northdoor

◦ Store IT ◦ Protect IT ◦ Use IT ◦

RiskXchange

AI-Enhanced Cyber Risk Management

# Cyber Risk Assessment of the UK Charity Sector

## Contents

## Welcome

Managing the risk of cyber threats and reducing the impact of breaches continues to be a top priority for UK organisations of all sizes, from charities and non-profits to FTSE 100 corporations. Today, UK organisations are managing cyber risk by adopting best practices, continuously improving cybersecurity and implementing government standards such as Cyber Essentials.

Northdoor and RiskXchange have partnered to produce this Cyber Risk Assessment of the UK Charity Sector, powered by the RiskXchange Cyber Risk Rating platform. To help charities manage what they measure, RiskXchange is offering complimentary subscriptions that allow any organisation to receive its individual RiskXchange Cyber Risk Rating and associated detailed reports.

The goal of the report is to provide a transparent and easy-to-understand benchmark to measure the UK charity sector's ability to protect customer data from the vast range of cybersecurity threats.

The RiskXchange ratings, based on readily available, public open-source data, represent an aggregate measure of security risk across a sample of organisations within the UK charity sector. The ratings should be seen as one component within a broader cyber-risk identification and assessment programme, which can help monitor organisational and third-party risks.

This report is designed to augment your organisation's existing risk-management plan. Our analysis will explore how charities can build on existing cybersecurity strategies and practices to reduce the risk of breaches by optimising the use of people, processes and technology.

We trust that you will find value in the Cyber Risk Assessment of the UK Charity Sector 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

## 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.

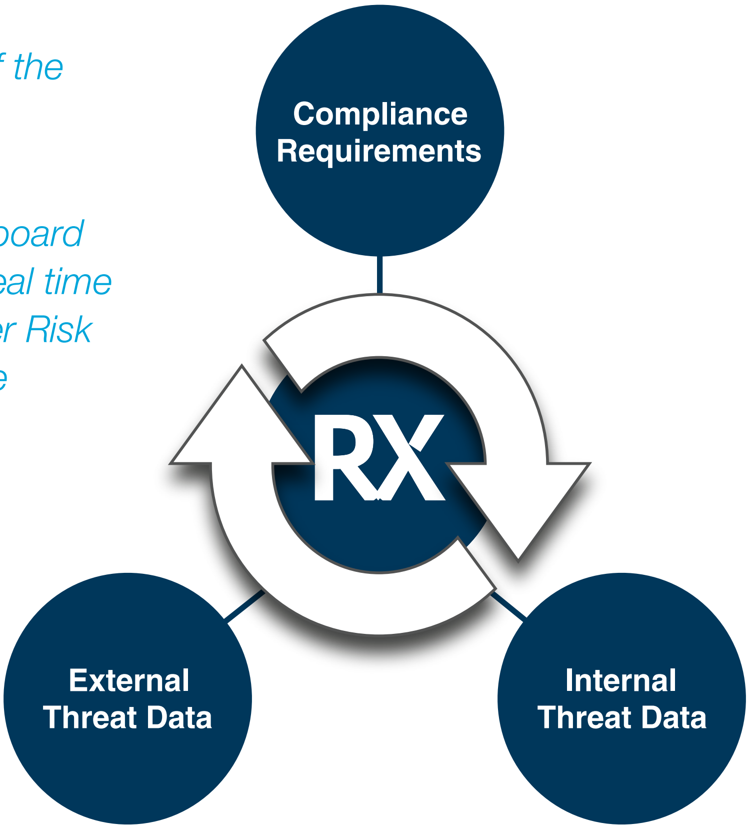
## Risk exposure

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.

*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.*



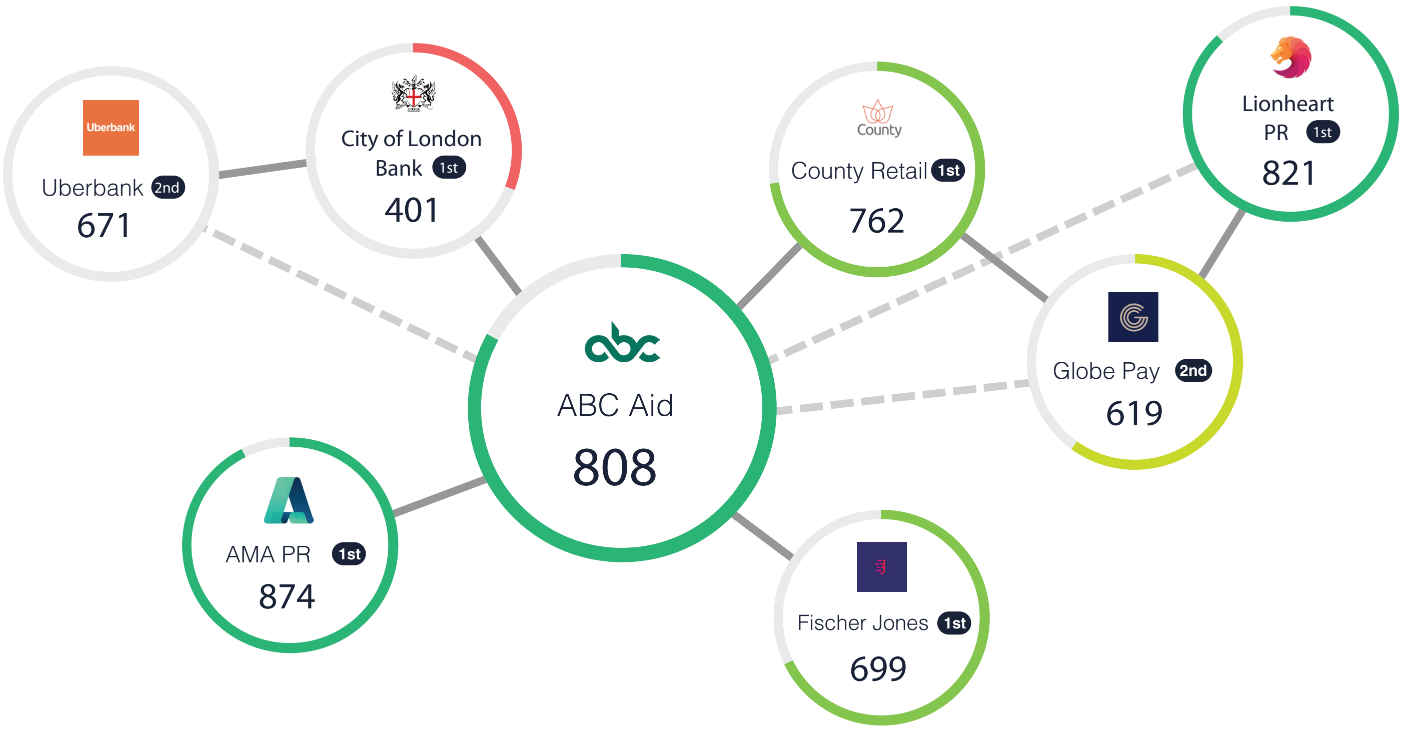
## Manage what you measure

Organisations best manage activities that can be measured effectively. Maximising the cyber-security posture of an organisation 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 Charity Sector is intended to advance cyber-security awareness within the UK charity sector 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 single organisation or an entire 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 Charity Sector report includes recommendations to help all information-security professionals to drive down the risk of an incident involving internet-facing assets.



## The UK Charity Sector Cyber Risk Ratings

### Analysis

The UK Charity Sector Cyber Risk Rating is a weighted average of the RiskXchange Cyber Risk Rating for 200 companies in the UK charity sector. 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 organisation's digital footprint and industry. The resulting numeric scores are translated to letter grades from "F" to "A".

### Overall Score

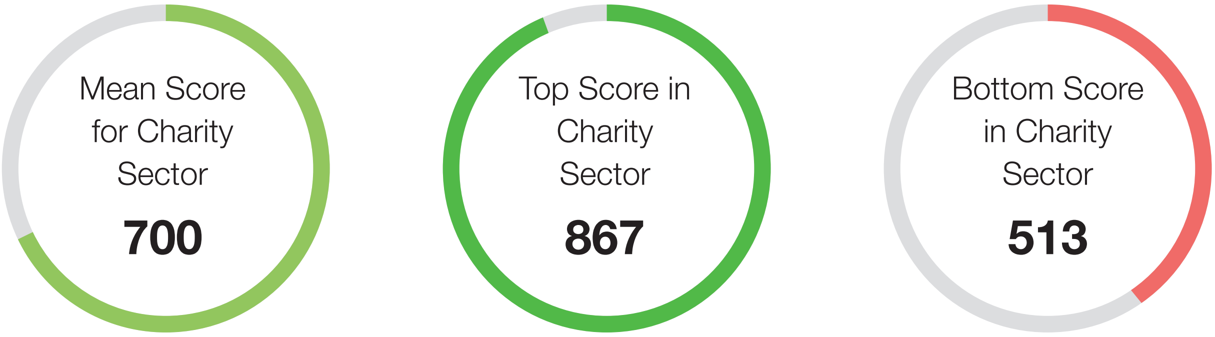
All the weighted factor scores described above are rolled into the total score which falls on a scale of 300 to 900. Please note: even organisations with great cybersecurity programs can still get hacked.

Please also note that scoring, as described above, is a data-driven process ensuring 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.

## Colour coding of charts

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

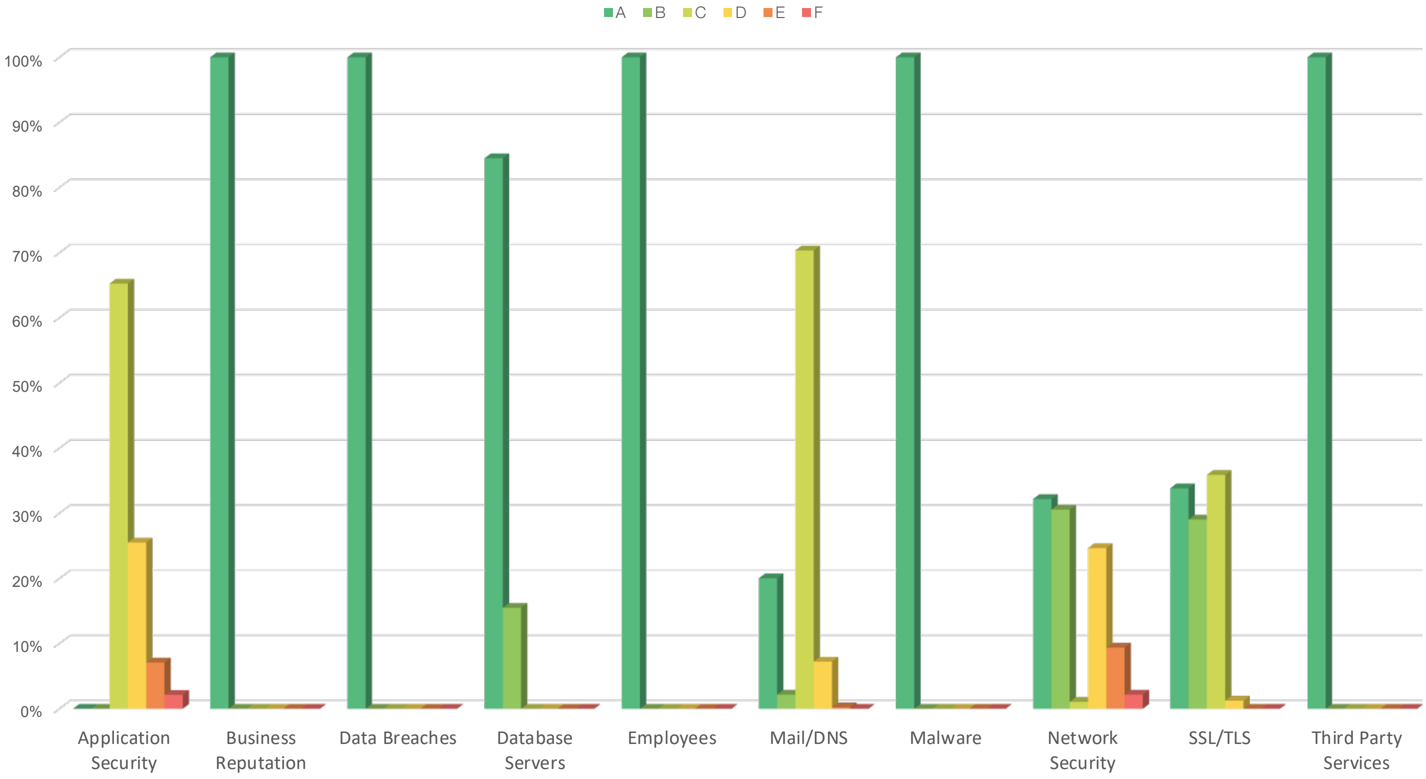
## Figure 1: Overall risk scores



### Key points:

- The mean overall score was 700. This figure hides some very poor scores at the bottom of the pile.
- The best score was 867, but only a single charity achieved this level of excellence.
- The lowest score was 513, recorded by 5 charities. These organisations are at medium risk of a security breach.

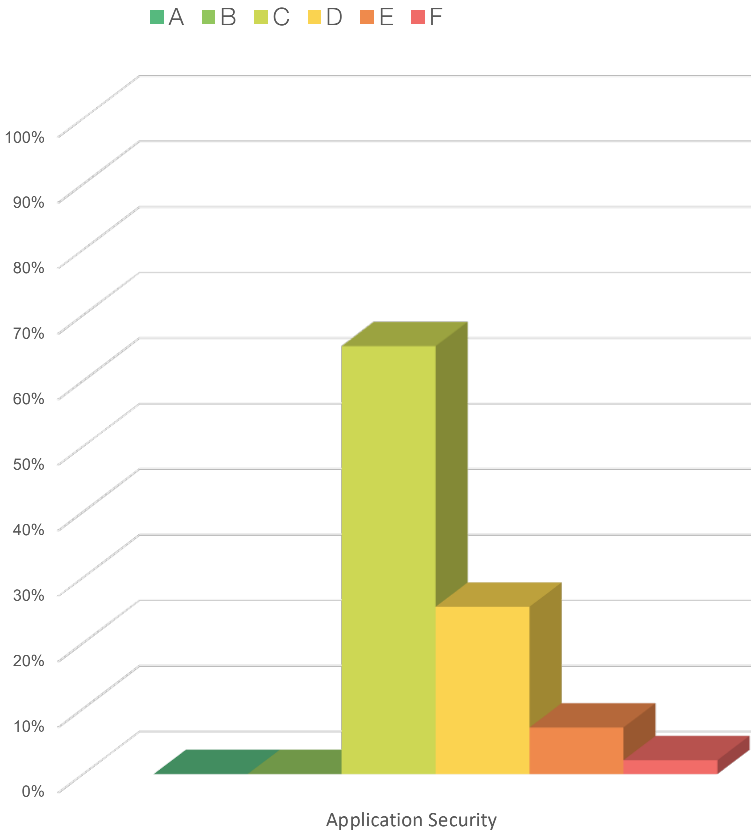
## Figure 2: Overall scores broken down by topic



### Key points:

- Only 73% of charities scored an A grade across all areas.
- The sector as a whole faces serious cyber risk issues in both application security and network security.

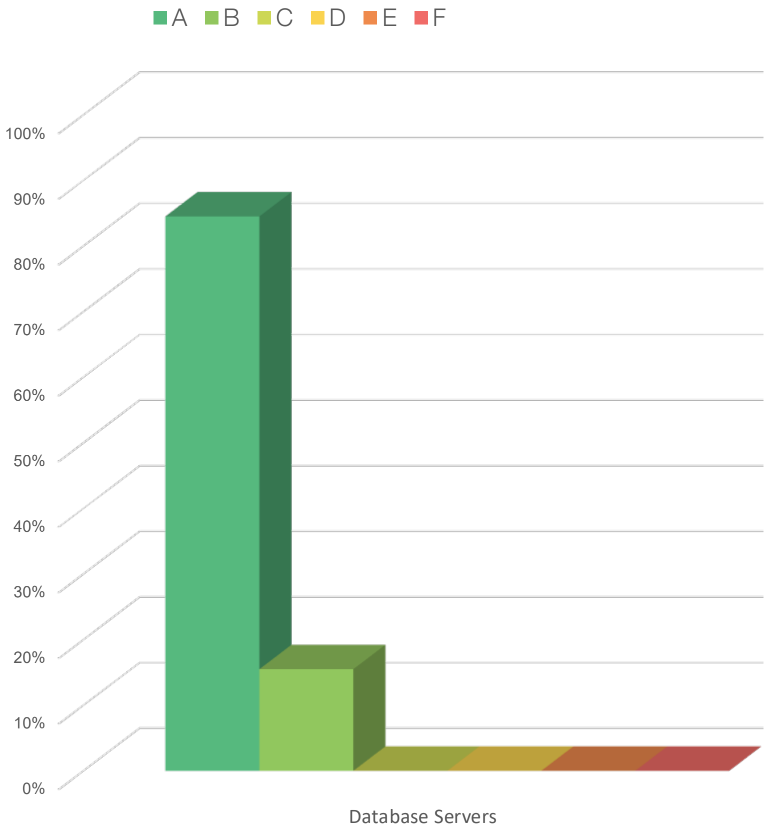
## Figure 3: Spotlight on Application Security



### Key points:

- No charity achieved a grade of A or B for application security. This highlights that charities have work to do when it comes to writing and maintaining their web applications.
- The most common issues include: personal data not being encrypted, and usernames and passwords not being secured in transit.

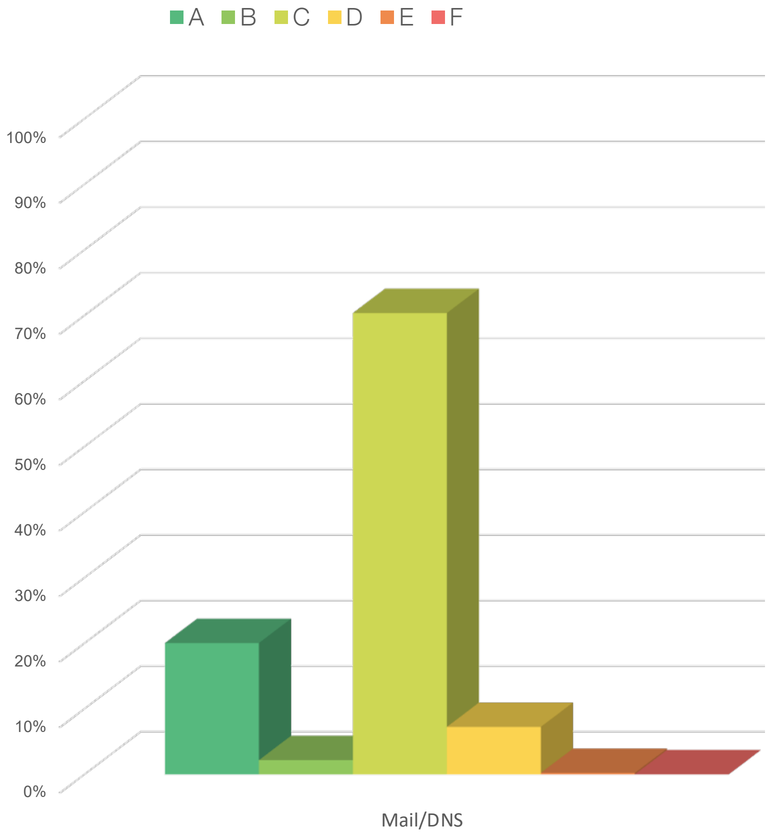
## Figure 4: Spotlight on Database Servers



### Key points:

- 15% of charities scored a B grade for database services.
- These charities are making it easy for hackers to target them by advertising their database services to the open internet.

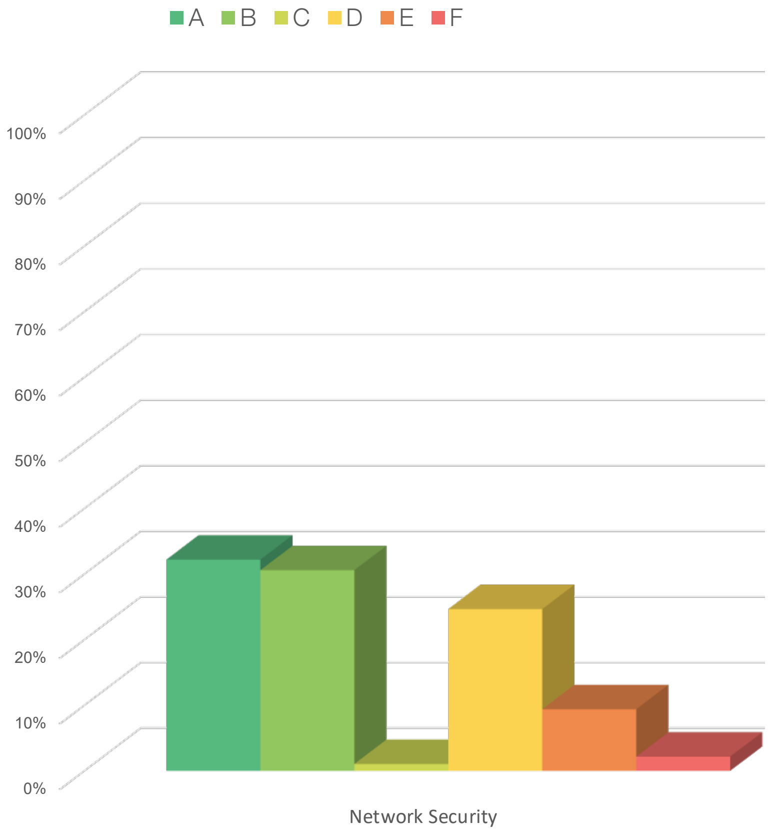
## Figure 5: Spotlight on Mail/DNS



### Key points:

- Only 20% of charities achieved an A grade in email security, with 70.4% getting a C grade.
- These charities are at risk of an email-based attack, such as a phishing email with a ransomeware payload.

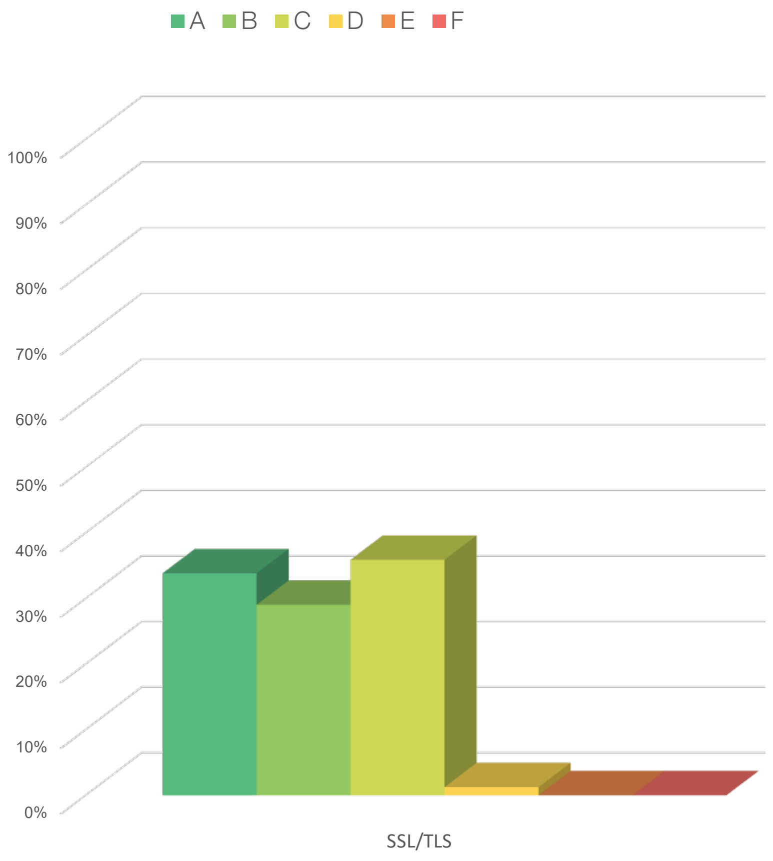
## Figure 6: Spotlight on Network Security



### Key points:

- Charities have some work to do when it comes to network security, with only 62% managing to get an A or B grade.
- This highlights that 38% of charities are not properly patching their systems.

## Figure 7: Spotlight on SSL/TLS



### Key points:

- More than 30% of charities scored a grade C or below for SSL/TLS.
- As digital donations continue to grow, charities must be completely confident in the security of their web presence.

## 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's more, the ratings help to identify challenges and opportunities to make improvements.

An 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, potentially improving the confidence of donors and patrons that their data is being safeguarded effectively.
- Enhanced cyber-security due diligence, demonstrating to stakeholders that the organisation is taking appropriate measures to protect systems and data.

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.
- 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 regulators.

## Methodology

The UK Charity Sector Cyber Risk Rating is an aggregate measure of security risk across charitable organisations of all sizes operating 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 charities included in the report are part of a rotating panel selected from a range of online sources using a sample design.

### Sample size

200 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 cyber security is about managing behavioural risk and skills gaps as well as technical flaws. Cyber security is a technical challenge, but one that is both enabled and constrained by humans.

The seven recommendations detailed below 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 primary 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 UK businesses and non-profits. We apply our knowledge and expertise to help organisations capture, manage, protect and analyse large volumes of 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 multiple industries mean that we have a strong understanding of all relevant UK 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 success. Within our Big Data and Analytics specialism, we provide the capability to gain genuine 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.

## Take the next step

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

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