**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.

**References**

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/>