Cybersecurity Vulnerabilities and Countermeasures Strengthening Digital Resilience at Pines Bay City Council

Name – Gunarathne Janith Deshan

ID – 10676638

Lecture – Mrs.Thanuja Irugalbandara

Computer Security CSI1101

ECU Sri Lanka Campus

Contents

1. Introduction

In the modern world, protecting organizational information systems is paramount as businesses and public entities utilize networked systems to deal with and store massive amounts of data. However, organizations such as Pines Bay (PB) integrate more digital services to enhance their delivery services, exposing themselves to diverse cybersecurity threats (*Essential Eight Maturity Model | cyber.gov.au*, n.d.). The latest triple extortion cyberattacks on PB exposed numerous security vulnerabilities that are technical and non-technical in nature (*Information Security Manual (ISM) | cyber.gov.au*, n.d.). This attack not only affected the council's operations but was also capable of compromising critical data leading to the outage of the community and subsequent thorough cleaning out of the cybersecurity domain. According to that, to prevent future hacking, PB must determine where it is most vulnerable and how to cover those vulnerabilities. This report aims to evaluate PB's current cybersecurity position regarding the identified issues and offer feasible solutions. This will analyze the scenario's vulnerabilities in extensive detail and emphasize how important it is to resolve them following the Confidentiality, Integrity and Availability (CIA) triad (CSRC Content Editor, n.d.). In addition, this case study will offer a comprehensive data backup strategy to facilitate company survival and quick recovery in scenarios of system failures or threats. However, the primary vulnerabilities of this scenario are poor password policies, outdated and insecure technologies, unsafe physical security and poor data protection protocols. According to PB company, safety issues like unrestricted administrative access, out-of-date SSL (Secure Sockets Layer) protocols and improper data encryption make cybercriminals to take advantage of substantial vulnerabilities (Feldman, 2022). The purpose of this case study is to provide a variety of ways to reduce these risks with a focus on numerous solutions to long-term improvements of PB's cybersecurity architecture. At least but not least to enhance the impact of these recommendations, this case study will utilize key strategies from reliable security frameworks such as (*NIST*, 2024) the Australian Government Information Security Manual (ISM), the National Institute of Standards and Technology (NIST), and the Australian Signals Directorate (ASD) mitigation strategies (*Cyber Security Training | SANS Courses, Certifications & Research*, n.d.). The last of this report will cover the key vulnerabilities that were been identified and emphasize the need of a proactive cybersecurity strategy in protecting confidential company data while strengthening PB's defenses against potential cyber threats.

2. Critical Cybersecurity Issues and Solutions

Pines Bay (PB) has several vulnerabilities that threaten its cybersecurity stance, especially after its recent triple extortion attack. This requires an immediate way to address these vulnerabilities to make certain that PB's systems remain secure and integrity. So below are six critical vulnerabilities identified in PB's current setup with solutions and implementation plan.

2.1 Issue 1: Inadequate Administrative Privileges

In the PinesBay Scenario, the breach occurred due to all employees having administrative privileges on their computers. This allows users unrestricted access to system settings and makes it easy for malicious intentions to leverage this permission and compromise the system (Cyber, 2024). Also, this issue is very significant when a termination of some employee's account isn't revoked, their admin-level access enables to facilitate the breach.

2.1.1 Impacts on CIA triad

Confidentiality: Sensitive data can be accessed by employees.

Sensitive data exposure happens when private or confidential information is not sufficiently safeguarded, making it open to unauthorized access (*What Is Sensitive Data Exposure and How Can You Prevent It?*, 2024). Confidentiality at PB is directly threatened when an employee has administrative privileges and it is allowing them to view, access, or maybe exploit that confidential data.

Integrity: Data could be changed or corrupted by administrative

Admin users can intentionally or accidentally modify, delete or corrupt critical files and system configurations. According to that, this compromises the accuracy and trustworthiness of PB's data.

Availability: The system can be disrupted by admins

Misusing administrative privileges by employees carries the danger of system outages such as misconfigurations or intentional denial-of-service(Dos) attacks, that could compromise the sensitive data and cause system crashes or downtime. (Bakharev, 2024)

2.1.2 Solution 1: Privileged Access Management (PAM)

Privileged Access Management is a critical tool for protecting administrative privileges and mitigating risks associated with elevated access. PAM solutions prevent any organization from obeying the rule of Least Privileged by just-in-time access, which provides temporary permissions to users for a specified time and revokes them automatically after time is ended (Delinea Inc., n.d.). It reduces the risk that hackers will find their way to enter sensitive systems and data to reduce the risk of internal and external breaches. PAM tools like CyberArk and BeyondTrust(Martinez, 2024) are commonly used to protect privileged accounts and help to PB's system prevent cyberattacks that exploit these vulnerabilities. Utilizing this method in PinesBay mitigates the risk associated with administrative privileges and ensures strong control over who accesses the critical systems.

2.1.3 Solution 2: Implement Role-Based Access Control (RBAC) with POLP

Role-Based Access Control limits the distribution of administrative privileges by assigning users roles based on their job functions and ensures they only have access to the resources required for their work. POLP (Principle of Least Privilege) enhances this by making certain that users are only given the minimal amount of access necessary to carry out their responsibilities to ensure that even within each job role. For example, employees who do not need administrative rights to complete their duties will not be granted such privileges. By limiting administrative access to those who genuinely need it, POLP reduces the possibility of unauthorized access to system changes or data breaches. Although, RBAC simplifies the process of managing user access the system in PB can easily add or remove users from specific roles without the need to adjust individual permissions (*What Is Role-Based Access Control (RBAC)? Examples, Benefits, and More | UpGuard*, n.d.). Incorporating RBAC with POLP ensures that PB's employees have the fewest privileges necessary which mitigates the attack surface for malware and insider threats.

2.1.4 Preferred Solution with Comparison

RBAC with POLP assigns users roles with predefined minimum privileges based on their job role and the Australian Signals Directorate supports RBAC to implement least privilege access to guarantee only necessary permissions are granted. However, PAM provides real-time monitoring and just-in-time access to comprehensively log privileged operations. This level of control mitigates risks associated with continuously high privileges, especially in sensitive environments.
While RBAC limits access based on roles, PAM offers dynamic control to ensure administrative permissions are only granted temporarily and audited successfully. PAM is also recommended by NIST for safeguarding critical infrastructure (NIST SP 800-53). According to these PAM's capabilities offer stronger safeguards against insider threat and misuse and it is more effective for protecting critical systems than RBAC's role-based permissions.

2.1.5 Implementation Plan

- Hardware – Null (PAM solutions are normally in cloud-based or existing server infrastructure)
- Software – Implementing tools like CyberArk, BeyondTrust or Thycotics for privilege management which include features such as session monitoring, audit logs and just-in-time access.
- Training – Conduct employee training workshops on how to use privileged access securely and train IT staff on PAM monitoring (access log), configuration and handling privilege sessions.

2.2 Issue 2: Weak Password Management

According to PB's policies, passwords need to be updated every 8 months with a requirement of a minimum 5-character length and one special element. The weakness of this policy enables cybercriminals to breach safeguards by attempting weak passwords using brute force approaches. This issue has a significant impact on PB's scenario because attackers can crack this type of passwords easily and increase the risk of unauthorized access and data breaches in the system.

2.2.1 Impacts on CIA triad

Confidentiality: Weak passwords are allowed to easily crack and expose data

Malicious actors can easily gain access to organizational or personal data when they use weak passwords to log on to their systems. In PineBay, they used weak password policies, and it significantly increased the risk of unauthorized access to their confidential and sensitive data.

Integrity: Hacked accounts could be able to manipulate the system data

PB's Weak password policies placed data integrity at risk because when they enter to the system easily gain access to admin accounts and possibly modify false information or corrupt important data.

Availability: System downtime due to unauthorized access

These weaker password policies increase the possibility of system outages brought on by hackers to get access and disrupt services or lockdowns of the system. This could harm operational interruptions at systems on PB.

2.2.2 Solution 1: Make Strong Password Policies

Enforcing stronger password policies has improved PB's cybersecurity. The existing password policy of changing the passwords is every eight months and a length longer than five characters is insufficient. To mitigate these security risks, PB must require all passwords to be (*Create and Use Strong Passwords - Microsoft Support*, n.d.)

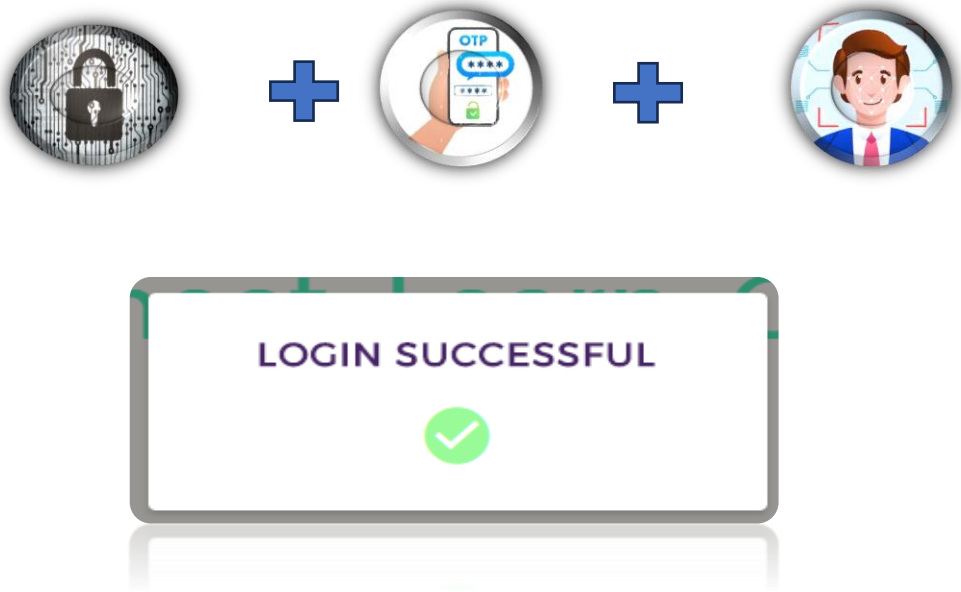
- at least 12 characters long
- combination of upper- and lower-case letters,
- add numbers
- symbols (special characters)

Additionally, according to NIST SP 800-63B guidelines (*NIST Special Publication 800-63B*, n.d.) password expiration should be reset every 90 days and new passwords significantly different from the previous three passwords. For instance, a Verizon (2021) analysis found that compromised credentials were involved in 61% of breaches, emphasizing the importance of strong password security. By enforcing stricter password policies, avoiding the use of dictionary words, consecutive letters and personal data like names and dates can guessed easily by hackers(*Essential Eight Explained | cyber.gov.au*, n.d.).

2.2.3 Solution 2: Implement Multi-Factor Authentication (2FA)

Even in this kind of scenario, when account passwords get hacked and Multi-Factor Authentication plays a crucial role in its security feature it can significantly decrease the chance of unauthorized access. Multi-factor authentication adds an extra layer of security by demanding multiple forms of verifications(*Turn on Multi-factor Authentication | Cyber.gov.au*, n.d.). In this PB's case, utilizing 2 Factor Authentication(2FA) such as one-time password(OTP) and biometrics(face ID) is sufficient to make it more difficult for malicious actors to exploit stolen credentials. For example, Microsoft's use of MFA has reduced account compromises by 99.9% by illustrating its efficiency in real-world environments (Maynes, 2024). According to that, this approach is particularly important for PinesBay, since the risk of unwanted access contributed by employees, is made worse by weak password security and the absence of MFA.

Figure 1 – Methods of 2-Factor Authentication(2FA)



Note. There should be a combination of 3 methodologies of Multi-Factor Authentication such as password, OTP and face recognition login to the system(self-constructed).

2.2.4 Preferred Solution with comparison:

Strengthening PB's password policy, and maintaining user convenience, involves requiring longer, more complicated passwords and reducing the period between password changes. Also using password management tools that are automated and require a minimum of 12 characters that include a variety of symbols are two ways that PB can improve its security. However, strong passwords can still be compromised through social engineering and phishing. According to that Multi-Factor Authentication (MFA) adds an extra layer of security to additional verification steps moreover to passwords. So, implementing MFA is the best solution to protect access logins from unauthorized personnel.

2.2.5 Implementation Plan:

- Hardware – Ensure all employees have access to smartphones capable of retrieving OTP and Biometric scanners are deployed across systems in requiring high-level security access.
- Software – Implementing MFA software such as Google Authentication or Microsoft Authenticator
- Training – Employees train on how to setup and handle MFA and give specific training to IT staff on how to monitor authentication-related issues or alerts.

2.3 Issue 3: Using Outdated SSL Protocol

The PBs use SSL (Secure Socket Layer) Protocol version 1.0, which is known to have several vulnerabilities. This outdated version exposes encrypted data to security flaws and makes it easier for attackers to exploit intercept communications and compromise sensitive information or disrupt the services. Those attacks commonly known as man-in-the-middle (MITM) attacks and its significantly harmful impact on the transferring of sensitive information such as personal and financial at Pines Bay.

2.3.1 Impacts on CIA triad

Confidentiality: Data can be intercepted and decrypted by attackers

Using outdated SSL 1.0 at Pines Bay compromises confidentiality as sensitive data like login credentials can be intercepted by attackers during its data transmissions.

Integrity: In transmitted of data could be manipulated by attackers

SSL 1.0's vulnerabilities able to hackers to modify data while it transmits resulting in mistakes or inaccurate data being added to the PB's system by undermining integrity.

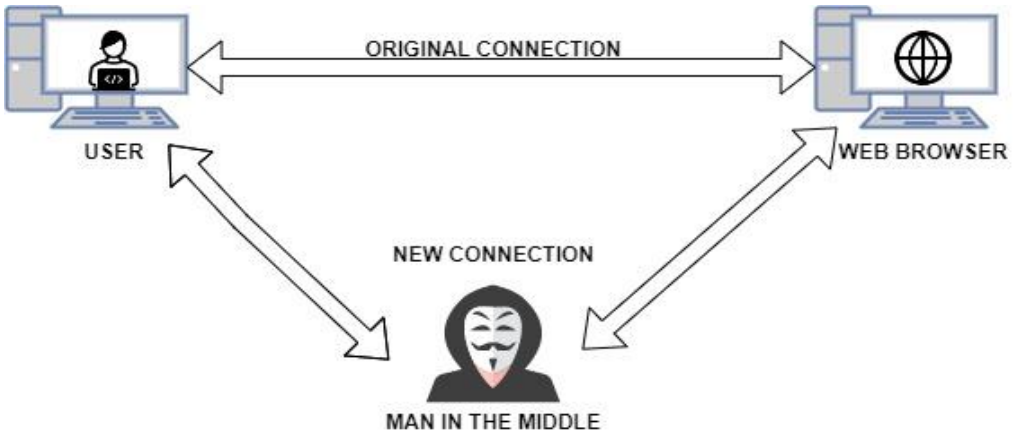
Availability: Compromised encryption can lead to system failure

Outdated SSL can lead to service disruptions with difficulty transmitting data via the PB's system and it can cause downtimes (delays) and unable to access the system.

2.3.2 Solution 1: Upgrade Transport Layer Security to version 1.3

Upgrading Pines Bay's outdated SSL 1.0 protocol to TLS 1.3 would especially improve the protection of secure data in transition with modern encryption. TLS 1.3 is the modern version of SSL, and it offers faster and more effective encrypted communication while eliminating vulnerabilities present in older protocols like man-in-the-middle attacks (MITM) (*Why Use TLS 1.3? | SSL and TLS Vulnerabilities | Cloudflare*, n.d.). Also, it reduces handshake latency, enhancing system speed and security. For example, in real-world scenarios, such as Facebook (Meta) has been implemented in TLS 1.3 and has illustrated that it reduces the risk of data interception while improving fast-loading websites (Guzman et al., 2020). Implementing TLS 1.3 in PB's system will secure confidentiality and guarantee data integrity and availability by preventing service interruptions caused by insecure connections.

Figure 2 – Man-In-The-Middle Attack



Note.Process of the man in the middle attack how it interrupts the connection between two devices(self-constructed)

2.3.3 Solution 2: Implementing a Virtual Private Network (VPN)

Implementing a Virtual Private Network (VPN) for remote access at Pines Bay can add a layer of encryption and security to the system. A Virtual Private Network facilitates the establishment of an additional level of encryption as it acts like a tunnel for all data exchanged over the VPN.VPNs take data transmitted between the users and the organization's network and encrypt them into a secure compromised tunnel. Also, it can prevent man-in-the-middle attacks even when accessing PB's system over insecure connections. For example, in the real world, NordVPN's use in corporate environments has shown that VPNs are effective in enhancing data security and protecting sensitive data and communication (Grigutytė & Grigutytė, 2024). This solution ensures that PB's network access is secure and adheres to all relevant standards in remote work security practices.

2.3.4 Preferred Solution with comparison:

Figure 3 – Comparison performance between TLS1.3 and VPN

Category	Upgrade TLS 1.3	Implement VPN
Encryption	Modern and strong web traffic	Have a secure tunnel for data transmission
Primary Purpose	Secures specific communications	Secures overall access and remote connections
MITM Attacks	Eliminates vulnerabilities present in older SSL versions	Secure from MITM attacks over insecure networks
Performance	Reduces handshake latency and fast	Have some latency due to encryption
User Experience	seamless experience once configured, and it has faster loader times	Must connect to the VPN before accessing the network
Real-world examples	Used by platforms like Meta for enhanced security	Widely adopted corporations like NordVPN to secure sensitive data

Note. Which implement is better with other performance TLS 1.3 or VPN (adopted)

TLS 1.3 is the best solution because it has modern encryption, and speed, and allows the user to overcome security issues which exist with other protocols and SSL or even VPN. Encryption in TLS version 1.3 has all the outdated vulnerabilities removed, integrity provisions guaranteed, as well as guarantees of confidentiality without interdependence on or additional resources typically required in the implementation of a virtual private network (*TLS 1.3 | Cloudflare SSL/TLS Docs*, n.d.).

2.3.5 Implementation Plan:

- Hardware – Null (There are no specific hardware requirements for enabling TLS 1.3)
- Software – TLS 1.3 enabled in the web application and server settings (such as Apache or Microsoft IIS - Internet Information Service)
- Training – IT staff should train to implement TLS 1.3 with configured web server environments and monitor SSL certificates

2.4 Issue 4: Non-Satisfied Physical Security

PB has an absence of physical security measures, with no mechanism to protect their sensitive areas such as server rooms, and data centers, from unauthorized access posing significant risks to the confidentiality, integrity and availability of PB's sensitive information. To prevent possible intruders or detect unauthorized access, PB does not have sufficient barriers or monitoring systems. This deficiency not only compromises the safety of PB's data but also undermines employee confidence and trust in the company's capacity to handle sensitive data.

2.4.1 Impacts on CIA triad

<u>Confidentiality: Non-secure physical access led to the theft of data</u>

Physical access to PB's system allows attackers to bypass digital security and leads to the theft of data via accessing directly its servers or devices by extracting sensitive information

<u>Integrity: Devices System integrity may be compromised by device manipulation</u>

Due to the lack of physical security circumstances, unauthorized persons tamper with servers to manipulate and potentially corrupt critical data.

<u>Availability: System outages may result in physical damage to the hardware</u>

Unauthorized physical access damages hardware components such as servers, switches routers with equipment, disconnects power sources or alters network settings. This can result in overheating, data loss or even permanent hardware failure.

2.4.2 Solution 1: Implementing physical security controls

To reduce the risk of physical security mechanisms at Pines Bay (PB), a comprehensive approach is based on the DID (Defense-In-Depth) model. Implementing a physical control system including access points like key cards and biometric authentications is a highly secure method that can be used for protection in server rooms, and it covers the **Physical Layer** of security. The **Administrative Layer** includes clear access policies for whoever has permitted access to sensitive areas and conducts background checks on that employee or person to ensure compliance has granted access privileges. In the **Technical Layer** deploying surveillance cameras (CCTV) able to real-time monitoring activities and alert security personnel to potential threats. According, to a study by the Security Industry Association (2021) 30% of unauthorized entries decrease by utilizing CCTV (Jeon et al., 2024). Implementing fire suppression systems (Fire alarms) is most of the time protecting the physical damage of servers and devices at the PB and it ensures the **Environmental Layer** of physical security.

2.4.3 Solution 2: Multi-Layered Protection for Physical Access

Implementing an extensive physical security system for Pines Bay, that includes multi-layered security on the DID model. At the **Physical Layer** Install reinforced doors and physical barriers such as baffle gates (automated gates) in sensitive areas of PB such as server rooms and admin rooms. Also, implement a digital visitor management system to record all visitors' details sign in and wear ID badges. This **Administrative Layer** ensures pre-approval of visitors and those who can access sensitive areas. In the **Technical Layer** of this security, utilizing an advanced alarm system is better to trigger alerts when unauthorized access is made in the sensitive areas at PinesBay. Devices and server equipment are working 24 hours due to their workload because of this it overheats and damages the circuits or other parts of the equipment. Implementing a temperature control system in sensitive areas such as server rooms could prevent that damage. This approach will accomplish the **Environmental Layer** physical security.

2.4.4 Preferred Solution with Comparison:

Both solutions focus on enhancing physical security at Pines Bay (PB) via using the Defense-In-Depth (DID) model. Solution 1 corporates biometrics and keycards for the Physical Layer, ensuring secure access to critical areas, while access policies in the Administrative Layer to secure entries. CCTV surveillance offers real-time monitoring in the Technical Layer and fire suppression systems address the Environmental Layer of security. However, implementing reinforced doors and baffle gates are extra physical barriers in solution 2. Also, its visitor management system regulates access in the Administrative Layer and advances alarms for immediate alert using in the Technical Layer. According to these resources, solution 2 is better, because it offers more comprehensive protection, especially in the Physical and Environmental layers with strong barriers and temperature controls.

2.4.5. Implementation Plan

- Hardware – Install Reinforced Doors and Baffle Gates entrance at sensitive areas and deploy advanced temperature control systems including cooling fans/units and sensors.
- Software – Implement Visitor Management software to track and log all visitors' details with provide real-time alerts in unauthorized access attempts in critical areas.
- Training – Train security staff on how to manage the digital visitor management system with monitor access logs and provide guidance to IT staff maintaining temperature control systems and alarm management software.

2.5 Issue 5: Single-Pass Data Deletion

PB uses a single-pass data deletion method to erase sensitive data from storage devices. This causes significant risk in the Pines Bay scenario because that method allows attackers to recover information easily. This makes vulnerabilities during device disposal of operational remaining data would be exposed. In Pines Bay handles large amounts of confidential data but utilizing the single-pass data deletion method undermines the strategy of protecting data at Pines Bay.

2.5.1 Impacts on CIA triad

Confidentiality: Sensitive Information can be recovered from disposed storage

This approach exposes data to restoration by hackers using sophisticated tools like TestDisk and this breach would result in the exposure of sensitive information such as personal and financial data following the device's disposal.

Integrity: Relevant data recovered could be modified and use malicious activities

When data is recovered and modified by an attacker, the integrity of its system is compromised manipulated data could be reintroduced to the system or sold to illegitimate parties and this will undermine the trustworthiness of PB's data.

Availability: Improperly deleted data could lead to system vulnerabilities

If an attacker obtains access to the recovered data, they could use it to sabotage PB's operations using ransomware attacks or deleting important files. Storage devices are disposed of improperly and they could be misused again which could result in inappropriate disclosure or interruptions to services

2.5.2 Solution 1: Implement Multi-pass Data Wiping

Multi-pass data wiping is a more secure solution to Pines Bay's inadequate single-pass data deletion method. This multi-pass wiping will overwrite the data on the storage device multiple times to make sure any sensitive information is no longer present and not recoverable by tools like TestDisk. For example, the U.S. Department of Defense (DoD) 5220.22 – M standard advocates the overwriting of data at least three times effectively cleaning them in the relevant system (*DOD 5220.22-M Explained - Data Erasure Standards | JeTICO*, n.d.). This ensures that no recovery tool can even extract the original data. Furthermore, a relevant real-world application known as DBAN (Darik's Boot and Nuke) tool supports multi-pass data wiping and it's widely used to securely erase data from hard drives (*Darik's Boot and Nuke – DBAN*, 2023). This method ensures attackers are prevented from recovering data and disposed of devices become safe for reuse or recycling.

2.5.3 Solution 2: Physical Destruction of Storage Devices

Discarding data on storage devices physically before disposal is a useful substitute for software-based deletion of data. Physical destruction of storage devices ensures data is completely irretrievable and eliminates the possibility of recovery by tools like TestDisk. Common methodologies of this physical destruction use such as shredding, degaussing (using a powerful magnetic field to erase data) or incinerating hard drives are common methods for destroying sensitive data. For instance, Google and Amazon physically destroy their decommissioned hardware to ensure that no data can be recovered from their systems (*Data Deletion on Google Cloud*, n.d.). Physical destruction is a secure method to eliminate the risk of data breaches, especially in high-risk locations such as Pines Bay (PB), where ideally all sensitive information should be exposed if any type of storage devices are poorly discarded.

2.5.4 Preferred Solution with comparison:

Figure 4- Performance in data deletion methods

Method	Effectiveness	Time Required	Security Level	Cost
Single-Pass deletion	Low	Fast	Low	Low
Multi-Pass deletion	High	Moderate	Medium	Moderate
Physical destruction	Very High	Slow	High	Very High

Note.Comparison of the performance between data deletion methods (adopted)

The recommended solution for Pines Bay is multi-pass data wiping, which offers a cost-effective and environmentally friendly option without requiring special equipment. It involves overwriting data multiple times which significantly reduces the chances of recovery using common tools like TestDisk. This method well aligns with PB's budget limitations and offers robust protection faster, against data recovery. So, these wiped drivers can be reused or recycled, making this solution more sustainable than physical destruction.

2.5.5 Implementation Plan:

- Hardware – Null (This doesn't require any extra hardware to delete data)
- Software- Install multi-pass wiping software such as DBAN or Blancco Drive Eraser and configure the number of overwrite passes to ensure data is securely erased (e,g; DoD 5220.22-M standard with 7 passes)
- Training – Train IT staff on how to use and verify multi-pass data wiping software including an appropriate number of passes for different types of devices that need to be set up.

2.6 Problem 6: Default Remote Desktop Protocol (RDP)

Pines Bay (PB) allows its staff members to work remotely using Remote Desktop Protocol (RDP) by using the standard configurations. This causes critical security risk due to it allows remote access without using adequate encryption or protocol, attackers can exploit vulnerabilities leading to unauthorized access, data breaches or malware infections. In the Pines Bay case study, many employees are working remotely and RDP is a convenient tool for remote access but it represents a significant security risk if the session is not fully configured or secured.

2.6.1 Impacts on CIA triad

Confidentiality: Default settings of RDP expose sensitive data

RDP default settings do not include advanced encryption protocols and multi-factor authentication making vulnerabilities in PB for unauthorized access and exposing sensitive data such as password credentials and admin logins.

Integrity: Attackers allows to manipulate data

Without enhancing the RDP security, attackers can modify or alter system settings after gaining access. Because of the possibility of undiscovered unauthorized modifications interfering with regular operations, this compromises the integrity of PB's systems.

Availability: RDP is a common attack vector for ransomware.

RDP (Remote Desktop Protocol) is a frequent target for ransomware attacks. In these incidents, attackers can remotely lock Pines Bay servers out of their systems and demand a ransom to restore access. This impact on service availability often leads to critical downtime for municipal operations.

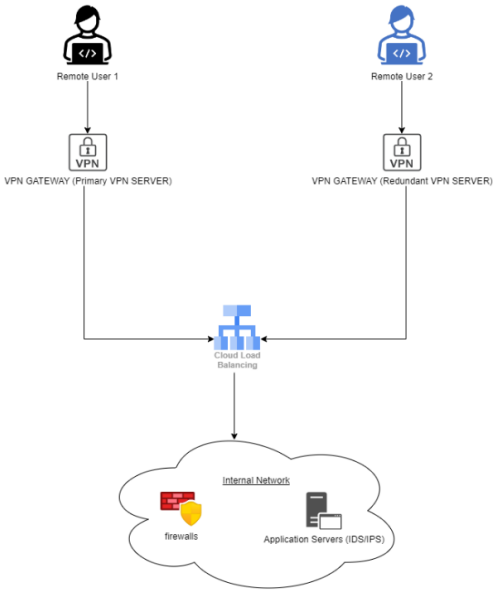
2.6.2 Solution 1: Implement Strong RDP Security with firewalls and network-level authentication

Network-Level Authentication (NLA) is a crucial initial step to reduce the risks involved with using the default Remote Desktop Protocol (RDP) settings at Pines Bay. NLA requires users to authenticate themselves before creating an RDP session, thereby decreasing the possibility of brute-force attacks and unauthorized access(Portnox, 2023). Also, firewalls should used by PB to block RDP access to particular IP addresses to limit the attack surface and prevent unauthorized external connection. organizations such as the FBI have recommended using firewall rules to secure RDP connections since there has been an increase in ransomware attacks targeting vulnerable RDP ports(SAFETY4SEA, 2018). By enforcing these security measures, PB can guarantee that remote access is strictly regulated, reducing the possibility of service interruptions or data breaches. Combining NLA with firewalls significantly enhanced the PB's security against cyberattacks on RDP.

2.6.3 Solution 2: Setup Virtual Private Network (VPN) for Remote Access

Implementing a Virtual Private Network is an efficient way to improve security for remote access at Pines Bay. VPNs establish encrypted tunnels to protect data transmission and safeguard remote desktop sessions from unauthorized access and man-in-the-middle (MITM) attacks. By directing remote connections through a secure VPN, PB can reduce the associated risks of using default RDP settings. An example of this is the UK's National Health Service (NHS) which experienced a significant reduction in cyberattacks after mandating staff to access systems through a VPN while working remotely (*Symantec Enterprise Cloud*, n.d.). Using these VPNs also hides the user's IP address and making it more challenging for attackers to identify and target PB's network. When combined with firewalls and multi-factor authentication (MFA), VPNs add an extra layer of security, ensuring that only authorized users can access PB's systems.

Figure 5 – VPN architecture with redundancy for secure remote access



Note: Showcasing secure remote access through a primary and redundant VPN server, with a load balancer to distribute traffic enhancing both security and availability in the internal network(self-conducted).

2.6.4 Preferred Solution with comparison:

Both solutions are improving the security of remote access at Pines Bay. Solution 1 illustrates securing remote access with Nework-Level Authentication and firewalls by limiting external threats control and reducing brute-force attacks. However, solution 2 evaluates leverages VPNs providing encrypted tunnels to safeguard remote sessions. According to that Most suitable security option for Pines Bay remote access is the implementation of a Virtual Private Network (VPN). It Enhances RDP security with authentication and firewalls by hiding user's IP addresses and comprehensive encryption for the entire remote connection by safeguarding all data traffic from unauthorized access. Also, VPNs are a more cost-effective and simpler solution to implement compared to configuring advanced RDP settings.

2.6.5 Implementation Plan:

- Hardware - Set up a dedicated VPN gateway, such as Cisco ASA, and guarantee seamless integration with PB's current firewall.
- Software - Deploy VPN software such as OpenVPN or Cisco AnyConnect with multi-factor authentication (MFA) integration to ensure secure encrypted remote access.
- Training – Provide training for employees on how to use VPNs and provide IT staff with instructions for managing and resolving issues with the VPN gateway.

3. Backup Strategy of Data in Pines Bay Scenario

The Pines Bay (PB) City Council handles large amounts of sensitive data as part of its digital operations. This data is crucial for Pines Bay's day-to-day activities and for serving the needs of the employee community. PB has recently experienced a cyberattack, highlighting the need for a reliable and safe data backup strategy. This report provides a comprehensive backup strategy designed to ensure PB can recover faster from future cyber attacks in the shortest possible time while maintaining data integrity, confidentiality, and availability.

3.1 Comparison of Data Backup Types

To develop an efficient backup strategy, it's essential the need of three primary types of backups

3.1.1 Full Backup

A full backup makes a complete copy of all data such as files, folders, and hard drives and ensures the entire system can be restored in one step in time. Although, this requires significant time and storage, which can be expensive, especially for large data sets. According to that, this is suitable for weekly backups to provide a baseline for data recovery (Marget, 2024).

3.1.2. Incremental Backup

In the Incremental backup, only backup data has changed since the last backup, and it will mitigate the required time and space of the storage. The restoring data requires multiple steps, as each incremental backup must be applied in sequence. This is Ideal for daily backups to capture the ongoing changes efficiently(Marget, 2024).

3.1.3. Differential Backup

All the backup data has changed since the last full backup and this enables a faster recovery than incremental backup since only two backups are needed (full and differential). As time goes on, differential backups grow larger and require more storage. Differential backups can be used mid-week to reduce recovery time compared to incremental backups(Marget, 2024).

3.2 On-Site vs, Off-Site Backup

PB must decide whether to store backups on-site (locally) or off-site (remotely, in the cloud).

3.2.1. On-Site Backup:

This provides faster recovery times since the data is stored in locally. So, this type of backup is mostly suitable for small to moderate incidents where immediate recovery is required. Since this backup is physically located on-site it will offer faster and instant access to data. However, this on-site backup is Vulnerable to local threats like theft, fire, natural disasters, or physical damage from power surges, and higher cost to maintain (Rock & Rock, 2024).

3.2.2 Off-Site Backup:

Off-site backup protects data from local disasters and ensures business continuity in the case of widespread damage. The security of this backup depends on the encryption techniques during the transmission of data.(Kirvan et al., 2024) Restoring data can be slower due to network latency or the transport of physical media and it also relies on third-party services, which introduces external risk factors, including potential data breaches.

3.3 Recommended Backup Strategy

According to given PB's needs and vulnerabilities, the recommended strategy is offsite backup. Offsite backups store data at a remote location and that sensitive data is safe from local disasters like fires, theft, or system failures that could affect onsite backups. By using offsite backups, PB can protect its data from physical disasters or cyberattacks that compromise local systems. Additionally, offsite backups, when encrypted and secured, offer a more resilient disaster recovery solution, allowing PB to quickly recover from disastrous events and minimize downtime.

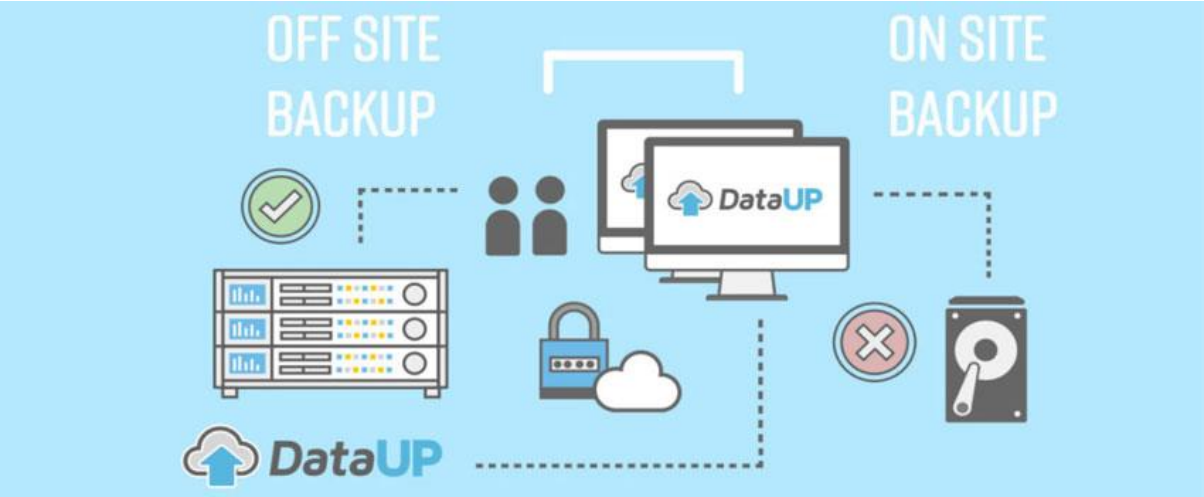
3.3.1 Full Weekly Backups:

Perform a full backup of all data every week to establish a complete data set. This ensures that PB can recover from major incidents or system failures. Store these full backups locate on the cloud and this should be encrypted to secure data during off-site transmission(*[Guide] Create a Weekly Full Backup, a Daily Differential Backup, and a Monthly Image Backup (With Retention)*, n.d.).

3.3.2 Daily Incremental Backups:

These backups are performed on weekdays and this will capture the changes since the last full backup. According to that this daily backup saves storage space and reduces network load as only modified files were backedup(*Protect Your Data With Daily Backups | DigitalOcean*, n.d.).

Figure – 6 Flow of data in Onsite and Offsite Backup



Note.Admin. (2023, November 6). *What are Offsite Backups and Why are they Important? - Backup Everything*. Backup Everything. https://backupeverything.co.uk/what-are-offsite-backups-and-why-are-they-important/

3.4 Data Backup Protection

To secure PB's data backups, encryption and access control play major critical roles in protecting sensitive information where located in data backups.

3.4.1 Encryption:

Utilizing AES-256 encryption (*Guidelines for Cryptography | cyber.gov.au*, n.d.) for all backup data is secure both in transit and at rest. This encryption standard ensures that, even if backup data is compromised, it cannot be easily decrypted. This method ensures that encryption keys are stored securely and accessible to only authorized personnel.

3.4.2. Access Control:

Implementing strict authentication and authorization protocols ensures that only designated employees can access or restore backup data. Role-based access controls (RBAC) should be used to limit access based on employee job functions.

4. Summary

Pines Bay (PB) is facing significant cybersecurity and physical security issues due to a combination of outdated systems, weak access controls, and poor security policies. Employees have excessive administrative privileges, and weak password policies make PB vulnerable to attacks like unauthorized access and data breaches. Moreover, the use of the default Remote Desktop Protocol (RDP) without proper security measures exposes PB to external threats. Physical security is also a concern, with inadequate protection for sensitive areas like server rooms. To address these issues, PB needs to implement several key solutions such as upgrading TLS 1.3 for secure communication, using VPNs to protect remote access, and strict access with stronger password policies and **administrative** controls. Lastly, improving physical security through multi-layered approaches and implementing a strong backup strategy with offsite backups ensures PB can recover quickly from any potential incidents.

References

Bakharev, N. (2024, September 6). Unauthorized Access: Risks, examples, and 6 defensive measures. Bright Security. https://brightsec.com/blog/unauthorized-access-risks-examples-and-6-defensive-measures/

Chakravarty, S. (2024, September 26). CIS Controls v8 Released | SANS Institute. https://www.sans.org/blog/cis-controls-v8/

Create and use strong passwords - Microsoft Support. (n.d.). https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb

Cyber Security Training | SANS courses, certifications & research. (n.d.). https://www.sans.org/apac/

Darik's Boot and Nuke – DBAN. (2023, August 15). Darik's Boot and Nuke. https://dban.org/

Delinea Inc. (n.d.). What is Just-in-Time Access (JIT)? Delinea. https://delinea.com/what-is/just-in-time-access

DOD 5220.22-M Explained - Data Erasure Standards | JeTICO. (n.d.). https://www.jetico.com/blog/dod-522022-m-explained-data-erasure-standards

Enzoic. (2024, April 24). NIST Digital Identity Guidelines: A Brief summary. Enzoic. https://www.enzoic.com/blog/nist-password-guidelines/

Feldman, P. D. O. K. R. G. W. L. (2022, November 29). 2021 Cybersecurity and Privacy Annual Report. NIST. https://www.nist.gov/publications/2021-cybersecurity-and-privacy-annual-report

Grigutytė, M., & Grigutytė, M. (2024, July 26). Can a VPN improve your online privacy? | NordVPN. NordVPN. https://nordvpn.com/blog/vpn-and-privacy/

Guzman, A., Nekritz, K., Iyengar, S., & Changigi. (2020, March 23). Delegated credentials: Improving the security of TLS certificates. Engineering at Meta. https://engineering.fb.com/2019/11/01/security/delegated-credentials/

Jeon, H., Kim, H., Kim, D., & Kim, J. (2024). PASS-CCTV: Proactive Anomaly surveillance system for CCTV footage analysis in adverse environmental conditions. Expert Systems With Applications, 254, 124391. https://doi.org/10.1016/j.eswa.2024.124391

Marget, A. (2024, August 6). Types of backup: full, incremental and differential backup. Unitrends. https://www.unitrends.com/blog/types-of-backup-full-incremental-differential

Martinez, J. (2024, September 27). CyberArk vs. BeyondTrust: Which PAM Solution is Better? StrongDM. https://www.strongdm.com/blog/cyberark-vs-beyondtrust

Maynes, M. (2024, March 28). One simple action you can take to prevent 99.9 percent of attacks on your accounts. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

NIST. (2024, September 24). NIST. https://www.nist.gov/

Portnox. (2023, June 13). What is Network Level Authentication (NLA)? - Portnox. https://www.portnox.com/cybersecurity-101/network-level-authentication-nla/

Protect your data with Daily Backups | DigitalOcean. (n.d.). https://www.digitalocean.com/blog/daily-backups-now-generally-available

Rock, T., & Rock, T. (2024, September 25). 7 Strategies to Avoid Data Loss from Natural Disaster. Invenio IT. https://invenioit.com/continuity/data-loss-from-natural-disaster/

SAFETY4SEA. (2018, October 4). FBI, DHS: Cyber security tips related to Remote Desktop Protocol. SAFETY4SEA. https://safety4sea.com/fbi-dhs-cyber-security-tips-related-to-remote-desktop-protocol/

Symantec Enterprise Cloud. (n.d.). https://www.broadcom.com/products/cybersecurity

Team, S. N. (2019, June 13). Baltimore, $18 million later: “this is why we didn’t pay the ransom.” Cybersecurity Conferences & News. https://www.secureworld.io/industry-news/baltimore-ransomware-attack-2019

Turn on multi-factor authentication | Cyber.gov.au. (n.d.). https://www.cyber.gov.au/learn-basics/explore-basics/mfa

What is Role-Based Access Control (RBAC)? Examples, Benefits, and More | UpGuard. (n.d.). https://www.upguard.com/blog/rbac

What is sensitive data exposure and how can you prevent it? (2024, September 20). Consent Management Platform (CMP) Usercentrics. https://usercentrics.com/knowledge-hub/sensitive-data-exposure/

Why use TLS 1.3? | SSL and TLS vulnerabilities | Cloudflare. (n.d.). https://www.cloudflare.com/learning/ssl/why-use-tls-1.3/