Cybersecurity & Infrastructure Resilience Report

Overview

The Cybersecurity & Infrastructure Resilience Report outlines Spike's comprehensive approach to safeguarding its operations through robust cybersecurity practices and infrastructure resilience strategies. The report details alignment with ISO 27001 and NIST frameworks, a layered defense model across IT, OT, and supply chain systems, and rigorous incident response readiness procedures. It also highlights resilience measures such as redundant systems, predictive maintenance, and AI-driven analytics to ensure operational continuity and stakeholder trust. Overall, the report reinforces Spike's commitment to governance, innovation, and the secure, reliable operation of its manufacturing and supply chain environments

Copyright © Spike

Table of Contents

01 Overview

02 Table of Contents

03 Introduction

03 Cyber Defense Framework

03 Certifications and Compliance

04 Layered Security Strategies

- » Perimeter Protection
- » Network Security
- » Endpoint Security
- » Application Security
- » Data Security
- » Human Layer

05 Incident Response Readiness

06 Infrastructure Resilience Planning

06 Conclusion

Introduction

Spike recognizes the critical importance of cybersecurity and infrastructure resilience in maintaining operational reliability, stakeholder trust, and long-term innovation. In line with the company's sustainability and governance commitments, this report outlines our cyber defense framework, security certifications, incident response readiness, and infrastructure resilience strategies.

Cyber Defense Framework

Our cybersecurity framework aligns with industry-leading standards and best practices to safeguard data, systems, and operations across our global footprint. Key elements of the framework include:

- Alignment with NIST Cybersecurity Framework (CSF) and ISO 27001 principles.
- Multi-layered defense-in-depth security controls across IT and operational technology (OT).
- Continuous monitoring of network traffic, user activity, and system vulnerabilities.
- Proactive risk assessments and penetration testing to identify and mitigate threats.
- Employee training programs focused on phishing, social engineering, and data security awareness.

Certifications & Compliance

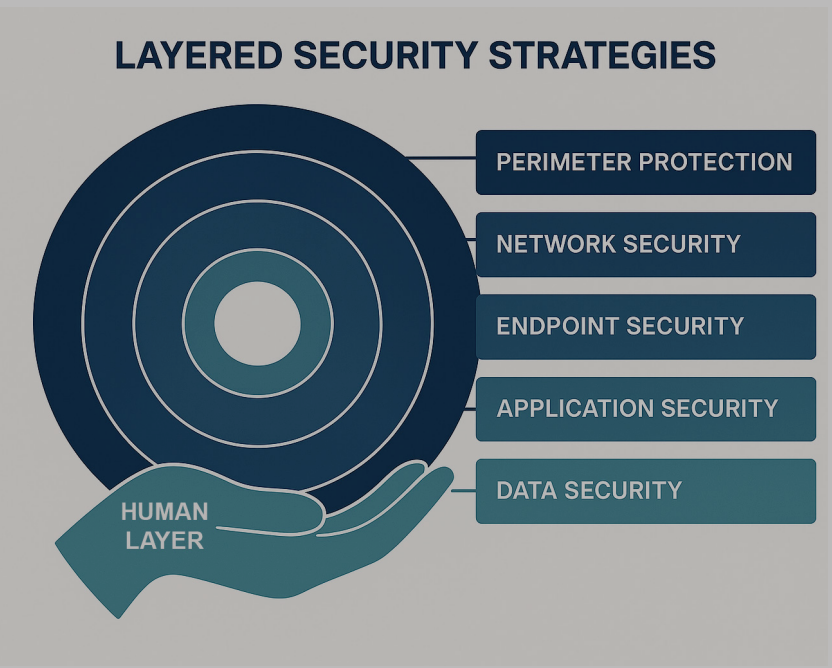
Spike maintains rigorous certifications and compliance standards, complementing our ISO 9001 and ISO 14001 certifications already in place. Cybersecurity and operational resilience are supported by adherence to international standards and frameworks such as:

- I**SO 27001** (Information Security Management Systems).
- **NIST** Cybersecurity Framework alignment.
- **UL and ETL** certifications reinforcing product safety and secure design.
- **ANSI/IEEE** standards for reliability and electrical safety.
- **Compliance with Build America, Buy America** (BABA) Act to ensure secure and traceable supply chains.

Layered Security Strategies

Spike employs a layered security model designed to prevent, detect, and respond to threats across IT, OT, and supply chain environments. This defense-in-depth approach integrates people, processes, and technology:

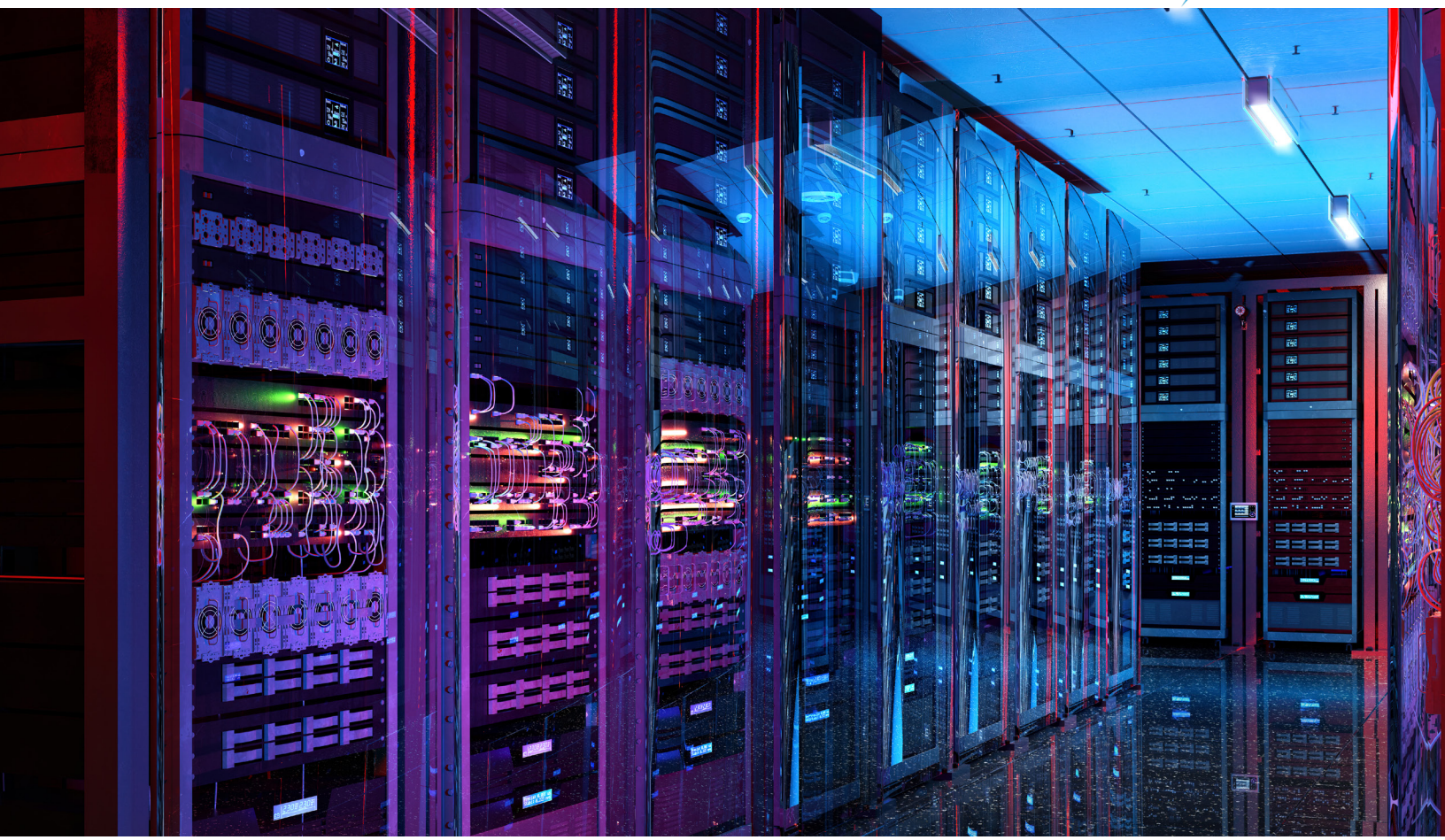
- **Perimeter Protection:** Firewalls, intrusion prevention systems, and secure remote access.
- **Network Security:** Segmentation of IT and OT networks, zero-trust authentication.
- **Endpoint Security:** Advanced malware protection, patch management, and access controls.
- **Application Security:** Secure coding practices, vulnerability scanning, and testing.
- **Data Security:** Encryption in transit and at rest, secure backups, and data loss prevention tools.
- **Human Layer:** Cyber awareness training and ongoing compliance education.



Incident Response Readiness

Spike has developed a comprehensive Incident Response Plan (IRP) to ensure quick containment, eradication, and recovery in the event of a cyber incident. Our readiness approach includes:

- Dedicated Cybersecurity Response Team trained to handle diverse threat scenarios.
- Predefined escalation procedures to ensure rapid decision-making.
- Regular tabletop exercises and simulations to test readiness.
- Integration with external law enforcement and industry partners.
- Communication protocols for timely and transparent stakeholder updates.
- Completely segregated internal drives which are not accessible remotely.



Infrastructure Resilience Planning

To protect critical infrastructure systems, Spike employs resilience strategies across its manufacturing and supply chain operations. Key measures include:

- Redundant power and communications systems to ensure continuity of operations.
- Disaster recovery and business continuity planning with regularly tested backups.
- Predictive maintenance programs to minimize downtime and equipment failures.
- Secure supply chain management, including supplier audits and critical component stockpiling.
- Adoption of AI-driven predictive analytics to anticipate disruptions and enhance reliability.

Conclusion

Spike's cybersecurity and resilience initiatives reflect our unwavering commitment to operational reliability, governance, and innovation. By aligning with leading standards, employing layered defenses, and maintaining robust incident response and resilience planning, we ensure the continued protection of our people, operations, and stakeholders

Copyright © Spike