Buzzle Case study	Donna Naadu Botchway	He has little concern for security, much to the annoyance of Trafford given his root access to majority of systems.
has root access to majority of systems	Buzzle Case study	Donna Naadu Botchway	He has little concern for security, much to the annoyance of Trafford given his root access to majority of systems.
relies on inventory management system	Buzzle Case study	Donna Naadu Botchway	Crowder relies on the inventory management system to create the master production schedule.
creates the master production schedule	Buzzle Case study	Donna Naadu Botchway	Crowder relies on the inventory management system to create the master production schedule.
works with j. turek on design feasibility	Buzzle Case study	Donna Naadu Botchway	Creates the master production schedule based on customer orders and inventory, Works with J. Turek to ensure new designs are feasible.
manages shop floor equipment remotely	Buzzle Case study	Donna Naadu Botchway	He also ensures the correct functioning of the shop floor equipment connected to the network, remotely managing these when off site.
ensures functioning of shop floor equipment	Buzzle Case study	Donna Naadu Botchway	Unknown
fast paced work nature	A Day in the Life of a Manufacturing Production Manager	Donna Naadu Botchway	The fast-paced nature of the manufacturing environment, with so many moving parts is what I love most about the job.
prepares report	A Day in the Life of a Manufacturing Production Manager	Donna Naadu Botchway	At the end of each day, I prepare a detailed handover report for the nightshift supervisor with updates on the progress of all

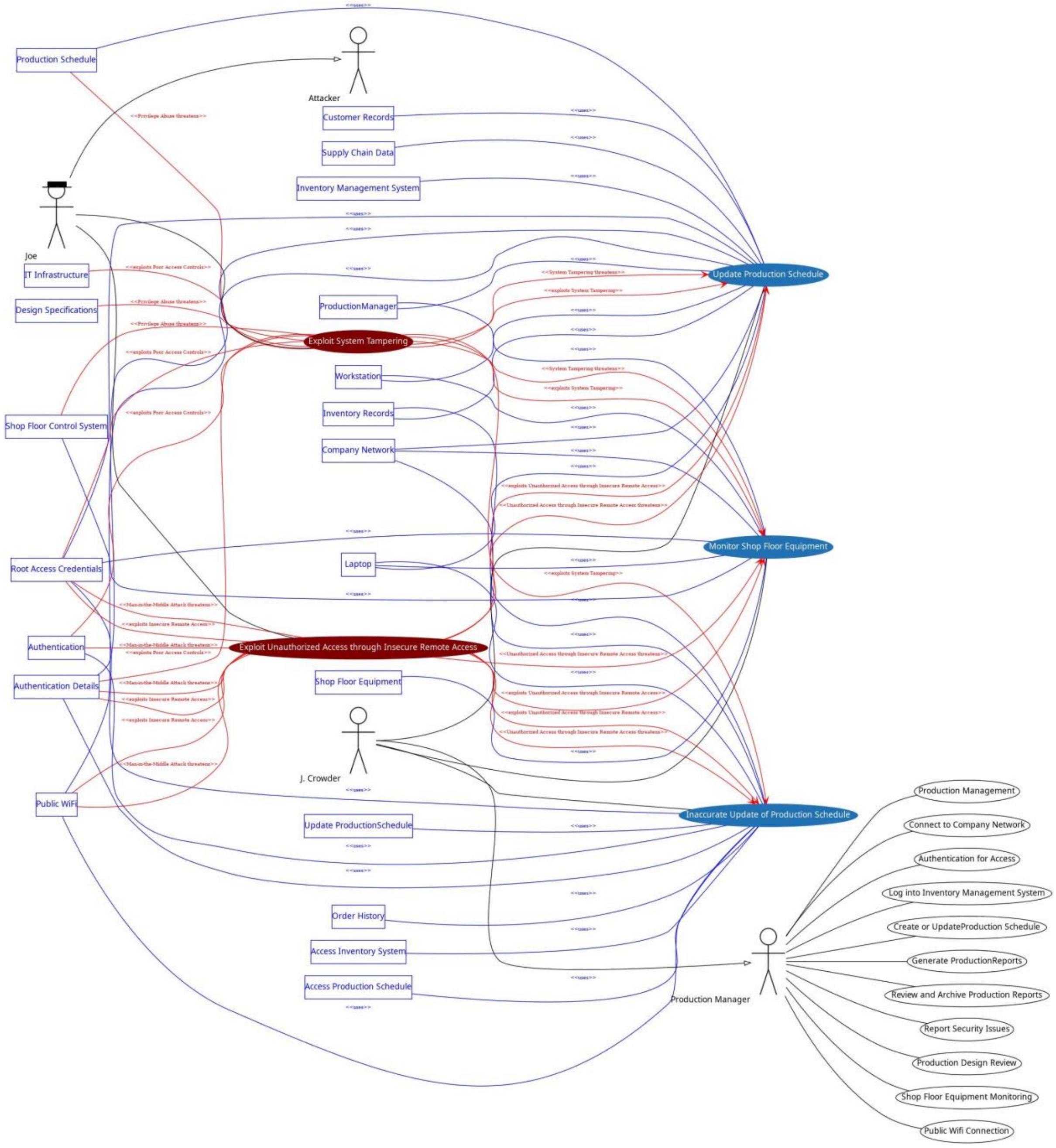
			parts, advising of any issues/ concerns from the day and setting priorities and actions during the shift.
constant communication	A Day in the Life of a Manufacturing Production Manager	Donna Naadu Botchway	Throughout the afternoon, I will stay in constant communication with all of the Production Supervisors, checking progress and addressing any issues. Strong communication between departments in manufacturing is crucial as there are so many deadlines and requirements running concurrently.
daily hurry	The daily life or hell of a production manager	Donna Naadu Botchway	The daily hurry and amount of unexpected changes keeps the production manager very busy.
unexpected changes	The daily life or hell of a production manager	Donna Naadu Botchway	The daily hurry and amount of unexpected changes keeps the production manager very busy.
work pressure	The daily life or hell of a production manager	Donna Naadu Botchway	This is caused by pressure from customers, i.e. meeting the promised delivery times, and from the manufacturing set-up itself, including all of its limitations, imperfections and of course the capacity
work theme hurry	The daily life or hell of a production manager	Donna Naadu Botchway	What does a typical production manager's day look like nowadays? If you look at the big picture the key theme is hurry.

7.3. Appendix 3: Usable Security Analysis

Below shows the interactions with the system and how the persona carries it out.

7.3.1. *Task Model*

The tasks are based on the production manager's workflow.


Production Schedule
Attacker
Customer Records
Supply Chain Data
Inventory Management System
Joe
IT Infrastructure
Design Specifications
Shop Floor Control System
Root Access Credentials
Authentication
Authentication Details
Public WiFi
ProductionManager
Exploit System Tampering
Workstation
Inventory Records
Company Network
Laptop
Exploit Unauthorized Access through Insecure Remote Access
Shop Floor Equipment
J. Crowder
Update ProductionSchedule
Order History
Access Inventory System
Access Production Schedule
Update Production Schedule
Monitor Shop Floor Equipment
Inaccurate Update of Production Schedule
Production Manager
Production Management
Connect to Company Network
Authentication for Access
Log into Inventory Management System
Create or UpdateProduction Schedule
Generate ProductionReports
Review and Archive Production Reports
Report Security Issues
Production Design Review
Shop Floor Equipment Monitoring
Public Wifi Connection
<<uses>>
<<Privilege Abuse threatens>>
<<exploits Poor Access Controls>>
<<Man-in-the-Middle Attack threatens>>
<<exploits Insecure Remote Access>>
<<System Tampering threatens>>
<<exploits System Tampering>>
<<exploits Unauthorized Access through Insecure Remote Access>>
<<Unauthorized Access through Insecure Remote Access threatens>>

7.3.1.1. Narrative of Inaccurate Update of Production Schedule

On a busy day, the Production Manager working offsite needed to update the production schedule quickly to keep up with fluctuating inventory levels and incoming orders. Using an available WiFi, probably a public Wi-Fi connection without a VPN, accessed the Inventory Management System and began making adjustments.

However, network interruptions caused delays, and in the rush to meet the production deadline, skipped double-checking some entries against the most recent inventory data. Feeling the pressure to update the schedule, the Production Manager prioritized completing the task over verifying every detail.

Unfortunately, the oversight led to an inaccurate production plan, disrupting the shop floor workflow and delaying order fulfillment.

7.3.1.2. Narrative of Update Production Schedule

The production manager using the inventory management system reviews current inventory and customer orders. Analyzing this data, the production schedule is updated to meet customer demands within the available production capacity and timelines. If gaps or shortages are identified, the production manager adjusts the schedule accordingly and communicates with suppliers to replenish inventory as needed.

7.4. Appendix 4: Threat Analysis

7.4.1. Data flow

The Production Manager connects to the company network via a workstation or if offsite, VPN using laptop. After authentication, they access the inventory management system to update the production schedule or monitor shop floor equipment. They review production designs with the Chief Technology Officer and generate production reports. These reports are archived, and sensitive data is protected. The IT department is notified of security issues. External elements like public Wi-Fi are outside the Production Manager's trust boundary, while production-related processes and datastores are within it.

The Data flow shows interactions between data, processes and the system.

Name	**From**	**Type**	**To**	**Type**	**Assets**	**Obstacles**
Access Inventory Data	Log into Inventory Management System	process	Inventory Database	datastore	• Authentication Details • Inventory Database • Inventory Records • Order History • Root Access Credentials • Supply Chain Data	None
archive report	ProductionManag	entity	Review and Archive Production Reports	process	• Office Related Files	None
Confirm status	Shop Floor Equipment Monitoring	process	Shop Floor Control System	datastore	• Authentication Details	None
Connecting to Company Network	Workstation	entity	Connect to Company Network	process	• Authentication Details •Company Network	None

Connecting to Company Network	Laptop	entity	Connect to Company Network	process	• Authentication Details • Company Network	None
Create or Update Schedule	ProductionManag	entity	Create or UpdateProduction Schedule	process	• Inventory Records • Order History • Production Schedule	None
generate report	ProductionManag	entity	Generate ProductionReports	process	• Production Schedule	None
internet	Public WiFi	entity	Public Wifi Connection	process	• IP Address	None
internet access	Public Wifi Connection	process	Laptop	datastore	• IP Address	None
Log into IMS	ProductionManag	entity	Log into Inventory Management System	process	• Authentication Details	None
Monitor Equipment	ProductionManag	entity	Shop Floor Equipment Monitoring	process	• Authentication Details • Production Schedule	None
Network Access	Connect to Company Network	process	Company Network	datastore	• Authentication Details	None
report security issues	ProductionManag	entity	Report Security Issues	process	• Email Accounts	None

reported	Report Security Issues	process	IT Department	datastore	• Email Accounts • Office Related Files	None
review design	Production Design Review	process	Design Specifications	datastore	• Office Related Files • Production Schedule	None
review design	ProductionManag	entity	Production Design Review	process	• Design Specifications	None
save report	Review and Archive Production Reports	process	Office Related Files	datastore	• Office Related Files	None
save report	Generate ProductionReports	process	Office Related Files	datastore	• Office Related Files	None
Save Schedule	Create or UpdateProduction Schedule	process	Inventory Database	datastore	• Production Schedule	None
User Authentication	Authentication for Access	process	Domain Controller Datastore	datastore	• Authentication Details •Domain Controller Datastore •Root Access Credentials	None
VPN Connection	Virtual Private Network	entity	Authentication for Access	process	• Authentication Details	None

7.4.2. Vulnerability

The identified vulnerabilities below arise due to the nature of Buzzle Inc's culture and systems.

7.4.2.1. Insecure Remote Access

A vulnerability resulting from an error in the configuration and administration of a system or component. It has severity as critical. Assets affected include Public Wi-Fi, and Authentication Details (Root Access Credentials)

When employees like J. Crowder connect to the company network using whatever available Wi-Fi (public Wi-Fi) without a Virtual Private Network (VPN) when not in the office, they create a serious security risk. Public Wi-Fi is often unencrypted, making it easy for attackers like Joe to intercept the connection. Using simple tools like packet sniffers or rogue access points, Joe can perform a Man-in-the-Middle (MITM) attack. This lets him capture sensitive information, such as login credentials or session tokens, which can then be used to gain unauthorized access to the system. Once in, Joe can move further into the company's network, potentially causing a data breach or system compromise. The risk introduced by this insecure remote access can lead to major security threats, putting sensitive company data and systems at significant risk.

7.4.2.2. Poor Access Controls

A vulnerability resulting from an error in the configuration and administration of a system or component. It has severity as catastrophic. Assets affected include IT Infrastructure, and Authentication Details (Root Access Credentials)

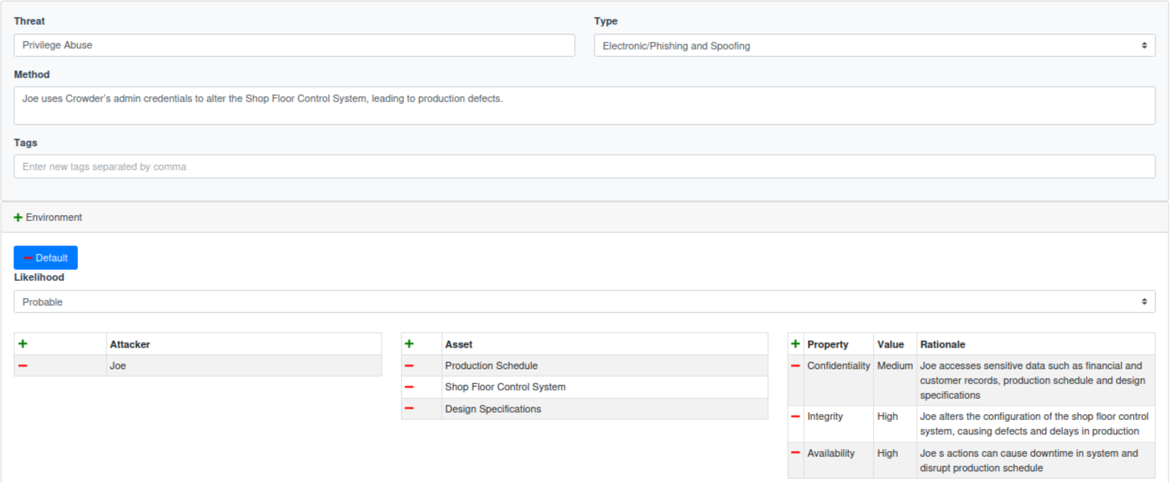
Roles and permissions are not properly enforcing the principle of least privilege, granting users and processes excessive permissions. Crowder has admin-level access to sensitive data, which far exceeds what his role demands. This creates an opportunity for unauthorized access to critical systems.

7.4.3. Threat

Below are threats identified that impact the system.

7.4.3.1. Privilege Abuse

I referred to CAPEC 122



Threat
Privilege Abuse

Type
Electronic/Phishing and Spoofing

Method
Joe uses Crowder's admin credentials to alter the Shop Floor Control System, leading to production defects.

Tags
Enter new tags separated by comma

Likelihood
Probable

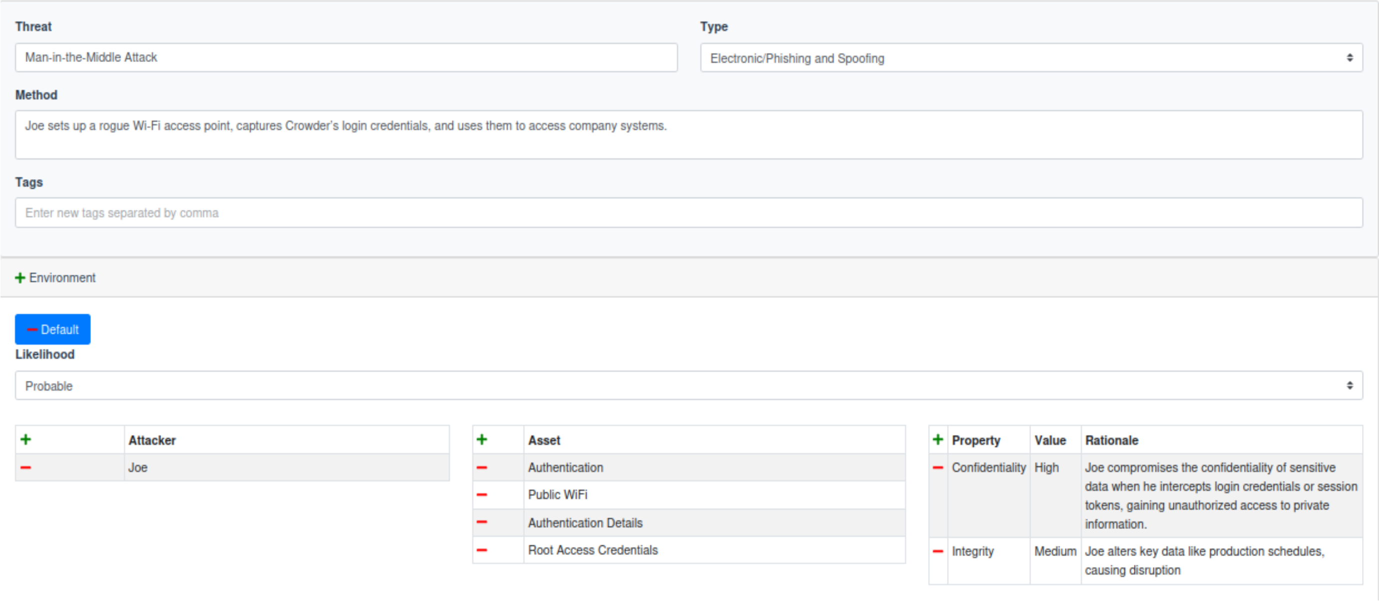
+	Attacker
−	Joe

+	Asset
−	Production Schedule
−	Shop Floor Control System
−	Design Specifications

+	Property	Value	Rationale
−	Confidentiality	Medium	Joe accesses sensitive data such as financial and customer records, production schedule and design specifications
−	Integrity	High	Joe alters the configuration of the shop floor control system, causing defects and delays in production
−	Availability	High	Joe s actions can cause downtime in system and disrupt production schedule

7.4.3.2. Man-In-The-Middle Attack

I followed CAPEC 94.



Threat

Man-in-the-Middle Attack

Type

Electronic/Phishing and Spoofing

Method

Joe sets up a rogue Wi-Fi access point, captures Crowder's login credentials, and uses them to access company systems.

Tags

Enter new tags separated by comma

+ Environment

− Default

Likelihood

Probable

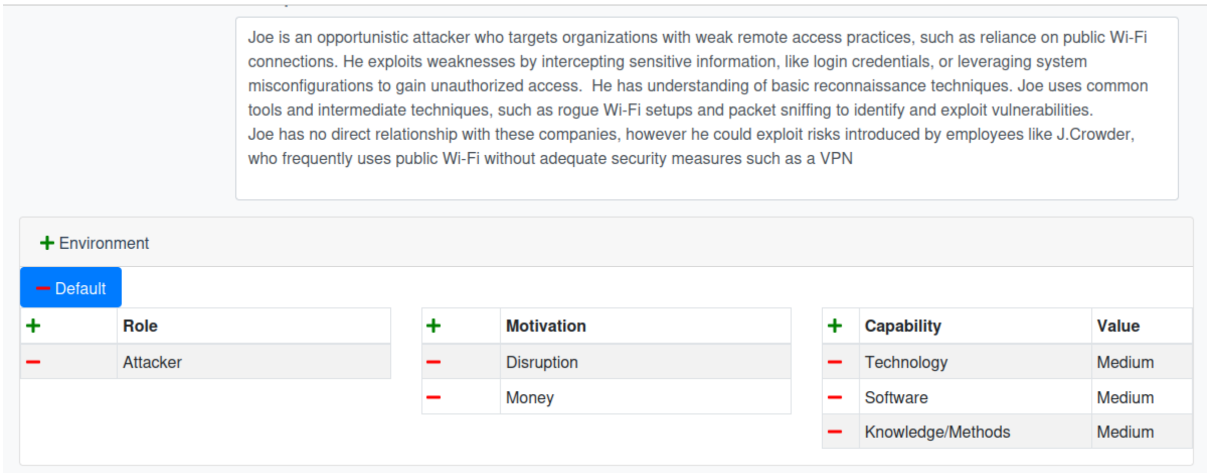
+	Attacker
−	Joe

+	Asset
−	Authentication
−	Public WiFi
−	Authentication Details
−	Root Access Credentials

+	Property	Value	Rationale
−	Confidentiality	High	Joe compromises the confidentiality of sensitive data when he intercepts login credentials or session tokens, gaining unauthorized access to private information.
−	Integrity	Medium	Joe alters key data like production schedules, causing disruption

7.4.4. *Attacker*

The attacker launches attacks in the shape of threats and take advantage of the vulnerabilities described above.



Joe is an opportunistic attacker who targets organizations with weak remote access practices, such as reliance on public Wi-Fi connections. He exploits weaknesses by intercepting sensitive information, like login credentials, or leveraging system misconfigurations to gain unauthorized access. He has understanding of basic reconnaissance techniques. Joe uses common tools and intermediate techniques, such as rogue Wi-Fi setups and packet sniffing to identify and exploit vulnerabilities.
Joe has no direct relationship with these companies, however he could exploit risks introduced by employees like J.Crowder, who frequently uses public Wi-Fi without adequate security measures such as a VPN

+ Environment

− Default

+	Role
−	Attacker

+	Motivation
−	Disruption
−	Money

+	Capability	Value
−	Technology	Medium
−	Software	Medium
−	Knowledge/Methods	Medium

7.4.5. *Misuse Case*

Risk arises when attackers launch attacks to target the above threats exposing the vulnerabilities. Misuse case covers the scenario and what happens when an attacker exploits each risk identified.

7.4.5.1. Exploit Unauthorized Access through Insecure Remote Access

Joe sets up a rogue Wi-Fi access point. J. Crowder, who often works remotely and is frequently on the move, connects to Joe's Wi-Fi while using public networks without a VPN. Joe, using a packet sniffing tool like Wireshark, intercepts Crowder's login credentials and session tokens. This allows Joe to gain unauthorized access to the company's internal systems. Unfortunately for Crowder, he uses his root access credentials, which Joe captures. With this access, Joe searches through the company’s systems, locating and manipulating the production schedule. This disruption causes operational chaos and severely damages the company’s reputation.

7.4.5.2. Exploit System Tampering

Joe, after gaining access to Crowder’s root-level credentials, which doesn’t require privilege escalation, logs into the company’s systems. Joe then accesses the Shop Floor Control System which is needed for managing production schedules, inventory, and equipment status. Joe tampers with the configurations, changing production progress and other quality control parameters. This causes defects in the manufacturing process, leading to delays and operational downtime.