7808ICT T1 Project and Cyber Security Management

Assessment 1 - Cyber Attacks, Issues and

Project Description (Option 2)

R.I.S.E.

Resilience Improvement through Security Enhancement

Prepared by

ZeroDay Response Team, Nathan Campus

Henry Ng, s5423376, (Project Manager and Team Leader)

Minhaj Ahmed, s5419774, (Security Architect)

Ansaf Althaf, s5405482, (Security Engineer)

Sherina Lu, s2717884, (Security Analyst)

11/04/2025

Table of Contents

1. Project Introduction

1.1. Project Title

Resilience Improvement through Security Enhancement: Tackling Phishing through Stronger IT Systems and Smarter Teams.

1.2. Background

Our project proposal is underpinned by two incredibly important articles written by SOC Radar and Trendmicro to address the key issues of cybersecurity attacks (with a special focus on email phishing) in the automotive industry (SOC Radar, 2024; Trendmicro, 2023). These articles surmised that numerous issues have arisen that can be attributed to the increasingly digitised system in which we live in and the systems that we have come to rely on (Griffiths, 2025). This is evidenced by reporting over the last two decades, whereby, cybersecurity attacks have increased from 6 persons being victimised every hour, to 97 persons every hour (Griffiths, 2025). The automotive industry has not been immune from this trend either, as statistics illustrate that there has been a consistent increase in cyberattacks across this industry. According to Pangarkar (2025), cybersecurity attacks in the automotive industry increased by 225% from 2018 to 2021. Furthermore, from 2022 to 2023, cybersecurity attacks have increased by more than 50% in this same industry (Messe Munchen GmBH, 2024).

This ever-increasing trend clearly illustrates that there is a gap between the people who work in the automotive industry and those entrusted with the cybersecurity knowledge and training of critical IT infrastructure required to protect against cyberattacks. As such, it has been observed that a clear opportunity is present for companies within the automotive industry to either implement new security systems or to integrate enhanced security systems within current IT

systems, enhance their risk and incidence management, as well as increasing cybersecurity training for workers in order to strengthen their cyber protection to prevent further cyberattacks.

1.3. Project Objectives

This project aims to address the challenges that the FeatherDrive Flying Car Company has experienced in relation to email phishing. The main goals of this project are to strengthen the company's cybersecurity posture by implementing new security systems to be integrated within the current working systems and improve cyber incident management. Furthermore, the project seeks to develop and implement new training for workers, to better protect themselves when using the organisation's computer systems.

This project contains these key objectives:

- To address and reduce the email phishing attacks the company has experienced
- To address the risk and incident management processes in this organisation
- To review and strengthen the existing IT systems the organisation is using
- To address the challenges staff members, encounter with the current technology used within the organisation.

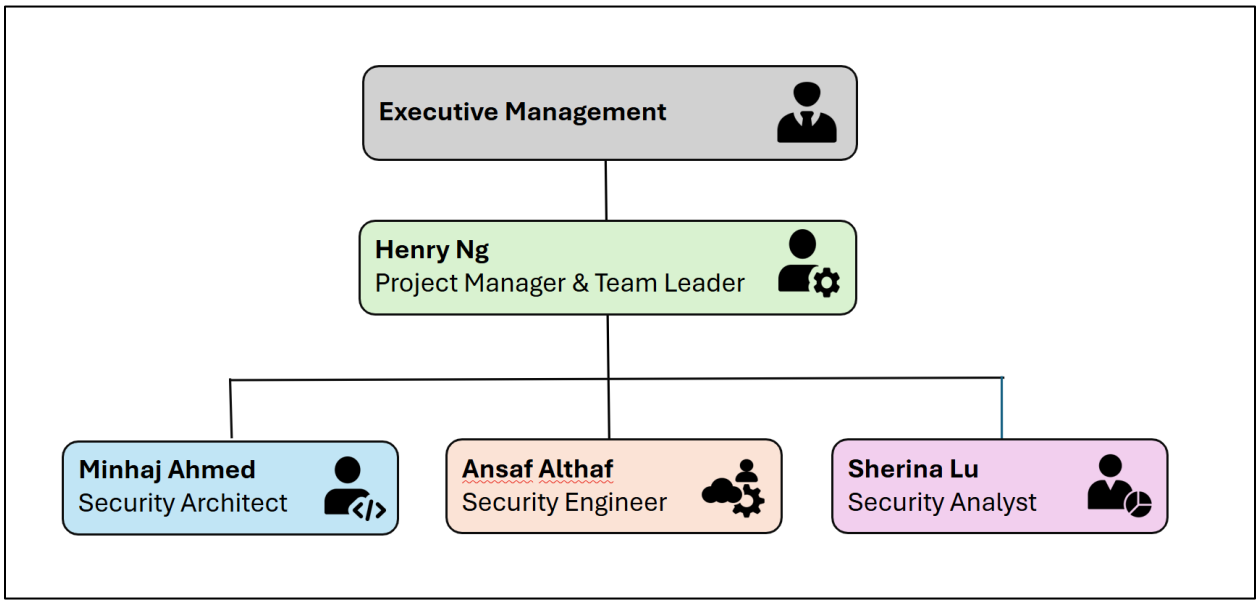
The output will consist of:

- Developing a comprehensive report of the cyberattacks the company has experienced
- Enhancing the company's cyber incident management process
- Implementing new and compatible security systems to integrate with the existing IT systems
- Enhancing the network security infrastructure to ensure robust systems are implemented to prevent further email phishing and other cybersecurity attacks

- Developing a thorough employee training program to ensure all staff members understand and are aware of how to appropriately react to cybersecurity threats

1.4. Organisation Structure

Figure 1. Organisation structure of this project



This illustration depicts the organisation structure for this project. We are led by Henry Ng, our Project Manager and Team Leader. Minhaj Ahmed is our Security Architect, followed by Ansaf Althaf, our Security Engineer. Sherina Lu is then our Security Analyst. The communication flow for this project consists of the Security Architect, Security Engineer and Security Analyst all communicating their work and progress to Team Leader and Project Manager, Henry Ng. Henry then liaises with the Chief Information Officer to discuss project progress, issues and setbacks. He will also be solely responsible for communicating with the executives in upper management and portfolio management.

In this project, the team leader (Henry Ng) is responsible for providing leadership to team members and ensuring that team performance is strong as well as complimentary to the organisation's regulations and policies.

In Henry Ng's role as project manager, he is responsible for providing governance at the project level to the other team members, conducting risk assessments, allocating project budget and resources, as well as ensuring that the team members are meeting all of their project deadlines and deliverables, in addition to adhering to their timelines and resources. Henry is also responsible for having and maintaining an open line of communication with key stakeholders of this project.

As the Security Architect for this project, Minhaj Ahmed is responsible for creating and designing security systems as well as identifying risks and vulnerabilities in the current IT systems.

In this project, Ansaf Althaf, fulfills the role of Security Engineer. He is responsible for implementing the new security systems as well as integrating them into the current IoT (Internet of things) platforms. Ansaf is also responsible for developing new firewalls and solving any technological problems in the system.

Lastly, Sherina Lu is the Security Analyst for this project. Sherina oversees the observation of the hardware, software and networks in the organisation's systems and will respond accordingly to any cyber threats that arise within these components.

2. Cyber Security Attacks or Issues or Challenges

2.1. Formal Definitions and Concepts

Phishing is defined as attackers impersonating legitimate and trustworthy sources to acquire sensitive personal information and login credentials through electronic communication such as social media platforms, online or auction sites, as well as payment services (Bhavsar et al., 2018). It also represents a type of social engineering attack which targets victims mainly via email communications (Bhavsar et al., 2018). According to Basit et al. (2020), phishing is termed as a cyberattack where the attacker tricks the victim into revealing login credentials or providing sensitive data through emails and malicious links, causing password compromise and data theft.

In the above definition, social engineering is a term used for a wide range of fraudulent activities, including phishing, to manipulate users into security errors and providing sensitive information (Bhavsar et al., 2018). This project will focus on three of the more common types of Phishing attacks: namely, Email Phishing, Man-in-the-Middle, and Spoofing.

2.2. Definition Types of Phishing

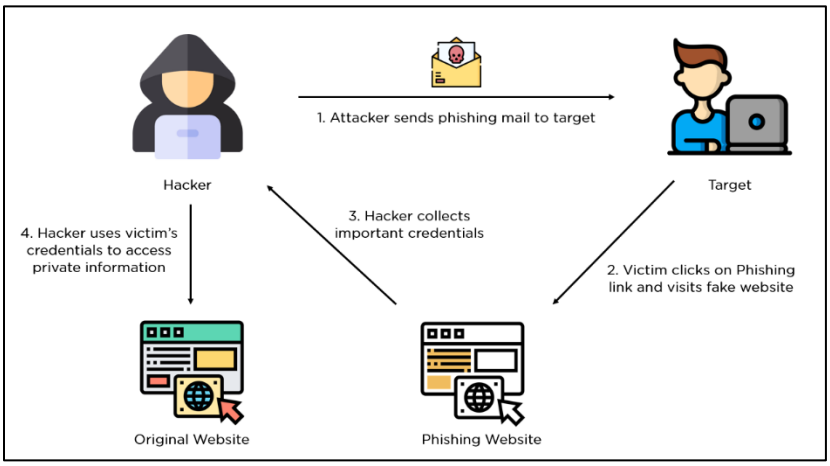
2.2.1. Email Phishing

Email phishing is termed as a cyber-attack which occurs when scammers mimic trusted entities to lure the target user into revealing user credentials and critical information, or clicking on malicious links, primarily through emails (Nadeem et al., 2023). Bhavsar et al (2018) posit a similar definition, whereby they described phishing as “a form of attack designed to deceive a

victim, which was more often initiated via an email". It is this definition that will be used throughout this paper.

Figure 2.

General concept of an email phishing attack



From *What is Phishing Attack? Definition, Types and How to Prevent it* by Jena, B. K, 2022, (https://www.simplilearn.com.cach3.com/tutorials/cryptography-tutorial/what-is-phishing-attack.html)

A "real world" example of an email phishing incident took place at a Toyota subsidiary in 2019. Lindsey (2019) surmised that the Toyota Boshoku Corporation lost $37 million dollars because of a business email phishing attack. In this attack, a hacker pretended to be a business partner and emailed the finance and accounting department, asking them to send money to a specific bank account controlled by the hacker (Lindsey, 2019). The email address looked remarkably like the genuine email address, making it hard to notice the scam (Lindsey, 2019). As such, the employee did not think twice before following the instructions through the phishing link (Lindsey, 2019).

2.2.2. Man In The Middle

A Man-in-the-Middle attack (MITM) refers to a third-party intruder that discreetly intercepts and alters the communication between two legitimate participants for malicious intent without their knowledge, allowing the attacker to control the information being exchanged (Cekerevac et al., 2025). According to Valentjin (2024), Man-in-the-Middle is also defined as an attack which occurs when an attacker intercepts a user's communication with a legitimate website. The attacker builds a fraudulent website that completely imitates the trustworthy website and then persuades the victim to give away their login access credentials and multi-factor authentication (MFA) code (Valentjin, 2024).

In the above definition:

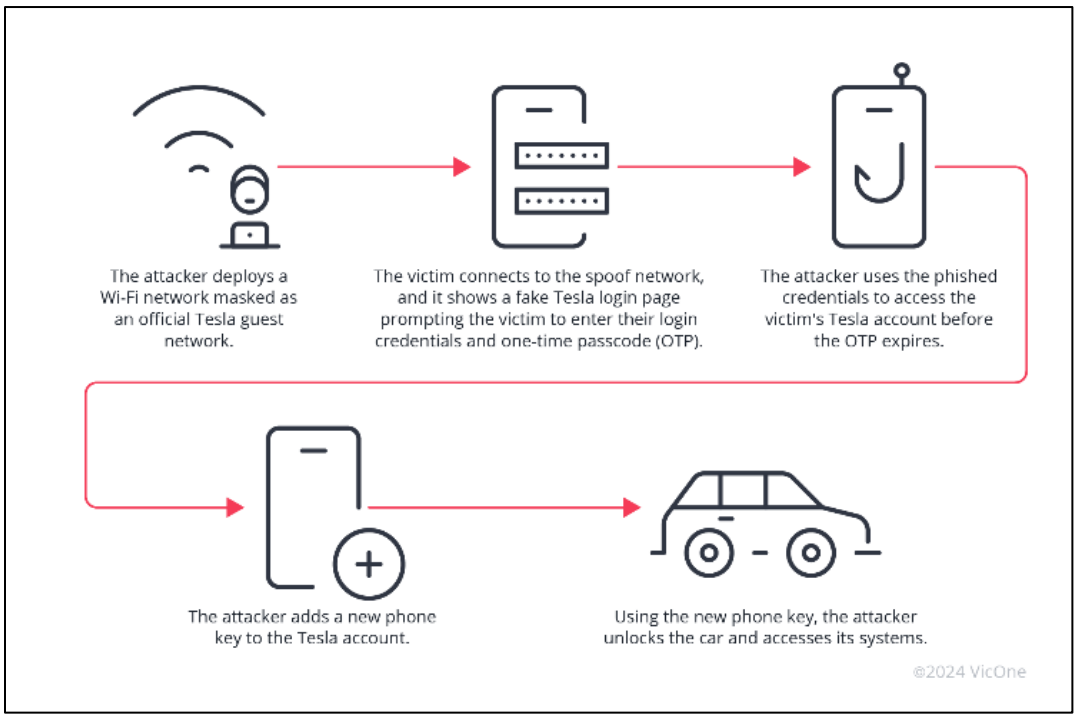
- Legitimate is defined as authentic, trustworthy and reliable, which can be verified by policies, secure networks and connections (Cekerevac et al., 2025).
- Multi-Factor Authentication (MFA) is a security process where users need to confirm their identity by providing more than one form of identification such as a password and a one-time code sent to their mobile phone or email (Valentjin, 2024).

A “real world” example of a MITM attack is as follows. Two researchers Yang and Cheng (2024) revealed that Tesla cars were vulnerable to theft via a MITM phishing attack. The process begins with an attacker setting up a fake Wi-Fi access point that mimicked a legitimate Tesla network, often at charging stations (Yang & Cheng, 2024). They explained that when Tesla owners connected to this network, they encountered a fraudulent login page resembling Tesla’s official site. If the owners entered their credentials, the attacker captured this information to access the real Tesla service. Yang and Cheng (2024) further said attackers could also bypass MFA by showing a fake prompt to obtain the owner's one-time passcode. Attackers could then

view vehicle information and create a digital key, allowing them to unlock and steal the Tesla (Yang & Cheng, 2024). The flowchart below demonstrated how the attack took place.

Figure 3.

The attack chain of the Telsa MITM phishing attack



From *How a Credential Phishing Attack Could Lead to Tesla Car Theft and How to Mitigate It* by Yang. O, & Cheng. L, 2024, (https://vicone.com/blog/how-a-credential-phishing-attack-could-lead-to-tesla-car-theft-and-how-to-mitigate-it)

2.2.3. Spoofing

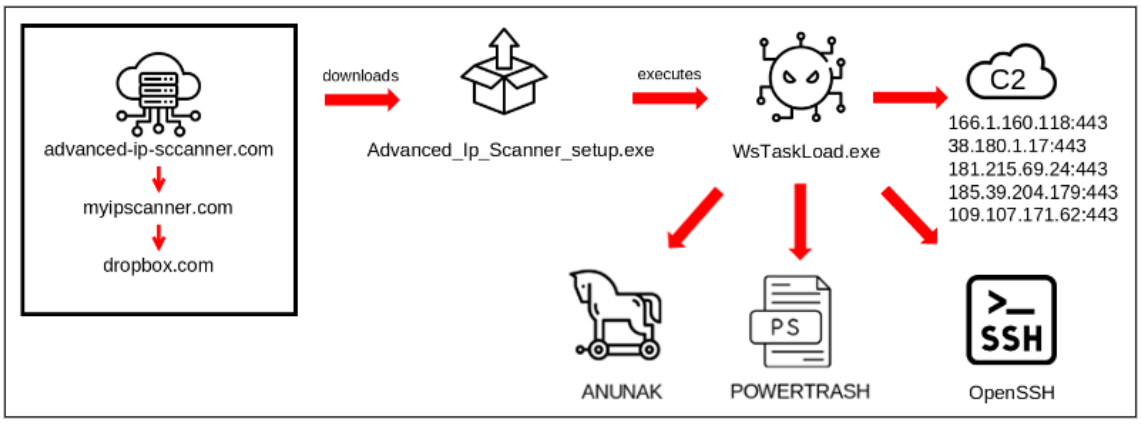
Spoofing is defined by Javanmardi et al. (2023) as a type of cyber-attack in which an invader uses fake characteristic information, such as email addresses, website URL, or IP addresses, to commit malicious acts. According to Alkhalil et al. (2021), a spoofed email is a deceptive email sent to a group of people from an untrusted sender by imitating a trustworthy

source to gain the trust of the recipient. It leads them to unknowingly sharing personal or financial information (Alkhalil et al., 2021).

A “real world” example of spoofing comes from an article in which it was reported that a large American car manufacturer experienced an email spoofing attack (Toulas, 2024). FIN7, a Russian based criminal group, began its attack by sending spoofing emails to key IT employees, illustrated in the flowchart below (*See Figure 4*). As seen in the flowchart, the emails contained links that led to "advanced-ip-sccanner[.]com," a fake version of the real site "advanced-ip-scanner.com." (Toulas, 2024). Researchers then found that this fake site redirected users to "myipscanner[.]com," (Toulas, 2024). From there, visitors were directed to a Dropbox page where they downloaded a malicious file called 'WsTaskLoad.exe,' disguised as the legitimate Advanced IP Scanner installer (Toulas, 2024). When executed, the file initiated a multi-stage process that involved DLLs, WAV files, and shellcode execution (Toulas, 2024). This process ultimately loaded a decrypted file called 'dmxl.bin,' which contained the Anunak backdoor payload, one of the malware tools FIN7 used to gain remote access to the compromised system (Toulas, 2024).

Figure 4.

The attack chain of the FIN7’s spoofed email attack



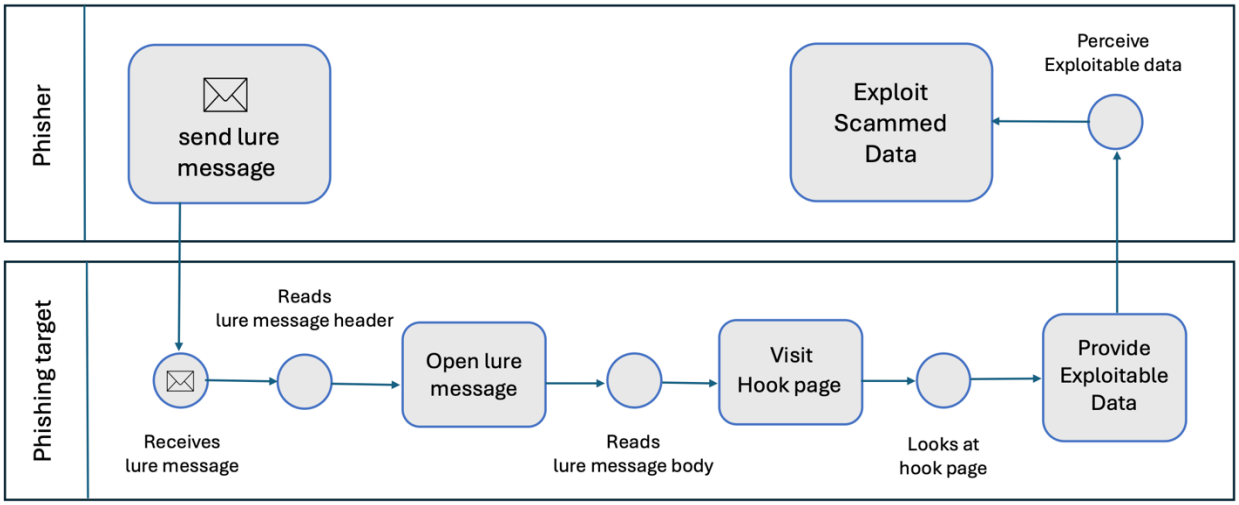
From *FIN7 targets American automaker's IT staff in phishing attacks* by Toulas. B, (2024), (https://www.bleepingcomputer.com/news/security/fin7-targets-american-automakers-it-staff-in-phishing-attacks/)

2.3. The Conceptual Models of The Attacks/Issues/Challenges

Phishing is a deceptive cyberattack where attackers attempt to trick individuals into revealing sensitive information such as passwords, bank details, or personal data (Wagner, 2024). This process typically unfolds in four steps. First, the attacker sends a lure message, usually an email or text disguised as communication from a trusted source like Microsoft or Amazon (Wagner, 2024). Next, the recipient is enticed to click a link within the message, which redirects them to a counterfeit website designed to mimic the legitimate one (Wagner, 2024). On this fake site, the victim unknowingly enters their confidential information (Wagner, 2024). Finally, the attacker exploits this stolen data to gain unauthorised access to accounts, commit financial fraud, or sell the information on the dark web. (Wagner, 2024).

Figure 5.

A general workflow of phishing attacks



2.4. The Goal and Landscape of The Attacks/Issues/Challenges

Phishing attacks are motivated by several damaging objectives and outcomes, chief of which is thought to be financial theft, whereby attackers use extortion, ransomware, or fraudulent fund transfers to misappropriate funds, usually using business email compromise attacks (McNeal, 2022).

Data theft is another significant risk. As data is incredibly valuable to businesses, cybercriminals target data to either demand ransom, sell it for a profit, or cause supply chain breaches (McNeal, 2022). Another significant consequence of phishing is identity theft, in which criminals take personal data such as names, addresses, or medical records and sell them on the dark web or use them for other illegal purposes (McNeal, 2022).

Furthermore, the desire to exercise authority and control is another driving force behind attacks (GCS Network, 2024). This is evidenced by insider threats, which originate from within the organisation (GCS Network, 2024). These threats pose a serious cybersecurity risk since they can be motivated by retaliation, in which disgruntled workers target the organisation to harm them, damage their reputation, and cause emotional distress (GCS Network, 2024).

The landscape of the attack, or the attack surfaces, includes all the vulnerable points through which an attacker can gain access to and exploit, and can be broadly categorised into digital, physical device, and social engineering attack surfaces (Illumio, 2025).

The digital attack surface covers internet-facing assets such as websites, servers, databases, laptops, cloud services, and third-party providers (Illumio, 2025). As more devices connect to the network, the attack surface grows, increasing risk (Illumio, 2025). The device attack surface includes all physical hardware such as workstations, mobile devices, routers, switches, printers, and even security cameras (Illumio, 2025). Once a device is compromised,

attackers can move deeper into the network (Illumio, 2025). The social engineering attack surface refers to the human element inside an organisation and their behavioural vulnerabilities which may lead to security breaches (Illumio, 2025). Attackers trick employees into giving access to their systems using methods such as email phishing, impersonating service personnel, or planting infected USB drives (Illumio, 2025). In this way, human error often becomes the easiest way for attackers to breach a company's defences (Illumio, 2025).

3. Vulnerabilities In The Existing Environment

3.1. Current State of Technology Environment

The automotive industry is becoming increasingly competitive with car manufacturers seeking to maintain a competitive edge through the development of connected cars, employing innovative ideas that have rapidly transformed and evolved as the industry progresses. (Andriiuk & Sokolova, 2025).

Andriiuk and Sokolova (2025) suggested that innovations such as Artificial Intelligence (AI), additive manufacturing or 3D-printing, the Internet of Things (IoT), and 5G are driving product development and enhancing manufacturing efficiency, leading to an enhanced customer experience in the industry.

They further explained that the ways in which humans interact with connected cars, with features such as navigation, remote diagnostics, and over-the-air updates are more enhanced than ever before. In addition, a shift in customer trends in terms of better safety features, connectivity and personalised experience in their vehicles, has meant that many companies have developed their own IoT platforms to better engage with buyers so that the new buyers are able to seamlessly connect their vehicles with mobile devices, meaning that physical car keys are no

longer required. Similarly, drivers' personal details and preferences are also saved which assists owners to customise their own vehicles (Andriiuk & Sokolova, 2025).

An additional impact on the automobile manufacturing landscape is the impact of robotics and automation within the automobile manufacturing process (International Federation of Robotics, 2024). A recent study from the International Federation of Robotics (IFR) (International Federation of Robotics, 2024) confirmed that the automotive sector has become the leading adopter of industrial robots, making up 33% of all installations in the United States, (International Federation of Robotics, 2024). The study from the IFR surmised that this early adoption has assisted such companies to reduce labour costs, increase productivity through the provision of real-time monitoring and optimisation of the manufacturing process. Such a notion is especially true for substantially large car manufacturers that rely on suppliers, dealers, staff and customers all over the world and advances as highlighted above, along with advanced analytics and automation within, inventory and supply chain controls has enabled efficiency improvements across the sector. (International Federation of Robotics, 2024).

FeatherDrive Flying Cars Company, is a large-scale company with around 10,000 staff across the Asia Pacific and Europe, the company is currently undergoing a digital transformation in an effort to streamline communications within the teams, and as a result, staff members are increasingly becoming more reliant on online communication tools such as email and the company's IT systems as a means of interacting with the customers, staff, and suppliers across the globe, etc. The move to increase usage of online forms of communication, along with customer data going online has resulted in increased customer and company convenience through the ability to access the information remotely, anytime and anywhere, with a commensurate improvement in communications, both internally and externally.

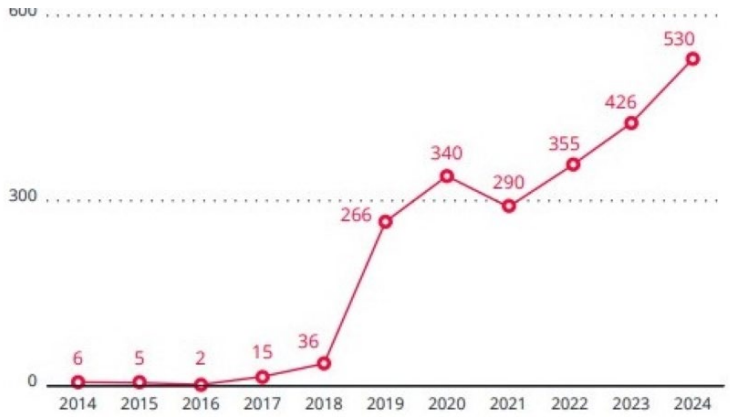
A converse problem that has arisen through such innovations and uptake of communications improvements has been the increased exposure to the possibility that malicious actors or hackers are able to exploit either software flaws or human error as a means of accessing sensitive staff/customer data. Such data is most a risk through inattention, poor security protocols, or inadequate investment in infrastructure, training or appropriate cybersecurity counter measures.

3.2. Existing System Vulnerabilities

The automotive industry as a whole and not just the FeatherDrive Flying Cars Company, face several existing system vulnerabilities, particularly as vehicles become increasingly connected and automated. It is reported by Vakulov (2025) that the industry reached a record high of 530 vulnerabilities in 2024, an increase of 24% from the previous year in 2023, with more than 77% of these related to onboard or in-vehicle systems. The two figures below explain these changes in further detail.

Figure 6.

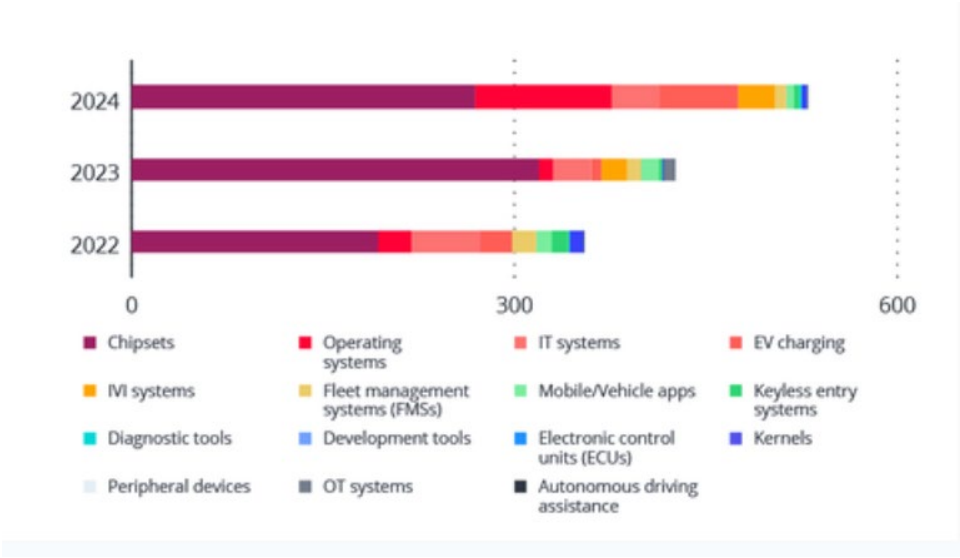
Number of automotive vulnerabilities published from 2014 to 2024



From *Shifting Gears for 2025: The Next Generation of Automotive Cybersecurity Challenges* by Vakulov, A, 2025, (https://www.forbes.com/sites/alexvakulov/2025/01/25/cybersecurity-threats-to-modern-cars-how-hackers-are-taking-control/)

Figure 7.

Distribution of automotive vulnerabilities from 2022 to 2024 by affected system or component



From *Shifting Gears for 2025: The Next Generation of Automotive Cybersecurity Challenges* by Vakulov, A, 2025, (https://www.forbes.com/sites/alexvakulov/2025/01/25/cybersecurity-threats-to-modern-cars-how-hackers-are-taking-control/)

Vakulov (2025) proposed five major vulnerabilities faced by the automotive manufacturers:

1. Weak authentication enables hackers to gain access to sensitive systems.
2. Systems are centralised storing copious amounts of sensitive, user and vehicle data, increasing the risk of data breaches.

3. Numerous connected car platforms possess data encryption issues, making them susceptible during transmission.
4. Ineffective integration with third-party apps creates security issues.
5. Manufacturers are slow to identify and address vulnerabilities, leading to vehicles being unprotected for longer than necessary.

As suggested in the example from the previous section, researchers found that Tesla cars were vulnerable to hackers via MITM phishing attacks (Yang & Cheng, 2024). They demonstrated how they could access the victims' account and view the drivers' information resulting in the ability to steal the Tesla cars (Yang & Cheng, 2024). Indeed, the result of hacking into connected vehicles are more than just financial losses. They also disrupt car operations or road safety which potentially creates physical danger to the public (Yang & Cheng, 2024). The importance of these hacks demonstrating the ease of access to confidential information stored on car systems and the value such data is to hackers cannot be overlooked or understated. (Yang & Cheng, 2024).

In addition, the automotive industry is increasingly reliant on various software systems to interact with staff and consumers alike (Vakulov, 2025). FeatherDrive Flying Cars Company, by way of example, has a Customer Relationship Management (CRM) system for customer data, Enterprise Resource Planning (ERP) for inventory & supply chain information, while the IoT platform is used to review real-time equipment status updates. When taking into consideration the numerous systems the company employs, threats across all these systems should be considered. This is due to these systems being open to compromise not only through staff actions, but those of external customers such as suppliers or car dealers (Vakulov, 2025). If suppliers and dealers do not maintain cybersecurity standards which are consistent with those of

the parent company, data may potentially be exploited by the external parties, leading to data breaches due to human error or software flaws (Vakulov, 2025).

Considering that an increasing number of connected cars are coming to the market, personal data exposure is another vulnerability that is emerging within the automotive industry (Linnell, 2025). The author posited that connected cars collect vast amounts of data, including location and driving behaviour, which can be targeted for unauthorised access or misuse. The author argued that it is important for the industry to address the vulnerabilities by implementing compatible security systems or providing thorough staff training programmes in order to reduce any kind of cyberattacks (Linnell, 2025).

3.3. Loopholes and Threats

With the increasing number of cyberattack incidents in the industry each year, it is essential for FeatherDrive Flying Car Company to address its vulnerabilities and resolve internal issues. Bale (2024) identified common cybersecurity loopholes, with weak passwords topping the list. He noted that many users create simple or easily guessable passwords, resulting in a demonstrated 80% of data breaches through compromised credentials. Furthermore, phishing attacks are another prevalent cybersecurity threat; statistics reveal that 1 in 99 emails is a phishing attempt, and 30% of these emails are opened (Bale, 2024). A significant factor contributing to the issues within the FeatherDrive Flying Car Company is the lack of security awareness among employees, evidenced by staff members receiving threatening emails purportedly from "HR" as well as phishing emails from "their offshore boss". Bale (2024) also pointed out that companies with inadequate access controls and insufficient data encryption are at a heightened risk of experiencing data breaches. This article illustrates that vulnerabilities arise

from employees exploiting excessive access rights and the presence of unencrypted data (Bale, 2024).

FeatherDrive Flying Car Company faces several cybersecurity threats due to identified loopholes. Lavrov et al. (2021) summarised the potential threats in the following ways. Firstly, weak passwords can lead to stolen account credentials and brute force attacks, while phishing attacks risk data theft and malware infections. Secondly, a lack of security awareness among employees increases vulnerability to social engineering and insider threats (Lavrov et al, 2021). Thirdly, inadequate access controls may result in unauthorised data access and data leaks, while insufficient data encryption leaves sensitive information exposed during breaches (Lavrov et al, 2021). Addressing these vulnerabilities will enhance the company's cybersecurity posture significantly, which we will discuss further in this project.

3.4. Attackers' Targets

The vulnerabilities at FeatherDrive Flying Car Company present several targets for attackers.

Weak passwords primarily allow unauthorised access to user accounts, enabling attackers to steal confidential company data and information from staff members or customers (Lavrov et al, 2021). Phishing attacks directly target employees, aiming to trick them into revealing credentials or clicking on malicious links that could lead to malware infections and financial losses (Lavrov et al, 2021). The lack of security awareness among staff makes internal processes vulnerable, as attackers can manipulate employees (either due to human error or without proper training) into compromising security (Lavrov et al, 2021). Inadequate access controls create opportunities for attackers to access sensitive data and systems that should be restricted, while

insufficient data encryption leaves unprotected data open to theft during breaches (Lavrov et al, 2021). By exploiting these vulnerabilities, attackers seek to steal confidential information and disrupt operations, ultimately leading to a loss of integrity and the potential for data corruption or unauthorised access.

4. Technical Issues

4.1. State of The Art Technologies and Issues

Most technologies present today, have mainly utilised outdated email filters and instructing staff members on what to be aware of when reading emails to prevent email phishing attacks (Ling et al., 2025). However, this reliance on basic software and instructing staff members to be more meticulous when reading emails, has largely been unsuccessful in preventing further cybersecurity attacks (National Cyber Security Centre, 2018). Furthermore, the email phishing methods that hackers use to gain entrance into an organisation's system are becoming increasingly more sophisticated, leaving most organisations in the position of trying to bridge the gap between their system detection and prevention methods, with hackers' skills and talents (Ling et al., 2025).

Additionally, there have been issues with third party vendors in the past (Van Enckevort, 2024). Third party vendors are defined as companies external to the organisation that provide IT services and can access the organisation's IT systems and networks (Van Enckevort, 2024). Due to the plethora of vendors that organisations can utilise to implement their IT systems, it is possible that there may be a difference in security standards that organisations were unaware they needed to circumnavigate, which is an element that hackers can leverage to gain unauthorised access (Van Enckevort, 2024). The failures of organisations to continually monitor

and adjust to this ever-changing cybersecurity landscape, clearly illustrates that solutions need to be more holistic, have multiple layers and be more targeted to the specific organisation and their cybersecurity requirements.

4.2. Technical Measures For The Solution

The first technical measure is introducing more robust email security software. This technique involves strengthening the organisation system's threat detection and protection. This is done by incorporating different elements such as spam filtering to recognise malicious or suspicious emails, and block them from being sent, as well as encrypting email correspondence so only the intended recipient receives it (Rao et al., 2024). Such a method also assists to maintain the integrity of the data in the system (Rao et al., 2024).

The second technical measure is implementing Multi-Factor Authentication (MFA). The MFA technique consists of requesting users to submit more than two forms of identification elements to gain access into a system (Klivan et al., 2023). For example, requesting a user's email address and password along with a special code sent to their trusted device, reduces the likelihood of attackers being able to gain access to all of the user's sensitive login data (Mukherjee, 2023).

The third technical measure is implementing role-based access controls in the organisation's systems. This provides an administrator the ability to grant and restrict access to certain elements of the system based on their job role within the organisation (McCarthy, 2025). An example of a role-based access control technique is identifying who requires access to the system's networks and servers, such as IT staff and system administrators, and granting them

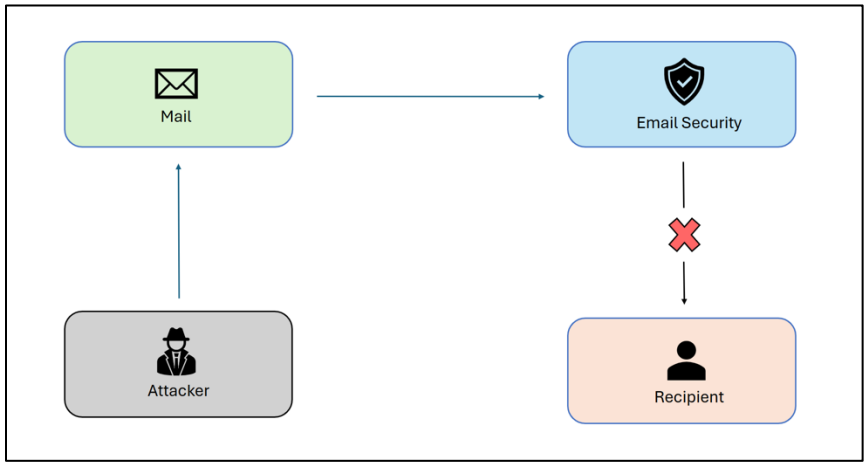
access (McCarthy, 2025). However, this same technique would then not grant access to these same components to the receptionist or secretary.

4.3. Types of Attacks That Can Be Addressed

The types of attacks that can be addressed utilising the three technical measures listed above come under various forms of phishing. They entail email phishing, spoofing, MITM and brute force attack.

Figure 8.

A brief diagram illustrating how email security software works

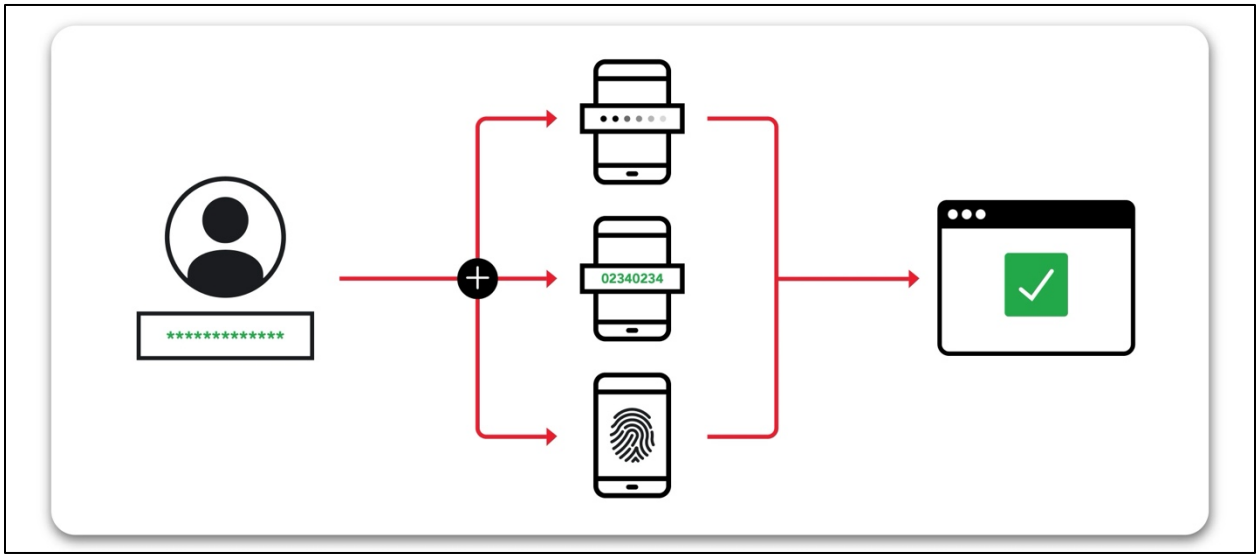


The implementation of a more robust email security software will ensure that all emails undergo a thorough analysis process before being either encrypted, filtered or blocked. Any malicious or suspicious emails that are identified would be prevented from reaching any staff member's inboxes (Rao et al., 2024). This software also ensures sensitive data is secured and cannot be leaked via email (Rao et al., 2024). Furthermore, this measure will lead to increased operational efficiency, as time will not have to be dedicated to incident response, thus increasing

the productivity output in the organisation (Rao et al., 2025). It also integrates well with the ERP system by strengthening the data security, fortifying communication channels and preventing data breaches (Rao et al., 2025).

Figure 9

The MFA Login Process



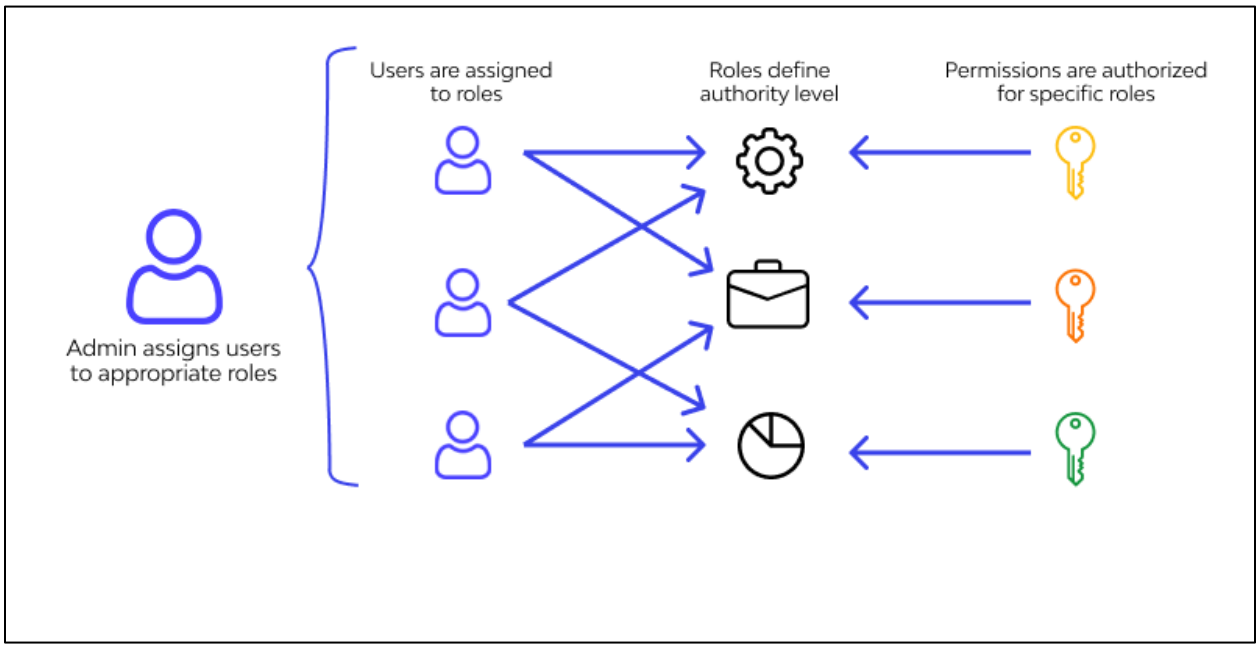
From *Ranking the Different Types of Multi-Factor Authentication (MFA)*, by Mancini, A, 2024, Impact, https://www.impactmybis.com/blog/ranking-mfa-types/

The implementation of adaptive MFA essentially prioritises cybersecurity risks and threats by placing a barrier between users and hackers. As a user is required to provide more than two forms of identification, even if one form of identification is breached, it remains difficult for a hacker to not only gain access to a system, but also then attempt to send phishing emails for the same purpose (Mukherjee, 2023).

This means that MFA is particularly valuable in reducing the risk of MITM attacks, as it increases the amount of user data that a hacker requires to gain access into a system (Valentijn, 2024). The MFA method will also integrate well with the ERP and will provide a more proactive approach to preventing cybersecurity attacks in the organisation (Mukherjee, 2023).

Figure 10

A diagram illustrating the process of role-based access control



From *What is RBAC (Role-Based Access Control)?* by Lee, I, 2025, Wallarm, https://www.wallarm.com/what/what-exactly-is-role-based-access-control-rbac

The implementation of role-based access controls in an organisation allows the administrator and company officials to have more control regarding which people are accessing what parts of the system at any given time (McCarthy, 2025). The staff members at an organisation are categorised by their roles and then given certain permissions based on their roles (McCarthy, 2025). This restriction on data and systems means hackers must navigate around

various layers of permission controls and privileges, reducing the rates of data loss and breaches (McCarthy, 2025). Role-based access controls will integrate easily with ERP as it allows secure access to data, processes and systems, leading to more optimised workflows (McCarthy, 2025).

4.4. Constraints and Limitations

There are some constraints and limitations associated with the implementation of the three technical measures discussed. For example, the implementation and utilisation of email security software can lead to instances of false positives, where legitimate emails are blocked and are not sent through to the intended recipient (Ling et al., 2025). This can then cause communication to break down between staff members or their clients (Ling et al., 2025).

The most prominent limitations with multi-factor authentication reside with the users. With the addition of extra forms of proof of identification that require recalling, it is relatively easy for users to feel frustrated and tired with the process, leading them to potentially forget their passwords (Mukherjee, 2023). The added layers of login complexity may also cause users to deliberately choose weaker passwords that are not only easier to remember, but make the login process less time-consuming, but run the risk of being easily compromised (Mukherjee, 2023).

The main limitation for remote-based access controls, concerns not only its implementation but how it is applied for future use. It does not provide organisations flexibility once organisations expand and obtain new staff members, leading to roles and permissions being out of alignment (McCarthy, 2025). Furthermore, this ongoing process of ensuring users are categorised into the correct roles and given the correct permissions is also a time-consuming task (McCarthy, 2025).

There are limitations that apply to all the technical measures mentioned above. They include expensive implementation costs due to software licensing as well as migration costs from having to integrate the new system with the existing one (Halyday, 2022). There are also ongoing fees associated with support and maintenance of the systems as well as staff training costs that also need to be factored in and considered (Halyday, 2022).

5. Impact, Benefits and Risks

5.1. Impact of The Attack/s

Phishing attacks lead to severe impacts to an organisation (CybSafe, 2023). Stolen credentials and data breaches, when the user clicks on malicious emails or links, bring about significant data loss (CybSafe, 2023). Attackers may gain full access to sensitive company data, which could be stolen or manipulated, and used for further crimes, held for ransom or sold on the dark web (CybSafe, 2023). Companies may have high costs expended on identity protection services, compensating affected customers or employees, and handling transfers caused by fraudulent personification (CybSafe, 2023).

Phishing attacks are not simply minor security issues; they also severely disrupt a company's daily operations (CybSafe, 2023). When an attacker successfully gains access to an organisation's network through phishing, they can install harmful software which cause systems to collapse (CybSafe, 2023). These shutdowns are likely to deprive employees of the ability to access important files, or even completely turn off critical operations (CybSafe, 2023).

The result of aforementioned attacks is likely to be a major loss of productivity because employees are not able to perform their tasks until the issue is resolved (CybSafe, 2023). Vital

services might cease, platforms may go offline, and the organisation's ability to provide service to the customers is likely affected (CybSafe, 2023). While most organisations manage to restore operations within 24 hours, nearly 41% of those who suffer significant financial, or data loss take more than a day to completely recover (CybSafe, 2023). Such delays can cost companies heavily in terms of sales, trust, and customer loyalty in the long run, while also resulting in loss of company value (CybSafe, 2023). Investors may lose confidence in the credibility of the organisation, leading to a downfall in market value (CybSafe, 2023).

Beyond financial, data and operational loss, phishing attacks cause serious impact on the employees (Davies, 2023). With stolen credentials and personal data, attackers bring about major damage to an individual's reputation (Davies, 2023). The affected employees could feel anxious and stressed, affecting their productivity and mental health (Davies, 2023). It could also result in detrimental psychological consequences if the attacker utilises fear tactics to make the employee make hasty decisions without careful forethought (Davies, 2023). In addition, news of a data breach also triggers customers to lose faith in the organisation (Davies, 2023). Regardless of the company's established reputation, the public may identify it as an unreliable entity, leading to long-term damage to its brand image and bringing about a decline in business (CybSafe, 2023).

After the incident has occurred, employees would have to dedicate a significant amount of time resetting passwords, restoring accounts and reporting incidents, which slows down business operations (Davies, 2023). It also instils constant fear, fatigue, and stress in the employees of being victimised by another phishing attack, often leading to job dissatisfaction (Davies, 2023). A toxic culture, where the management blames the employees for falling victim to the attack and being irresponsible, would most likely make an individual doubt their abilities and weaken their morale (Davies, 2023).

5.2. Outcomes and Goals

This project revolves around mitigating the serious impacts caused by phishing in the company. The project outputs are aligned to establish a strong security defence system and the fostering of a strong security culture at FeatherDrive Flying Cars. This is enabled through:

- Improving Data Security Measures: This project will implement robust encryption procedures to protect data from security breaches. Access to sensitive information will be restricted to authorised employees based on their position or role, and continuous monitoring of critical systems will be enforced. We will also be implementing MFA which requires employees to confirm their identities using multiple forms of identificatio (such as password and a one-time code sent to their mobile phone).
- Data Loss Prevention and Risk Management: Our implementation would impose policies to strictly monitor the activities related to and sharing of sensitive data, and regular backup strategies to restore any disruptions swiftly.
- Enhancing Security Incident Response and Vulnerability Management: A solid incident management framework will be set up. This procedure will include assessments, automated alerts and retaliation mechanisms to prevent escalation of the attack and minimise system disruptions.
- Employee Awareness and Training Programs: Employees will be trained to recognise and avoid phishing patterns, emails and links and report them to reinforce a strong security mindset at FeatherDrive Flying Cars.

The goal of the outlined outputs is to tackle the vulnerable security systems in the organisation, which is apparent by the recent events of phishing attacks and password

compromise. The objectives of the project also include mitigating sensitive data leaks and theft, as indicated by the threats received by the employees about their professional and personal lives. It also aims at addressing the susceptibility of the employees to phishing attacks and foster a resilient security culture at the organisation.

5.3. Benefits: New and Enhanced Capabilities

One of the primary benefits by implementing MFA and advanced email filtering systems is, the likelihood of successful phishing attacks will be drastically minimised (Pawar, 2024) MFA requires employees to verify their identities using multiple factors, such as a password and a one-time code sent to their mobile phone, making it nearly impossible for attackers to compromise accounts with stolen credentials alone, reducing data breaches by 81% (Pawar, 2024). Advanced email filtering systems will block malicious emails before they reach employees, reducing exposure to phishing attempts. FeatherDrive Flying Cars can expect a reduction in phishing success rates by 86%, significantly mitigating credential theft and unauthorised access (Baker & Cartier, 2025).

Another critical reduction that is bought about through the application of implementing these measures is in the financial losses caused by cyberattacks. Likewise, preventing data breaches through strong encryption protocols, role-based access controls, and continuous monitoring will mitigate the financial impact of phishing attacks (IBM, 2024). According to a report by IBM in 2024, the average cost of a phishing attack globally as of 2024, is $4.91 million which includes expenses related to identity protection services, compensating affected customers or employees, and handling fraudulent transactions (IBM, 2024). By implementing these

measures, FeatherDrive Flying Cars could save approximately 70% of potential financial losses annually, preserving millions in revenue.

This project could potentially reduce downtime caused by cyberattacks. Automated threat detection systems and incident response frameworks will enable rapid containment of threats, ensuring that critical operations resume quickly after an attack. FeatherDrive Flying Cars enhanced systems could reduce recovery time by 60%, enabling employees to access important files and restore vital services without prolonged delays (Araiza, 2025).

In addition to the stated reductions, this project will improve data security and privacy through advanced encryption protocols, role-based access controls, and continuous monitoring. These measures will safeguard sensitive company data against unauthorised access and employee awareness programs will further strengthen cybersecurity culture by educating staff on recognising phishing attempts and minimising human error-related incidents.

5.4. Cyber Risks, Prioritisation and Analytics

Risks stemming from phishing attacks and password compromises present a critical threat to operational continuity, financial stability, and organisational integrity (Illumio, 2025). These risks are compounded by the increasing reliance on digital infrastructure, including email systems, CRM, ERP, and IoT platforms. As digital dependency deepens, so too does the organisation’s exposure to exploitation, particularly through human-centric vulnerabilities such as social engineering and poor credential hygiene (Illumio, 2025).

Email systems and staff credentials remain the primary targets of phishing campaigns, with attackers employing sophisticated deception tactics to gain unauthorised access and

quantitative metrics from industry sources underscore the gravity of these threats. (Illumio, 2025) According to the 2024, IBM Cost of a Data Breach Report, phishing remains the most financially damaging initial attack vector, averaging USD $4.91 million per incident. The report illustrates not only the direct losses attributed to phishing, but also the cascading costs of reputational damage, regulatory penalties, and operational downtime (IBM, 2024).

Risk prioritisation is conducted through the evaluation of both the likelihood of occurrence and the magnitude of potential impact (Bale, 2024). In FeatherDrive Flying Car's case, phishing and password-related threats rank at the highest tier characterised by a high frequency of attempted breaches and a substantial impact on internal systems and customer trust. (Bale, 2024) Recent research suggests that over 80% of breaches involve stolen or weak credentials, while approximately 30% of phishing emails are opened by recipients, highlighting the persistent vulnerability of end-users to deception (Bale, 2024).

To manage these risks effectively, the deployment of adaptive Multi-Factor Authentication (MFA) is expected to significantly reduce the success rate of credential-based attacks, with studies indicating a potential reduction of up to 99% (Mancini, 2024). Advanced email filtering solutions, incorporating artificial intelligence and cloud-based threat detection, have demonstrated the capability to block approximately 86% of phishing emails before they reach users (Rao et al., 2024). The integration of these technologies will enhance the organisation's capability to detect and respond to threats more efficiently, while also minimising the cognitive burden on employees.

Furthermore, employee awareness programs remain an essential component of the risk reduction strategy. By increasing staff vigilance and response accuracy, such programs can lower

the incidence of human error by as much as 55% (CybSafe, 2023). The combination of technical controls and human-centric interventions provides a robust foundation for resilience (CybSafe, 2023).

In conclusion, this proposal has illustrated that the through the implementations of above-mentioned measures, FeatherDrive Flying Cars will be better equipped to manage the complex cybersecurity threats it faces, safeguarding both its digital infrastructure and organisational reputation.

References

Alkhalil, S., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science,* 3(1), 1–23. https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full

Andriiuk, A. & Sokolva. V. (2025, March 21). Key Technology Trends in the Automotive Industry in 2025. *Epicflow*. https://www.epicflow.com/blog/5-latest-trends-in-the-automotive-industry/#:~:text=New%20technology%20in%20the%20automotive,revolutionary%20changes%20in%20customer%20experience.

Araiza, R (2025, March 31). *Automated Threat Hunting: How to Stay Ahead of Cyber Threats*. (2025). Digitalguardian. https://www.digitalguardian.com/blog/automated-threat-hunting-how-stay-ahead-cyber-threats

Baker , E & Cartier, M (2025, February 26). *Phishing Trends Report (Updated for 2025)*. Hoxhunt. https://hoxhunt.com/guide/phishing-trends-report#failure-rate-improvement-by-industry

Bale, S. (2024, September 13). *Common Cybersecurity Loopholes and How to Fix Them*. LinkedIn. https://www.linkedin.com/pulse/common-cybersecurity-loopholes-how-fix-them-suddhir-bali-vubbe/

Basit, A., Safar, M., Liu, X., Javed, A. R., Jalil, S., & Kifayat, K. (2020). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, 76(1). https://doi.org/10.1007/s11235-020-00733-2

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on Phishing Attacks. *International Journal of Computer Applications,* 182(33), 27–29. http://dx.doi.org/10.5120/ijca2018918286

Cekerevac, S. P., Cekerevac, P., Prigoda, L., & Al-Naima, F. (2025). SECURITY RISKS FROM THE MODERN MAN-IN-THE-MIDDLE ATTACKS. *MEST Journal,* 13(1), 34–51. https://doi.org/10.12709/mest.13.13.01.04

CybSafe (2023, July 3). The ripple effect: How one phishing attack can cause disaster across your organisation. *CybSafe*. https://www.cybsafe.com/blog/how-can-phishing-affect-a-business/

Davies, V. (2023, April 27). The psychological impact of phishing attacks on employees. *Cybermagazine.* https://cybermagazine.com/articles/the-psychological-impact-of-phishing-attacks-on-your-employe

GCS Network (2024, November 13). The Psychology Behind Cyber Attacks. (2024). *Global Cyber Security Network*. https://globalcybersecuritynetwork.com/blog/the-psychology-behind-cyber-attacks/

Griffiths, C. (2025, January 1). *The Latest 2025 Cyber Crime Statistics.* Aag-It. https://aag-it.com/the-latest-cyber-crime-statistics/

Halyday, S. (2022, March 11). Tips on implementing a new ICT system. *Qao.* https://www.qao.qld.gov.au/blog/tips-implementing-new-ict-system

IBM (2024). *Cost of a data breach report 2024.* IBM. https://www.ibm.com/reports/data-breach

Illumio (2025). Attack Surface - Cybersecurity 101. Illumio. https://www.illumio.com/cybersecurity-101/attack-surface

International Federation of Robotics. (2024, April 30). *U.S. Companies Invest Heavily in Robots - IFR Preliminary Results*. IFR. https://ifr.org/ifr-press-releases/news/u.s-companies-invest-heavily-in-robots

Javanmardi, S., Shojafar, M., Mohammadi, R., Alazab, M., & Caruso, A. M. (2023). An SDN perspective IoT-Fog security: A survey. *Computer Networks*, *229*, 109732. https://doi.org/10.1016/j.comnet.2023.109732

Jena, B. K. (2022, February 15). *What is Phishing Attack? Definition, Types and How to Prevent it.* Simplilearn. https://www.simplilearn.com.cach3.com/tutorials/cryptography-tutorial/what-is-phishing-attack.html

Klivan, S., Holtervenhoff, S., Huaman, N., Krause, A., Simko, L., Acar, Y., Fahl., S. (2023, November 26-30). *"We've Disabled MFA for You." An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments* [Conference Session]. Conference on Computer and Communications Security, Copenhagen, Denmark. https://dl.acm.org/doi/10.1145/3576915.3623180

Lavrov, E. A., Solkin, A. L., Aygumov, T. G., Chistyakov, M S., & Akhmetov, I. V. (2021). Analysis of information security issues in corporate computer networks.

IOP Conference Series: Materials Science and Engineering, 1047(1), 012117. https://doi.org/10.1088/1757-899x/1047/1/012117

Lee, I. (2025, February 6). *What is RBAC (Role-Based Access Control)?* Wallarm. https://www.wallarm.com/what/what-exactly-is-role-based-access-control-rbac

Ling, F., Yang, H., Xiao, Y. C., & Hu, L. (2024, December 6-8). *Meta GPT-Based Agent for Enhanced Phishing Email Detection.* [Conference session]. International Conference on Communication and Network Security, Shanghai, Xiamen, China. https://dl-acm-org.libraryproxy.griffith.edu.au/doi/10.1145/3711618.3711619

Linnell, C. (2025, January 9). The Data-Driven Future: Data Protection in the Automotive Industry. *Bridewell.* https://www.bridewell.com/insights/blogs/detail/data-protection-in-the-automotive-industry#:~:text=Vehicles%20now%20routinely%20capture%20sensitive,of%20data%20breaches%20and%20misuse.

Lindsey, N. (2019, September 20). Toyota Subsidiary Loses $37 Million Due to BEC Scam. *CPO Magazine.* https://www.cpomagazine.com/cyber-security/toyota-subsidiary-loses-37-million-due-to-bec-scam/

Mancini, A. (2024, April 3). *Ranking the Different Types of Multi-Factor Authentication (MFA).* Impact. https://www.impactmybis.com/blog/ranking-mfa-types/

Messe Munchen GmBH. (2024). *Cybersecurity in the automotive industry: new challenges and solutions.* Electronica. https://electronica.de/en/industry-portal/detail/cybersecurity-in-the-automotive-

industry.html#:~:text=The%20number%20and%20complexity%20of,2.5%2Dfold%20compared%20to%202022.

McCarthy, M. (2025, January 2). *The Definitive Guide to Role-Based Access Control (RBAC).* StrongDM. https://www.strongdm.com/rbac

McNeal, A. (2022, December 16). What is the Goal Behind Phishing Emails? *Graphus.* https://www.graphus.ai/blog/what-is-the-goal-behind-phishing-emails/

Mukherjee, A. (2023, October 4). Is MFA As Secure As It Used To Be? *Threat Intelligence.* https://www.threatintelligence.com/blog/mfa#:~:text=One%20of%20the%20biggest%20problems,becoming%20increasingly%20fraught%20with%20risks.

Nadeem, M., Sahra, S. W., Abbasi, M. N., & Ahmed, W. (2023, September 25). Phishing Attack, Its Detections and Prevention Techniques. *ResearchGate; Springer Nature.* https://www.researchgate.net/publication/374848676_Phishing_Attack_Its_Detections_and_Prevention_Techniques

National Cyber Security Centre. (2018, February 5). *Phishing Attacks: defending your organisation*. Ncsc. https://www.ncsc.gov.uk/guidance/phishing#section_3

Pangarkar, T. (2025, January 14). *Automotive Cyber Security Statistics 2025.* Scoop Market. *https://scoop.market.us/automotive-cyber-security-statistics/*

Pawar, S. (2024, August 22). *How Multifactor Authentication (MFA) Reduces Cyber Attack Risk*. Parablu. https://parablu.com/multifactor-authentication-mfa-reduces-cyber-attack-risk/

Rao, S., Liu, E., Ho, G., Voelker, G. M., & Savage, S. (2024, May 13-17). *Unfiltered: Measuring cloud-based email filtering bypasses.* [Conference session]. Association for

Computing Machinery, Singapore. https://dl-acm-org.libraryproxy.griffith.edu.au/doi/pdf/10.1145/3589334.3645499

SOC Radar. (2024, July 16). *Major Cyber Attacks That Target The Automotive Industry.* SOC Radar. https://socradar.io/major-cyber-attacks-targeting-the-automotive-industry/

Toulas, B. (2024, April 17). *FIN7 targets American automaker's IT staff in phishing attacks*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/fin7-targets-american-automakers-it-staff-in-phishing-attacks/

Trendmicro. (2023, December 12). *Rising Security Weaknesses in the Automotive Industry and What It Can Do on the Road Ahead*. Trendmicro. https://www.trendmicro.com/vinfo/au/security/news/cybercrime-and-digital-threats/rising-security-weaknesses-in-the-automotive-industry-and-what-it-can-do-on-the-road-ahead

Vakulov, A. (2025, January 25). *Cybersecurity Threats To Modern Cars: How Hackers Are Taking Control*. Forbes. https://www.forbes.com/sites/alexvakulov/2025/01/25/cybersecurity-threats-to-modern-cars-how-hackers-are-taking-control/

Vakulov, A. (2025, March 19). *Shifting Gears for 2025: The Next Generation of Automotive Cybersecurity Challenges*. https://www.forbes.com/sites/alexvakulov/2025/01/25/cybersecurity-threats-to-modern-cars-how-hackers-are-taking-control/

Valentijn, F. (2024). *Detection and Detection Evasion with Man-in-the-Middle Phishing* [Unpublished master's thesis]. Radboud University.

Van Enckevort, B. (2024, September 3). Understanding Third Party Risk in Cyber Security. *Metomic*. https://www.metomic.io/resource-centre/third-party-risk-in-cyber-security#:~:text=Third%2Dparty%20risk%20in%20cyber,software%20getting%20into%20the%20systems.

Wagner, G. (2023). *A Conceptual Model and Simulation Model for Phishing*. https://www.utwente.nl/en/eemcs/fois2024/resources/papers/wagner-a-conceptual-model-and-simulation-model-for-phishing.pdf

Yang, O. & Cheng, L. (2024, March 13). *How a Credential Phishing Attack Could Lead to Tesla Car Theft and How to Mitigate It*. VicOne. https://vicone.com/blog/how-a-credential-phishing-attack-could-lead-to-tesla-car-theft-and-how-to-mitigate-it