White Paper Financial

Infoprotect

WE BRIDGE THE [CYBER] GAP

How Cyber Risk Assessments Transform Insurability for:

Financial Institutions

White Paper | Financial

Infoprotect
WE BRIDGE THE [CYBER] GAP

Transforming Higher Risk Clients into Insurable Risks

EXECUTIVE SUMMARY

The financial services sector faces unprecedented challenges in 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 financial services firms...

BRAD FRASER, CEO
@bradfrasergo-giver

This white paper examines how Infoprotect's comprehensive **CYBER ASSESS** framework enables brokers to effectively place financial sector risks, while helping financial institutions secure broader coverage at more competitive rates.

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

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

Why Traditional Approaches Fail Financial Institutions

The Limitations of Standard Cyber Security Assessments

Financial services 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 financial institutions, where business email compromise and social engineering are primary attack vectors, this creates a critical gap in risk evaluation.

Compliance-Oriented vs. Risk-Oriented

Financial regulatory frameworks (PCI DSS, FCA requirements, 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:

- Social engineering controls
- Third-party risk management
- Authentication for high-value transactions
- Employee security awareness

Self-Attestation vs. Validated Assessment

Traditional cyber insurance applications rely heavily on self-attested questionnaires, where financial institutions 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 financial environments.

The Broker Advantage: Placing Financial Sector Risks with Confidence

Transforming Broker Capabilities for Financial Services Clients

For insurance brokers specialising in financial services, 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:

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

2. Negotiation Leverage

Armed with validated risk intelligence, brokers gain significant leverage in negotiations.

3. Client Advisory Value

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

Financial Institution Benefits: Beyond Insurance Placement

Comprehensive Value Beyond Policy Procurement

For financial institutions, Infoprotect's risk assessment delivers value :

1. Premium Reduction and Coverage Enhancement

The risk intelligence provided allows financial 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 operational resilience, FCA expectations (including SM&CR responsibilities), GDPR, and PCI DSS requirements.

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 Financial Sector Cyber Resilience

Financial institutions' cyber insurance challenges require a new approach, bridging the [cyber] gap between technical security implementations and underwriter expectations. Infoprotect's financial services-specific assessment framework provides this bridge, enabling brokers to effectively place complex risks while helping financial 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 financial 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.

For insurance brokers and financial institutions 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 rates.

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 financial institutions 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.