PCI Security Standards Council

The Verizon 2024 Payment Security Report

Protecting Data at the Point of Input

Stephen Ward

Chief Marketing Officer – Worldwide
Source Defense

Ciske van Oosten

Associate Director, Head of Global Business Intelligence – Cyber Security Consulting
Verizon

verizon

source DEFENSE

PCI Security Standards Council

Protecting Data at the Point of Input

A New Challenge for the PCI Community

- The Battlefield has Moved…
  - From Protecting Data in Transit & Data at Rest…to Data at the Point of Input
- Protecting Our Digital Storefronts is Our New Community Challenge
  - Significant Data Security and Data Privacy Concerns
- The Modern Website has its Own Third-party, Digital Supply Chain
  - Unmonitored, Unmanaged, Unprotected…Highly Targeted JavaScript
    - MageCart, eSkimming, Form-jacking, Click-jacking, Credential Harvesting

PCI Security Standards Council®

From Transit & Rest – To Point of Input

source DEFENSE

2005-2015

EMV Liability Shift (US 2015)
Card not present becomes the target

2016

Dawn of ‘Magecart’

2018

High Profile Attacks
Major Airline Ticketing

2019

Massive GDPR Fine
Major Airline

2020

Exponential Shift
Global Pandemic pushes quantum leap

High Profile Breaches Continue
Adversaries Shift to Small Merchants as a Target

2022

PCI DSS v4.0 Intro

2023

100m+ Cards Online
Vast Majority CNP

2024

2x Increase
in Digital Supply Chain

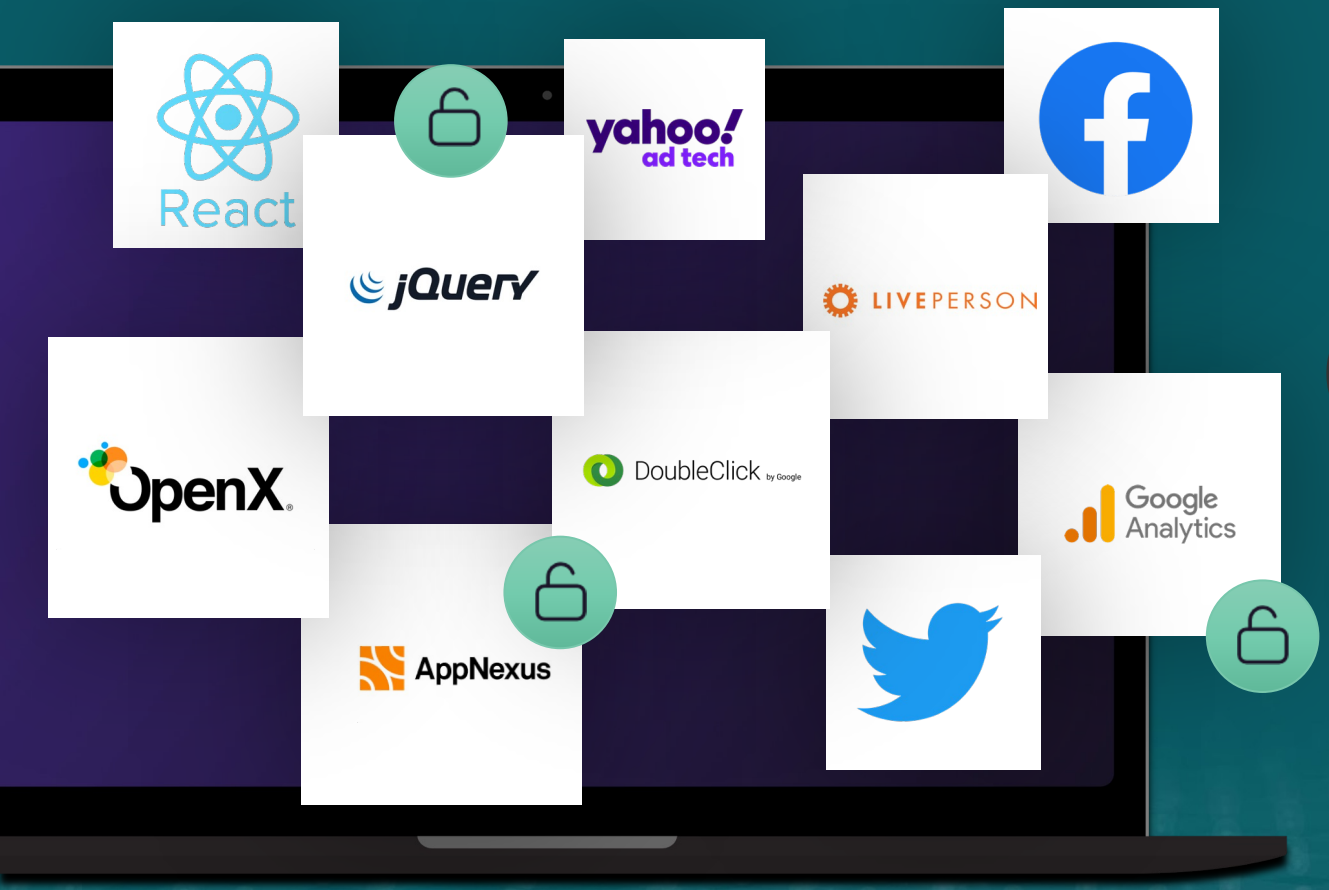
2025

PCI Security Standards Council

PCI Security Standards Council

Protecting Data at the Point of Input

A New Challenge for the PCI Community



82%

of code and actions
are outside your control

PCI Security Standards Council

What Makes Unmanaged Scripts So Dangerous?

JavaScript compromised by an adversary can:

Change page content

Record keystrokes

Add content (images, text, video, & form fields)

Track website behavior

Capture and exfiltrate credit card data

Redirect visitors to websites under attacker control

PCI Security Standards Council

Acknowledging the Problem

eSkimming Security Controls in PCI DSS v4.0

> “The targeting of eCommerce platforms and third-party code integrations are among the most common tactics utilized by threat actors…
>
> …threat actors are targeting supply chains and third-party service providers with high frequency and exhibiting continued interest in payment account data and personally identifiable information (PII).”
>
> Visa Inc. – June 2022

The PCI Council Takes Action… PCI DSS v4.0

- Confirm that each script is authorized (6.4.3)
- Assure the integrity of each script (6.4.3)
- Maintain an inventory of all payment page scripts and justify why they are necessary (6.4.3)
- Monitor Payment Page headers for changes at least once every seven days (11.6.1)
- Alert and block all malicious scripts on your payment pages (11.6.1)

PCI Security Standards Council®

Understanding the Scope of the Issue

The 2024 Verizon Payment Security Report – First of Its Kind Analysis

- Everyone's Issue Regardless of Industry or Geography
- 7,000 of the World's Largest Websites Analyzed
  - North America, Europe, Latin America
- 129,897 Scripts Identified – 3rd, 4th, nth party

40%

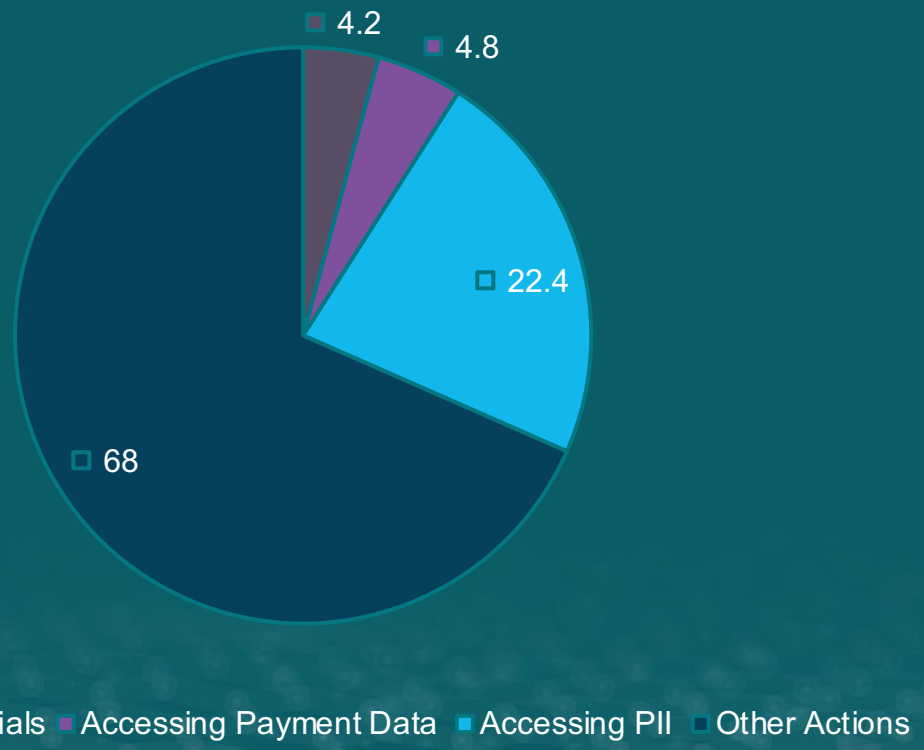
of scripts analyzed found on Payment Pages

PCI Security Standards Council

Understanding the Scope of the Issue

The 2024 Verizon Payment Security Report – First of Its Kind Analysis

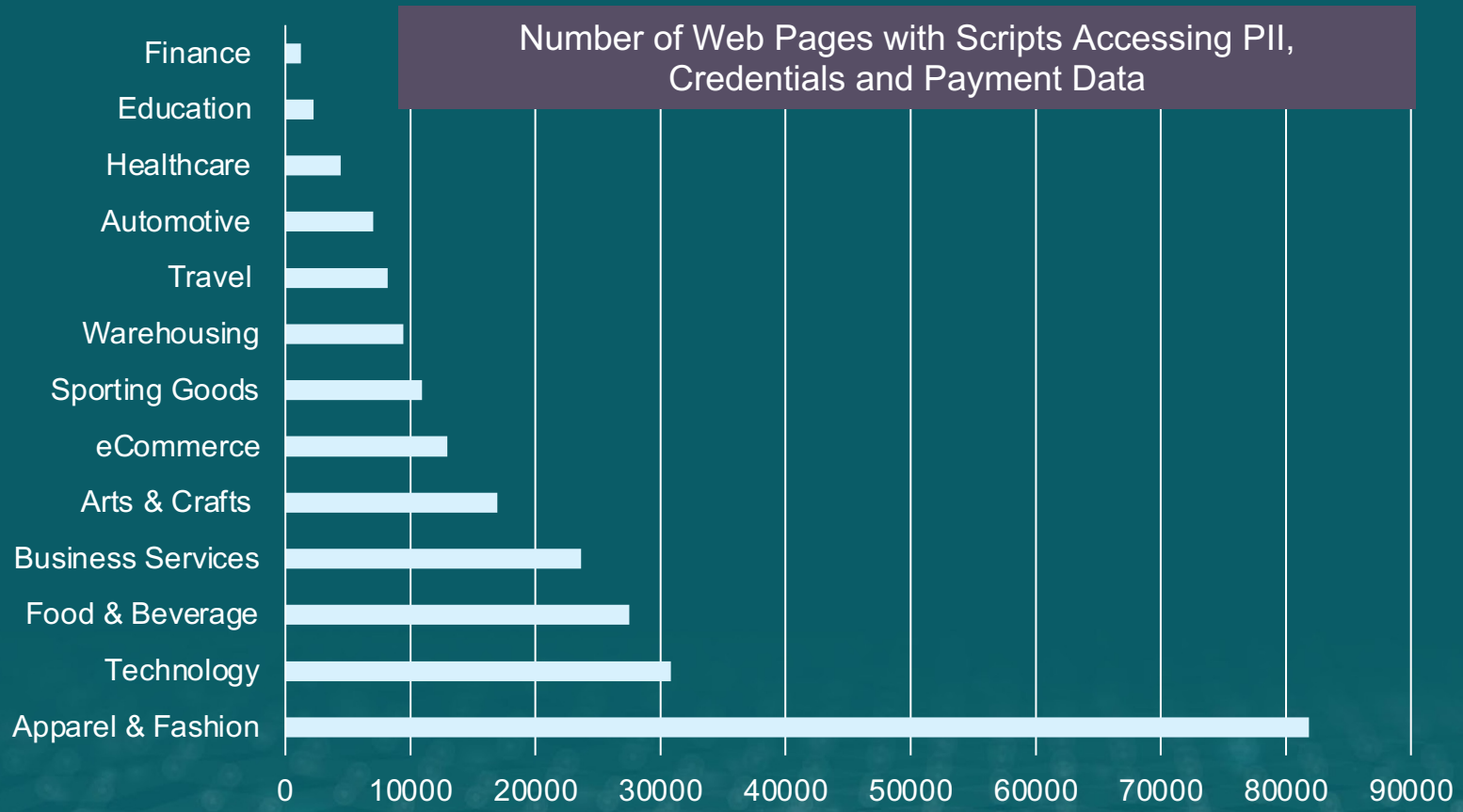
- Widespread and Growing use of the Digital Supply Chain
  - Average of 18 Scripts Per Page
    - 13 third-party scripts
    - 8 fourth-party scripts
  - 50% increase in the past 2 years
- Significant Risk to Data Security
  - Transferring Data
  - Executing Risky Actions
  - Accessing PII
  - Accessing Card Data
  - Accessing Credentials



PCI Security Standards Council

Understanding the Scope of the Issue

The 2024 Verizon Payment Security Report – First of Its Kind Analysis



Certain Industries More Reliant

- Strong online presence
- Highly customizable product offerings
- Lower initial customer conversion ‘electronic window shopping’

PCI Security Standards Council®

Addressing This and Other Issues
Security Program Life Cycle Management

PCI Security Program Life Cycle Management

1. PROGRAM PLANNING & DESIGN		2. PROGRAM EXECUTION & MANAGEMENT		3. EVALUATION & IMPROVEMENT	
Conception & initiation	**Definition & planning**	**Program launch**	**Program performance & control**	**Program effectiveness**	**Program efficiency**
• **Program office** • **Program charter** - purpose - stakeholders - assumptions - risks • **Program approval**	• **Program plan** - program goal - requirements - objectives - constraints • **Scope** - work breakdown schedule • **Budget** • **Risk management**	• **Communication** • **Program & projects kick off** • **Status & tracking** • **Quality** • **Forecasts**	• **Milestones & objectives** • **Execution & delivery performance** - throughput • **Monitoring & reporting** • **Management** - scope - resources - constraints - input: time & effort - budget	• **Program outcome evaluation** - quality of deliverables • **Program process evaluation** - capability maturity - process maturity • **Projects performance evaluation** - project post-mortems • **Continuous improvement**	

PCI Security Standards Council®

Source: Verizon 2023 Payment Security Report

Essential PCI Security Program Design and Evaluation Outcomes

An effective program	• **Get the right work done** – contributing to the achievement of the goal • **Evidence of assurance** that its control environment and requirements effectively meet the intent of all control objectives
Strategically aligned	• Programs that supports **business objectives and strategy** • Program design and execution are neither tactical nor reactive
Efficiently executed and economical	• **Produce economical program results** • Program is executed in a better manner with minimum waste of resources • The capability to achieve more with less (despite scarcity of resources)
Sustainable performance	• **Integrated life cycle management** • The ability to sustain performance over extended periods without significant deviations. Rapid detection and correction of deviations
Ongoing capability improvement	• Program includes ongoing **capability measurement, reporting,** and **improvement**

PCI Security Standards Council®

The Security Management Canvas

Security business model	Security strategy	Security operating model	Frameworks & standards	Security program
Business model: • value proposition • stakeholders • goals and objectives • core process architecture • resources • culture • regulations • risk management • governance	**Strategy:** • **stakeholders** • **priorities** - goals - objectives • scope - focus - in-scope - excluded • **resources** - in-house - 3d party **The top 7 strategic management traps**	**Operations:** - value chains visual representation • **stakeholder relationships** • **organizational charts** • **geographic maps** - facilities and operations • **organization processes** - core processes - supporting processes • **security processes** • **network architecture** • **functional responsibilities** • **capabilities map** • **constraints map**	**Integration frameworks & standard** • **PCI DSS** • **PCI PIN** • **PCI P2PE** • **PCI 3DS** • **CIS CSC** • **NIST CSF** • **SWIFT CSP** **Coverage of standard/ framework elements:** - partial/full implementation **Scope of implementation across the environment:** - partial/full implementation	**Program management:** - program office - program charter **Program design:** - life cycle management **Project score:** - resources (4Ls) - constraints (7Cs) - sustainability (9Fs) **Project management:** **Maturity** - process - capability **Performance** - metrics - reporting

PCI Security Standards Council®

Source: Verizon 2023 Payment Security Report

Parting Thoughts

Addressing eSkimming is NOW a Critical Priority - But…

- It should have been prior to the introduction of PCI DSS v4.0 – and it should be an ongoing, expanding concern regardless of the scope of requirements (compliance programs lag behind risks, represent the floor not the ceiling)
- Our online businesses will continue to grow and evolve – we need to make security a primary concern and evolve our security controls faster than our adversaries

How do you accomplish a focused, goal-driven PCI security compliance program?

- It's not about cramming more activities into an overloaded schedule
- The program measurement and evaluation are about doing LESS with your program
- Focus on what matters most
- Study, adapt and apply the various PCI security program performance and evaluation management methods that are available

Contact either of us for more detail: steve@sourcedefense.com ; ciske.vanoosten@verizon.com