

INFOBRIEF

Security awareness and training program

Empowering business and building trust through security awareness and training

At Ciena, security is a strategic pillar that drives innovation and builds trust within our organization. Our comprehensive security awareness and training program equips our teams to recognize and mitigate evolving cyber threats, ensuring seamless and confident operations. This document outlines how our program aligns with industry-leading standards, emphasizing proactive engagement and robust practices that strengthen our internal resilience.

Ciena's security awareness strategy is based on industry-recognized frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and ISO 27001. These frameworks guide our comprehensive practices for identifying, detecting, responding to, and protecting and recovering from potential threats. This structured approach underpins our commitment to continual improvement and transparency, ensuring our internal stakeholders have confidence in our security posture.

Core training initiatives

Our training modules are designed to meet the specific needs of our workforce, focusing on:

- Adhering to internal security policies and industry best practices
- Identifying and preventing social engineering and phishing attacks
- Safeguarding data privacy and ensuring secure communication practices
- Learning incident reporting protocols

Training is delivered through interactive workshops, e-learning, and real-time updates. This reinforces our security-first approach and empowers employees to uphold high security standards.

Adapting to evolving threats

With the fast-paced evolution of cybersecurity risks, Ciena's security awareness team continually updates training content based on emerging threats and insights from global threat intelligence. This ensures that all employees, especially those in key roles, are prepared to anticipate and mitigate sophisticated attacks, fortifying the organization's resilience.

Simulated threat exercises

To maintain readiness, Ciena regularly conducts simulated threat exercises that replicate real-world cyber risks such as phishing attempts and malware scenarios. These exercises reinforce employee training and readiness, supporting Ciena's goal of maintaining a secure and prepared workforce.

Commitment to transparency and trust

Transparency is integral to Ciena's security strategy. We provide detailed metrics and regular security briefings to internal stakeholders, enhancing accountability and fostering a culture of security awareness. This transparency helps ensure our teams are informed, vigilant, and confident in their roles.

Preparing for the future

Security is a fundamental commitment at Ciena that drives innovation, trust, and operational confidence. By aligning with global standards and fostering an adaptive approach, we create a secure environment for our internal operations. Our dedication to training, transparency, and continual improvement underscores our proactive approach to building a resilient and trusted organization.

As the cybersecurity landscape evolves, Ciena remains committed to refining our security practices and fostering a culture that anticipates and adapts to new challenges. This approach ensures our teams are empowered and equipped to operate securely, reinforcing trust and supporting long-term organizational success.