

Examining the Realities of Cyber Risk for SMBs.





Eimear Dunne
SVP Product Marketing

Thomas Patterson
EVP Product Management

Will cover:

SMB Merchant Risk

What the PCI DSS Sees, and What It Misses

What the Data Shows Across Real Portfolios

Closing the Blind Spot

20 YEARS OF SECURING PAYMENT DATA

PCI Security Standards Council



Our Journey Begins

#1 SMBs see cybersecurity risk to their business

VikingCloud Threat Landscape Report 2026

SMBs – the backbone of the economy, and of your book

- ⚠ They are online.
- ⚠ They are a target; their risk is real.
- ⚠ They are unprepared.
- ⚠ Cybersecurity disruption has consequences.
- ⚠ They know they can't do it on their own.













20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The Ground has Shifted

From card swipes to multiple payment rails.
From offline to online business operations, including customer management and marketing.

And now …

83% Of small businesses have a website. **Link**

77% Engage with customers via social media.

7 Cloud apps SMBs use to run their business on average.



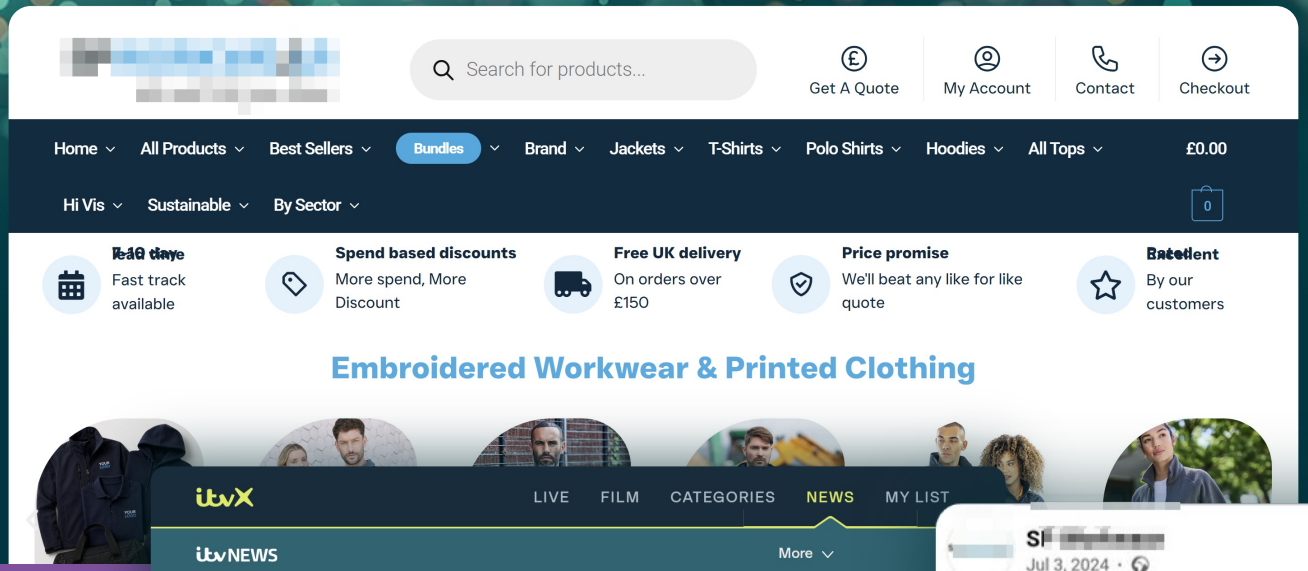




20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

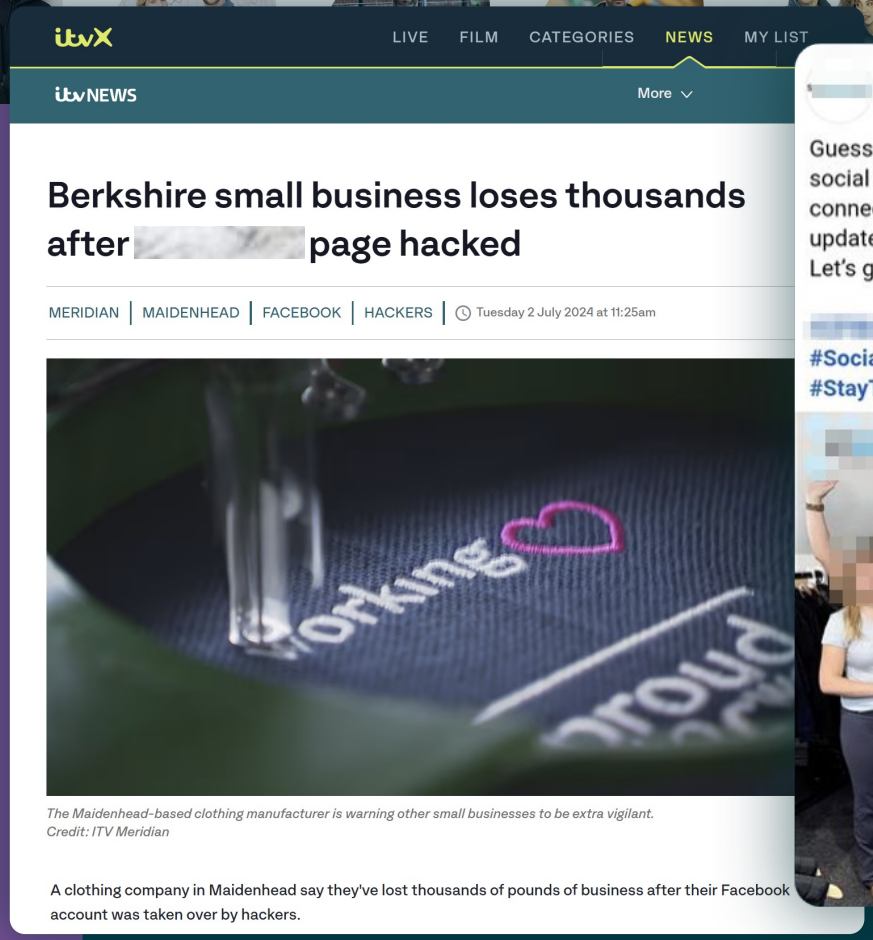
Small UK Workwear Business.

- 1 Office Location
- Website - Online Ordering
- 3 Social Media Profiles



Social media account hacked.

- ⚠ **£20,000** lost earnings.
- ⚠ **2 months** locked out of account.
- ⚠ **£2,100** in fraudulent charges.
- ⚠ **Customers unable to contact** them via their social media page.





UK Micro Business Children's Clothing

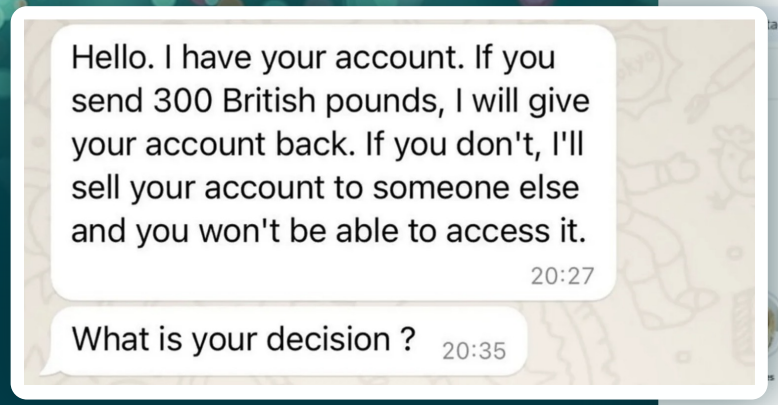
- 1 office location.
- Website - online ordering.

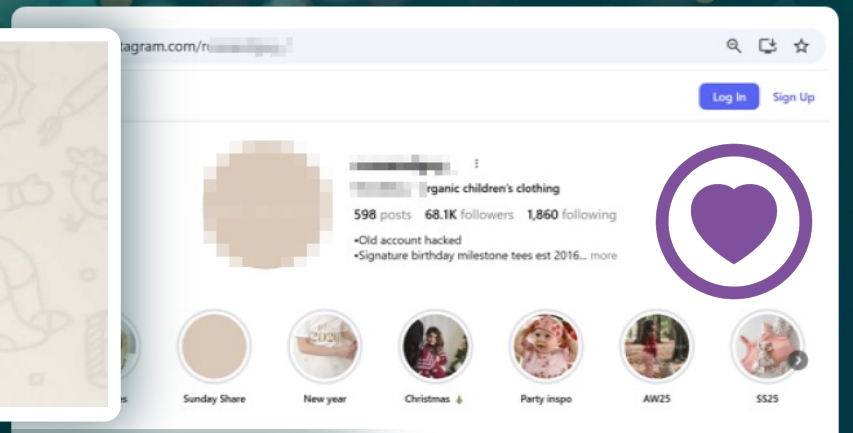
Social media account takeover.

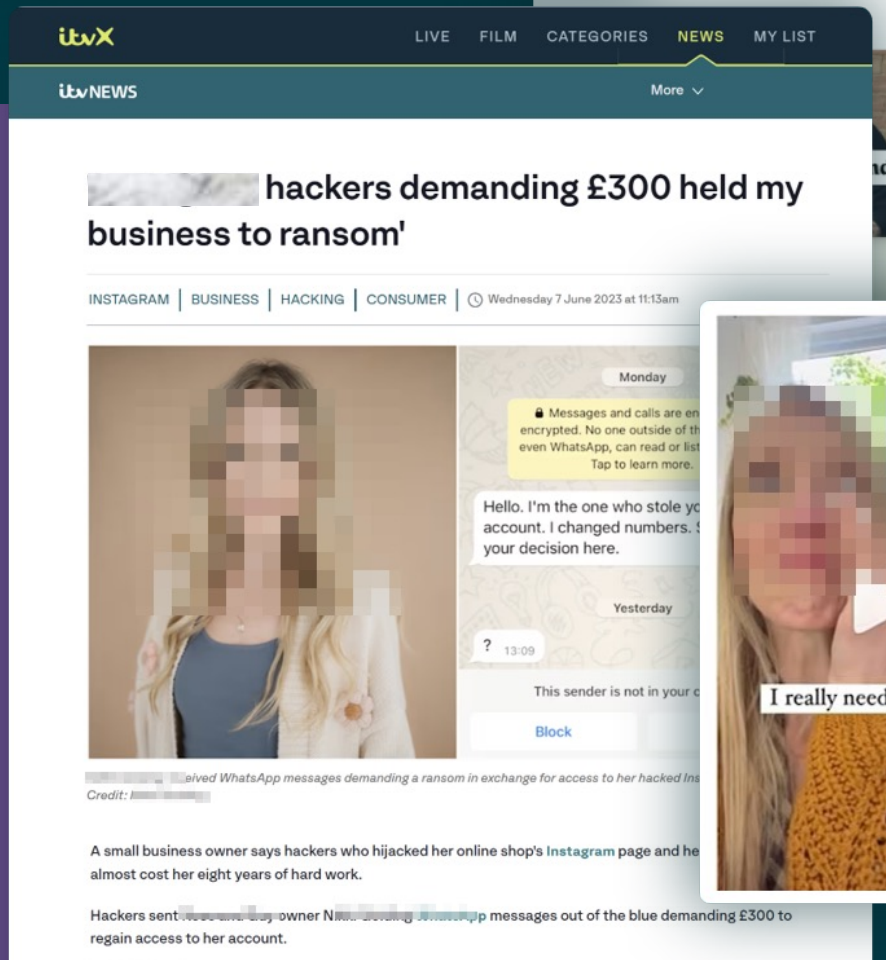
⚠ **Locked** out of their social media account.

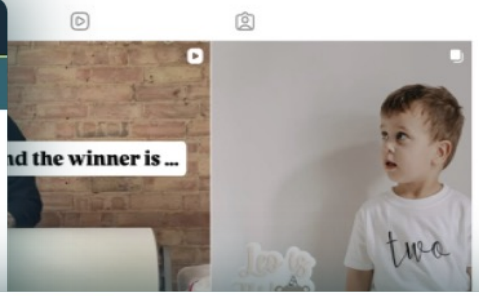
⚠ **95% of sales via hacked account** – near complete shutdown of all sales.

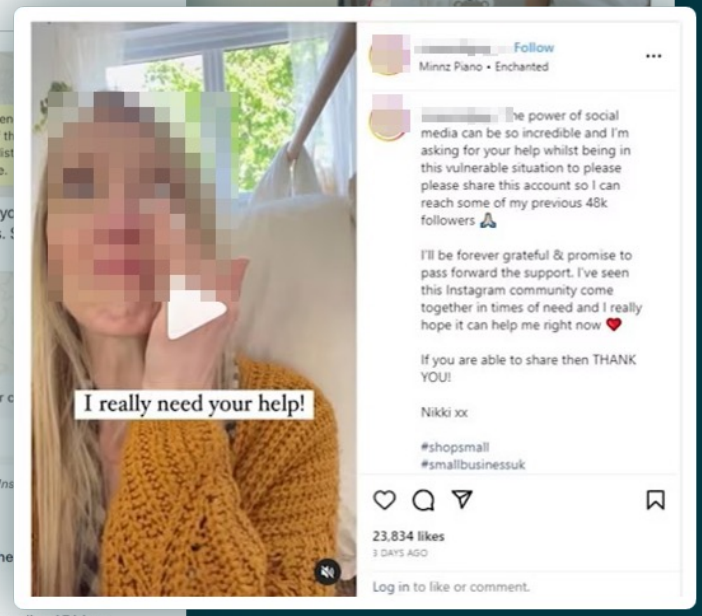
⚠ **48,000 followers** lost, starting again from scratch.











PCI DSS Status **Does Not** Provide A Clear View Of Merchant Risk

The Numbers Tell the Story:

2,035
merchant sites risk-assessed

6
merchant segments compared

Assessments are based on an A-F Security Score where A is doing great C-D has actions to take and F is at serious risk.

20 YEARS OF SECURING PAYMENT DATA

The Compliance-Security Gap: What We Can See

1 in 3 merchants non-compliant

yet,

1 in 2 have identified cyber risk



A compliant merchant is just as likely to have an identified cyber risk as a non-compliant one.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Low Risk Channels: Compliant, Still Exposed

Acquirer and bank-direct L3/L4 merchants are typically the most PCI DSS compliant in every portfolio; merchants who are exempt are deemed low risk.
The cyber assessment consistently flags around half with addressable risk.

Banking Channel

Perceived Risk - PCI DSS non-compliant.

27%

Identified cyber risk.

50%

⚠

Includes **10% scoring** a risky F rating

Gap: 23 points their own assessment never flagged.

Direct to Acquirer

Perceived Risk - PCI DSS non-compliant.

29%

Identified cyber risk.

52%

⚠

Includes **2% scoring** a risky F rating

Gap: 23 points their own assessment never flagged.

PCI DSS Exempt Merchants

Perceived Risk - PCI DSS non-compliant.

0%

Identified cyber risk.

58%

⚠

Includes **6% scoring** a risky F rating

Gap: 58 points never flagged.

ISO and PayFac Channels: Compliance Swings, Risk Holds

Compliance status is a reporting outcome, not a risk measurement.

It moves with channel behavior.

Real exposure does not.

ISO Partner

Perceived Risk - PCI DSS non-compliant.

35%

Identified cyber risk.

54%

No merchants scoring a risky F rating

Gap: 19 points their own assessment never flagged.

Partner

Perceived Risk - PCI DSS non-compliant.

36%

Identified cyber risk.

71%

⚠

Includes **7% scoring** a risky F rating

Gap: 35 points their own assessment never flagged.

Payment facilitator

Perceived Risk - PCI DSS non-compliant.

84%

Identified cyber risk.

56%

⚠

Includes **6% scoring** a risky F rating

Gap: 28 points misrepresenting risk.

The Case For a Holistic Risk View

PCI DSS compliance answers: Did the merchant report their compliance?
The Cyber Risk Defense answers: Is the merchant actually exposed?

01

No correlation

Compliance is flat across grades A to F. A merchant graded F is as likely to be PCI compliant as one graded A.

02

Consistent blind spot

In every channel, at least half of merchants carry identified cyber risk, including many that PCI already calls compliant.

03

Channel-blind

PCI status swings from 16% to fully exempt by channel. Real risk stays at 50% or more. PCI status tracks reporting, not exposure.

Cyber Risk Defense adds **continuous security scoring, monitoring, and remediation** across the **whole portfolio;** not just a compliance checkbox.

Pulls significant merchant risk into view – unidentified by PCI DSS.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

ASGARDPLATFORM®
BY VIKINGCLOUD®

Need help

- Dashboard
- Security Score
- Identity Theft Protection
- Scam Prevention
- Security toolkit
- Marketplace

Collapse

Dashboard

Customize

Your policy protects you up to

$100,000 — one ceiling, applied across every active category

3 of 7 coverage categories active

INSIDE YOUR $100,000 POLICY

- Breach coverage
- Business data recovery coverage
- Ransomware coverage
- Identity recovery coverage
- Business impersonation coverage
- Crime and phishing coverage
- Website downtime coverage

See what's covered

Build your protection

Each action below strengthens your business security.

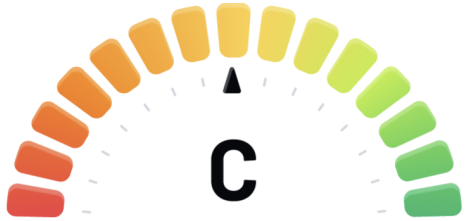
1. **Identity recovery coverage** — Add your date of birth to activate. Activate
2. **Business impersonation coverage** — Connect a social media account to activate. Activate
3. **Crime and phishing coverage** — Confirm a few business details to activate. Activate

View all

Security Score

Grade | Score

Your cyber protection is now active.



A 'C' means there's room to improve your protection based on current information. Your score improves as you take action on your high priority alerts and build your insurance protection.

Understand your score

High priority alerts

Take action and improve your security score.

IDENTITY ALERTS

1 View all

- Business email

SECURITY INCIDENTS

3 View all

- SSL Certificate expired
- Unpatched Web Server
- Website Malware detected

A Living View.
Not a Snapshot.

A live view of risk across your merchant book:

- Continuous monitoring.
- Internal and external signals.
- Site-specific visibility.



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Thank you.

VIKINGCLOUD®

Visit us at booth: **#8**

