AON

# Cyber Preparedness in the Food and Beverage Sector

February 2024

# Industry expertise

## Leveraging Food & Drink Industry Expertise to Deliver Distinctive Value

At Aon, we believe it is important to understand the dynamics of the industry in which you operate.

We have a global presence and regional hubs to offer **best-in-class insurance broking and risk financing** solutions for your sector.

We achieve this through industry insight, thought leadership, client conversations, and benchmarking. This helps us enhance our risk modeling capabilities and design the most appropriate solutions.

### Food, Agribusiness & Beverage Credentials

More than
**1,500**
global FAB clients

**100+**
captives under management


A Globally aligned team

Greater than
**90%**
retention rate
(most clients choose to stay with Aon as their preferred risk, retirement and health advisor)

We advise
**9** of the **10**
largest food and beverage brands in the world


Strategy & Innovation Council

AON

# Question 1
Cyber defence

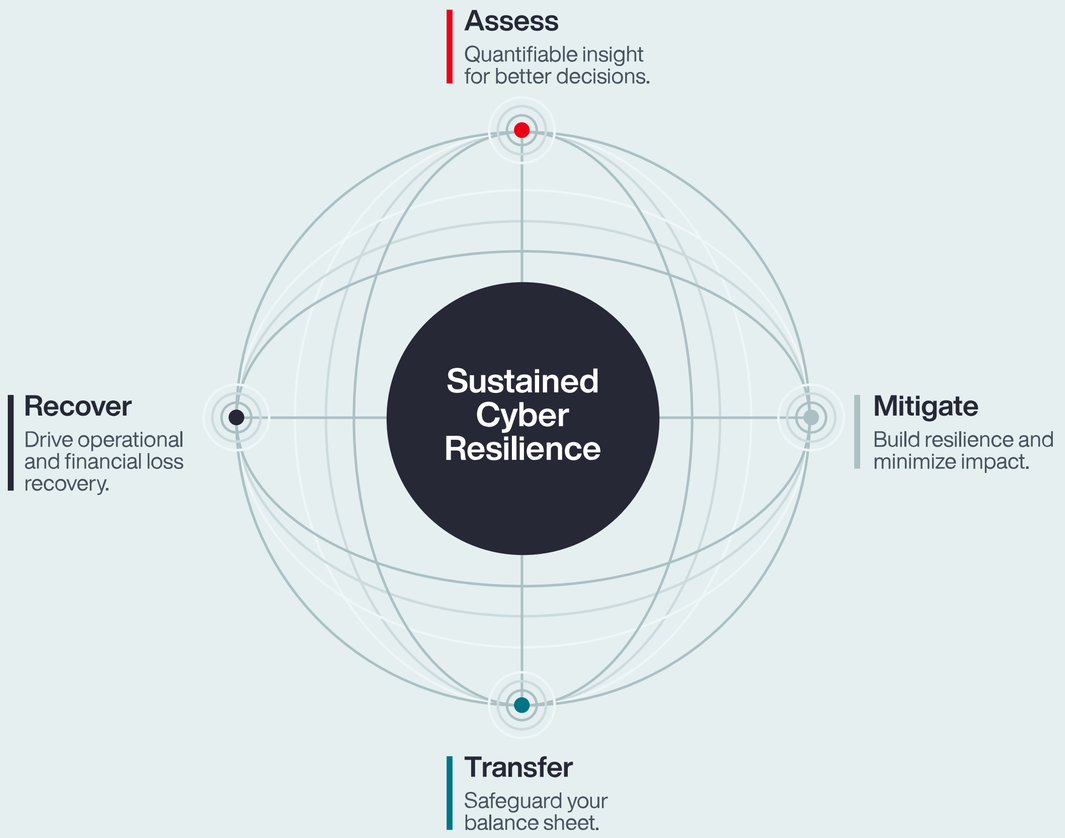
# There is Nothing Linear About Cyber Security.

This is the guiding principle of the Cyber Loop, a risk management model that **unites stakeholders** to make better decisions around cyber risk.

Aon's Cyber Loop model acknowledges that each organization will be at a different place in its cyber risk journey: **assess, mitigate, transfer, or recover**.

In a Loop model, businesses become informed participants in managing risk, engaged in continuous review, improvement, and investment in security – guided by data.

**The Result. Sustained Cyber Resilience.**

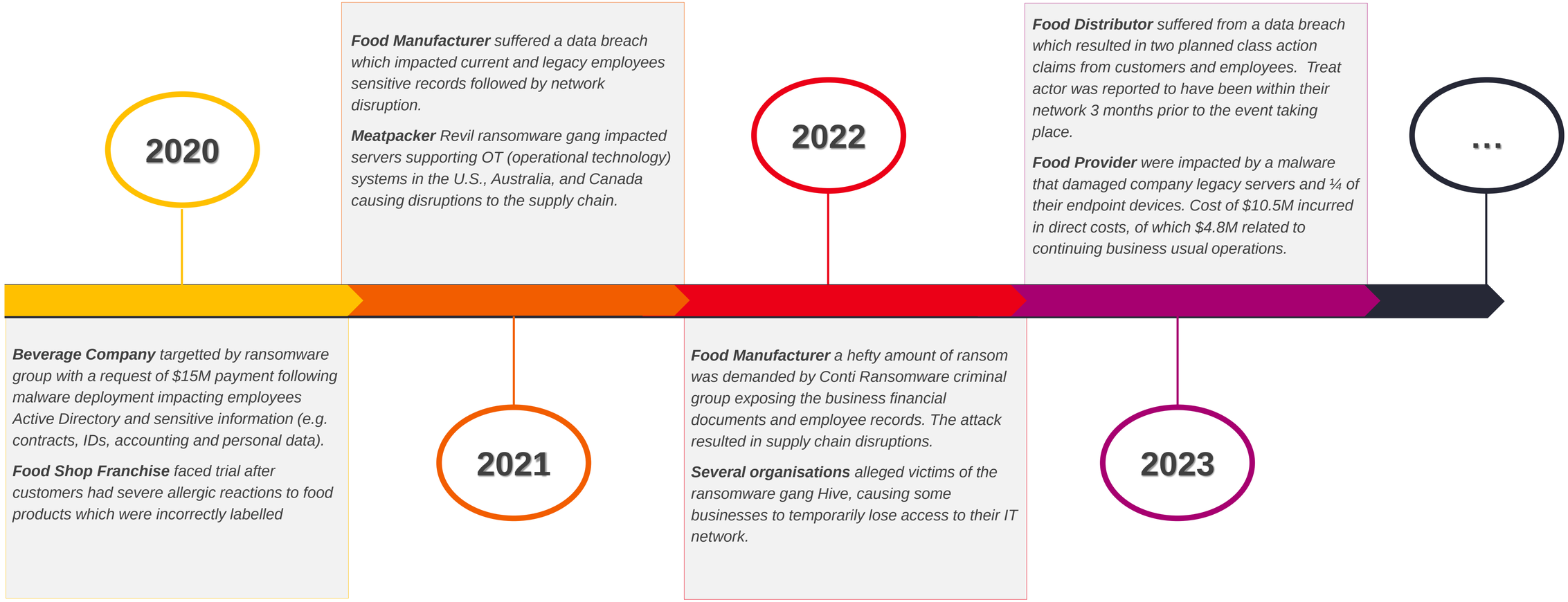



AON

# Question 2
Cyber threats

# Examples of Cyber Attacks

## Food and Beverage Sector



# Cyber Risk Overview

## Food and Beverage Sector Trends

EXPOSURE

**2023 top 5 risks in Food and Beverages (including Agribusiness):**

**#1** Commodity Price Risk or Scarcity of Materials
**#2** Supply Chain or Distribution Failure
**#3** Business Interruption
**#4 Cyber Attack or Data Breach**
**#5** Climate Change

Since 2020, the number of insider cyber threats, both inadvertent and malicious, has risen by **44%**.

An average of **$184,548** is spent to contain insider threats, with business interruption costs (**23%** of total) typically being the greatest expense.

PREPAREDNESS

**Five domains demonstrated** the most **significant risk profile improvements**, and from this inferred budget increases: **Data Security, Application Security, Remote Work, Access Control, and Endpoint & Systems Security**.

**Food and Beverage sector clients** have shown score changes of **+0.2 points** in **Third Party Domain**.

For most organisations, the best way to address cyber risk is **understanding what technology assets are crucial to the business** from a revenue generation and/or risk aggregation stance.

AON

# Question 3

IT Security investment priorities

# Case Study 1: Supermarket Chain

## Assessing & Transferring Cyber Risk

### The Challenge

Insurance Manager instructed by top management to review cyber insurance to determine the company appropriate and proportionate insurance limits & coverage and assist in building a cyber underwriting submission.

### Solution

**Aon and the client to determine the 5 ‘severe yet plausible’** cyber risk scenarios to be **quantified and analysed against existing insurance coverage**.

### Result

- Aon’s analysis indicated that estimated maximum losses (EMLs) were greater than original policy limits, giving the client the necessary information to make data - informed decisions at renewal.
- **Aon’s** Cyber Risk (AGRC) and Broking teams provided an **integrated approach**, assessing potential losses through a Cyber Impact Analysis which **enabled the client to make an informed decision regarding its risk transfer strategy**.

# Case Study 2: Food Producer

## Assessing & Mitigating Cyber Risk

### The Challenge

A multinational processed food producer with manufacturing locations across Europe was concerned about how their technical and executive teams would be able to respond to a cybersecurity response.

### Solution

Our Cyber Risk Advisory Team managed the construction of both a technical and executive simulation exercise, designed to get both teams to discuss a carefully bespoke scenario. The 5-hour* exercise allowed the teams to fully understand their incident response process. This exercise supported us in identifying key risks to the organisation.

### Result

- The client said that the exercises were an '**eye-opening experience**' that showed them the importance of conducting regular cyber simulations.
- **Recommendations helped the client** to identify and execute security improvements to reduce their risk exposure and **improve their cyber resilience.**

# Case Study 3: Food & Beverage Producer

## Assessing Cyber Risk & Building a Roadmap

### The Challenge

A multinational food and drink producer with manufacturing locations across the world was concerned about the IT dependency of their operations in the event of a cyber incident and its impact on the insurance eligibility.

### Solution

Our Cyber Risk Advisory Team managed the construction of a robust strategy to **identify key risk areas using CyQu to effectively and efficiently collect data needed to build a security roadmap to improve cyber posture and meet underwriting requirements.**

### Result

- The security roadmap guided the client to understand their cyber risk and security posture.
- **Recommendations helped the client** to identify and execute security improvements required **to reduce their risk exposure and become ready for the underwriting submission**.

# Question 4

Cyber risk maturity

# CyQu Freemium

We are inviting you…

## Aon are currently offering a free 'CyQu' Cyber Risk Assessment to FDF members.

- The evaluation is based on **9 risk security domains** and **35 control areas**.
- Provides an **instant CyQu Score** and snapshot of an organisation's cyber maturity.
- A tailored readout session with a Cyber Specialist will be provided after submitting.
- The CyQu answers can also form part of future insurance broking presentation.

# CyQu Freemium
## Self-Assessment

**CyQu is an award winning online cyber risk self-assessment enabling organisations to take an important step in strengthening their cyber risk posture.**

In about **90 minutes or less**, CyQu will provide you with a cyber risk maturity score (CyQu Score) giving you an immediate snapshot of your cyber maturity and insight into the areas posing the greatest risk.

**View your CyQu score across 9 security domains**


**Key benefits to your business**

- Gain **instant visibility** into your cyber risk posture
- Identify **quick wins** to strengthen security
- Obtain clear, **actionable strategies** for remediation
- **Benchmark** against industry peers
- **Align security functions** across your organisation

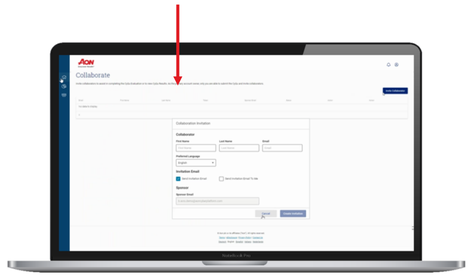
# CyQu Freemium
## How it Works

An IT representative and appropriate colleagues to complete a concise online self-assessment, across nine security domains, broken down into sub-categories or “critical controls”.

1. **Data security**
2. **Access control**
3. **Endpoint and systems security**
4. **Network security**
5. **Physical security**
6. **Application security**
7. **Third party**
8. **Business resilience**
9. **Remote work**

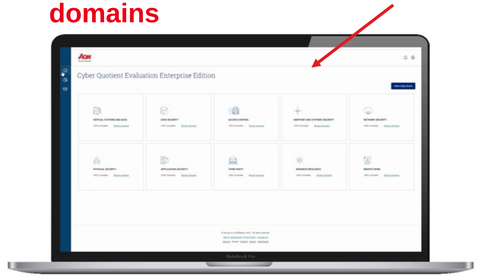
**Step 1:** Cross collaboration feature

**Quickly share the CyQu assessment with colleagues**

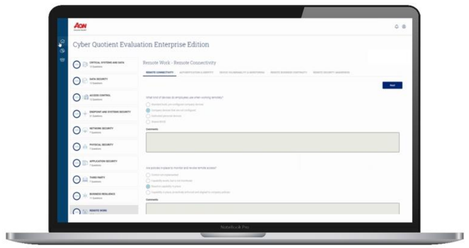



**Step 2:** Complete a concise online self-assessment

**Concise question set across 9 security domains**



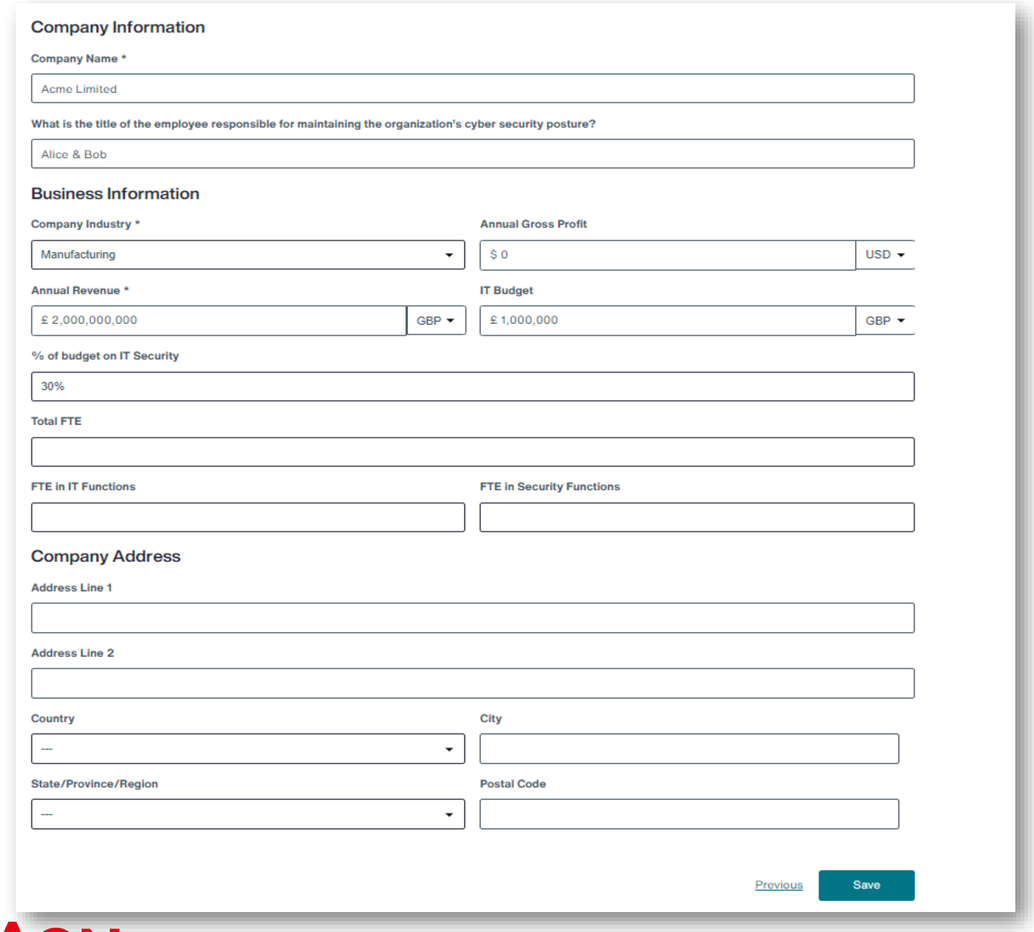

**CyQu Q&A is for its most part multiple choice**



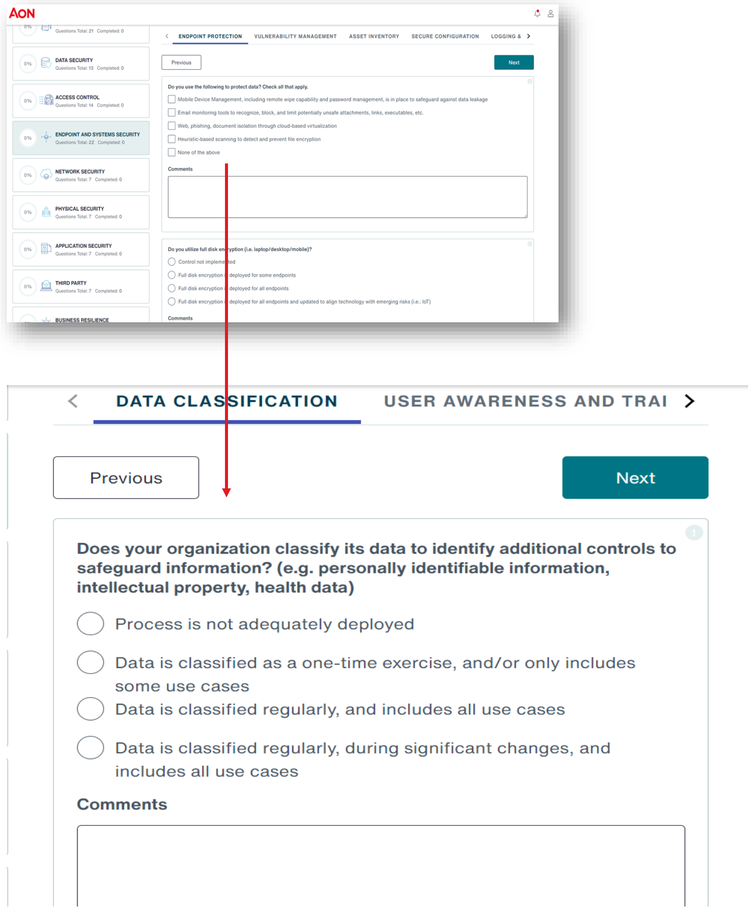

**Step 3:** Get an immediate snapshot of your cyber maturity with your CyQu Score

# CyQu Freemium
## Q&A Samples

### Company Profile Information
This section may require the assistance of colleagues that sit outside the IT department




### Domain Q&A
Multiple Choice (e.g. Data Security)



# CyQu Report

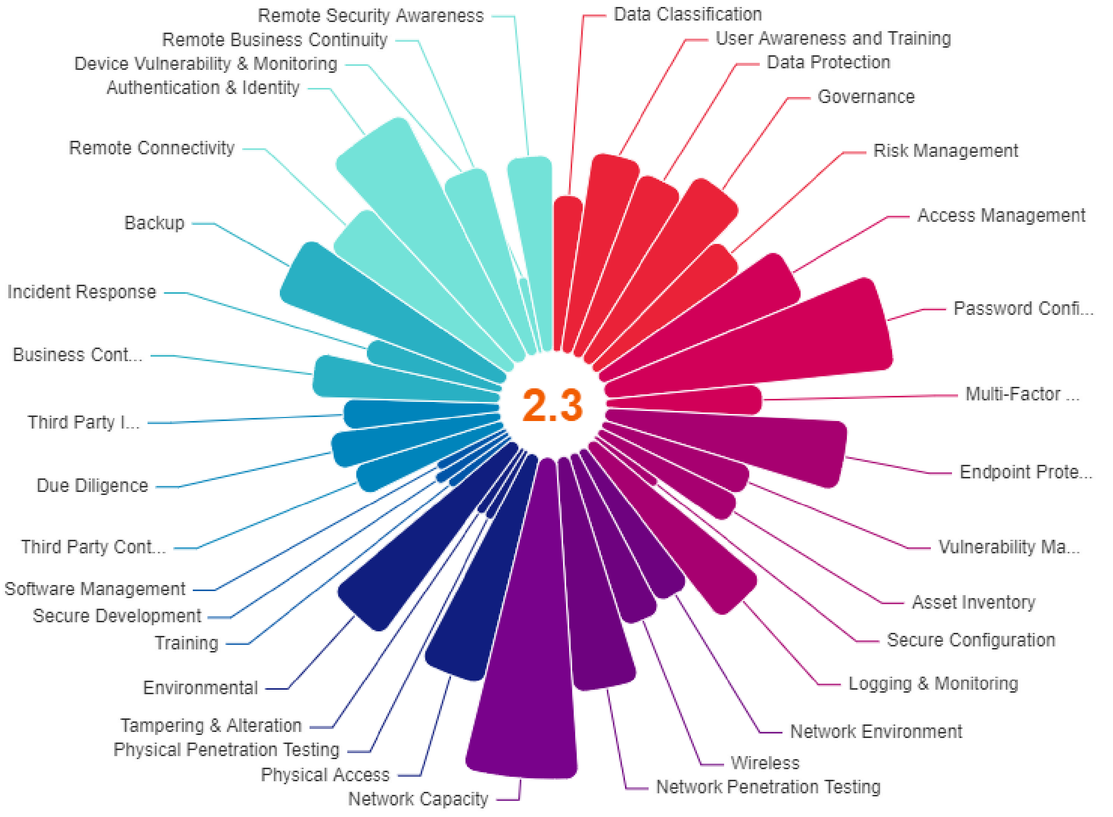
## Sample Output For Illustrative Purposes

### Performance Breakdown

The overall cyber security performance score is **2.3**.
The score is on a scale of 1 (Initial) to 4 (Advanced).
This score has been achieved according to responses provided in January 2023.

| Control Domain | Your CyQu | Peer CyQu |
|---|---|---|
| Data Security | 2.5 | 2.7 |
| Asset Control | 2.7 | 2.9 |
| Endpoint and Systems Security | 2.6 | 3.0 |
| Network Security | 2.6 | 3.0 |
| Physical Security | 2.4 | 2.9 |
| Application Security | 1.0 | 2.3 |
| Third Party | 2.1 | 2.3 |
| Business Resilience | 2.3 | 2.6 |
| Remote Work | 2.5 | 2.9 |

### CyQu Score




AON

# CyQu Report

## Sample Output For Illustrative Purposes

| Data Security | You | Peer |
|---|---|---|
| Data Classification | 2.0 | 2.5 |
| User Awareness Training | 2.6 | 3.2 |
| Data Protection | 2.5 | 2.9 |
| Governance | 2.8 | 2.7 |
| Risk Management | 2.3 | 2.5 |

| Network Security | You | Peer |
|---|---|---|
| Network Environment | 2.2 | 3.1 |
| Wireless | 2.3 | 2.8 |
| Network Penetration Testing | 3.0 | 3.2 |
| Network Capacity | 4.0 | 2.8 |

| Third Party | You | Peer |
|---|---|---|
| Third Party Contracts | 2.0 | 2.3 |
| Due Diligence | 2.2 | 2.1 |
| Third Party Inventory | 2.0 | 2.9 |

| Access Control | You | Peer |
|---|---|---|
| Access Management | 2.8 | 2.8 |
| Password Configuration | 3.7 | 3.5 |
| Two-Factor Authentication | 2.0 | 2.7 |

| Physical Security | You | Peer |
|---|---|---|
| Physical Access | 3.0 | 3.2 |
| Physical Penetration Testing | 1.0 | 1.9 |
| Tampering & Alteration | 1.0 | 2.0 |
| Environmental | 3.0 | 3.2 |

| Business Resilience | You | Peer |
|---|---|---|
| Business Continuity/DR | 2.4 | 2.6 |
| Incident Response | 1.8 | 2.6 |
| Backup | 3.1 | 2.7 |

| Endpoint & Systems Security | You | Peer |
|---|---|---|
| Endpoint Protection | 3.1 | 3.1 |
| Vulnerability Management | 2.0 | 3.0 |
| Asset Inventory | 2.0 | 2.8 |
| Secure Configuration | 1.0 | 3.1 |
| Logging and Monitoring | 2.8 | 2.9 |

| Application Security | You | Peer |
|---|---|---|
| Training | 1.0 | 2.3 |
| Secure Development | 1.1 | 2.4 |
| Software Management | 1.0 | 2.3 |

| Remote Work | You | Peer |
|---|---|---|
| Remote Connectivity | 2.8 | 3.4 |
| Authentication & Identity | 3.5 | 3.2 |
| Device Vulnerability & Monitoring | 2.5 | 2.7 |
| Remote Business Continuity | 1.0 | 2.2 |
| Remote Security Awareness | 2.5 | 2.5 |

AON

# Next Steps

If you have further questions, please contact a member of Aon's Cyber Solutions team via:

**richard.s.fawcett@aon.co.uk**

1. Request access to CyQu via richard.s.fawcett@aon.co.uk.
2. Complete CyQu Self Assessment.
3. Review results of CyQu with Aon’s cyber professionals and internal stakeholders.
4. Implement risk mitigation and remediation strategies and work collaboratively to improve your cyber resilience.

Forthcoming Aon & FDF webinar:

*Cyber & Artificial Intelligence,*

*16th April 2024.*

# Your questions

# Thank you!

## About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance. For further information on our capabilities and to learn how we empower results for clients, please visit : http: //aon.mediaroom.com.



The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The information contained in this document should not be considered or construed as legal or tax advice and is for general guidance only. Accordingly, the information contained herein is provided with the understanding that Aon, its employees and related entities are not engaged in rendering legal or tax advice. As such, this should not be used as a substitute for consultation with legal and tax counsel.

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

www.aon.com

## Contact Us

**Richard Fawcett** | Client Director
Aon Risk Solutions
12th Floor I The Colmore Building I20 Colmore Circus Queensway
Birmingham I B4 6AT
richard.s.fawcett@aon.co.uk | aon.co.uk

**Carl Shanks** | Director EMEA
Aon Risk Solutions | Cyber Solutions
1 Redcliff Street | Bristol, BS1 6NP
United Kingdom
carl.shanks@aon.com | aon.co.uk

**Ryan Hembery** | Cyber Client Director
Aon Risk Solutions | Cyber Solutions
1 Redcliff Street | Bristol, BS1 6NP
United Kingdom
ryan.hembery@aon.co.uk | aon.co.uk

**Luiza Meziat** | Senior Consultant – Cyber Risk
Aon Risk Solutions | Cyber Solutions
The Aon Centre | The Leadenhall Building I 122 Leadenhall Street
London | EC3V 4AN | United Kingdom
luiza.meziat@aon.co.uk | aon.co.uk