National Institute of
Standards and Technology
U.S. Department of Commerce

CASE STUDIES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Observations from Industry

Palo Alto Networks, Inc.

INTERVIEWEES:
Jason Ledgerwood - VP Supply Chain Operations and Procurement
Brian Riggs - Sr. Director, Supply Base Management
Jim Sugg - Sr. Product Manager
Shae Trautwein - Supply Chain Risk and Compliance Manager

February 4, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.02042020-6

Jon Boyens
Celia Paulsen
Computer Security Division
Information Technology Laboratory

Nadya Bartol
Kris Winkler
James Gimbi
Boston Consulting Group

SERIES DESCRIPTION

The *Case Studies in Cyber Supply Chain Risk Management* series engaged with several companies that are mature in managing cyber supply chain risk. These case studies build on the Best Practices in Cyber Supply Chain Risk Management case studies originally published in 2015 with the goals of covering new organizations in new industries and bringing to light any changes in cyber supply chain risk management practices.

For information on NIST's Cyber Supply Chain Risk Management project, see https://csrc.nist.gov/projects/cyber-supply-chain-risk-management.

DISCLAIMER

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

Contents

Company Overview

Palo Alto Networks, Inc. (commonly known as Palo Alto Networks) is an American multinational cybersecurity company headquartered in Santa Clara, California. Palo Alto Networks is one of the world's leading producers of cybersecurity products, including next generation firewalls (NGFW), cloud-based security services, advanced endpoint protection, and threat intelligence. Cybersecurity products are an important enabler for public and private organizations, and Palo Alto Networks' offerings have been adopted by over 60,000 enterprise organizations in 150 countries.

Risk Profile

Security and data protection are inseparable from Palo Alto Networks' role as a cybersecurity product provider. Thousands of companies and governments around the world rely on these products to protect highly sensitive information. For Palo Alto Networks, cybersecurity and product integrity are an implicit corporate mandate.

Highlighted Practices in Cyber Supply Chain Management

- **End-to-end risk management.** All products are subject to Palo Alto Networks' end-to-end product security framework, which was designed to provide defense in depth for each stage of the product lifecycle.
- **Continuous improvement.** Cyber Supply Chain Risk Management (C-SCRM) processes must rapidly adapt to changes in the threat landscape. Palo Alto Networks' cross-functional security council rebalances the C-SCRM program's security priorities every six months.
- **Public-private partnerships**. Palo Alto Networks participates in multiple voluntary public-private partnerships, including the Department of Homeland Security's Information and Communications Technology Supply Chain Risk Management Task Force and the U.S. Customs and Border Protection's Customs-Trade Partnership Against Terrorism. These programs encourage Palo Alto Networks' suppliers and the broader security community to develop robust supply chain and cybersecurity practices.
- **Contract manufacturers simplify cyber supply chain risk management.** Managing thousands of supplier relationships is challenging for organizations at every maturity level. Palo Alto Networks leverages established contract manufacturers with demonstrably diligent cybersecurity and supplier risk management programs.

Organizational Approach to Supply Chain Risk and Cybersecurity

Given Palo Alto Networks' role as a cybersecurity vendor, the company is subject to intense scrutiny from potential customers and is a target for a variety of threat actors. Recognizing that a product security incident could have an enormous impact on customers, Palo Alto Networks considers cybersecurity and product integrity an implicit corporate mandate. All products are subject to the company's end-to-end product security framework (E2E Framework). The framework is designed to provide defense in depth for each stage of the product lifecycle—design, sourcing, manufacturing, fulfilment, and service. Each stage is independently evaluated to determine security risks, and domain experts select relevant public standards and best practices to target those risks. Selected standards include the Federal Information Processing Standards (FIPS)[i], Common Criteria[ii], and the United Kingdom's Commercial Product Assurance (CPA)[iii].

The E2E Framework is governed by the security council, which is composed of cross-functional senior management from product engineering, product line management, information security, product security, supply chain risk and compliance (SCRC), facility safety and security, and legal. Quarterly security council meetings direct the implementation schedule for individual contributors from each function. While framework-based planning is a cross-functional exercise, the resulting controls are ultimately owned and operated by each function.

The E2E Framework relies on strong control over each stage of the production process. Palo Alto Networks consolidates all product assembly, manufacturing, and shipping to a single contract manufacturer (CM) based in California to secure this control. Relationships with the CM, CM sub-suppliers, and other direct Palo Alto Networks suppliers are centrally managed by the SCRC team.

Palo Alto Networks is an active participant in the broader C-SCRM community. The company sponsors cybersecurity and SCRM industry conferences and is a member of the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force[iv]. The Task Force is a public-private partnership facilitated by the Department of Homeland Security, designed to examine the global ICT supply chain ecosystem and develop recommendations for industry and government.

Internally, Palo Alto Networks fosters a strong security culture. Role-based physical and logical controls ensure that only authorized individuals are able to access intellectual property, components, finished products, and customer information. This includes multiple layers of perimeter and internal physical security at all Palo Alto Networks and CM facilities. Cybersecurity training is widely available, and security is considered part of every employee's role.

Supplier Management

Key Aspects of Managing Supplier Relationships

Contractual requirements are the principal mechanism for setting a baseline foundation to manage cyber supply chain risks. During the onboarding process, new suppliers are subject to a detailed security assessment. These assessments are based on specific security council priorities, the NIST Cybersecurity Framework (NIST CSF)[v], International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 28001[vi], and other standards and best practices. The assessment ensures that all supplier employees receive security training and that the assessment team inspects the supplier's factory and warehouse facilities to confirm that unauthorized personnel cannot access Palo Alto Networks components. Suppliers must also demonstrate conformance to relevant requirements, such as FIPS, CPA, and the U.S. Customs and Border Protection's (CBP) Customs-Trade Partnership Against Terrorism (CTPAT) program.

CTPAT is the Department of Homeland Security's largest public-private partnership for supply chain risk management[vii]. The voluntary program grants Palo Alto Networks a low-risk customs designation for demonstrating compliance with a broad range of supply chain security assurances, including secure transit and storage, personnel controls, and IT security. To maintain this certification, Palo Alto Networks' logistics partners and suppliers must independently demonstrate to CBP that they meet all of the program's security requirements.

In addition to supplier onboarding and annual security assessments, suppliers are contractually obligated to disclose component vulnerabilities, data loss, and security incidents to Palo Alto Networks. This process provides the SCRC team a more complete view of the supplier's cybersecurity posture, including real-time alerts of a potential incident. Strategic suppliers must use Palo Alto Networks' cybersecurity products to provide confidence in the supplier's cyber incident detection and response capabilities.

Internally, formal interfaces with suppliers are strictly controlled. Release processes govern all initial designs and design changes before they may be released to Palo Alto Networks' manufacturing partners. This process requires multiple levels of cross-functional review to ensure unauthorized changes cannot occur to design documents, schematics, and bills of materials. All authorized changes are permanently documented and traceable to specific Palo Alto Networks employees. Intellectual property and other sensitive information may only be shared with suppliers over dedicated secure platforms.

Palo Alto Networks invests in the security posture of high-risk suppliers. The SCRC team proactively engages technical leadership at these companies to develop their internal cybersecurity and SCRM capabilities. Technical security personnel are made available to the supplier to clarify Palo Alto Networks' security requirements and inform maturity road maps. This engagement is often a two-way exchange as suppliers are able to share practices and insight from their other downstream partners.

Palo Alto Networks deliberately cultivates close relationships with suppliers of specialized components. Because of the security role of products such as NGFW, these suppliers work with Palo Alto Networks to deploy security fixes proactively. For instance, Palo Alto Networks works with hardware developers to rapidly implement any needed mitigations for hardware-level vulnerabilities before they are prepared for public release.

Measuring Supplier Risk

The supplier risk measurement process begins long before production. Risk assessments are performed early in the product development lifecycle to help determine the feasibility of product design decisions. Component requirements identified by engineering are evaluated by the SCRC team, which assesses potential suppliers to determine a risk score by evaluating dimensions including the relative sensitivity of the component, cybersecurity risks, the supplier's financial condition, availability of alternative sourcing, and compliance risks (e.g., Restriction of Hazardous Substances Directive[viii] obligations).

Palo Alto Networks operates a suite of commercial supply chain risk management products and internally developed utilities to track the risk presented by each supplier. This suite includes intelligence and news-mining subscription services to collect live information on acute cybersecurity threats, natural disasters, political unrest, and other disruptive events. These events are automatically mapped to potentially impacted components and suppliers, allowing the SCRC team to anticipate disruptions or compromised supply and prepare a response plan.

Quality Management and Continuous Improvement

Palo Alto Networks ensures consistent quality management and product security with a wide range of handling policies. All materials related to the production of Palo Alto Networks products must be stored in facilities with strict access controls and 24/7 physical and electronic monitoring. The CM is required to perform complete background, reference, and employment history checks for every candidate before they may access and work on Palo Alto Networks products. CM ICT networks are designed around well-established security standards, including the NIST CSF and ISO/IEC 27001[ix]. The CM features a dedicated cybersecurity team and is required to perform regular third-party assessments, including penetration testing and vulnerability assessments. Palo Alto Networks' products are not built or packaged for any particular customer. Rather, the CM prepares prepackaged inventory to satisfy sales forecasts and prevent would-be attackers from targeting specific customers during the production phase.

Palo Alto Networks provides functional testing infrastructure for all products to the CM. These platforms are designed in-house and perform software diagnostics to ensure product integrity. While the tests are performed by the CM, the testing infrastructure remains under Palo Alto Networks' control. Tested products are outfitted with tamper-evident packaging and shipping labels featuring unique product identifiers, such as part and serial numbers, to ensure that the products received by the customer were not compromised in transit. While Palo Alto Networks transfers delivery risk to the customer when the customer's selected courier takes possession of the product, all hardware products leverage software integrity checks to prevent software tampering during transit.

All returned customer storage drives are logically wiped according to U.S. Department of Defense (DOD) procedures to prevent unauthorized access to customer information from decommissioned devices. Scrapped drives are destroyed, and a certificate of destruction is available to customers upon request.

Continuous improvement is an embedded feature of the E2E Framework, ensuring that Palo Alto Networks adapts to changes in the threat landscape. While developing a holistic view of the entire cross-functional E2E Framework, visibility is a critical requirement to the continuous improvement process. The security council works with each function to capture a current state "snapshot" of their program and measure it against the implementation schedule. This progress is thoroughly documented, allowing the security council to track the development of the product's security program and identify potential blind spots or redundancies. The security council meets regularly for checkpoints to rebalance the program's security priorities accordingly.

Customers routinely request information about Palo Alto Networks' security and supply practices. While many customers request common copies of system and organizational control reports or simple questionnaires, some customers require unusual or specific information to engage cybersecurity vendors. The SCRC team carefully tracks the nature of each request to inform cybersecurity and supply chain risk management road maps.

Incident Response and Recovery

The SCRC is responsible for detecting and responding to potential security incidents across the supplier community. Aside from automated monitoring, the SCRC may receive incident reports directly from an affected supplier through their contractually defined reporting obligations. Palo Alto Networks also works with independent security researchers who identify potential security risks through their dedicated security disclosure service[x], conformant with the coordinated vulnerability disclosure process defined in ISO/IEC 29147:2018[xi].

All components involved in product assembly are individually traceable through serial numbers, lot codes, and date codes at every stage of production. This allows the SCRC team to trace any product security incident to a particular supplier or testing failure. Palo Alto Networks prefers to source components from multiple vendors whenever possible to mitigate the impact of supply disruptions and keep a buffer quantity of critical products in reserve. These buffers vary by component criticality and availability and may be adjusted to account for changing business forecasts, vendor stability issues, security events, or as part of a larger response to global events.

Confirmed incidents trigger the formal incident response plan (IRP). While the SCRC and the security operations center are responsible for handling incidents within their respective domains, they cooperate through the IRP when responding to incidents that impact both domains. Suppliers are contractually obligated to cooperate with Palo Alto Networks during an incident and are required to provide their internal incident response procedures during the onboarding process to more effectively manage incidents that affect both companies. The SCRC team runs regular, cross-functional tabletop exercises to identify any potential capability gaps in a controlled context. Tabletop exercises are simulations of dynamic incidents with stakeholders, including teams from Palo Alto Networks and critical suppliers.

Lessons Learned and Improvement Opportunities

The nature of Palo Alto Networks' cybersecurity offerings requires an enormous amount of complex risk management. Dependable cybersecurity products have to account for threats during every stage of the product lifecycle, from design through to service. Palo Alto Networks' thorough and holistic product security approach at each product development stage addresses unique challenges and uncovers potential vulnerabilities.

Palo Alto Networks recommends that organizations interested in maturing or developing C-SCRM programs consider the following tenets when designing their approach:

- The program should be end-to-end, featuring controls that cover every stage of the product lifecycle.
- The organization should implement compensating controls and practice defense in depth. Because each layer of defense adds friction to attacks, even basic controls may deter, slow, or prevent a broader compromise.
- Since no program has unlimited resources for security, organizations should invest in thoughtful and dynamic prioritization processes.
- The organization should foster a security-conscious culture and exercise basic process hygiene.

Because effective implementation of these tenants requires executive sponsorship, Palo Alto Networks recommends engaging cross-functional senior leadership early in the program design process.

References

[i] Federal Information Processing Standards Publications (FIPS PUBS), National Institute of Standards and Technology, https://www.nist.gov/itl/itl-publications/federal-information-processing-standards-fips, (retrieved September 26, 2019)

[ii] ISO/IEC 15408: Common Criteria, International Organization for Standardization, https://www.commoncriteriaportal.org/, (retrieved September 16, 2019)

[iii] Commercial Product Assurance, National Cyber Security Centre, https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa, (retrieved September 26, 2019)

[iv] DHS Announces ICT Supply Chain Risk Management Task Force Members, Department of Homeland Security, https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members, (retrieved September 24, 2019)

[v] Cybersecurity Framework, National Institute of Standards and Technology, https://www.nist.gov/cyberframework, (retrieved September 16, 2019)

[vi] ISO/IEC 28001: Best practices for implementing supply chain security, assessments and plans, International Organization for Standardization, https://www.iso.org/standard/45654.html, (retrieved September 26, 2019)

[vii] CTPAT: Customs Trade Partnership Against Terrorism, U.S. Customs and Border Protection, https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat, (retrieved September 16, 2019)

[viii] The RoHS Directive, European Commission, https://ec.europa.eu/environment/waste/rohs_eee/index_en.htm, (retrieved September 24, 2019)

[ix] ISO/IEC 27001: Information Security Management, https://www.iso.org/isoiec-27001-information-security.html, (retrieved September 24, 2019)

[x] Security Disclosure, Palo Alto Networks, https://paloaltonetworks.com/security-disclosure, (retrieved September 24, 2019)

[xi] ISO/IEC 29147: Information technology — Security techniques — Vulnerability disclosure, International Organization for Standardization, https://www.iso.org/standard/72311.html, (retrieved September 24, 2019)