Relevant Ethical Guidelines Related to Information Security

- A guideline used by ISSA states that maintaining appropriate confidentiality of sensitive information encountered during professional activities is a priority.
- This applies to the case because Carl Jaspers failed to implement policies to maintain confidentiality of information within the BI unit therefore, he was in violation of this ethical guideline.

- An ethical guideline used by ISSA states to perform all professional activities in accordance with all applicable laws.
- This applies to the case because Sarah Miller the senior analyst of the BI unit directed the scanning of other companies' networks using TechFite computers. This was unauthorized access and could constitute a violation of CFAA.

Unethical Practices

1. The BI unit scanned other companies' networks using TechFite computers. This fostered an unethical practice of breaking federal communications laws. The BI unit employees Sarah Miller, Megan Rogers, and Jack Hudson are the perpetrators of the unethical practice.

2. Carl Jaspers failed to properly implement information confidentiality. No Chinese wall policy or separation of duties were implemented nor was the principle of least privilege. This fostered an unethical practice of accessing unauthorized information within and outside of the organization.

Factors

1. One factor from the case study that led to lax behavior is that there was no training on safeguarding sensitive or proprietary information. This led to an instance of lax behavior on the part of Sarah Miller who conducted and instructed other employees to conduct unauthorized scanning of networks. Had proper training been in place it may have prevented the BI unit employees from engaging in the illegal scanning.
2. Another factor that led to lax behavior from the CISO was the relationship between Carl Jaspers and Nadia Johnson. This led to the CISO getting inaccurate and bolstered reports from the BI unit on account of Nadia Johnson. This later led to Carl Jasper's abusing his power as head of the department to steal proprietary information.

InfoSec Policies

1. Implementing a Chinese wall policy may have stopped the unauthorized access of information by the BI unit. A policy separating the BI unit from the information that was abused would help prevent said unauthorized access. This would also decrease the chances that intellectual property laws would be broken by curious or ill-intentioned employees.
2. Adding separation of duties to company policy would decrease the likelihood of IP law being broken. Carl Jaspers and other members of the BI unit were able to access proprietary information because this policy was not implemented. This is a standard infosec policy that prevents any one employee from having too much power over the system.

SATE Components

1. Business intelligence unit employees will be required to participate in the SATE training. It is important for employees that deal with protected computers and financial information to know exactly what is expected of them when it comes to the protection of important data.
2. The repercussions for non-compliance could include further training or depending on the severity of the situation termination of employment. Adding increased training for employees with a history of non-compliance will help to dissuade that behavior. If non-compliance has risen to the point that training will no longer mitigate these behaviors termination would be the next step.

SATE Program Communication

1. The SATE program will be introduced through email. The CISO will send out SATE program requirements through said email and will further require employees to verify they have received the information. If verification isn't received it may call for further communications like a desk visit or phone call. Refusal to acknowledge the SATE program requirements could call for termination of that employee.

SATE Program Justification

1. The BI unit scanned other companies' networks without authorization. Implementing proper information security training into the SATE program will go a long way to teach employees the proper and improper ways to access information. The applicable laws and consequences should be discussed. Tactics to maintain confidentiality of information should also be taught.
2. Carl Jaspers failed to properly implement information confidentiality. Increased training to employees with higher levels of permissions should be included in the SATE program. Increased permissions increase the likelihood that someone will be able to misuse or access information. Carl Jaspers should have been aware that accessing information that he didn't explicitly have permission for is a violation of federal law. Furthermore, Carl Jaspers should have been able to recognize the illegal behavior of employees under his responsibility.

C. Ethical Issues and Mitigation

1. The first ethical issue we discussed breaking federal communications laws. Proper oversight on employee activity needs to be implemented. This would decrease the likelihood that illegal activity goes unnoticed. In this case the BI unit employees in violation of CFAA could have been caught sooner and handled internally before any federal laws were broken.
2. Then we discussed accessing unauthorized information within and outside of the organization. Implementing a least privilege policy here is essential. No such policy was in place and that allowed employees access to information they should not have. Implementing training on safeguarding confidentiality would also increase the likelihood that employees are following the right procedures.