Organization Selection

The Real Estate Wealth Network is the organization selected. The Real Estate Wealth Network organization is responsible for real estate, mentorship, and resources in an online platform environment according to (Fowler, 2023). This organization was founded in 1993 by Cameron Dunlap (Fowler, 2023). Real Estate Wealth Network had a cyber-attack in December of 2023, that exposed 1,523,776,691 records according to (Kosling, 2024). The leaked information contained according to (Kosling, 2024) street addresses, purchase prices, dates of purchase, mortgage company, taxes owed, mortgage loan amount, property owners, sellers, investors, internal user logging data, tax ID number and more.

Overview Of the Goals and Objectives

The goal and objective of an insurance plan is to protect important information from falling into the wrong hands. This can happen if you don't require authentication to view important information. You can require identification for important information by access control with Role Based Access Control or (RBAC). This is where you restrict users from viewing information based on their roles within the organization. For an organization that keeps Personal Identifiable Information or (PII) it is strongly recommended to use RBAC alongside multifactor authentication. This requires anyone to know two things to authenticate to view the PII. These two things for example could be a key card and a password like an employee number, one you can physically hold to authenticate and the other you must know like a password.

Having integrity for an organization would mean putting encryption on the data they contain on their servers, for their customers, so that no one can modify it without properly authenticating first. Having integrity would also mean protecting this data from viruses that can delete or damage files. This can be done by using antivirus software to help protect against this threat of information and provide a layer of protection. Another integrity layer would be having policies such as how often you perform audits in a database to check for any modifications of data. If data is changed it should be a policy to have the name of who made the change, when was it changed, and what was changed.

Finally, we have availability, which is also an important step in an insurance plan. Availability in one way is how fast you can recover from a failure such as a server crashing or running out of room in your virtual machine (Information Assurance (IA): Defined & Explored | Unitrends, 2022). Instead of having customers wait for a repair that could take hours. They instead don't have to wait because the organization has a backup server (Information Assurance (IA): Defined & Explored | Unitrends, 2022). If the first server fails or the virtual machine is at full data capacity, it can go offline, and the backup server becomes the first server in a sense that the customers will use until the repairs are done on the first server. After repairs on the first server are finished, the second server goes offline, and the first server comes back online without affecting the organization's website or information customers need to access, giving their customer’s twenty-four seven around the clock access.

The overall benefits of having an insurance plan are helping your business stay up twenty-four seven, giving your business more money and when something goes wrong having a failover in place to still support your customers. You also gain policies and procedures for everyday use of your database that holds the most important information such as PII that your customers need access to. Having those policies and procedures helps keep the organization a step ahead of a data breach with another layer of defense. Also, you put in motion security for your data that people in your company must follow to have access to customer’s data, which saves the company from an inside attack. Lastly you gain a reputation for protecting customer’s data with constant audits of who changed the data, what data was changed, and when was it changed, helping in case there is an attack and data is altered. Also, in the event of a virus alerting or deleting data, the company can have data backups of that data, so that customers don't suffer from the virus. Your organization can know how the attack happened and if their security had weaknesses or their polices, they can add more after, so it does not happen again.

Confidentiality, Integrity, and Availability of Information

In the event of the Real Estate Wealth Network cyber-attack the lack of integrity and authorization is vital to why 1,523,776,691 records got exposed (Kosling, 2024). According to (Kosling, 2024) Jeremiah Fowler, a security researcher found that Real Estate Wealth Network's database was unprotected. Meaning unencrypted, with no confidentiality involved with securing customer's street addresses, purchase prices, dates of purchase, mortgage company, taxes owed, mortgage loan amount, and much more (Kosling, 2024). This also means there was no authentication for gaining access to the information. The integrity of the database found by the security researcher lacks knowing if any of the information has changed. As from research in the integrity of the Real Estate Wealth Network there were only log records according to (Kosling, 2024) that showed that the "files belonged to New York-based Real Estate Wealth Network." In other reports it fails to mention whether audits were done on the database, which would be why the database was unprotected and that's why Real Estate Wealth Network was not aware of the database not having any protection against attacks. As according to (Fowler, 2023) "it is unknown how long the data was publicly exposed or even if anyone else may have accessed it." The availability of the Real Estate Wealth Network database was not only available to authenticated users as anyone could view this information. Logging records showed according to Fowler (Fowler, 2023) "The records I saw included the user's name, phone number, email, device information, and what files the user accessed." Fowler also noted that internal search data was also seen by him (Fowler, 2023).

Current Protocols and Policies

In the event of the attack in December 2023 Real Estate Wealth Network did not have any protocols in place for authenticating the users who accessed the database that contained PII. For protecting this information, the user should have to know PII such as social security number to authenticate, and the person's birthdate. As well as using multifactor authentication alongside this there are a handful of options. The user could have to take part in verifying their email address and know their username and password on the site. Just to recap, the customer would need to know their social security number, their birthdate, their email address and verify their email by waiting on email sent from the website. The customer would then have to access their email knowing the email address and password and find the document and click verify. After doing this, you would get redirected to another page that would ask for your username and password on the website. This would check the username and password on the server in the database to authenticate you. Also, the database should have AES-256-bit encryption that is industry leading to protect against hackers.

For integrity in the system audits should be done so that Real Estate Wealth Network knows when an outside attacker is accessing their database. Basically, this part of the audit can help Real Estate Wealth Network know when other people besides their employees are accessing the database. Finally, the last part of the audit will be internal and will require only employees who have access to the database to use a log to keep track of internal threats inside the organization. This log tells the company the who accessed their database, why did they access the database, and when they accessed the database. This is another protocol that must be put in place to address issues that will arise from protecting PII.

Real Estate Wealth Network did not have availability for authenticated users but for everyone. This is a security issue and needs to be addressed. For availability the Real Estate Wealth Network database should only be available to those who have an account with the Real Estate Wealth Network. This still allows potential customers/users to access Real Estate Wealth Network and to view what services they can provide but they cannot access the database without first creating an account with a social security number, birthdate, password, username, and email address. This part of availability allows Real Estate Wealth Network to make sure the database is only available to people who are authorized customers/users. The next part of availability is making sure this database is always available for those customers/users, as it contains PII they need to have access to twenty-four seven. Real Estate Wealth Network should have backups of the database in case of viruses or stolen data. This also means that the backup needs to follow strict protocol to have the data encrypted with AES-256-bit encryption. As AES is the strongest encryption available so far, it should be used for the most important information. The last protocol to have in place is to have a backup server in case the first server goes down your customers/users will need around-the-clock availability to access this information. The organization can also use the cloud such as Microsoft Azure for large amounts of data (v-amallick, 2023). If the company chooses cloud service for backups they will need the Azure Database for PostgreSQL servers, as these can backup Azure PostgreSQL databases and retain the backups for up to 10 years (v-amallick, 2023).

Finally, the potential barriers of following and implementing these protocols will be training of employees for logs in the database. This is because if an employee checks into the database to change a piece of PII of a customer but does not log it, this could lead to an investigation from an employee's mistake wasting the company's time and resources for nothing.

Another barrier is implementing backups of all customer data. This is a barrier because Real Estate Wealth Network holds billions of records of customer's information. It would be important to invest in backups in case of disaster but then the company would need more protocols in place to keep up to date with making sure the backups are kept safe from attackers. The last part of the implementation that would be a barrier is implementing multifactor authentication to users. As customers may take resistance to multiple steps of login to view their PII.

Role of the key leaders

Real Estate Wealth Network's leader is Cameron Dunlap. According to (ZoomInfo: B2B Database | Business Leads & Company Contacts, 2025) he is the founder and Chief Executive Officer. The role Cameron plays in security is overseeing the risks involved in development and implementation of risk mitigation strategies, incident response plans, and disaster recovery plans (Eide, 2024). Cameron must be sure to align cybersecurity with business goals and objectives (The CEO's Role in Cybersecurity: A Vital Component of Organizational Defense - CYPFER, 2023). Instead of hindering cybersecurity by not having policies that make sure your computer is up to date with the latest software, you build policies wherever there could be an attack (The CEO's Role in Cybersecurity: A Vital Component of Organizational Defense - CYPFER, 2023). This is positioning cybersecurity as the enabler of good business and success (The CEO's Role in Cybersecurity: A Vital Component of Organizational Defense - CYPFER, 2023). As founder of Real Estate Wealth Network Cameron is responsible for the allocation of resources to cybersecurity. This entails setting up a budget for the cybersecurity tolls needed to keep the organization safe (The CEO's Role in Cybersecurity: A Vital Component of Organizational Defense - CYPFER, 2023). Making sure to address any threats (The CEO's Role in Cybersecurity: A Vital Component of Organizational Defense - CYPFER, 2023) that are talked about from the cybersecurity team in meetings to be effective and active in safety for the organization. Also, assigning the correct training for employees (The CEO's Role in Cybersecurity: A Vital Component of Organizational Defense - CYPFER, 2023) to be effective in fighting against real threats by learning procedures and understanding why the organization has those policies and procedures and what is required to meet them.

Key ethical and legal considerations

The ramifications of key leaders not accounting for legal and ethical considerations can be disastrous for an organization. Key leaders who don't account for legal and ethical considerations make their organization less likely to thrive in business. Customer trust will significantly degrade, due to not properly handling customer information. According to (William & Mary, 2023) the fallout of the Enron scandal in 2001, that resulted in unethical accounting practices. According to (William & Mary, 2023) showing a facade of profitability that led to Enron's bankruptcy. This also made the fallout worse to shareholder's losing money and public trust in corporate governance being eroded (William & Mary, 2023). This is why it is important to consider ethical and legal considerations, as doing so should involve ensuring privacy, fairness, transparency, and accountability in handling data, implementing security measures, and responding to threats according to (Gomez, 2024). When handling sensitive customer data, the employees withing the company should not say anything to the public, giving away what information they have access to. Also, employees should not transmit this data in any way besides, what is acceptable to protect this information from potential actors (Chin, 2023). In the event of a buinsess that has a data breach attack, their customers should have an alert telling them what has been potentially accessed in the event of this attack. This can lead to eroded trust from customers, if the business is not transparent about the breach (Chin, 2023). Also, the importance of reporting these breaches is important as it gives industry professionals a better grasp on how to protect information better for their clients, from potential actors (Chin, 2023).

Key components of information assurance

The responsibility of information assurance is according to (SentinelOne, 2024) “spread out among IT security teams, senior management, and employees.” The IT security teams are responsible for the maintenance and installation of the security measures of the organization (SentinelOne, 2024). The key leaders such as the CEO are the ones to give oversight in compliance and risk management (SentinelOne, 2024). The employees are the people responsible for practicing compliance with the procedures and policies (SentinelOne, 2024). The employees are also responsible for giving important feedback to IT or CEO to give them better insights into their daily tasks, and any security measures that need to be taken to better support them in doing those daily tasks. The five pillars of information assurance are confidentiality, integrity, availability, identification, and non-repudiation (SentinelOne, 2024). The existing policies of the Real Estate Wealth Network organization did not account for any of these, besides having logs for the database that was breached. If installation of information assurance is to help with the database that was attacked. Real Estate Wealth Network should consider using a risk assessment to better understand the consequences of threats, vulnerabilities, and security incidents (SentinelOne, 2024). This will give the correct number of resources to respond to these threats, vulnerabilities, and security incidents. A clear development of security policies for the data Real Estate Wealth Network is responsible for protecting. The security policies should be centered around data protection, access controls, and what to do in case of responding to a threat (incident response) (SentinelOne, 2024). The training of employees would also help the database according to (SentinelOne, 2024) so that employees know how to handle the Personal Identifiable Information within their database. Also, a better monitoring and auditing system. As they were told by a cyber security expert that their database was not protected. Not one of their systems caught this. Correctly installing a monitoring system and auditing the database will help find security weaknesses and vulnerabilities (SentinelOne, 2024). This will help the security team allocate resources (SentinelOne, 2024) to these areas to more effectively protect their organization's customer data.

Analyze the environment

The environment that the Real Estate Wealth Network operates from, including the policies and protocols, is only having logging records on the database that was breached (Fowler, 2023). Information assurance is not implemented as this does not remotely help against any attacks. Real Estate Wealth Network is not adhering to the law. Having customer's data available for anyone to see and steal from the database without any authentication and integrity. The organization getting attacked ruins customer's trust, reputation of the organization, and loss of revenue from not only losing customer's but facing penalties form not following the law.

Threat environment

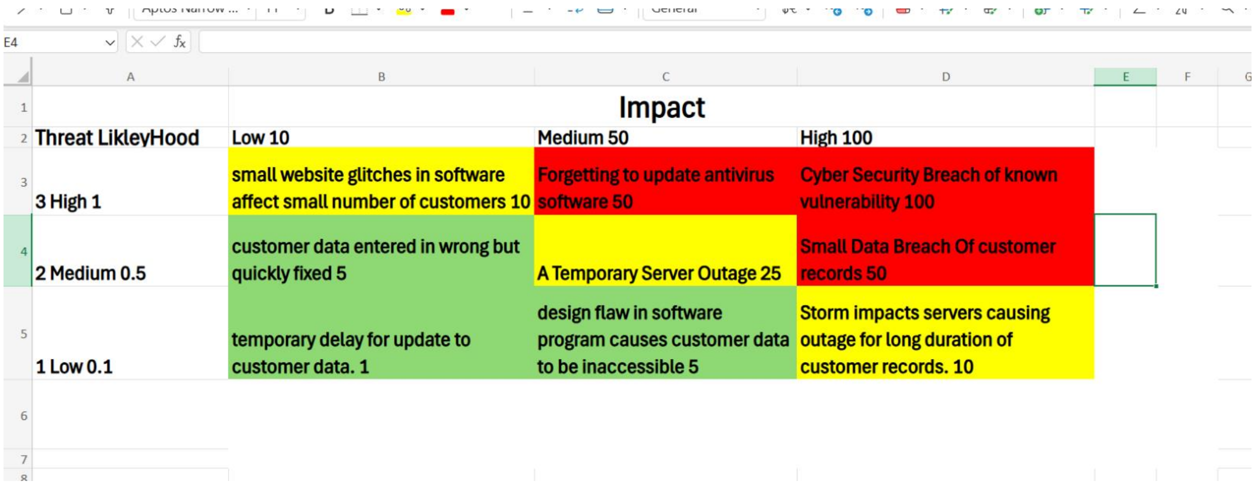
What could go wrong if Real Estate Wealth Network's database gets attacked? For Real Estate Wealth Network's database only having logging records of the database (Fowler, 2023) this opens any attacks a malicious actor wants to expose. These attacks could be placed on Real Estates Wealth Network's database due to financial gain, espionage from a competitor, hacktivism, or ransom attack (Sophos, 2024). The database of Real Estate Wealth Network is not encrypted making the information of customer's easier for attackers to use and obtain. Due to no policies or procedures an employee of Real Estate Wealth Network could accidentally give their employee username and password in an email phishing attack (The Top 5 Cyber Threats Facing Businesses Today, 2025). This could give the malicious actor access to more databases from

Real Estate Wealth Network. The malicious actor could also use the customer's emails from the database to perform scams for financial gain (Sophos, 2024). The website could have malware installed from malicious actor in the form of a link (The Top 5 Cyber Threats Facing Businesses Today, 2025). This allows the attacker to run harmful programs on the site to any visitors (The Top 5 Cyber Threats Facing Businesses Today, 2025). Malware could then destroy or take control of the victim's computer (The Top 5 Cyber Threats Facing Businesses Today, 2025). If an employee of Real Estate Wealth Network's IT team or cyber security team clicked on the link containing the malware this could be disastrous. The attacker could then take control of the computer containing all files it has from Real Estate Wealth Network's other databases. The attacker could potentially continue to spread the malware through most, if not, all Real Estate Wealth Network's databases. Another attack that could take place is an SQL injection. In this attack an attacker uses input fields to insert malicious code to make a harmful query on the database (The Top 5 Cyber Threats Facing Businesses Today, 2025). If executed by the attacker and with no protection from Real Estate Wealth Network's database this would delete data, change data, or take control of the whole database (The Top 5 Cyber Threats Facing Businesses Today, 2025).

Best approaches

What is the best way to mitigate these risks associated with Real Estate Wealth Network's database? To mitigate these threats Real Estate Wealth Network will need to implement encryption to customer information so that the information taken from the database can be harder for attackers to decrypt. Using Bcrypt a hashing algorithm, will help store the password safely, along with AES or Advanced Encryption Standard for decrypting and encrypting it from the Bcrypt key (Securing User Passwords: Hashing vs. Encrypting – Preventing the Unpreventable | QwietAI, 2023). Next, employee training, policies, and procedures for what to do, how to spot malicious emails, and how to handle reporting a phishing email to avoid disaster (CISA, 2024). This will help employees give away important information to malicious actors. The policy for malicious emails should be to according to (CISA, 2024) report any suspicious emails, prohibit clicking links from emails employees do not know, and to not download anything from emails that are unknown. Also, the cyber security team should create and update filters for malicious emails, from reports from employees (CISA, 2024). To avoid SQL injection input validation should be checked by cyber security team. Allowing no special characters for inputs and implementing an open-source firewall called ModSecurity (Kime, 2023) to help catch most SQL injection attacks through web channels. To avoid a malware attack to the organization's databases, Real Estate Wealth Network should use according to (Protect Yourself from Malware - Google Ads Help, 2025) antivirus programs to scan anything that employees need to download. This will help against malware attacks by scanning your computer (Parker, 2019) to determine if files are malicious. The policies in place to keep the antivirus programs effective and secure your computer are updating your computer and software regularly, running scans every day, and always adhere to security policy of not clicking on everything you see on a website or email according to (Parker, 2019).

Risk matrix



	Impact		
Threat LikleyHood	Low 10	Medium 50	High 100
3 High 1	small website glitches in software affect small number of customers 10	Forgetting to update antivirus software 50	Cyber Security Breach of known vulnerability 100
2 Medium 0.5	customer data entered in wrong but quickly fixed 5	A Temporary Server Outage 25	Small Data Breach Of customer records 50
1 Low 0.1	temporary delay for update to customer data. 1	design flaw in software program causes customer data to be inaccessible 5	Storm impacts servers causing outage for long duration of customer records. 10

Possible methods to mitigate the identified threats and dangers to vulnerabilities outlined in the risk matrix. Audits or code reviews according to (Sachedina, 2019) done to mitigate this impacting customer availability of information in real-time for the database of Real Estate Wealth Network. To avoid temporary server outages which make customer's Personal Identifiable Information or PII inaccessible. The company should have a backup server or use the cloud as a failover in the event their server needs maintenance. To avoid falling victim to attacks of known vulnerabilities the cyber security team should use IBM Guardium Vulnerability Assessment software scans (IBM Guardium Vulnerability Assessment, 2024). This will help identify security issues in databases and make sure the security posture of Real Estate Wealth Network is suited for production environments (IBM Guardium Vulnerability Assessment, 2024). This will help for known vulnerabilities by giving recommendations (IBM Guardium Vulnerability Assessment, 2024) of how to secure it before production environment. It will also help for unknown vulnerabilities and provide the best way to mitigate those so Real Estate Wealth network does everything possible from a security standpoint before public use of the database.

incident response protocols

The incident response protocols to implement for Real Estate Wealth Network would be in case of a ransomware attack. The company should start by isolating infected computer systems (Clarke, 2023). Then activate backup computers so that employees can still work, while the cybersecurity team works to mitigate the threat and vulnerabilities. The cybersecurity team needs to work to identify where the vulnerabilities on the computer are that lead to the incident (Clarke, 2023). The employee who identified the issue should say what he or she did before the incident occurred, giving clear communication to the cyber security team, so that they can mitigate the threat faster (Clarke, 2023). Cyber security team should report to law enforcement of the attack, as this is a legal obligation (Clarke, 2023) to customer’s privacy and data protection regulations. Cyber security will sanitize all effected computer systems (Clarke, 2023). The cyber security team will then check with antivirus software for any ransomware on the computer (Clarke, 2023). If no sign of ransomware is found the cyber security team can then reset passwords (Clarke, 2023) and enable two factor authentication. Customers will be notified immediately by email and physical mail so that they are notified about the attack, so that they can change their bank accounts and passwords as well. After computers have been wiped, passwords have been reset and two factor authentication has been reset, computers can then be restored with trusted backups from the company (Clarke, 2023). The cyber security team will make a report of lessons learned from the incident and how to prevent the incident in the future (Clarke, 2023). Also, where resources would be allocated internally within the company to help defenses against a ransomware attack (Clarke, 2023). Systems will be checked for software updates and patches (Clarke, 2023) to decrease the attack surface of systems. Employees will be educated (Clarke, 2023) on how to avoid clicking untrusted emails and avoiding suspicious emails that could lead to an attack.

Justify the incident response protocols

This incidence response is justified by protecting all phases of the company. As the company is taking preventive measures by educating employees, implementing software updates and patches (Clarke, 2023). The company is also detecting and responding to the threat by determining impacted systems, determining what happened and examining logs (Clarke, 2023). The company is communicating and reporting the incident by being transparent with their customers about what information was breached and how it was breached (Clarke, 2023). Also, Real Estate Wealth Network is reporting this issue by mail and email to make sure the message gets out to everyone. They are also reporting to legal authorities about the incident (Clarke, 2023). The Real Estate Wealth Network is containing this threat by removing all affected systems away from unaffected systems, so the ransomware doesn't spread (Clarke, 2023). The next step for the company is eradication which involves resetting password (Clarke, 2023) or multifactor authentication, sanitizing and removing the ransomware attack, and using antivirus software to make sure it is removed before installing backups (Clarke, 2023). Real Estate Wealth Network is addressing identified threats and vulnerabilities by making sure they know what resources to allocate to help prevent attacks in the future. Restoration strategies for incident response are met by reinstalling trusted backups after wiping and removing the ransomware from the affected computers (Clarke, 2023). There is also a post-incident evaluation the cyber security team will fill out telling where the threat came from and how they mitigated the threat (Clarke, 2023).

disaster response protocols

Establishing good disaster response protocols for Real Estate Wealth Network would be first having backups to keep the company running during a disaster (Proof, 2024), while in the background the company can still mitigate the disaster. The best backup for Real Estate Wealth Network would be a cloud backup in this case (Proof, 2024). The next is having data protection so the company does not lose data in the event of a disaster. The company should have encrypted data (Proof, 2024) at rest by AES-256 bit as this is the top of the line. The next data protection is for data in motion which would be IPSec. The IPSec will help by keeping the data private so hackers cannot see it (Manimit Haldar, 2023). Also, the IPSec should be used with a VPN to enhance security by adding encrypted tunnels to ensure data is confidential (Manimit Haldar, 2023). Using strict content control of data internally to help prevent unauthorized content (Proof,

2024) can be done using RBAC. Assigning employees privileges based only on their roles within the company. The most important part of Real Estate Wealth Network's disaster response protocols should be a SIEM. This tool can help support and facilitate collection of data, analyzing data, and response and remediation processes and procedures according to (IRS, 2024). This will help maintain coordination within the cyber security team by seeing the activity on the Real Estate Wealth Network's network (IRS, 2024). Taking legal action after a disaster in the case of a massive data breach and reporting it to individuals will help keep the company from having a bad reputation and help their customers know when to change their passwords.

Justify the disaster response protocols

The justification for the disaster response protocols is correct for the organization by covering all aspects of data information. As the company will protect their customer's data (Proof, 2024) first by AES when data is at rest and when in motion, they will use IPSec with a VPN to keep data confidential and ensure integrity (Manimit Haldar, 2023). Data will be backed up in the cloud for files and a backup server in the event of a disaster. The company must meet legal obligations, so they are not at fault. The company does this by sending an email or letter of data breach with what information has been leaked and when it was leaked. The company is not losing any revenue from this disaster as they have met their legal obligations and have kept their customers' data safe and secure, while keeping their services online. The company is also using SIEM tool to help keep track of Real Estate Wealth Network's network activity to help prevent the next attack (IRS, 2024), while keeping data customer PII safe.

access control protocols

Real Estate Wealth Network should use Role Based Access Control or (RBAC) for access control protocols. As this access control protocol will allow users to operate without experiencing a denial of service. This is due to having a structured approach to permissions allowing easy access (Imperva, 2022) even during high traffic on Real Estate Wealth Network. This also allows for managing large groups permissions with ease (Imperva, 2022). If an attack is successful, it will only affect permissions that are assigned to the role preventing a full range attack on Real Estate Wealth Network according to (Imperva, 2022).

Justify your access control protocols

By using RBAC the company is reducing the attack surface to insider threat, as privileges are only assigned to the role the employee has within the company. Also, helping to prevent denial of service attacks during high traffic as this access control protocol uses structure to assign privileges to certain roles (Imperva, 2022). Real Estate Wealth Network can manage their resources better for each department by only giving them access to what they need to do their daily tasks (Imperva, 2022). If an attack is successful, the attacker would only have access to resources associated with that role (Imperva, 2022). This helps information assurance as there are strict privileges regarding who has access to those resources and why (Imperva, 2022) within the company. An example of information assurance is to only allow permissions to a writer to edit, delete, and read, while the reader only gets the permission to read the article (Imperva, 2022).

method for maintaining the information assurance plan

The best way to maintain information assurance is to have employee awareness training (SDI, 2020). Run audits, security assessments of the company, and update security systems regularly (SDI, 2020). Having a password polices how long you can keep your password before you must change it. Have meetings to discuss with the cyber security team the most possible vulnerabilities (SDI, 2020) to the company and how to mitigate that. Making sure to comply with legal requirements if there is a data breach. If a company does not comply, they are open to heavy fines, loss of customer trust, and revenue loss. The cyber security team should always monitor the network with SIEM to watch out for attacks on Real Estate Wealth Network's network.

Justify your maintenance plan

By always auditing the system to keep up with latest vulnerabilities (SDI, 2020). Any security problems that have been missed, or any requirements such as forgetting to install encryption to customer PII, the company can decrease the odds of missing this, helping information assurance. By continually updating software and patching systems regularly (SDI, 2020) you help minus threats and vulnerabilities on the computers Real Estate Wealth Network uses. Actively watching the network for activity can help the cyber security to react and respond faster to an attack helping keep customer PII safe faster and prevent a possible data breach. Complying with legal requirements helps the company be trusted by customers, gain more customers, not pay fines, and stay on top of keeping customer PII confidential. Finally, having normal meetings about vulnerabilities and how to mitigate them (SDI, 2020) gives the company's employees more of a cyber security mindset helping them make better decisions. Also, having awareness training (SDI, 2020) for how to mitigate the most common threats like phishing emails, can help your company not be exposed to an attack and keep customer information safer overall.

Summarize the need for an information assurance plan

The need for information assurance is to adhere to protecting data using confidentiality, integrity, and availability. One example of an organization using confidentiality in their information insurance plan is encryption Advanced Encryption Standard or AES. An example of using information assurance for integrity is Role-Based Access Control or RBAC as this gives strict access to resources by roles within the company, controlling who can view and modify data. An example of information assurance for availability is the company using cloud as a backup for their servers. In the case of an incident or disaster taking place that makes the company's servers go from online to offline, they will still remain online by using the cloud as a trusted backup service. To adhere to legal considerations, if the company breached and data is stolen, they will report two ways to customers to inform them of a data breach. The company will send by physical mail to customers' mailbox and by email to the customer's email. The company is adhering to the law to report an incident as soon as they have proof of a data leak. This protects them from fines, loss of customer trust, and revenue loss. Having incident response protocols in place to help with responding to a potential threat such as monitoring logs, updating software to fix bugs and patches, educating employees of how to respond to an incident, resetting passwords and more.

Defend the key elements of your information assurance plan

In the event of an incident authorities should be contacted to help find the culprit. The IT team will help by sending emails out to customers about the data breach. The IT team will also be in charge of finding logs long side the cybersecurity team. The cyber security team will investigate monitoring the network to see if the attack is still happening and how much data the attack has gotten. The cyber security team will also be getting rid of the attack while monitoring it. So, if the attack is ransomware, they will be removing it by antivirus software and wiping all data from the computer. This is all being done in quarantine environment. Next, the IT team will be getting a new computer for the employees who got the ransomware attack and installing backup organization data to it so that employees can get back to working their role within the company. After wiping the infected computer, the company will check for any more signs of attacks on the computer by using antivirus software that will search for ransomware. After this the new computer for the employees that got infected will be resetting their computers with the help of the rest of the IT team. After the attack is over and the data of the organization is gone the cyber security team, IT team, and the rest of the employees will be given a post-incident evaluation of what happened, how it happened, how they responded, steps taken, and what can be done to stop this type of threat of happening in the future. This post-incident evaluation will be read only by Cameron Dunlap, the leader of the organization and founder. There will be meetings held after with the IT team and cybersecurity team, to adjust resources for the company to defend against the ransomware attack better in the future.

References

Kosling, K. (2024, January 10). Data Breaches and Cyber Attacks in the USA in December 2023 – 1,613,496,782 Records Breached. IT Governance USA Blog. https://www.itgovernanceusa.com/blog/data-breaches-and-cyber-attacks-in-the-usa-in-december-2023-1613496782-records-breached

Information Assurance (IA): Defined & Explored | Unitrends. (2022, March 17). Unitrends. https://www.unitrends.com/blog/information-assurance/

Atlan. (2023, September 27). 7 Data Integrity Best Practices You Need to Know. Atlan.com. https://atlan.com/data-integrity-best-practices/

The 5 Pillars of Information Assurance | Norwich University - Online. (n.d.). Online.norwich.edu. https://online.norwich.edu/5-pillars-information-assurance

Fowler, J. (2023, December 26). 1.5 billion records leaked in Real Estate Wealth Network data breach. Security Info Watch. https://www.securityinfowatch.com/cybersecurity/article/53081265/15-billion-records-leaked-in-real-estate-wealth-network-data-breach

v-amallick. (2023). What is Azure Backup? - Azure Backup. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/backup/backup-overview

ZoomInfo: B2B Database | Business Leads & Company Contacts. (2025). ZoomInfo. https://www.zoominfo.com

Eide, N. (2024, July 11). What does your CEO need to know about cybersecurity? Cybersecurity Dive. https://www.cybersecuritydive.com/news/ceo-cyber-security-strategy-CISO/721102/

The CEO’s Role in Cybersecurity: A Vital Component of Organizational Defense - CYPFER. (2023, November 27). Cypfer.com. https://cypfer.com/the-ceos-role-in-cybersecurity-a-vital-component-of-organizational-defense/

William & Mary. (2023, July 24). The Importance of Ethics and Professional Standards in the Accounting Industry. William & Mary. https://online.mason.wm.edu/blog/the-importance-of-ethics-and-professional-standards-in-the-accounting-industry

Gomez, A. (2024, April 25). Cybersecurity Ethics: Everything You Need To Know. Www.ollusa.edu. https://www.ollusa.edu/blog/cybersecurity-ethics.html

Chin, K. (2023, August 21). Cybersecurity and Social Responsibility: Ethical Considerations | UpGuard. Www.upguard.com; UpGuard. https://www.upguard.com/blog/cybersecurity-ethics

SentinelOne. (2024, September 6). What is Information Assurance? Benefits & Challenges. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-information-assurance/

The Top 5 Cyber Threats Facing Businesses Today. (2025). Www.pentestpeople.com. https://www.pentestpeople.com/blog-posts/the-top-5-cyber-threats-facing-businesses-today

Sophos. (2024). Threat Actors Explained: Motivations and Capabilities. SOPHOS. https://www.sophos.com/en-us/cybersecurity-explained/threat-actors

Fowler, J. (2023, December 26). 1.5 billion records leaked in Real Estate Wealth Network data breach. Security Info Watch.

https://www.securityinfowatch.com/cybersecurity/article/53081265/15-billion-records-leaked-in-real-estate-wealth-network-data-breach

CISA. (2024). Teach Employees to Avoid Phishing | CISA. Www.cisa.gov. https://www.cisa.gov/secure-our-world/teach-employees-avoid-phishing

Securing User Passwords: Hashing vs. Encrypting – Preventing the Unpreventable | QwietAI. (2023, August 29). Qwiet.ai. https://qwiet.ai/securing-user-passwords-hashing-vs-encrypting/

Kime, C. (2023, May 16). How to prevent SQL injection attacks. ESecurityPlanet. https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks/

Protect yourself from malware - Google Ads Help. (2025). Support.google.com. https://support.google.com/google-ads/answer/2375413?hl=en#zippy=%2Cuse-antivirus-software

Parker, C. (2019, August 28). 7 Ways To Protect Your Computer From Malware. WhatIsMyIPAddress. https://whatismyipaddress.com/protection-from-malware#google_vignette

Sachedina, F. (2019, December 2). Quality Begins With Code: 10 Ways to Reduce Software Bugs. Simple Programmer. https://simpleprogrammer.com/reduce-software-bugs-quality-code/

IBM Guardium Vulnerability Assessment. (2024, October 22). Ibm.com. https://www.ibm.com/products/guardium-vulnerability-assessment?utm_content=SRCWW&p1=Search&p4=43700081185950380&p5=p&p9=58700008820167337&gad_source=1&gclid=CjwKCAiAzPy8BhBoEiwAbnM9O7hf3eBwSSeuJ0h9quDoBt76b7YE3HJGlri6HA_6UGj2fetlw9AZAxoC3nwQAvD_BwE&gclsrc=aw.ds

Clarke, C. (2023, August 2). 6 Step Ransomware Response Plan | Veeam. Veeam Software Official Blog. https://www.veeam.com/blog/ransomware-response-plan.html

Manimit Haldar (2023, February 5). What is the best encryption strategy for protecting your data? | Encryption Consulting. https://www.encryptionconsulting.com/what-is-the-best-encryption-strategy-for-protecting-your-data/

IRS. (2024, Aug 20). "Security Information and Event Management (SIEM) Systems | Internal Revenue

Service."*Www.irs.gov*, 20 Aug. 2024, www.irs.gov/privacy-disclosure/security-information-and event-management-siem-systems.

Proof. (2024). How Businesses Can Create a Cybersecurity Disaster Recovery Plan. Proof.com. https://www.proof.com/blog/how-businesses-can-create-a-cybersecurity-disaster-recovery-plan-lc

Imperva. (2022). What is role-based access control | RBAC vs ACL & ABAC. Learning Center. https://www.imperva.com/learn/data-security/role-based-access-control-rbac/

SDI. (2020, November 13). 5 Principles of Information Assurance. Sentient Digital, Inc. https://sdi.ai/blog/5-principles-of-information-assurance/