Computer Security Vulnerabilities and Countermeasures Audit

CSI1101 – Computer Security

Jordan Farrow (10653054)

Edith Cowan University, Joondalup

Imran Malik

22 August, 2024

Table of Contents

1. Introduction

Pines Bay (PB) is a city council relying heavily on digital operations to support the accessibility of its services to residents and for the council's management, utilising and storing large volumes of sensitive data for operations. Prior to this audit, a disgruntled employee took advantage of vulnerabilities within these digital operations, successfully extracting and encrypting PB's data and systems with ransomware, halting PB's services. In addition, the now cybercriminal employed a triple extortion attack, threatening to use this data against PB and its residents unless a sum of money was provided which PB agreed to (Tatar, 2024). As a result of this incident, PB's reputation declined with demands for a security analysis to be conducted to find crucial shortcomings which impact both the systems and sensitive data. Through this analysis, six issues within PB's digital operations and use-cases were determined as a critical security risk which must be addressed.

Security issues within PB have shown to breach the aims of security; standards which must be upheld to ensure the protection of systems and data (Malik, n.d.a; Fortinet, n.d.). A breach occurring in any aim signifies vulnerabilities within the company's security which can hinder their digital operations and must be resolved quickly before cybercriminals can exploit it (Fortinet, n.d.). The aims of security PB have breached include the confidentiality, integrity and availability (CIA) triad and authenticity, each defined within Table 1 (Malik, n.d.a; Fortinet, n.d.).

Table 1

Aims of security definitions

Aim of security	**Definition**
Confidentiality	Only authorised entities can access systems and information.
Integrity	Data has not been manipulated from its original state in an unauthorised manner.
Availability	Authorised entities have the ability to access systems and information.
Authenticity	Entities can correctly verify their identity and ensures they are who they claim to be.

Note. Adapted from *Module 1 Slides Pack* [PowerPoint slides], by Malik, n.d.a, Canvas (https://courses.ecu.edu.au/), *CIA Triad*, n.d., Fortinet (https://www.fortinet.com/resources/cyberglossary/cia-triad)

The purpose of this audit was to explore these issues within PB's current digital operations which leaves them vulnerable to cyberattacks, offer solutions and their implementation requirements, in addition to a backup strategy which allows PB to recover from incidents similarly discussed prior.

This audit will include two major sections. The first consisting of six individually discussed critical issues within PB's current digital operations, which can be exploited and their urgency to be resolved quickly through a comparison with the aims of security. For each issue, two solutions will be discussed and compared, resulting in the choice of one solution and the requirements for its implementation within PB. The next section discusses and compares aspects of data backup strategies which PB can implement to recover from future cyber-attacks in the least time possible, with a final recommendation that benefits the company. Information used for the production of this audit had been gathered from various sources, including academic literature, government publications, articles and blogs from reliable companies which specialise in the cybersecurity domain.

2. Issue 1: Power Surges

Pines Bay noted that the company is regularly impacted by power surges, hindering their digital operation abilities. Power surges are sudden increases in voltage within an electrical network which are sent towards connected electronic devices, caused by either external environmental or internal factors (Tara Energy, n.d.; Anker, 2024).

2.1. Why Is It Critical?

Computers accept specific voltages for both the powering of its components and the communication of information between them through binary (Arulampalam, n.d.). Power surges cause these components to become burdened by fluctuations of voltage which they were not designed to sustain, causing the components to degrade at increased rates (Lenovo, n.d.a; Schneider Electric, n.d.). As a result, the company's servers and computers will decrease in performance or outright fail as core components cease to function, breaching the aim of availability as the systems become unavailable, hindering PB’s digital operations whilst repairs or replacements are performed (Schneider Electric, n.d.; Malik, n.d.a). In addition, power surges can impact the data stored within the servers, breaching the aim of integrity by causing data to become corrupted or lost as its storage medium degrades and cease function, which in small amounts can cost a company up to $35,730 in damages and further reputational damage (Lenovo, n.d.a; Anker, 2024; Schneider Electric, n.d.).

2.2. Recommended Solutions

2.2.1. Solution 1 – Surge Protection Device (SPD)

A Surge Protection Device (SPD) takes voltage above desired thresholds, rerouting it away from the electronic devices, resulting in electronic devices not receiving the increased voltages caused by a power surge (Anker, 2024; Lenovo, n.d.a). Like a device’s components, an SPD’s ability to stop excess voltage will decrease, thus will need replacements over time (Lenovo, n.d.b).

2.2.2. Solution 2 – Reducing Electronic Device Overload

By reducing the number of devices connected to an electrical system at a time, the electrical system does not have to sustain the varying voltage of the devices, reducing the possibility of a large surge of power being sent to the devices requiring less voltage and reducing its impact on those devices (Morris, 2022; Tara Energy, n.d.).

2.3. Preferred Solution

Although solution two is free to implement, it will limit the number of electronic devices PB will be able to concurrently use, whilst relying on employees to follow a new solution which addresses the issue, costing PB time and money to train their employees. In addition, maintaining IT systems will become challenging as its various components will need to be spread across the premises in order to reduce overloading in comparison to solution 1, which allows these systems to remain within the same circuit and therefore secure location. Solution 1 has the ability to stop power surges which occur from a variety of factors, whereas solution two can only prevent power surges occurring from the overload of electronic devices (Morris, 2022; Anker, 2024). Overall, solution one is recommended.

2.4. Implementation Requirements

Table 2

Power surge solution implementation requirements

Hardware	Surge Protection Device
Training	Train IT employees how to safely replace a faulty SPD Train IT employees to detect when an SPD requires replacement

3. Issue 2: Widespread Administrative Privilege Access

Pines Bay had discussed that all employees are provided systems with administrative privileges to perform their daily operations.

3.1. Why Is It Critical?

The Australian Cyber Security Centre (ACSC) deems the restriction of administrative privileges one of its essential eight mitigation strategies to secure IT systems against cyber threats, which when implemented correctly has shown to reduce the success rate of cyber-attacks by 98% (Australian Cyber Security Centre, 2023a; Taylor, 2020).

Mitigating administrative privileges is critical as it allows individuals with system access ability to install and execute software (Microsoft, n.d.a). This can be intentional such as PB's previous disgruntled employee executing ransomware, or unintentional due to lack of cyber security awareness or vulnerabilities as a human (Imperva, n.d.). An example of this is a successful phishing attempt which impersonates a reputable source with the goal of executing malware on the system (Australian Cyber Security Centre, n.d.a). In addition, it allows all data and settings within the system to be accessed and manipulated including critical security settings (Malik, n.d.e; Microsoft, n.d.a; Imperva, n.d.). The aim of confidentiality has been breached as all employees and possibly cybercriminals can access all software and data which they were not authorised by PB to access, for instance, a project manager having access to the hashed password list or PB's database software (Malik, n.d.a).

3.2. Recommended solutions

3.2.1. Solution 1 – Principle of Least Privilege

This solution is a concept where the users of a system are given access to only the software, data and actions which allow them to fulfill their daily operations (Microsoft, n.d.b; Malik, n.d.e; Australian Cyber Security Centre, 2024a).

3.2.2. Solution 2 – Monitor All Privileged Employees

This solution allows all employees to retain their administrative access, which can be used to maintain workflows as all software and data can be accessed, however, requires the actions performed by all employees to be monitored through software (Imperva, n.d.; Ekran System, 2022).

3.3. Preferred Solution

Solution one is recommended due to the ability to mitigate and manage access to administrative privileges, whilst also preventing unauthorised individuals from accessing data and executing software and does not require employee supervision (Australian Cyber Security Centre, 2024a; Imperva, n.d.). Solution two can negatively impact employees trust with PB as their workflows are watched closely, which may cause employees to become disgruntled and retaliate, resulting in harmful use of administrative privileges which solution 1 would mitigate (Australian Cyber Security Centre, 2024a). In addition, solution one meets multiple of ACSC's maturity model implementation requirements to secure administrative privilege access, whilst allowing PB the opportunity to further secure privilege use by meeting the requirements of higher maturity levels (Australian Cyber Security Centre, 2024b).

3.4. Implementation Requirements

Table 3

Administrative access solution implementation requirements

Hardware	Central system to control access restriction software
Software	Access restriction software
Training	Train IT administrators how to apply and disable access restriction to users. Train employees to request access to software & data deemed outside their authorisation.

4. Issue 3: Lacklustre Authentication

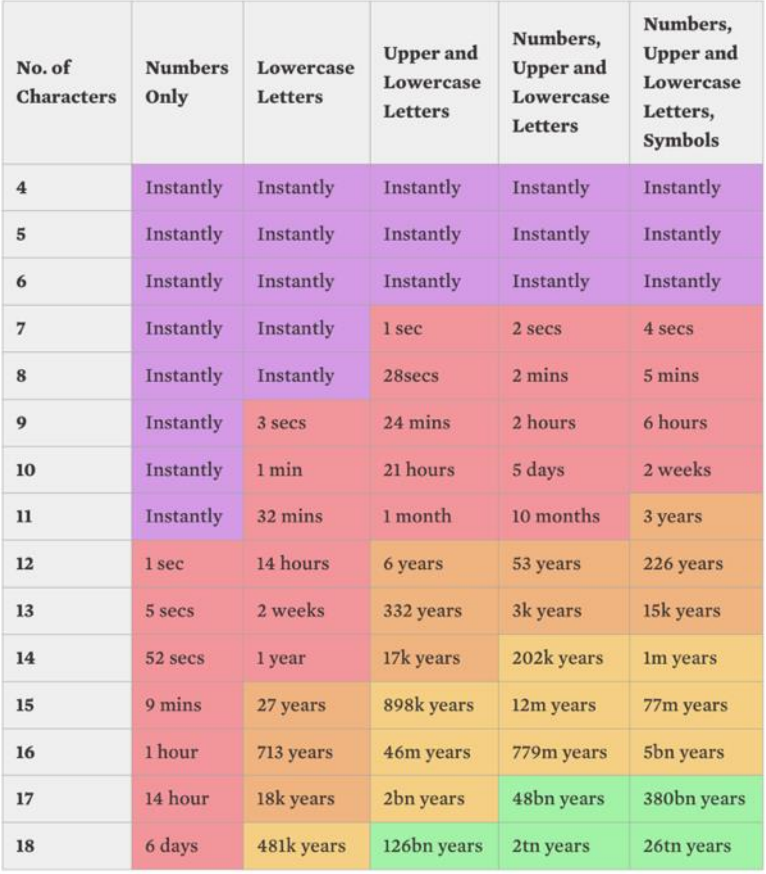
Pines Bay utilises password-based authentication for ensuring account security, requesting passwords consist of a minimum of five characters, including at least one special character, for instance, $, % or &.

4.1. Why Is It Critical?

Although PB allows passwords of greater lengths, there is the possibility that employees will choose the minimum character length, which shown in Figure 1 is breached instantaneously, regardless of its complexity (Whitney, 2023; European Information Technologies Certification Academy, 2023). Poor passwords alone have caused 80% of data breaches within companies, as cybercriminals have the ability to brute-force password-based authentication by guessing over 1,000 passwords each second (Laborde, 2024; Descope, 2023; Weinert, 2023; European Information Technologies Certification Academy, 2023). If a cybercriminal successfully obtains the password to an employee's account, the aim of authenticity is breached since the entity falsely verifies as another individual, providing unauthorised access to PB's systems and data, breaching confidentiality (Malik, n.d.a).

Figure 1

Time taken to brute-force passwords of varying complexities



No. of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hour	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Note. From *BeCyberSmart: How Fast Can a Hacker Break YOUR Password?*, by Centre for Information Technology, 2023, Oberlin College and Conservatory (https://www.oberlin.edu/cit/bulletins/passwords-matter)

Pines Bay must come to a resolution quickly otherwise it may negatively impact the company and its residents similarly to the Ticketmaster incident in May 2024; a data breach resulted in the exposure of 1.3TB of customer data, caused by an employee's exposed password providing cybercriminals successful authentication into their database (Genesis Platform, 2024; Polymer, 2024).

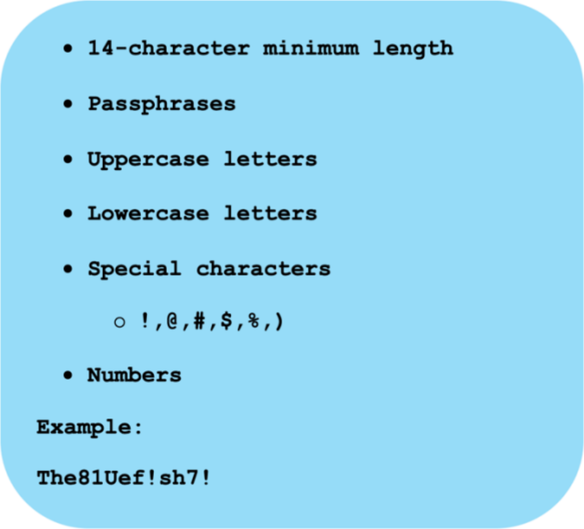
4.2. Recommended Solutions

4.2.1. Solution 1 – Modify Minimum Password Requirements

By using the proposed minimum requirements within Figure 2, this solution ensures that PB accounts cannot be brute-forced in Figure 1, increasing security of password-based authentication.

Figure 2

Minimum recommended password requirements



- 14-character minimum length
- Passphrases
- Uppercase letters
- Lowercase letters
- Special characters
  - !,@,#,$,%,)
- Numbers

Example:

The81Uef!sh7!

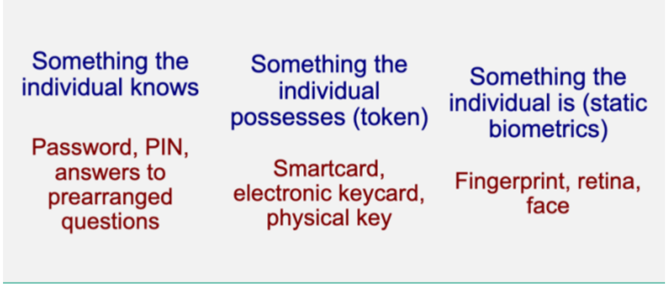
Note. Adapted from *What is Password-Based Authentication?*, 2023, Descope (https://www.descope.com/learn/post/password-authentication), *What are the limitations of using passwords for authentication in computer systems?*, 2023, European Information Technologies Certification Academy (https://eitca.org/cybersecurity/eitc-is-cssf-computer-systems-security-fundamentals/architecture/security-architecture/examination-review-security-architecture/what-are-the-limitations-of-using-passwords-for-authentication-in-computer-systems/)

4.2.2. Solution 2 – Two-Factor Authentication

This solution involves using two multiple authentication methods to verify the authenticity of employee’s (Malik, n.d.c; European Information Technologies Certification Academy, 2023; Australian Cyber Security Centre, n.d.b). This ensures that if an unauthorised entity successfully bypasses password-based authentication, another authentication method is providing a second layer of security which must be bypassed to enter the account (European Information Technologies Certification Academy, 2023; Australian Cyber Security Centre, n.d.b). There are three types of authentications which can be used, including something you know, something you have and something you are, displayed in Figure 3 (Malik, n.d.c; Australian Cyber Security Centre, n.d.b; Microsoft, n.d.c).

Figure 3

Authentication types with examples



Something the individual knows	Something the individual possesses (token)	Something the individual is (static biometrics)
Password, PIN, answers to prearranged questions	Smartcard, electronic keycard, physical key	Fingerprint, retina, face

Note. Adapted from *Module 6 Slides Pack* [PowerPoint slides], by Malik, n.d.c, Canvas (https://courses.ecu.edu.au/)

4.3. Preferred Solution

Although implementing both solutions concurrently would provide greater security, solution one is the weaker option for long term protection as password-based protection authentication remains the only defence for PB's accounts. Despite passwords increasing in length and complexity to where it cannot be exposed within a single lifetime as seen in Figure 1, an employee can unintentionally share passwords, exposing the account to unauthorised entities (Nemko, 2023). Furthermore, the password can still be used for employee's personal accounts, increasing number of locations of possible exposure for data breaches; if one account is exposed in a data breach, all other accounts are now vulnerable, including PB's (European Information Technologies Certification Academy, 2023).

Solution two is the preferred solution as it fixes the shortcomings of solution 1. This solution requires two successful authentications to occur before allowing access to PB's services therefore, no matter how weak a password is, account access will not be successful until authorisation occurs twice (European Information Technologies Certification Academy, 2023; Australian Cyber Security Centre, n.d.b). It is recommended that PB employs an authenticator app as a *something you know* authentication for instance, an authentication app (Malik, n.d.c).

4.4. Implementation Requirements

Table 4

Two-factor authentication solution requirements

Hardware	Mobile device
Software	Authentication app Password-based authentication software
Training	Train employees to successfully authenticate through both factors Train employees to use authentication app Train employees to alert when password-based authentication is breached.

5. Issue 4: Lack of Network Security Device Redundancy

Pines Bay uses all networking and security devices without redundancy, therefore relies on one of each security device to protect their network.

5.1. Why Is It Critical?

Redundancy in networking is crucial as it ensures that if a security device ceases function, another is immediately activated which is utilised in its place, ensuring network security remains present (Malik, n.d.f; Cloudflare, n.d.). Furthermore, redundant devices can be layered, therefore if a security device fails to stop malicious traffic from entering PB's network, it is met by another to prevent entry (Cloudflare, n.d.).

If a device does not stop malicious traffic or ceases function whilst redundancy is absent, PB's network will be vulnerable to 7% of malicious traffic per day, allowing cybercriminals to send malware across all connected systems to the network, for instance, ransomware which encrypts PB's data, breaching integrity and availability as PB would lose access to their systems and data which has been manipulated (Cloudflare, 2024; Malik, n.d.a; Australian Cyber Security Centre, n.d.c). In addition, the network compromission allows cybercriminals to transfer data from PB's network to their own and inject Server Query Language statements through web traffic, allowing data within their database to be observed and acquired, providing unauthorised entities access to PB's data, breaching confidentiality (RiskRecon, 2024; Malik, n.d.a).

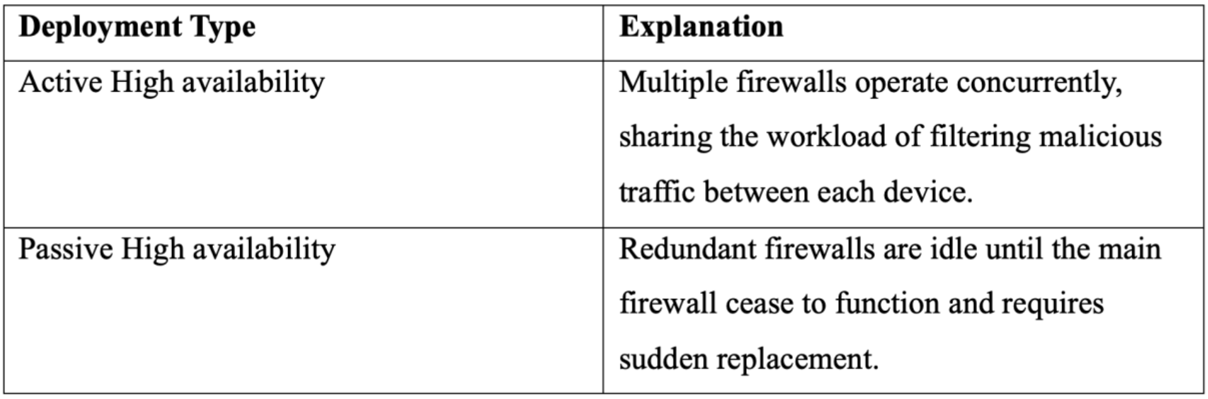
5.2. Recommended Solutions

5*.2.1. Solution 1 – High Availability (HA) Firewalls*

This solution involves the use of multiple firewalls which filter and block malicious traffic inbound to PB through the use of perimeter firewalls, or within PB's network through Network firewalls (Darnell, 2023; NordLayer, n.d.). Pines Bay can deploy HA firewalls in two ways, explored in Table 5.

Table 5

High Availability firewall deployment types



Deployment Type	**Explanation**
Active High availability	Multiple firewalls operate concurrently, sharing the workload of filtering malicious traffic between each device.
Passive High availability	Redundant firewalls are idle until the main firewall cease to function and requires sudden replacement.

Note. Adapted from *What Is a Firewall and Why It Is Often Confused with DDos Protection*, by Darnell, 2023, DDoS-Guard (https://ddos-guard.net/blog/what-is-a-firewall-and-how-it-works), *What is a high availability (HA) firewall?*, n.d., NordLayer (https://nordlayer.com/learn/firewall/high-availability/)

5.2.2. Solution 2 – Redundant Intrusion Prevention Systems (IPS)

This solution involves using IPS at the network perimeter, within the network or both. This will detect and alert PB of malicious traffic in the same way that the currently implemented intrusion detection system does while also attempting to block the malicious traffic from impacting the network and reaching IT systems (IBM, n.d.a; Malik, n.d.f). Similarly to solution one, solution two can be utilised as HA, as seen within one of IBM's products and in the two ways explored in Table 5 (IBM, n.d.b).

5.3. Preferred Solution

Both solutions are optimal in ensuring redundancy in PB's network security devices, as each can be used in a HA setting (NordLayer, n.d.; IBM, n.d.b). If one device ceases function, its idle equivalent will begin to operate (NordLayer, n.d.). In addition, both can be used at the perimeter and inside of a network to block malicious traffic outbound of other networks, and within PB's network (Darnell, 2023; Palo Alto Networks, n.d.). Although both solutions are effective, solution two is more advantageous. This solution has the ability to alert PB's security team of malicious traffic and can update existing firewalls with new policies to stop traffic which had successfully passed the firewall prior and not the IPS (IBM, n.d.a).

5.4. Implementation Requirements

Table 6

Network security redundancy solution implementation requirements

Hardware	Server to contain IPS software
Software	Intrusion Prevention System software
Training	Train IT employees on how to respond to IPS false positive alerts Train IT employees on how to respond to positive IPS alerts Train IT employees how to resolve a faulty IPS Train IT employees how to use IPS in redundancy Train IT employees how to observe network traffic

6. Issue 5: Lack of Physical Security Mechanisms

Pines Bay has no physical security mechanisms to protect IT systems, and any individual can enter the server room containing servers and networking devices.

6.1. Why Is It Critical?

In comparison to digital security mechanisms, physical mechanisms have declined in priority, leading to 60% of companies being impacted by their complacency in physical security (Shaik, 2018; Hutter. 2016). Physical security is crucial as it ensures only authorised individuals can access PB's IT systems, whilst protecting from harm and misuse (Malik, n.d.d).

Without physical security mechanisms, unauthorised individuals can breach authenticity by falsely verifying themselves as employees and enter PB's premises (Malik, n.d.a). This results in a breach of confidentiality as access to end devices which operate at an administrative level, networking devices connecting systems together, and servers which contain vast amounts of customer data and manages PB's web application employees operate in are provided (Malik, n.d.a). Furthermore, unauthorised individuals can also take IT devices or physical storage housing PB's personal data. This highlights breaches in confidentiality and availability as one system is missing reducing accessibility (Malik, n.d.a).

6.2. Recommended Solutions

6.2.1. Solution 1 – Physical Access Control Prevention

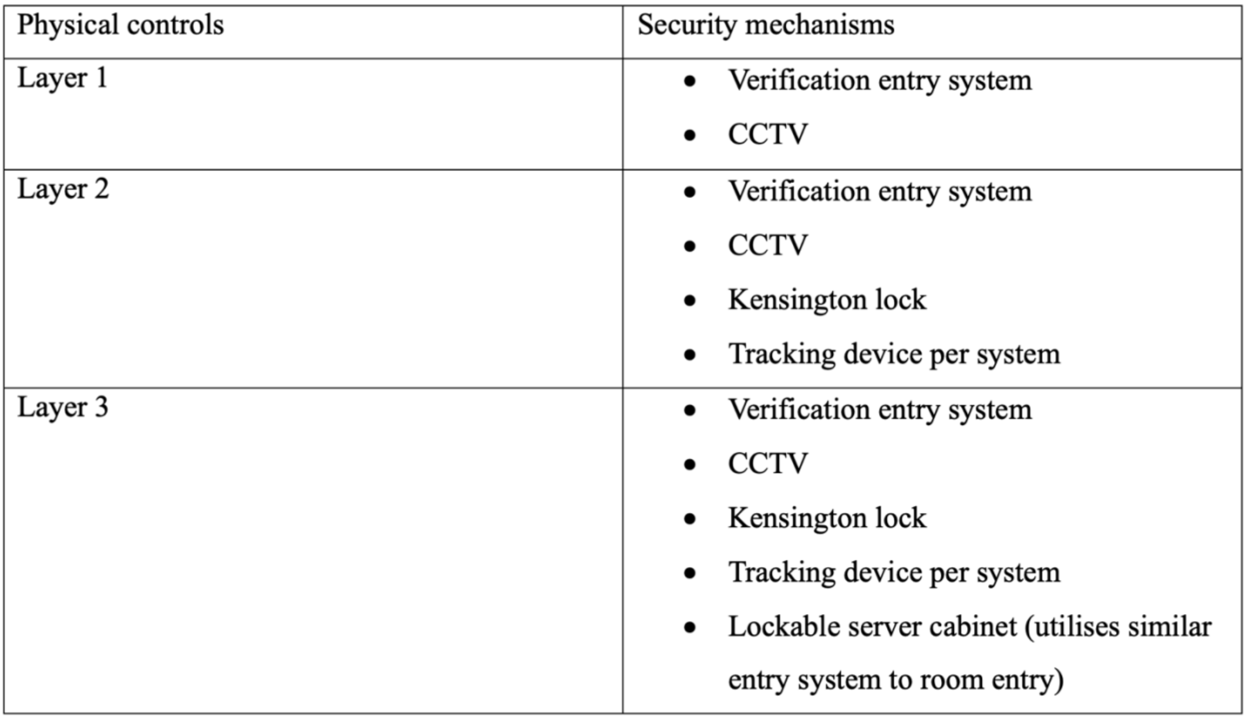
This solution involves preventing physical access individuals have within PB's building in relation to their role, creating physical barriers prevents unauthorised individuals from passing through (Australian Cyber Security Centre, 2024b). This solution would be employed within three layers; the perimeter of the building (layer 1), ensuring only employees of PB can access the premises; the IT locations (layer 2), only accessible to employee's which require the use of the systems, servers and network devices (Australian Cyber Security Centre, 2024b). For added security, it would be best to separate layer two further, creating layer three that contains the servers and network devices of PB, only accessible by those necessary (Australian Cyber Security Centre, 2024b). Access control would be implemented through a *key fob or card door entry system*, allowing those with an electronic card with the correct permissions to enter the location (Avigilon, n.d.).

6.2.2. Solution 2 – Defence-in-Depth

This solution involves defence in depth, utilising multiple physical security mechanisms within each layer to control the physical access to PB's IT systems and infrastructure, including the access control prevention discussed in solution one (Australian Cyber Security Centre, 2024b; Malik, n.d.b). Table 7 provides the various mechanisms which would be implemented at each layer.

Table 7

Physical security mechanisms deployable at each layer



Physical controls	Security mechanisms
Layer 1	• Verification entry system • CCTV
Layer 2	• Verification entry system • CCTV • Kensington lock • Tracking device per system
Layer 3	• Verification entry system • CCTV • Kensington lock • Tracking device per system • Lockable server cabinet (utilises similar entry system to room entry)

6.3. Preferred Solution

Both solutions restrict employee access to all PB systems through verification entry which is only successful to individuals which require access to the systems (Australian Cyber Security Centre, 2024b). Although solution one occurs within all layers, it does not stop authorised employees from exploiting administrative privileged accounts or server and network access, nor does it stop the possibility of systems or storage devices being taken from PB. Solution two is the preferred solution. It mitigates these issues as it uses physical mechanisms which record all individuals within the layer two and three locations, ensuring actions are documented and are unable to be denied (Malik, n.d.a). In addition, the use of Kensington locks keeps all systems immobile with tracking devices enabled in all systems; in the chance the locking mechanism fails, a stolen system's location can be traced (Lenovo, n.d.c). When paired with the resolution of issue two, administrative privilege exploitation can be physically and digitally mitigated.

6.4. Implementation Requirements

Table 8

Physical security mechanism solution implementation requirements

Hardware	Access control door with hard disk and card reader Smart card CCTV with hard disk Kensington lock Tracking device Lockable server cabinet with hard disk and card reader
Software	Software implemented with hardware
Training	Train employees to access premises using smart cards Train employees to scan and enter the premises one at a time Train IT employees to lock server cabinet after each use Train IT employees to use software implemented with hardware

7. Issue 6: Vulnerable Operating Systems

Pines Bay had noted that all computers utilise a version of the operating system (OS) Windows 10 released within 2021, which also uses its default settings.

7.1. Why Is It Critical?

Operating systems receive updates regularly to improve the quality of their product, and to address security concerns which can be exploited by cybercriminals (Sophos, 2020; Australian Cyber Security Centre, 2024a). Using outdated OS leaves PB susceptible to vulnerabilities compared to updated OS which have addressed and documented the previous vulnerabilities (Sophos, 2020; ITConvergence, 2023; Australian Cyber Security Centre, 2024a). The impacts can be damaging, as seen in 2017 where a ransomware named 'WannaCry' exploited outdated windows 10 OS to encrypt 230,000 systems, leading to 4 billion dollars in damages (Kaspersky, n.d.; ITConvergence, 2023). This global incident could have been prevented by utilising up-to-date OS which had addressed the vulnerability months prior (ITConvergence, 2023). In addition to outdated OS, all systems use the default settings Microsoft provides to serve a variety of users, therefore lacks the security required for PB's digital operations which use sensitive data (Corptek Solutions, n.d.). The default environment is well documented, with cybercriminals having high levels of knowledge with the expertise to exploit the vulnerabilities (Corptek Solutions, n.d.). An outdated and unsecure OS can result in the execution of malware, as seen with 'WannaCry', manipulating data through encryption which the unauthorised entity can decrypt and read, whilst rendering the system unusable, breaching the aims of integrity, availability and confidentiality (Kaspersky, n.d.; Sophos, 2020; Malik, n.d.a).

7.2. Recommended Solutions

7.2.1. Solution 1 – Patch Operating System

The ACSC note this security strategy as another of its essential eight strategies for protecting IT systems, involving applying the latest OS patch available no more than 48 hours after release (Australian Cyber Security Centre, 2023a; Australian Cyber Security Centre, 2023b). In PB's case, this update will prevent vulnerabilities which have been resolved since 2021.

7.2.2. Solution 2 – Remove Unrequired Operating System Functionalities

This solution involves only allowing accounts, components, services and functionalities of OS which are required for digital operations to be accessible by employees, creating a principle of least privilege effect within the OS (Australian Cyber Security Centre, 2024a; Ross & Pillitteri, 2023). This provides PB a stronger and more secure control over their OS environments, reducing the number of possible attack avenues a cybercriminal can utilise and must be accounted for.

7.3. Preferred Solution

Both solutions are distinct from one another in how it improves upon PB's current OS security, with solution one patching its vulnerabilities which had existed so they can no longer be exploited and solution two preventing misuse of the OS environment altogether by disabling functionalities and services (Australian Cyber Security Centre, 2024a). Although using both concurrently would provide the most effective OS security, solution one is currently the ideal choice over solution two as vulnerabilities between 2021 and current date may be present within solution two. This means cybercriminals can then use the allowed functionalities to gain access to the system through vulnerabilities which could have been resolved by the latest OS patch. Applying OS patches in less than 48 hours after release, PB will achieve one of ACSC's essential eight requirements at the highest maturity level (Australian Cyber Security Centre, 2024b). Once OS are updated to its current patch, a baseline can then be determined to implement solution two across all PB systems.

7.4. Implementation Requirements

Table 9

Outdated OS solution implementation requirements

Software	Latest OS patch
Training	Train IT employees to implement latest OS patch

8. Data Backup Strategy

Data backup is the act of duplicating important data to a secondary location, external of the data's source which is then used to recover from data loss and manipulation (Cloudian, n.d.; Amazon Web Services, n.d.; Acronis, 2023). Backups of PB's data is crucial as it allows the company to recover from incidents for instance, natural disasters, malware, device malfunctions or the actions of a disgruntled employee which can cause data to be corrupted or lost; data can be collected from the backup and implemented, replacing the impacted data to allow PB's core operations to continue which utilise their data (Cloudian, n.d.; Amazon Web Services, n.d.; Seagate, n.d.).

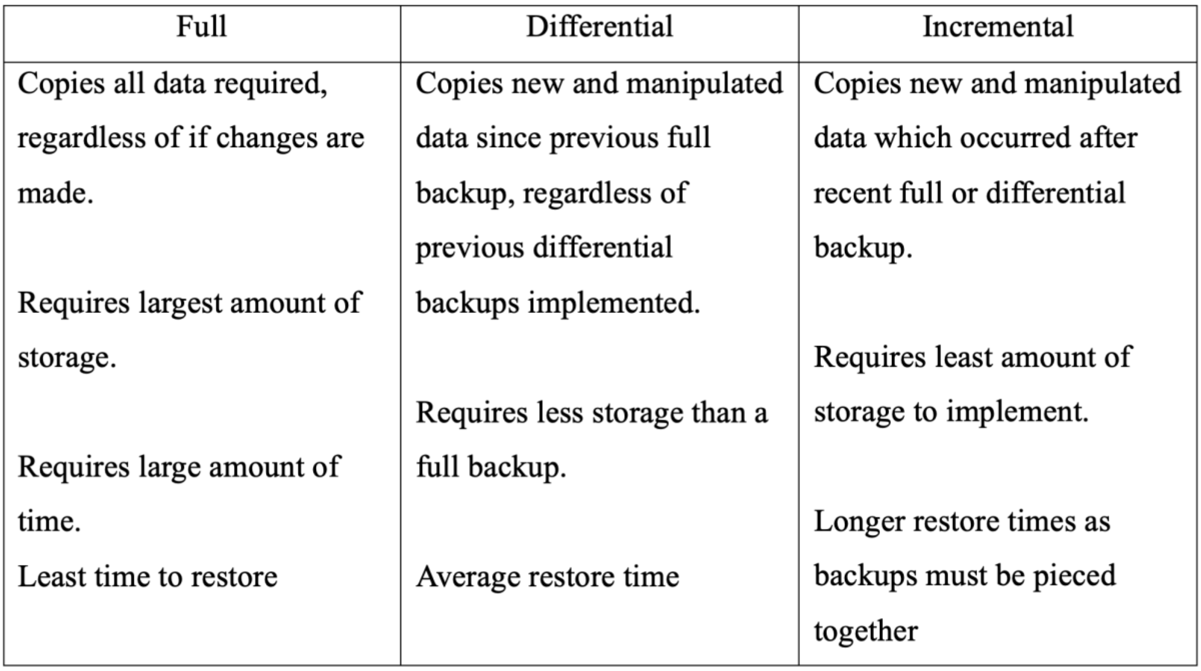
8.1. Data Backup Types

For a backup to be effective after its first, its data must be updated to contain data's latest revisions and data previously inexistent (Australian Cyber Security Centre, 2023c). If regular updates do not occur, PB will be unable to recover data past the backup date, with previous data being outdated (Australian Cyber Security Centre, 2023c).

There are three main backup types which PB can implement, including full, differential and incremental; each type varies in data which is copied, the time it takes to perform the backup and the amount of storage each revision requires, which are shown in Table 10.

Table 10

Backup types and their differences



Full	Differential	Incremental
Copies all data required, regardless of if changes are made. Requires largest amount of storage. Requires large amount of time. Least time to restore	Copies new and manipulated data since previous full backup, regardless of previous differential backups implemented. Requires less storage than a full backup. Average restore time	Copies new and manipulated data which occurred after recent full or differential backup. Requires least amount of storage to implement. Longer restore times as backups must be pieced together

Note. Adapted from *What is Backup? (Data Backup) Comprehensive Guide*, by Kerr, 2023, Acronis (https://www.acronis.com/en-sg/blog/posts/data-backup/), *Types of Backup: Understanding Full, Differential, and Incremental Backup*, by Wallen, n.d., Spanning (https://spanning.com/blog/types-of-backup-understanding-full-differential-incremental-backup/)

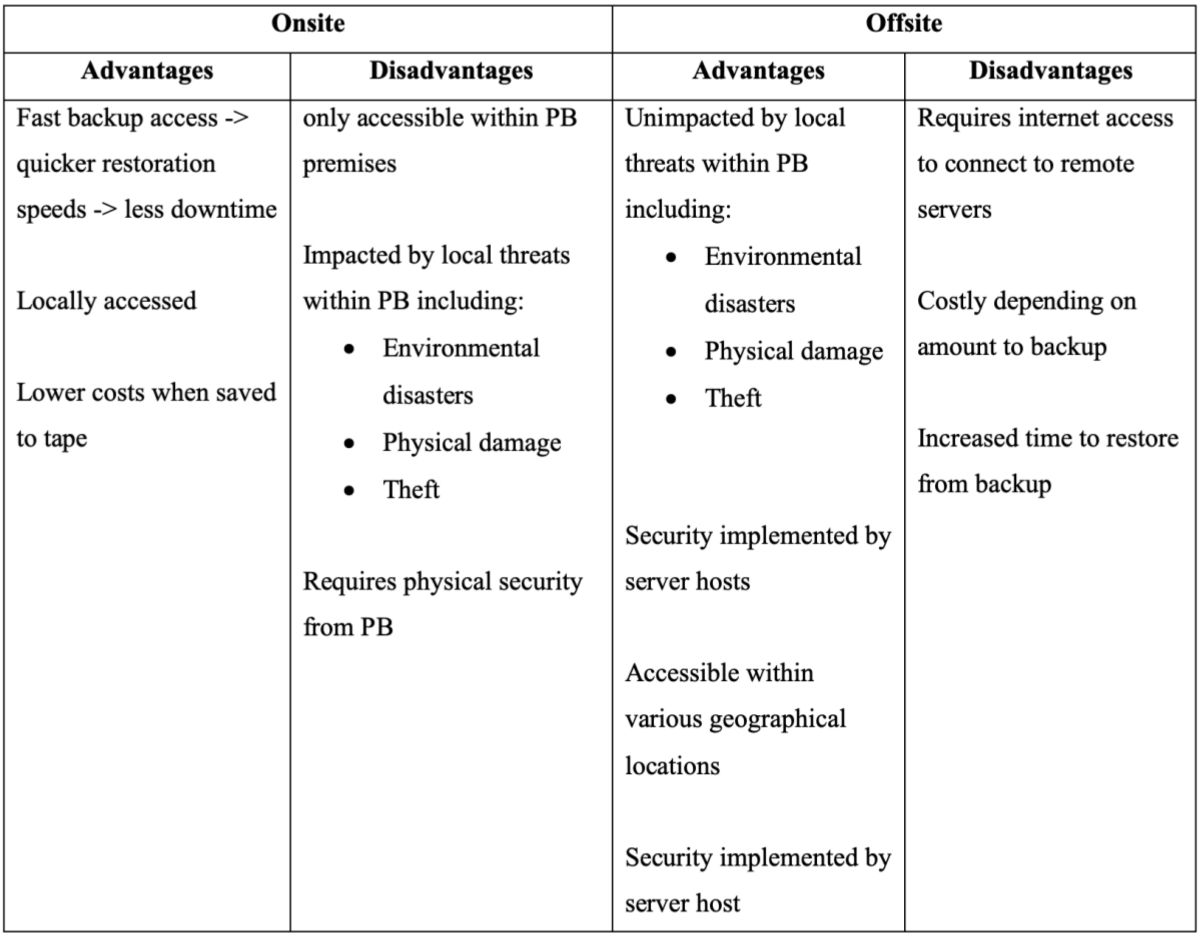
After the first full backup, it is recommended that PB implements a daily incremental backup to ensure new and manipulated sensitive data is consistently accounted for in the shortest times possible, ensuring data accounted for, with weekly full backups that can be used to restore PB's large data quantities when required quickly.

8.2. Onsite Vs Offsite

Pines Bay can store their backups onsite, where the backup and its source are stored within the same geographical location, for instance inside PB's premises (Seagate, n.d.; Malik, n.d.d). In addition, backups could be stored offsite, situated in a separate geographical location unique to the source for instance, cloud storage (Seagate, n.d.; Malik, n.d.d). Both location types have advantages and disadvantages explored within Table 11, which will impact its implementation within PB.

Table 11

Advantages and disadvantages of onsite and offsite backups



Onsite		Offsite	
Advantages	**Disadvantages**	**Advantages**	**Disadvantages**
Fast backup access -> quicker restoration speeds -> less downtime Locally accessed Lower costs when saved to tape	only accessible within PB premises Impacted by local threats within PB including: • Environmental disasters • Physical damage • Theft Requires physical security from PB	Unimpacted by local threats within PB including: • Environmental disasters • Physical damage • Theft Security implemented by server hosts Accessible within various geographical locations Security implemented by server host	Requires internet access to connect to remote servers Costly depending on amount to backup Increased time to restore from backup

Note. Adapted from *Onsite vs. Offsite Backup & Recovery: Which is Best for Your Business?*, by Nheu, 2023, BackupAssist (https://www.backupassist.com/blog/onsite-vs-offsite-backup-recovery-which-is-best-for-your-business), *Onsite vs Offsite Backup Reviews, Strategies, and Best Practice*, by Helen, 2023, MiniTool (https://www.minitool.com/news/offsite-onsite-backup.html), *Difference Between Onsite and Offsite Data Backup*, n.d., BackupAssist (https://www.backupassist.com/education/articles/difference-between-onsite-and-offsite-data-backup.html)

It is recommended that PB utilises both onsite and offsite for their backups, prioritising restoration from onsite which can be accessed and implemented faster than offsite, reducing the downtimes PB may face (Nheu, 2023). If onsite backups are inaccessible due to factors explored in Table 11, then the offsite backups can be used to restore the data within any location requiring more time.

8.3. Backup Protection

The physical and digital security of backups are usually neglected, resulting in backups being more susceptible to cyber and physical threats rather than its source, allowing entities to gain access to a company's relevant data (Malik, n.d.d). To combat this, PB can implement the following security mechanisms to safeguard backups.

8.3.1. Encryption

Encryption takes in data, known as plaintext, and manipulates it into incoherent text, known as ciphertext, which can only be decrypted using a key individual to PB (Groot, 2024). As a result, cybercriminals which gain unauthorised access to the backups will not gain benefits as it requires unique decryption (Groot, 2024). The key used to decrypt PB's data should be stored separately to the location of the encrypted data to ensure it is not easily found and should be unknown to individuals which do not require it for their workflow (OWASP, n.d.).

8.3.2. Access Control

As explored in issue two and five, access control would ensure only authorised individuals have access to onsite and offsite backups to reduce misuse (Microsoft, n.d.b; Australian Cyber Security Centre, 2024b). Onsite backups would be positioned within layer three since it contains data identical to the server which are crucial to PB's digital operations and must be protected at the highest layer (Australian Cyber Security Centre, 2024b).

8.4. Recommended Backup Strategy

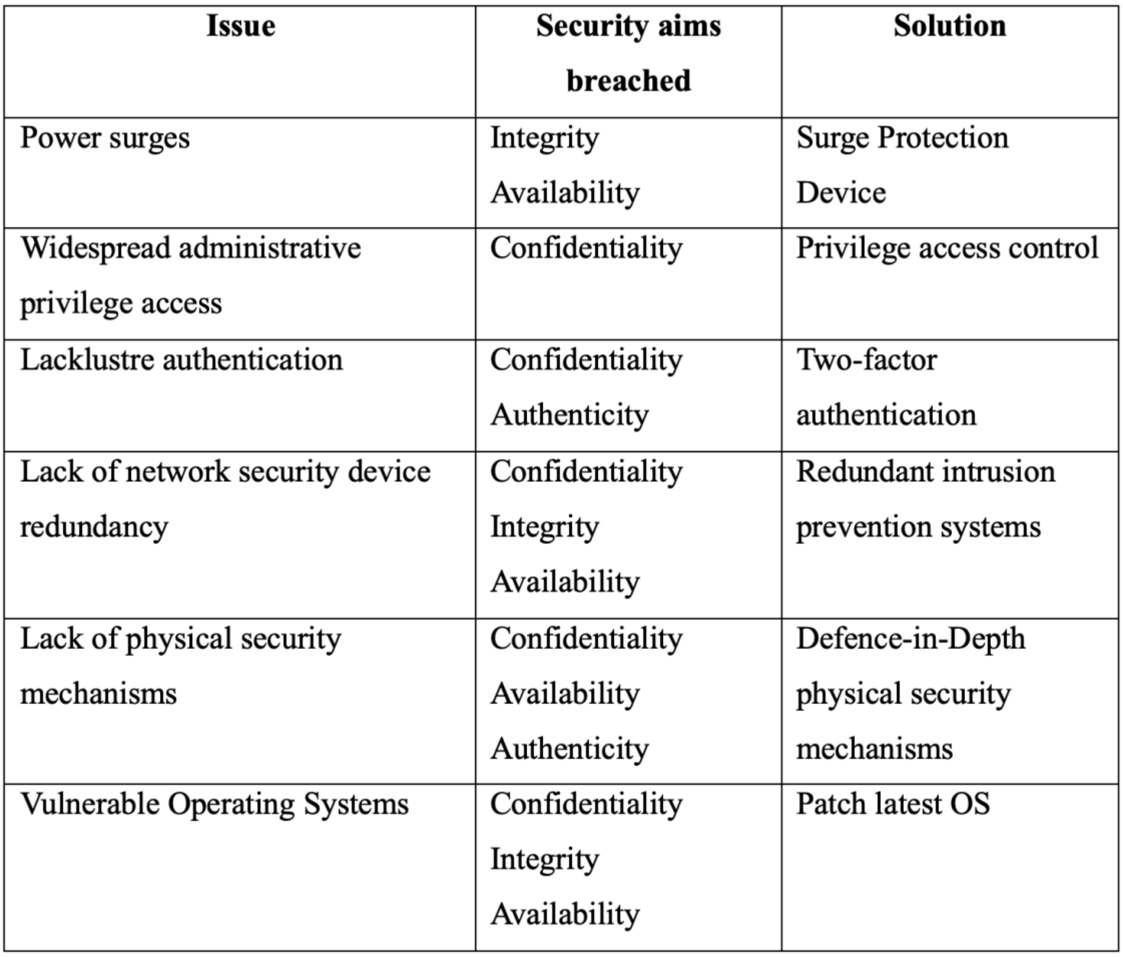
The data backup strategy recommended for PB uses both onsite and offsite backups, creating three data copies that will be backed up incrementally each day, with a full back up each week. The onsite backup will be stored within PB's premises inside layer three for highest physical security. The offsite backup will be stored within a cloud server that can be connected to through the internet.

9. Conclusion

Summarised within Table 12, this audit explored six issues within PB’s current digital operations determined as critical security risks which breach the aims of security. In addition, solutions seen within Table 12 were determined, with the requirements to implement these solutions discussed in each issue.

Table 12

Issues within PB’s digital operations, the security aims each breached and their solutions



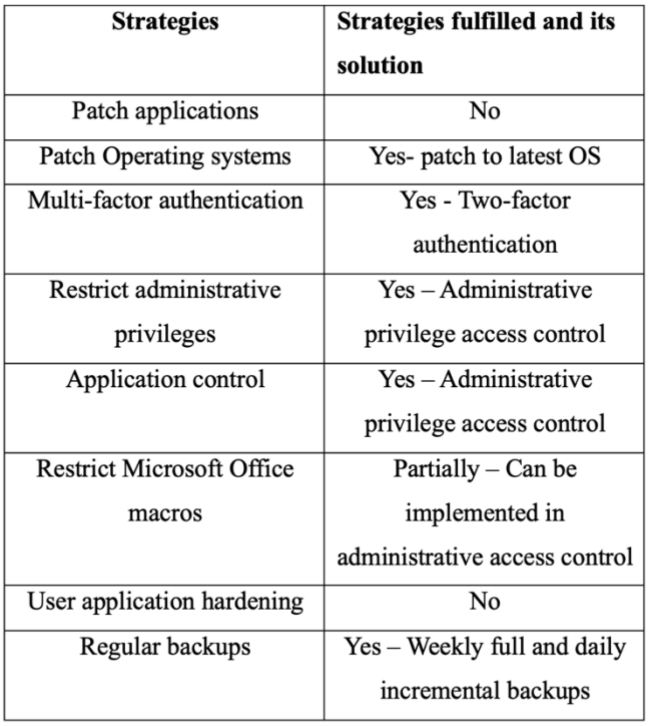
Issue	Security aims breached	Solution
Power surges	Integrity Availability	Surge Protection Device
Widespread administrative privilege access	Confidentiality	Privilege access control
Lacklustre authentication	Confidentiality Authenticity	Two-factor authentication
Lack of network security device redundancy	Confidentiality Integrity Availability	Redundant intrusion prevention systems
Lack of physical security mechanisms	Confidentiality Availability Authenticity	Defence-in-Depth physical security mechanisms
Vulnerable Operating Systems	Confidentiality Integrity Availability	Patch latest OS

In addition, a data backup strategy benefiting PB was discussed. It involved onsite and offsite backups which will occur daily through incremental backups with a full backup occurring weekly. The onsite backup would be stored within PB’s premises inside layer three for highest physical security, whilst the offsite within a cloud server.

By incorporating the backup strategy and solutions within PB’s digital operations, almost six of the ACSC’s essential eight mitigation strategies can be achieved, as seen within Table 13.

Table 13

Essential eight mitigation strategies achieved after implementation solutions



Strategies	Strategies fulfilled and its solution
Patch applications	No
Patch Operating systems	Yes- patch to latest OS
Multi-factor authentication	Yes - Two-factor authentication
Restrict administrative privileges	Yes – Administrative privilege access control
Application control	Yes – Administrative privilege access control
Restrict Microsoft Office macros	Partially – Can be implemented in administrative access control
User application hardening	No
Regular backups	Yes – Weekly full and daily incremental backups

10. References

Amazon Web Services. (n.d.). *What is Data Backup?*. https://aws.amazon.com/what-is/data-backup/

Anker. (2024, April 11). *What is a Power Surge: Cause, Effects and Protection*. https://www.anker.com/blogs/chargers/what-is-a-power-surge

Arulampalam, G. (n.d.). *ENS1161 Module 1 content slides*. Canvas. https://courses.ecu.edu.au/

Australian Cyber Security Centre. (2023a, November 27). *Essential Eight Explained*. Australians Signal Directorate. Retrieved September 19, 2024, from https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained

Australian Cyber Security Centre. (2023b, November 27). *Essential Eight Maturity Model*. Australians Signal Directorate. Retrieved September 19, 2024, from https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

Australian Cyber Security Centre. (2023c, April 11). *How to back up your files and devices*. Australian Signals Directorate. Retrieved October 25, 2024, from https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-back-up-your-files-and-devices

Australian Cyber Security Centre. (2024a, September 26). *Guidelines for System Hardening*. Australian Signals Directorate. Retrieved October 1, 2024, from https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening

Australian Cyber Security Centre. (2024b, September 26). *Guidelines for Physical Security*. Australians Signals Directorate. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-physical-security

Australian Cyber Security Centre. (n.d.a). *Phishing*. Australian Signals Directorate. https://www.cyber.gov.au/threats/types-threats/phishing

Australian Cyber Security Centre. (n.d.b). *Multi-factor authentication*. Australian Signals Directorate. https://www.cyber.gov.au/protect-yourself/securing-your-accounts/multi-factor-authentication

Australian Cyber Security Centre. (n.d.c). *Ransomware*. Australian Signals Directorate. https://www.cyber.gov.au/threats/types-threats/ransomware

Avigilon. (n.d.). *Why physical access control systems are important for any security strategy*. https://www.avigilon.com/blog/physical-access-control

BackupAssist. (n.d.). *Difference Between Onsite and Offsite Data Backup*. https://www.backupassist.com/education/articles/difference-between-onsite-and-offsite-data-backup.html

Centre for Information Technology. (2023, October 6). *BeCyberSmart: How Fast Can a Hacker Break YOUR Password?*. Oberlin College and Conservatory. https://www.oberlin.edu/cit/bulletins/passwords-matter

Cloudflare. (2024, July 11). *Application Security report: 2024 update*. https://blog.cloudflare.com/application-security-report-2024-update/

Cloudflare. (n.d.). *What is defence in depth? | Layer security*. https://www.cloudflare.com/en-gb/learning/security/glossary/what-is-defense-in-depth/

Cloudian. (n.d.). *What Is Data Backup? The Complete Guide*. https://cloudian.com/guides/data-backup/data-backup-in-depth/

Corptek Solutions. (n.d.). *Why are Default Cybersecurity Settings Dangerous?*. https://www.corptek.net/why-are-default-cybersecurity-settings-dangerous/

Darnell, H. (2023, November 7). *What Is a Firewall and Why It Is Often Confused with DDos Protection*. DDoS-Guard.

https://ddos-guard.net/blog/what-is-a-firewall-and-how-it-works

Descope. (2023, April 17). *What is Password-Based Authentication?*. https://www.descope.com/learn/post/password-authentication

Ekran System. (2022, November 21). *Privileged User Monitoring best practice for mitigating cybersecurity risks*. LinkedIn. https://www.linkedin.com/pulse/privileged-user-monitoring-best-practices-mitigating-cybersecurity-

European Information Technologies Certification Academy. (2023, August 4). *What are the limitations of using passwords for authentication in computer systems?*. https://eitca.org/cybersecurity/eitc-is-cssf-computer-systems-security-fundamentals/architecture/security-architecture/examination-review-security-architecture/what-are-the-limitations-of-using-passwords-for-authentication-in-computer-systems/

Fortinet. (n.d.). *CIA Triad*. https://www.fortinet.com/resources/cyberglossary/cia-triad

Genesis Platform. (2024, July 2). *Ticketmaster Data Breach-Full Timeline and New Updates*. LinkedIn. https://www.linkedin.com/pulse/ticketmaster-data-breach-full-timeline-new-updates-l6hxc

Groot, J. D. (2024, September 26). *What Is Data Encryption? (Definition, Best Practices & More)*. Fortra. https://www.digitalguardian.com/blog/what-data-encryption

Helen. (2023, November 20). *Onsite vs Offsite Backup Reviews, Strategies, and Best Practice*. MiniTool. Retrieved October 1, 2024, from https://www.minitool.com/news/offsite-onsite-backup.html

Hutter, D. (2016). *Physical Security and Why It Is Important* [White paper]. SANS Institute. https://www.sans.org/white-papers/37120/

IBM. (n.d.a). *What is an intrusion prevention system (IPS)?*. https://www.ibm.com/topics/intrusion-prevention-system

IBM. (n.d.b). *Introducing IBM Security Network Intrusion Prevention System (IPS) Products*. https://www.ibm.com/docs/en/snips/4.6.0?topic=introducing-security-network-intrusion-prevention-system-ips-products

Imperva. (n.d.). *Privileged User Monitoring*. https://www.imperva.com/learn/data-security/privileged-user-monitoring/

ITConvergence. (2023, April 6). *Risks of Using Outdated Operating System*. https://www.itconvergence.com/blog/risks-of-using-outdated-operating-system/

Kaspersky. (n.d.). *What is WannaCry ransomware?*. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

Kerr, A. (2023, July 17). *What is Backup? (Data Backup) Comprehensive Guide*. Acronis. https://www.acronis.com/en-sg/blog/posts/data-backup/

Laborde, S. (2024, June 4). *Password Reuse Statistics: Over 60% Have a Password Problem*. Techreport. Retrieved September 20, 2024, from https://techreport.com/statistics/cybersecurity/password-reuse-statistics/

Lenovo. (n.d.a). *What is surge?*. https://www.lenovo.com/us/en/glossary/what-is-surge/

Lenovo. (n.d.b). *What are surge protectors?*. https://www.lenovo.com/au/en/glossary/surge-protectors/

Lenovo. (n.d.c). *What is Kensington lock?*. https://www.lenovo.com/au/en/glossary/kensington-lock/

Malik, I. (n.d.a). *CSI1101 – Module 1 Slides Pack* [PowerPoint slides]. Canvas. https://courses.ecu.edu.au/

Malik, I. (n.d.b). *CSI1101 – Module 2 Slides Pack* [PowerPoint slides]. Canvas. https://courses.ecu.edu.au/

Malik, I. (n.d.c). *CSI1101* – Module 6 Slides Pack [PowerPoint slides]. Canvas. https://courses.ecu.edu.au/

Malik, I. (n.d.d). *CSI1101 – Module 7 Slides Pack* [PowerPoint slides]. Canvas. https://courses.ecu.edu.au/

Malik, I. (n.d.e). *CSI1101 – Module 9 Slides Pack* [PowerPoint slides]. Canvas. https://courses.ecu.edu.au/

Malik, I. (n.d.f). *CSI1101 – Module 10 Slides Pack* [PowerPoint slides]. Canvas. https://courses.ecu.edu.au/

Microsoft. (n.d.a). *How do I log on as an administrator?*. https://support.microsoft.com/en-au/windows/how-do-i-log-on-as-an-administrator-63267a09-9926-991a-1c77-d203160c8563

Microsoft. (n.d.b). *Implementing Least-Privilege Administrative Models*. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models

Microsoft. (n.d.c). *What is: Multifactor Authentication*. https://support.microsoft.com/en-au/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661

Morris, J. (2022, December 12). *WHAT IS A POWER SURGE & COMMON CAUSES*. Precision and Electrical Plumbing. https://electricalandplumbing.com.au/blog/what-is-a-power-surge

Nemko. (2023, August 25). *Common Ways Employees Accidentally Leak Company Data*. https://www.nemko.com/blog/unintentional-data-exposure-8-common-ways-employees-accidentally-leak-company-information

Nheu, W. (2023, September 7). *Onsite vs. Offsite Backup & Recovery: Which is Best for Your Business?*. BackupAssist. https://www.backupassist.com/blog/onsite-vs-offsite-backup-recovery-which-is-best-for-your-business

NordLayer. (n.d.). *What is a high availability (HA) firewall?*. https://nordlayer.com/learn/firewall/high-availability/

OWASP. (n.d.). *Cryptographic Storage Cheat Sheet.* https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html

Palo Alto Networks. (n.d.). *What is an Intrusion Prevention System?*. https://www.paloaltonetworks.com.au/cyberpedia/what-is-an-intrusion-prevention-system-ips

Parmar, B. (2012). Protecting against spear-phishing, *Computer Fraud & Security*, 2012(1), 8–11. https://doi.org/10.1016/s1361-3723(12)70007-6.

Polymer. (2024, June 3). *Ticketmaster data breach: Everything you need to know*. https://www.polymerhq.io/blog/ticketmaster-data-breach-everything-you-need-to-know/

RiskRecon. (2024, January 18). *Malicious Traffic Detection: A Guide For Businesses*. https://blog.riskrecon.com/malicious-traffic-detection-a-guide-for-businesses

Ross, R., & Pillitteri, V. (2024). *Protecting controlled unclassified information in nonfederal systems and organizations* (NIST SP 800-171r3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-171r3

Schneider Electric. (n.d.). *WHAT ARE VOLTAGE FLUCTUATIONS, AND WHY DO THEY MATTER?*. https://eshop.se.com/in/blog/post/what-are-voltage-fluctuations-and-why-do-they-matter.html

Seagate. (n.d.). *7 Reasons to Back Up Your Media Offsite and Onsite*. https://www.seagate.com/au/en/blog/7-reasons-to-backup-your-media-offsite-and-onsite/

Shaikh, H. (2018, May 9). *The importance of physical security in the workplace*. Infosec. https://www.infosecinstitute.com/resources/general-security/importance-physical-security-workplace/

Sophos. (2020, October 28). *Updating Your Operating System – the Risks of Staying Out of Date*. https://home.sophos.com/en-us/security-news/2020/updating-your-operating-system

Tara Energy. (n.d.). *Power Surge: How They Happen and What to Do About Them*. https://taraenergy.com/blog/power-surge-how-they-happen/

Tatar, S. (2024, March 19). *The Dangers of Double and Triple Extortion in Ransomware*. Arctic Wolf. https://arcticwolf.com/resources/blog/dangers-of-double-and-triple-extortion/

Taylor, C. (2020, January 6). *Administrator Rights*. CyberHoot. https://cyberhoot.com/cybrary/administrator-rights/

Wallen, D. (n.d.). *Types of Backup: Understanding Full, Differential, and Incremental Backup*. Spanning. https://spanning.com/blog/types-of-backup-understanding-full-differential-incremental-backup/

Weinert, A. (2023, January 26). *2023 identity security trends and solutions from Microsoft*. Microsoft. https://www.microsoft.com/en-us/security/blog/2023/01/26/2023-identity-security-trends-and-solutions-from-microsoft/

Whitney, L. (2023, August 7). *How an 8-Character Password Could be Cracked in Just a Few Minutes*. TechRepublic.

https://www.techrepublic.com/article/how-an-8-character-password-could-be-cracked-in-less-than-an-hour/