The National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) is structured around five key functions: identifying, protecting, detecting, responding, and recovering. It would ensure TechFite establishes a foundation for secure operations such as information security and risk management. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have created two standards that work together: ISO/IEC 27001 and 27002. Specifically, ISO/IEC 27001 outlines best practices for implementing, maintaining, and improving an information security management system. TechFite lacks oversight mechanisms, leaving sensitive data and proprietary information at risk. By adopting this standard, TechFite can enforce stronger internal controls and reduce the risk of unethical practices.

The justification for this reasoning is to allow TechFite to ensure compliance and to reduce organizational risk. Frameworks like NIST and ISO/IEC 27001 help ensure compliance with legal and industry standards. Without these ethical guidelines and frameworks, TechFite risks financial losses, legal action, and reputational damage.

One behavior that fostered unethical practices is by Carl Jaspers, the head of the Applications Division, who signed NDAs with the potential clients Orange Leaf and Union City Electronic Ventures but failed to ensure compliance with them. Both of those companies' proprietary data was shared with their competitors, violating the NDAs. This unethical behavior eroded client trust and exposed TechFite to potential legal action.

One omission of behavior that fostered unethical practices was the Applications Division failing to deactivate accounts for employees who no longer worked at TechFite and allowing these accounts to remain active and be used for unethical purposes. These accounts were used to conduct unauthorized activities such as intelligence gathering activities against various companies. The failure to regularly audit and deactivate unused accounts enabled them to be used for unethical behaviors.

Some factors that led to lax ethical behavior at TechFite include an absence of organizational policies and lack of rules regulating personal relationships between staff in oversight positions, Carl Jaspers and Nadia Johnson being the focus of this issue, creating a conflict of interest. Employees in the BI unit were granted full administrative rights across systems without restrictions which violates the principle of least privilege. Division leadership failed to set a standard of ethical behavior, which fostered an environment where unethical practices were normalized.

Two security policies that could have reduced criminal activity and deterred negligent acts are a Data Segregation Policy and an Account Management and Oversight Policy. The Data segregation policy would have implemented a Chinese wall methodology to separate data between clients and internal units, this would have prevented proprietary information from being disseminated to competitors. The Account Management and Oversight Policy could have enforced privilege escalation tracking and routine auditing, disabled inactive accounts, and prevented their unauthorized use, this would have prevented rogue accounts from running unchecked. A combination of these policies could have drastically reduced the amount of criminal activity and negligent acts.

There are several key components to a Security Awareness Training and Education (SATE) program, to list a few, there are cybersecurity basics, which teaches employees foundational principles such as the CIA triad of data (Confidentiality, Integrity, and Availability). There is incident reporting and response, which provides guidelines on how to identify and report suspicious behavior and potential breaches. Ethical data handling is another key component to help train staff on the proper handling of sensitive data and proprietary information. There is also access management which educates employees about the importance of the principle of least privilege, proper account usage, and addresses the risk of privilege escalation and the abuse of administrative rights. Lastly, there is social media and relationship ethics, these components highlight the risk of sharing company related data on social media and provides guidelines on maintaining professional boundaries and avoiding conflicts of interest.

The SATE program can be effectively communicated to TechFite employees in several ways, there can be workshops and seminars, where in-house training sessions can be setup for employees to engage in interactive learning sessions. Online training modules can also be effective with online learning platforms that contain quizzes and simulations to reinforce security concepts. Lastly, regular updates, which can vary anywhere from daily to monthly, through internal newsletters and emails can be used to share cybersecurity information and reminders.

Some justifications of the SATE programs relevance to mitigating undesirable behaviors is it can prevent the misuse of proprietary information and addresses unethical competitive intelligence practices. These are just two examples of what TechFite struggles with, however improving account management practices and enhancing awareness of professional boundaries are also more justifications for the SATE program and are just extra areas that TechFite struggles with.

SUMMARY TO SENIOR MANAGEMENT:

TechFite faces several ethical issues ranging from the misuse of proprietary client information, lack of internal oversight, conflicts of interest, fraudulent practices, and unethical competitive intelligence activities. Starting with the first issue listed, client data from the companies Orange Leaf and Union City Electronic ventures was inappropriately accessed and used to benefit their competitors, who are clients of TechFite, violating the NDAs. Second, the absence of strong internal auditing allowed the mismanagement of accounts to persist unchecked. Third, personal relationships between oversight staff compromised professional accountability and facilitated misconduct. Fourth, the creation of shell companies exposes TechFite to regulatory and reputational risks by inflating sales figures and highlighting financial misrepresentation. Lastly, unauthorized network scanning and dumpster diving violated professional ethical standards, leading to potential legal consequences.

There are several proposed mitigation strategies for TechFite to use: policy implementation, comprehensive training, strengthened oversight mechanisms, and ethical leadership. First, data segregation and account management policies must be enforced. Implement a Chinese wall methodology and use access controls to protect sensitive client data. Second, launch a SATE program to educate employees on ethical practices, cybersecurity basics, and professional boundaries. Third, conduct routine audits to detect irregularities in data handling and account usage and limit opportunities for unethical behavior by introducing a separation of duties policy and removing unrestricted administrative rights. Lastly, promote a culture of integrity by establishing accountability at all leadership levels, and regulate relationships that may create conflicts of interest and compromise oversight.