White Paper

Retail and E-commerce

Infoprotect

WE BRIDGE THE [CYBER] GAP

How Cyber Risk Assessments Transform Insurability for:

Retail and E-commerce

White Paper | Retail and E-commerce

[I] Infoprotect

WE BRIDGE THE [CYBER] GAP

Transforming Higher Risk Clients into Insurable Risks

EXECUTIVE SUMMARY

The retail and e-commerce sector faces unprecedented challenges securing adequate cyber insurance coverage. As cyberattacks targeting financial institutions have increased in frequency, sophistication, and impact, insurers have responded by tightening underwriting criteria, raising premiums, and sometimes declining to write policies altogether for retail & e-commerce firms...

"TURN 'HARD TO PLACE' INTO 'EASY TO INSURE' - WE HELP HIGHER RISK CLIENTS MEET INSURER EXPECTATIONS."

BRAD FRASER, CEO
@bradfrasergo-giver

This white paper examines how Infoprotect's comprehensive **CYBER ASSESS** framework enables brokers to effectively place retail sector risks while helping e-commerce businesses secure broader coverage at more competitive rates.

Infoprotect **BRIDGES THE [CYBER] GAP** between retailers' security posture and insurer expectations through a structured, validated risk assessment, transforming even high-risk retail operations into preferred insurance risks.

By addressing the specific governance, risk management, and compliance factors that concern underwriters most about retail and e-commerce organisations, Infoprotect's approach **A)** delivers measurable improvements in coverage terms, **B)** reduces premiums, and **C)** ensures these businesses maintain the comprehensive protection required in today's threat landscape.

Why Traditional Approaches Fail Retail and E-commerce Businesses

The Limitations of Standard Cyber Security Assessments

Retail and e-commerce organisations typically invest heavily in security technology and often undergo numerous compliance assessments. However, these standard approaches frequently fail to address insurer concerns for several key reasons:

Technical Focus vs. Governance Reality

Most security assessments concentrate primarily on technical controls (firewalls, encryption, endpoint protection) while underplaying the governance, processes, and human factors that insurers know drive claims. For retail businesses, where point-of-sale breaches, payment card data theft, and social engineering are primary attack vectors, this creates a critical gap in risk evaluation.

"TECHNOLOGY IS ONLY HALF THE STORY. WE HELP INSURERS ASSESS THE HUMAN SIDE OF CYBER RISK."

Compliance-Oriented vs. Risk-Oriented

Retail regulatory frameworks (PCI DSS, consumer data protection, GDPR) drive many security programs, but compliance-focused assessments often fail to address the actual risk scenarios that concern underwriters. Meeting regulatory requirements doesn't necessarily translate to insurability, particularly in areas like:

- Bot attack prevention controls
- Third-party payment processor security
- Authentication for high-value transactions
- Employee security awareness for phishing prevention

"BEYOND SCANS AND SOFTWARE - WHAT ABOUT GOVERNANCE, CULTURE, AND RESPONSE CAPABILITY? WE MEASURE IT ALL."

Self-Attestation vs. Validated Assessment

Traditional cyber insurance applications rely heavily on self-attested questionnaires, where retail and e-commerce businesses answer based on their interpretation of security controls. This creates a significant information gap, as underwriters lack validated evidence of control effectiveness, particularly for complex retail environments with multiple payment channels, customer databases, and third-party integrations.

The Broker Advantage: Placing Retail and E-commerce Risks with Confidence

Transforming Broker Capabilities for Retail Clients

For insurance brokers specialising in retail and e-commerce, Infoprotect's **CYBER ASSESS** provides a powerful competitive advantage in a challenging market:

1. Enhanced Risk Presentation

The detailed risk intelligence from Infoprotect's **CYBER ASSESS** enables brokers to create submissions that stand out from standard applications:

"WHEN INSURERS SAY NO, WE SHOW THEM WHY THEY SHOULD SAY YES. OUR ASSESSMENTS DRIVE APPROVALS."

The difference in detail and credibility transforms how underwriters perceive the risk.

2. Negotiation Leverage

With validated risk intelligence, brokers gain significant negotiation leverage: We arm you with data to negotiate the best deals.

3. Client Advisory Value

The assessment process positions brokers as strategic advisors rather than just policy intermediaries.

Retail and E-commerce Benefits: Beyond Insurance Placement

For retail and e-commerce businesses,, Infoprotect's risk assessment delivers value that extends far beyond insurance placement:

1. Premium Reduction and Coverage Enhancement

The risk intelligence provided allows law firms to secure better coverage at a lower cost.

2. Regulatory Alignment

The risk assessment process aligns with and complements existing regulatory requirements, including mapping controls that support PCI DSS compliance, data protection requirements, customer privacy expectations, and third-party vendor management.

3. Board-Level Risk Intelligence

The assessment provides executives and boards with actionable risk insights.

4. Competitive Differentiation

Strong cyber risk management creates market differentiation and enhanced customer confidence.

Conclusion

Transforming Retail and E-commerce Cyber Resilience

Cyber insurance challenges for retail and e-commerce businesses require a new approach, bridging the [cyber] gap between technical security implementations and underwriter expectations.

Infoprotect's retail sector-specific assessment framework provides this bridge, enabling brokers to effectively place complex risks while helping retail firms secure the comprehensive coverage they require.

By focusing on the governance, process, and human factors that truly determine insurability, rather than just technical controls, Infoprotect transforms how insurers perceive retail sector risks.
The result is broader coverage, lower premiums, and enhanced cyber resilience for an industry that remains a primary target for sophisticated threat actors.

"DON'T SETTLE FOR MINIMAL COVER. USE INFOPROTECT'S CYBER ASSESS SOLUTION TO NEGOTIATE THE BEST POLICY TERMS."

For brokers and retail businesses looking to navigate the challenging cyber insurance market, Infoprotect's approach offers a proven methodology for turning declined risks into preferred accounts, restrictive terms into comprehensive coverage, and excessive premiums into competitive rate.

Work with us

By working with Infoprotect, insurance brokers, MGA's and insurers can improve their ability to assess and price cyber risk, which will ultimately benefit both themselves and their customers.

To find out more about how Infoprotect's **CYBER ASSESS** can transform the buying journey, making cyber insurance not just accessible but economical, drop Brad Fraser a line on **01689 487055** or at **brad.fraser@infoprotect.co.uk** or connect on LinkedIn.

BRAD FRASER, CEO
@bradfrasergo-giver

Our new website:
infoprotect.co.uk
Call us:
01689 487056
Drop us a line:
info@infoprotect.co.uk
Or grow with us on LinkedIn:
@infoprotect-uk

Infoprotect specialises in helping insurance brokers place complex cyber risks through comprehensive, industry-specific risk assessments that address underwriters' exact concerns about higher risk clients. Our cyber expertise enables us to bridge the [cyber] gap between security implementation and insurance outcomes, transforming how underwriters perceive cyber risks.

Contact us for a confidential consultation to learn more about how Infoprotect can help your organisation or your higher risk clients.

This white paper is intended for insurance brokers and retail/e-commerce businesses seeking to navigate the challenging cyber insurance market. The case examples presented are based on actual engagements, though specific identifying details have been modified to protect client confidentiality.