

# 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





### Question 1 Cyber defence



	С
1	C

# 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.







Safeguard your balance sheet.

### Question 2 Cyber threats



### **Examples of Cyber Attacks** Food and Beverage Sector



Food Manufacturer suffered a data breach which impacted current and legacy employees sensitive records followed by network disruption.

Meatpacker Revil ransomware gang impacted servers supporting OT (operational technology) systems in the U.S., Australia, and Canada causing disruptions to the supply chain.

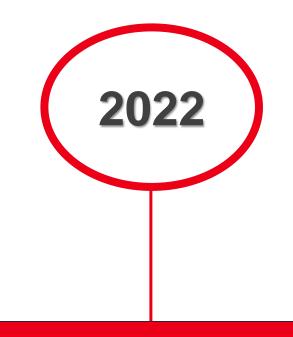
**Beverage Company** targetted by ransomware group with a request of \$15M payment following malware deployment impacting employees Active Directory and sensitive information (e.g. contracts, IDs, accounting and personal data).

Food Shop Franchise faced trial after customers had severe allergic reactions to food products which were incorrectly labelled



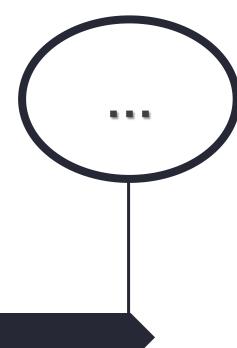
network.





**Food Distributor** suffered from a data breach which resulted in two planned class action claims from customers and employees. Treat actor was reported to have been within their network 3 months prior to the event taking place.

Food Provider were impacted by a malware that damaged company legacy servers and ¼ of their endpoint devices. Cost of \$10.5M incurred in direct costs, of which \$4.8M related to continuing business usual operations.



**Food Manufacturer** a hefty amount of ransom was demanded by Conti Ransomware criminal group exposing the business financial documents and employee records. The attack resulted in supply chain disruptions.

Several organisations alleged victims of the ransomware gang Hive, causing some businesses to temporarily lose access to their IT

















































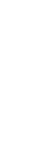




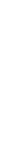














































































### **Cyber Risk Overview** Food and Beverage Sector Trends

#### 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

**Cyber Attack or Data Breach** #4

**#5** Climate Change

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

EXPOSURE

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.



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

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.

### Question 3 IT Security investment priorities



8

### **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.



- make data informed decisions at renewal.
- enabled the client to make an informed decision regarding its risk transfer strategy.



• Aon's analysis indicated that estimated maximum losses (EMLs) were greater than original policy limits, giving the client the necessary information to

• Aon's Cyber Risk (AGRC) and Broking teams provided an integrated approach, assessing potential losses through a Cyber Impact Analysis which



### **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.



- 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**

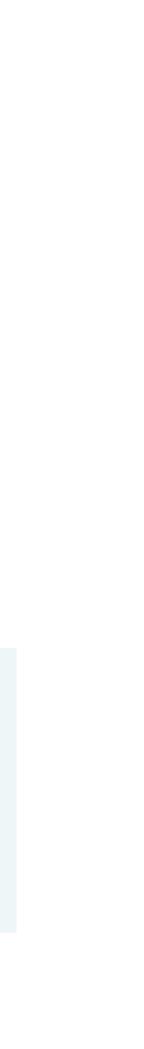
Our Cyber Risk Advisory Team managed the construction of a robust strategy to identify key risk areas using CyQu to effectively and efficiently collect data needed to build a security roadmap to improve cyber posture and meet underwriting requirements.



- The security roadmap guided the client to understand their cyber risk and security posture.
- underwriting submission.



• Recommendations helped the client to identify and execute security improvements required to reduce their risk exposure and become ready for the



### 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.



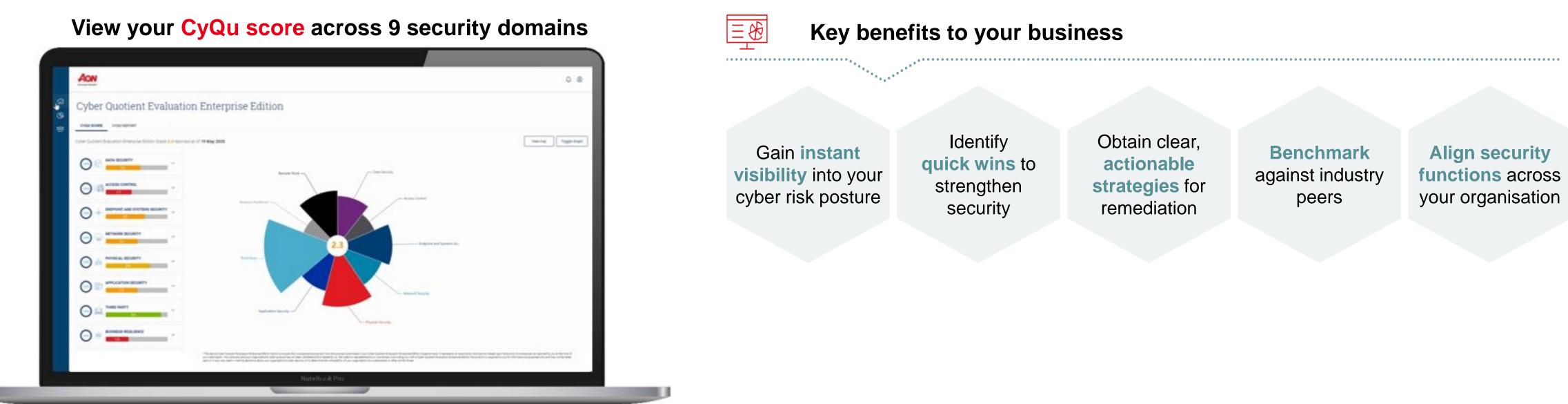




### **CyQu Freemium** Self-Assessment

### 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.









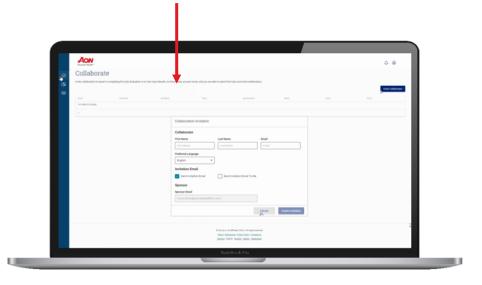
### CyQu Freemium How it Works

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".



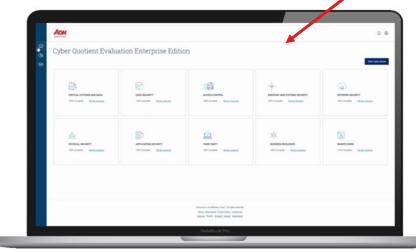
#### **Step 1:** Cross collaboration feature

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

Cyber Quotient Ev	A standard and a state
	valuation Enterprise Edition
	Remote Work - Remote Connectivity
	The set of
	ere
	C Revents
	are placed region to restore per water what a source
	C Execution and ingeneration C regarding works, for or of information (D transformation in yours)
	memory     memory     memory

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

Asmolimited			
Acme Limited			
What is the title of the employee responsible	or maintaining the organization's o	cyber security posture?	
Alice & Bob			
Business Information			
Company Industry *		Annual Gross Profit	
Manufacturing	•	\$0	USD 👻
Annual Revenue *		IT Budget	
£ 2,000,000,000	GBP ▼	£ 1,000,000	GBP 👻
% of budget on IT Security			
30%			
Total FTE			
			]
FTE in IT Functions	]	FTE in Security Functions	
Company Address			
Address Line 1			
Address Line 2			
Country		City	
	•		
L		Postal Code	
State/Province/Region	•		
State/Province/Region		L	]
[			
[		Previous	Save

#### Domain Q&A

Multiple Choice (e.g. Data Security)

Image: Section of the section of th	0% C DATA SECURITY Questions Total: 13 Completed: 0	Previous
<b>ODE: INCOMPARENT: INCOMPARE</b>		
Original and a control of the second se		Heuristic-based scanning to detect and prevent file encryption
Dees your organization classify its data to identify additional controls to safeguard information; (e.g. personally identifiable information, intellectual property, health data)  Process is not adequately deployed Data is classified as a one-time exercise, and/or only includes some use cases Data is classified regularly, and includes all use cases Data is classified regularly, during significant changes, and includes all use cases		Comments
I define the product of the prod		
Description of the start of		
<ul> <li>ATA CLASSIFICATION USER AWARENESS AND TRAI</li> <li>Previous Next</li> <li>Does your organization classify its data to identify additional controls to safeguard information? (e.g. personally identifiable information, intellectual property, health data)</li> <li>Process is not adequately deployed</li> <li>Data is classified as a one-time exercise, and/or only includes some use cases</li> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>		Full disk encryption deployed for all endpoints
Previous       Next         Does your organization classify its data to identify additional controls to safeguard information? (e.g. personally identifiable information, intellectual property, health data)       Process is not adequately deployed         Process is not adequately deployed       Data is classified as a one-time exercise, and/or only includes some use cases         Data is classified regularly, and includes all use cases       Data is classified regularly, during significant changes, and includes all use cases	BUSINESS RESILIENCE	Comments
Previous       Next         Does your organization classify its data to identify additional controls to safeguard information? (e.g. personally identifiable information, intellectual property, health data)       Process is not adequately deployed         Process is not adequately deployed       Data is classified as a one-time exercise, and/or only includes some use cases         Data is classified regularly, and includes all use cases       Data is classified regularly, during significant changes, and includes all use cases		
Previous       Next         Does your organization classify its data to identify additional controls to safeguard information? (e.g. personally identifiable information, intellectual property, health data)       Process is not adequately deployed         Process is not adequately deployed       Data is classified as a one-time exercise, and/or only includes some use cases         Data is classified regularly, and includes all use cases       Data is classified regularly, during significant changes, and includes all use cases		
<ul> <li>Does your organization classify its data to identify additional controls to safeguard information? (e.g. personally identifiable information, intellectual property, health data)</li> <li>Process is not adequately deployed</li> <li>Data is classified as a one-time exercise, and/or only includes some use cases</li> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>		A CLASSIFICATION USER AWARENESS AND TRAI
<ul> <li>Does your organization classify its data to identify additional controls to safeguard information? (e.g. personally identifiable information, intellectual property, health data)</li> <li>Process is not adequately deployed</li> <li>Data is classified as a one-time exercise, and/or only includes some use cases</li> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>		
<ul> <li>Does your organization classify its data to identify additional controls to safeguard information? (e.g. personally identifiable information, intellectual property, health data)</li> <li>Process is not adequately deployed</li> <li>Data is classified as a one-time exercise, and/or only includes some use cases</li> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>		
<ul> <li>safeguard information? (e.g. personally identifiable information, intellectual property, health data)</li> <li>Process is not adequately deployed</li> <li>Data is classified as a one-time exercise, and/or only includes some use cases</li> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>		
<ul> <li>safeguard information? (e.g. personally identifiable information, intellectual property, health data)</li> <li>Process is not adequately deployed</li> <li>Data is classified as a one-time exercise, and/or only includes some use cases</li> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>	Previou	IS Next
<ul> <li>safeguard information? (e.g. personally identifiable information, intellectual property, health data)</li> <li>Process is not adequately deployed</li> <li>Data is classified as a one-time exercise, and/or only includes some use cases</li> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>	Previou	JS
<ul> <li>safeguard information? (e.g. personally identifiable information, intellectual property, health data)</li> <li>Process is not adequately deployed</li> <li>Data is classified as a one-time exercise, and/or only includes some use cases</li> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>	Previou	IS Next
<ul> <li>Process is not adequately deployed</li> <li>Data is classified as a one-time exercise, and/or only includes some use cases</li> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>		
<ul> <li>Data is classified as a one-time exercise, and/or only includes some use cases</li> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>	Does you	↓ ur organization classify its data to identify additional controls to
<ul> <li>Data is classified as a one-time exercise, and/or only includes some use cases</li> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>	Does you safeguar	ur organization classify its data to identify additional controls to rd information? (e.g. personally identifiable information,
some use cases Data is classified regularly, and includes all use cases Data is classified regularly, during significant changes, and includes all use cases	Does you safeguar intellectu	↓ ur organization classify its data to identify additional controls to rd information? (e.g. personally identifiable information, ual property, health data)
<ul> <li>Data is classified regularly, and includes all use cases</li> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>	Does you safeguar intellectu	↓ ur organization classify its data to identify additional controls to rd information? (e.g. personally identifiable information, ual property, health data)
<ul> <li>Data is classified regularly, during significant changes, and includes all use cases</li> </ul>	Does you safeguar intellectu	ur organization classify its data to identify additional controls to rd information? (e.g. personally identifiable information, ual property, health data) cess is not adequately deployed
includes all use cases	Does you safeguar intellectu O Proc	In organization classify its data to identify additional controls to rd information? (e.g. personally identifiable information, ual property, health data) cess is not adequately deployed a is classified as a one-time exercise, and/or only includes
includes all use cases	Does you safeguar intellectu O Proc Data som	ur organization classify its data to identify additional controls to rd information? (e.g. personally identifiable information, ual property, health data) cess is not adequately deployed a is classified as a one-time exercise, and/or only includes the use cases
	Does you safeguar intellectu O Proc Data som Data	ur organization classify its data to identify additional controls to rd information? (e.g. personally identifiable information, ual property, health data) cess is not adequately deployed a is classified as a one-time exercise, and/or only includes he use cases a is classified regularly, and includes all use cases
Comments	Does you safeguar intellectu O Proc Data som Data	<ul> <li>ur organization classify its data to identify additional controls to rd information? (e.g. personally identifiable information, ual property, health data)</li> <li>cess is not adequately deployed</li> <li>a is classified as a one-time exercise, and/or only includes</li> <li>a is classified regularly, and includes all use cases</li> <li>a is classified regularly, during significant changes, and</li> </ul>
	Does you safeguar intellectu O Proc Data som Data	<ul> <li>ur organization classify its data to identify additional controls to rd information? (e.g. personally identifiable information, ual property, health data)</li> <li>cess is not adequately deployed</li> <li>a is classified as a one-time exercise, and/or only includes</li> <li>a is classified regularly, and includes all use cases</li> <li>a is classified regularly, during significant changes, and</li> </ul>
	Does you safeguar intellectu Proc Data som Data Data inclu	<ul> <li>ur organization classify its data to identify additional controls to a dinformation? (e.g. personally identifiable information, ual property, health data)</li> <li>cess is not adequately deployed</li> <li>a is classified as a one-time exercise, and/or only includes he use cases</li> <li>a is classified regularly, and includes all use cases</li> <li>a is classified regularly, during significant changes, and udes all use cases</li> </ul>
	Does you safeguar intellectu Proc Data som Data Data inclu	<ul> <li>ur organization classify its data to identify additional controls to a dinformation? (e.g. personally identifiable information, ual property, health data)</li> <li>cess is not adequately deployed</li> <li>a is classified as a one-time exercise, and/or only includes he use cases</li> <li>a is classified regularly, and includes all use cases</li> <li>a is classified regularly, during significant changes, and udes all use cases</li> </ul>



### CyQu Report Sample Output For Illustrative Purposes

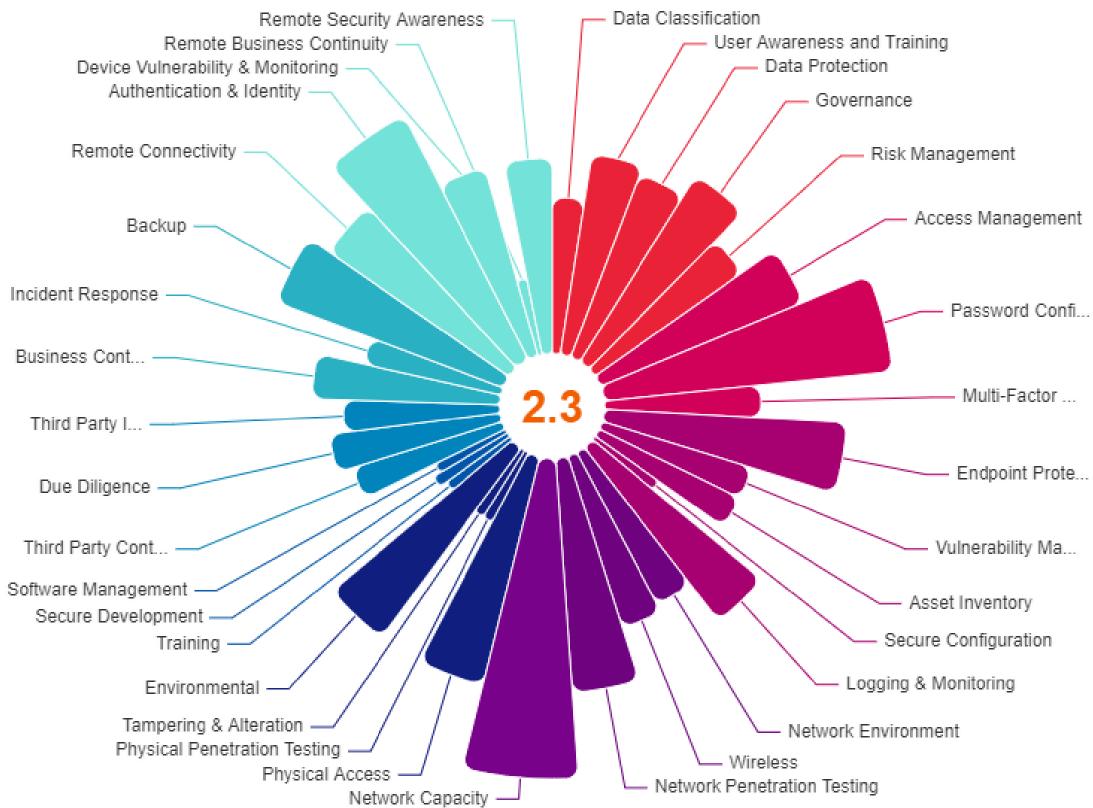
#### **Performance Breakdown**

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



### **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

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

#### Network Security

Network Environment Wireless Network Penetration Testing Network Capacity

#### Physical Security

Physical Access

Physical Penetration Testing

Tampering & Alteration

Environmental

#### **Application Security**

Training

Secure Development

Software Management



You	Peer
2.2	3.1
2.3	2.8
3.0	3.2
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

You	Peer
3.0	3.2
1.0	1.9
1.0	2.0
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

You	Peer	
1.0	2.3	
1.1	2.4	
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







### **Next Steps**

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

richard.s.fawcett@aon.co.uk



Forthcoming Aon & FDF webinar: *Cyber & Artificial Intelligence, 16th April 2024.* 



Request access to CyQu via richard.s.fawcett@aon.co.uk.

Complete CyQu Self Assessment.

Review results of CyQu with Aon's cyber professionals and internal stakeholders.

Implement risk mitigation and remediation strategies and work collaboratively to improve your cyber resilience.

### Your questions









### About Aon

<u>Aon plc</u> (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.

© Aon plc 2024. All rights reserved.

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 <u>luiza.meziat@aon.co.uk</u> | aon.co.uk