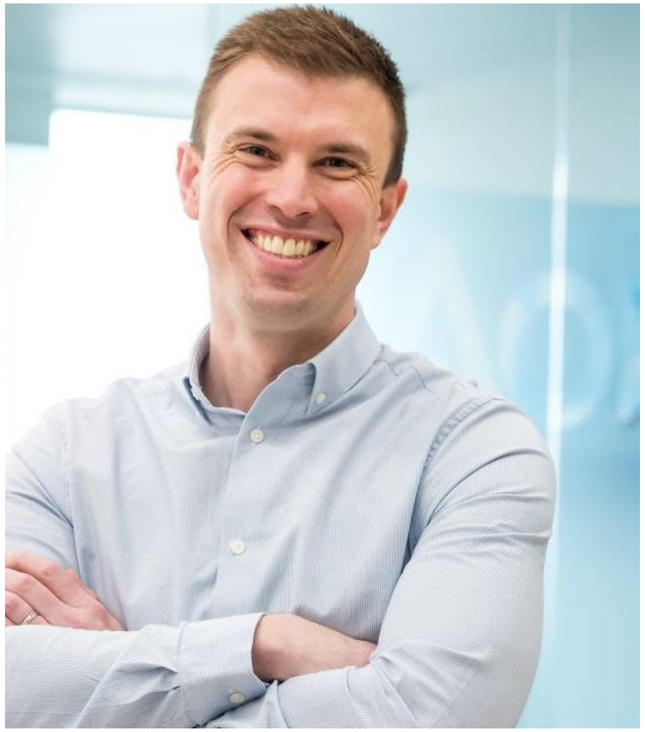
Are you ready for the new Network and Information Security Directive (NIS2)?

Food & Drink Federation (FDF) webinar

26 September 2024

Introductions

Chris Scott
Head of Cyber Solutions - UK



Richard Fawcett
Industry Leader – Food, Agribusiness & Beverage (UK)

- Identify
- Assess/Quantify
- Address
- Retain
- Mitigate
- Transfer

Sector expertise

We understand your business and the industry in which you operate. This is demonstrated by our sector expertise:

Aon clients represent **52%** of the **top 100** food manufacturers in the UK including **7** of the **top 10** (The Grocer report, 2022)

Globally, Aon advises **9** of the **top 10** largest food manufacturing companies in the world

Our UK Food & Drink Practice brings together our experts from across the UK and internationally. Our group meets regularly to share insights and best practice, but also brief colleagues on new and innovative solutions available for our clients

Our industry experts contribute regularly to our thought leadership communications, and these can be found on our

Aon is an Associate Member of the Food & Drink Federation and regularly support and attend its events

Over the last 5 years our claims consultants have **actively managed over £200m** of major losses in the Food & Drink Sector to accelerate positive claims settlements and avert crises

Addo Foods Apetito **Arla** Asda
Associated British Foods
Bernard Matthews **Bacardi** Bidfood
Boparan/2SFG Brake Brothers
Country Style Foods Cranswick
Dairy Crest Daniel Thwaites **Danone**
Danish Crown **Douwe Egberts** First Milk
Fox's Burtons Company Fentimans
Ferrero UK Frontier Agriculture **Glen Grant**
Grenade **Greencore** Hazlewood Foods
Hills Biscuits Iceland Seafoods **Kerry Foods**
Kettle Produce **Lidl** Marr Seafoods
Martin Brower McQueens Dairies **Morrisons**
Mondelez **Nestle** North British Distillery
Ocado Pets Choice **Peters Foods** Pork Farms
Quintessential Brands Saputo UK
S&A Foods Scottish Salmon **Sofina Foods**
Tesco Thomas Tunnock **Unilever**
Upfield Foods **Walkers** William Jackson Foods
Whyte & Mackay Wyke Farms **Zwanenberg**

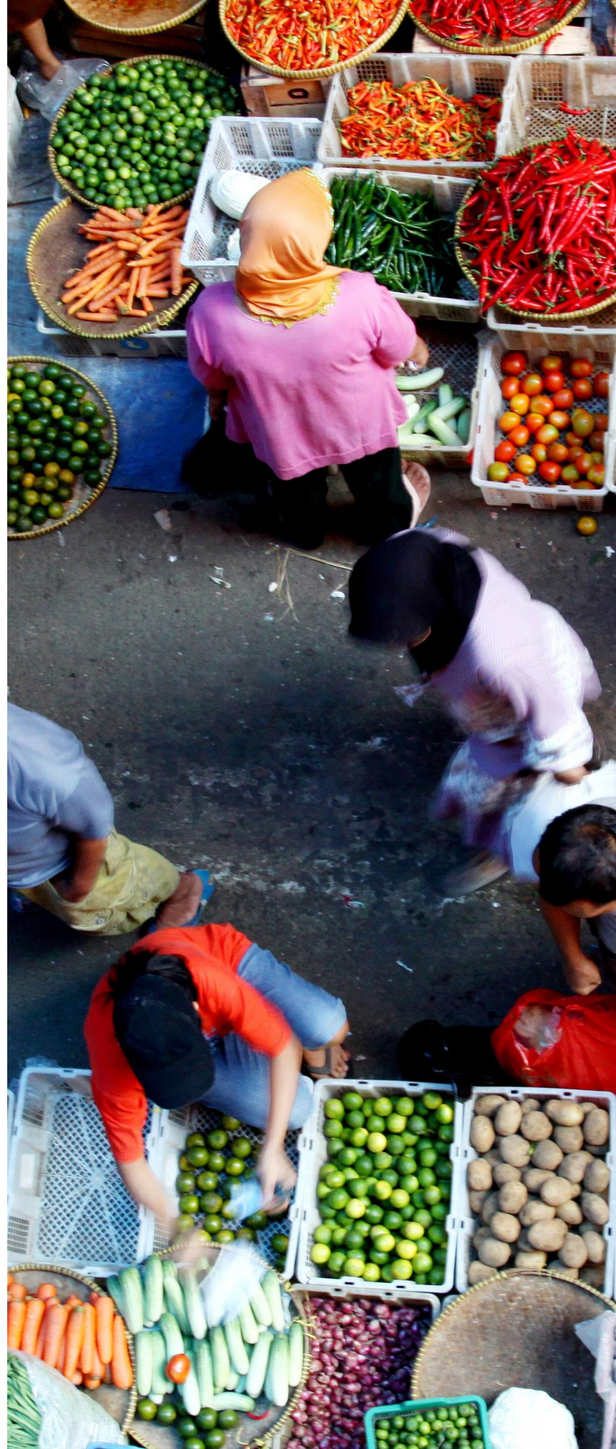
Aon's Insights

Top Risks in the Food, Agribusiness and Beverage Industry

Current Top 10 Risks

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
6 Weather or Natural Disasters	7 Damage to Reputation or Brand	8 Regulatory or Legislative Changes	9 Failure to Attract or Retain Top Talent	10 Product Liability or Recall

Source: Aon Global Risk Management Survey Results 2023



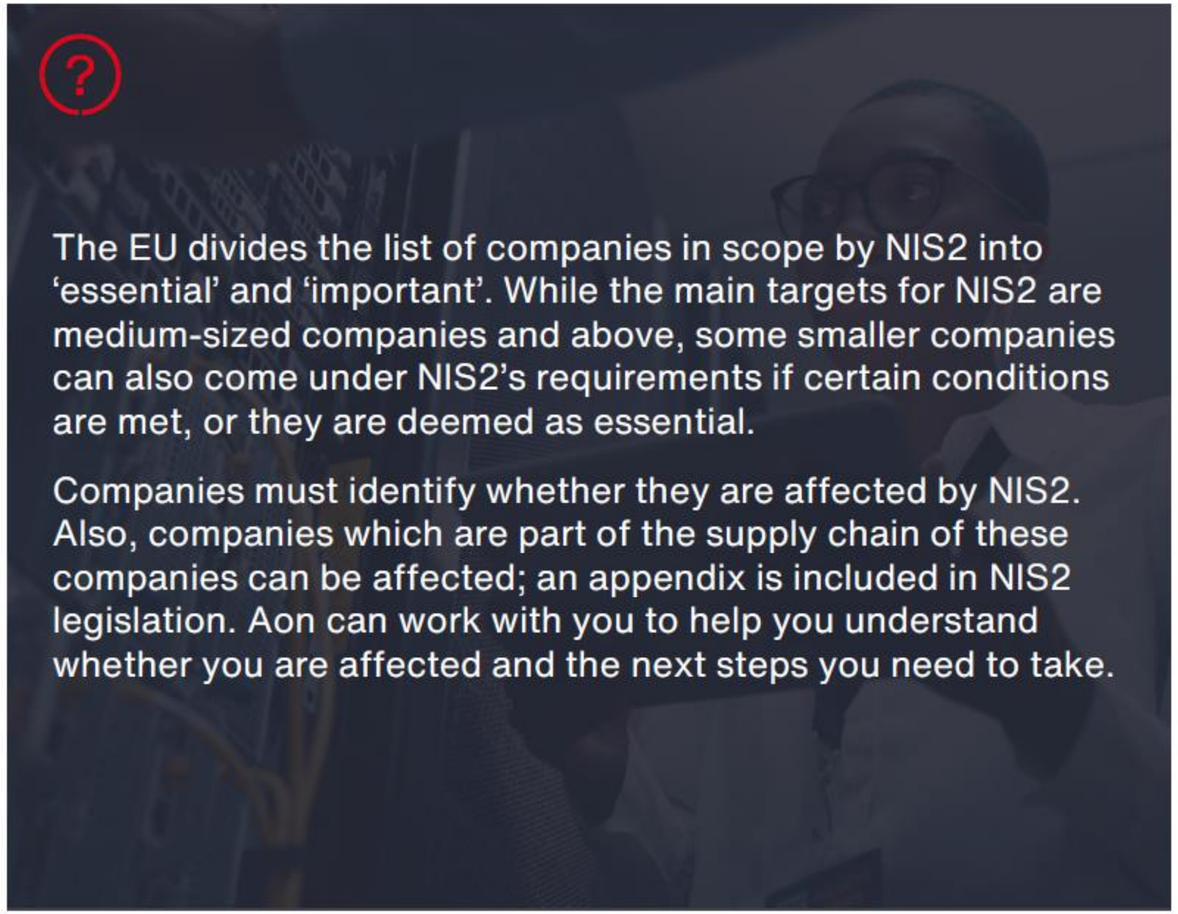
What is it?

The European Union's Network and Information Security (NIS2) Directive replaces the NIS Directive 2016 and aims to ensure a "high common level of cybersecurity across the EU's Member States" by further strengthening cyber security requirements in critical infrastructure, and those industries and organisations that are indispensable for the functioning of the economy.

NIS2 was ratified on 16 January 2023, and each of the EU's member states must ensure it **adopts and publishes measures necessary to comply with the directives by 17 October 2024, with those measures taking effect 18 October 2024.**

For businesses in the UK, the EU law will not be implemented, but it's **expected that an expansion of the UK NIS Directive will include similar requirements to NIS2. And those UK businesses who operate within the EU will have to comply with NIS2 to ensure they can show consistent levels of cyber security standards.**

Who is Affected?



The EU divides the list of companies in scope by NIS2 into ‘essential’ and ‘important’. While the main targets for NIS2 are medium-sized companies and above, some smaller companies can also come under NIS2’s requirements if certain conditions are met, or they are deemed as essential.

Companies must identify whether they are affected by NIS2. Also, companies which are part of the supply chain of these companies can be affected; an appendix is included in NIS2 legislation. Aon can work with you to help you understand whether you are affected and the next steps you need to take.

Essential Entity (EE)		
Finance (Banking and Financial Market Infrastructure)	Energy (Electricity, Oil, Gas, Hydrogen, District Heating)	Transportation (Air, Rail, Road, Water)
Health (Public & Private Healthcare providers)	Water (Drinking and Wastewater)	Digital (Telecoms, Data Centres, Cloud Services)
Space	Public Administration	

Important Entity (IE)		
Postal & Courier Services	Chemicals	Research
Foods	Manufacturing (Medical Devices, computers & Electronics, machinery & equipment, motor vehicles, transport equipment)	Digital Providers (Search Engines, online markets and social networks)

Poll question 1

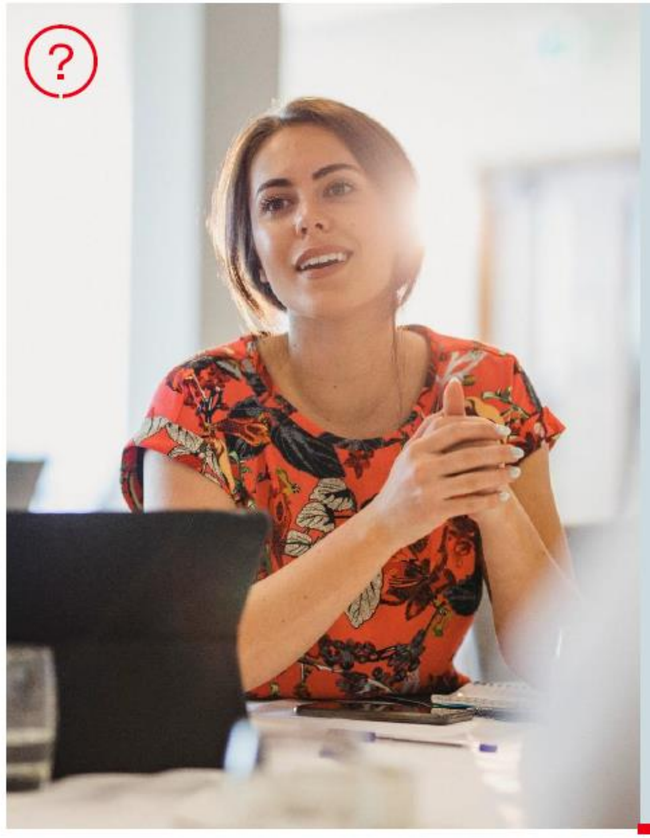
What is the nature of your business in the EU:

1. Large operational footprint including manufacture / distribution
2. Limited operational footprint with some distribution
3. No operational footprint but significant EU customer base
4. Unsure or no significant EU presence or exposure

What is Required?

1 Cyber Incident reporting	2 Cyber Incident handling	3 Supply chain security	4 Assess the effectiveness of cybersecurity risk-management measures	5 Policies and procedures to assess effectiveness of risk management	6 Basic cyber hygiene
7 Policies and procedures regarding cryptography	8 Policies on risk analysis and information system security	9 Security in network and information systems	10 Policies and procedures to assess effectiveness of risk management	11 Multi-factor or continuous authentication (MFA)	

So What?



Reporting

In the event of a cyber incident, organisations must fulfil three specific steps within a tight timeframe:

- Within 24 hours of a cyber-attack, an initial warning must be sent to the authority responsible in their country.
- Within 72 hours, further information about the incident must be provided.
- Within one month, a final detailed report on the incident must be available.

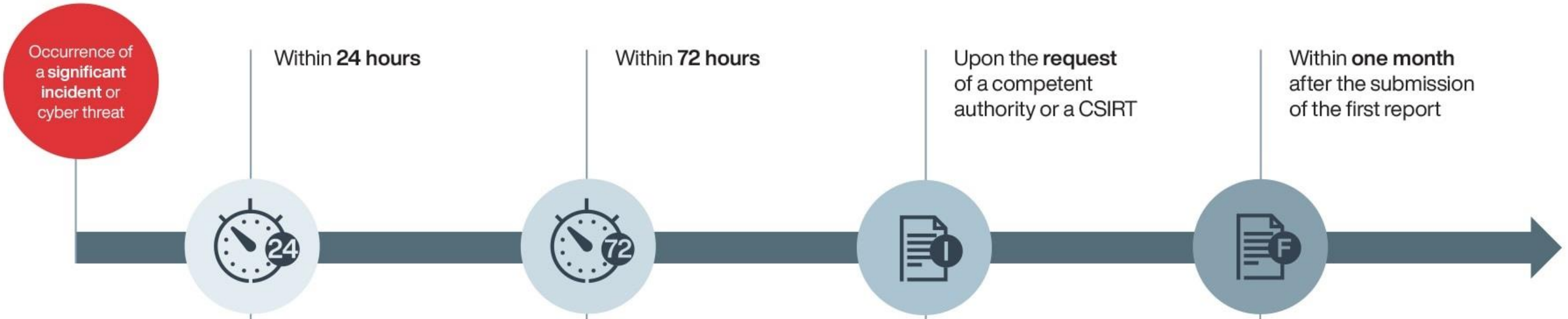
Fines

"Essential" companies found to be non-compliant with NIS2 will face administrative fines of a maximum of €10 million or a maximum 2 percent of their total worldwide annual turnover (whichever is higher)

"Important" companies will see fines of up to €7 million or 1.4 percent (whichever is higher)

NIS2: Reporting Obligations

Timeline in the event of a significant incident or cyber threat



An **initial notification** to competent authorities or the CSIRT, indicating whether it is suspected of being caused by unlawful or malicious acts or could have a cross-border impact

An **incident notification** to update the previous information and indicate an initial assessment of the significant incident, including its **severity and impact**, as well as where available, the **indicators of compromise**

An **intermediate report** on relevant status updates

A **final report** including at least the following:

- A detailed description of the incident, its severity and impact
- The type of threat or root cause that likely triggered the incident
- Applied and ongoing mitigation measures

If the incident is **still ongoing** at that time entities should provide:

- A progress report at that time
- A final report within one month of their handling of the incident

NIS2 details specific reporting obligations in Article 23 - Reporting obligations and not following them could lead to administrative fines being imposed on the entity.

Downstream Implications

Poll question 2

How confident are you that you meet the NIS2 control requirements:

1. We have undertaken a full gap analysis and are compliant
2. We have undertaken a full gap analysis and are working to close gaps
3. We have not undertaken a formal analysis
4. We are not compliant / Unsure if we are compliant

Aon Global Risk Management Survey 2023

Food, Agribusiness & Beverage Risks

Risk Readiness: Are You Prepared?

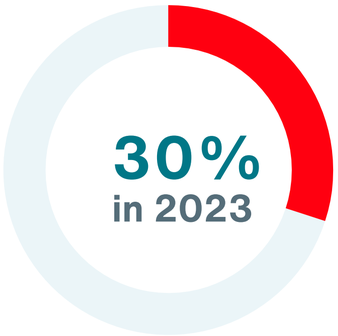
Average Reported Readiness for Top 10 Risks

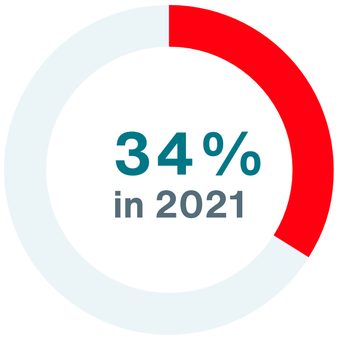
2023
62% Ready

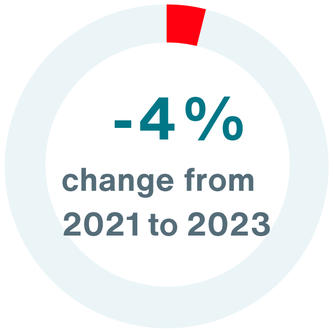
2021
56% Ready

Change from 2021 to 2023
6%

Average Loss of Income from Top 10 Risks





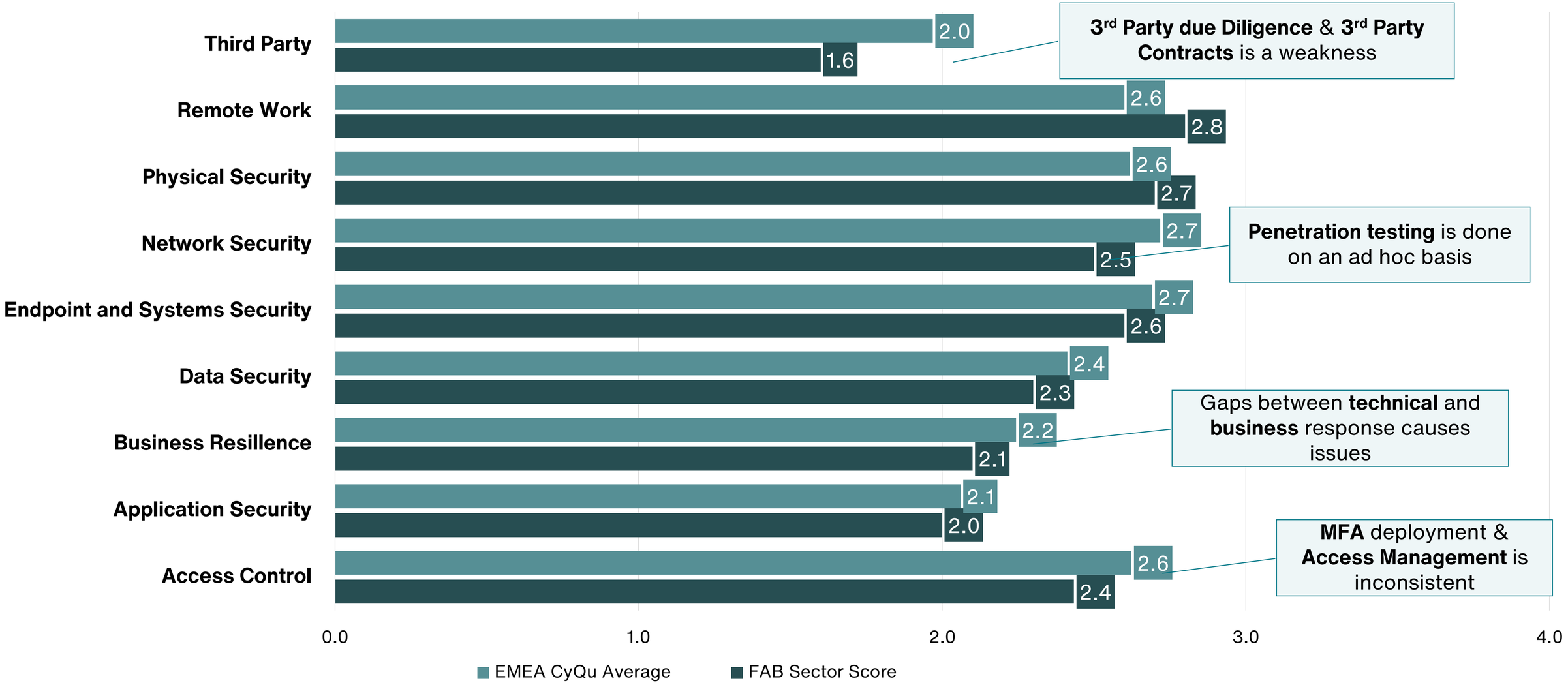


How Organisations Evaluated Their Risk Posture against the Top 10 Risks	
31%	Assessed risk
27%	Developed risk management plan
21%	Developed continuity plans
16%	Evaluated risk finance and/or transfer
13%	Quantified risk

How the FAB Sector Stacks Up

On a par.... The devil is in the detail

Industry Total Score: **2.4**



AON

Poll question 3

How have you engaged with third parties:

1. We have proactively engaged with customers, suppliers and regulators
2. We have engaged with our major customers and suppliers
3. We have engaged with regulators
4. We have not yet communicated with third parties on NIS2

How customer needs may impact you

Currently in the investigation stage

- Customers in the EU are focusing on making a distinction between essential / important providers and the rest of providers – this is driven by risk not revenue spend
- Tiered outreach programme based on the above – focus so far tends to be on Incident Response capability
- Considering contractual language to attempt to enforce mandatory reporting requirements
- Requesting proof of governance process via request for ISO standard compliance
- Evaluation of alternative providers where possible and initiating relationship building

Transmitting confidence to customers

Early outreach and prepared communications

- Training and awareness of frontline staff to equip them to answer customer questions – dedicated “taskforce” with an email inbox to support
- Early engagement with major customers to highlight how you are looking to comply
- Ask customers how quickly they need services up and running. Then provide insight into how you are set up to meet or exceed these
- Focus on promoting their certifications, ISO etc.

Uncertainty over local interpretation

Many are focusing on internal security uplift

1. **Identify your key customers and their regulators (usually driven by HQ location) and engage early**

2. **Leverage best practice standards – realistically evaluate incident notification capabilities**

3. **Prepare for customers to include NIS2 reporting requirements into contracts**

AON

How Aon Can Help

1

NIS2 Gap Analysis

Aon has developed a NIS2 GAP analysis that supplies insight of your current cyber maturity. In about 3 hours two questionnaires are completed by your CISO/IT manager.

An Aon consultant creates a report based on the results of your assessment. Technical and organizational measures will be presented in a report together with our recommendations.

With this insight, Aon prepares a valuable NIS2 GAP analysis.

2

NIS2 board member training

With our years of experience and inhouse expertise in the field of risk management, Aon has developed a workshop that focuses on the additional role of the board.

The two requirements from the mentioned above elements have been incorporated into an interactive workshop to be taken by board members. It is of vital importance that your board members, CISO and IT manager are all present.

After attending the workshop, every member will be aware of his/her role regarding cyber risks.

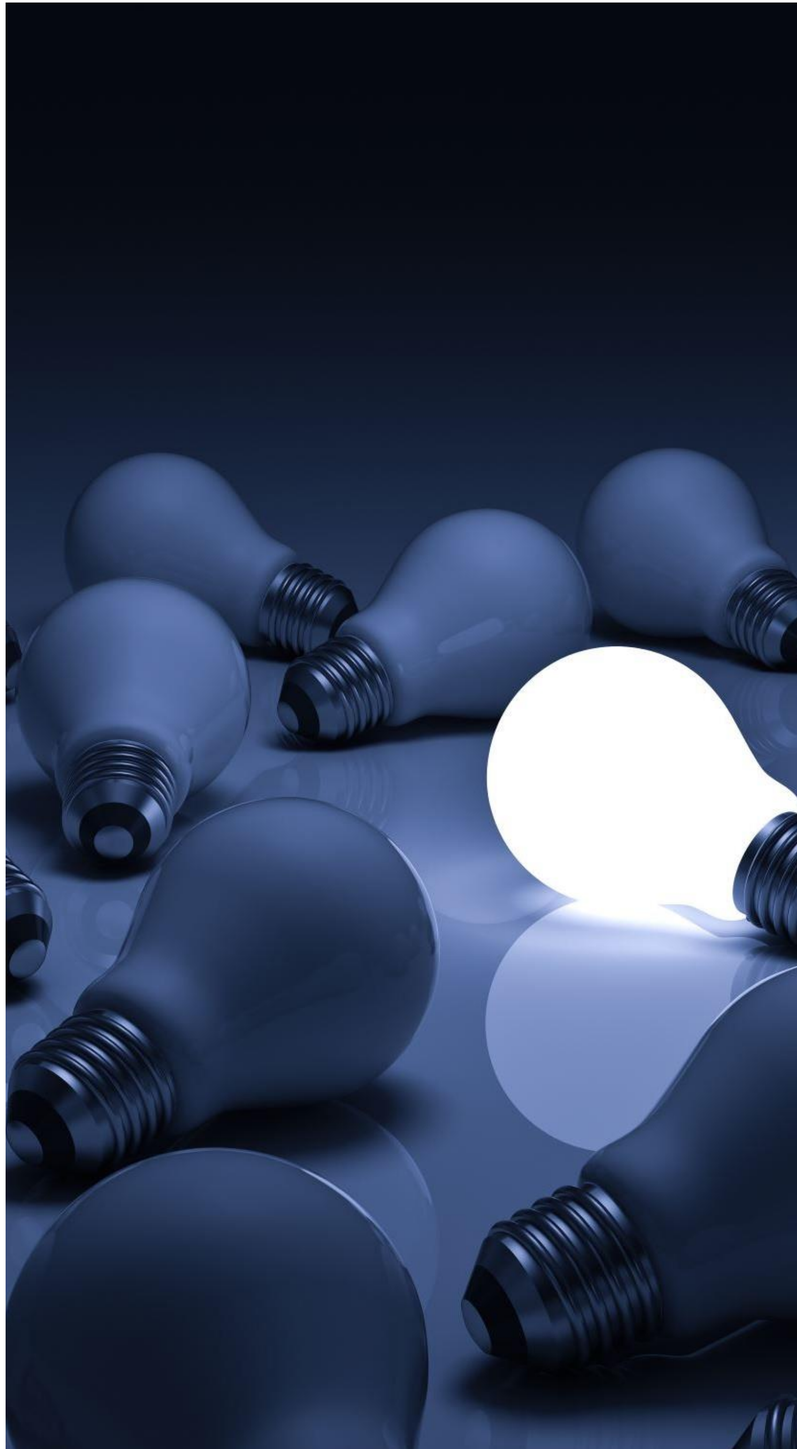
3

Roadmap Development

The insights from the workshop will be put together by an Aon consultant into a consolidated report. This report will be discussed with all stakeholders to determine possible next steps.

With this report we will establish a roadmap to prepare your organisation for the upcoming change in legislation.

Aon will help you clarify the implementation of the appropriate measures.



Our diverse team of consultants and risk and insurance specialists will give you insight of your current level of cyber resilience and how to increase it. As an additional service, we may also quantify the financial impact and advise on ways to mitigate it. This can be done by taking out insurance: we guide this process completely for you. We work for very large organizations as well as for small and medium-sized enterprises. The Cyber Solutions team is part of Aon Global Risk Consulting, one of the largest risk advisors in the world.

AON

Questions and answers

Contact Us

Chris Scott
Head of Cyber Solutions - UK
chris.p.scott@aon.com
+44 7386 655 212

Richard Fawcett
Industry Leader – Food, Agribusiness & Beverage (UK)
Richard.s.fawcett@aon.co.uk
+44 (0) 777 475 1378

https://www.aon.com/en/industries/food-agribusiness-and-beverage

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.

www.aon.com