Charities and their Cyber Security

Source Cyber Security Breaches Survey '23

Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Charities and their Cyber Security

In this document we have put together Charity Specific Stats from the NCSC's 2023 Breach Report and added our opinions as to where we think the minimum standard for Charities is where relevant.

- 4. Extent to which Cyber Security is a high or low priority for Trustees
- 5. How Often are Trustees given an update on any actions around Cyber Security
- 6. Awareness of the following Government guidance, initiatives or campaigns
- 7. Activities carried out to identify security risks over the last 12 months
- 8. Why Don't Charities review Supply Chain risks?
- 9. Charities undertaking action in each of NCSC's 10 Steps areas
- 10. Charities that have the following rules or controls in place
- 12. When Charities last created, updated, or reviewed their Cyber Policies or Documentation
- 13. Charities with Cyber Policies that have the following given features within
- 14. Charities adhering to various cyber security standards or accreditations
- 15. 10 Step Action / Breach reported in last 12 months
- 16. Types of breaches affecting Charities over the last 12 months
- 17. Charities reporting breaches over time
- 18. How often Charities reported breaches over last 12 months
- 19. Outcomes of the breaches reported by charities in the last 12 months
- 20. Charities that have done any of the following since their most disruptive attack or breach (last 12 months)

Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

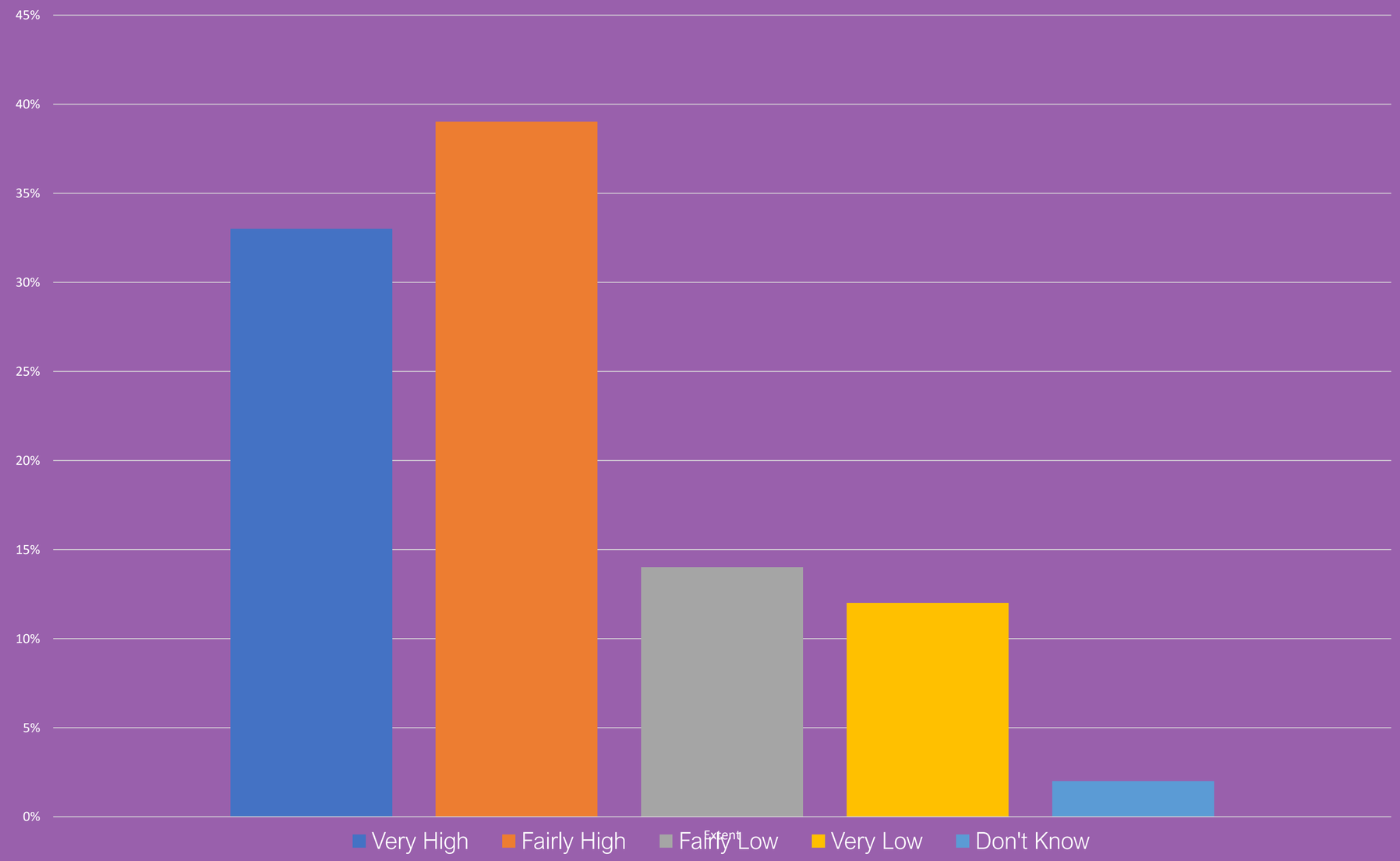
Charities and their Cyber Security

Charities are particularly vulnerable to cyber-attacks. Their focus is understandably fundraising, and they often hold a lot of sensitive personal information including high net worth individuals, and have limited budgets for investing in the highest level of cyber security.

Charities rely more on personal devices than organisations generally and supply chain security is (like many organisations) weak.

The stats in this document are based on the 2023 Cyber Breaches report produced by the NCSC…

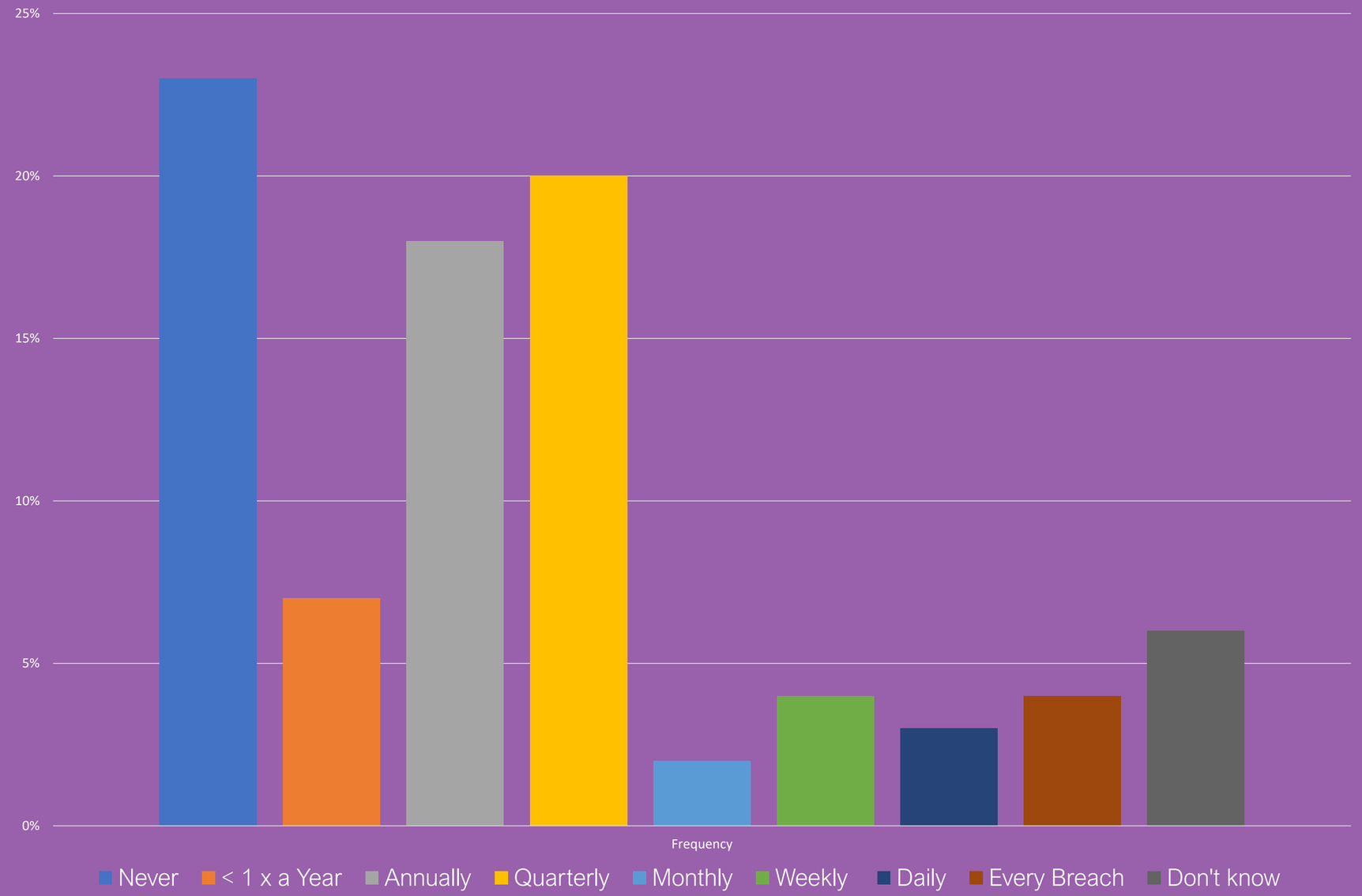
Extent to which Cyber Security is a high or low priority for Trustees - %



Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

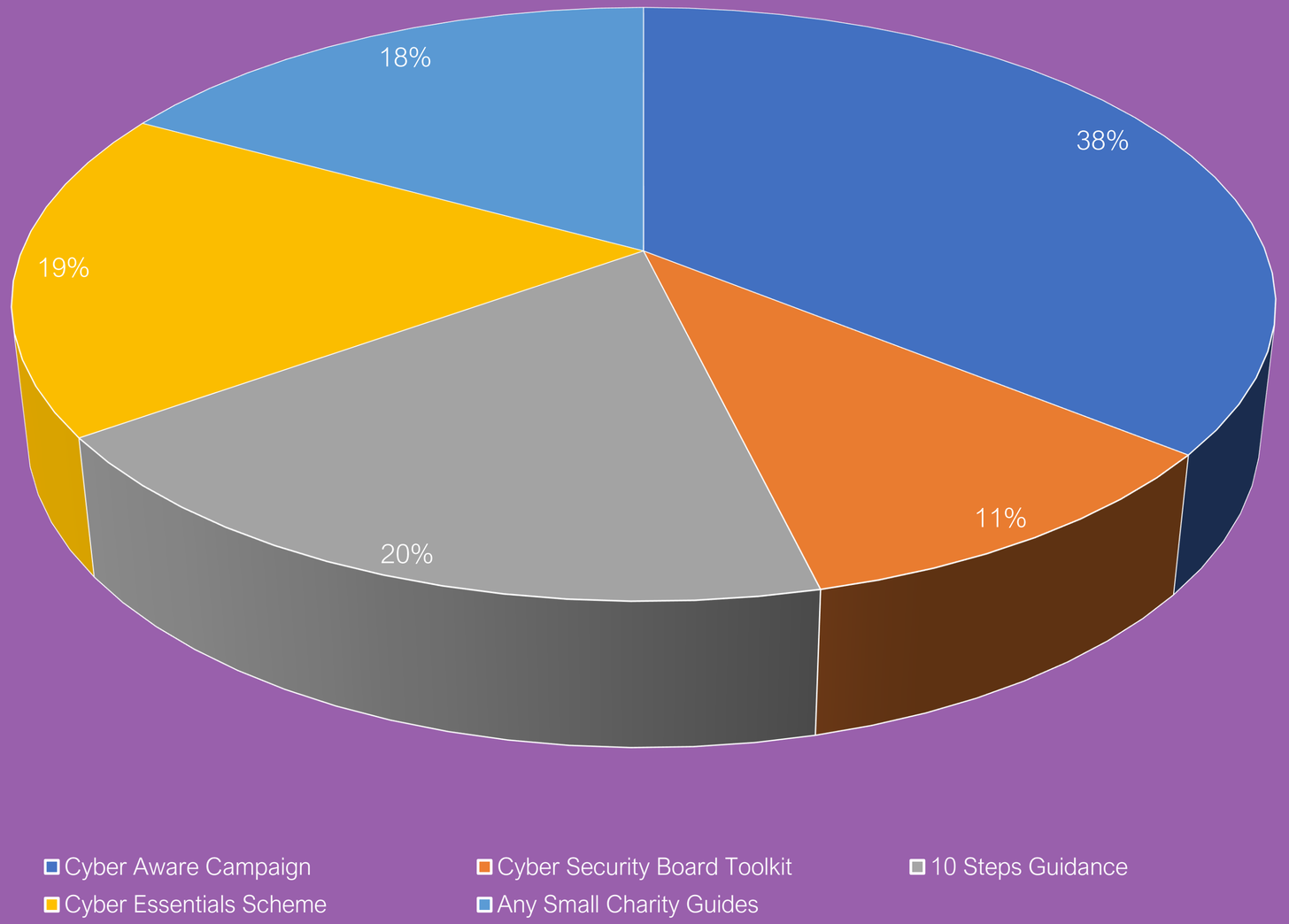
How Often are Trustees given an update on any actions around Cyber Security - %



Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

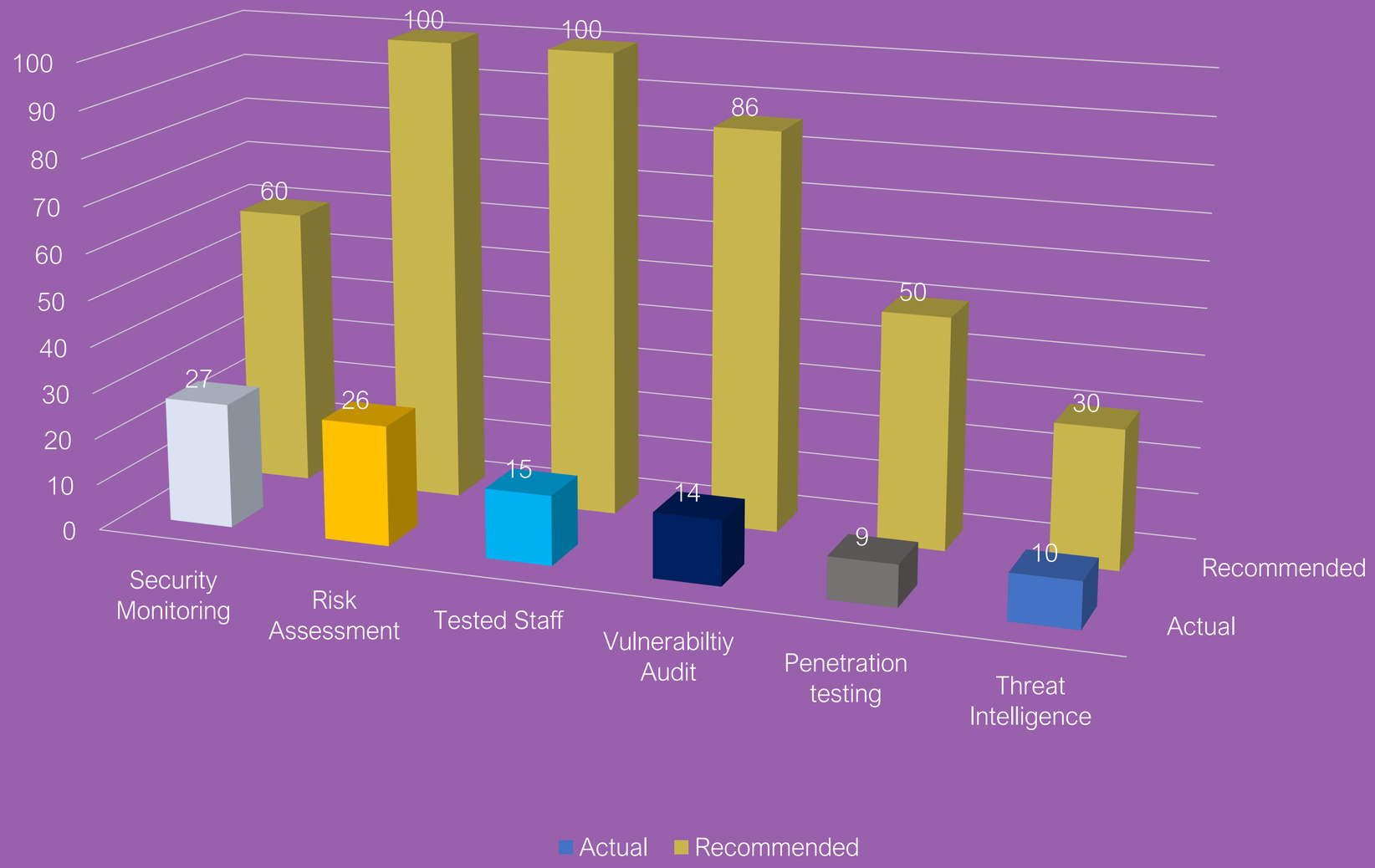
Awareness of the following Government guidance, initiatives or campaigns - %



Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

Activities carried out to identify security risks over the last 12 months - %

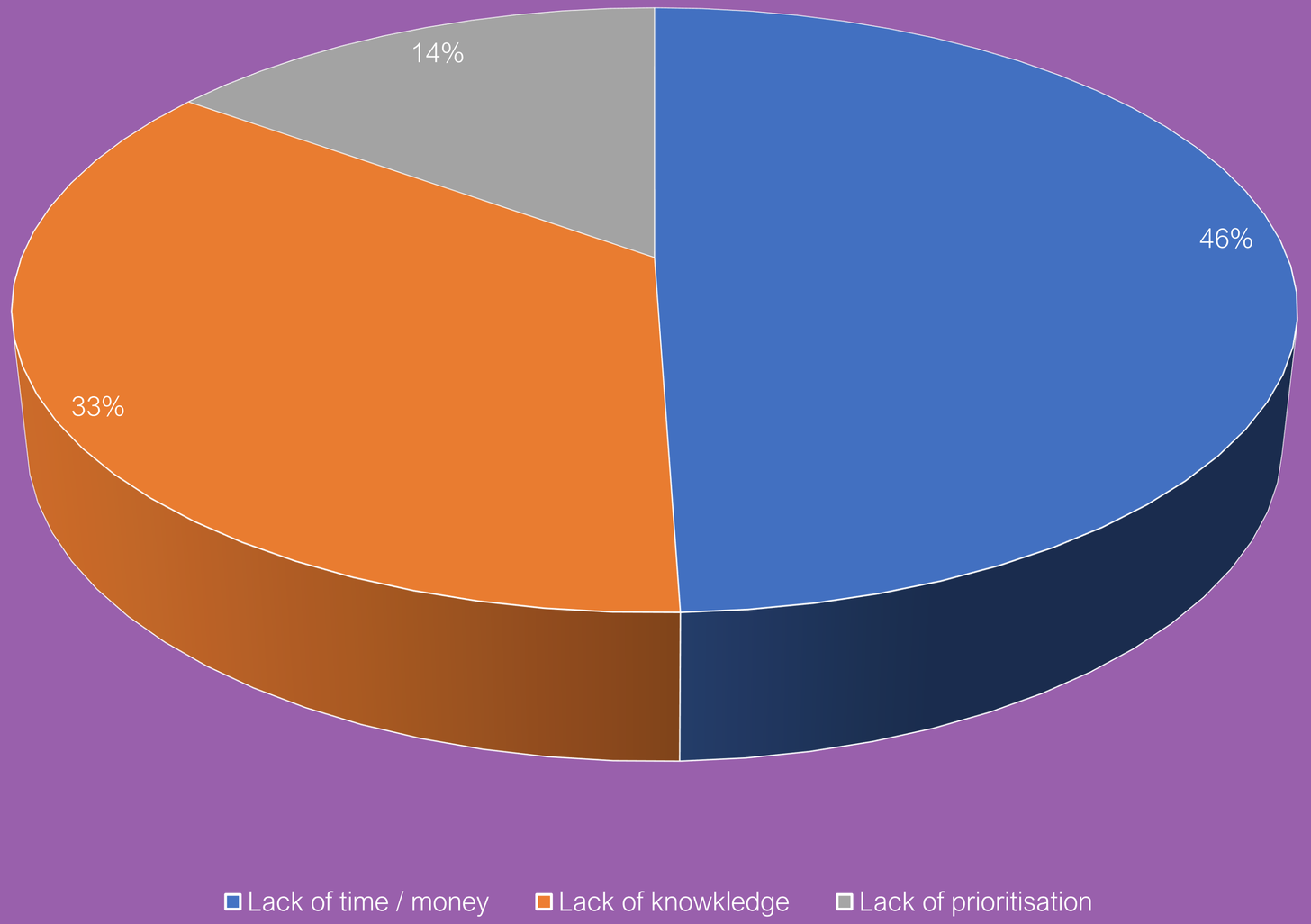


Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

Why Don't Charities review Supply Chain risks?

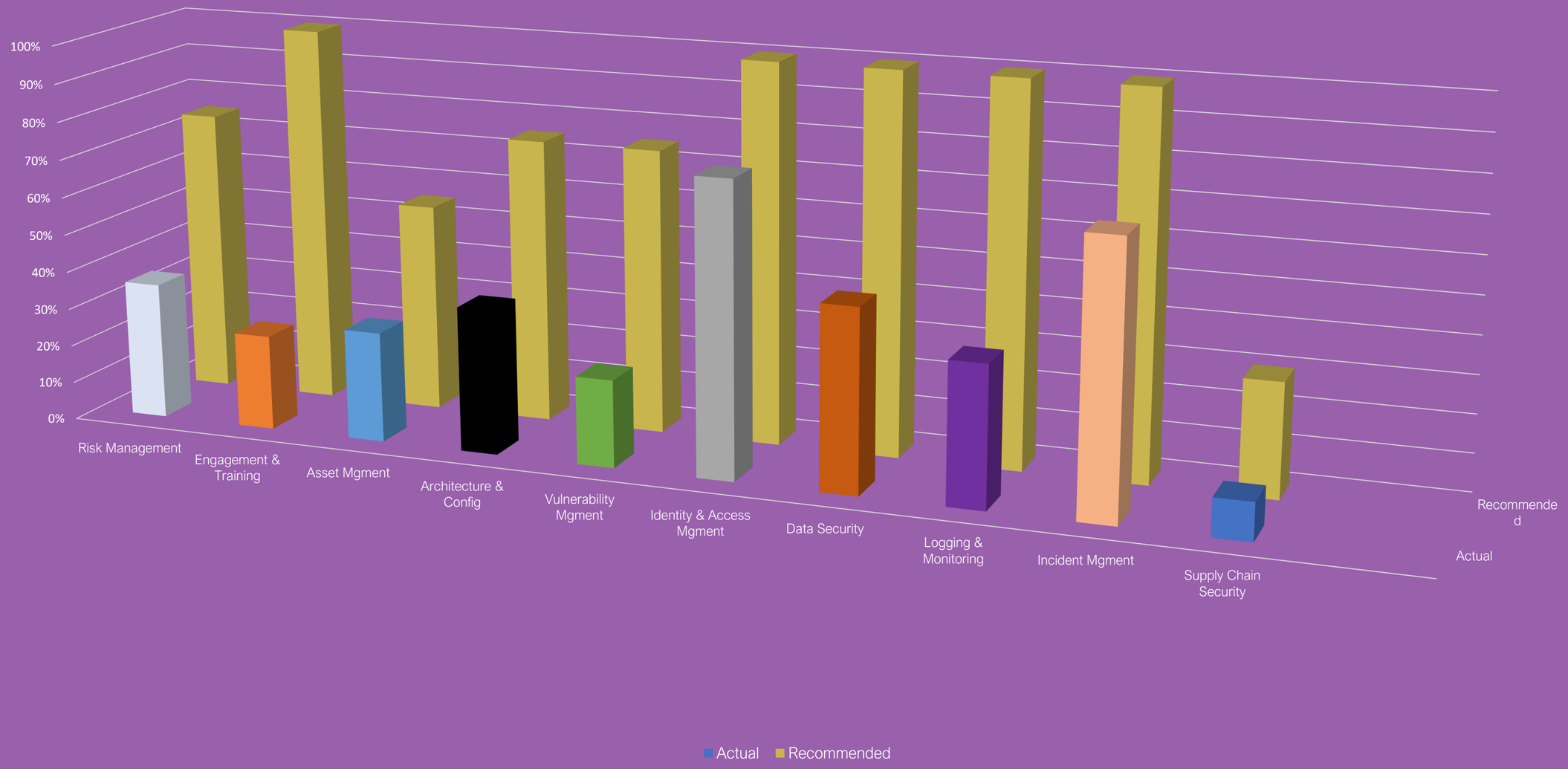
Only 10% do – see next page)



Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

Charities undertaking action in each of NCSC's 10 Steps areas - %

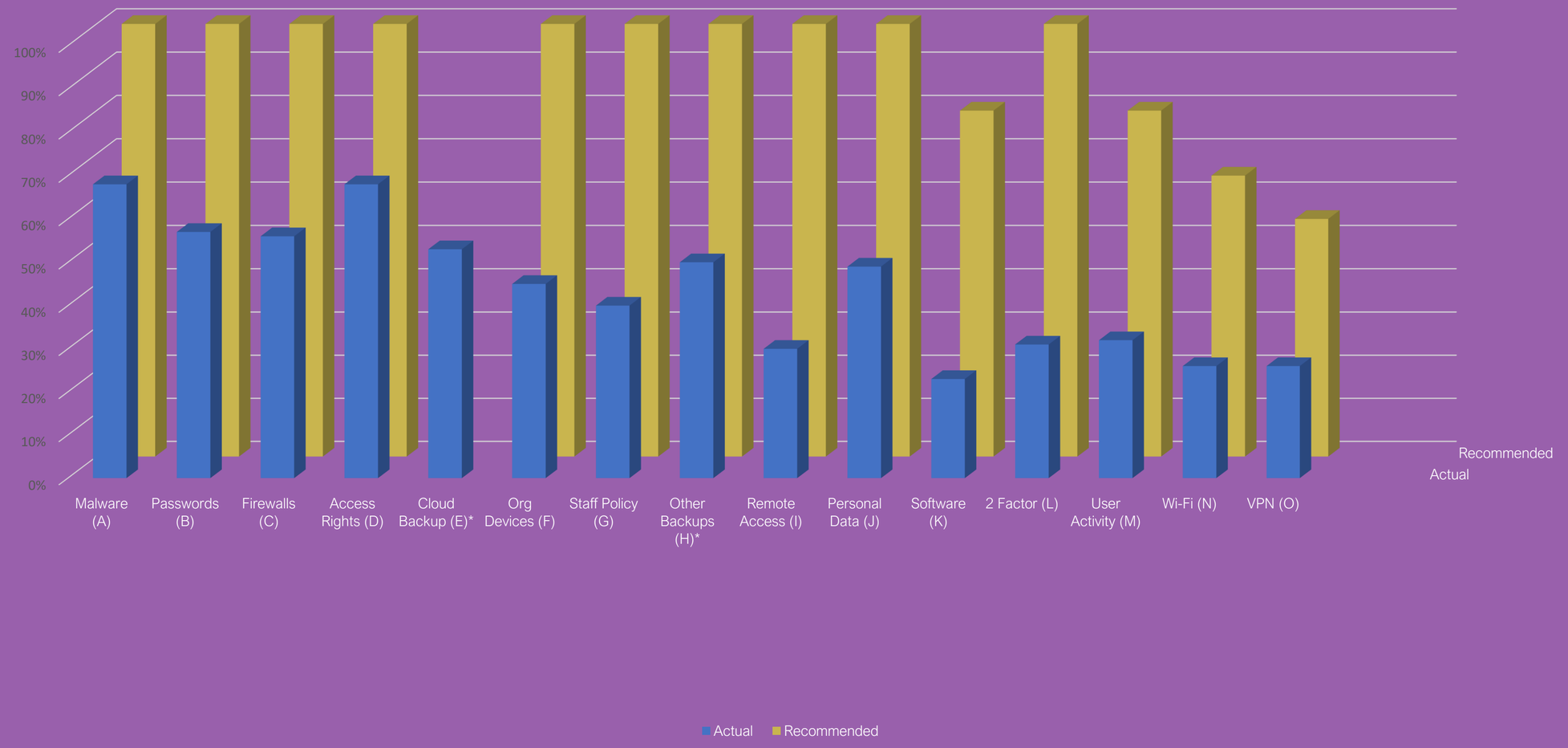


Source Cyber Security Breaches Survey '23

Charities that have the following rules or controls in place - %

Full rule detail on next page

*Together should be 100%

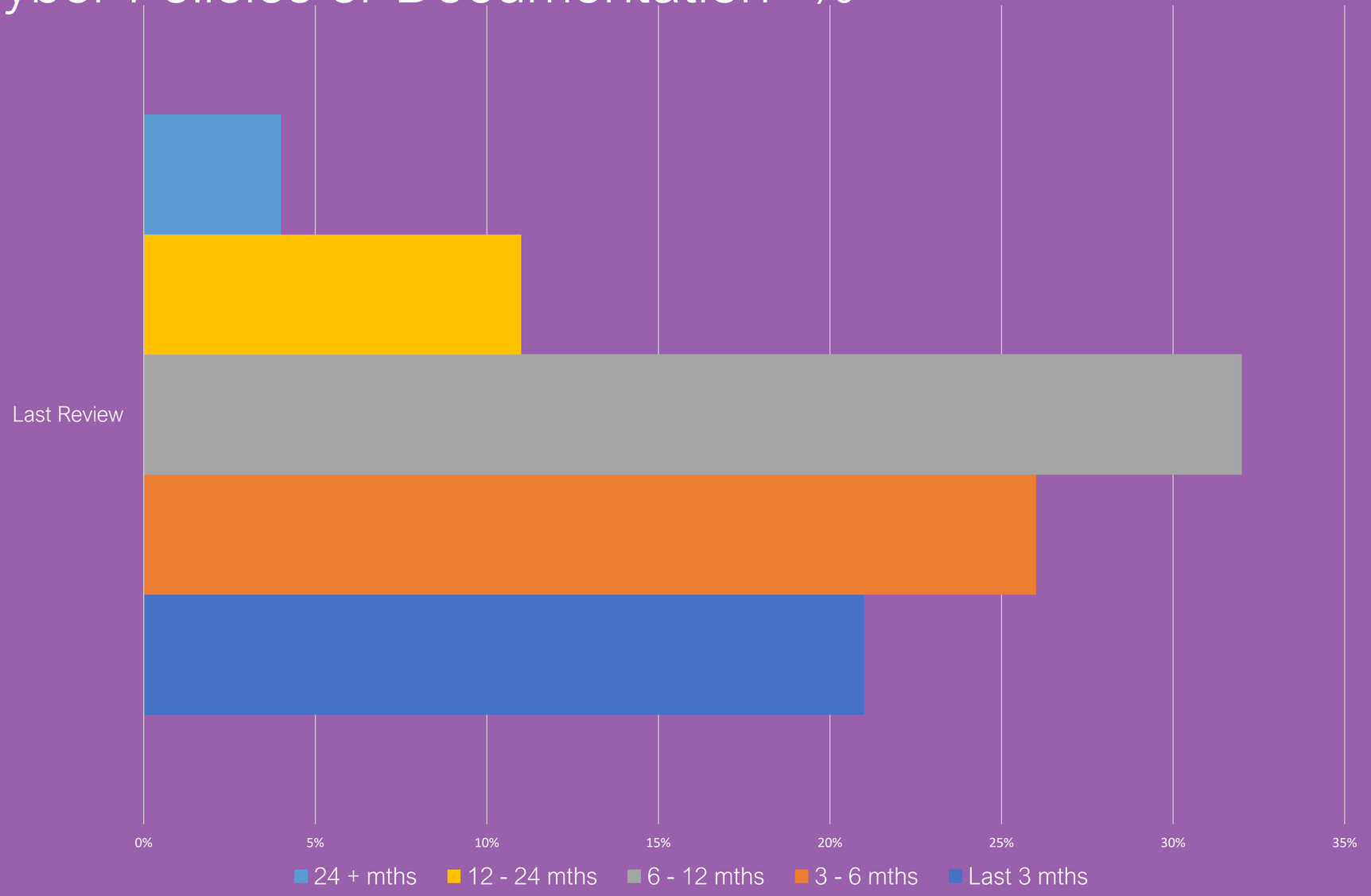


Charities that have the following rules or controls in place – full detail

Up-to-date malware protection	A
A password policy that ensures users set strong passwords	B
Firewalls that cover the entire IT network, as well as individual devices	C
Restricting IT admin and access rights to specific users	D
Backing up data securely via a cloud service	E
Security controls on company owned devices	F
An agreed process for staff to follow with fraudulent emails or websites	G
Backing up data securely via other means	H
Only allowing access via company-owned devices	I
Rules for storing and moving personal data securely	J
A policy to apply software security updates within 14 days	K
Any requirement for two-factor authentication	L
Monitoring of user activity	M
Separate Wi-Fi networks for staff and visitors	N
A virtual private network, or VPN, for staff connecting remotely	O

Source Cyber Security Breaches Survey '23

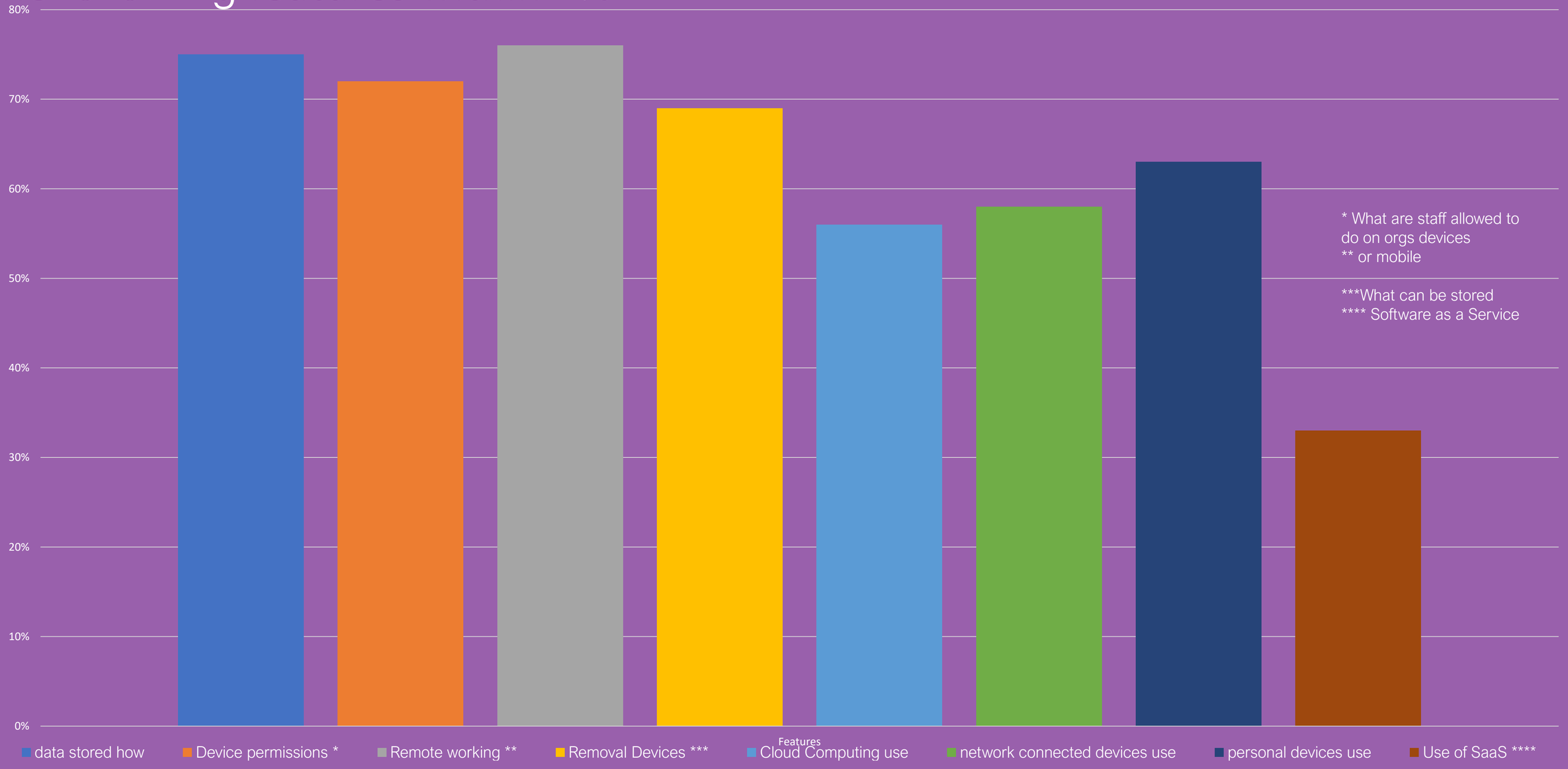
When Charities last created, updated, or reviewed their Cyber Policies or Documentation- %



Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

Charities with Cyber Policies that have the following features within - %

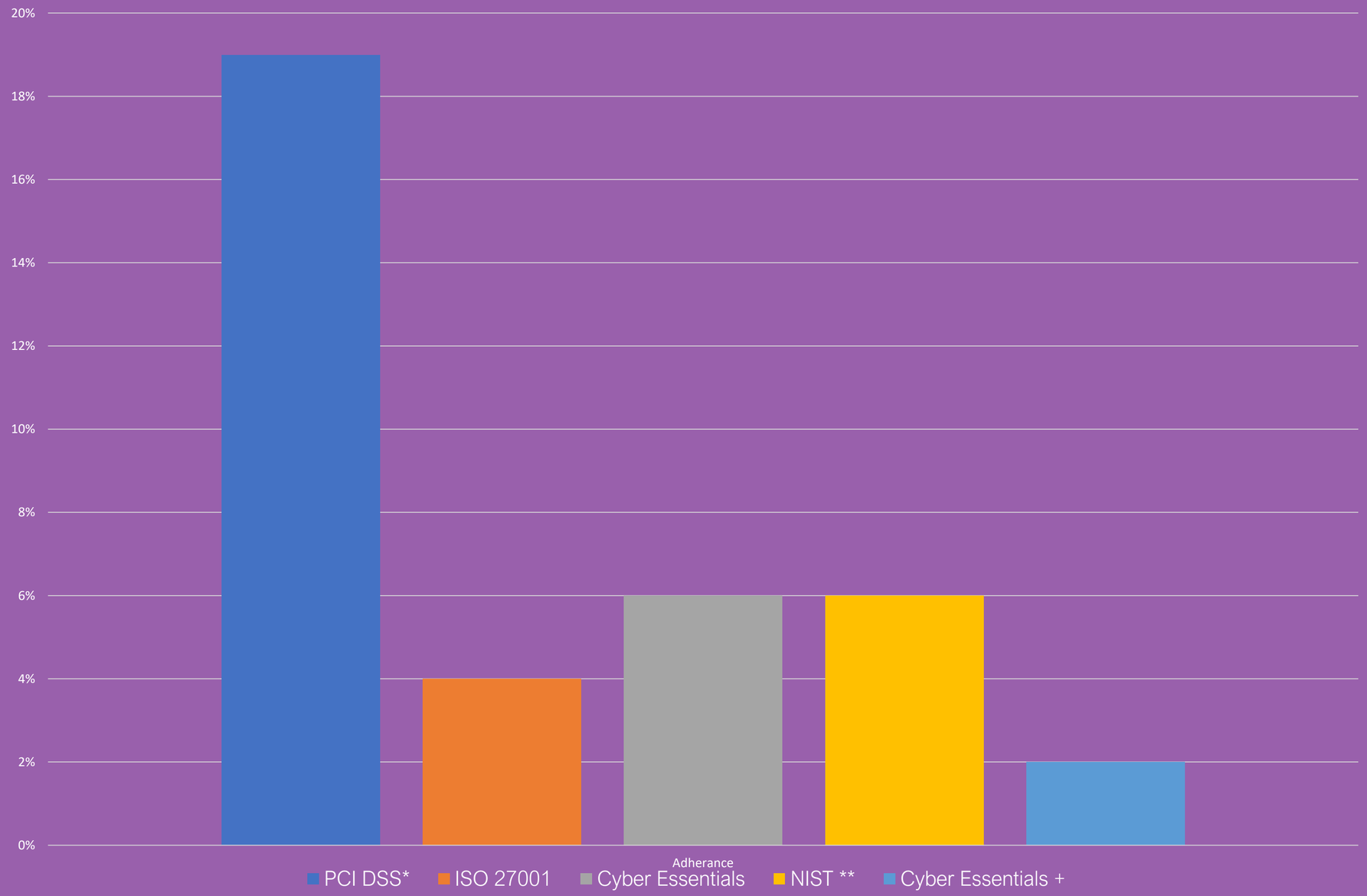


Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

Charities adhering to various cyber security standards or accreditations - %

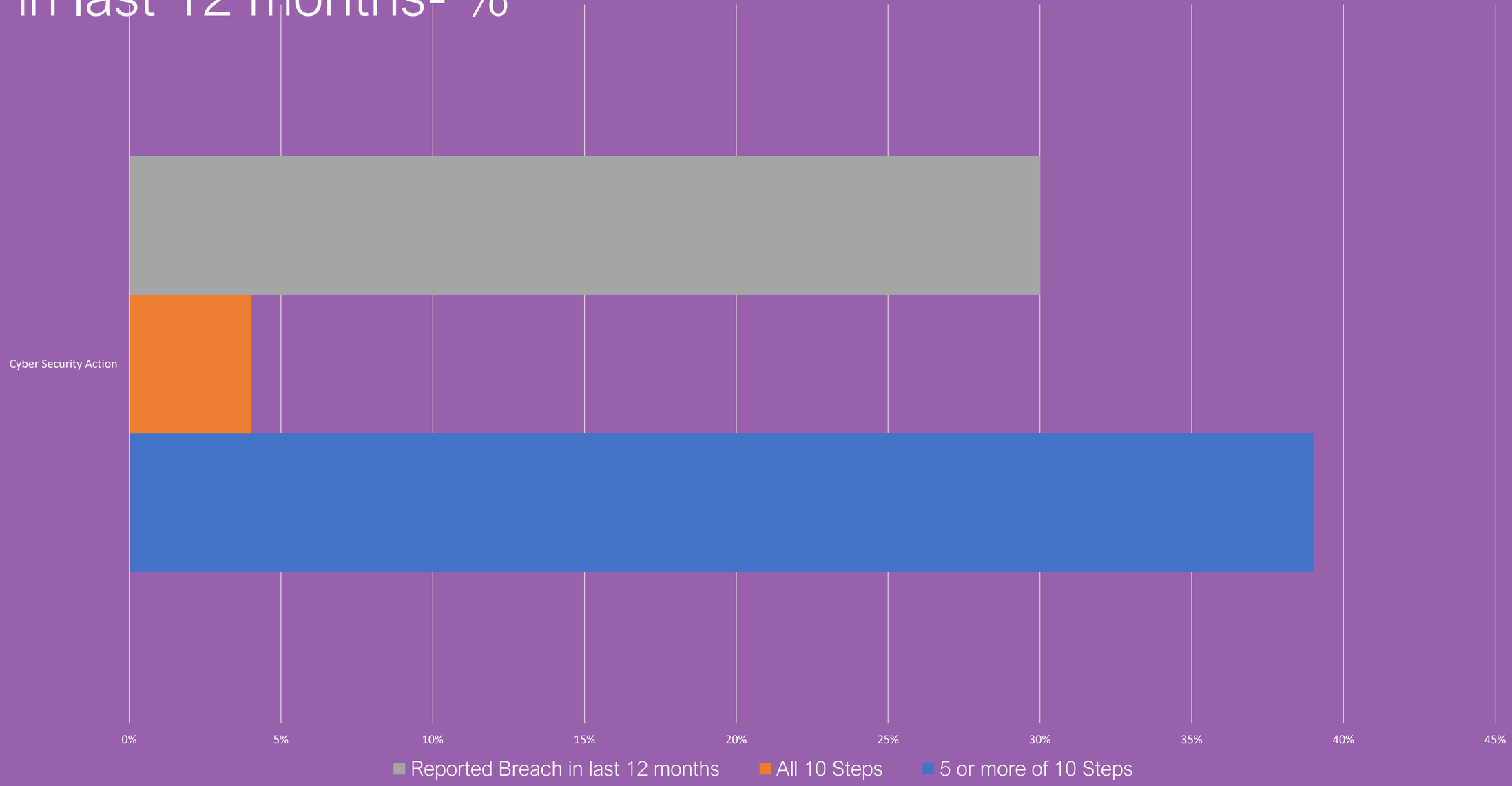
* Payment card Industry Data Standard
** National Institute of Standards and Technology Standards



Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

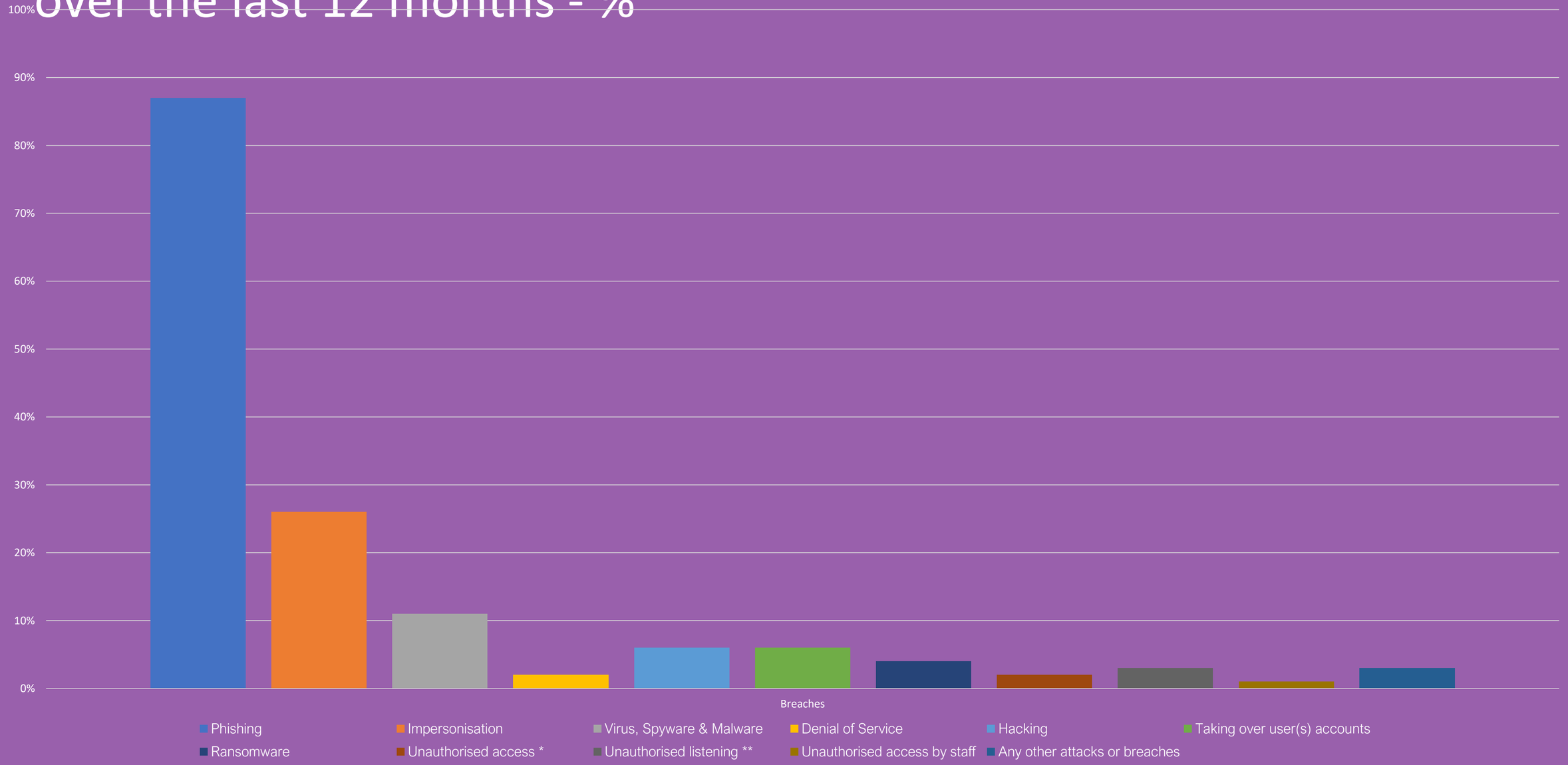
10 Step Action / Breach reported in last 12 months- %



Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

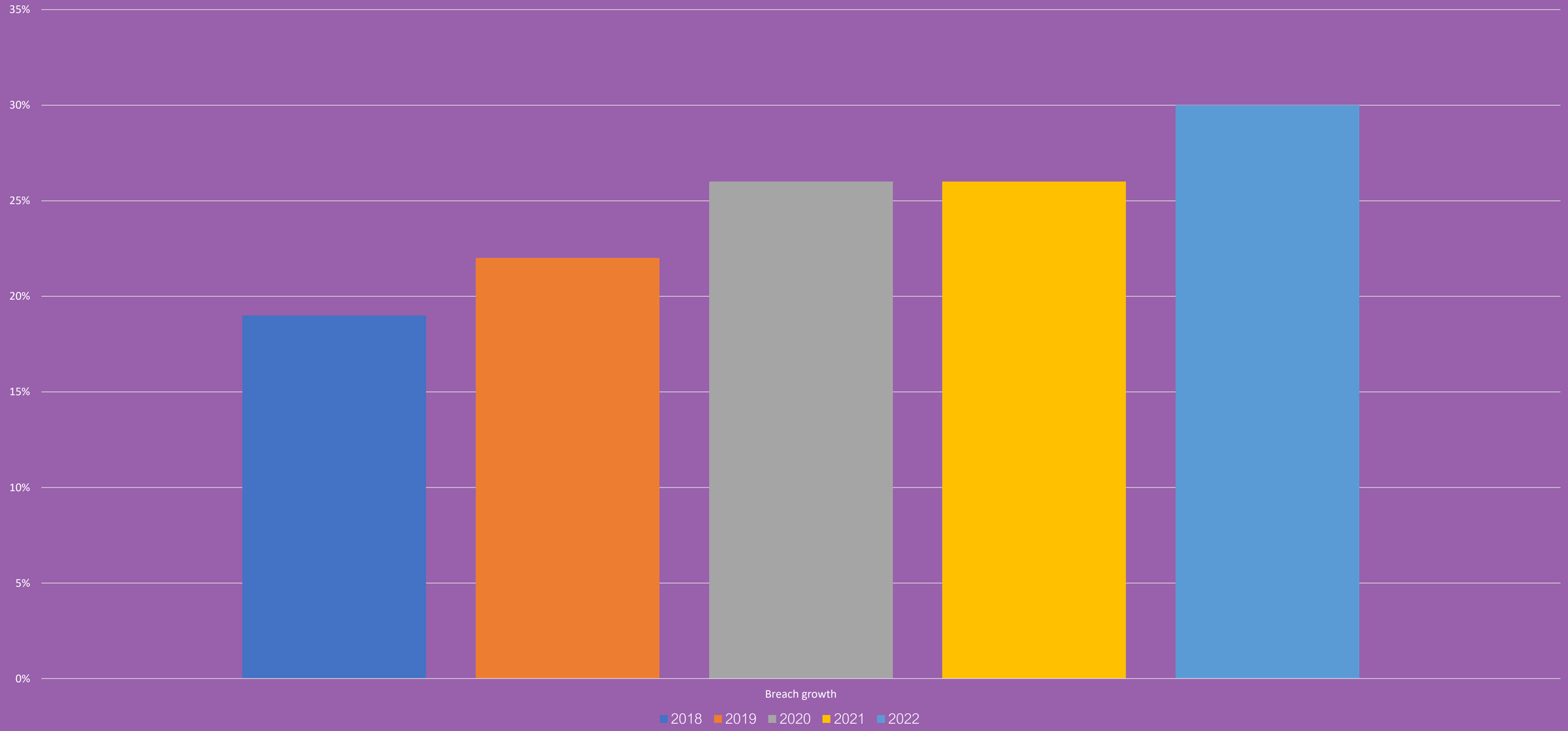
Types of breaches affecting Charities over the last 12 months - %



Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

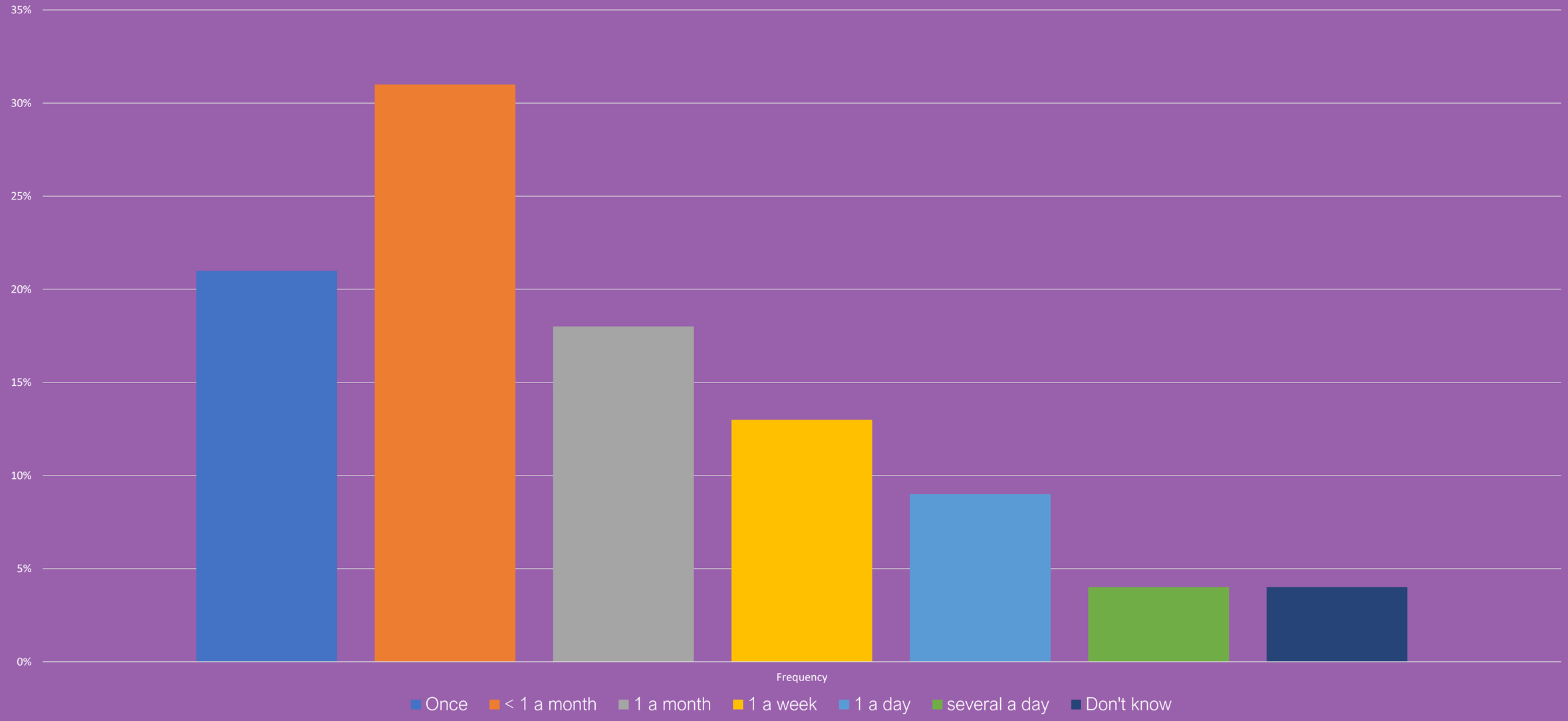
Charities reporting breaches over time - %



Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

Source Cyber Security Breaches Survey '23

How often Charities reported breaches over last 12 months - %



Cyber & Data Protection Limited
https://www.cyber-data.co.uk
hello@cyber-data.co.uk

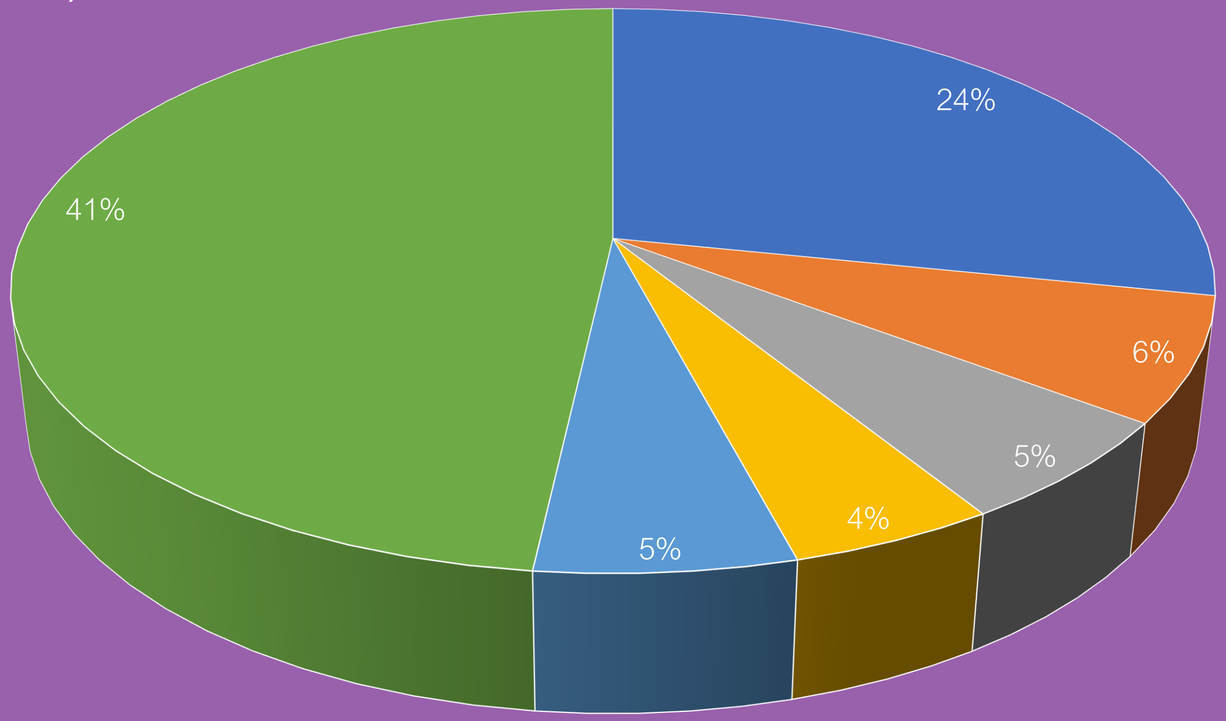
Source Cyber Security Breaches Survey '23

Outcomes of the breaches reported by charities in the last 12 months

Any of the listed outcomes	19%
Website or online services taken down or made slower	5%
Temporary loss of access to files or networks	9%
Software or systems corrupted or damaged	5%
Compromised accounts or systems used for illicit purposes	4%
Lost access to relied-on third party services	2%
Money was stolen	5%
Physical devices or equipment were damaged or corrupted	3%
Lost or stolen assets, trade secrets or intellectual property	2%
Personal data altered, destroyed or taken	2%
Permanent loss of files (not personal data)	1%

Charities that reported their most serious breach outside of the organisation in the last 12 months	24%

Charities that have done any of the following since their most disruptive attack or breach (last 12 months) - %



Source Cyber Security Breaches Survey '23