The Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA) each specifically relate to the criminal activity described in the case study of TechFite.

For the CFAA there is unauthorized access to computer systems, escalation of privileges on unauthorized accounts, use of hacking tools such as the Metasploit Tool, and the misuse of proprietary information from the companies Orange Leaf and Union City Electronic Ventures.

For the ECPA, there is potential violations in intercepting and accessing sensitive information with the use of the Metasploit tool, there is unauthorized access to the questionnaires from Orange Leaf and Union City Electronic Ventures since the questionnaires were intended for internal use only, and the information being sent to competitors was unauthorized. TechFite had a lack of data loss prevention (DLP) measures and safeguards which allowed the Business Intelligence (BI) unit employees to misuse internal systems.

Three laws and regulations that apply in the justification of legal action based on negligence are the General Data Protection Regulation, a breach of Nondisclosure Agreements, and the Sarbanes-Oxley Act.

The General Data Protection Regulation (GDPR) aims to protect sensitive information and data of EU citizen and companies. International clients and partners would bring the GDPR under consideration if any data from an EU company was involved, even if TechFite is a US based company. TechFite failed to protect the proprietary information that was in the questionnaires from Orange Leaf and Union City Electronic Ventures. The absence of any DLP mechanisms and data segregation policies displays a failure to meet basic data protection requirements.

Nondisclosure agreements (NDA) are meant to protect sensitive and confidential data shared between parties. The Applications Division of TechFite breached these NDAs with Orange Leaf and Union City Electronic Ventures by sharing this sensitive information with competitors. Both Orange Leaf and Union City Electronic Ventures could seek legal action against TechFite for damages caused by the disclosure of this sensitive information.

The Sarbanes-Oxley Act (SOX) states that publicly traded companies, which TechFite is, are to maintain accurate financial records and prevent fraudulent financial reporting and calls for transparency and accountability in financial operations. This case study of TechFite shows some instances of SOX violations. Shell companies such as Bebop Software, Dazzling Comet Software, and FGH Research Group are used as fake dummy clients to inflate sales figures in the Applications Division. There is an escalation of privileges and unauthorized access to financial data within the BI unit. There is also a lack of segregation of duties which could allow an individual to create inaccurate financial records.

Two instances in which duty of due care was lacking at TechFite are the lack of safeguards for the sensitive/proprietary data of their clients and the lack of internal oversight. TechFite did not enforce any policies to separate client information such as a Chinese Wall Methodology and

there were no checks to prevent the sharing of this sensitive data with competitors. Accounts created for former employees were not deactivated and were still being misused for unauthorized activities.

The Sarbanes-Oxley Act (SOX) applies to TechFites case study for a few reasons, already mentioned. TechFite is receiving payments from several shell companies, all coming from the same bank, Freeworkers' Pennsylvania Bank, which indicates falsified revenue. There is a lack of oversight in the BI unit's financial practices which allowed them to have unauthorized access to financial records and compromise the integrity of the records.

There is evidence in this case study of alleged criminal activity. The criminal actors would be Carl Jaspers, head of the Applications Division, who oversaw questionable business practices and orchestrated misuse of accounts and privileges. There is also Sarah Miller, Megan Rogers, and Jack Hudson who all conducted unauthorized penetration testing and competitive intelligence gathering. Sarah Miller conducted unauthorized scanning of external company networks. Megan Rogers and Jack Hudson used penetration tools like Metasploit to do unauthorized intelligence gathering activities. The victims of this criminal activity would very clearly be Orange Leaf Software and Union City Electronic Ventures, both companies had proprietary information disseminated and misused.

There are several reasons the existing cybersecurity policies and procedures failed to prevent the alleged criminal activity. The BI unit was granted full administrative privileges across all systems, violating the principle of least privilege. Lack of DLP policies lead to unauthorized sharing of client information. Improper use of security tools such as the Metasploit tool was misused for gathering intelligence on competitors and scanning external networks.

There is evidence in this case study of alleged acts of negligence. The negligent parties include Carl Jaspers, who did not enforce principles such as least privilege and separation of duties. The BI unit analysts Sarah Miller, Megan Rogers, and Jack Hudson all failed to set and enforce ethical boundaries in their intelligence gathering activities. The Chief Information Security Officer (CISO) neglected to perform detailed internal audits and relied on blanket summaries claiming, "no irregularities." The victims of this negligence would again be Orange Leaf and Union City Electronic Ventures because they lost control of their sensitive data. Other victims include many of the TechFite employees whose sensitive information could be accessed by the BI unit. The BI unit has access to legal, human resources, and finance departments.

There are several reasons the existing policies and procedures failed to prevent negligent practices. The absence of a Chinese wall methodology allowed sensitive data from the affected clients to be accessed and misused by the BI unit. There were inadequate internal audits, the BI unit was limited to blanket statements with no specific audits. There were also weak policies on ethical boundaries when it came to employee relationships, specifically the relationship between Carl Jaspers and Nadia Johnson which undermined objective oversight of BI unit activities.

SUMMARY TO SENIOR MANAGEMENT:

TechFite is currently facing legal and regulatory challenges from non-compliance with US federal laws such as the Computer Fraud and Abuse Act (CFAA), Electronic Communications Privacy Act (ECPA), Sarbanes-Oxley Act (SOX), as well as breaches of Nondisclosure agreements (NDAs), and potentially even the EUs General Data Protection Regulation (GDPR) if any EU citizens or companies were affected. Unauthorized activities, financial irregularities, and the misuse of proprietary client information all highlight critical lapses in oversight, data protection, and ethical governance. These compliance issues expose TechFite to reputational harm, regulatory penalties, and even lawsuits, which could severely impact future business opportunities and risks shareholder value. TechFite must begin enforcing strict access controls, have independent audits conducted, add strong data protection policies, and deal with financial irregularities. A heavy focus on enhancing ethical guidelines and finally rebuilding clients trust is essential for TechFites long term success. The company can mitigate its current risks, strengthen its compliance position, and rebuild its reputation by taking these corrective actions.