GPA
Global Privacy Assembly

International Enforcement Cooperation Working Group

Cybersecurity survey
Summary report

August 2023

Contents

Findings – Key points

- Over three quarters of respondents reported that their jurisdictions have one or more cybersecurity law and cybersecurity authority.

- Just under a third of data protection / privacy authorities have competence, for a range of activities, under their jurisdictions' cybersecurity laws, in addition to responsibilities under their data protection / privacy laws.

- This creates overlaps between requirements in data protection / privacy laws and cybersecurity laws, and between the competencies of data protection / privacy authorities and cybersecurity authorities. For example:

    - Almost all responses indicated the existence of duplicate breach reporting requirements, with varying timeframes and thresholds for reporting.

    - Almost half of respondents do not have responsibility for incident response under data protection / privacy laws, but it is one of the most common tasks data protection / privacy authorities reported having under their jurisdictions' cybersecurity laws.

- To manage potential conflicts such as these, most data protection / privacy authorities are collaborating with their domestic cybersecurity authorities, particularly their jurisdictions' national CSIRT / CERT (Computer Security Incident Response Team / Computer Emergency Response Team).

- Responses show that collaboration between data protection / privacy authorities and cybersecurity authorities is primarily focused on policy and engagement activity, rather than operational joint working (such as threat analysis or investigations).

- Key challenges to cooperation are limited resources, and difficulty of engaging cybersecurity authorities.

- Far fewer data protection / privacy authorities collaborate internationally on cybersecurity matters than domestically. Where international collaboration does happen, it is primarily between national data protection / privacy authorities, and occasionally with others such as standards bodies and supranational organisations. Limited resources and lack of legislative power are most often cited as challenges to international cooperation.

Findings – In more detail

Response rate

46 GPA members responded to the survey, covering five continents: Africa (4%), Asia (18%), Europe (56%), North America (18%), South America (4%).

Data protection / privacy laws

The data protection and privacy laws (DP laws) in every respondent's jurisdictions contain general provisions on security of personal information (see Fig 1), but almost none of the DP laws refer explicitly to *cybersecurity* (see Fig 2).

Every respondent indicated that their authority is responsible for supervision of the security provisions in their jurisdiction's DP laws (see Fig 3), with most responsible for tasks such as issuing guidance and enforcing. But almost half of authorities do not have responsibilities for incident response (see Fig 5).

Cybersecurity laws

Over three quarters of respondents reported that their jurisdictions have laws that regulate cybersecurity (cyber laws) in addition to DP laws (see Fig 6).

41% of these cyber laws apply horizontally, to all organisations, and 59% apply vertically, only to certain sectors (see Fig 7). Where this is the case, the most common sectors to which the cyber laws apply are: critical infrastructure (e.g., energy, transport, finance, communications); public sector; and digital / cloud services.

Where cyber laws are present in their jurisdiction, all respondents reported that at least one authority, beyond their own, has supervisory responsibilities for the cyber laws (see Fig 12), while just under a third of respondents indicated that their own authority is responsible for supervision of some aspects of those laws (see Fig 8). Of these authorities, 40% are responsible for supervising only certain organisations subject to cyber laws, such as: public sector, government, and digital / cloud services. The remaining 60% percent supervise all organisations (see Fig 9).

Of the respondents whose authorities have some responsibility for supervision of cyber laws, the most common tasks / powers they have in this regard are: investigations, public awareness raising, handling breach reports, incident response, and enforcement (see Fig 10).

Just under a quarter of all respondents said that their authorities carry out further activity in relation to cybersecurity beyond the tasks and powers they have (see Fig 11), such as: research / threat assessments, advice to government, and running conferences / workshops.

Over two thirds of respondents noted duplicate requirements for breach reporting in their jurisdiction under DP laws and cyber laws (see Fig 13). Most respondents noted the commonality that breach reporting under both DP and cyber laws are mandatory. However, almost all also indicated discrepancies in timeframes, with longer reporting periods for DP laws (usually 72 hours), and shorter for cyber laws (most often 24 hours, and in some cases 'immediate'). Several also reported differences in thresholds, with the bar for reporting under cyber laws generally lower than under DP laws. Despite this, only a small number of respondents noted steps taken to deconflict these overlaps, including the publication of guidance, and the creation of a single environment for breach reporting.

Just under a quarter of respondents also indicated other areas of conflict between their DP and cyber laws (see Fig 14), including: duplicate risk assessment requirements; excessive retention of logging data; challenges with the proportionality of processing of personal information by some cybersecurity solutions; and balancing incident response and investigatory duties. Steps to deconflict some of these issues include development of multi-use risk assessment methodologies, and consultation with industry.

Two thirds of respondents noted that their DP or cyber laws require them or other relevant authorities to map / analyse harms from cyber incidents (see Fig 15), although many indicated this is an implicit requirement rather than one set out explicitly in law. Factors to assess in this regard include: volume of people affected; sensitivity of information; and probability of misuse of data. Some respondents noted that while their authority would typically only undertake such analysis on a case-by-case basis, their national CSIRT / CERT provides broader landscape wide analysis and statistics.

Almost all respondents reported that their laws do not forbid payment of ransom in response to a ransomware attack (see Fig 16). Respondents were almost equally split between having taken no public position on payment of ransom, and advising against it.

Domestic collaboration on cybersecurity

Under half of respondents reported that their DP or cyber laws contained explicit provisions that enable cooperation between relevant domestic authorities (see Fig 19). Despite this, 80% of respondents said that their authority has collaborated with other domestic authorities in relation to cybersecurity (see Fig 17). Of these respondents, just over a third have at least one MoU in place with a domestic authority, and some have MoUs in development (see Fig 20).

The most common authority within respondents' jurisdictions with whom they have cooperated was the national CSIRT / CERT, followed by law enforcement, and sector regulators (see Fig 18).

The most reported ways in which respondents cooperate with domestic authorities in relation to cybersecurity were: information sharing (regular and case specific); joint awareness raising (regular and case specific); and joint workshops / events (case specific). From the options provided, responses indicated that authorities work together the least on joint investigations and joint threat analysis (see Fig 21). For the few that had undertaken a

joint investigation, these were mostly led by data protection / privacy authorities (DPAs), with technical expertise provided by cyber authorities.

The most common challenge to domestic collaboration respondents noted is lack of legislative power. Others include: insufficient resources; lack of engagement / interest from cyber authorities; conflicting roles; and confidentiality.

International collaboration with other DPAs on cybersecurity

80% of DPAs said that their jurisdictions' DP or cyber laws contain explicit provisions enabling international cooperation with other DPAs (see Fig 23), but only just over a third reported that they had collaborated with another DPA on cybersecurity matters (see Fig 22). Under half of these respondents (which is just one sixth of all respondents) said they had an MoU with another DPA to support this collaboration (see Fig 24).

The most reported ways in which respondents cooperate with international DPAs in relation to cybersecurity were: information sharing (regular and case specific); complaint referrals (case specific); joint investigations (case specific); and joint workshops / events (regular and case specific). From the options provided, responses indicated that authorities work together the least on joint incident response (see Fig 25).

Examples of joint investigations included concluded and ongoing co-led bilateral investigations into single organisations, and a multilaterally coordinated investigation into a whole sector.

Commonly reported challenges to cooperating with other DPAs on cybersecurity included lack of resources, and lack of legislative powers.

International collaboration with other authorities on cybersecurity

Only around a quarter of respondents reported that their DP or cyber laws contain explicit provisions that enable international cooperation with other authorities (see Fig 28), and just 13% indicated that their authority has collaborated internationally with other authorities in relation to cybersecurity (see Fig 26). Of these respondents, fewer still (4% of all respondents) reported having an MoU in place with another international authority (see Fig 29).

For the few authorities that have cooperated with other international authorities on cybersecurity, the most common types of authority with whom they have cooperated were: law firms; consultancies; standards bodies; and supranational organisations (see Fig 27). The most common types of collaboration were: information sharing (case specific); joint awareness raising (case specific); joint guidance (case specific); and joint workshops / events (regular) (see Fig 30). The most commonly reported challenge to international cooperation with other authorities on cybersecurity was lack of legislative powers.

Conclusion and next steps

- The findings from this survey provide a useful snapshot of the cybersecurity regulatory landscape across GPA members' jurisdictions.

- The landscape is complex, but many DPAs share the same or similar circumstances and challenges in relation to their role in the cybersecurity space, but with differing levels of experience and maturity, e.g.,

    - All DPAs are responsible for supervision of the security provisions in their jurisdiction's DP laws.

    - Many DPAs do not have competence for supervision of their jurisdictions' cyber laws, while some do.

    - Most jurisdictions have duplicate breach reporting requirements. Some have other areas of overlap or conflict between DP and cyber laws.

    - Many DPAs have cooperated with their domestic cyber authorities, but some have not.

    - Some DPAs have undertaken joint investigations, but most have not.

    - Some DPAs have cooperated internationally on cybersecurity matters, but most have not.

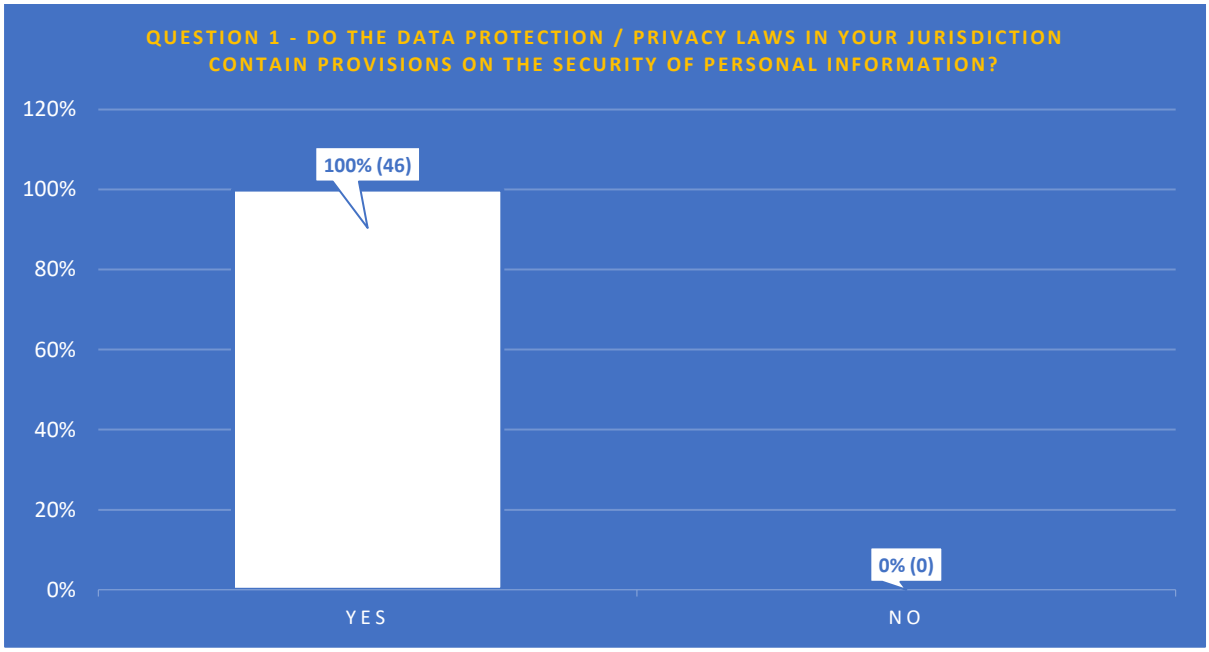
- This presents potential opportunities for: strengthening of DPA-DPA cybersecurity-focused relationships; development of relationships between DPAs and cyber authorities; capacity building and exchange of expertise; exploration of scope for joint activities, such as investigations.

- The IEWG will hold a 'closed enforcement session' in due course to present the findings from this survey and discuss the potential opportunities it raises.

- The IEWG will consolidate this paper, and discussions at the closed enforcement session, into a single report, and make recommendations to the 2023 GPA Closed Session on any further activity on cybersecurity in the GPA.

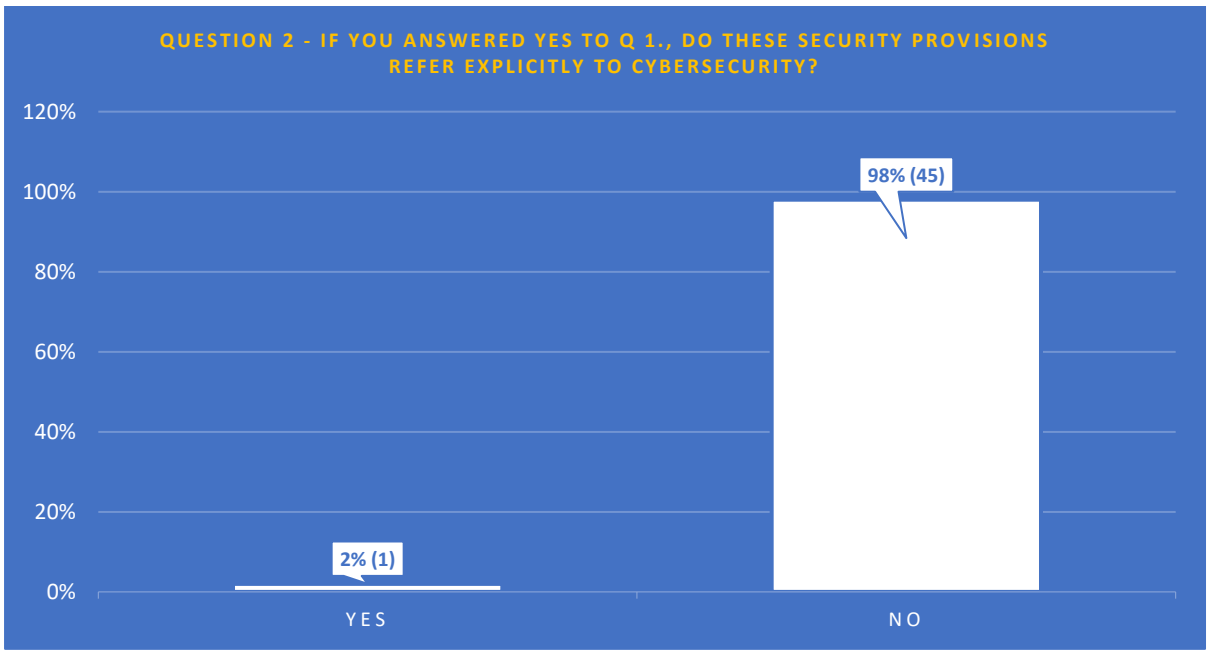
Annexe - Figures

Fig 1



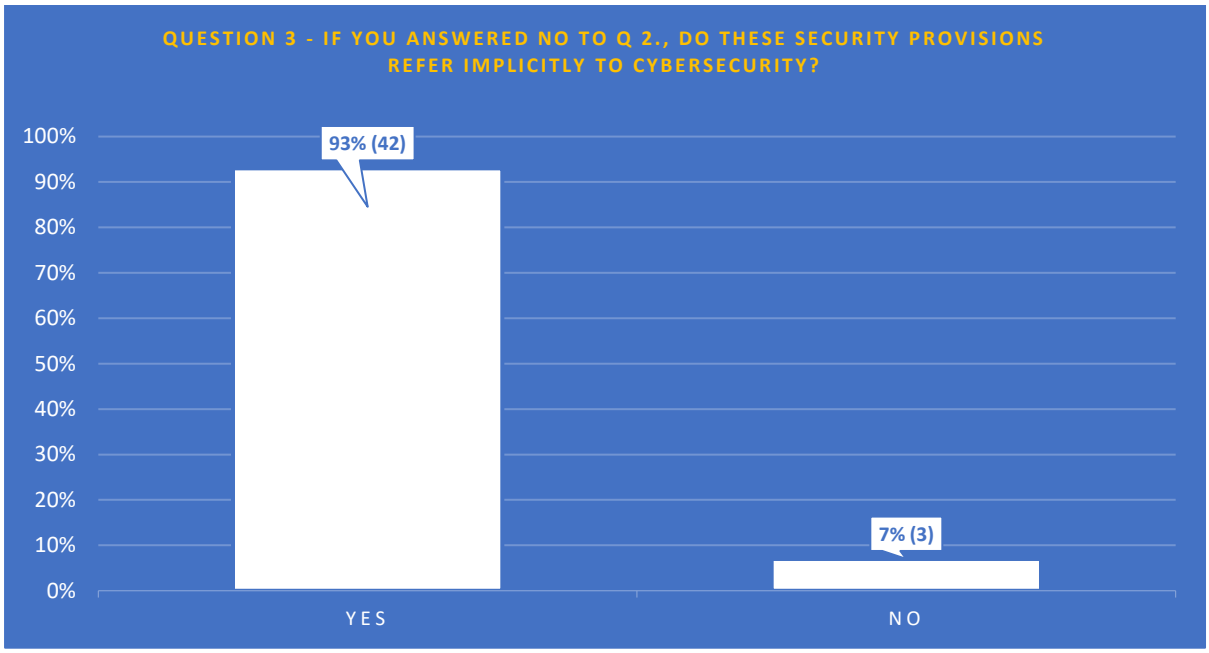
Return to report

Fig 2



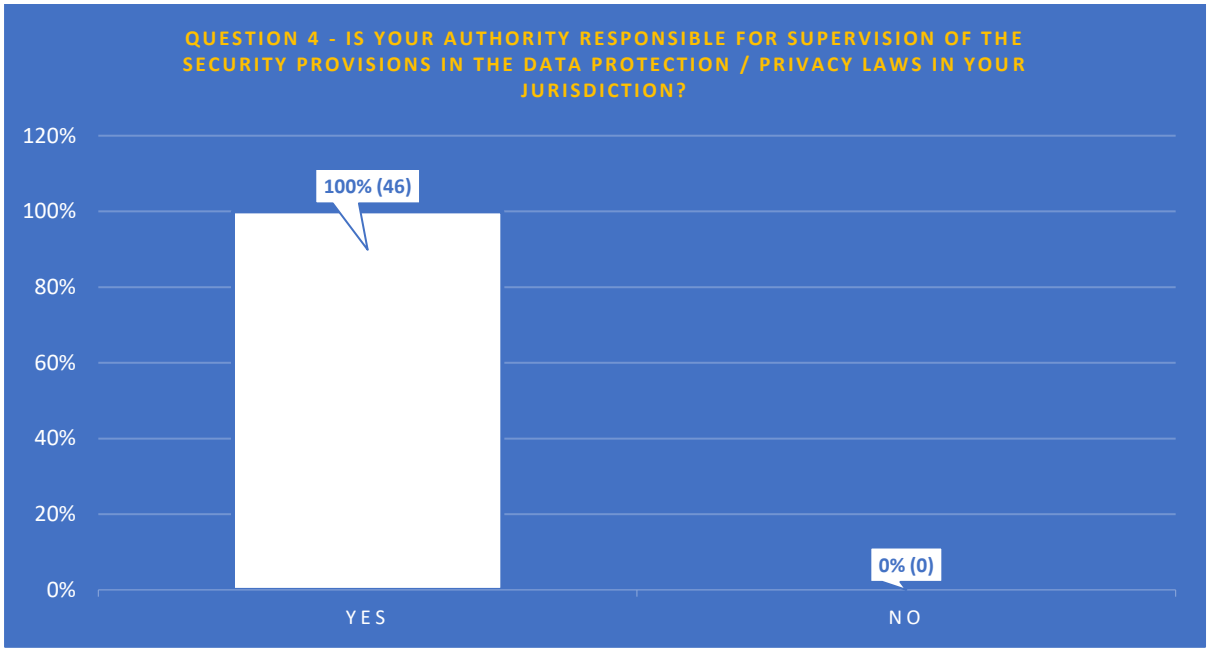
Return to report

Fig 3



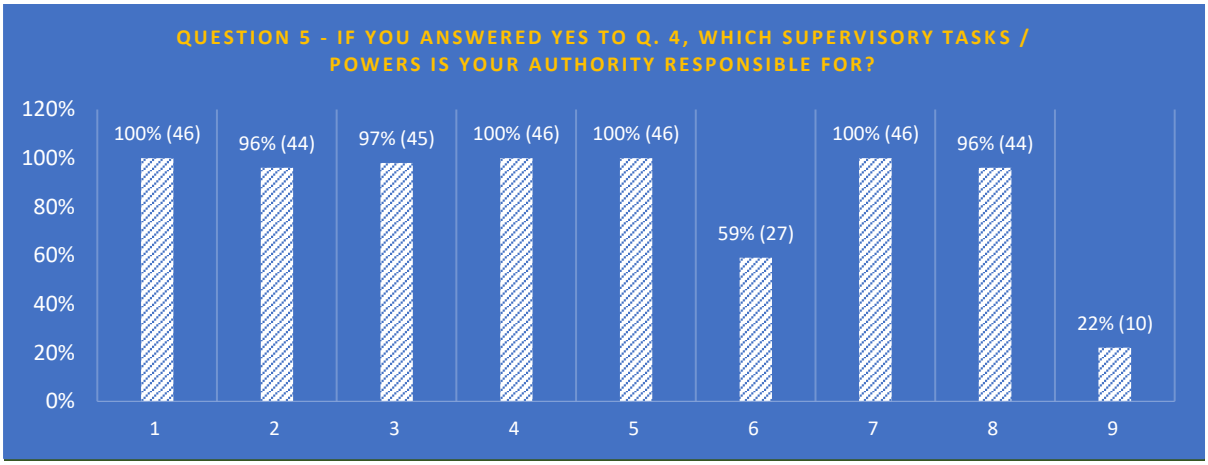
Return to report

Fig 4



Return to report

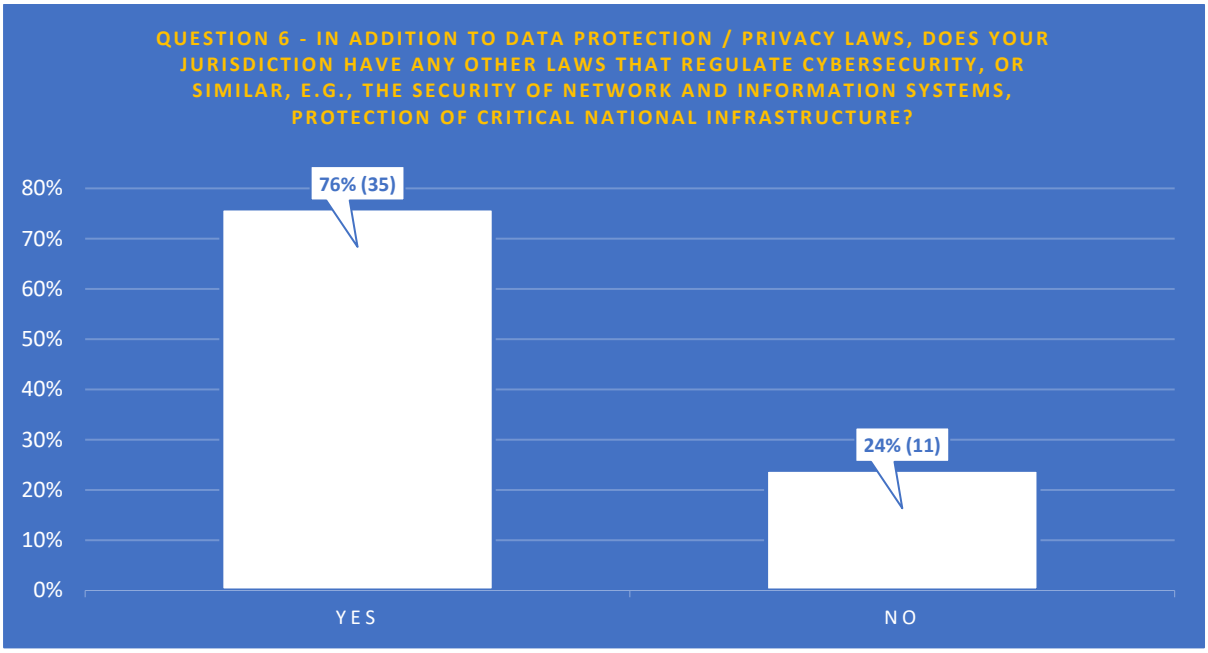
Fig 5



1	Raising public awareness
2	Publishing guidance for organisations
3	Monitoring compliance
4	Handling complaints
5	Handling self-reported breach notifications
6	Incident response
7	Investigations
8	Enforcement
9	Other

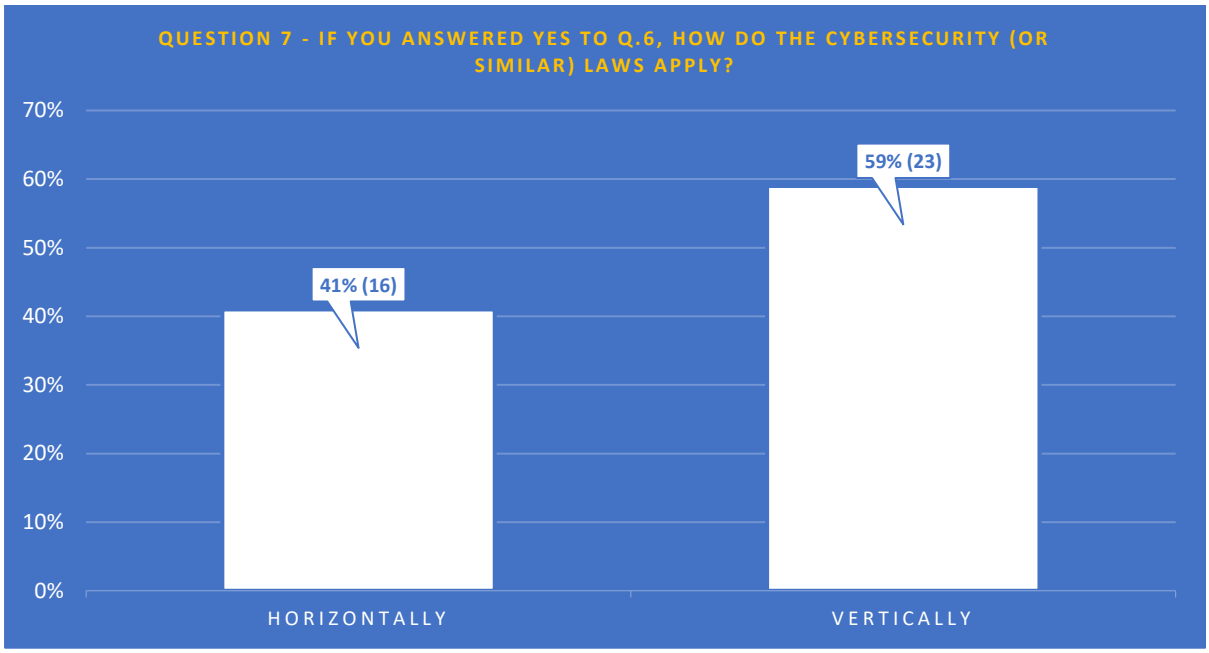
Return to report

Fig 6



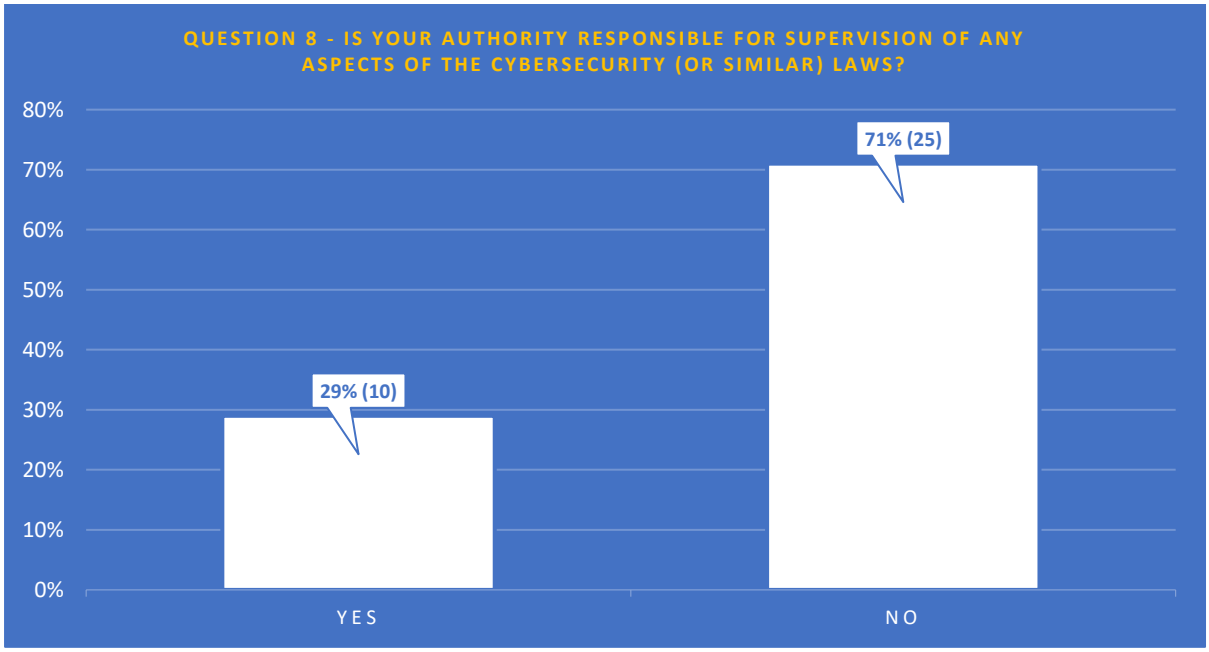
Return to report

Fig 7



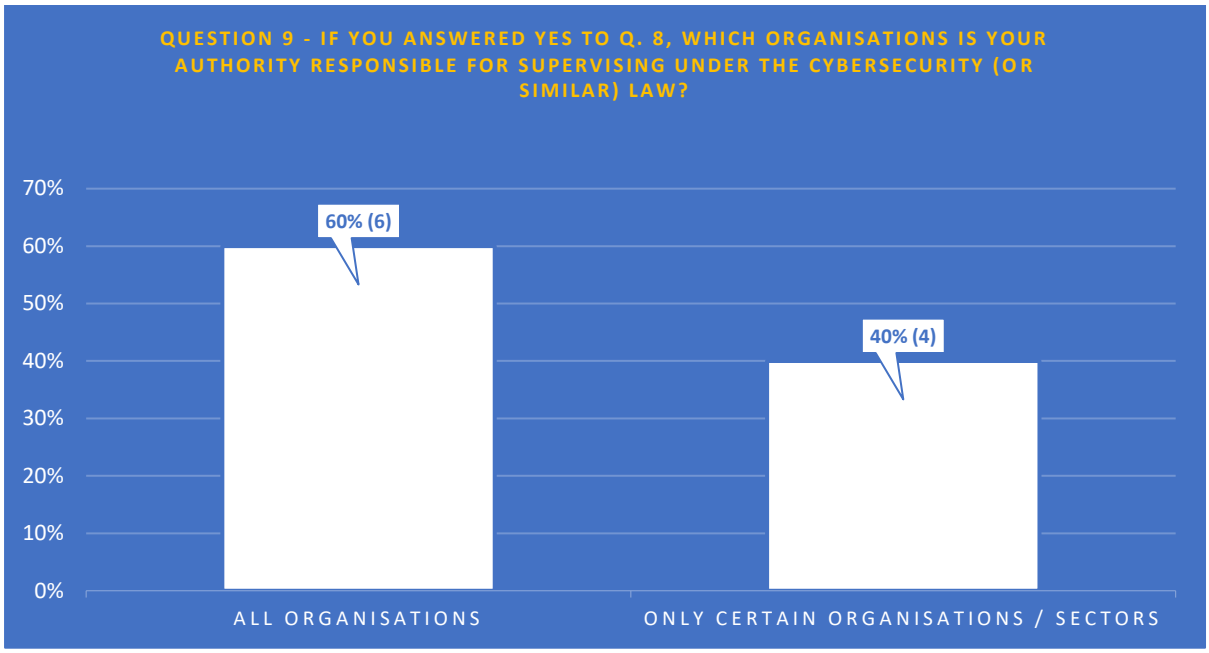
Return to report

Fig 8



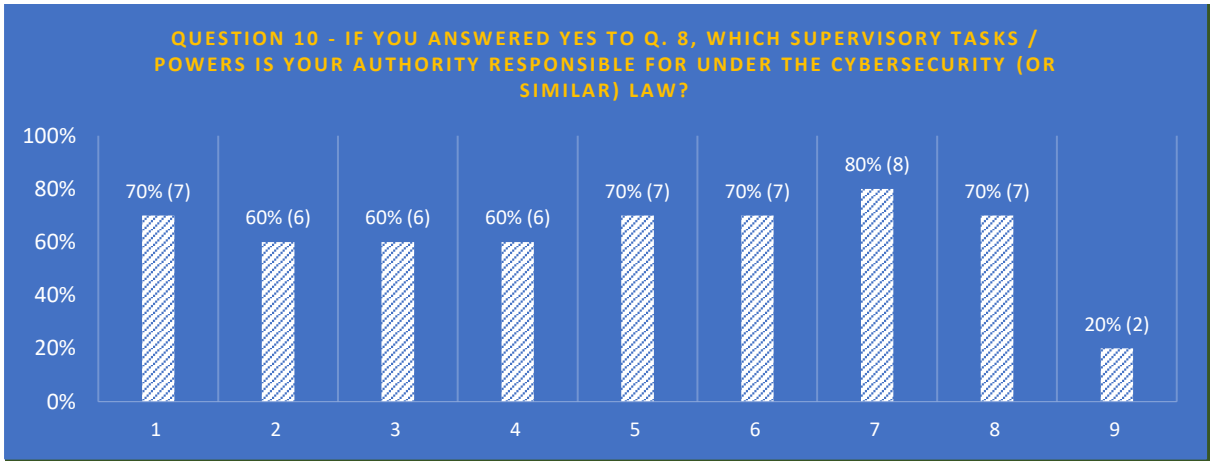
Return to report

Fig 9



Return to report

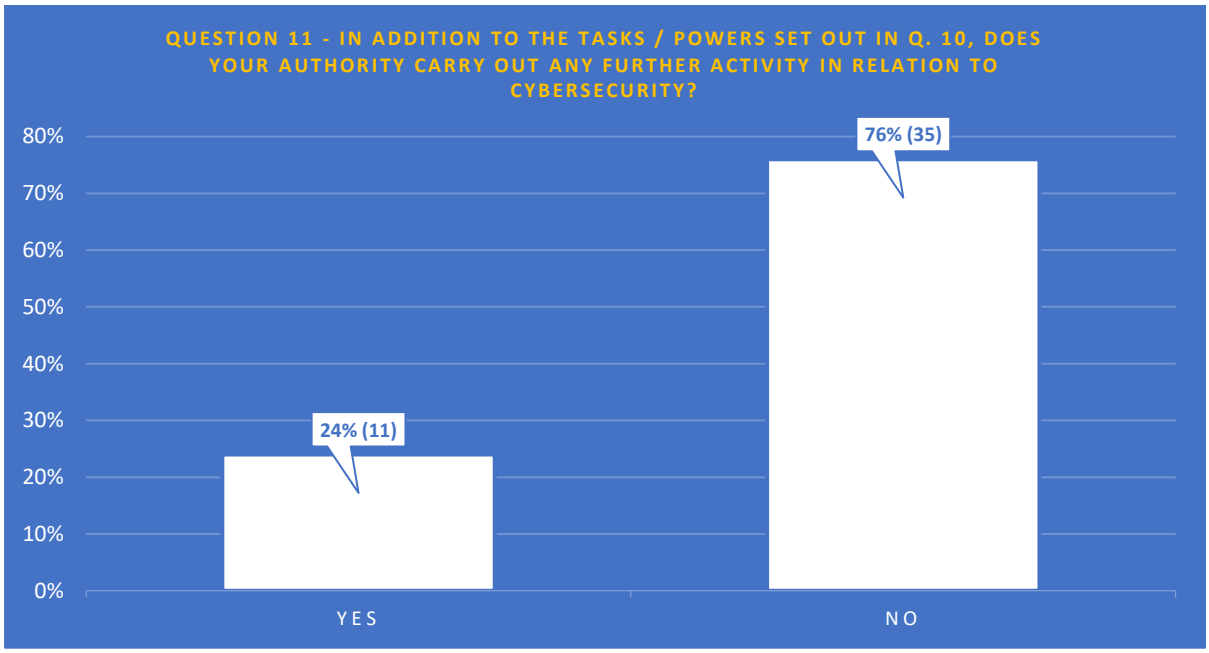
Fig 10



1	Raising public awareness
2	Publishing guidance for organisations
3	Monitoring compliance
4	Handling complaints
5	Handling self-reported breach notifications
6	Incident response
7	Investigations
8	Enforcement
9	Other

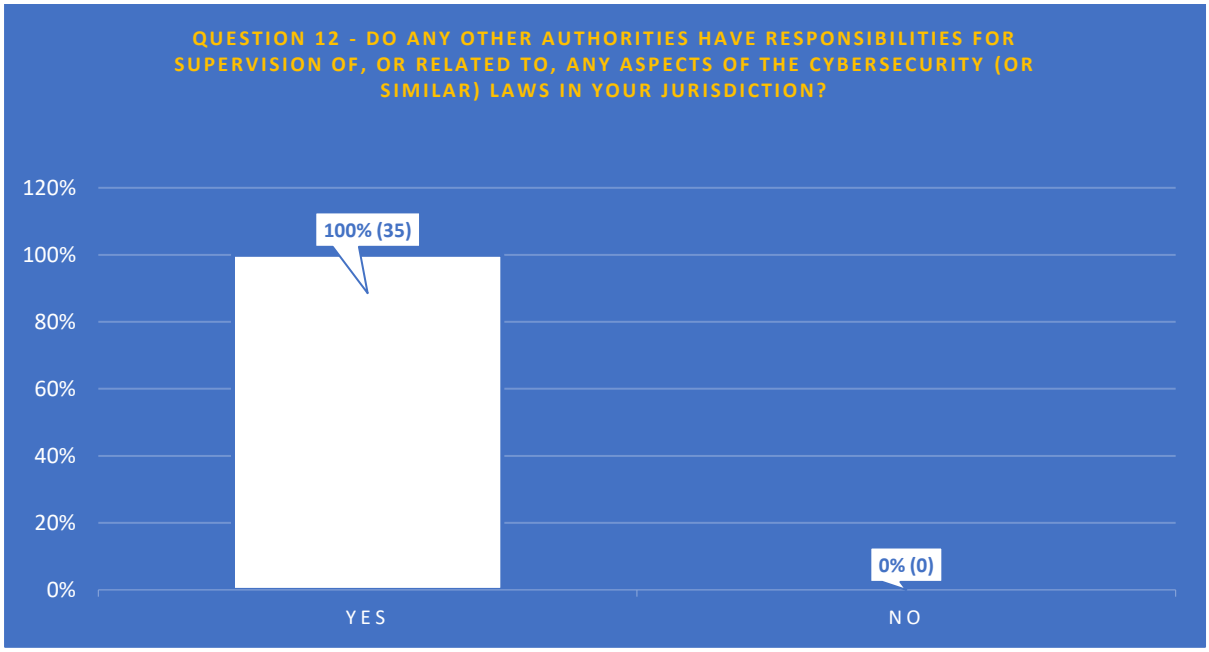
Return to report

Fig 11



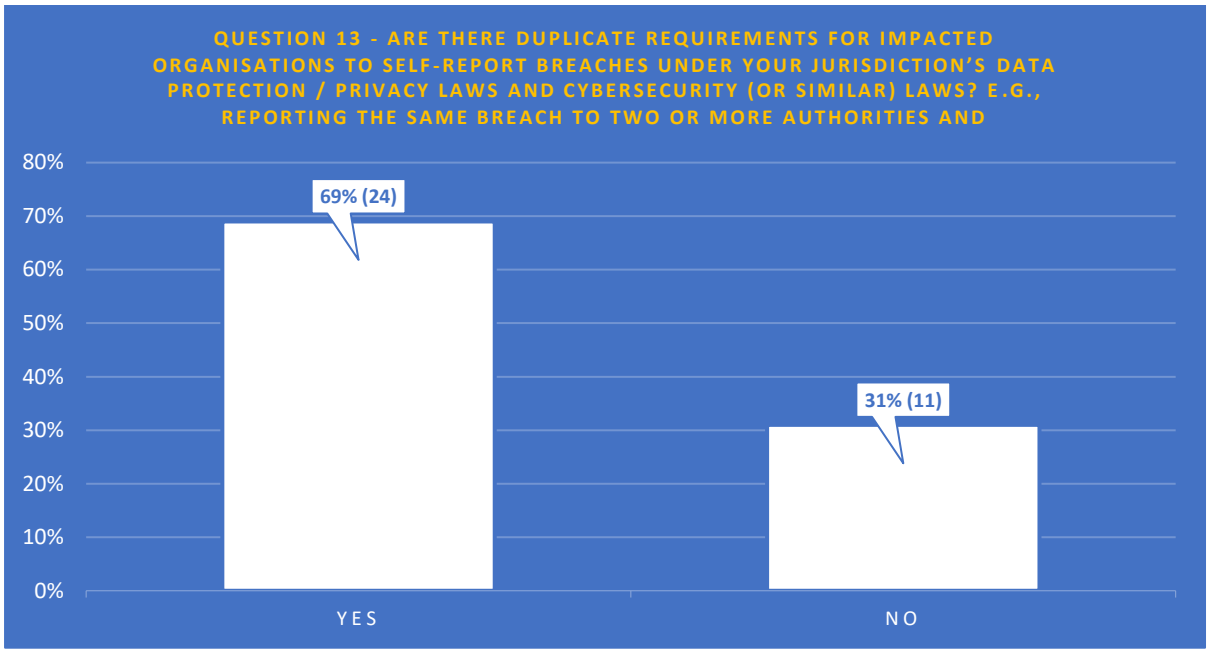
Return to report

Fig 12



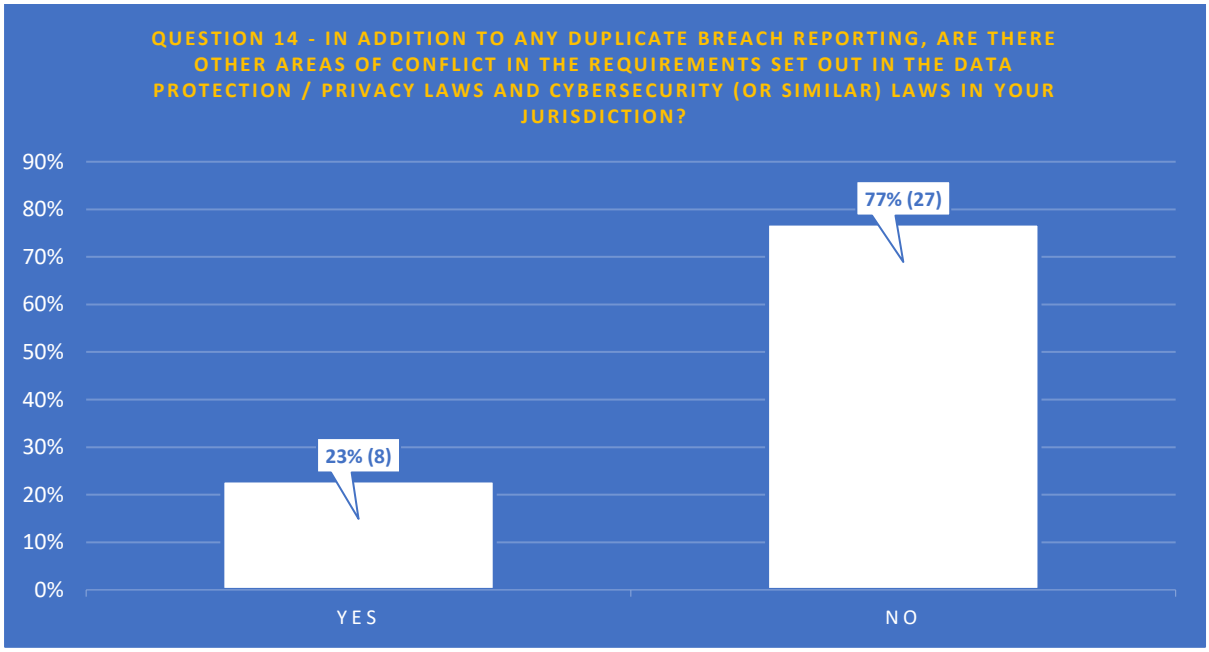
Return to report

Fig 13



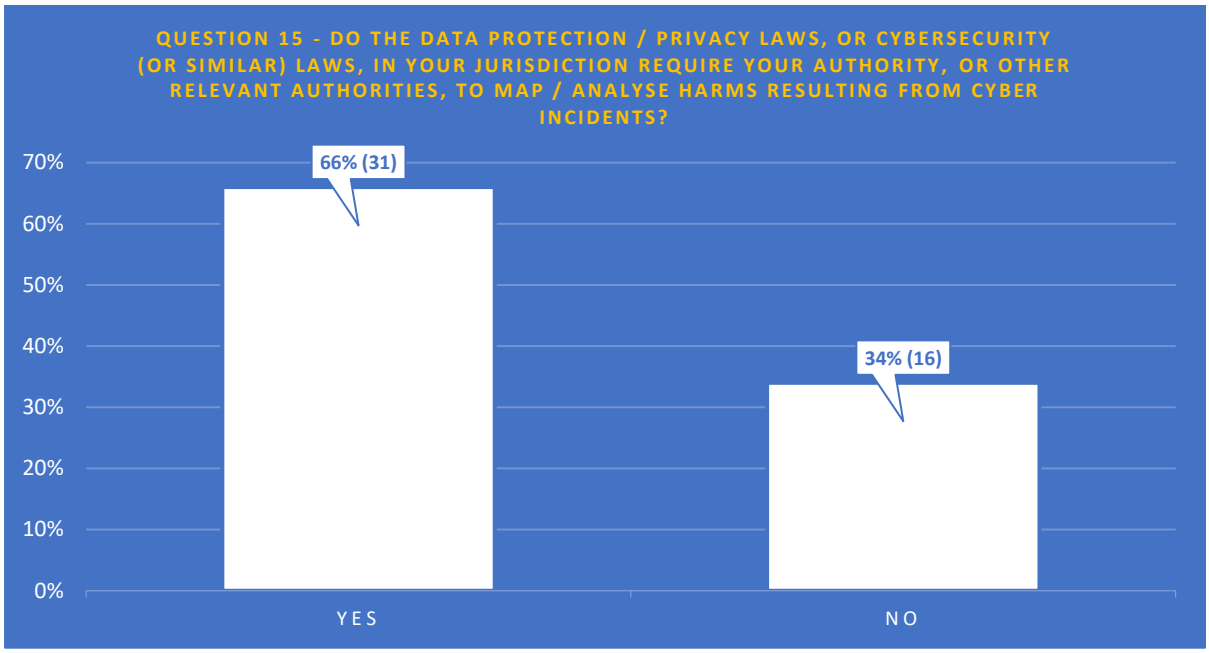
Return to report

Fig 14



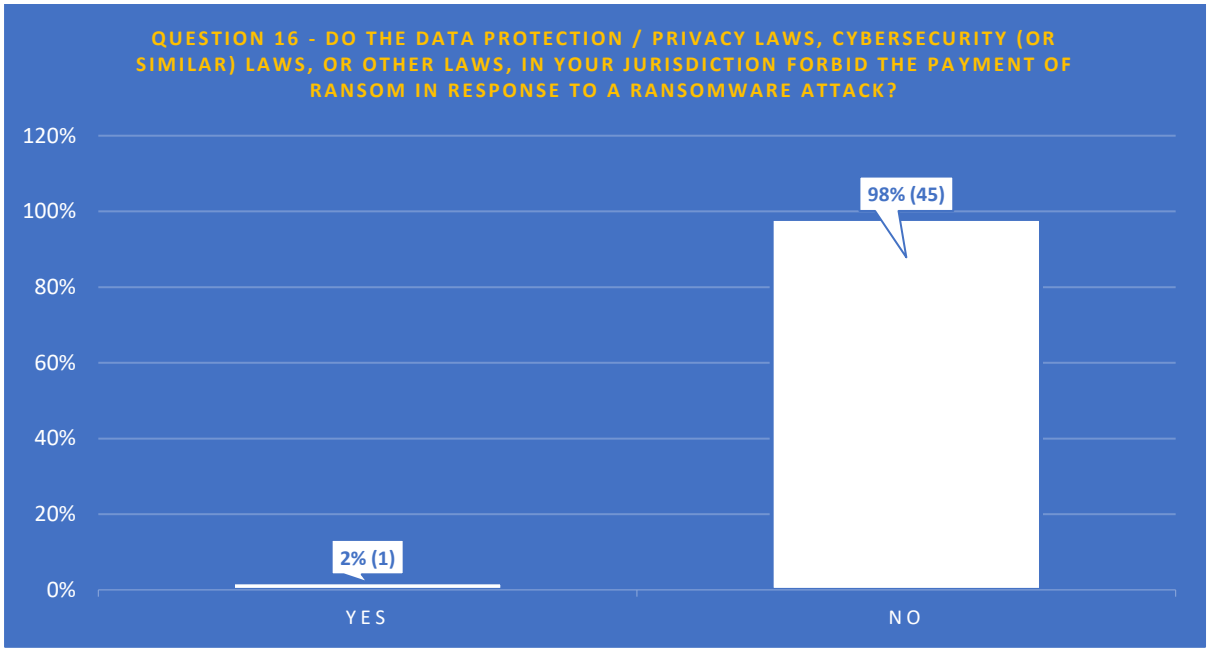
Return to report

Fig 15



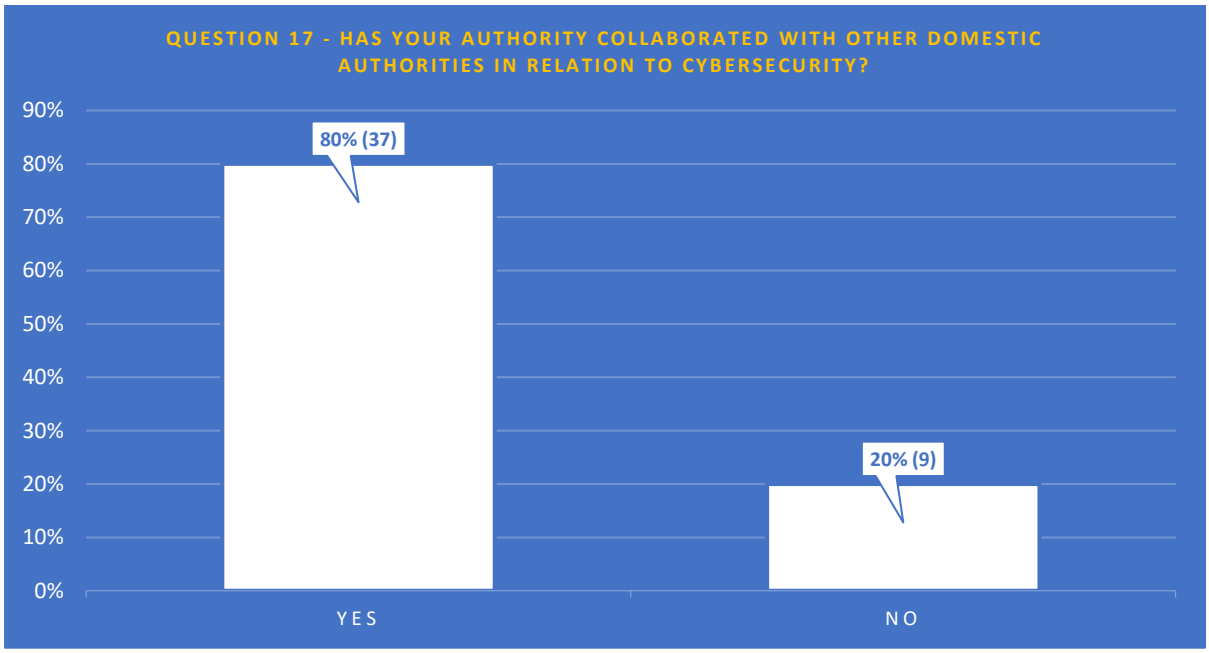
Return to report

Fig 16



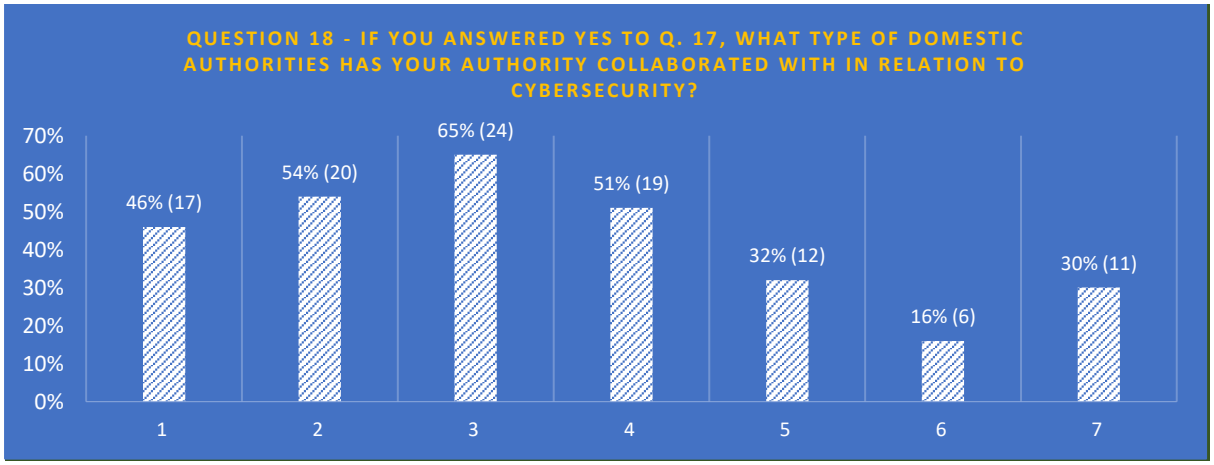
Return to report

Fig 17



Return to report

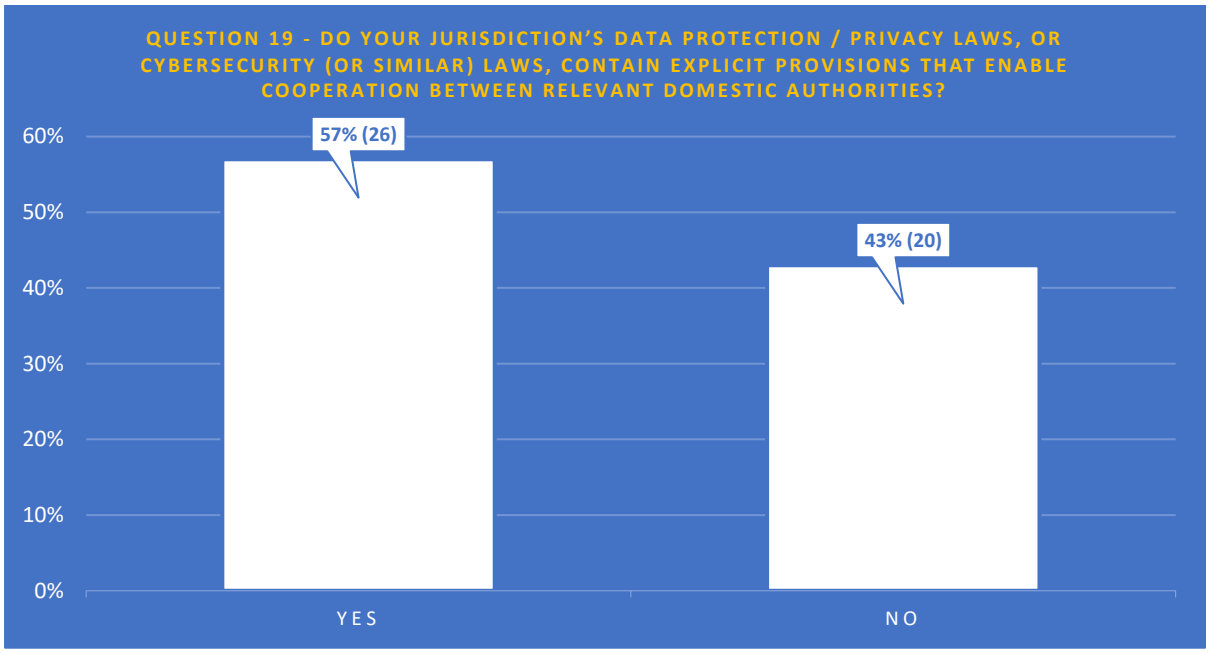
Fig 18



1	National security
2	Law enforcement
3	Computer Security Incident Response Team
4	Sector regulators
5	Standards bodies
6	Trade bodies
7	Other

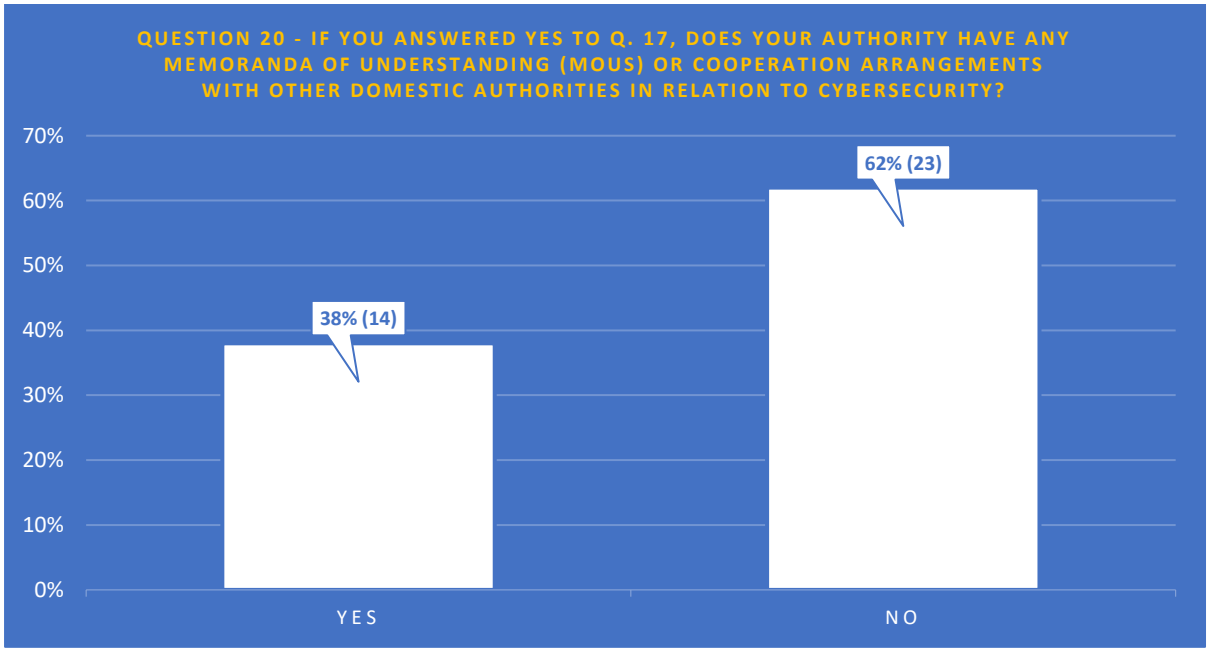
Return to report

Fig 19



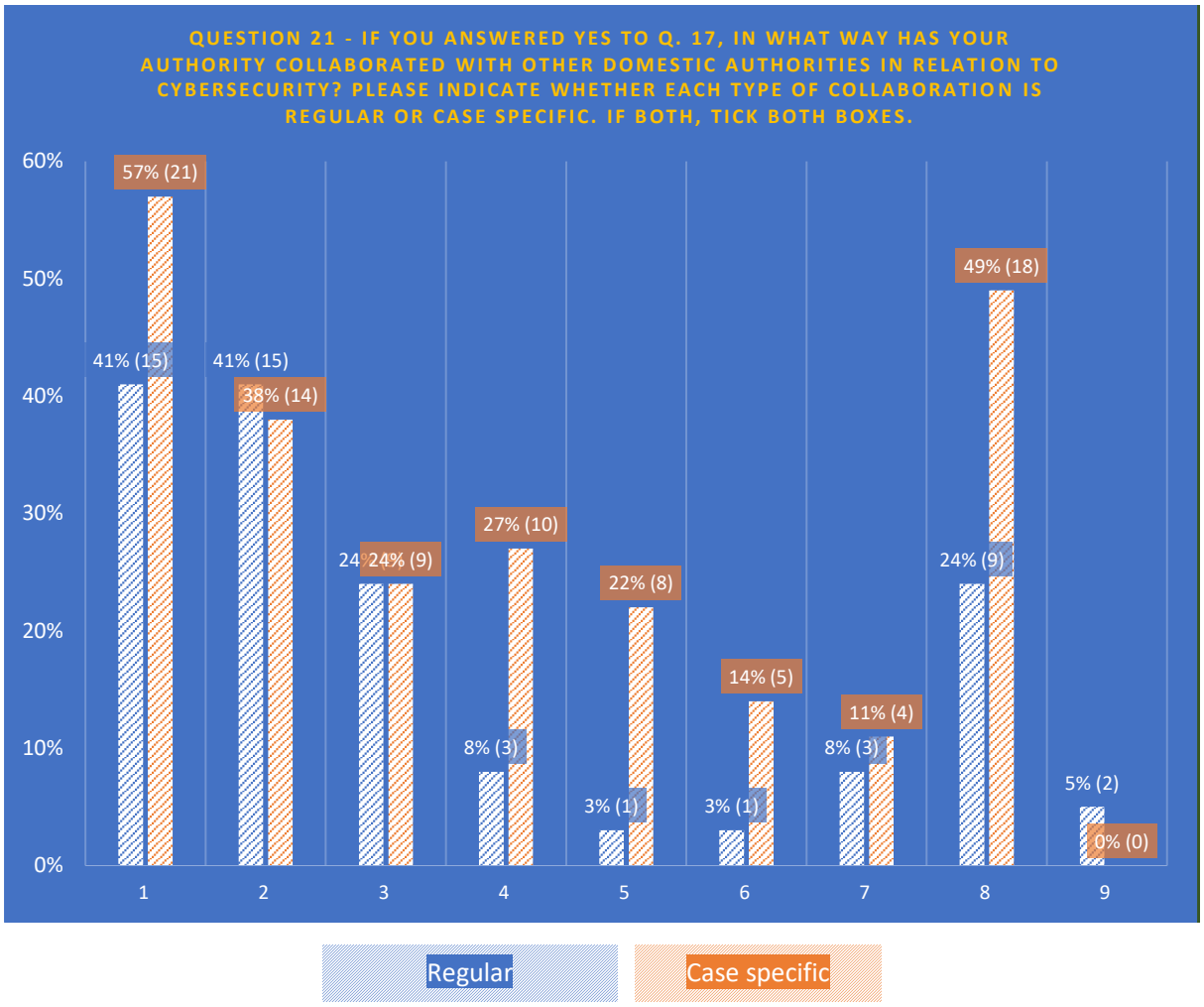
Return to report

Fig 20



Return to report

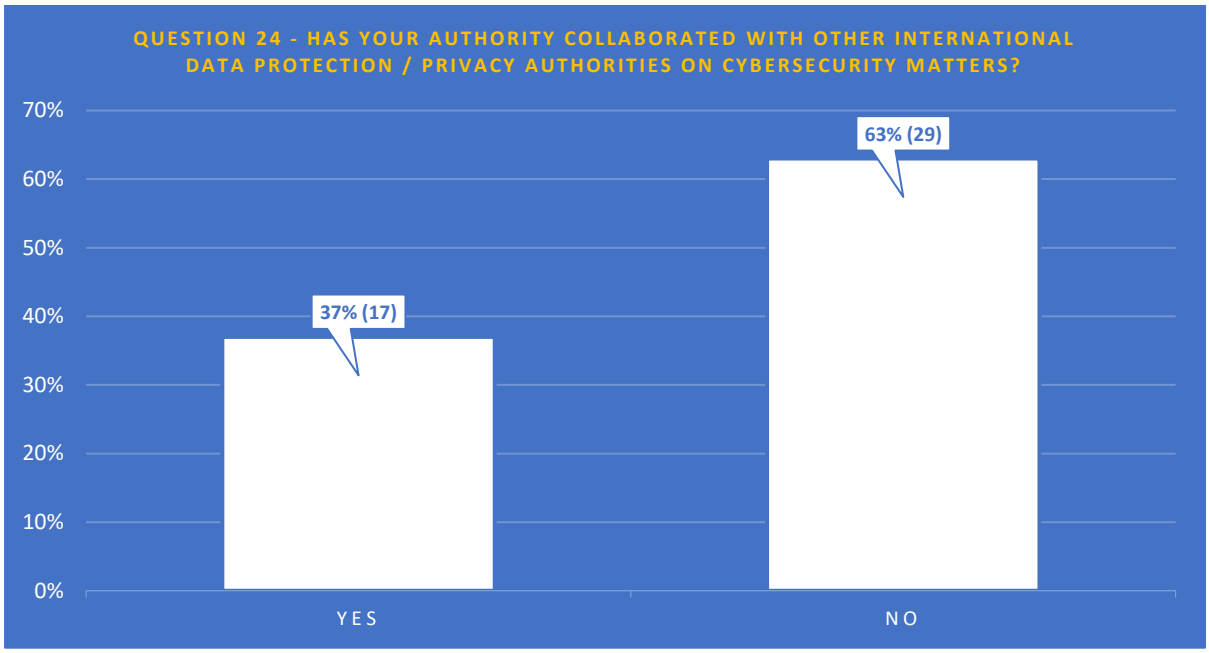
Fig 21



1	Information sharing
2	Joint public awareness raising
3	Joint guidance for organisations
4	Complaint referrals
5	Joint incident response
6	Joint investigations
7	Joint threat analysis
8	Joint workshops / events
9	Other

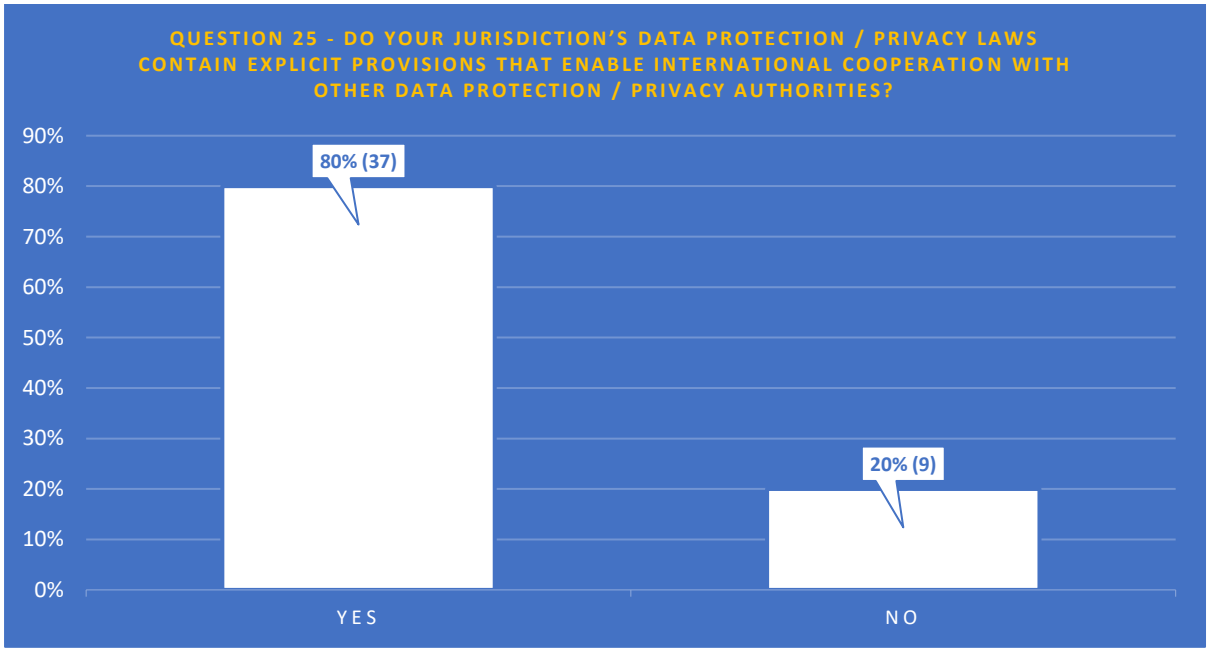
Return to report

Fig 22



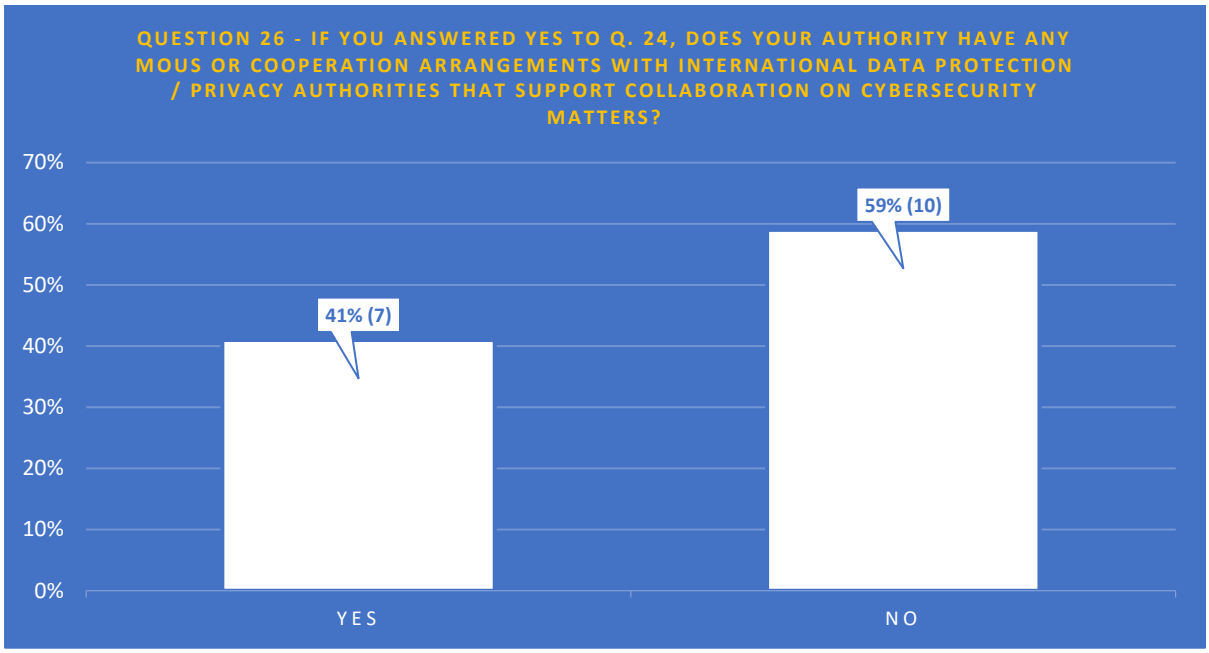
Return to report

Fig 23



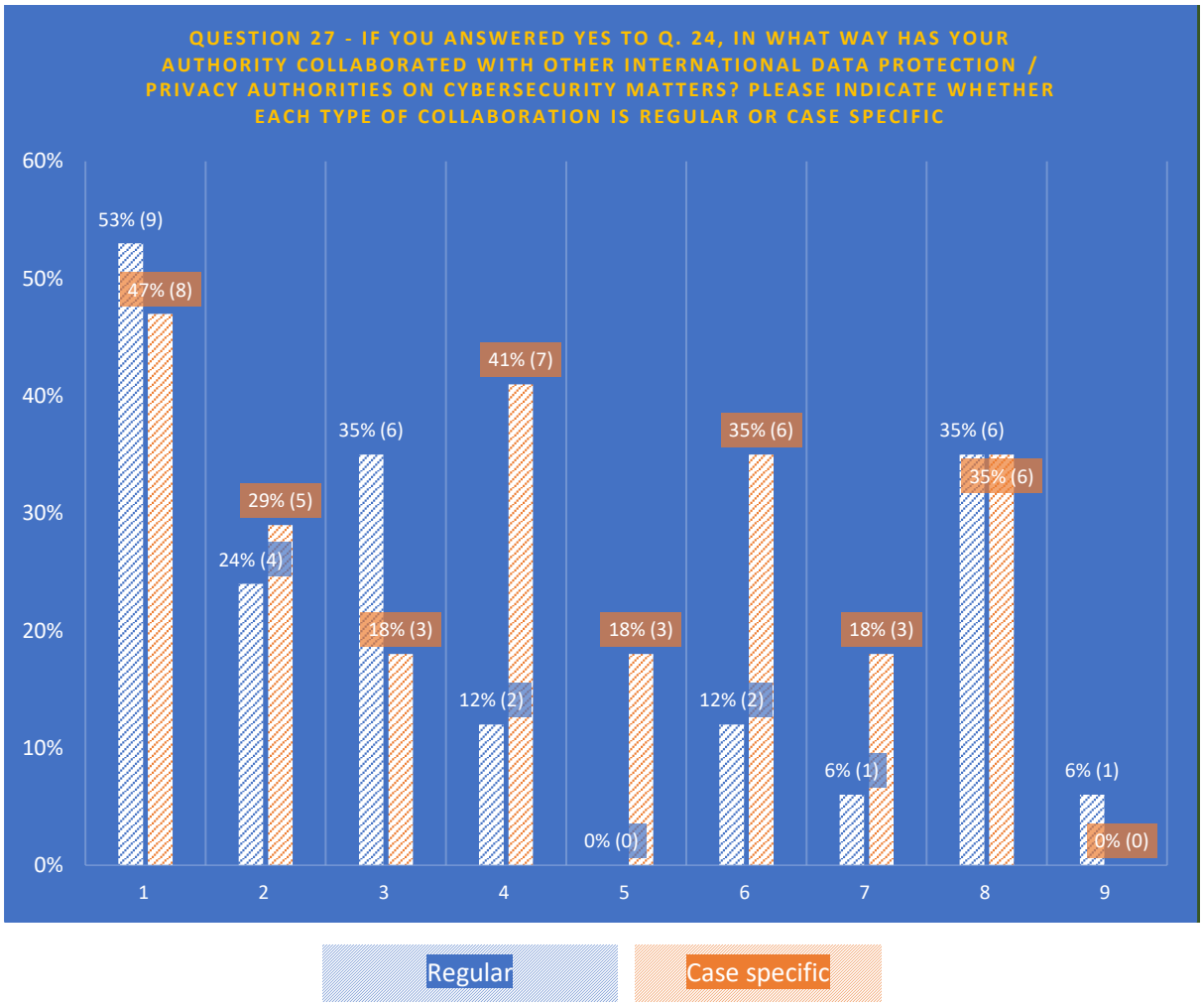
Return to report

Fig 24



Return to report

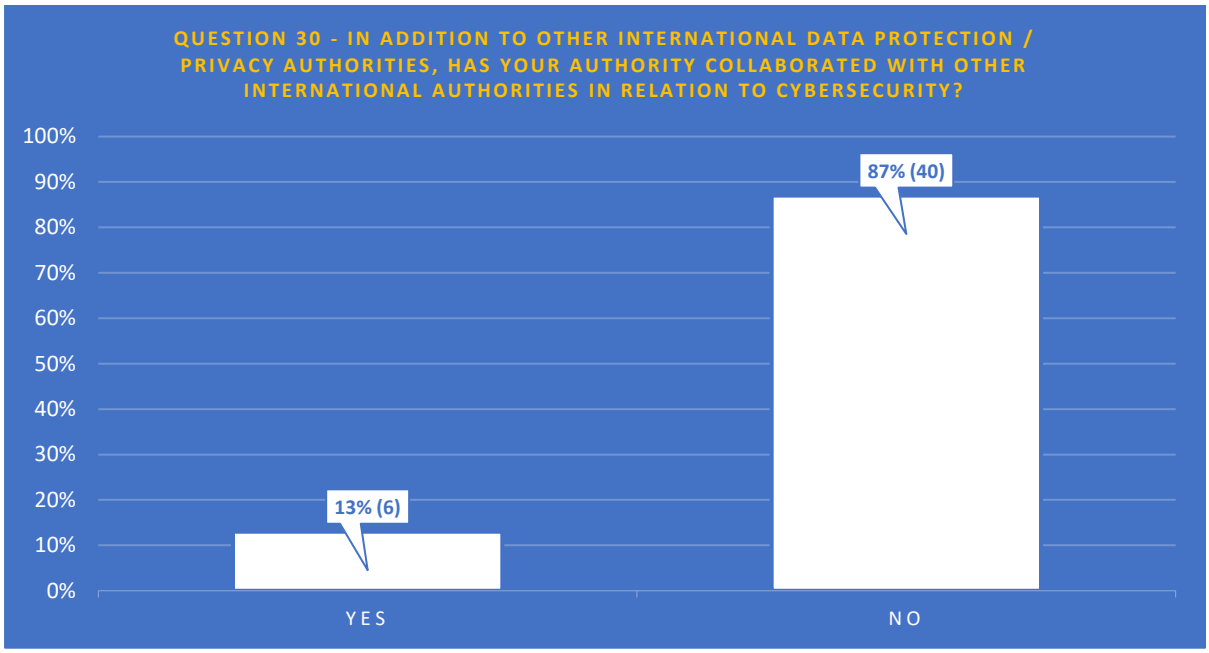
Fig 25



1	Information sharing
2	Joint public awareness raising
3	Joint guidance for organisations
4	Complaint referrals
5	Joint incident response
6	Joint investigations
7	Joint threat analysis
8	Joint workshops / events
9	Other

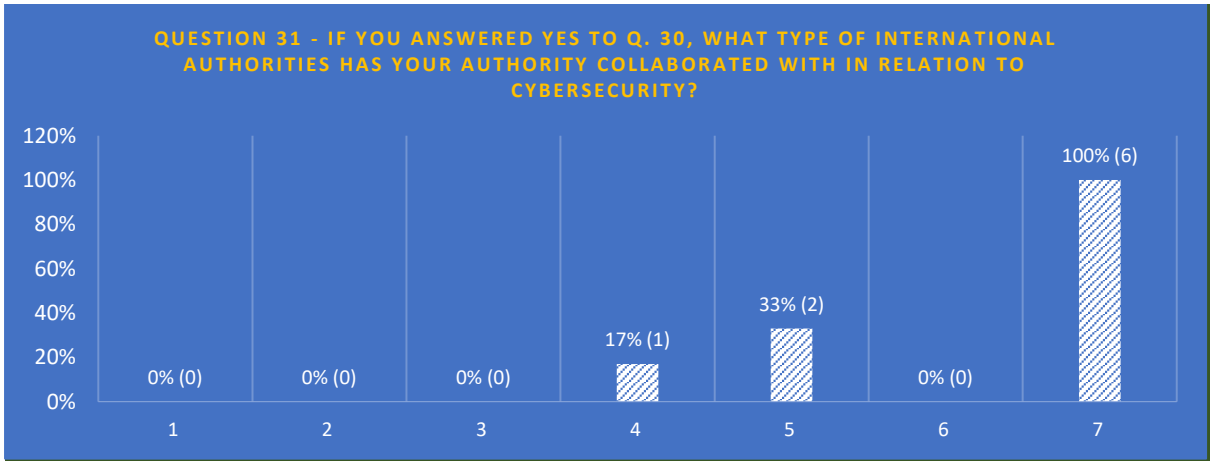
Return to report

Fig 26



Return to report

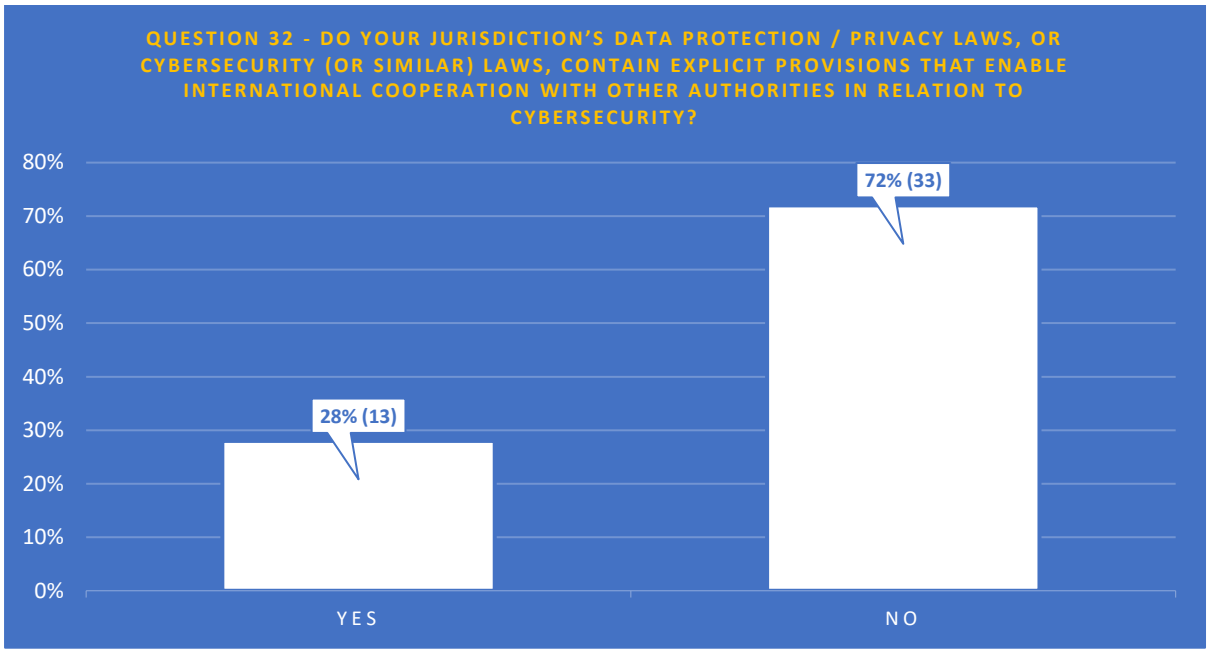
Fig 27



1	National security
2	Law enforcement
3	Computer Security Incident Response Team
4	Sector regulators
5	Standards bodies
6	Trade bodies
7	Other

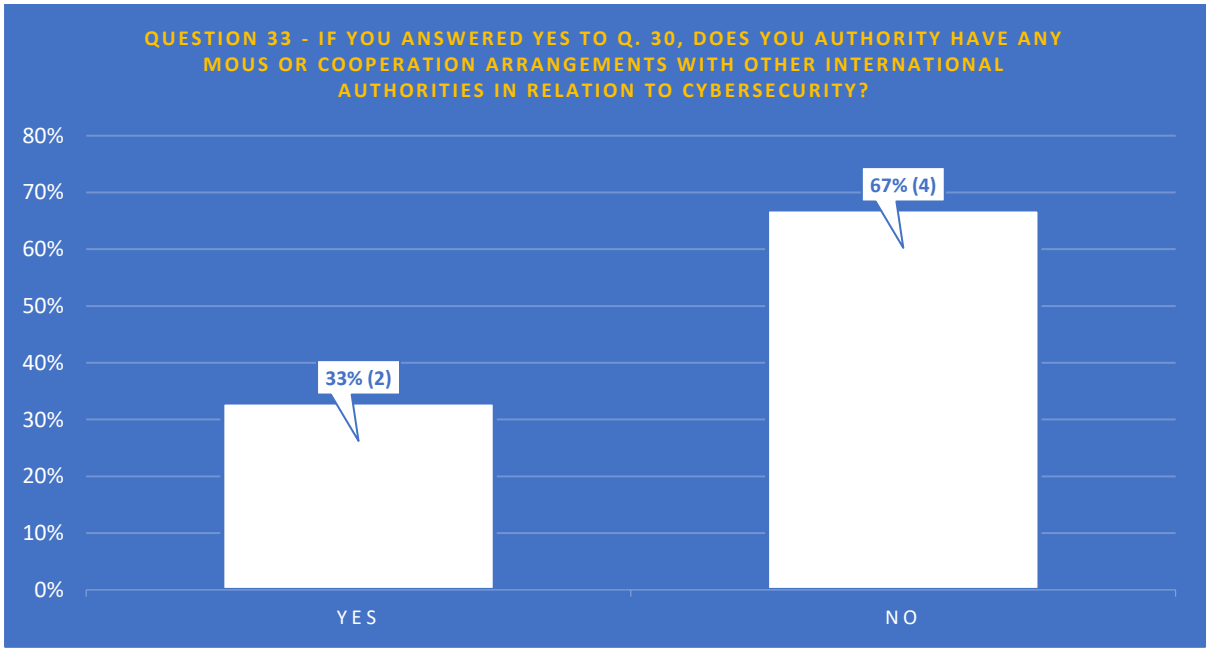
Return to report

Fig 28



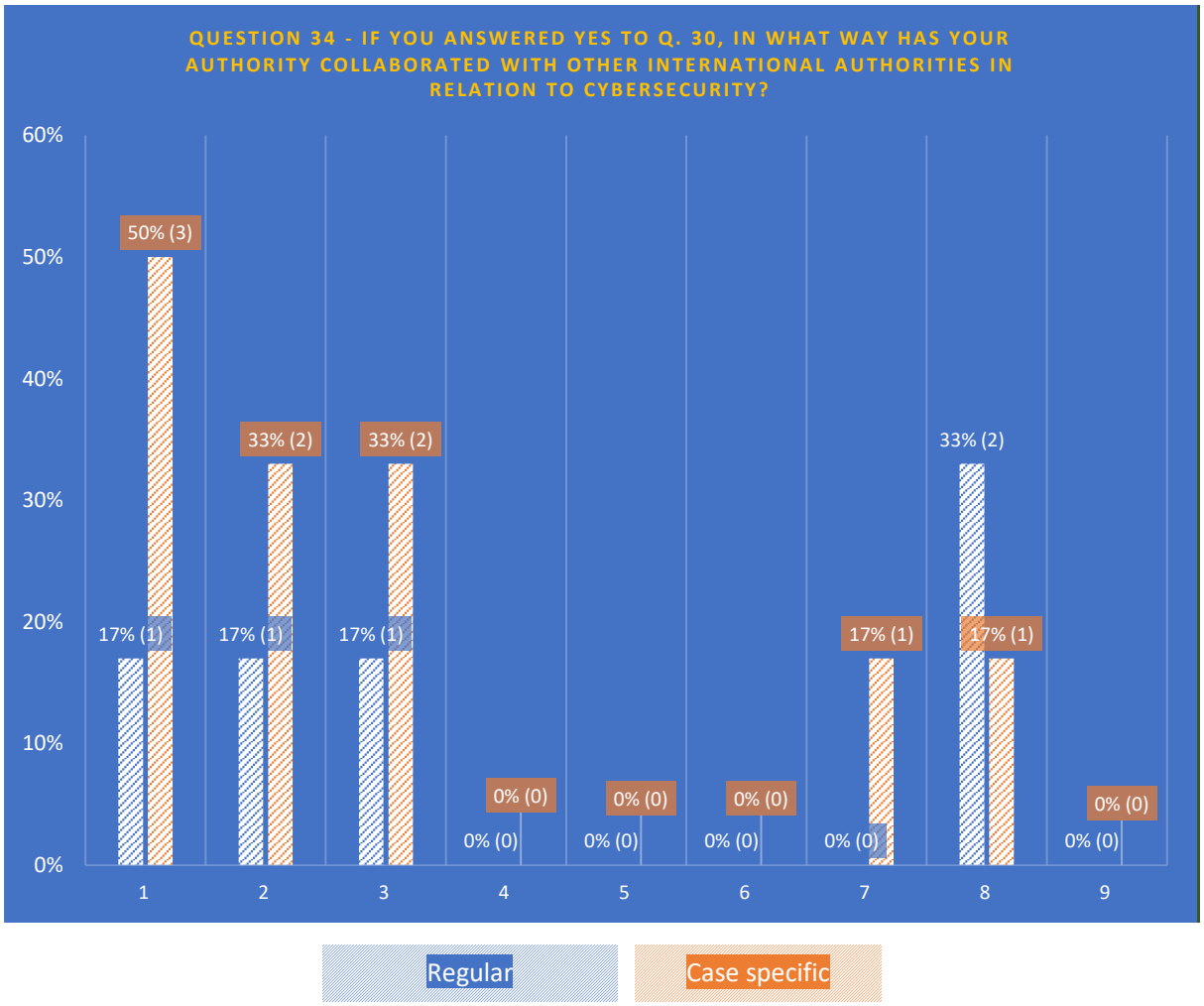
Return to report

Fig 29



Return to report

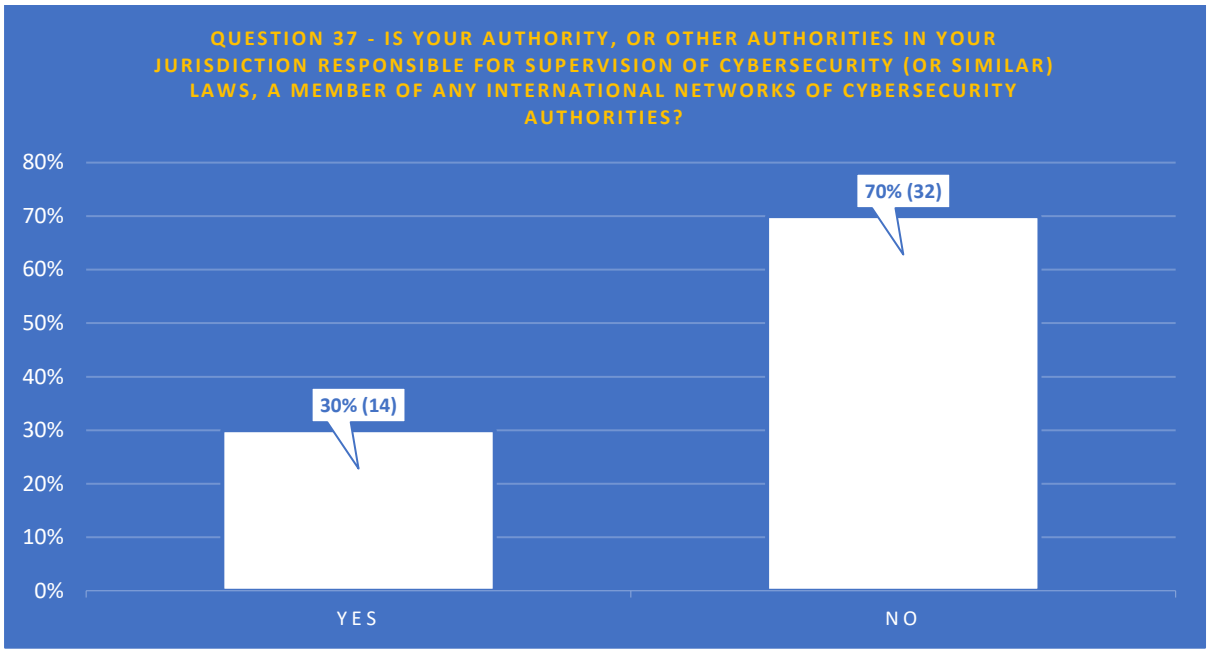
Fig 30



1	Information sharing
2	Joint public awareness raising
3	Joint guidance for organisations
4	Complaint referrals
5	Joint incident response
6	Joint investigations
7	Joint threat analysis
8	Joint workshops / events
9	Other

Return to report

Fig 31



Return to report