PCI Security Standards Council

Cyber Supply Chain Risk Management

Navigating Vendor and Third-Party Relationships in PCI Compliance: Best Practices and Pitfalls

PCI Security Standards Council

Kapil Sharma

Assistant Director, Advisory, Ensign InfoSecurity (Asia Pacific) Pte. Ltd.

ENSIGN INFOSECURITY

Ensign InfoSecurity Company Introduction

Asia's largest pure play cybersecurity services company with **over 900 cybersecurity professionals**.

Our clients trust and rely on us to bring our collective capabilities and innovative solutions across **Consulting, Systems Integration, Managed Services** and **Labs** to deliver cyber excellence. We work with our clients to transform them into cyber-resilient leaders, helping them **Conquer the Unknown**.

1 Strategic Advisory

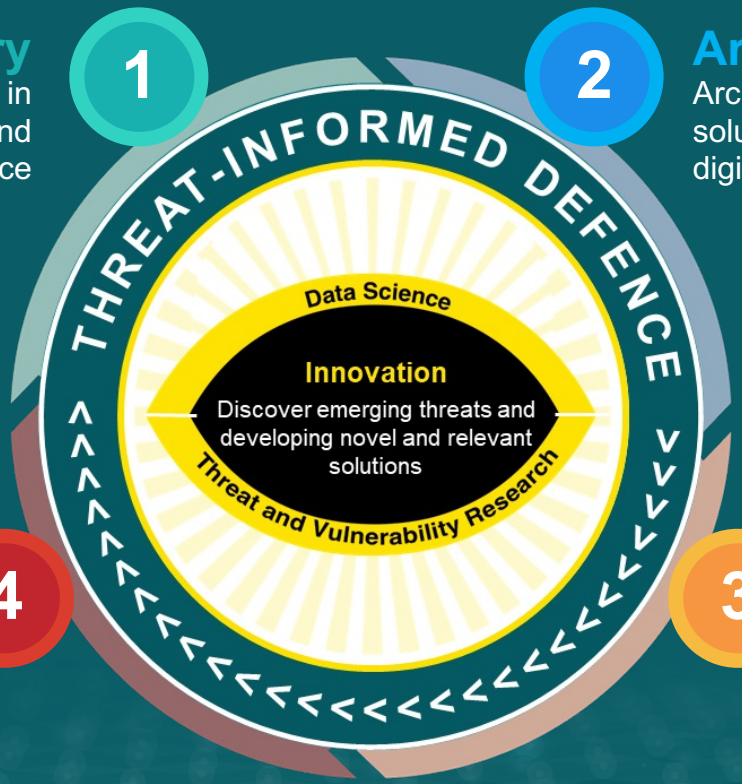
Utilising our expertise to assist clients in comprehending their cyber defence posture and devising strategies to enhance their resilience

- Executive Advisory
- Cyber Strategy
- Cyber Assurance
- Training and Simulation
- Threat Intelligence

2 Architecture & Implementation

Architecting and implementing cybersecurity solutions to bolster the defences across the digital attack surface

- Cyber Command Centres
- System of Systems
- Zero-trust Infrastructure
- End-to-end Automation
- Security-by-design



3 Cyber Operations

End-to-end management of cybersecurity operations through advanced threat detection, continuous monitoring services

- Cyber Threat Hunting
- Adv. Threat Detection & Response
- End-to-end Security Management
- Advanced Security Operations
- Red and Purple Teaming

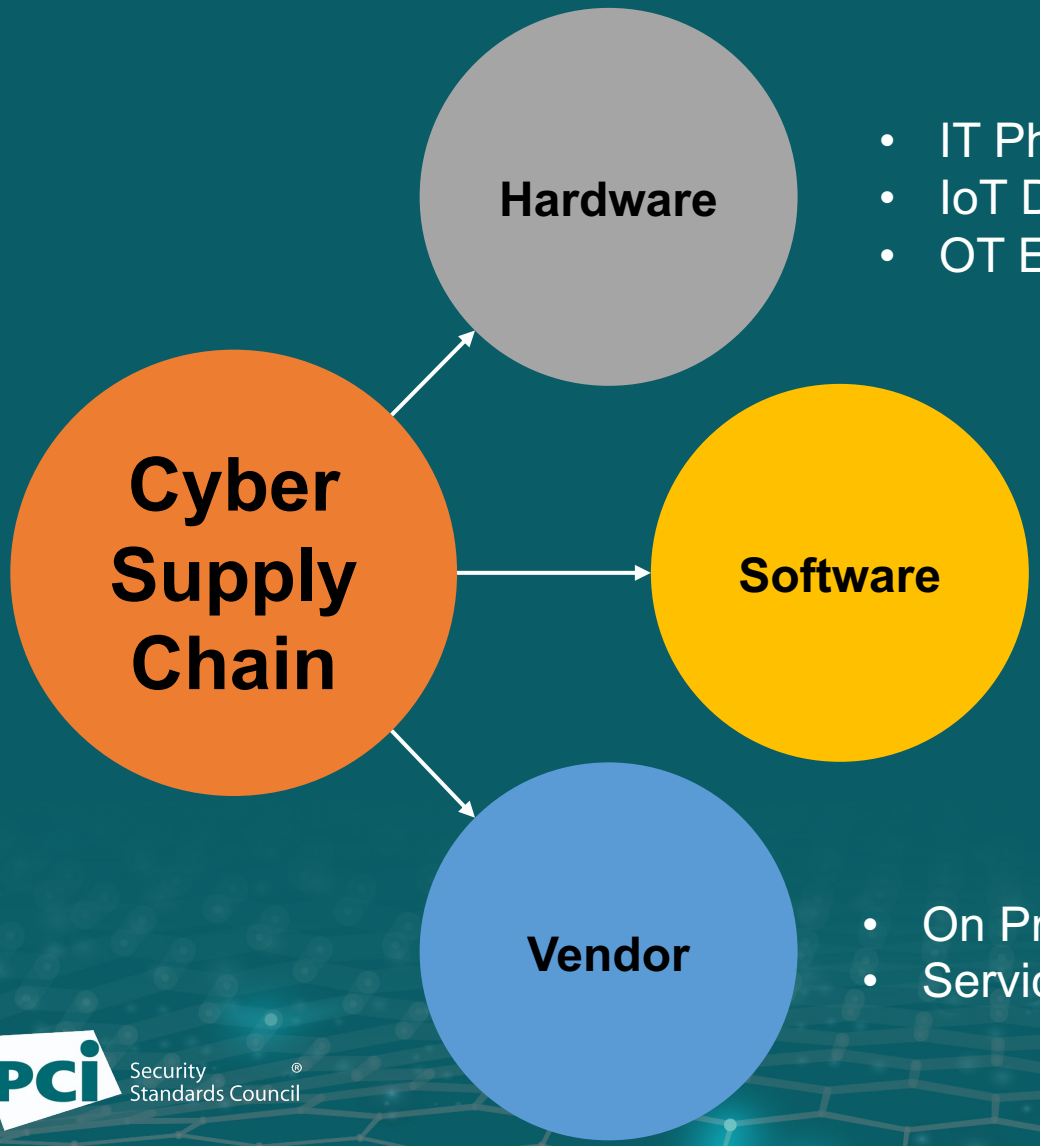
4 Response

Using advanced technologies and threat intelligence to identify, analyse, and respond to threats

- Digital Forensics
- Incident Response
- Crisis Management
- Malware Reverse Engineering
- Adversarial Threat Analysis

PCI Security Standards Council®

The Triad of Cyber Supply Chain



- IT Physical Assets
- IoT Devices
- OT Equipment

- In house software
- Commercial Off The Shelf (COTS)
- Open Source Software Components

- On Premise Contractors
- Services Providers

PCI Security Standards Council

Top Risks in the Cyber Supply Chain

HARDWARE

- Insertion of counterfeits
- Unauthorised production
- Tampering
- Insertion of unauthorised hardware
- Poor manufacturing quality
- Design flaws
- Firmware and microcode vulnerabilities

SOFTWARE

- Source code compromise
- Insertion of malicious code
- Tampering
- Bugs and vulnerabilities
- Design flaws

VENDOR

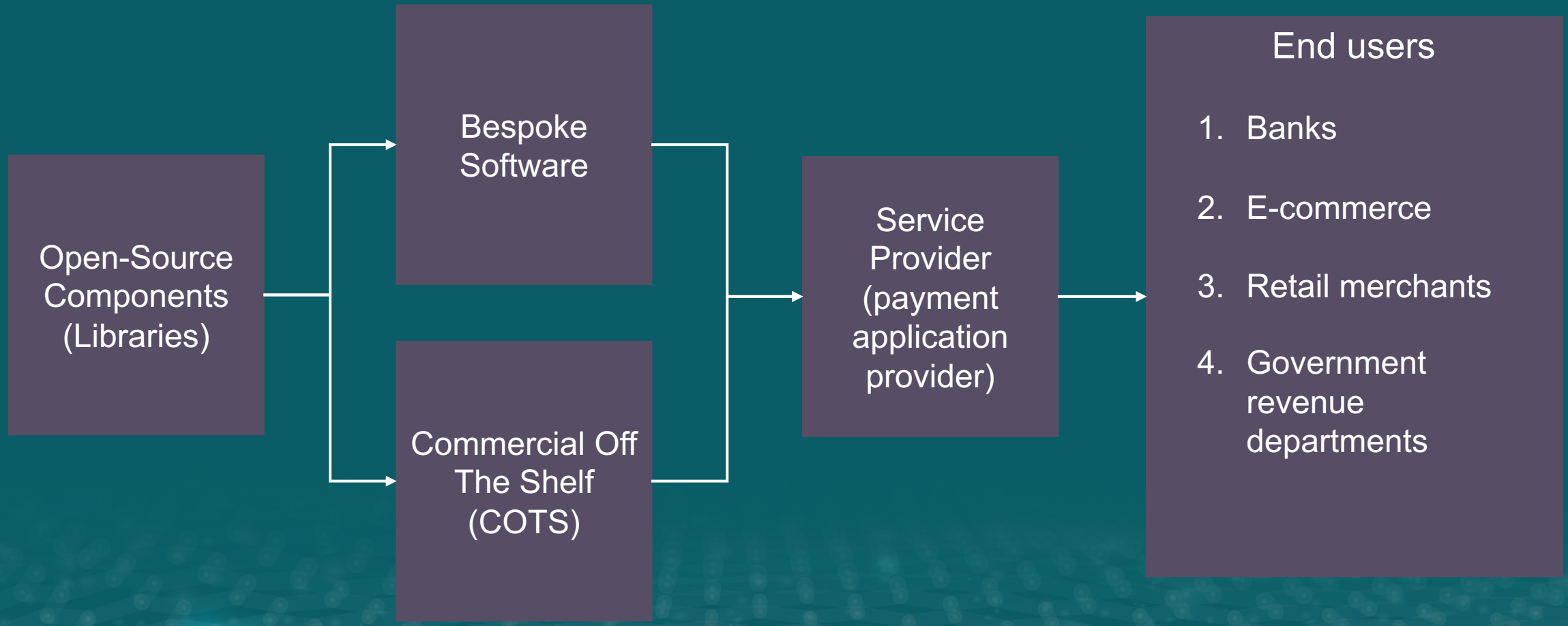
- Insider risk
- Poor sensitive information handling processes
- Poor cyber hygiene practices

Ultimately, it is the systemic implications of dependencies in the supply chain and consideration of collateral damage affecting the business (and cyber) resilience

PCI Security Standards Council

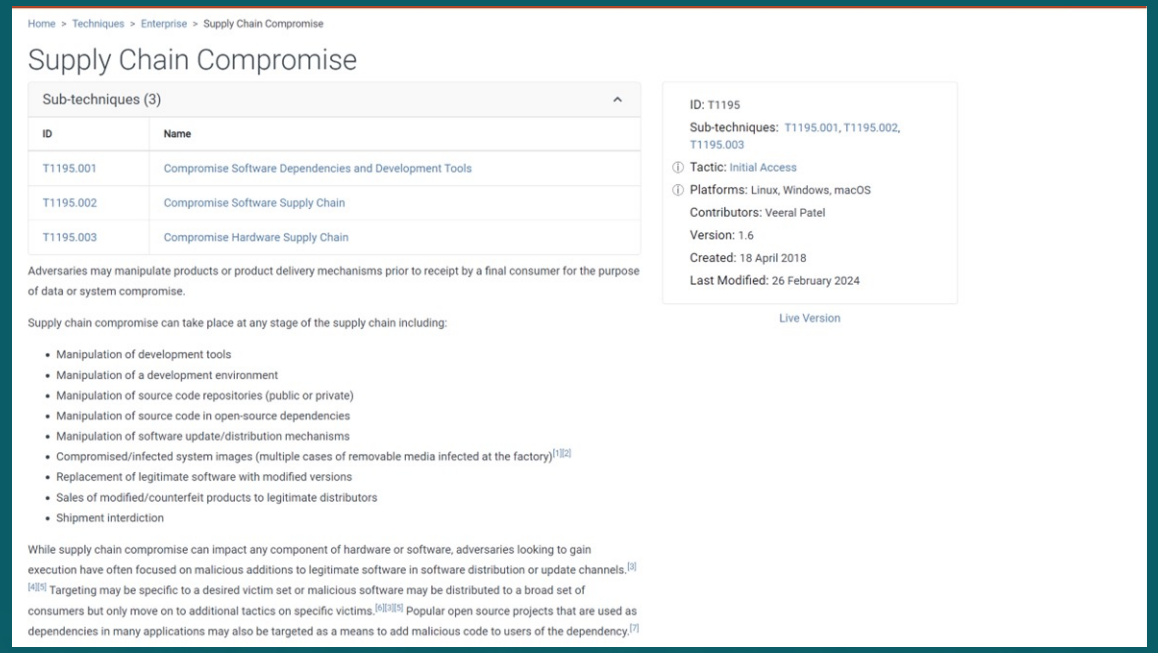
Supply Chain Value in PCI DSS

Software is a Critical Component in Payment Processes



PCI Security Standards Council

Reality of Supply Chain Cyber Attacks



Home > Techniques > Enterprise > Supply Chain Compromise

Supply Chain Compromise

Sub-techniques (3)

ID	Name
T1195.001	Compromise Software Dependencies and Development Tools
T1195.002	Compromise Software Supply Chain
T1195.003	Compromise Hardware Supply Chain

ID: T1195
Sub-techniques: T1195.001, T1195.002, T1195.003
Tactic: Initial Access
Platforms: Linux, Windows, macOS
Contributors: Veeral Patel
Version: 1.6
Created: 18 April 2018
Last Modified: 26 February 2024

Live Version

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take place at any stage of the supply chain including:

- Manipulation of development tools
- Manipulation of a development environment
- Manipulation of source code repositories (public or private)
- Manipulation of source code in open-source dependencies
- Manipulation of software update/distribution mechanisms
- Compromised/infected system images (multiple cases of removable media infected at the factory)[1][2]
- Replacement of legitimate software with modified versions
- Sales of modified/counterfeit products to legitimate distributors
- Shipment interdiction

While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.[3][4][5] Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.[6][3][5] Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.[7]

WIRED SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH SIGN IN

BY KIM ZETTER THE BIG STORY MAY 2, 2023 6:00 AM

The Untold Story of the Boldest Supply-Chain Hack Ever

The attackers were in thousands of corporate and government networks. They might still be there now. Behind the scenes of the [redacted] investigation.

November 2020 – "Major IT Management Company" Supply Chain Compromise

The Log4j Vulnerability: Millions of Attempts Made Per Hour to Exploit Software Flaw

Hundreds of millions of devices are at risk, U.S. officials say; hackers could use the bug to steal data, install malware or take control

December 2021 – Log4J Supply Chain Compromise

PCI Security Standards Council®

And after that, we had, many more…

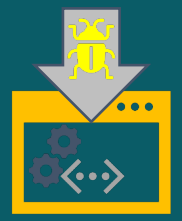
Case Study on Supply Chain Compromise

1

Threat Actor targets Major IT Management Company

2

Threat Actor injects malicious code into software through the code repository



3

Malicious code is uploaded to installed instances though software updates

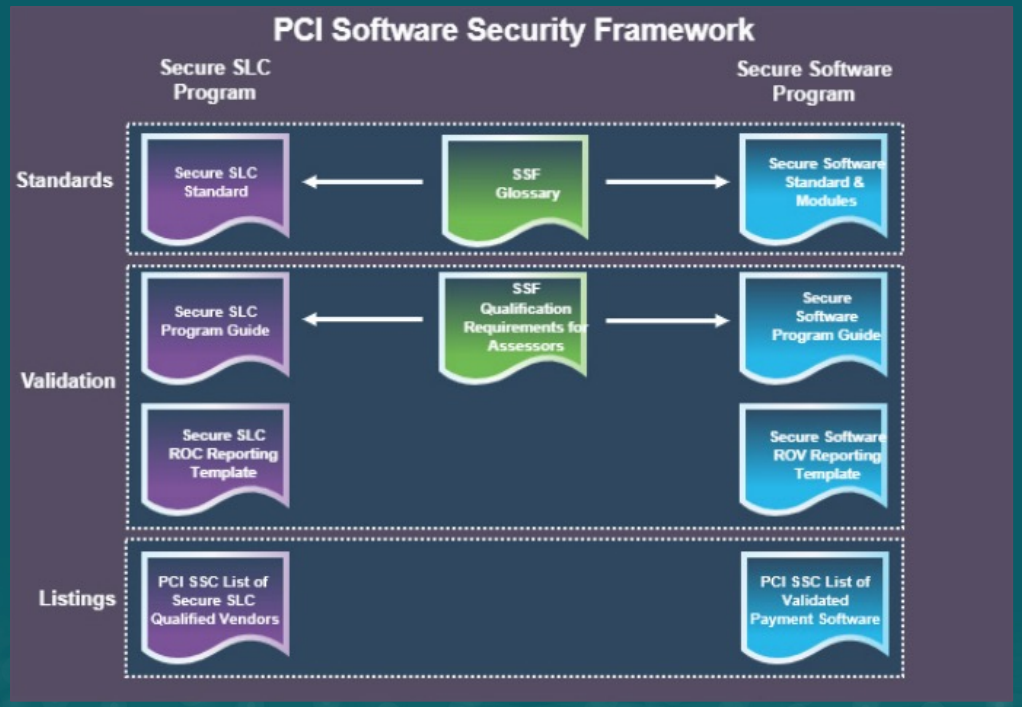
4

Threat Actor goes on to attack victims with the compromised software

PCI Security Standards Council®

PCI Contribution for Secure Design and Development of Software

PCI Software Security Framework



Source: PCI

PCI DSS v4.0.1 – Section 6

Requirement 6: ***Develop and Maintain Secure Systems and Software***

Sections	
6.1	Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.
6.2	Bespoke and custom software are developed securely.
6.3	Security vulnerabilities are identified and addressed.
6.4	Public-facing web applications are protected against attacks.
6.5	Changes to all system components are managed securely.

Overview

Actors with bad intentions can use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All system components must have all appropriate software patches to protect against the exploitation and compromise of account data by malicious individuals and malicious software.

Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For bespoke and custom software, numerous vulnerabilities can be avoided by applying software lifecycle (SLC) processes and secure coding techniques.

Code repositories that store application code, system configurations, or other configuration data that can impact the security of account data or the CDE are in scope for PCI DSS assessments.

See *Relationship between PCI DSS and PCI SSC Software Standards* on page 7 for information about the use of PCI SSC-validated software and software vendors, and how use of PCI SSC's software standards may help with meeting controls in Requirement 6.

Refer to *Appendix G* for definitions of PCI DSS terms.

***Note**: Requirement 6 applies to all system components, except for section 6.2 for developing software securely, which applies only to bespoke and custom software used on any system component included in or connected to the CDE.*

Source: PCI DSS

PCI Security Standards Council®

Key Recommendations for Securing the Software Supply Chain

Vendor Risk Assessment

Continuous assessments provide early detection of vulnerabilities.

Zero-Trust Approach

Use micro-segmentation to isolate third-party software from sensitive data environments

Strengthen Incident Response

A well-prepared incident response plan helps mitigate the impact of breaches

Leverage SBOM

SBOMs allow you to track software dependencies and identify vulnerable components

PCI Security Standards Council®


PCi
Security
Standards Council
®