northdoor
Store IT · Protect IT · Use IT

RiskXchange
AI-Enhanced Cyber Risk Management

Northdoor 2021 Cyber Risk Assessment of the UK Insurance Industry

northdoor
Store IT ◦ Protect IT ◦ Use IT ◦

Contents

3 Welcome

4 Introduction

5 Why This Matters: a Real-World Breach

7 Highlights of the 2021 Report

8 The UK Insurance Industry Cyber Risk Ratings 2021

15 The RiskXchange Cyber Risk Ratings

16 Methodology

18 Recommendations

19 About Us

Welcome

The tumultuous events of 2020 created significant opportunities for cybercriminals: the explosive growth in working from home brought millions of new endpoints into UK corporate networks and dramatically increased the scale of the challenge for those tasked with managing cybersecurity.

In this second annual survey of the cybersecurity readiness of the UK insurance industry, Northdoor and RiskXchange have again used the RiskXchange Cyber Risk Rating platform to benchmark a representative sample of companies. As before, the goal of the report is to help companies within the UK Insurance industry understand how they stack up against their peers in terms of cybersecurity maturity.

This year's report includes for the first time London-market central service providers, in recognition of the fact that many insurance companies operating in the London / Lloyd's market use the same third-party technology platforms to run business services. Clearly, this creates a systemic risk in the shared supply chain—any breach of cybersecurity at a central service provider could quickly ripple through large numbers of insurance firms, exposing them in turn.

The RiskXchange ratings, based on readily available public open-source data, represent an aggregate measure of security risk across brokers, MGAs/cover-holders, and carriers within the UK insurance industry. The ratings should be treated as just one element within a broader cyber-risk identification and assessment programme, which can help monitor organisational and third-party risks.

The report is designed to augment your organisation's existing risk-management plans, and includes advice on how to build on existing cybersecurity strategies and practices to reduce the risk of breaches.

We trust that you will find value in the 2021 Cyber Risk Assessment of the UK Insurance Industry report, and we look forward to helping you assess and improve your organisation's cyber-risk posture.

Darren Craig
CEO
RiskXchange

AJ Thompson
CCO
Northdoor

Richard Jefferies
Insurance Client Manager
Northdoor

Introduction

Information security is a field in which dialogue is often focused on absolutes; after all, responsible organisations surely strive for perfect security. As a result, business leaders have grown to think of security in black and white terms as something they either have or lack. But as with most other complex, multifaceted disciplines, security is relative and perfect security is, in fact, unattainable. Risk is a factor of the threat landscape and vulnerabilities. The scope and severity of the risk that organisations face depends on many interrelated and constantly changing factors, some of which are under the control of the organisation, while many others are not.

Risk exposure

It is common to think about cybersecurity solely in terms of technology. While technology is indeed an important component of cyber risk mitigation and cyber defence efforts, a more holistic view takes into consideration the human factor and the risk-management strategies and processes. Every day, organisations are exposed to risks that are largely dependent on the nature of the businesses they run, the assets under their control, and the data they require to function.

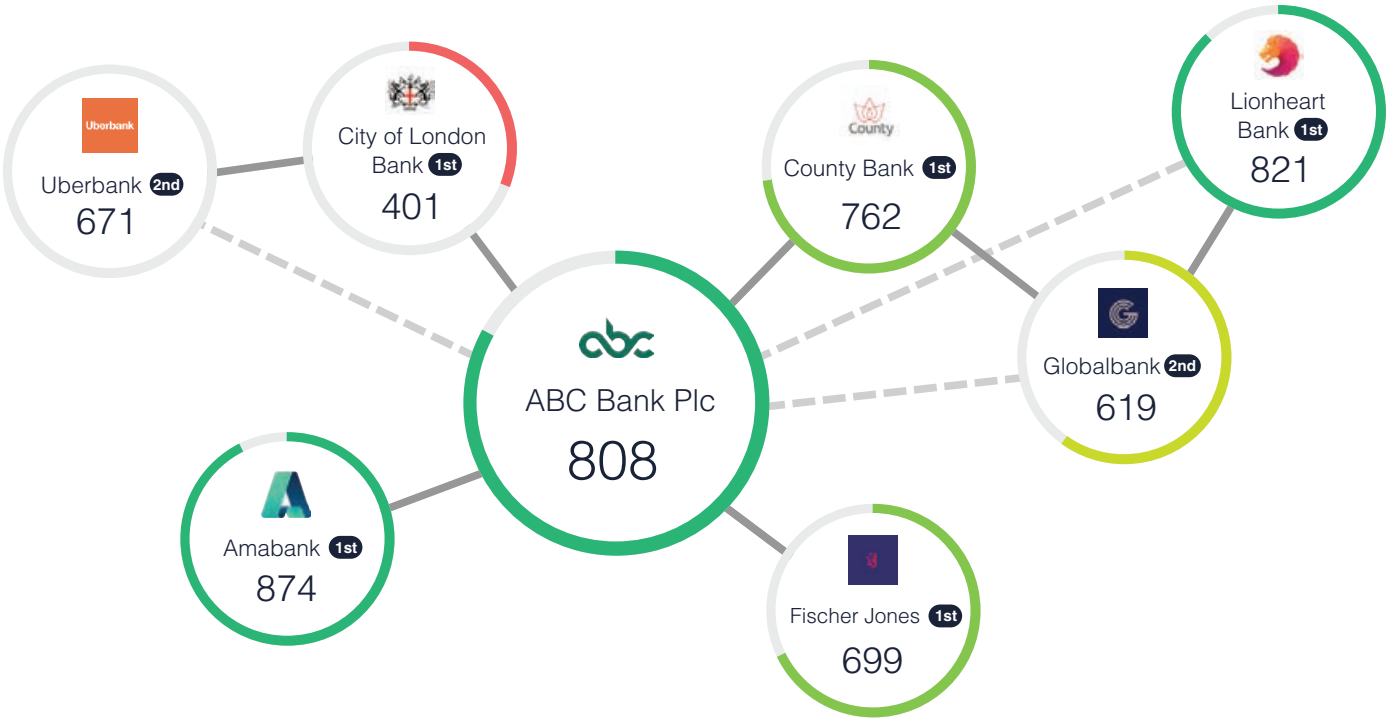
Protecting against cybersecurity risks is tough enough when it comes to just the systems and data on the internal network. Expanding the view to encompass all the connected business partners—and the long chain of other third parties that those companies work with—makes the challenge significantly greater.

In addition, a relatively new class of systemic risk has emerged from the widespread adoption of shared cloud-based services to replace locally installed and managed business services. A cybersecurity attack against a shared services provider therefore has the potential to expose multiple organisations—even entire industries—to the risk of data breaches, damage, or loss.

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, helping them to make informed and measureable business risk decisions.

The RiskXchange platform enables the centralised sharing of risk score data upstream and downstream for simple, one-to-many exchange of cyber risk data.



Supply chain security risk

The systemic supply chain security risk inherent in shared cloud-based services is not merely a theoretical scenario. During 2020, the UK insurance industry faced the risk of disruption from a real-world malware incident suffered by Xchanging, a major UK-based global supplier of technology-enabled business services and Lloyd's market shared services.

In this incident, a cybercriminal accessed Xchanging's systems two days before launching the attack, using a publicly available security testing tool to create a backdoor in Microsoft Windows and install malware. Once activated, the malware encrypted files, and the cybercriminal invited Xchanging to negotiate a ransom payment to unlock them. Unwilling to negotiate or make any payment, Xchanging swiftly notified the relevant authorities and set to work on shutting the attack vector and recovering the affected systems.

Diligence averts major incident

It was fortunate that the attack took place on a Saturday, buying Xchanging time to resolve the situation before the Monday re-opening of its clients' London insurance offices. The security team was able to isolate and neutralise the threat without any damage to data, so that Xchanging was able to serve its clients as normal the following week.

Thanks to Xchanging's vigilance and speed of response, there was no broader impact on the UK insurance market. Emsisoft research suggests that the average downtime associated with critical systems hit by ransomware attacks is 16 days. When the next attack on a supplier of shared services to the insurance industry takes place, can the industry be sure that the victim will be as diligent and responsive as Xchanging? If the next shared services provider to be hit by malware is less well prepared, the industry would potentially be facing enormous damage.

The Xchanging incident neatly illustrates the way in which cybersecurity risks can extend beyond the boundaries of each organisation. The inclusion of shared service providers in this year's survey should help the UK insurance industry to understand its exposure to risk from this part of the landscape.

Manage what you measure

Businesses best manage activities that can be measured effectively. Maximising the cyber-security posture of an enterprise depends on the ability to understand and manage the trade-offs in a landscape of constantly evolving threats. This, in turn, requires companies to balance the relative risks and rewards of investments in security.

Based on the RiskXchange Cyber Risk Rating, the Cyber Risk Assessment of the UK Insurance Industry is intended to advance cyber-security awareness within the UK insurance industry and to improve the overall effectiveness of cyber-defence programs using observable risk signals and other factors. It is important to emphasise that a lower score, whether for a company or a sector, does not necessarily imply that insufficient diligence is being applied by the entity or entities in question. Any such entities simply have a higher risk profile; that is, they face greater risk of breach.

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 by looking at internet-facing assets for weaknesses such as outdated software and exposed data or devices, among other key data signals, which are collected using passive data-gathering methods across a range of compiled sources. It should be noted that certain internal security-risk management programmes and other compensating controls which increase the security of a firm's data are not assessed and therefore not quantified in this rating.

Correcting the issues identified by this data gathering, however, will help reduce an organisation's exposure to external threats. As a result, the Cyber Risk Assessment of the UK Insurance Industry report includes recommendations to help all information-security professionals to drive down the risk of an incident involving internet-facing assets.

The UK Insurance Industry Cyber Risk Ratings

Analysis

The UK Insurance Cyber Risk Rating is a weighted average of the RiskXchange Cyber Risk Rating for 159 companies in the UK insurance industry split across brokers, MGAs/cover-holders, carriers, and central service providers. 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. Conversely, a lower score indicates greater risk of a successful data breach, based on years of historic breach data and expert analysis.

The RiskXchange score is produced and presented in two ways:

Target area scores

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, as well as each company's digital footprint and industry. The resulting numeric scores are translated to letter grades from "F" to "A".

Overall Score

All the weighted factor scores described above are rolled into the total score which falls on a scale of 300 to 900. Please note that even companies with great cybersecurity programs can still get hacked. Please also note that scoring, as described above, is a data-driven process that ensures that lower scores are always more predictive of breach than higher scores. Put simply, an "F" company has a higher likelihood of getting breached than an "A" company, which is why action should always be taken if the overall score of a company is low.

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.
- The average cover-holder score has fallen slightly, and the highest-achieving firm in this category achieves only 810 points out of 900.
- Scores among carriers have increased overall, with the average rising from 764 to 778. One exceptional carrier came in just two points shy of perfection at 898. However, there are still several carriers who need to better secure their public-facing digital footprints and work harder to improve their security operations.
- This year's survey includes central service providers to the London insurance market. 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.
- Still on the topic of central service providers, the past year saw a large rise in companies using Microsoft services such as Office 365—a trend not only within the insurance industry, but also across other areas of financial services. This growth creates a larger systemic risk around resilience and data availability within the London / Lloyd's insurance market.

Colour coding of charts

Exceptional: 800-900	Very good: 700-799	Good: 600-699	Fair: 500-599	Poor: 400-499	Very poor: <400
Highly unlikely to experience cyber incident in 12 months	Unlikely to experience cyber incident in 12 months	Low risk of experiencing cyber incident in 12 months	Medium risk of experiencing cyber incident in 12 months	High risk of experiencing cyber incident in 12 months	Very high risk of experiencing cyber incident in 12 months

Figure 1: Overall risk score

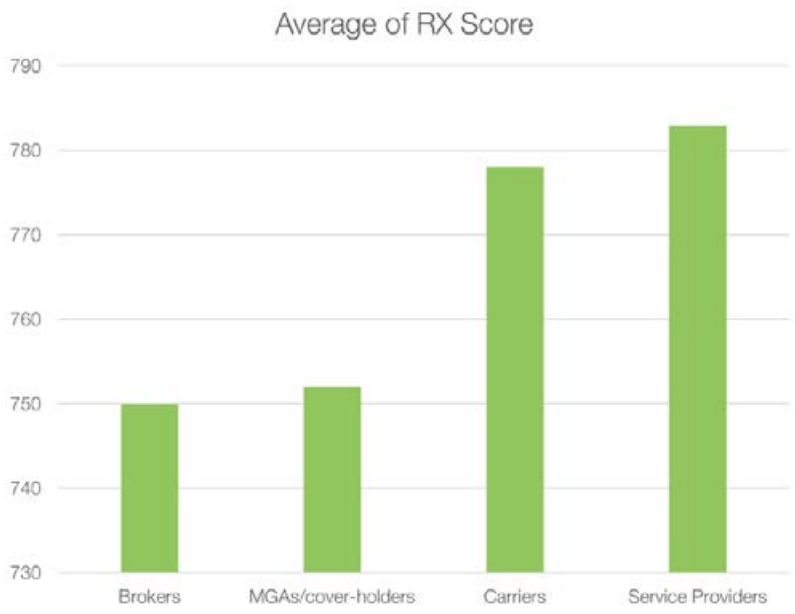


Figure 2a Overall scores broken down by brokers and MGAs/cover-holders

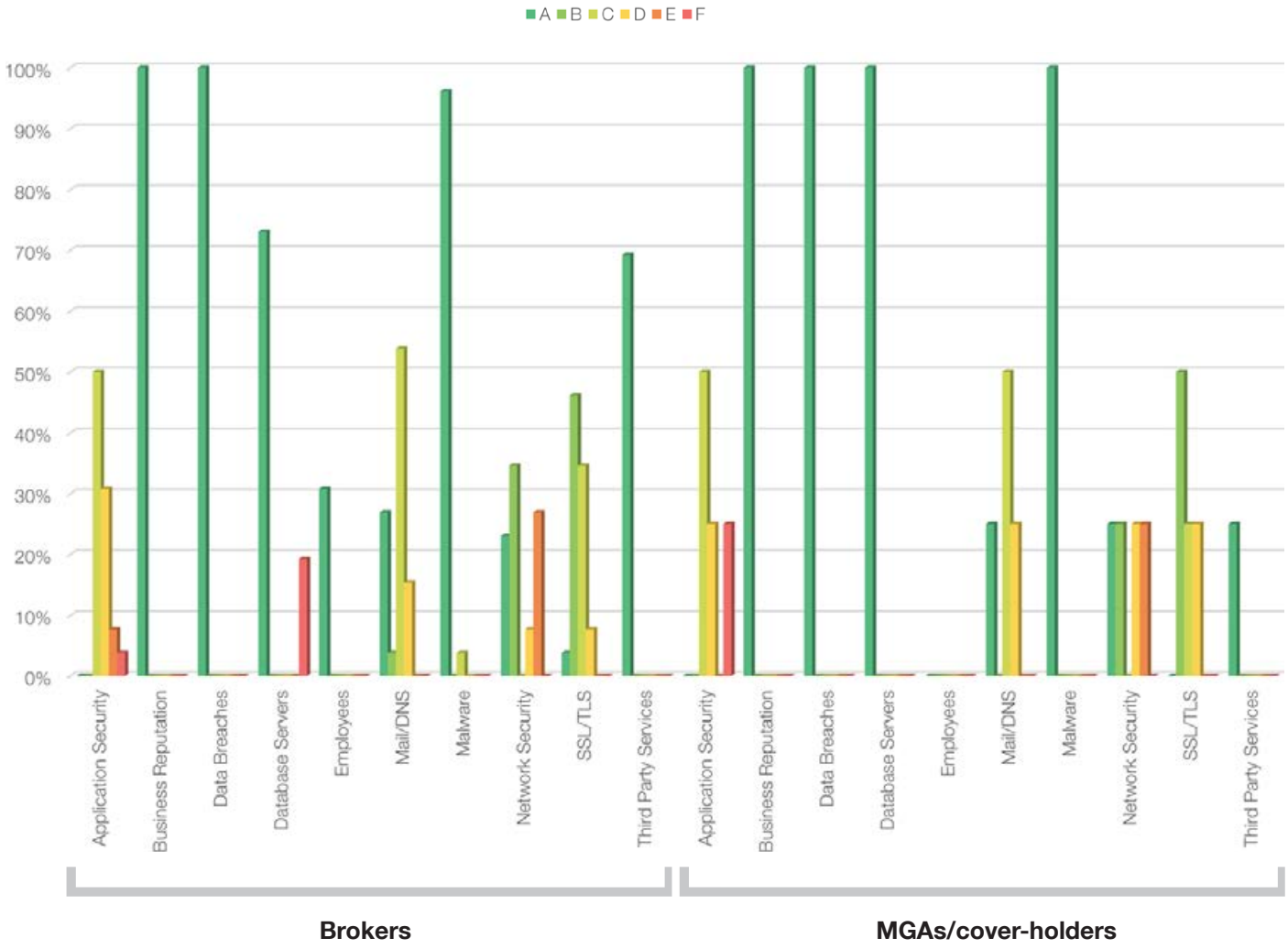


Figure 2b Overall scores broken down by carriers and central service providers

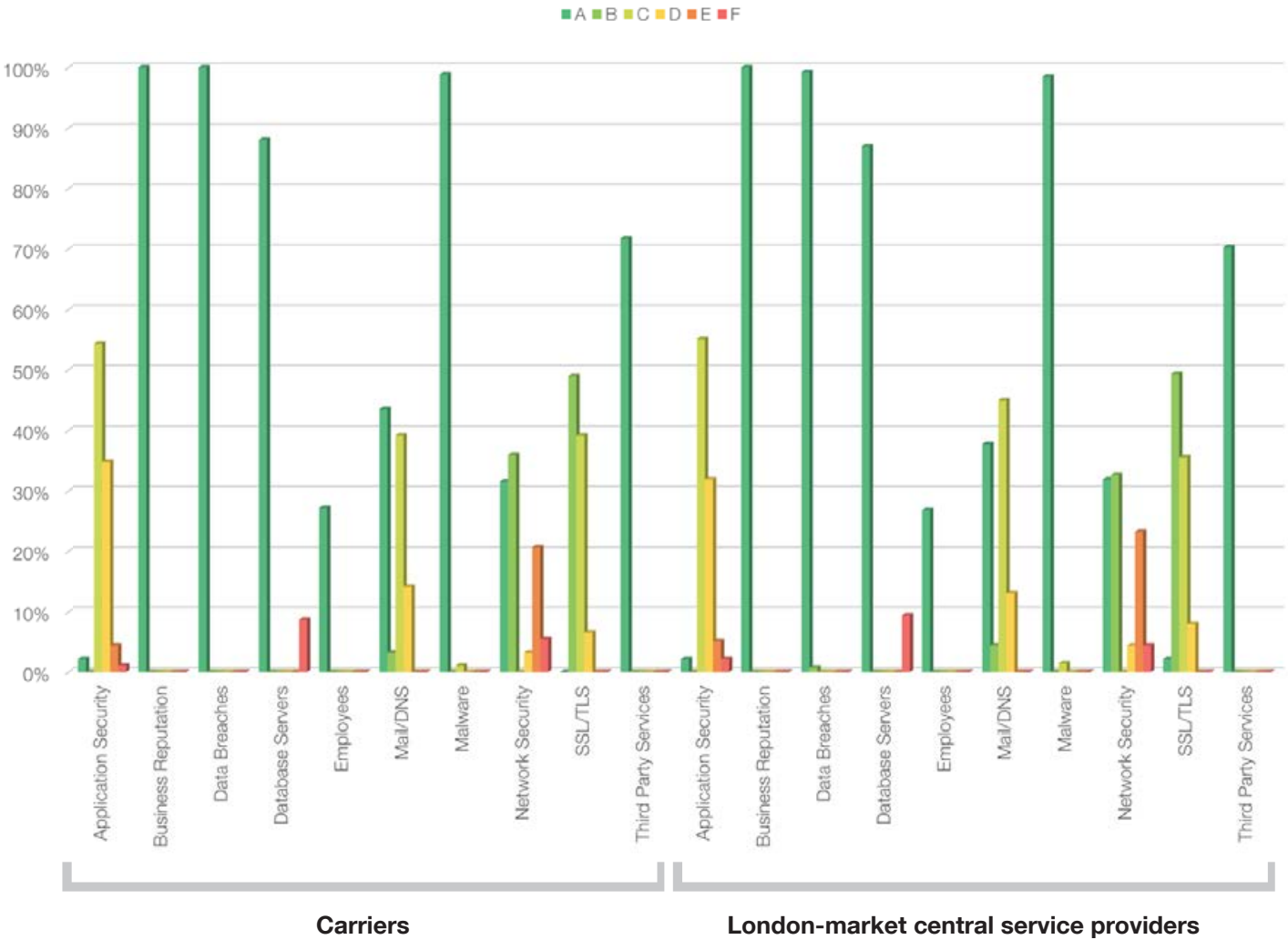


Figure 3: Security grades broken down by issue type for all firms

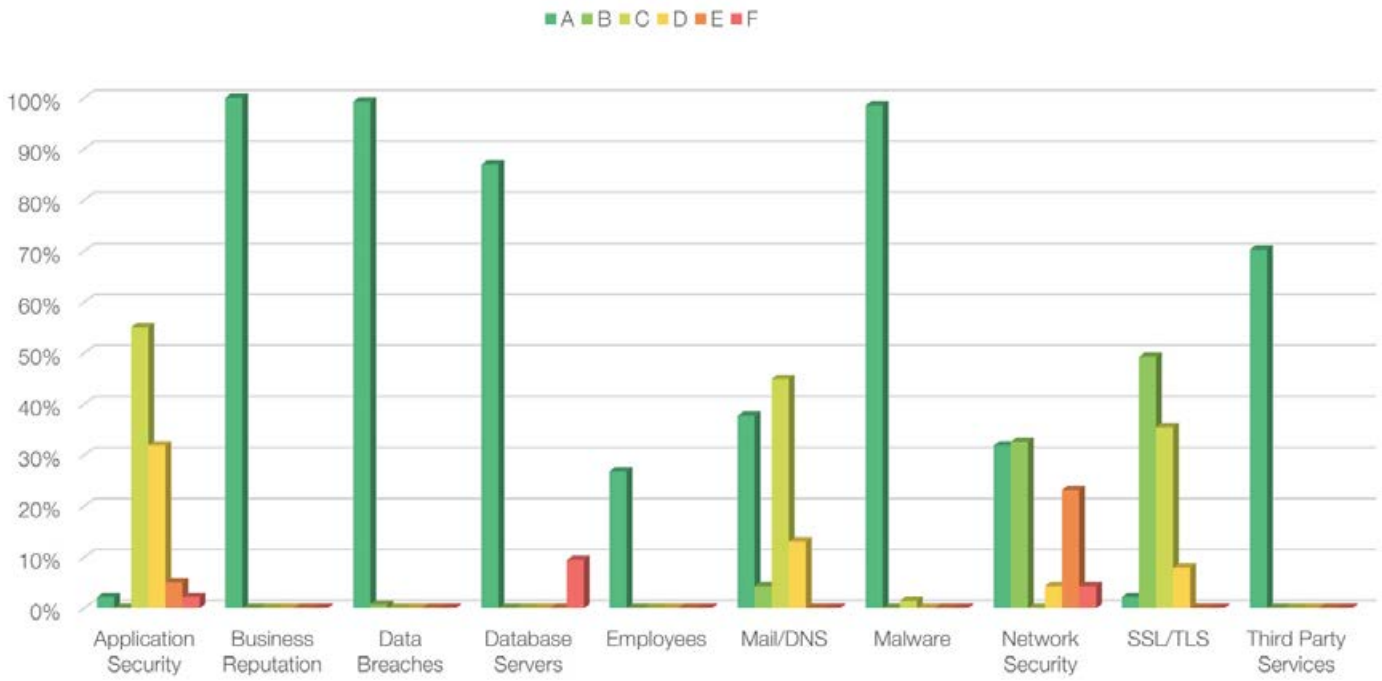


Figure 4: Security grades for each organisation type (broker, MGA/cover-holder, carrier, London-market central service provider)

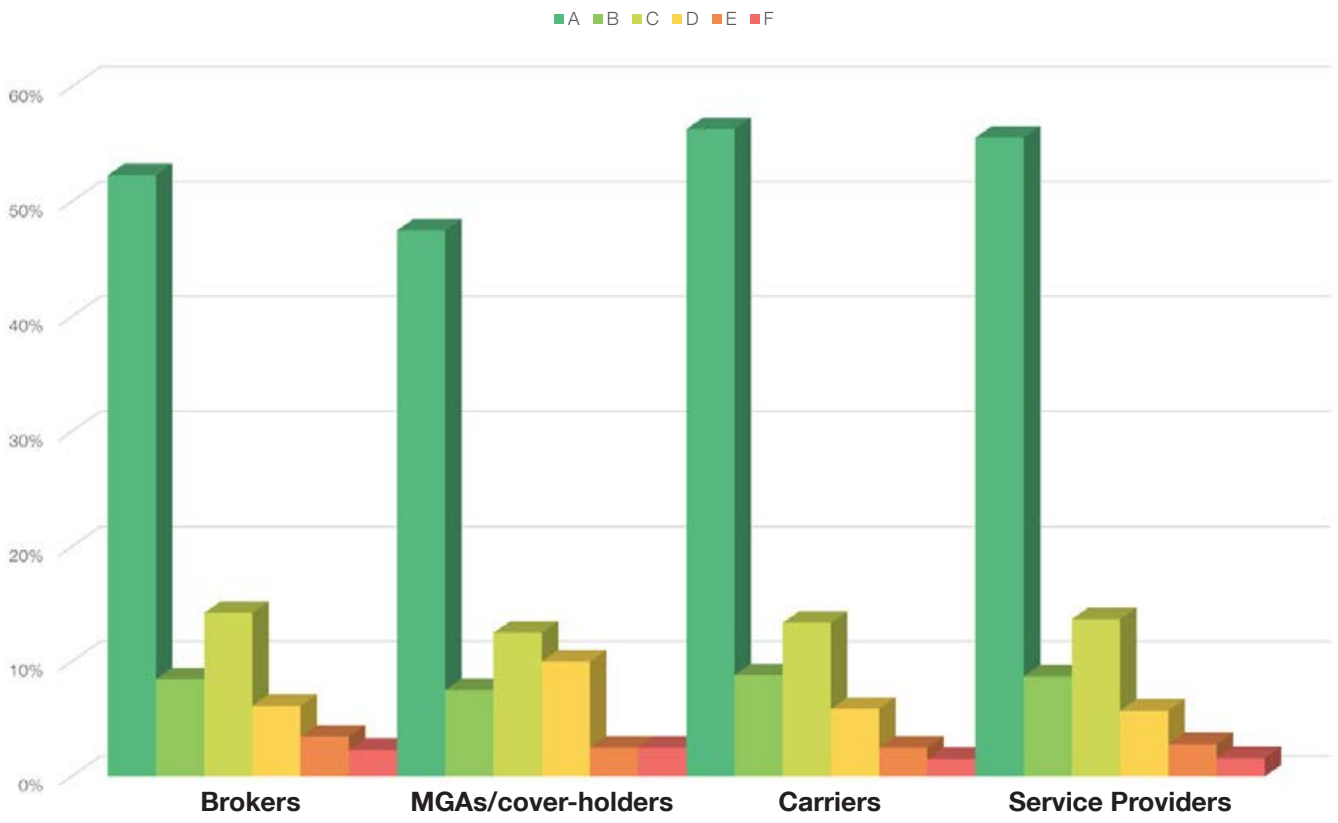


Figure 5: Security grades broken down by issue type for brokers

- This year, the average RiskXchange score among brokers is 750 out of 900, with sampled firms' scores ranging from 513 to 847. Those brokers with scores of around 500 are putting their firm's and clients' data at risk of security breaches through external-facing systems within the next 12 months.
- 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 UK GDPR regulations.
- 50% of broker firms surveyed are using Microsoft Office 365 services, highlighting a potential systemic resilience issue within the community.
- In other systemic risks, 20% of the broker population is exposed to the following security vulnerabilities:
  - » CVE-2010-12783—a high-risk issue that can result in SPA/NTLM authentication bypass.
  - » CVE-2010-3972—a high-risk issue that affects Microsoft ISS server and allows an attacker to execute arbitrary code or create a denial of service to the applications running on that server.
  - » CV-2010-2730—a high-risk issue that affects Microsoft ISS server and allows an attacker to execute arbitrary code on the server in question.

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

- This year, MGAs/cover-holders have an average RiskXchange score of 752 out of 900, with the scores of sampled firms ranging from 700 to 810.
- 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 (for number of reasons including protocol support, key exchange and cipher strength, or a combination of these). Weak ciphers can allow a bad actor to gain access to a firm's company-confidential or client-personal data.
- 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 the following security vulnerabilities:
  - » CV-2010-2730—a high-risk issue that affects Microsoft ISS server and allows an attacker to execute arbitrary code on the server in question.
  - » CVE-2010-3972—a high-risk issue that affects Microsoft ISS server and allows an attacker to execute arbitrary code or create a denial of service to the applications running on that server.

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

- This year, carriers have an average RiskXchange score of 778 out of 900, with the scores of surveyed firms ranging from 622 to a near-perfect 898. Carriers with a score of around 600 are putting their firm's data and their clients' data at risk of security breaches through their external-facing systems within the next 12 months.
- 21% of carriers score an E when it comes to network services security, caused by the use of 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.
- 33% of the carrier population is using a mix of Microsoft Office 365 and/or Skype services, highlighting a potential resilience issue if Microsoft were to have an outage.
- As a further systemic risk, 12% of the carrier population is exposed to the following security vulnerabilities:
  - » CV-2010-2730—a high-risk issue that affects Microsoft ISS server and allows an attacker to execute arbitrary code on the server in question.
  - » CVE-2010-3972—a high-risk issue that affects Microsoft ISS server and allows an attacker to execute arbitrary code or create a denial of service to the applications running on that server.

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

- This year, London-market central service providers have an average RiskXchange score of 783 out
  of 900, with the scores of surveyed firms ranging from 615 to a near-perfect 898.
- 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 a number of 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.
- 50% of central service providers to the London insurance market use Microsoft Office 365 services, highlighting a potential systemic resilience issue.
- As a further systemic risk, 28% of central service providers are exposed to the following security vulnerabilities:
  - » CV-2010-2730—a high-risk issue that affects Microsoft ISS server and allows an attacker to execute arbitrary code on the server in question.
  - » CVE-2010-3972—a high-risk issue that affects Microsoft ISS server and allows an attacker to execute arbitrary code or create a denial of service to the applications running on that server.

A note about risk

Risk is a function of both the threat landscape and vulnerability. The ratings reflect the probability of a data breach. A low rating does not imply that an organisation is destined to suffer a data breach. Similarly, a high rating does not indicate that an organisation is impervious to the risk of a breach—it simply implies a lower likelihood that the organisation will experience a breach.

Organisations that wish to understand their individual Risk Ratings in more detail are encouraged to contact us for a detailed report that can act as the basis for:

- Objective self-assessment
- Third-party and supply chain risk assessment
- Comparative assessments (between organisations or over time).

The RiskXchange Cyber Risk Ratings

The RiskXchange Cyber Risk Ratings are an empirically derived set of metrics that rely on a comprehensive and diverse set of cyber-security risk signals, collected at internet scale, to measure the forward-looking security risk of any organisation.

Security ratings give a calculated assessment of an organisation's effectiveness on all aspects of security performance. Ratings draw upon a range of data to analyse and inform, ultimately enabling organisations to objectively review and act upon their processes and the security measures they have in place. What is more, the ratings help to identify challenges and opportunities to make improvements.

A up-to-date security-risk rating enables better management of an organisation's cyber risk, delivering:

- Insight into risks associated with third or fourth parties and supply chain relationships. When a security rating is in place, it can significantly aid the effective management of cyber risk from external parties.
- Better transparency to help insurance underwriters in the assessment, calculation and risk management of security processes and performance.
- Enhanced cyber-security due diligence, which is hugely important during periods of business growth, including the acquisition of or investment in a company. Organisations must be able to access enhanced information and continually review any investment; access to a security rating facilitates this.
- Improved insight into Critical National Infrastructure (CNI) for governments, ultimately enabling better management of national cyber-security performance.

What's more, security ratings also aid the ongoing management of an organisation's internal cyber activity, including risk and compliance. In this domain, a rating enables:

- Rolling assessments of internal security activity, helping to provide clarity to a range of stakeholders.
- Industry-wide benchmarking, including peer-to-peer and competitor.
- Greater customer confidence in the organisation's digital presence and activities. This higher level of confidence impacts other organisations with vested interests including third parties, stakeholders and industry regulators.

Methodology

The UK Insurance Industry Cyber Risk Rating is an aggregate measure of security risk across insurance brokers, MGAs/cover-holders, carriers, and shared service providers ranging from small to large enterprises within the UK economy.

The RiskXchange security ratings are based on vast aggregated data sets that are constantly updated from a wide range of sources 24 hours a day. RiskXchange looks beyond routine techniques, such as limited-scope penetration testing, instead utilising data, insights, and other valuable indicators—generating ratings that are objective and ready to action. The ratings take advantage of external data, sourced from around the globe, that has been cross-referenced against risk assessment-as-a-service (RAaaS) datasets.

RiskXchange maps its findings to individual organisations. By collecting terabytes of information and allocating it across 21 categories including security configuration, operational-security hygiene, user behaviour, discovered parties, dark-web disclosure, data breaches, business reputation, network security and risk-management procedures, data is placed into a hierarchy reflecting the extent of the risk it represents to organisations. Finally, this information is used as the basis to calculate a security rating.

Included businesses

The UK insurance businesses included in the report are part of a rotating panel selected from a range of online sources using a sample design.

Sample size

159 companies.

Recommendations for reducing security risk and raising ratings

Reducing security risk is both a science and an art. An organisation's security posture is subject to evolving threats and the technology that supports the security posture. It is also dependent on the diligence, skill and adaptability of the people who manage it. In addition, an organisation's security posture can be impacted by the actions of the users who depend on the technology that underpins the business functions.

For every technology asset that an organisation deploys to enhance its security, there are multiple ways in which the same organisation might act to inadvertently undermine the effectiveness of the asset through inadequate training, processes, or maintenance. The discussion below focuses on some of the key aspects of security risk that can be measured by the broader RiskXchange platform but have not been documented in this report.

Measuring risk

In the case of security scores or ratings, in which the primary goal is measuring risk, it is neither feasible nor advisable to look only at exploitable technical flaws. Assessing risk must also include measuring noncausal conditions that are associated with behaviour, rather than simply cataloguing technical flaws. As we consider ways to reduce risk, the formula for issue remediation may be complicated and will likely involve the interpretation of measurements to uncover the root causes of risk. This is especially true when measurements imply problems with policy, skills, and personnel, rather than simply the presence (or absence) of a technical condition.

In short, managing security risk in the world of cybersecurity is about managing behavioural risk and skills gaps as well as technical flaws. Cybersecurity is a technical challenge, but one that is both enabled and constrained by humans.

The seven recommendations detailed overleaf provide guidance that will help organisations improve their security posture and better protect sensitive data.

Recommendations

1. Use the NIST Cybersecurity Framework (or an equivalent framework) to develop an information security program. The framework enables organisations—regardless of size, risk profile or cyber sophistication—to develop a cyber security plan or improve an existing one.
2. Develop a reliable understanding of your own network. This includes identifying assets to apply security management based on risk.
3. Identify functions and teams whose process and policy maturity are underperforming. This will enable you to identify weak links in technology, personnel, policy and leadership.
4. Oversee your organisation's network team to confirm alignment to the details of network management policies. Avoid unnecessarily exposing network infrastructure assets and ensure correct configuration for those that need to be exposed.
5. Protect and monitor network endpoints. Organisations that monitor endpoints are able to provide an early warning of potential problems.
6. Develop a process to confirm that active certificate-management programs are in place and are being implemented.
7. Develop a process to confirm that all assets are fully patched and are upgraded with the latest supported versions of their software.

About RiskXchange

RiskXchange is a global cyber-risk ratings and cyber-risk analysis platform. RiskXchange provides a simple, automated, and centralised risk management solution that enables organisations manage their own cyber risk score as well as ensuring their suppliers and third-party partners meet their security policy and GDPR requirements.

RiskXchange uses powerful machine-learning capabilities to map an enterprise's ecosystem and determine the 360° cyber risk rating score and posture of multiple degrees of relationships to the prime enterprise. This information is also very beneficial in providing visibility of the industry average cyber-risk score and peer benchmarking for competitive advantage.

About Northdoor

Northdoor plc is a corporate IT consultancy firm with more than 30 years of experience in serving blue-chip businesses. We apply our knowledge and expertise to help businesses capture, manage, protect, and analyse large volumes of commercial data. Our solutions help enterprises across all sectors gain clear strategic insights and reinforce their competitive advantage.

Northdoor's core business and IT management consultancy services cover the entire data journey from acquisition to archival or disposal. Our long-standing client relationships in the insurance and financial markets industries mean that we have a strong understanding of the regulatory and compliance frameworks.

The Northdoor Store IT offering helps our clients ensure that their data is stored in an efficient and performant way. Within Store IT we have two areas: Cloud, and Systems and Storage. We assist clients with Public Cloud, Private Cloud, Hosted and on-premises solutions, or a hybrid combination of these. Our consultancy-led approach ensures our clients get the right solution for their needs.

The Northdoor Protect IT offering is our Security specialism. We help clients secure their data within their enterprise and also when shared with third parties, ensuring that clients can fully exploit their data assets without compromising their or their clients' security.

The Northdoor Use IT offering is all about exploiting data assets to achieve competitive advantage. Within our Big Data and Analytics specialism, we provide the capability to gain genuine business insight from large data sets. In our SQL and BI practice, we help our clients efficiently use their structured business data, and in our Collaboration and Productivity practice we provide solutions that manage data workflows.

northdoor
Store IT ◦ Protect IT ◦ Use IT

Take the next step

To gain visibility of your enterprise's 360° cyber-risk score, please register to become a member of the RiskXchange platform.

To register, please contact: info@northdoor.co.uk