**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**

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.

**References**

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>