PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING

2025
EUROPE
COMMUNITY
MEETING

Digital Battlegrounds: Mastering the Art of Cyber War Through Asset-Threat Alignment

Lessons from a Ransomware Attack against a major UK merchant retailer specializing in clothing, food and goods.

PCI Security Standards Council

Jim Seaman

MSc (Security Management), CISM, CRISC, CDPSE

IS Centurion Consulting Ltd

PCI Security Standards Council

Sun Tzu's Wisdom

The Art of War

"If you know the enemy and know yourself, you need not fear the result of a hundred battles."

PCI Security Standards Council

The Modern Threat Environment

Initial Access Brokers (IABs), e.g., Scattered Spider:
- Specialists in intrusion
- Use phishing, MFA fatigue, SIM swapping
- Sell access to ransomware groups

Ransomware-as-a-Service (RaaS) , e.g., DragonForce:
- Rentable ransomware tools
- Focus: delivery, exfiltration, extortion
- Drives attack volume and sophistication

Business Risks
- Disruption, data loss, reputational/financial impact

Key Definitions

Asset

An item of value to stakeholders. An asset may be tangible or intangible.
The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle.
Such concerns include but are not limited to business or mission concerns.

Vulnerability

A weakness that can be exploited or triggered to produce an adverse effect.

Threat Source

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

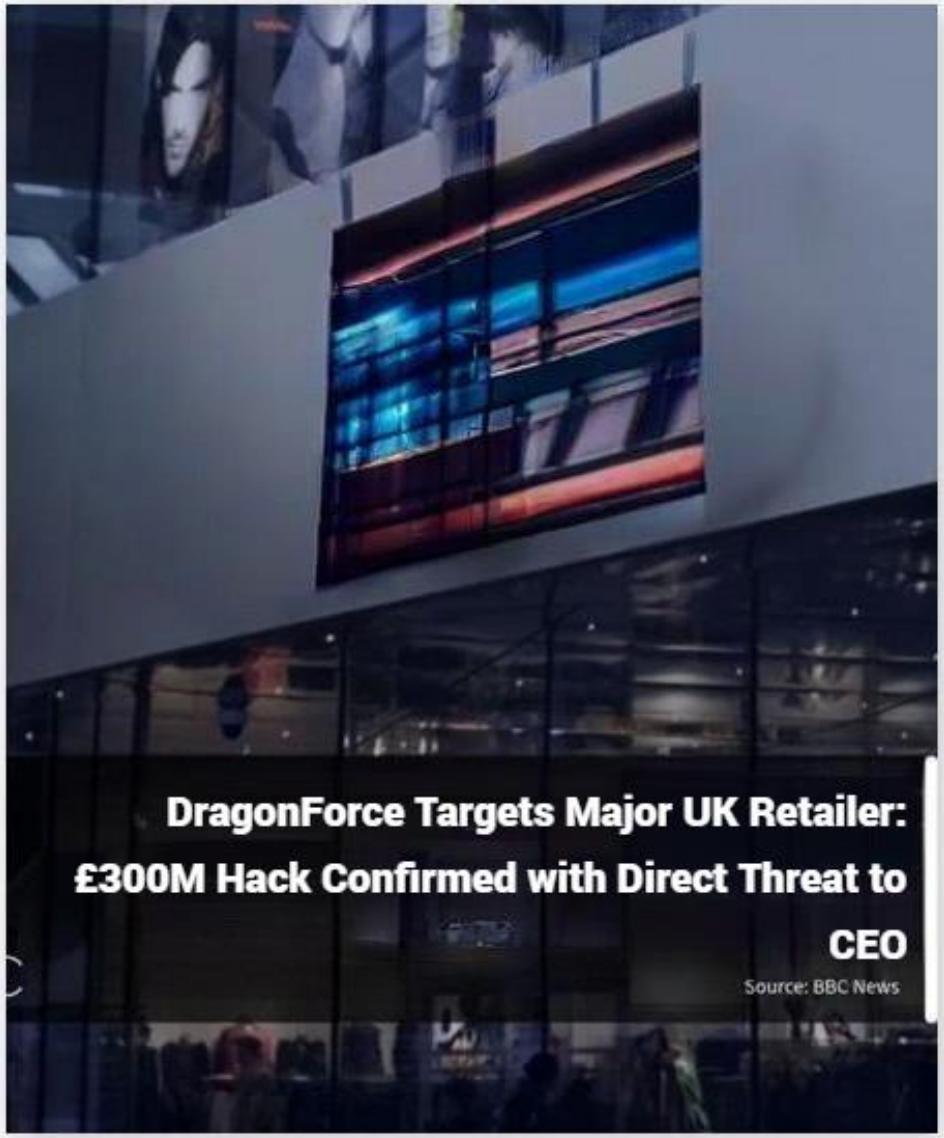
Sources:

NIST SP 800-160 Vol. 2 Rev. 1.
NIST SP 800-37, Revision 2.

PCI Security Standards Council

Why Asset-Threat Alignment?

- Critical operations depend on high-value digital assets:
  - *The "Crown Jewels"*
- Attackers target what matters most for maximum leverage
- Asset-threat mapping enables prioritization of controls and response
- Defending everything equally is impossible:
  - Focus on what matters
    - Mission critical/high value business operations



Case Study: Ransomware Attack Overview

- **Feb 2025:** Retailer's infrastructure initially compromised.
- **April 2025:** Retailer's operations are disrupted by coordinated ransomware attack.
- Attackers exploited third-party supplier and internal IT processes.
- **Result:** E-commerce, payments, and logistics halted;
  - Only truncated *(last 4 digits of PAN)* compromised *(limited value to criminals).*
  - Major financial and reputational loss.

PCI Security Standards Council

The Attack Chain: From Initial Access to Impact

Initial Access

Scattered Spider:

- Vishing
- MFA Request Generation

DragonForce:

- Exploit Public-Facing Application
- External Remote Services

Persistence

Scattered Spider:

- Remote Access Software
- Modify Authentication Process: MFA

DragonForce:

- Scheduled Task

Credential Access

Scattered Spider:

- OS Credential Dumping
  - Disabling EDR
  - LSASS memory

DragonForce:

- OS Credential Dumping
  - Extract passwords & hashes

Lateral Movement

- Scattered Spider:
  - Remote Services
    - Cloud Services

DragonForce:

- Remote Desktop Protocol

Impact

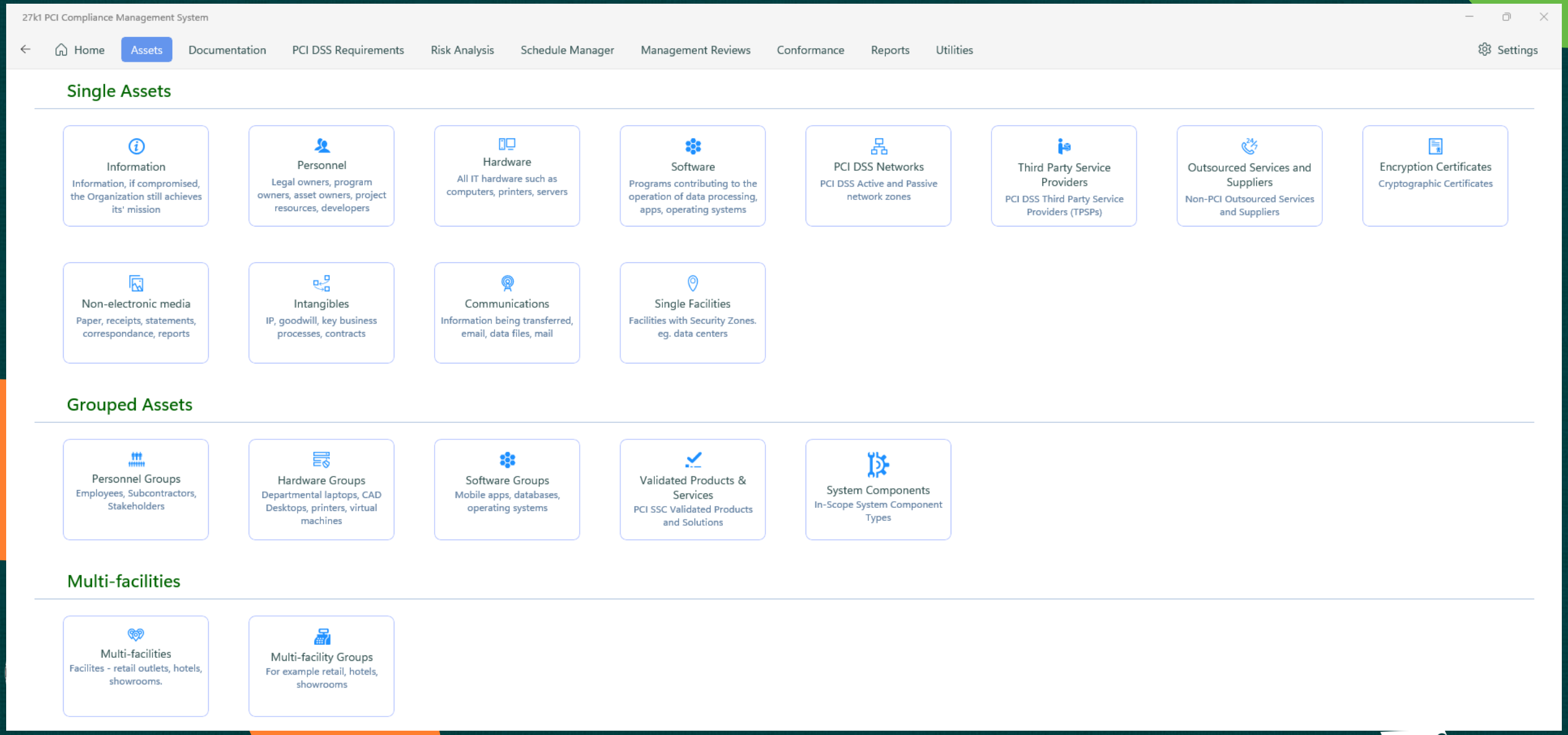
Scattered Spider:

- Data Encrypted for Impact
  - BlackCat/ALPHV ransomware

DragonForce:

- Data Encrypted for Impact
  - DragonForce ransomware

PCI Security Standards Council

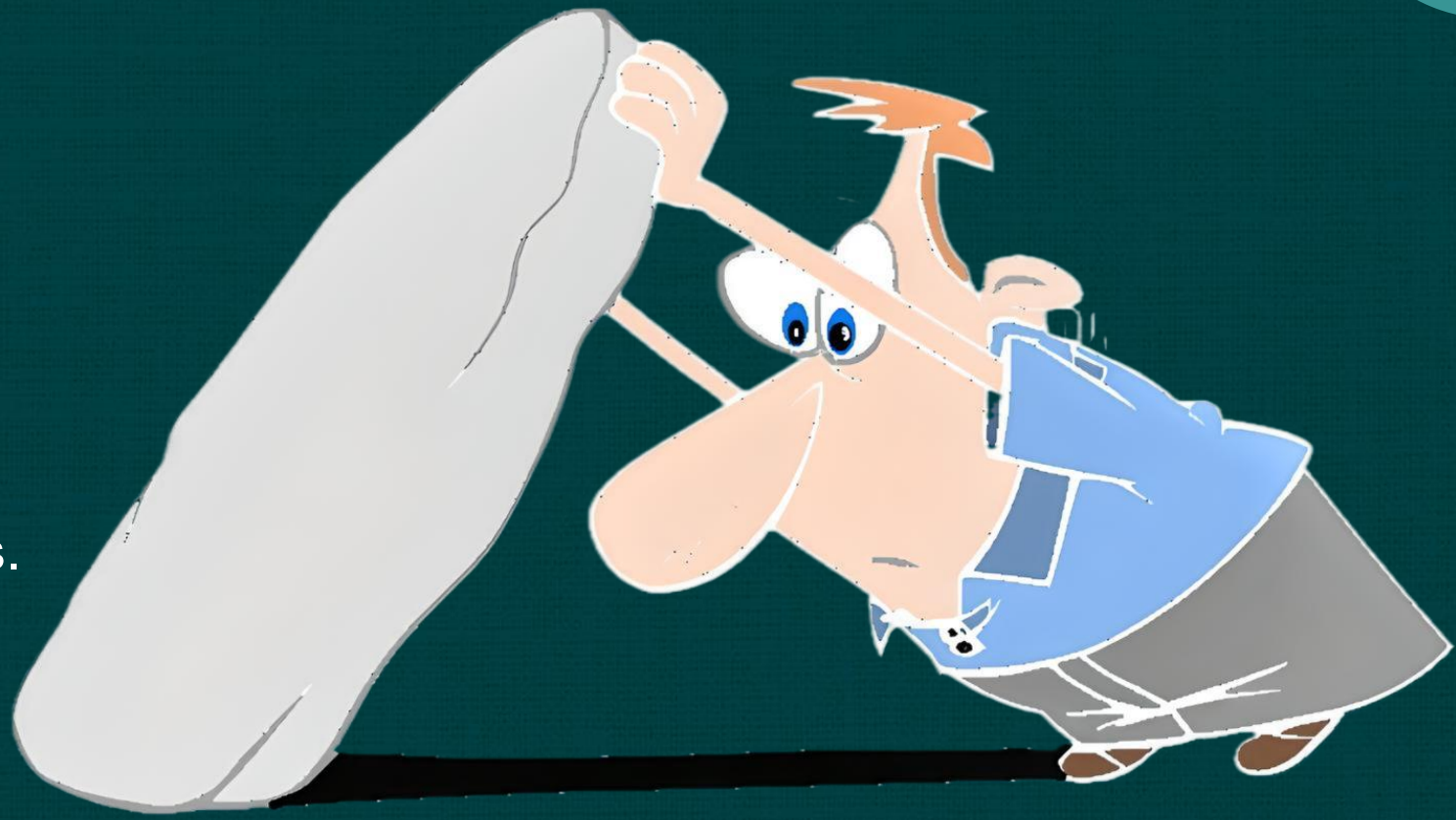


PCI Security Standards Council

UK Retailer Know Yourself: Leave No Stones Unturned

High-value assets:

- Active Directory.
- VMware ESXi.
- Customer data.
- Supplier integrations.



Weaknesses revealed:

- Overprivileged third-party access.
- Inadequate credential hygiene.
- Poor network segmentation.

Lesson: Asset visibility and governance are foundational.

Dwell Time – The Hidden Threat

Definition

- The amount of time an attacker has undetected access to a system.
  - It can be measured in days or months depending on how they gain entry and what they do once inside.

Source: https://bestcybersecuritynews.com

UK Retailer Cyberattack:

- 8–10 weeks between initial breach.
  - (Feb 2025) and ransomware deployment (late April).
- Activities during dwell:
  - Credential harvesting and privilege escalation.
  - Lateral movement and staging of ransomware.
  - Data exfiltration and extortion preparation.
- Extended dwell time maximized business impact.

Lesson: Early Mean Time To Detect (MTTD) is critical for limiting damage.

Value of UK Retailer's PCI DSS Compliance Program

PCI DSS scoping limited payment card exposure

- Only PCI-compliant "truncated" card data stored (e.g., 4111 11** **** 1111).
- No full cardholder data, CVV, or PINs retained post-authorization (PCI DSS 3.2).

Impact on the attack

- Attackers exfiltrated only masked card data and reference numbers.
- Could not monetize payment card data.
  - Pivoted to less-protected Personal Data.

Lessons for asset-threat alignment

- PCI DSS reduced payment system attack surface.
- Highlighted need to extend rigorous controls to non-PCI critical assets .
  - e.g., AD, customer Personal Data

BBC NEWS

Home | InDepth | Israel-Gaza war | War in Ukraine | Climate | UK | World | Business | Politics | Culture

Business | Economy | Technology of Business | AI Business

** says customer data stolen in cyber attack

Michael Race & Joe Tidy

Business reporter & Cyber correspondent, BBC News

13 May 2025

The High Street giant said the personal information taken could also include online order histories, but added the data theft did not include useable payment or card details or any account passwords.

Major UK Car Manufacturer to halt production until next month after cyber attack

Story by Karl Matchett • 3d • 2 min read

Carmaker has announced it will extend its pause in production until 1 October as it recovers from a cyber attack.

Production and sales at , which is owned by Indian firm were halted at the start of September and IT systems were shut down after the hack was discovered on 31 August.

PCI Security Standards Council