

Data protection, information security and cake

29 March 2023



About Adapta

- We are a **specialist** information systems consultancy
- We only work with **charities**, associations, trusts and others in the not-for-profit sector
- We are completely **supplier-independent**
- Our consultants have held **senior** positions in a broad range of different organisations
- Our advice and guidance is based on **practical experience** gained over many years

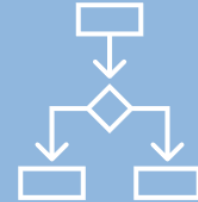
About Adapta



Digital, Data & Technology Strategies



Reviews & Health Checks



Business Processes & System Requirements



Supplier & Solution Selection



Interim Technical Leadership



Programme & Change Success



Risk, Compliance, Data Protection & Security



Governance & Business Cases



Digital Workforce & Operating Models





Programme

- 14:00 **Arrival and welcome**
Welcome - introductions and overview of the agenda for the afternoon.
- 14:10 **Data protection and information security – what’s new in the sector?**
Fiona Brookes, Adapta Consulting
Case Study 1
Beverley Adams-Reynolds, Data Protection Officer, Crisis
- 15.00 **Mid-afternoon break (tea/coffee and more cake)**
- 15.20 **Case study 2**
Arturo Dell, Director, Knowledge Industries
- 15:45 **Roundtable discussion & feedback**
All
- 16.30 -
17.00 **Review & close**
Paul Sypko, Adapta Consulting



Introductions

Fiona Brookes, Adapta:

Data protection and information security – what's new in the sector?



Data protection and information security – what's new in the sector?

29 March 2023

Outline agenda

- Data Protection Act 2018 & UK GDPR – reminder
- What's new ? – Data Protection & Digital Information Bill
- Common data protection risks and practical steps

1984



1998



2003



2018



2021



2022



2023



Data Protection Act 2018



Article 5 Principles

- Lawfulness, fairness & transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity & confidentiality (security)
- Accountability

Data Subject Rights

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

What's new?

Data Protection & Digital Information Bill (DPDI)

Initial key takeaways from the Bill are:

1. Clarification around legitimate interests
2. Records of processing only required for organisations that carry out high risk processing activities
3. Direct marketing – soft opt in continues
4. Greater fines for nuisance calls and texts
5. Cookie rules to be relaxed
6. Creation of a framework for the use of digital verification services
7. DPO changes to Senior Responsible Individual (SRI)
8. ICO reform

Common risks and practical steps

Risk area	Practical steps
Privacy policy	- Review and update regularly
Staff training	- Refresher training, new staff, volunteers
Storage limitation	- Review data retention
New projects, new processing	- Assess risk, DPIA
International transfers of personal data	- Map and document transfers

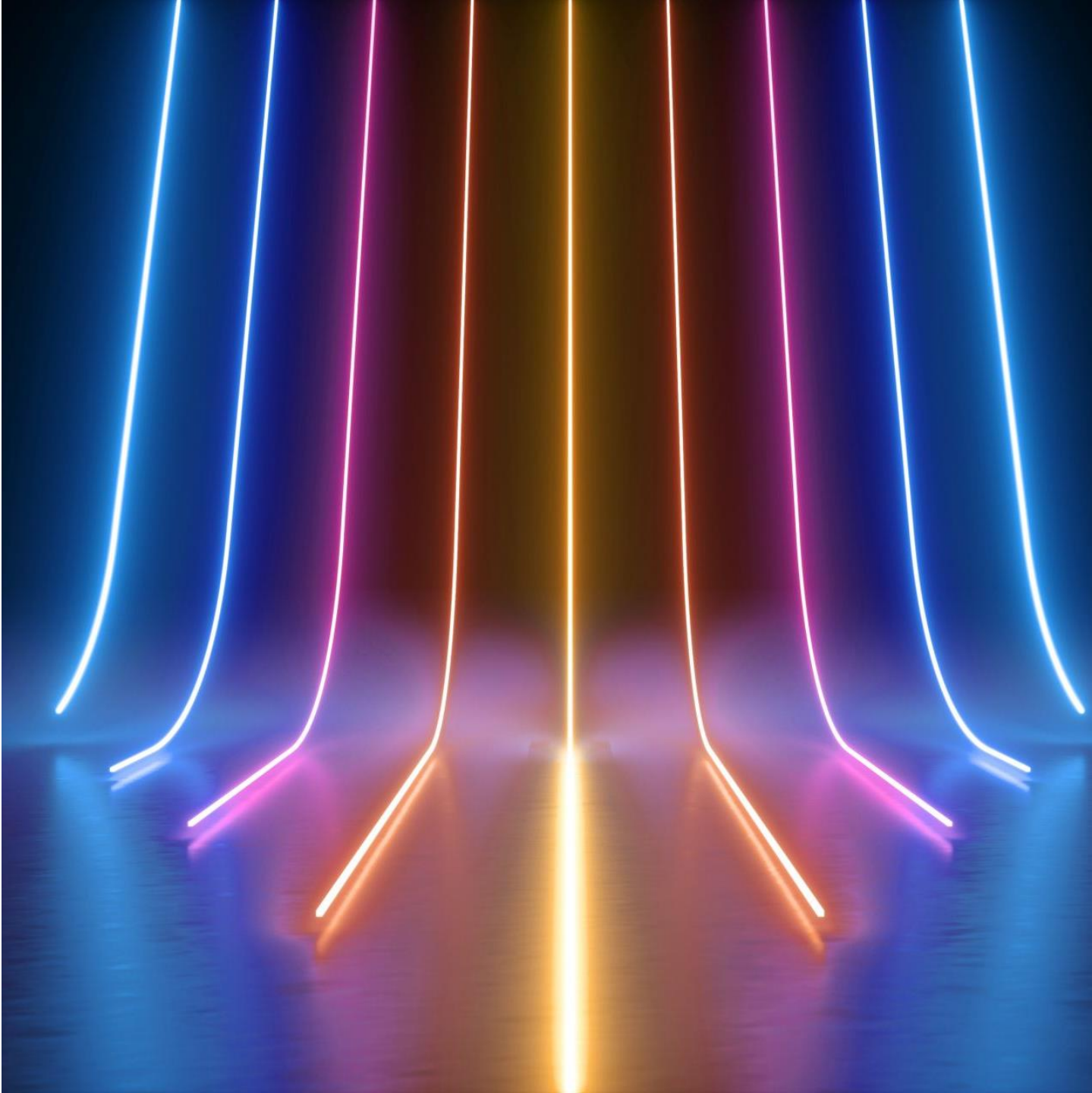


Case study 1:

Beverley Adams-Reynolds, Data Protection Officer - Crisis

GPDR – 5 years on....

*Impact on DP in the
charity sector*



What's in store...

- + A (tiny) bit about me & Crisis
- + Consent isn't everything... know your lawful basis
- + Get your DSAs (*data sharing agreements*) right..
- + Programmatic advertising & cookies
- + Understanding your organisational risk appetite
- + International transfers
- + Privacy Maturity & Accountability
- + Q & A

A brief history ...

- Around since the early 1960s...
 - Crisis at Christmas
 - 11 regional 'skylight' centres
 - Politically active
- Bev (not Beverley)
- 20+ years in DP & IG
- Dabbles in PECR & Security
- Over a decade in Charity sector
- Passionate about protection of citizen rights



Consent isn't everything know your lawful basis

- + Consent in the charity sector...

Informed?

Freely given?

Capable of being withdrawn?

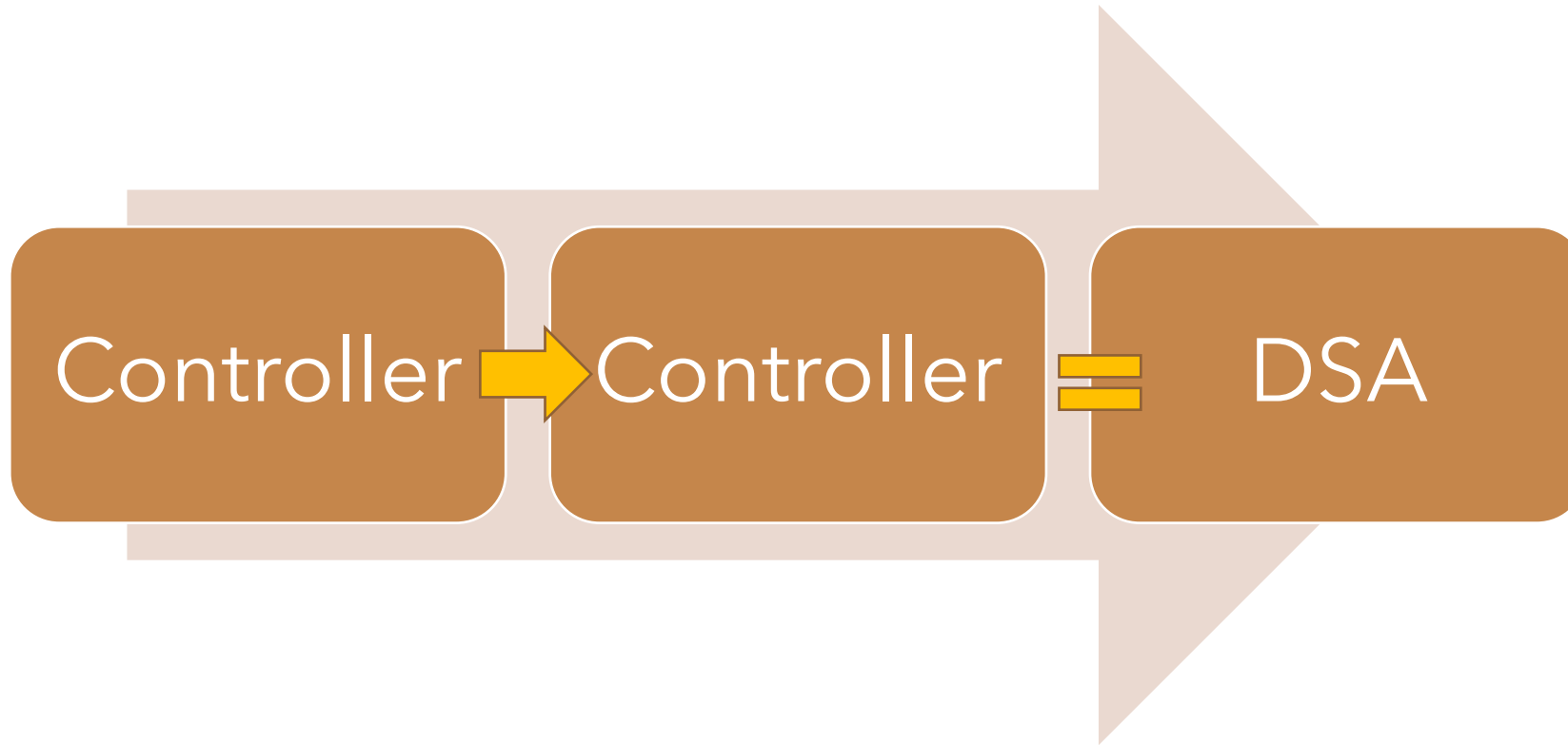
Access to a service dependant on consent being given?

- + Alternatives?



Document the purpose*....

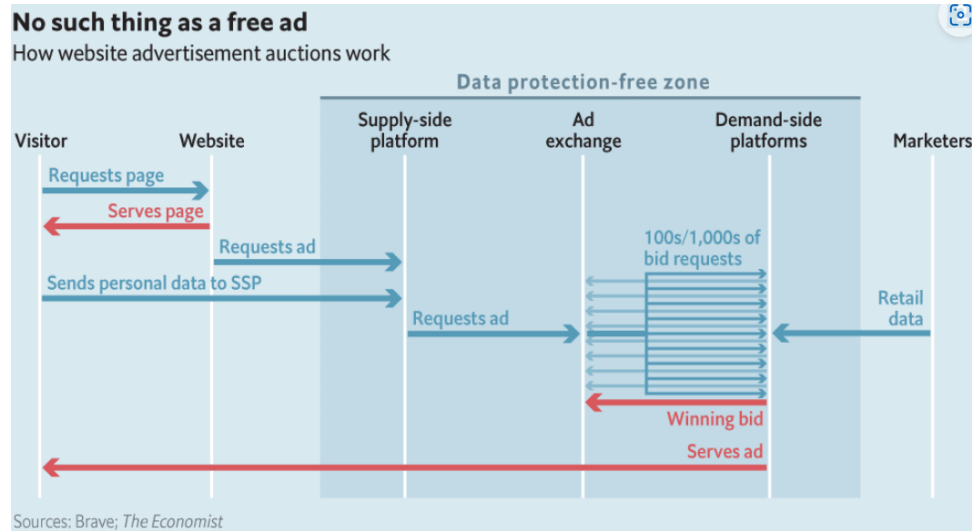
DPIAs....



**Get your
DSAs right....**

- For systemic sharing
- Documented :
 - purpose
 - Lawful basis
 - Data fields
 - Security
- Rights Management
 - Informed
 - Access
 - RTBF
- Retention
- Secondary usage

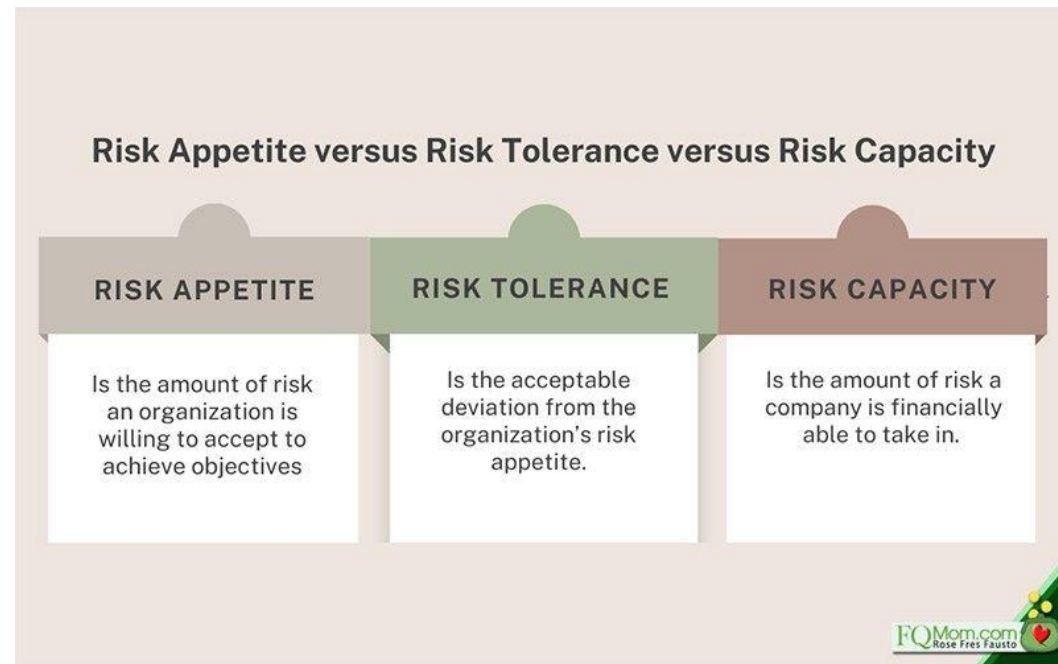
Programmatic advertising & cookies...



- PECR:
 - Informed consent needed to drop all bar 'essential' cookies on to a user's device
 - Accept / Reject All buttons
- Understanding your cookies
 - audit
 - Due diligence (as far as you can...)
 - Data journeys
 - Cookie maintenance & management
- Who are your users?
- Webpage replication? Or precision loading?
- What are the ramifications in terms of privacy....

Understanding your organisation risk appetite...

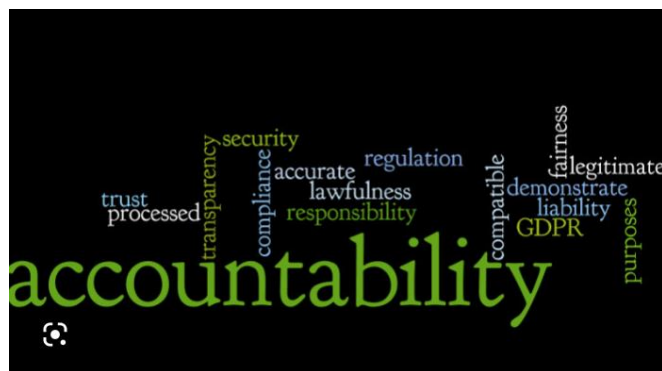
- Appetite and tolerance to risk will vary according to activity
- Do you have conflicts of interest?
 - Zero tolerance to regulatory non-compliance Vs high risk for income generation
- Has there been a shift since the pandemic and cost of living crisis?
- Where does the Privacy & the DPO sit?





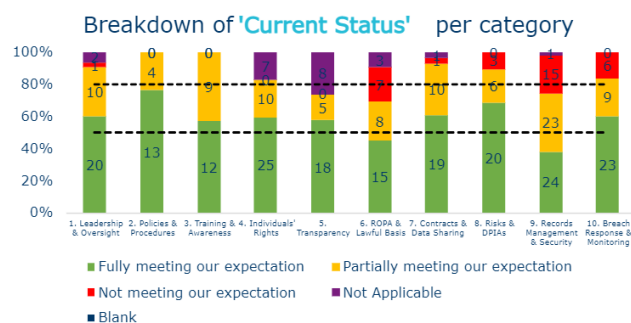
International data Transfers...

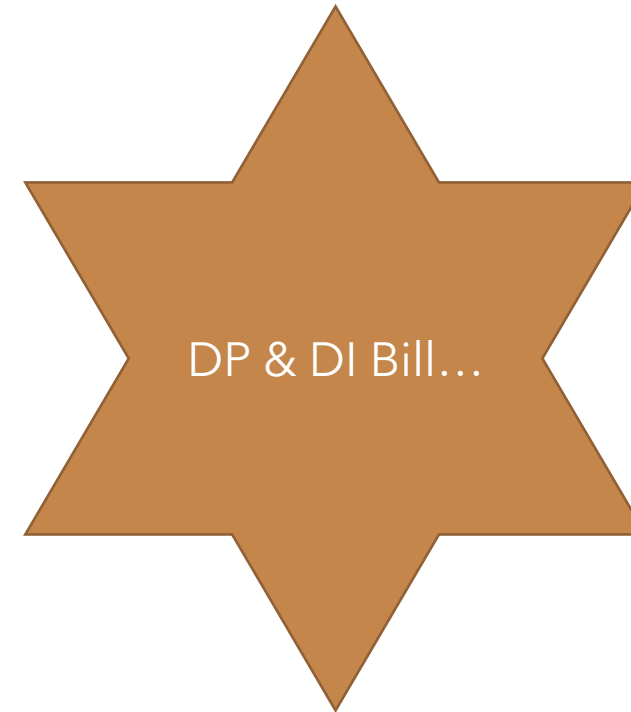
- Due diligence and the full data journey
 - Project management & DPIAs
- Adequacy, SCCs, SCC addendums or IDTAs...
- Transfer Impact Assessments
 - & what about cookies....
- EU>US agreement & Schrems III (?)



Accountability & Maturity – the golden thread...

- The overarching Principle
- Evidence & action plan
 - ICO framework?
- Links to risk appetite & proportionality
 - Trustee engagement
 - Interplay with your stated risk appetite
 - How good is good enough?
 - Cost Vs Reward





Case study 2:

**Arturo Dell, Director,
Knowledge Industries**



Running a WARP

What I've learned from running a Warning, Advice and Reporting
Point over the last 4 years

Arturo Dell - Director



Everything has changed

Fast forward button



Fast forward button



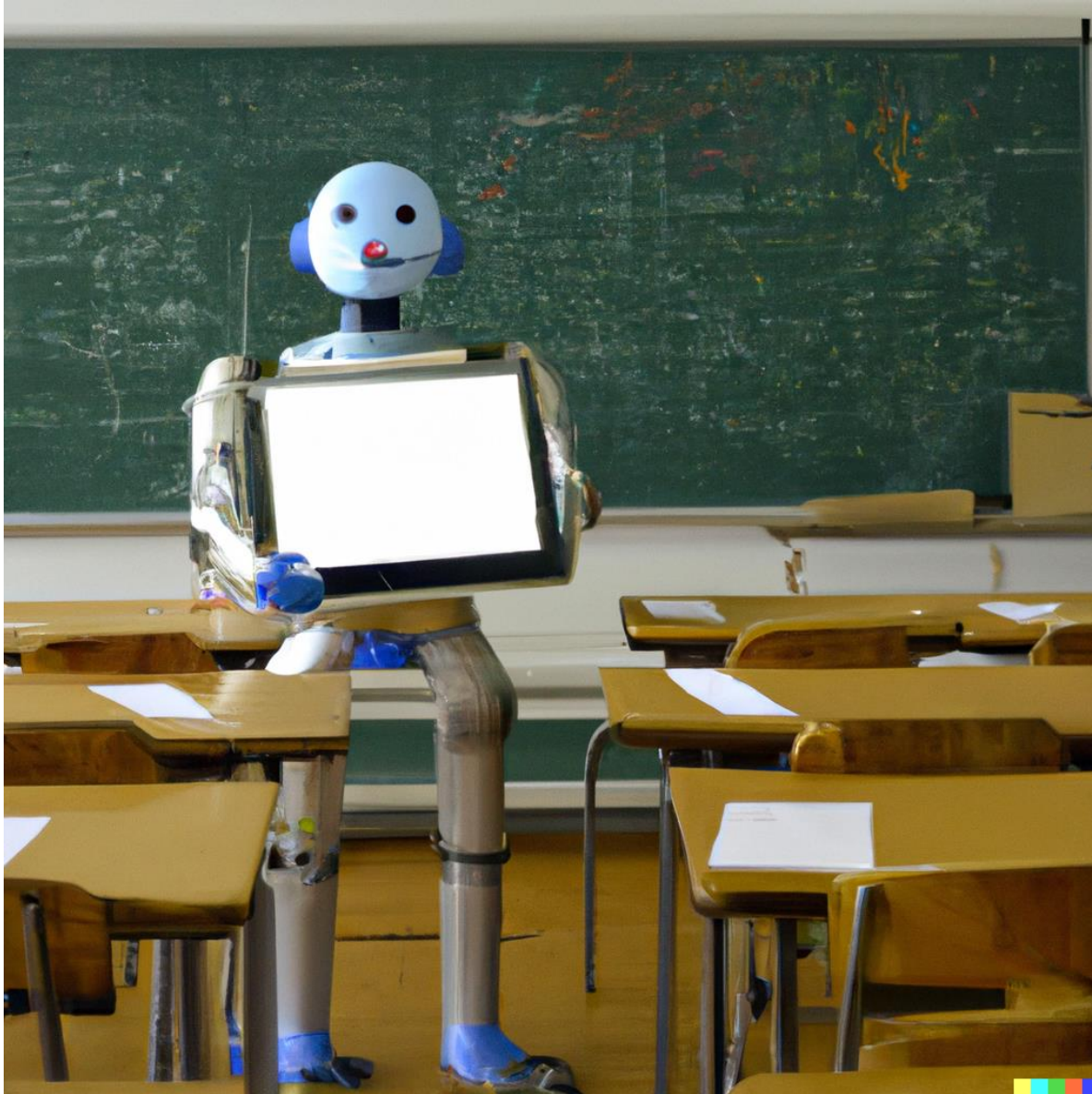
“We’ve seen two years’ worth of digital transformation in two months”.

Satya Nadella – CEO Microsoft

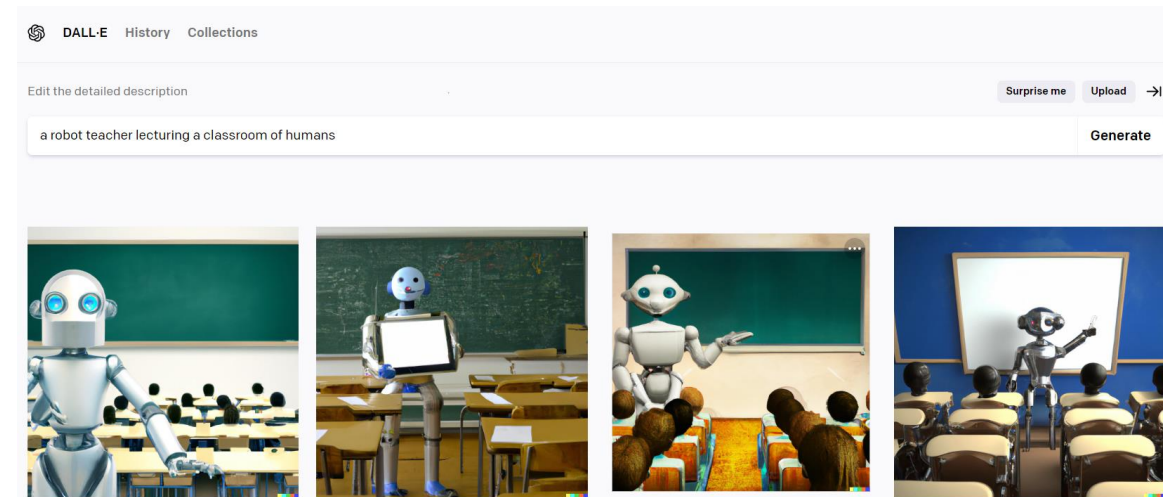
Forced experiment – Home working



The explosion of AI



‘A robot teacher
lecturing a classroom
of humans’



The current cyber risk landscape

2022 Data Breach Investigations Report

Gain vital cybersecurity insights from our analysis of over 23,000 incidents and 5,200 confirmed breaches from around the world—to help minimize risk and keep your business safe.

**Know what your
business is up against.**

82%

of breaches involved the Human Element, including Social Attacks, Errors and Misuse.

13%

increase in Ransomware breaches—more than in the last 5 years combined.

62%

of incidents in the System Intrusion pattern involved threat actors compromising partners.

An unfair advantage



Hackers share intelligence and resources to coordinate attacks



While we try to manage a growing number of risks and demands with limited resources

Working together to fight back

W arning

A dvice

R esponse

P oint



National Cyber
Security Centre

a part of GCHQ

- Trusted information Sharing
- Established in 2003 by a group of London Boroughs
- All across the public sector
- Model exported to Netherlands and Japan

Housing Providers WARP



ForHousing



Sanctuary



Getting to know and trust your WARP colleagues







Working together to solve real problems

Two tribes: Cyber or governance?



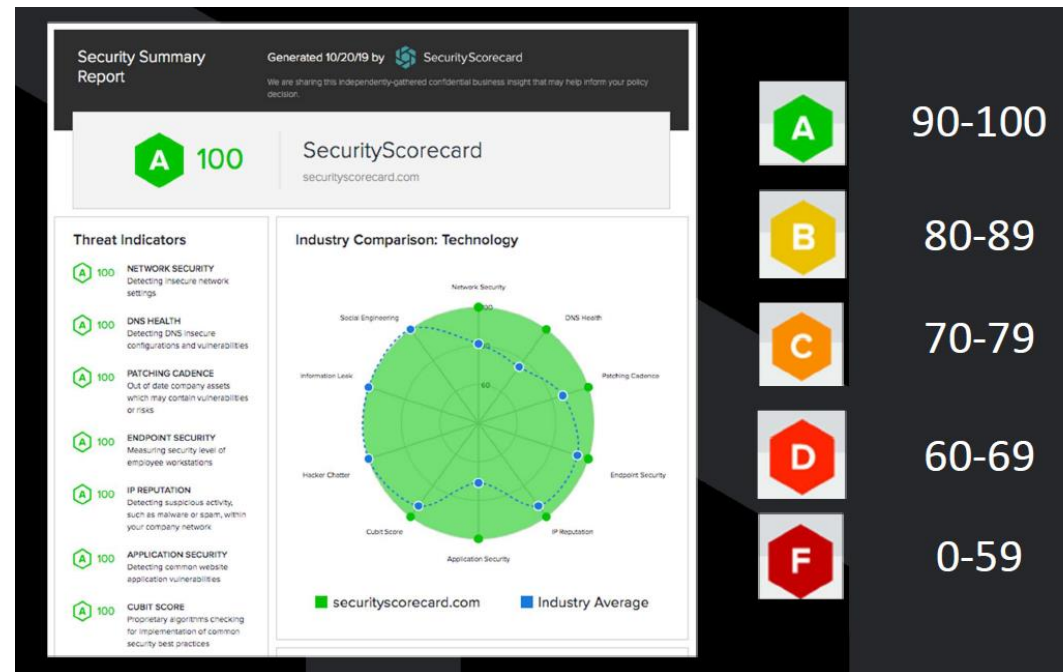
Developing trust

Traffic Light Concept/Chatham House Rules

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

When a meeting, or part thereof, is held under the **Chatham House Rule**, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

What have we learned over the past year?

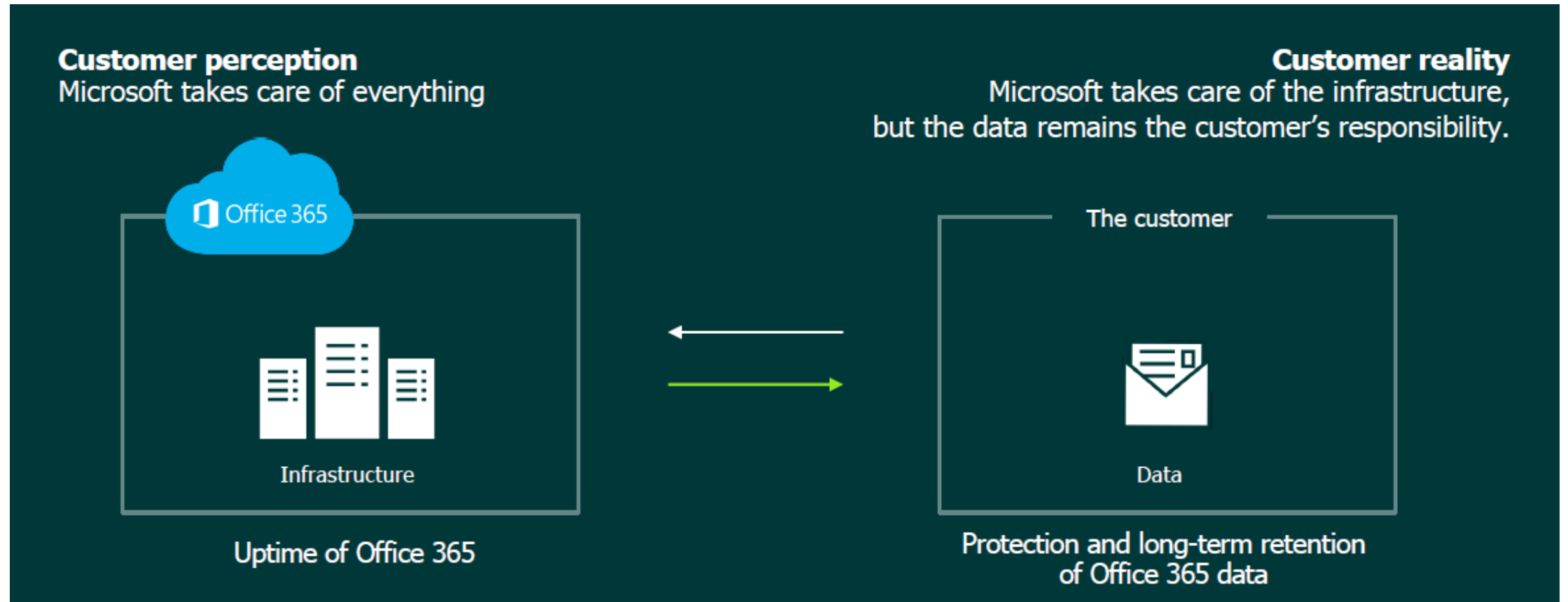


Passwords remain a problem





Do we need to backup Office 365?



Who does what in the cloud?

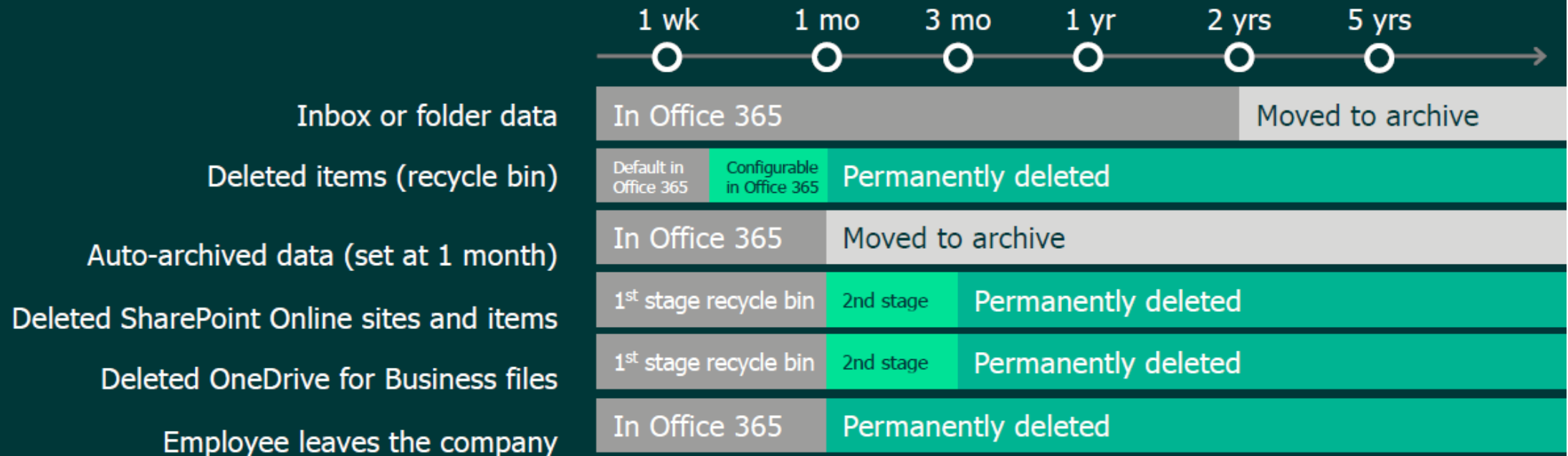
The Office 365 Shared Responsibility Model

Microsoft's Responsibility Learn more from the Office 365 Trust Center	Primary Responsibility	Supporting Technology	Security	Regulatory
	Microsoft global infrastructure Uptime of the Microsoft Office 365 Cloud Service	Office 365 Data Replication DC to DC geo-redundancy Recycle Bin Limited, short term data loss recovery (no point-in time recovery)	Infrastructure-Level Physical Security Logical Security App-level Security User/Admin Controls	Role as data processor Data Privacy Regulatory Controls Industry certifications <i>HIPPA, Sarbanes-Oxley</i>
YOUR Responsibility	Your office 365 data Access and control of your data residing in Office 365	Office 365 Backup Copy of your data stored in a different location Full Data Retention ST & LT retention filling any/all policy gaps <i>granular & point-in time recovery options</i>	Data-Level <i>Internal:</i> Accidental Deletion Malicious Insiders Employee Retaliation Evidence Tampering <i>External:</i> Ransomware Malware Hackers Rogue Apps	Role as data owner Answer to corporate and industry regulations Demands from internal legal and compliance officers

A complex, evolving picture

Retention policies:

What exactly does
Microsoft back up?



Office 365 backup and retention policies can **only protect you from data loss in a limited way** and are not intended to be a complete backup solution.

Retention policies are always evolving and tend to be **very complicated to manage and monitor**. Commonly, Admins believe they are covered, only to find that in fact certain items are gone.

Cyber insurance: what are you covered for?



Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine

Email Phil Follow @philmmuncaster



More than 80% of UK businesses still don't have cyber-related insurance despite widespread recognition of the risks associated with rising threat levels, according to [Gallagher](#).



The insurer polled 1000 UK business leaders in organizations of various sizes, and nearly two-fifths (39%) cited cyber-attacks as one of their biggest concerns. However, 82% claimed not to have specialist insurance.



Gallagher argued that many firms may be buying catch-all policies which may not pay out in the event of a serious security breach, while others either underestimate cyber-threats or have too much confidence in their ability to defend against attacks.

It claimed that nearly half (46%) of respondents from mid-sized firms believe that cyber-attacks are "mainly an issue for bigger organizations."

Of course, the stats show that, while sophisticated targeted attacks may only strike larger companies, firms of all sizes are regularly the subject of automated cyber-raids. ISP Beaming [warned in January](#) that the average UK firm was hit by over half a million attempts to compromise systems last year, a 152% increase on 2018.

Network device admin tools and IoT endpoints like connected security cameras and building



Related to This Story

Why Cyber Insurance Works

Cyber Insurance Achilles Heel Contains Opportunity

Human Error Linked to 60% of Security Breaches

Some helpful guidance from NCSC



GUIDANCE

Cyber insurance guidance

Cyber security considerations for organisations thinking about taking out cyber insurance.

PUBLISHED

6 August 2020

REVIEWED

6 August 2020



Download Article
PDF

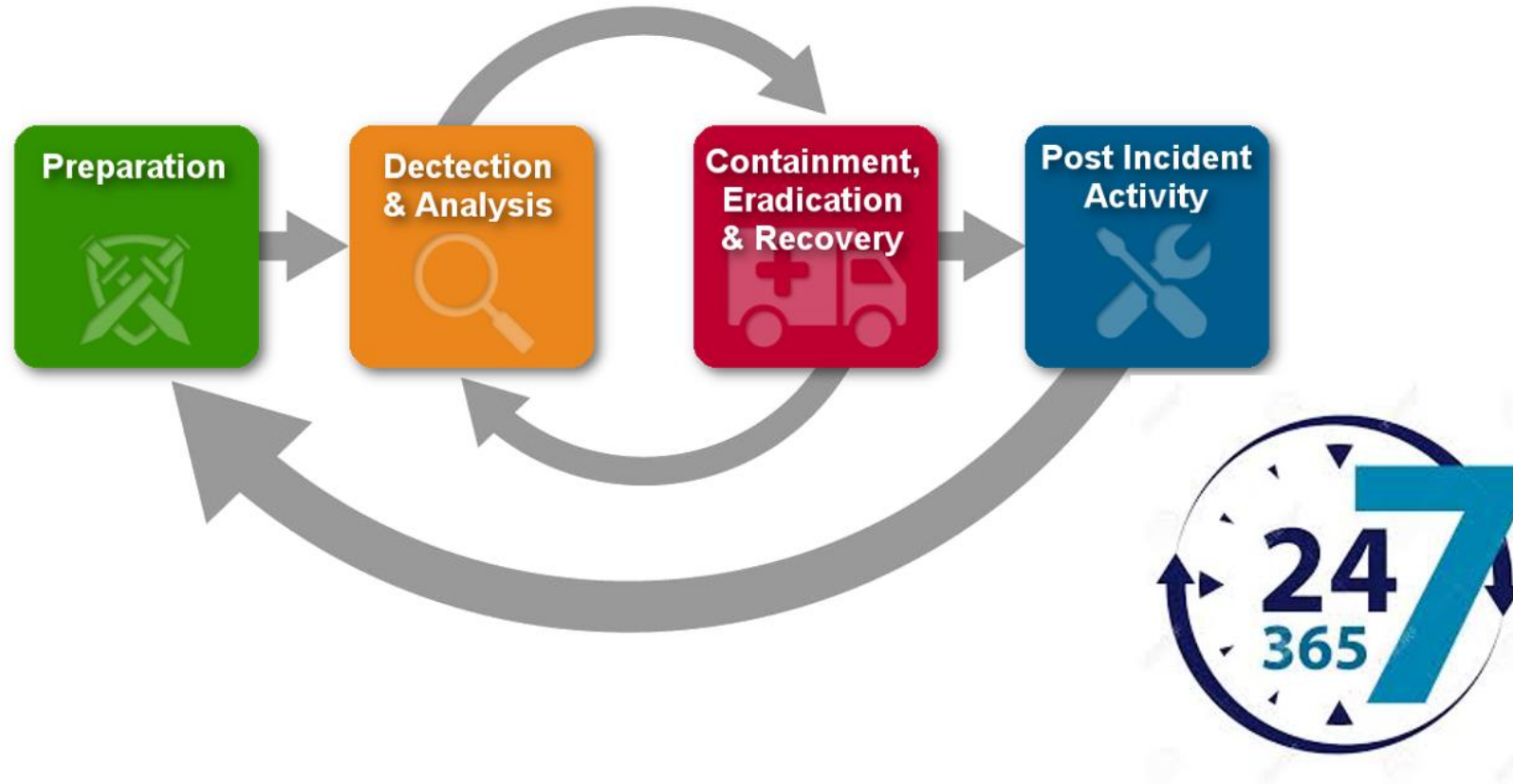


Share



Print

Cyber incident response retainer: a must-have



Security ratings: a credit score for cyber

Board Report

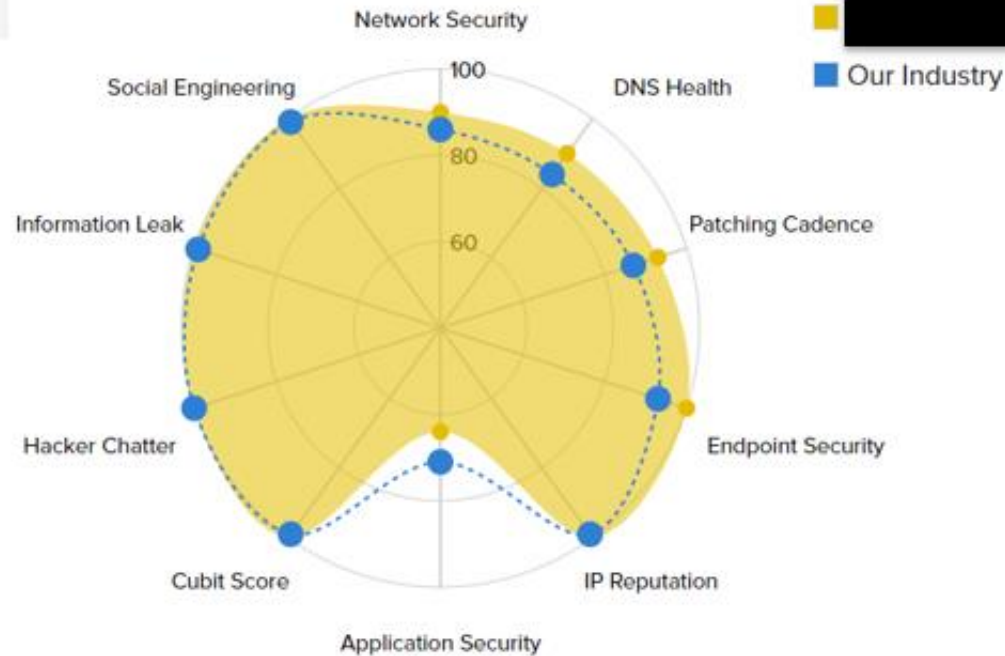
Prepared by  SecurityScorecard






SECURITY POSTURE SUMMARY FOR [REDACTED]

PREPARED ON DEC 01, 2020

OUR CURRENT SECURITY SCORE

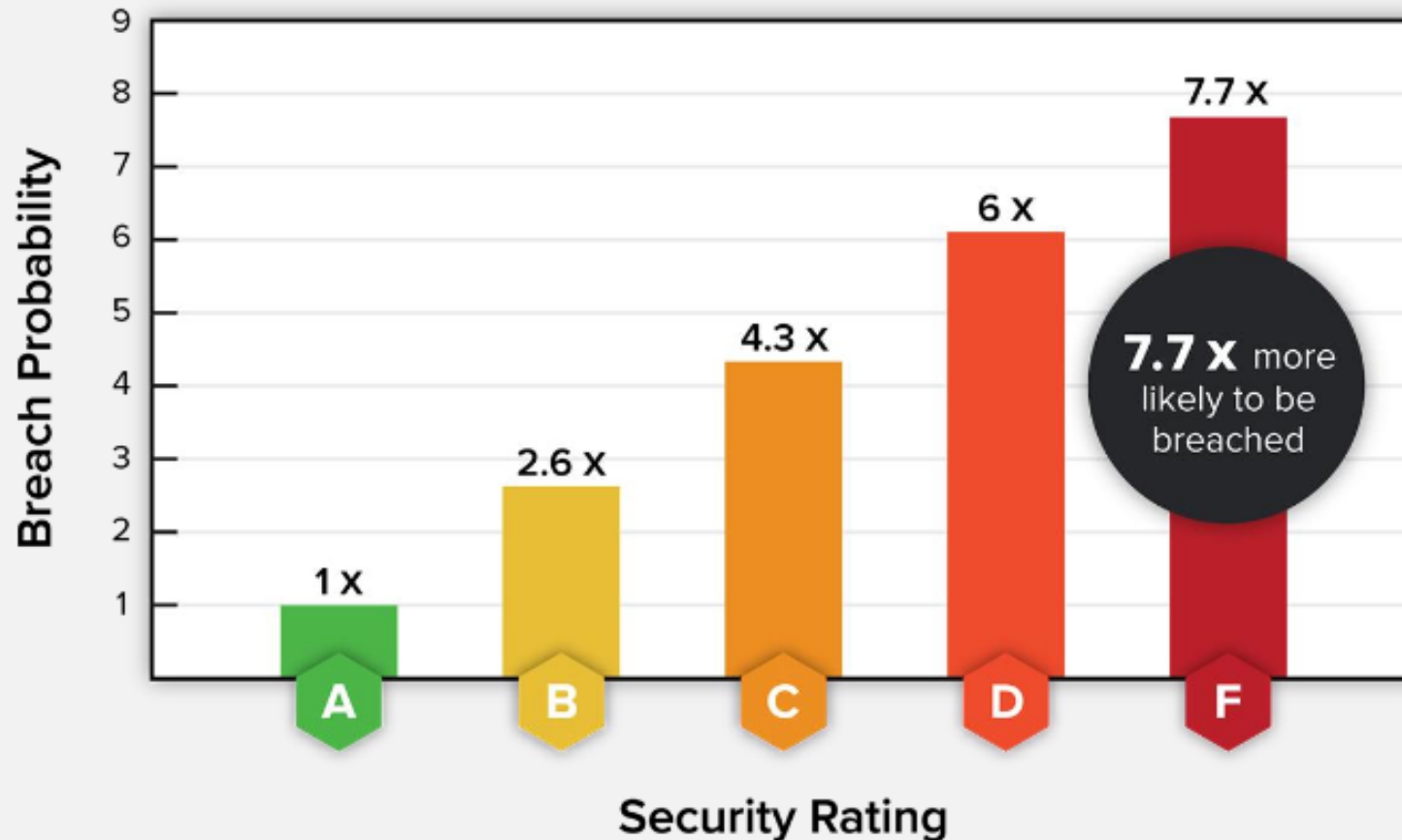
B 88



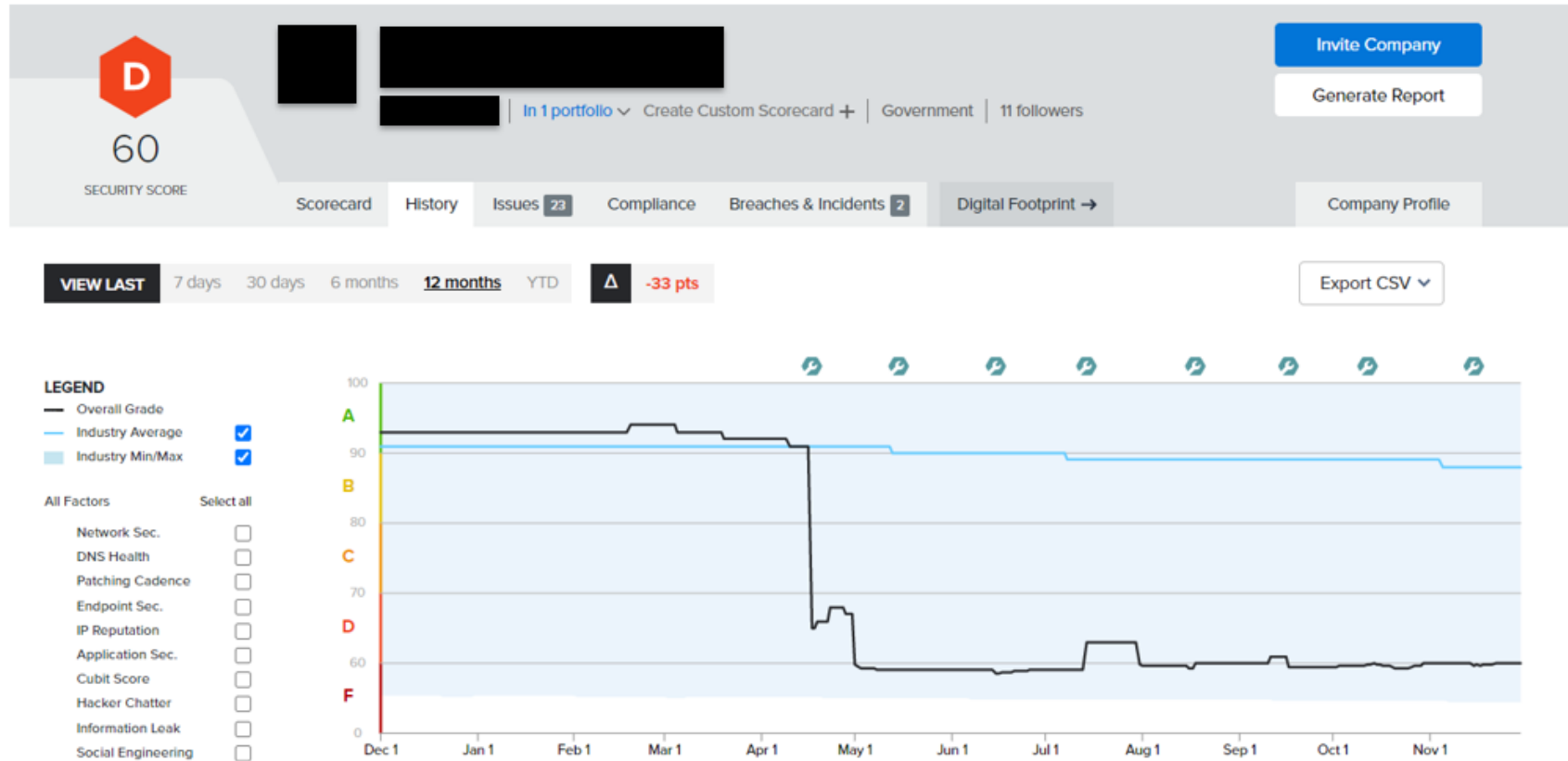
	90-100
	80-89
	70-79
	60-69
	0-59

Why does the score matter?

Companies with a better SecurityScorecard rating are more resilient



Constantly monitoring security helps spot issues



Improve Your Score

We can generate a plan to improve your score ?

C → **A**

Generate Plan

(Don't worry, you can adjust it afterwards)

Already know what to do? **Create Your Own Plan**

Cancel

Benchmarking: how is our security relative to others?

7 companies

Print to PDF



FACTORS

Network Security	D 62	D 66	A 100	A 94	A 96	A 93
DNS Health	A 90	A 100	A 90	A 90	A 100	A 90
Patching Cadence	A 90	F 42	A 100	A 100	F 50	A 91
Endpoint Security	A 100	F 39	A 90	A 100	A 100	A 100
IP Reputation	A 100	A 100	A 100	A 100	A 100	A 100
Application Security	F 55	D 62	B 83	B 89	C 77	C 78
Cubit Score	A 100	A 100	A 100	A 100	A 100	A 100
Hacker Chatter	A 100	A 100	A 100	A 100	A 100	A 100
Information Leak	A 100	A 96	A 100	A 100	A 100	A 100
Social Engineering	A 100	A 92	A 100	A 100	A 96	A 100

Only as strong as our weakest link



How secure are our vendors and suppliers?

Streamlined *Third Party Risk Management* is a “must-have” for organizations of all sizes

59%

of organizations
experienced a data breach
caused by one of their
third parties or vendors

583

average number of third-
parties with access to
organizations' sensitive
data

16%

of organizations say
they effectively
mitigate third-party
risks

How can we improve the security of everyone?

- Security ratings as a simple metric of cyber risk
- Benchmark your security position against your peers
- Manage the risk of third party suppliers
- Learn from your peers and share intelligence
- Engage Exec teams and Boards
- Monitor regularly and focus on the high-risk areas either internally or with suppliers
- Don't forget the dreaded passwords!

Roundtable discussion

- **Question topic 1:**
 - What do you think are the main risks in relation to data protection and information security that most not-for-profit organisations should be thinking about right now?
- **Question topic 2:**
 - What can/should you be doing to make sure your organisation minimises its risks?

Event feedback

Please use the QR code to view and complete the online feedback form.



Thanks & Goodbye!



Upcoming events... Managing and resourcing your IT function and cake

17 May 2023, 2pm-5pm

Live at The RCN, London.

www.adaptaconsulting.co.uk/adapta-events



hello@adaptaconsulting.co.uk



www.adaptaconsulting.co.uk



5 St John's Lane, London, EC1M 4BH



020 4558 8070

We hope you find this presentation enjoyable and thought-provoking. Please note that this document (or this recording of the presentation, as applicable) is provided for general information purposes only and does not constitute professional advice. No user should act on the basis of any material contained in the presentation or any of its supporting materials without obtaining proper professional advice specific to their situation.

Adapta has made reasonable efforts to ensure that the information provided is accurate and reliable, however no warranty is given regarding the accuracy or reliability of such information. All content is subject to change at any time and without notice.

The presentation may include references to specific products or services and/or links to other resources and websites. These references and links are provided for your convenience only and do not signify that Adapta endorses, approves or makes any representation or claim regarding the accuracy, copyright, compliance, legality, or any other aspects of the products, services resources or websites to which reference is made.

Additionally, the presentation may contain confidential and/or proprietary information, and must not be re-used or disclosed to third parties without the prior written approval of Adapta Consulting LLP.

© Adapta Consulting LLP 2023

If you would like further information or any advice regarding your own specific issues, then please do contact the Adapta team at hello@adaptaconsulting.co.uk