CFAA and ECPA

1. **CFAA**: The business intelligence unit gained access to employee groups outside of their unit without proper permission. Privilege escalation was used to gain access to legal, HR, and financial documents. This constitutes intentional access without authorization and is a violation of CFAA.
2. **ECPA**: Two accounts were created by Carl Jaspers. The employees associated with the accounts haven't worked for the company in over a year, but they are in constant use. Emails sent through the accounts are addressed to non clients of TechFite. This is an unauthorized transmission of information using TechFite systems and justifies legal action under ECPA.

Three Laws

1. **CFAA**: Nadia Johnson failed to properly audit user accounts which allowed the business intelligence division to continue accessing unauthorized accounts. Documentation on internal oversight was found lacking. This unauthorized access to accounts violates CFAA as the privilege escalation implies that this was an intentional access to information that the BI unit wasn't authorized for.
2. **ECPA**: TechFite displayed negligence in their user account creation process and related policies. The fact that an employee was able to create multiple unauthorized accounts for terminated employees shows this. The accounts were then used for unauthorized communication. This violates ECPA and justifies legal action.
3. **SOX**: The SOX act was violated when TechFite failed to implement proper information security policies to protect their financial information. This justifies legal action because SOX requires that financial information has safeguards in place.

Duty of Due Care

1. Reports from the Nadia Johnson implied proper procedure was being followed. However, documentation regarding these procedures was found lacking. There were blanket statements about procedures, and missing discussions on basic auditing practices. This allowed the business intelligence division to conduct illegal activities with no company intervention.
2. There was no plan or safeguards in place to protect proprietary information. Separation of duty and least privilege were not enforced. Every workstation had full admin rights. No separation between marketing and business intelligence divisions was implemented. This allowed employees to create and access unauthorized accounts. The unauthorized accounts were then used for unauthorized communications and access to financial information.

SOX

- The SOX act was violated when fake customer accounts were created to bolster sales figures. This bolstering of the sales data misrepresents the company to investors. Creating a situation where TechFite may seem more appealing to invest in.
- SOX's stance on auditing is that auditors need to be independent and accountable. The internal auditor at TechFite failed to properly audit employees, nor did they create proper policies regarding auditing.

Criminal Evidence, Activity, actors and Victims

1. There was a clear violation of the non-disclosure agreement between Applications Division Head Carl Jaspers and Orange Leaf Software LLC's Noah Stevenson. The competitors of Orange Leaf Software obtained proprietary information through TechFite and are confirmed customers in the TechFite customer database. The questionnaires conducted by Carl Jaspers contained the proprietary information that was obtained by the competitors.
2. A violation of CFAA occurred by accessing information to unauthorized company computers. Business Intelligence unit employees Sarah Miller, Jack Hudson, and Megan Rogers are the employees in violation of the law. The victim in this case is the TechFite computers that were accessed unlawfully.

Cybersecurity Policies & procedures

1. A Chinese Wall approach was not implemented. A procedure for implementing network segmentation between departments is crucial. This created an environment for potential abuse. In this case it may have prevented the unauthorized access to company resources by the BI unit.
2. There was no separation of duties policy implemented. This allowed Carl Jasper to access and disseminate information that he wouldn't have, had separation of duties been in place. In this case separating the storage of proprietary information and the employee that conducts interviewing processes would prevent or minimize the ability to violate the nondisclosure agreement.

Evidence of Negligent Activity, actors and Victims

1. The reviewed reports for proper procedure were approved though they were missing vital information. Nadia Johnson approved the reviews and vouched for the validity of the reports. TechFite was the victim of the negligence as their operations and legal compliance are under question.
2. There was a lack of training of safeguarding information. Permissions to access confidential information were extended to everyone. TechFite committed this negligence by failing to implement policies that would prevent this type of activity. Orange Leaf and Union City Electronic Ventures are victims of the negligent behavior.

Cybersecurity Policies & procedures

1. A policy for employee relationships could potentially address the negligent behavior of Nadia Johnson. Implementing proper auditing procedures for employees in relationships could have prevented the negligent behavior.
2. A Chinese wall policy was not implemented. Separating access to important or confidential information needs to be in place. The negligent behavior led to employees being able to access sensitive information without authorization. Orange Leaf's and Union City Electronic Ventures competitors would not have access to this information otherwise.

Legal Compliance Summary

Law #1: CFAA

Compliance Status: Not Compliant

Contributing Factors: The company is not compliant as employees of the company accessed information they were not authorized to. A violation of CFAA occurred when Carl Jaspers escalated his privileges without authorization with the intent to access and use that information.

Legal Compliance Summary

Law #2: ECPA

Compliance Status: Not Compliant

Contributing Factors: The company is not compliant with the law. Employees of the company illegally communicated through email with accounts that were not authorized. This is what violated the ECPA law.

Legal Compliance Summary

Law #3: SOX

Compliance Status: Not Compliant

Contributing Factors: Policies to safeguard financial information were not properly implemented. This led to illegal and negligent behavior within the organization. SOX requires financial information to be properly safeguarded and the companies' disregard of proper security practices constitute a violation of the law.