

Cyber Risk Assessment of the UK Insurance Industry 2021



RiskXchange

- RiskXchange provides a 360° view of the Enterprise Cyber Risk Posture using AI Machine Learning
- A simple, clear and informative dashboard enables senior executives to see in real time their Enterprise and Third-Party Cyber Risk Score position
- The underlying RiskXchange Cyber Risk Rating leverages powerful predictive analytics to measure the likelihood that an organisation will experience a breach event in the next 12 months.



RiskXchange

Approach



Colour coding of charts



Exceptional: 800-900
Highly unlikely to experience cyber incident in 12 months

Very good: 700-799
Unlikely to experience cyber incident in 12 months

Good: 600-699
Low risk of experiencing cyber incident in 12 months

Fair: 500-599
Medium risk of experiencing cyber incident in 12 months

Poor: 400-499
High risk of experiencing cyber incident in 12 months

Very poor: <400
Very high risk of experiencing cyber incident in 12 months

- The UK Insurance Cyber Risk Rating is a weighted average of the RiskXchange Cyber Risk Rating a random sample of companies split across brokers, carriers and underwriters. Based on the methodology, the higher the score, the lower the likelihood that an organisation will experience a data breach in the next 12 months
- **Target Areas** - First, raw target area scores are calculated based on a weighted sum of the underlying issues in the factor. These weights are based on issue severity, graded from low to medium, high and critical. The resulting numeric scores are translated to letter grades from **"F" to "A"** and are presented to the user on the platform, along with a list of the issues, organised by severity
- All the weighted factor scores described above are rolled into the total score which falls on a scale of **300 to 900**

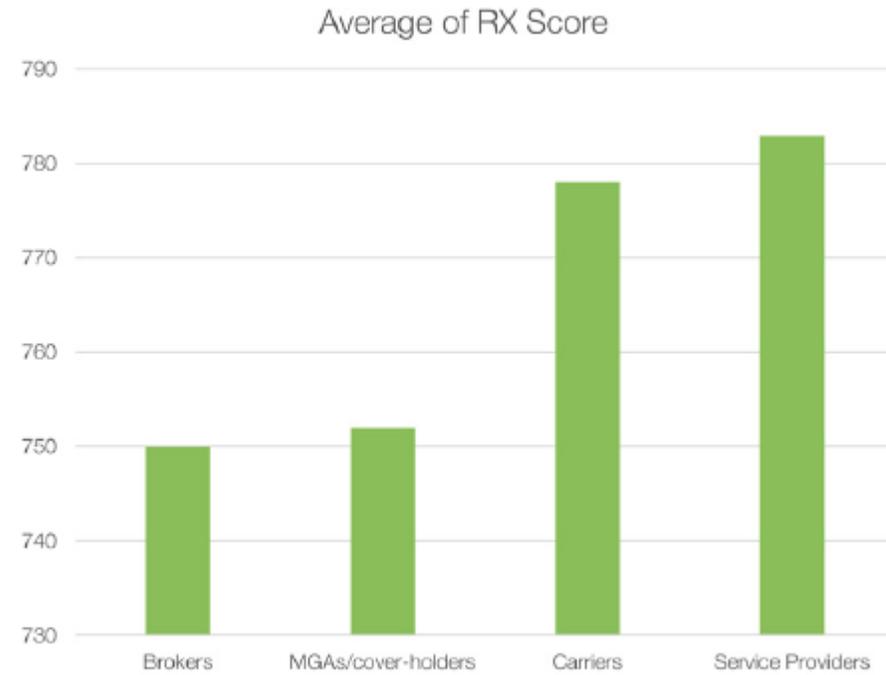


Highlights of the 2021 report

- Across the board, many insurance companies continue to exhibit weaknesses in their security operations across external attack surfaces. In many cases, firms need to go back to basics.
- A large proportion of the insurance companies surveyed have failed to implement DMARC (Domain-based Message Authentication, Reporting & Conformance) policy management, and so remain vulnerable to phishing attacks.
- Personal and/or sensitive data is being put at risk across several firms because the applications they use to collect and process this data have weak or non-existent encryption. This puts the firms at risk of confidentiality breaches as well as potential large GDPR fines or personal litigation from clients.
- While the average score for brokers has fallen slightly, from 758 to 750, several companies have significantly improved their scores—with one firm achieving an excellent score of 847.
- This year's survey includes central service providers to the UK insurance industry. The results reveal some potentially worrying long-term security vulnerabilities which, if exploited by criminals, could put the entire market at risk of a large-scale data breach.

Overall Scores

Figure 1: Overall risk score



Brokers

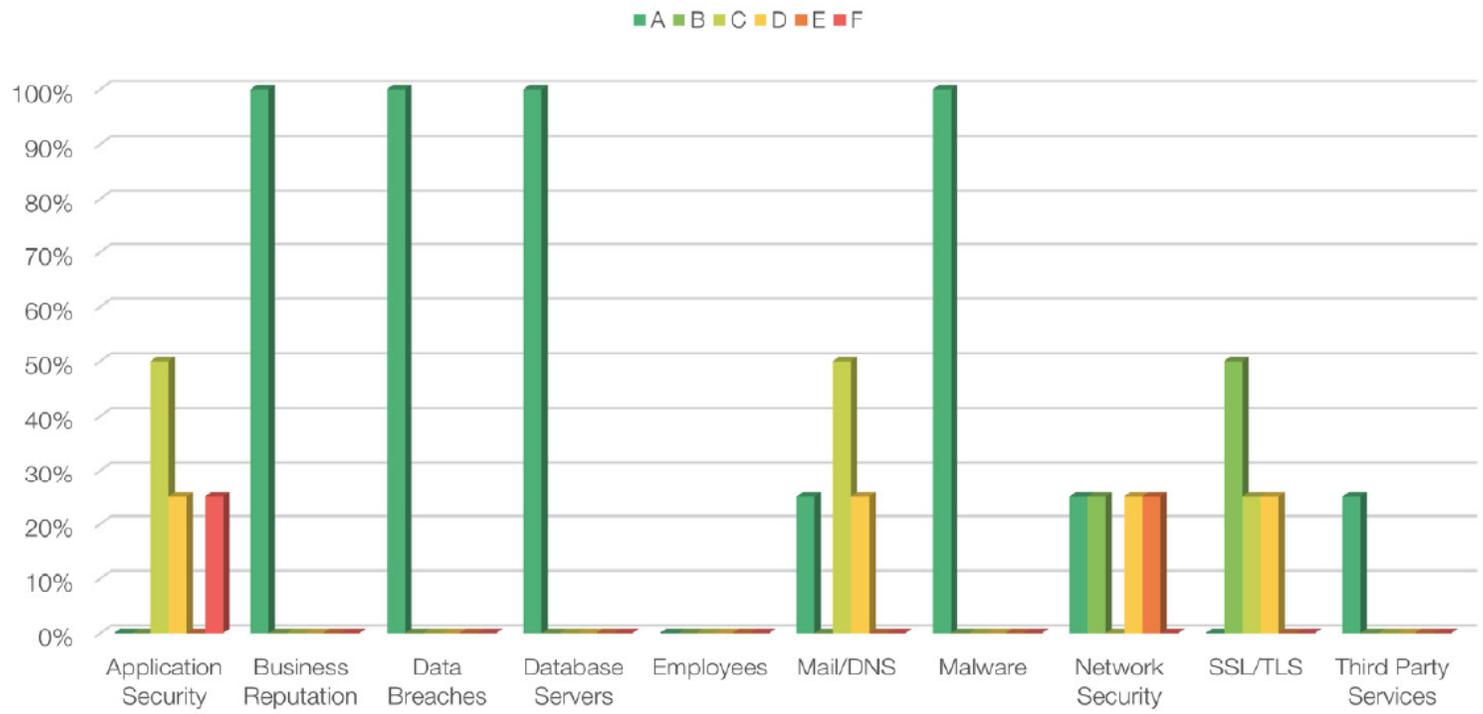
Key points:

- **54%** of brokers score a D on email security, including such issues as non-enablement of DMARC, the result of which is the exposure of email recipients to possible phishing attacks. 91% of all cyber-attacks begin with a phishing email.
- **35%** of brokers score a C when it comes to basic encryption on their websites. This could result in breaches of client data confidentiality.
- Several of the web applications used across the broker population are not correctly configured when it comes to security. Many are missing basic security headers.
- A few firms are currently collecting personal data, including passwords, without using any form of encryption, which is a direct breach of GDPR regulations.
- In other systemic risks, **20%** of the broker population is exposed to several high-risk security vulnerabilities.

Figure 5: Security grades broken down by issue type for brokers



Figure 6: Security grades broken down by issue type for MGAs/cover-holders



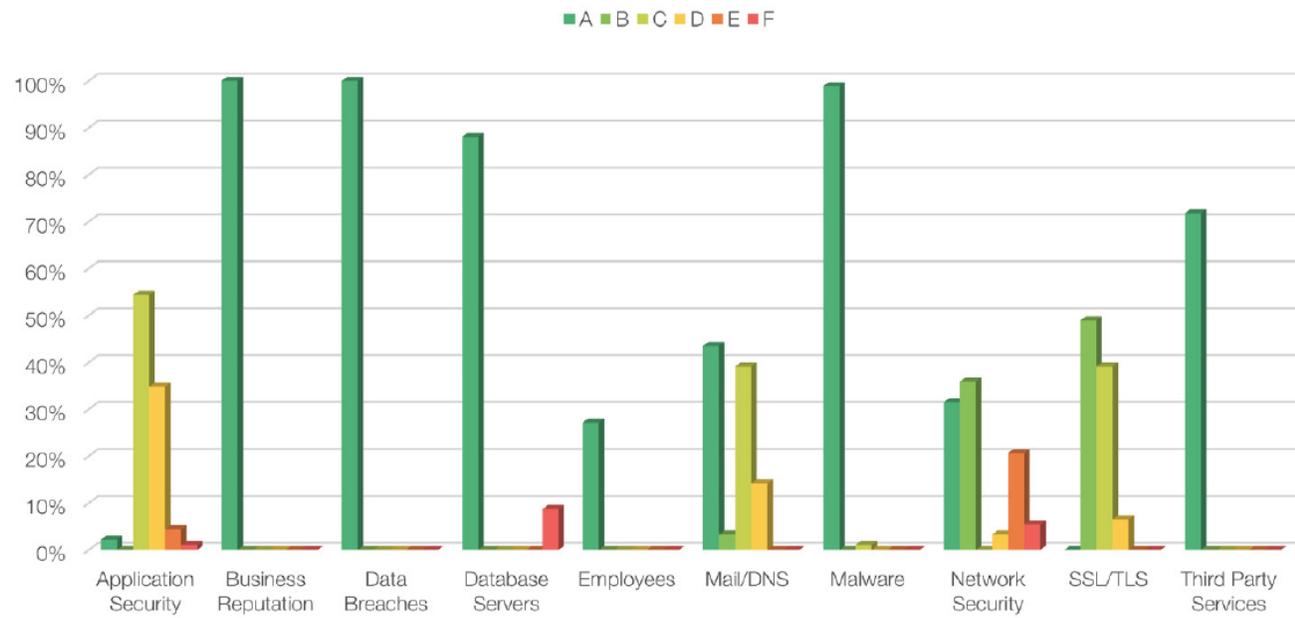
MGAs / Cover holders

Key points:

- **25%** score an C when it comes to encryption. Within the cover-holder population, we have identified several systems using encryption ciphers that are insecure
- **25%** of cover-holders with external-facing web applications score a C. This is because many of the firms are failing to install or maintain basic encryption of username and password pairs or client data collected via these web applications.
- As a systemic risk, **25%** of the cover-holder population is exposed to several high-risk security vulnerabilities.

Carriers

Figure 7: Security grades broken down by issue type for carriers



Key Points:

- **21%** of carriers score an E when it comes to network services security, caused using outdated, end-of-life versions of Apache web services.
- **39%** of the carrier firms using database services are exposing these databases to the open internet for bad actors to discover.
- **39%** of the firms with external-facing web applications score a C. This is because many of the firms are failing to install or maintain basic encryption of username and password pairs or client data collected via these web applications.
- As a further systemic risk, **12%** of the carrier population is exposed to several high-risk security vulnerabilities.

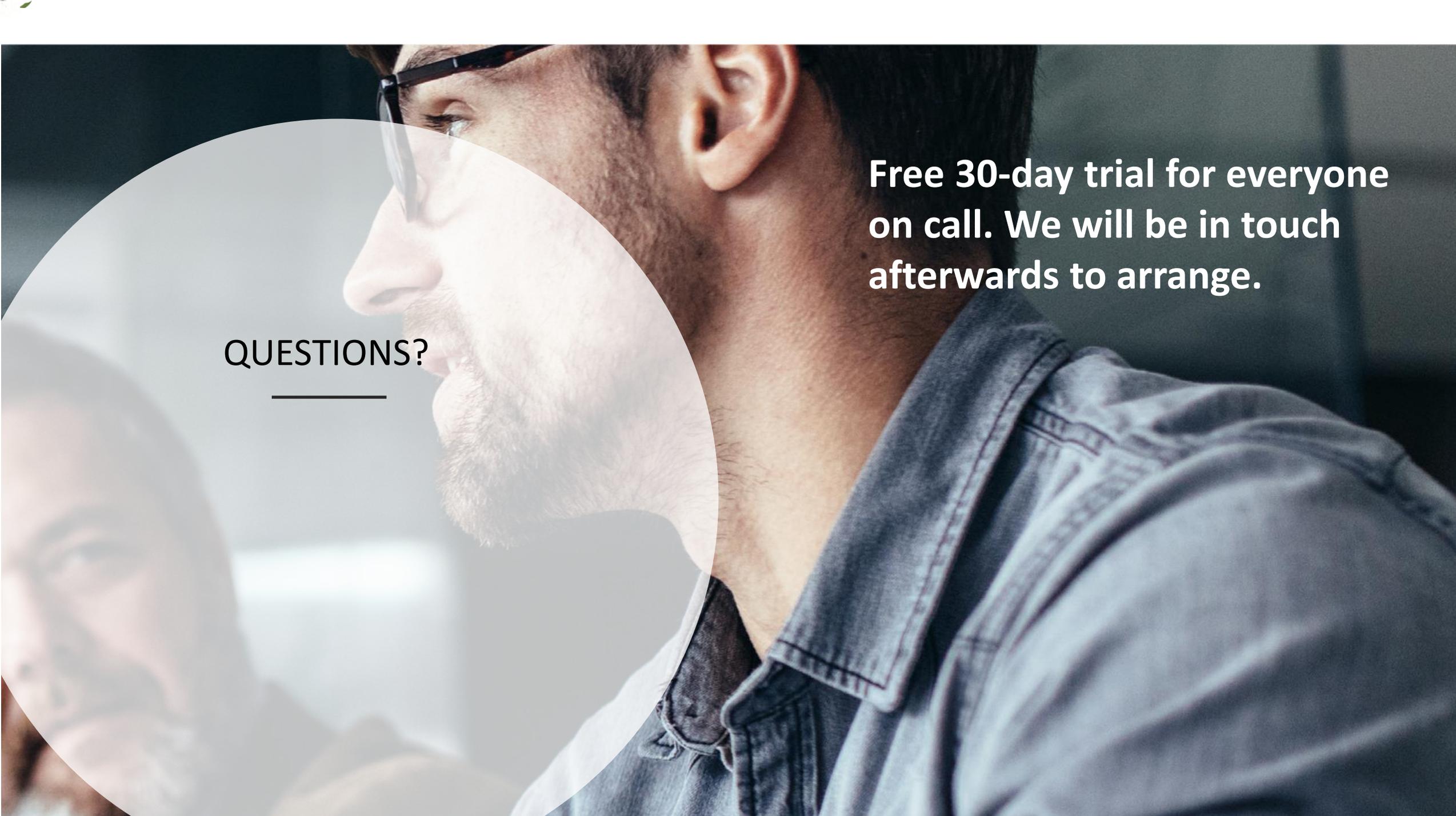
Figure 8: Security grades broken down by issue type for London-market central service providers



Service providers

Key Points:

- **31%** of service providers score an E when it comes to network security. This very low grade is because there are a few very large services providers who continue to use weak and insecure encryption methods.
- **19%** score a D when it comes to application security. This is caused by the incorrect security configuration of several the web applications used across the central service provider population, many of which are missing basic security headers.
- **63%** score a C when it comes to email security, including such issues as non-enablement of DMARC, the result of which is the exposure of email recipients to possible phishing attacks. 91% of all cyber-attacks begin with a phishing email.
- As a further systemic risk, **28%** of central service providers are exposed to several high-risk security vulnerabilities.



**Free 30-day trial for everyone
on call. We will be in touch
afterwards to arrange.**

QUESTIONS?
