Adtran

Cybersecurity Framework

February 2024

Contents

Definitions

- **AEO (Authorized Economic Operator):** A certification recognizing businesses that meet strict customs compliance and supply chain security standards, facilitating smoother international trade. Led by the World Customs Organization (WCO)
- **Bundesamt für Sicherheit in der Informationstechnik (BSI):** The BSI is responsible for managing computer and communication security for the German government and is involved in developing IT security guidelines and best practices for businesses and private users.
- **Chief Information Security Officer (CISO):** A high-ranking executive charged with overseeing and ensuring the security of an organization's information and data.
- **CTPAT (Customs-Trade Partnership Against Terrorism):** A voluntary program where businesses in the trade community collaborate with customs authorities to enhance security along the supply chain, reducing terrorism-related risks. Led by U.S. Customs and Border Protection (CBP).
- **Cybersecurity:** The practice of defending digital systems, networks, and programs from cyber-attacks, theft, and damage.
- **Employee:** All individuals employed by Adtran around the world.
- **ENISA (European Union Agency for Cybersecurity)**: ENISA assists EU Member States, EU institutions, and businesses in enhancing their cybersecurity capabilities.
- **GDPR**: General Data Protection Regulation is an EU law effective from May 25, 2018, focused on data protection and privacy for EU residents.
- **Information:** Data gathered in a specific context that allows for conclusions to be drawn.
- **Information Security:** The safeguarding of information to ensure its confidentiality, integrity, and availability.
- **Information Security Management (ISM):** This is a management program designed to meet the international standard ISO27001 which focuses specifically on information security.
- **Information Security Management System (ISMS):** A comprehensive approach to managing an organization's sensitive information to keep it secure, encompassing both processes and policies.
- **Information Security Program:** A compilation of policies, processes, standards, awareness training, and initiatives that uphold information security guidelines.
- **ISO 27001**: An international standard outlining a risk management framework for the protection and management of sensitive information.
- **NCSC (National Cyber Security Centre):** The UK's authority on cybersecurity, providing guidance, support, and advice on protecting IT infrastructures from cyber threats. Part of GCHQ, it aims to make the UK the safest place to live and work online.
- **NIST (National Institute of Standards and Technology):** A U.S. federal agency that develops technology, metrics, and standards to drive innovation and economic competitiveness, including guidelines for cybersecurity and privacy.
- **Risk Management:** The identification, assessment, and mitigation of risks threatening an organization's assets and earnings.
- **Security Incident:** Any suspected, attempted, successful, or imminent threat that affects the security of information, including vulnerabilities, faults, disturbances, disruptions, or interruptions.

Version: 4.0, Febraury 2024
Author: Raymond Harris
Validity: This guideline applies to all Adtran entities and all Adtran functions worldwide.

Our company

Adtran is a company founded on innovation and driven to help our customers succeed. Our technology is the foundation of a shared digital future and empowers networks across the globe. We're continually developing breakthrough hardware and software products that lead the networking industry in performance, speed, and security and create new business opportunities. Together, we're building a truly secure, connected, and sustainable future.

Introduction

Adtran is a leading provider of networking and communications solutions that enable secure and reliable connectivity for businesses and consumers. As a trusted partner in the digital economy, Adtran is committed to protecting its ecosystem from cyber threats and ensuring the privacy and security of its data and systems. This document summarizes the key aspects of Adtran's Cybersecurity program, which covers the following areas:

- Strategy
- Cybersecurity Governance and Communications
- Detection and Monitoring
- Incident Response and Recovery
- Data Protection and Privacy
- Vendor and Third-Party Risk Management
- Business Continuity
- Cybersecurity Awareness and Training

The management board at Adtran is dedicated to integrating information security practices throughout all pertinent product lifecycles and business operations, with a continuous commitment to their maintenance and enhancement. The cybersecurity framework presented here outlines the foundational principles managing our approach to information security. These principles draw extensively from relevant legal requirements, as well as standards and frameworks like ISO 27001, ISO 27034-1, BSI, NCSC, ENISA, and the NIST Cybersecurity Framework, reflecting our strong commitment to information security which is further reinforced by our code of conduct.

Strategy

As an ISO 27001 certified organization, Adtran's high-level information security strategy is centered around the development, implementation, maintenance, and continuous improvement of our Information Security Management System (ISMS). This strategy is built on several key pillars:

Awareness
Compliance
Leadership
Risk MGT
Security Controls
Continuous Improvement
Internal Audits

- **Risk Management:** We prioritize identifying, analyzing, and addressing information security risks through a comprehensive risk assessment process. Our approach includes implementing tailored security controls to mitigate identified risks to an acceptable level, in alignment with our risk appetite.

- **Security Controls Implementation:** Based on our risk assessment outcomes, we deploy appropriate security measures from the ISO 27001 Annex A controls, customized to our specific needs and the evolving cybersecurity landscape. These controls span various domains, including access control, operations security, and incident management.

- **Compliance:** Adtran ensures adherence to all relevant legal, regulatory, and contractual information security obligations, thereby safeguarding against compliance risks.

- **Continuous Improvement:** Our strategy embraces continual enhancement of the ISMS, leveraging regular audits, management reviews, and the latest cybersecurity best practices to evolve our security posture.

- **Leadership Commitment:** The effectiveness of our ISMS is underpinned by strong management support, evidenced by resource allocation, policy setting, and strategic direction.

- **Awareness and Training:** Recognizing the critical role of our workforce in maintaining security, we invest in ongoing awareness and training programs to keep our team informed and vigilant.

- **Internal Audits:** Regular internal audits of our ISMS are essential for assessing its effectiveness and ensuring it meets ISO 27001 standards, driving improvements where necessary.

Through this strategy, Adtran demonstrates a robust commitment to securing our information assets, ensuring the confidentiality, integrity, and availability of data, and maintaining trust with our customers, partners, and stakeholders.

Cybersecurity Governance and Communications

Adtran has implemented a comprehensive governance framework for cybersecurity, delineating clear roles and responsibilities for both leadership and staff. This framework is supported by detailed policies and procedures that ensure data protection and regulate acceptable use, aligning with industry standards and legal requirements.

Central to Adtran's cybersecurity governance is the Chief Information Security Officer (CISO), who ensures continuous, transparent communication with all stakeholders. This includes providing quarterly updates to the Board of Directors, monthly briefings to the Management Team, and weekly summaries to the CEO and Executive Management, keeping them abreast of cybersecurity statuses, challenges, and advancements. Beyond executive communication, the CISO and the Security Team engage the wider organization through Town Halls and departmental meetings, fostering a culture of cybersecurity awareness and shared responsibility.

This structured approach to governance and communication, spearheaded by the CISO and supported by a team of certified security professionals, underscores Adtran's commitment to a strong cybersecurity posture. Regular reviews by the Audit Committee and direct accountability to the CEO and Board of Directors ensure that cybersecurity remains a top priority, with sufficient resources dedicated to its initiatives. The organization's layered communication strategy enhances understanding and implementation of cybersecurity practices across Adtran, reinforcing the collective effort to safeguard information assets.

Secure Product Lifecycle Management

Secure Product Lifecycle Management within the Adtran Cybersecurity Framework is aimed at safeguarding Adtran products and their users. This is achieved by incorporating security measures and industry-leading practices throughout the product development process at Adtran. The Information Security Manager (ISM) sets forth secure development standards, principles, and strategies for managing threats, vulnerabilities, and risks across all stages of a product's lifecycle. The ISM and the dedicated ISM Team play a crucial role in supporting the engineering and development teams at Adtran. They help identify and tackle security issues in products during development and address security concerns for products already in the market. The goal is to seamlessly integrate security into the development and customer support processes for all Adtran products. For detailed information on Adtran's approach to Secure Product Lifecycle Management, please visit the Product Security section on our website or follow this link: Product Security at Adtran.

Detection and Monitoring

Our Detection and Monitoring strategy at Adtran is a core pillar designed to ensure the ongoing integrity and security of our digital assets. By integrating advanced technological solutions and expert support, we aim to identify and respond to threats swiftly, minimizing potential impacts on our operations. Below is an overview of our approach, which encompasses a range of tools and services tailored to meet the dynamic challenges of today's cyber threat landscape.

- Intrusion Prevention System (IPS)
    - Our IPS is strategically deployed to analyze network traffic for malicious activities and known threat signatures. This proactive measure is crucial for preventing unauthorized access and attacks before they can infiltrate our systems, ensuring a first line of defense that is both robust and responsive.

- Endpoint Detection and Response (EDR)

  - At the heart of our endpoint security is the EDR system, which monitors and collects data from networked endpoints to detect, investigate, and respond to potential cybersecurity threats. This allows us to not only react to immediate threats but also to perform advanced analysis and forensics to prevent future incidents.

- Email Security
  - To combat email-based threats, our Email Security strategy employs advanced filtering, anti-phishing, anti-malware, and data leak prevention technologies. These tools scrutinize incoming and outgoing emails to detect and block threats such as phishing attempts, malicious attachments, and unauthorized data exfiltration. By implementing stringent email security measures, we protect the Adtran organization from the increasingly sophisticated email threats that organizations face today, ensuring the integrity and security of our communication channels.

- Security Information and Event Management (SIEM)
  - Our SIEM solution aggregates and analyzes log data from across our IT environment, providing real-time visibility into security alerts generated by applications and network hardware. This comprehensive oversight enables our cybersecurity team to detect complex threats quickly and coordinate an effective response.

- 24/7/365 External Security Operations Center (SOC) Support
  - Recognizing the need for constant vigilance, we have partnered with an external SOC that provides round-the-clock monitoring and support. This collaboration extends our capabilities to detect and respond to cybersecurity incidents, ensuring expert eyes are always on our systems, every day of the year.

- Cloud Security
  - As we leverage cloud services for enhanced agility and scalability, securing this environment is paramount. Our approach includes advanced cloud security measures to protect data, applications, and infrastructure hosted on the cloud. This includes continuous monitoring for abnormal activities and unauthorized access attempts, ensuring our cloud footprint remains secure.

- Ransomware Detection
  - Given the rise of ransomware attacks, we have implemented specialized detection mechanisms designed to identify and isolate ransomware behaviors before they can lock or encrypt critical data. This proactive stance allows us to thwart ransomware attacks, safeguarding our valuable digital assets.

- Vulnerability Management
  - We employ a thorough vulnerability management program that regularly scans and assesses both internal and public-facing systems for vulnerabilities. This program ensures timely identification and remediation of security weaknesses, reducing the attack surface and fortifying our defenses against external and internal threats.

- Next-Generation Firewall (NGFW) Architecture
  - Our NGFW architecture is the backbone of our network security, offering more than traditional firewall capabilities. It integrates application awareness, intrusion detection/prevention, and advanced threat intelligence to provide a multi-layered defense against sophisticated cyber threats.

Our Detection and Monitoring strategy is built on the foundation of advanced technology and expert support to create a resilient and responsive cybersecurity posture. By integrating IPS, EDR, email security, SIEM, external SOC support, cloud security measures, vulnerability management, ransomware detection, and NGFW architecture, we ensure comprehensive protection against a wide array of cyber threats. This approach not only defends our digital assets but also supports the continuity and success of our operations in the face of evolving cyber challenges.

Incident Response and Recovery

Adtran's Incident Response and Recovery strategy details a robust framework designed to adeptly manage and reduce the effects of security incidents, guaranteeing adherence to legal and regulatory standards. The strategy's primary aim is to diminish impacts on operations, reputation, and assets, alongside ensuring efficient communication with essential stakeholders. It includes a systematic approach for gauging the significant impact of all incidents. Additionally, Adtran has taken proactive steps by revising its Board of Directors charter and updating its incident response plan and workflows. These updates are aimed at aligning with the SEC's requirements for public companies to report material cybersecurity incidents after determining their materiality, ensuring comprehensive compliance and readiness.

Adtran's incident response plan is a structured process designed to manage and mitigate security incidents effectively. It begins with **preparation**, where training and readiness activities are conducted to ensure the organization is equipped to handle potential incidents. Following this, incidents are **identified** and analyzed through logging, reviewing, and classifying to understand their nature and severity. The next step is **containment**, where affected systems are isolated to prevent further damage. This is followed by **eradication**, where identified threats are removed from the system. The **recovery** phase then focuses on restoring and reinforcing systems with improved controls to prevent future breaches based on thorough investigation and identification. After an incident is resolved, a **lessons learned** review is conducted to improve future response efforts. Essential to this process is the documentation and revision aspect, where detailed records of incidents, actions taken, lessons learned, and recommendations for system improvements are maintained. Additionally, a revision history is kept for tracking changes to the plan, including the authors and reasons for these adjustments, ensuring the incident response plan remains effective and up to date.

Data Protection and Privacy

Adtran's commitment to data protection and privacy is encapsulated in its comprehensive approach, ensuring adherence to GDPR and establishing rigorous data protection controls across the organization. Key internal groups, including a dedicated Data Privacy Committee chaired by the CIO, work in unison to enforce privacy principles and manage personal data responsibly, in line with contractual and legal obligations. Adtran prioritizes the security of personal data through extensive risk assessments and the implementation of strong safeguards, promptly addressing data breaches in compliance with regulatory requirements. The company also maintains strict protocols for international data transfers and actively cooperates with regulatory bodies to uphold data privacy standards.

For a detailed overview of our practices and your rights regarding data privacy, please refer to our public-facing Privacy Policy here. This policy further solidifies Adtran's pledge to protect personal information and foster trust with all stakeholders.

Vendor and Third-Party Risk Management

Adtran adopts a holistic approach to vendor and third-party risk management, focusing on thoroughly assessing and managing the security posture of its vendors to ensure robust protection against potential risks. This responsibility is overseen by the Board of Directors, which ensures comprehensive risk management across the company. Further supporting this endeavor, the Audit Committee plays a critical role in coordinating the Board's oversight of Adtran's risk management program. This includes overseeing the methodology through which management evaluates, prioritizes, and addresses the company's significant risks, with a keen focus on major financial, data security, and enterprise challenges.

The vendor management process at Adtran is meticulously designed to cover various aspects, such as software release development and management, defect management, Engineering Change Request management, Product Change Notification management, and Manufacture Discontinuance/End of Life management. This multifaceted approach aims to foster successful business partnerships through a tightly managed vendor engagement strategy, emphasizing the importance of maintaining high standards throughout the product development lifecycle and operational processes.

To further enhance our vendor risk assessment capabilities, Adtran also employs external security posture vulnerability assessment platforms specifically for evaluating our top strategic vendors. This addition to our risk management strategy allows for a more in-depth analysis of our vendors' security frameworks, ensuring they meet Adtran's stringent security requirements. By leveraging these external platforms, Adtran ensures a comprehensive evaluation of potential security vulnerabilities, reinforcing our commitment to maintaining a secure and resilient operational environment.

Incorporating CTPAT (Customs-Trade Partnership Against Terrorism) and AEO (Authorized Economic Operator) certifications into our third-party risk management strategy has strengthened our approach. Adtran has maintained these certifications for multiple years, demonstrating our consistent commitment to secure and efficient international supply chain practices. These certifications reflect our ongoing efforts to manage and mitigate risks in global trade and vendor relations, aligning our operations with international security and operational standards. The maintenance of CTPAT and AEO certifications supports our risk management practices by ensuring compliance and adding a level of trust and security for our partners and customers.

Business Continuity

Our approach to Business Continuity and Disaster Recovery (DR) is rooted in our commitment to resilience and robust backup and recovery operations. Recognizing the critical importance of maintaining uninterrupted business operations, we have developed comprehensive plans that ensure our readiness to respond effectively to any disruption, whether due to cyber incidents, natural disasters, or other unforeseen events.

- Resilience by Design
  - Our infrastructure and operations are designed with resilience at their core, minimizing the risk of service interruptions and ensuring the stability of our systems. This involves redundant systems, failover capabilities, and a distributed network architecture that can withstand various failure modes without compromising service delivery.

- Comprehensive Backup and Recovery Operations
  - We implement rigorous backup and recovery procedures, ensuring that all critical data, applications, and systems are regularly backed up and can be quickly restored in the event of data loss or system failure. Our backup strategy encompasses multiple layers of protection, including on-site and off-site backups, as well as the use of cloud-based backup solutions for added flexibility and scalability.

- ISO 22301 Certification for Business Continuity
  - Demonstrating our commitment to best practices in business continuity, Adtran holds ISO 22301 certification. This international standard specifies requirements for setting up and managing an effective Business Continuity Management System (BCMS), highlighting our capability to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

- Regular Testing and Improvement

- To ensure the effectiveness of our Business Continuity and DR plans, we conduct regular testing and drills, simulating various scenarios to identify potential weaknesses and areas for improvement. These exercises enable us to refine our response strategies, update our plans based on lessons learned, and stay prepared for a wide range of contingencies.

Cybersecurity Awareness and Training

Adtran understands that effective cybersecurity hinges on the collective vigilance and involvement of all stakeholders, emphasizing the critical role of ongoing education and engagement in our defense strategy. To this end, Adtran commits to comprehensive training initiatives for our employees, including mandatory annual awareness training courses that cover key cybersecurity principles and defensive practices. Additionally, we proactively assess our readiness through quarterly phishing and ransomware testing, simulating real-world attack scenarios to evaluate and enhance our collective response capabilities. Beyond our internal efforts, Adtran extends its educational outreach to customers and partners, offering awareness programs that share vital best practices and guidelines for safeguarding digital assets. These multifaceted training and testing activities are pivotal in fostering a security-conscious culture and ensuring that everyone within our ecosystem is equipped to contribute to our shared cybersecurity objectives.

Summary

This document offers a detailed summary of Adtran's Cybersecurity program, showcasing the company's commitment to cybersecurity through a proactive security posture. It outlines our strategic focus on risk management, compliance, and ongoing improvement, backed by robust governance and leadership support. Furthermore, it underscores the significance of teamwork and knowledge exchange in preserving a secure digital landscape.

Our comprehensive strategy ensures the protection of our information assets while fostering trust within our stakeholder community, highlighting our firm dedication to cybersecurity. Adtran encourages stakeholders to collaborate in our pursuit of maintaining high cybersecurity standards for everyone's advantage.

Sincerely,

2/27/2024

X Ray Harris

Raymond Harris
CIO/CISO
Signed by: Verified Email: raymond.harris@adtran.com

R. Harris
CIO/CISO