# TechFite Case Study

### Background of Company:

TechFite is traded on NASDAQ and has approximately 1,000 employees. The company’s core business involves consulting with and advising Internet organizations on promoting and monetizing their online business ventures. Most of the company operates legally and ethically with good internal financial oversight. However, its Applications Division has recently been reported in the news media for undertaking some disturbing business practices. This division consults with start-ups on launching new applications and apps online.

### Assignment:

The chairperson of the board commissioned me, John Jackson, to investigate the IT and business practices of the Applications Division. I hold an MS in network security and am qualified as a Certified Information Systems Security Professional (CISSP), and I have 12 years’ experience in cybersecurity. In addition, the chairperson has consented to allow Maria Harrison to assist me. She is a private investigator who holds an MS in criminal justice and has 15 years’ experience in corporate investigations.

### Findings:

I interviewed Noah Stevenson, the chief executive officer (CEO) of Orange Leaf Software LLC, whose company was cited in recent news articles about the Applications Division. Stevenson indicated his company had meetings with the division’s representatives to possibly hire TechFite for consulting services. Prior to divulging any technical details, Applications Division head Carl Jaspers executed a nondisclosure agreement (NDA) with Orange Leaf. As a part of the preconsulting process, Orange Leaf’s CEO, chief technology officer (CTO), and lead software engineer completed questionnaires that included technical information about Orange Leaf’s products. Ultimately, Orange Leaf decided not to hire TechFite’s Applications Division for a variety of business reasons. Months later, Noah Stevenson was disturbed to find out a competitor was launching some products very similar to those of Orange Leaf.

A similar scenario occurred in an interview with Ana Capperson, CTO for Union City Electronic Ventures. She described the same fact pattern as Orange Leaf’s. That is, after this company decided not to use the Applications Division, proprietary information eventually found its way into the hands of a competitor.

Both potential clients provided copies of the questionnaires to me, and they do contain information that could be of value to a competitor. Copies of the NDAs executed by Carl Jaspers were also provided. A check of the Applications Division’s customer database revealed that the two competitors identified by Stevenson and Capperson are existing clients of TechFite’s Applications Division.

The Applications Division has a Business Intelligence (BI) Unit, which gathers publicly available information about companies in the Internet sector to benefit the division’s marketing of its services and to aid clients. Such an operation is legal and is common in the industry. However, I was interested in what kind of oversight the unit had to prevent the abuses alleged by Stevenson and Capperson.

IT Security Analyst Nadia Johnson of TechFite’s Applications Division reviewed reports for the chief information security officer (CISO) and revealed the organization had performed a credible job of protecting the division’s network against external threats. Vulnerability scanning, penetration testing, and UTM (unified threat management) were all in place. Documentation on internal oversight, especially of the BI Unit, however, was lacking. There were blanket summaries that no irregularities were found in internal operations. What was missing were specific discussions of auditing users’ accounts, checking for escalation of privilege, enforcing data loss prevention (DLP) on sensitive documents, and surveilling internal network traffic and activity.

Also disturbing was the lack of coverage on the critical issue of safeguarding sensitive and proprietary information belonging to existing clients, potential clients, and previous clients. No plan was evident in keeping different clients’ information segregated from each other and employing a Chinese wall methodology. (No general policy at TechFite requires such a methodology.) Within the BI Unit, the principles of least privilege and separation of duties were not enforced. Every workstation and computer had full administrative rights. In the marketing/sales unit associated with the BI Unit, the same person can create customers (clients), report sales, and post sales on the system. In fact, there is no IT segmentation or separation between the two units—data or applications. Each unit has full visibility and access into the other.

Additionally, background checks into IT Security Analyst Nadia Johnson raised some questions. First, Jaspers (head of Applications Division) regularly gives Johnson’s boss, the CISO, positive recommendations about Johnson during annual reviews and she gets ample raises. Johnson’s social media posts have photos and text documenting her frequently attending social events hosted by Jaspers. A recent post even thanks Jaspers for a gift on Johnson’s birthday. (Currently, no policy at TechFite bars social relationships between IT Security staff and those they conduct oversight on.)

We audited the client list database for the division (an action never done by Johnson). Most of the clients are well-known companies in the Internet arena. We researched the businesses we did not immediately recognize online. All but three came up as legitimate companies in the Internet field. These three organizations—Bebop Software of Alberta, FGH Research Group of Indiana, and Dazzling Comet Software of Florida—had no real Internet presence. Further investigation revealed they were all incorporated in Nevada. The registered agent for all three corporations was Yu Lee, who attended graduate school with Carl Jaspers at Stanford University.

We crosschecked with the TechFite Financial Unit and found all three companies pay for services at TechFite with checks drawn from the same bank: Freeworkers’ Pennsylvania Bank, NA in Scranton, Pennsylvania. Given this pattern, these three clients may not be actual, real clients but may simply be conduits for moving money into TechFite’s sales figures for the division. Since TechFite does not do business with Freeworkers and does not have accounts there, the bank may provide an off-the-books method of making payments elsewhere.

In auditing IT user accounts for the division, we found most to be created in the normal manner for TechFite. (A manager requests that an employee receives account access with the appropriate privileges.) However, two accounts were created solely upon the request of Carl Jaspers. The employees assigned to the accounts have not worked for TechFite for over a year. However, the accounts are in constant use. Emails associated with these accounts are addressed to parties who are not clients of TechFite. Some of the emails refer to intelligence-gathering activities against various companies, including references to “dumpster diving” and “trash surveillance.”

All TechFite employees at the time of hire sign a release permitting company surveillance of any electronic communications using TechFite equipment. Accordingly, we remotely deployed Encase Endpoint Investigator on BI Unit computers and digital devices. We discovered the Metasploit tool (used for system penetration) on multiple machines. In addition, evidence on the hard drives indicates recent penetration and scanning activity into IP addresses for several Internet-based companies.

Among the BI Unit employees, Sarah Miller, the senior analyst, has the most traffic in scanning other companies’ networks. Analysts Megan Rogers and Jack Hudson take direction from Miller in doing similar efforts. Hudson also coordinates efforts by third parties to gather intelligence through surveilling and through mining companies’ trash. Furthermore, social media research on Hudson revealed his membership in the Strategic and Competitive Intelligence Professionals (SCIP), which has a very strong code of ethics against covert and illegal BI activities.

Finally, and very disturbing, the BI Unit, through its dummy user accounts, has gained access to other groups and units within TechFite outside its own division, without proper authorization. Escalation of privilege has occurred on these accounts to permit access to legal, human resources (HR), and finance departments. Networking monitoring logs reflect regular traffic between the BI Unit and these other departments to examine financial and executive documents.

[End of report]