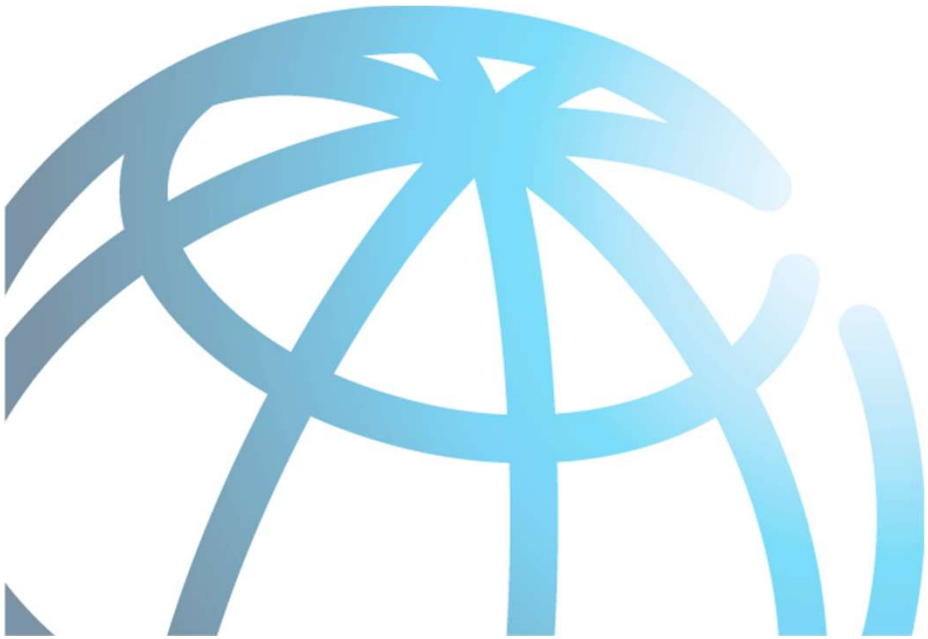
ICCR
INTERNATIONAL COMMITTEE ON CREDIT REPORTING

Cybersecurity in Credit Reporting



November 2019

OUTLINE

- Background
- Survey
  - Respondents
  - Survey findings
  - Policy considerations
- Suggested way forward

ICCR
INTERNATIONAL COMMITTEE ON CREDIT REPORTING

BACKGROUND

- Changes in credit reporting industry landscape including the adoption of new technologies and business models and the emergence of new players posing additional risks for CRSPs.
- Several CRSPs have been subject to data breaches, denial-of-service attacks, and phishing attacks, among other cyber incidents in the past decade resulting in financial, economic, operational, and reputational loss.
- Against this background, the ICCR drafted Guidelines on the Cybersecurity in Credit Reporting building on General Principles on Credit Reporting.
- This guideline provides findings of a landscaping survey conducted by the Committee on CRSPs across the globe on current practices and proffers some policy considerations.

ICCR
INTERNATIONAL COMMITTEE ON CREDIT REPORTING

General Principles on Credit Reporting

Data Processing: Security and Efficiency
GP 2: Credit reporting systems should have rigorous standards of security and reliability, and be efficient.

Governance and Risk Management
GP3: The governance arrangements of CRSP and data providers should ensure accountability, transparency and effectiveness in managing the risks associated with the business and fair access to the information by users.

Recommendation E: Central Banks, Financial supervisors, and other relevant authorities, both domestic and international should cooperate with each other, as appropriate in promoting the safety and efficiency on credit reporting systems.

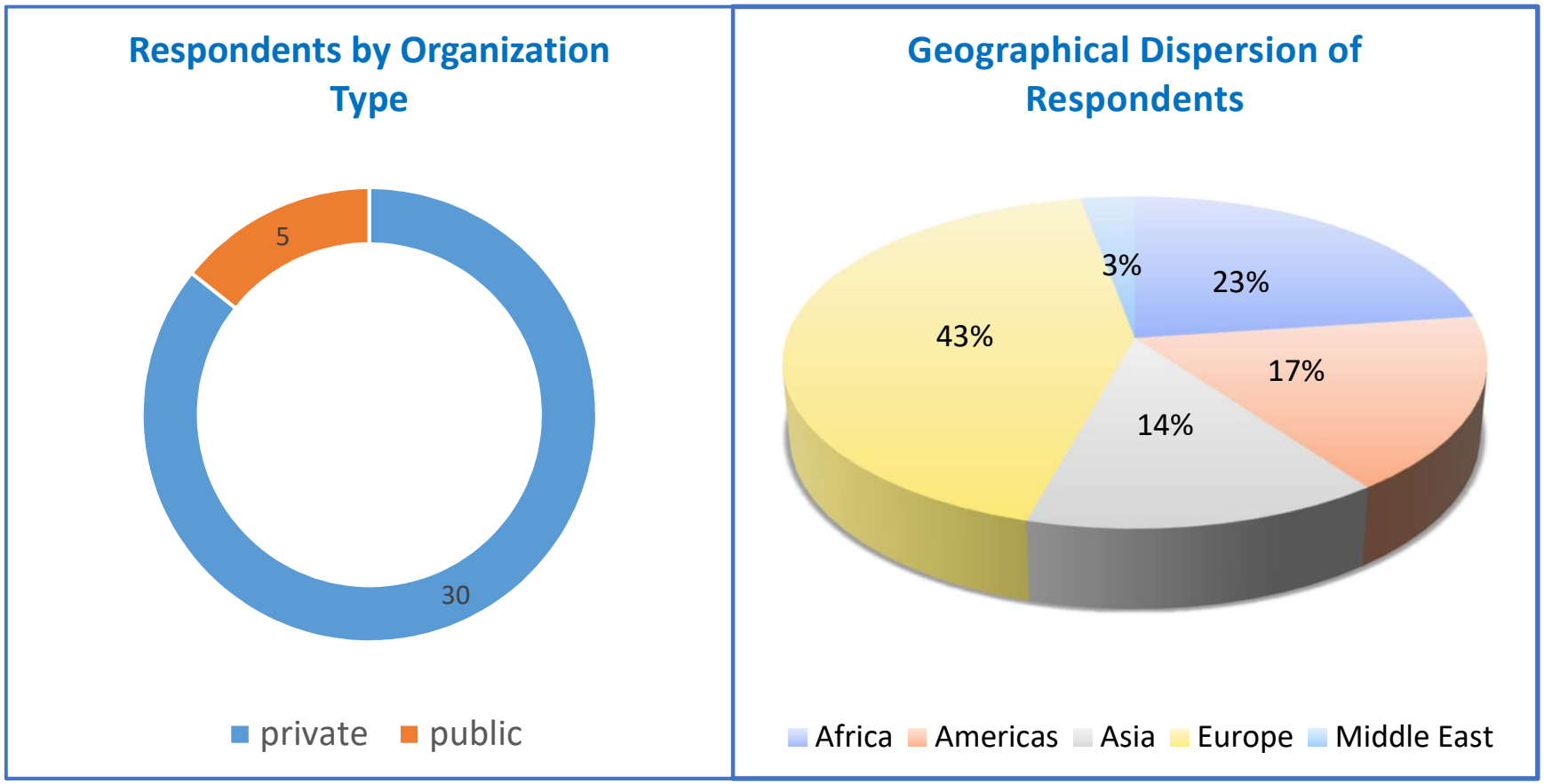
Survey:

Response Statistics

Number of Responses	45
Completion Rate	85%
Exclusions	10
Number Analyzed	35

7 – Incomplete Responses
3 - Duplications

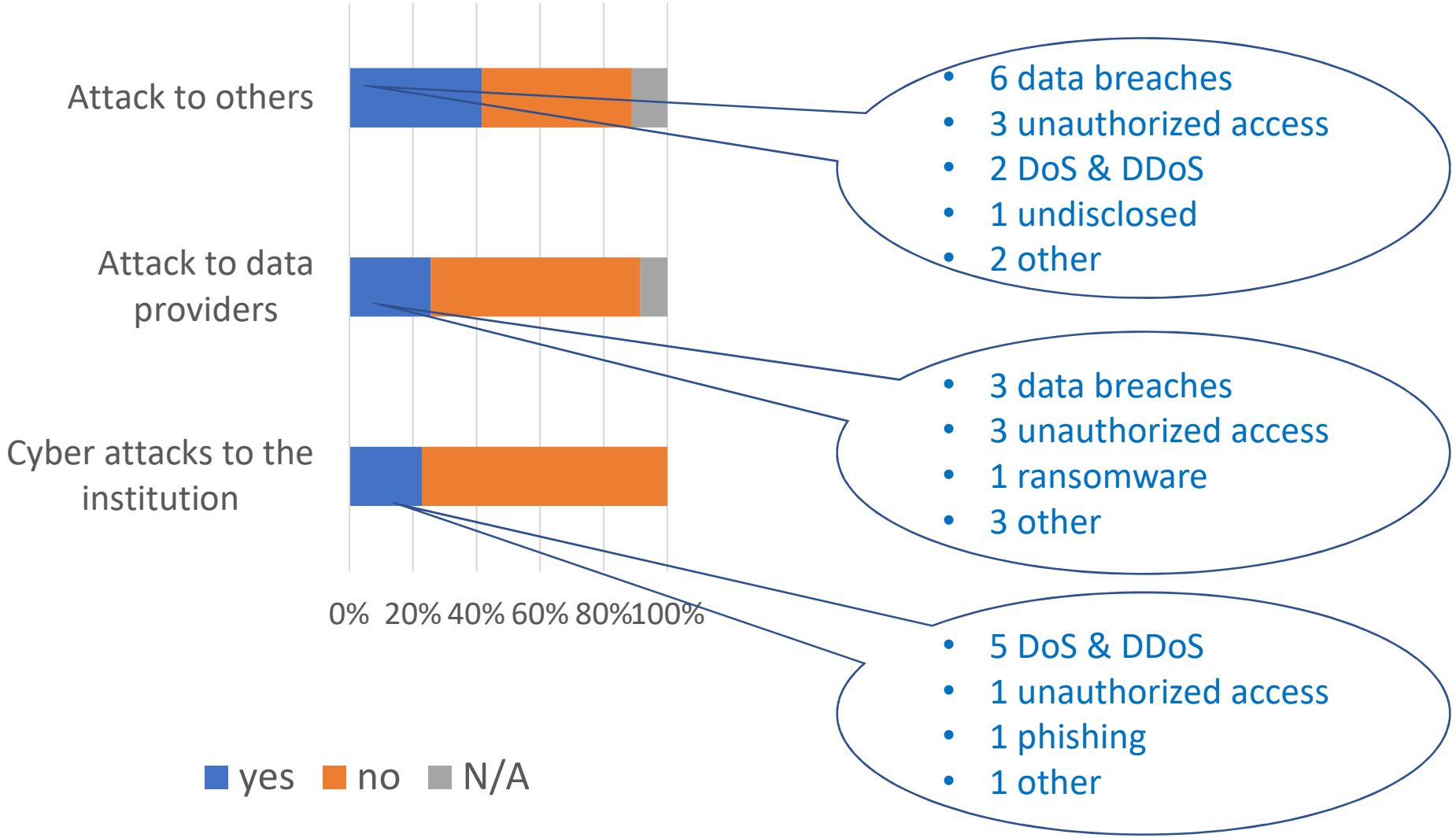
Respondents Demographics



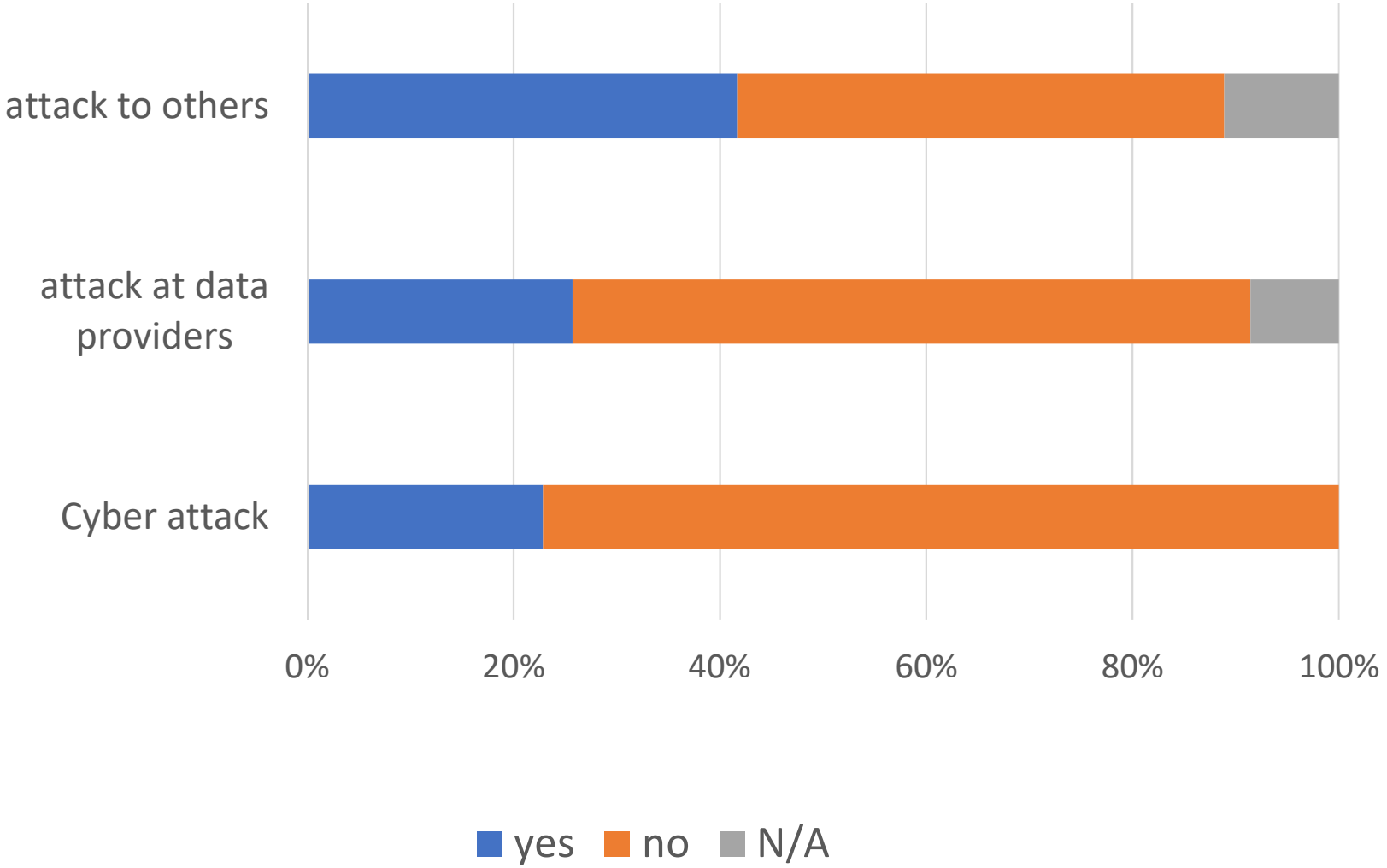
Survey Topics

- Local cybersecurity environment
- Legal and regulatory environment
- Board, Management and Cybersecurity and Information Security Strategy
- Outsourcing Critical IT services
- Information Sharing
- Training and Awareness
- Resources
- Risk Management and compliance
- Audit
- Incident response
- Data loss prevention
- Preventive controls

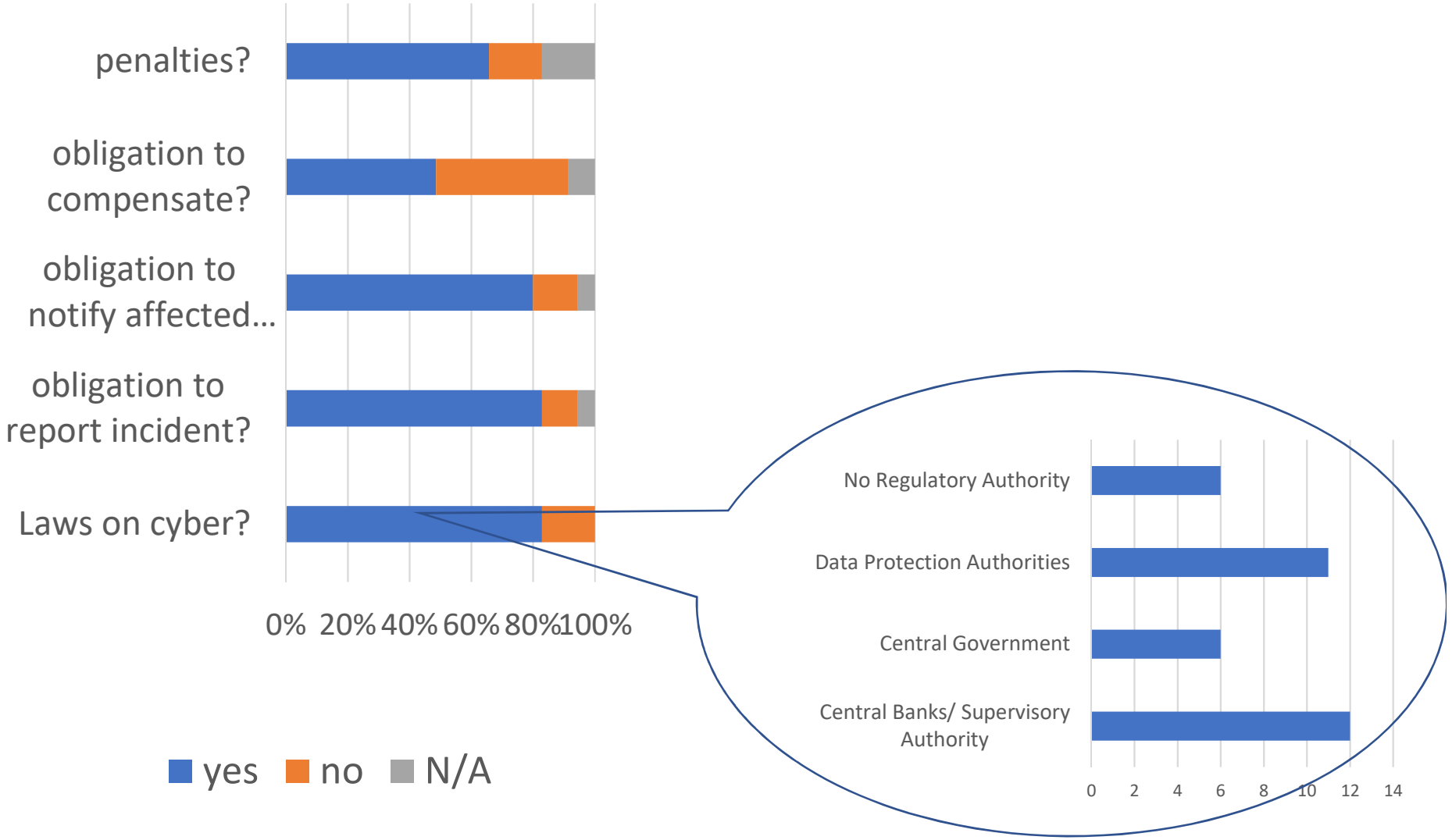
Cybersecurity incidents Q5-13



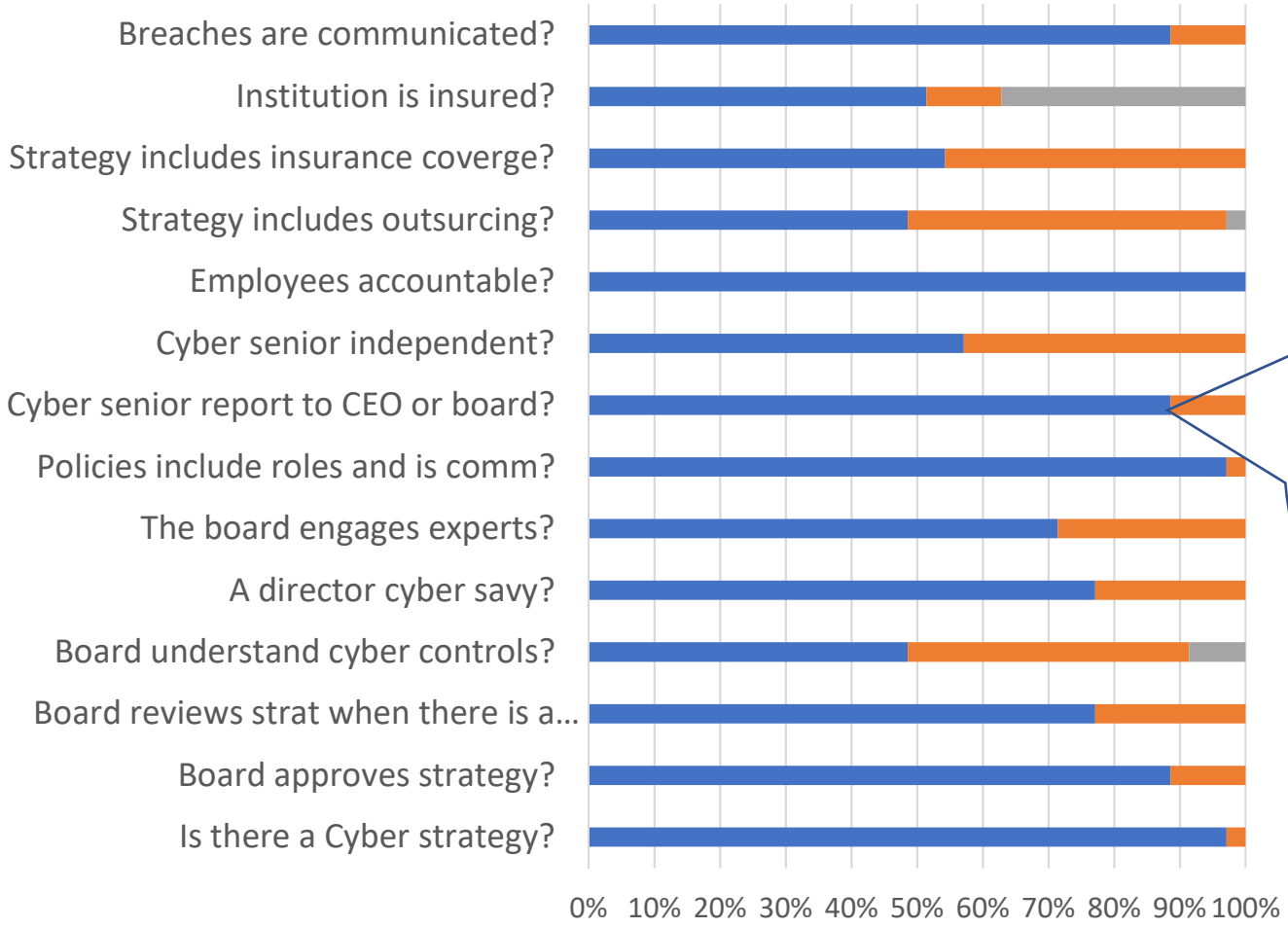
Cybersecurity incidents Q5-13



Legal and regulatory environment Q14-19



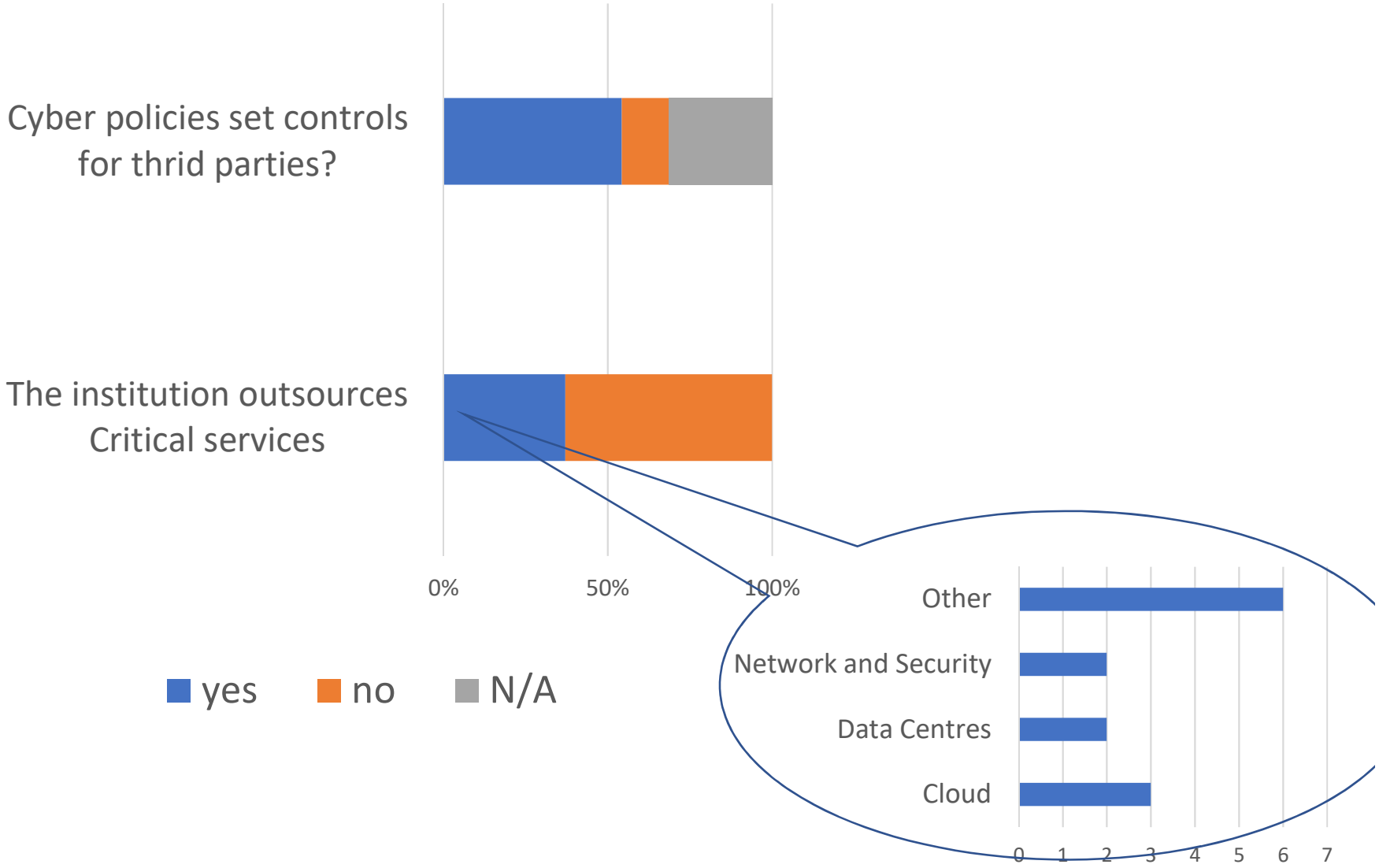
Board, Management and Cybersecurity and Information Security Strategy Q20- 34



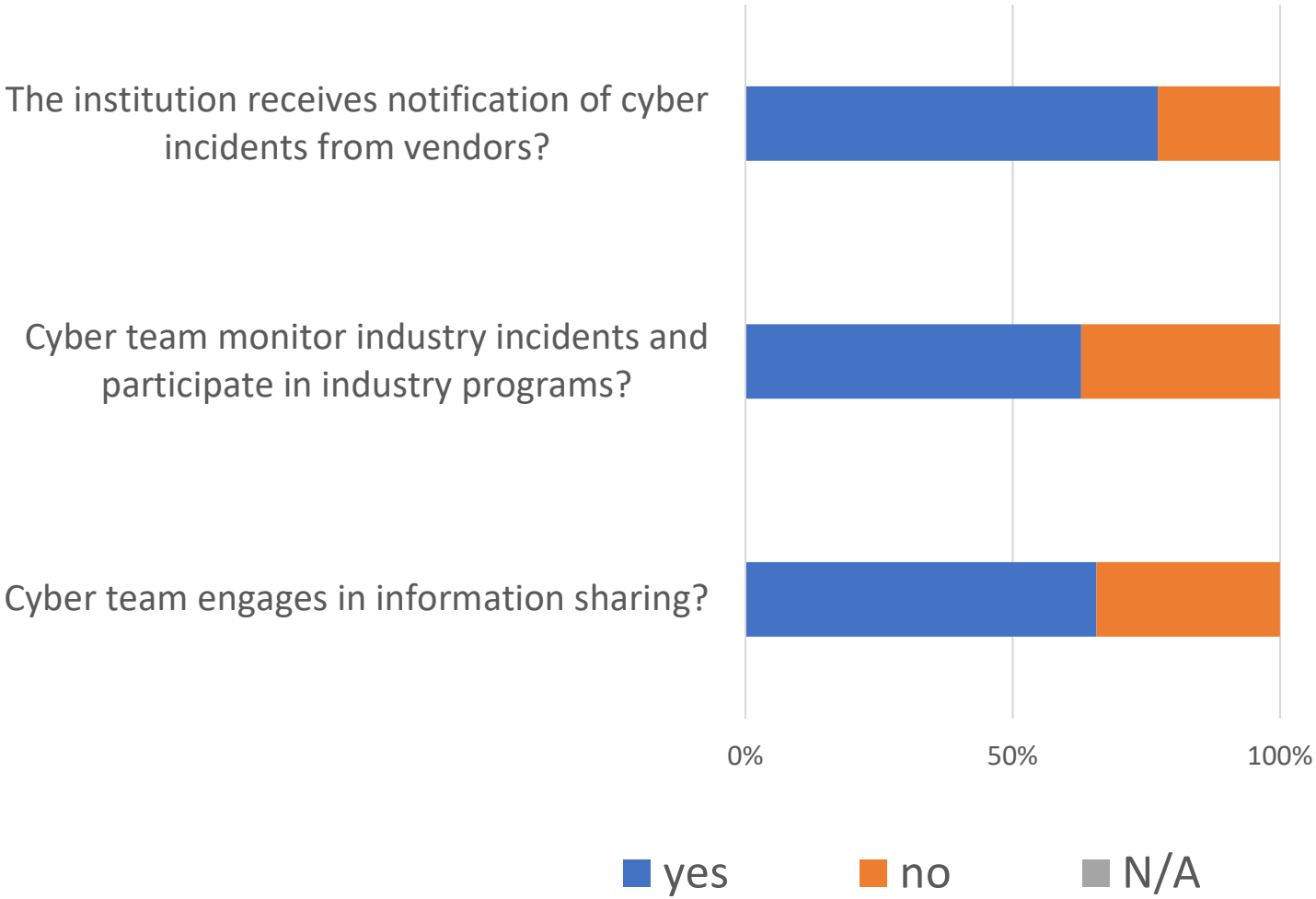
Most senior Cyber officer

- 17 CIO
- 14 CISO
- 1 CEO
- 1 General counsel
- 1 VP
- 1 CRO

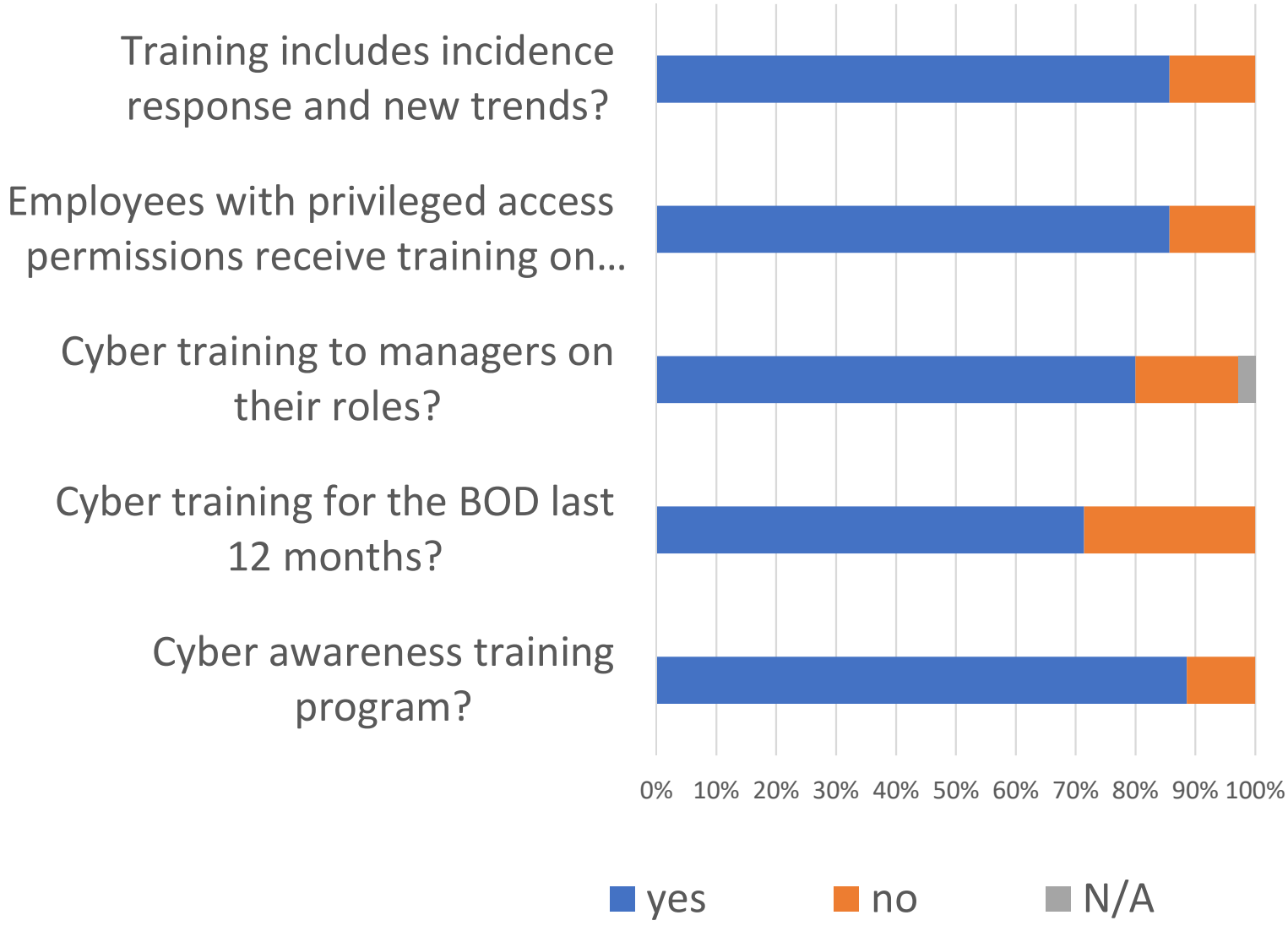
Outsourcing Critical IT services Q35- 37



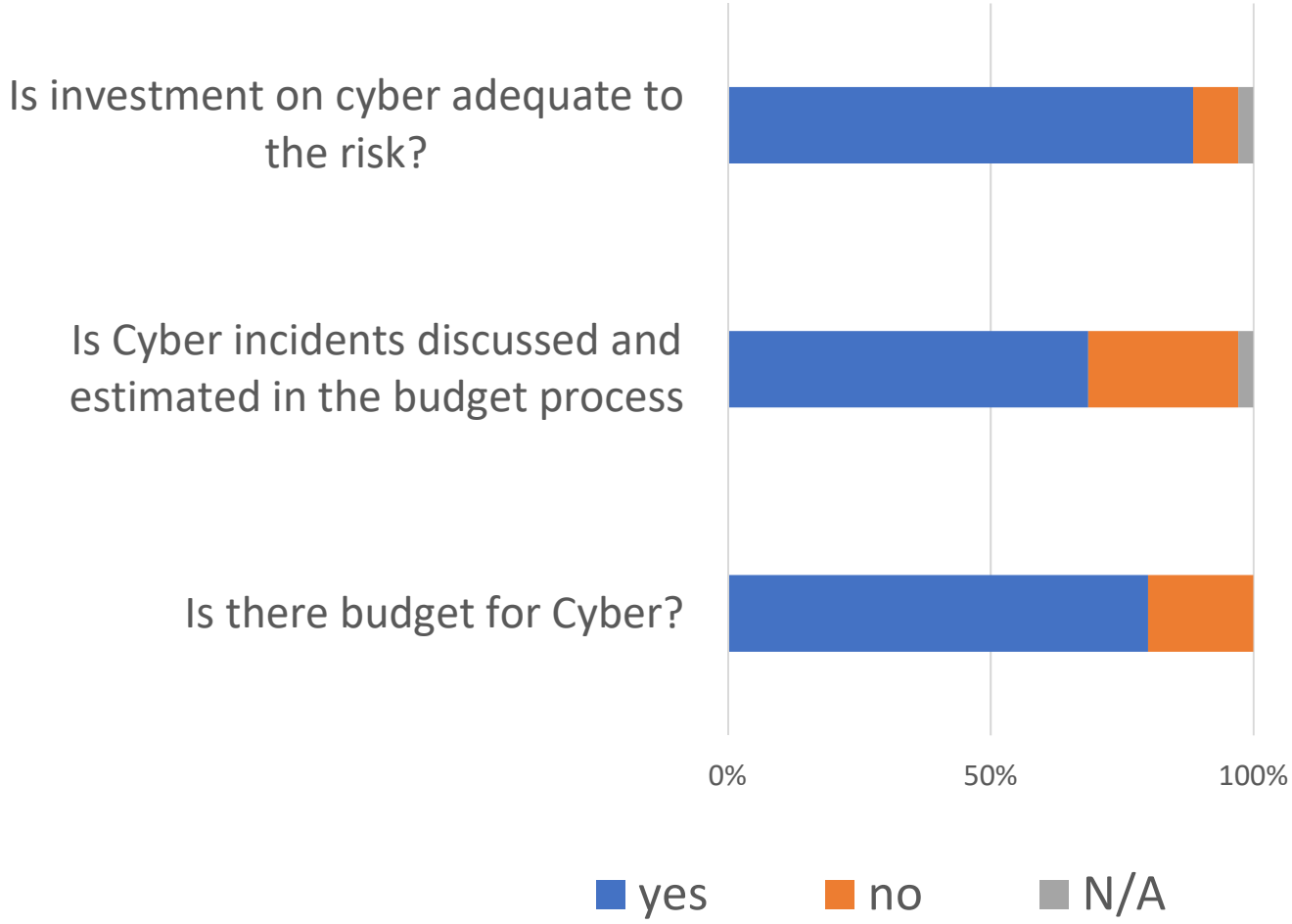
Information Sharing Q38- 40



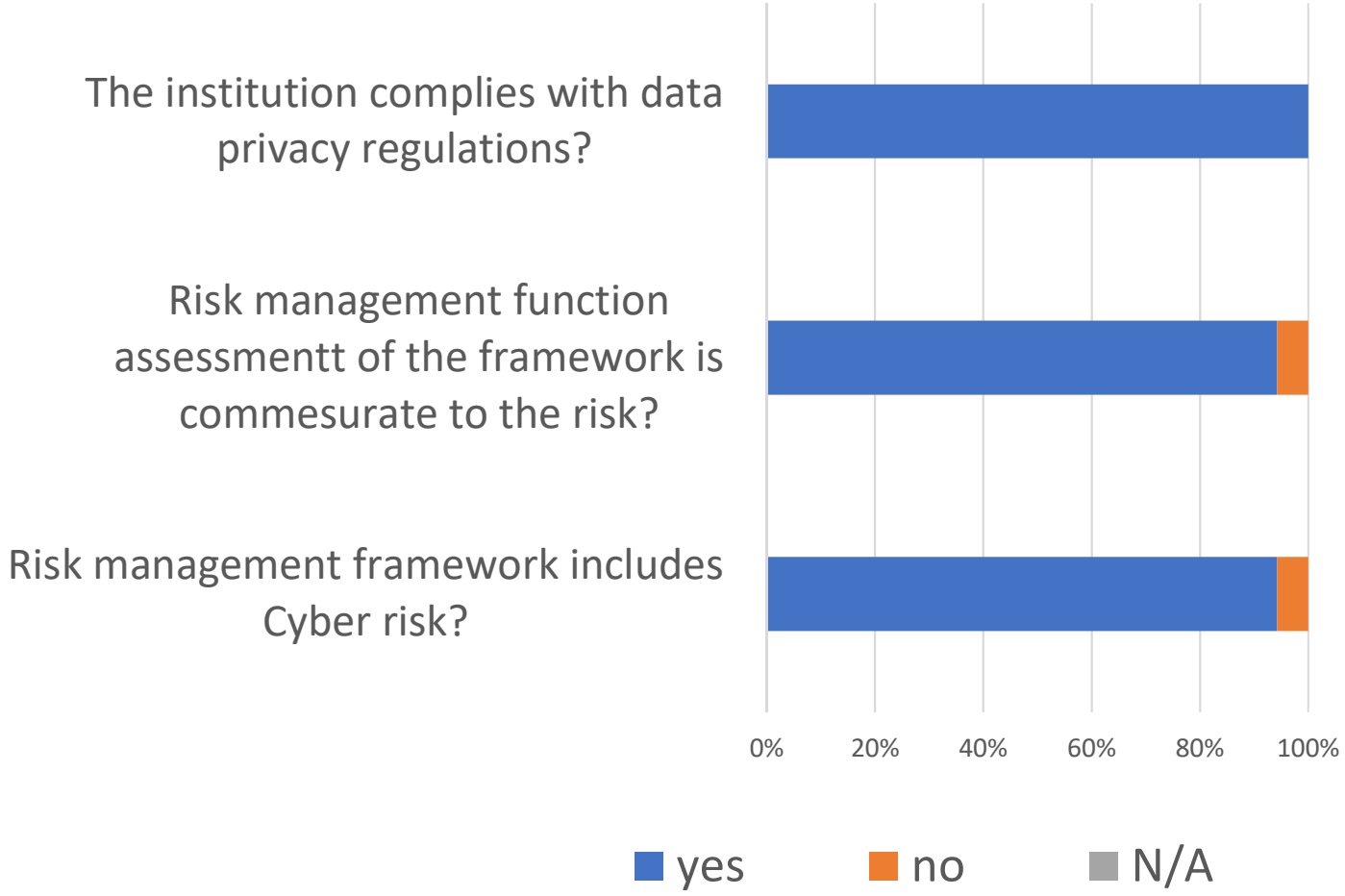
Training and Awareness Q41- 45



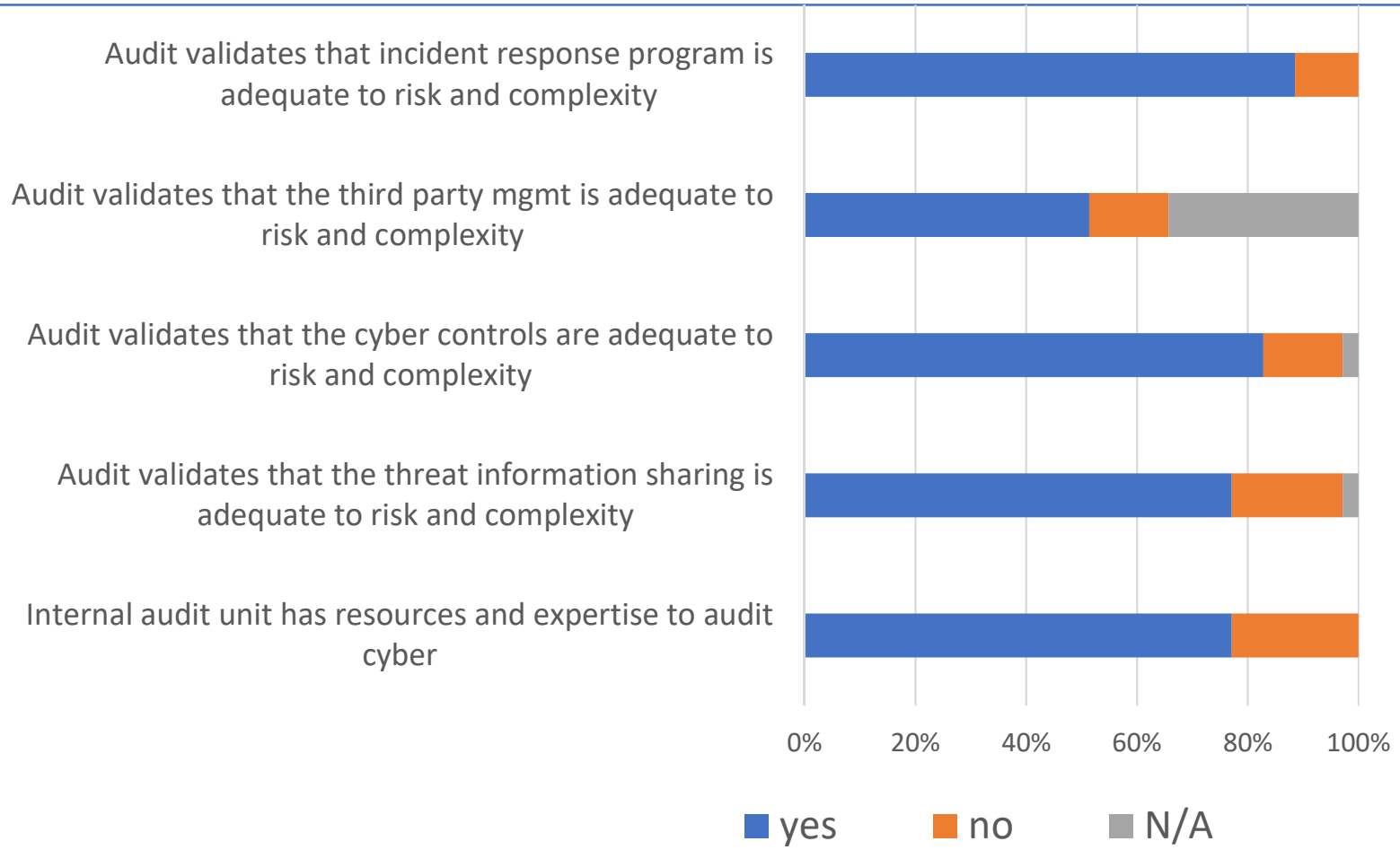
Resources Q46- 48



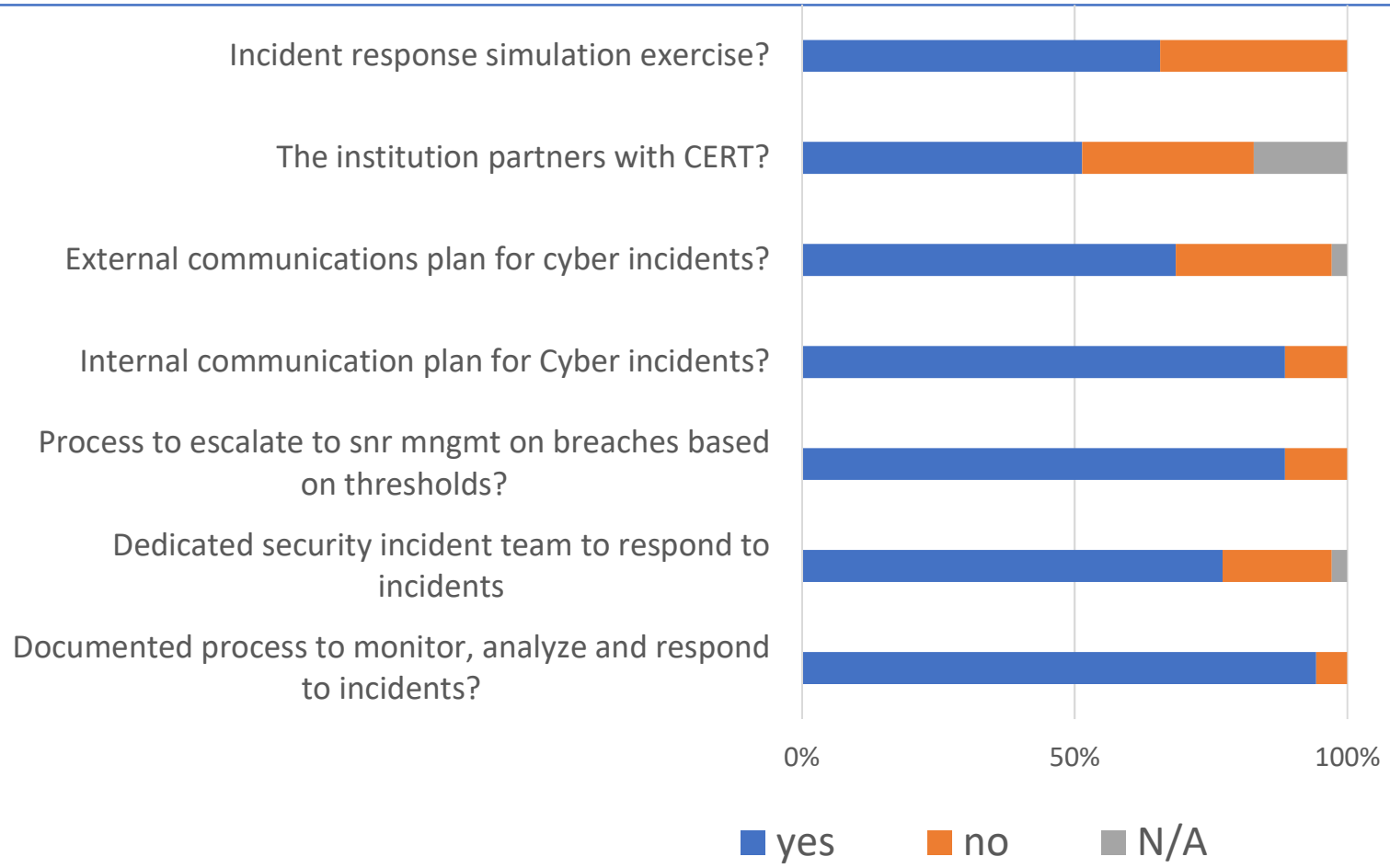
Risk Management and compliance Q49- 51



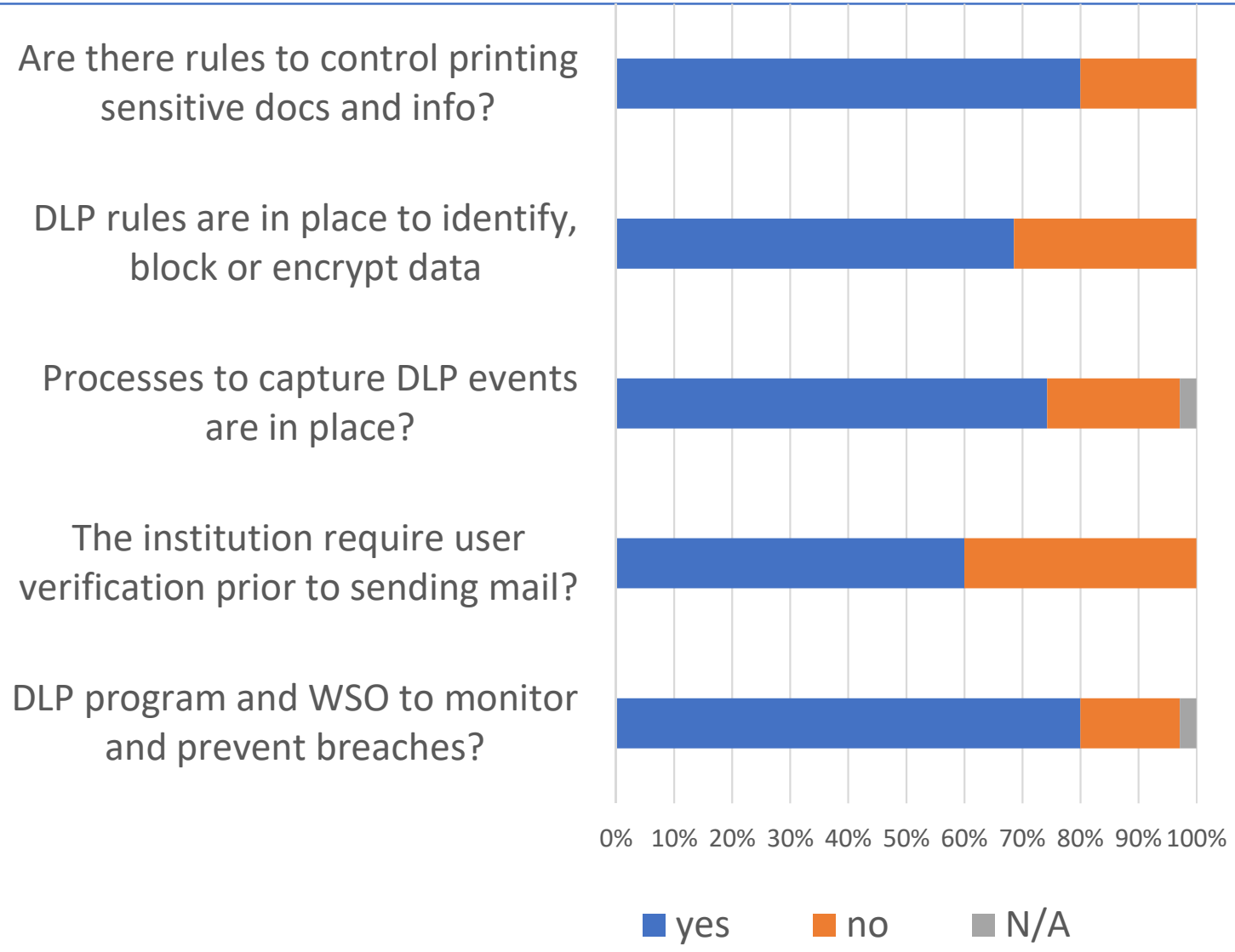
Audit Q52- 56


Audit validates that incident response program is adequate to risk and complexity
Audit validates that the third party mgmt is adequate to risk and complexity
Audit validates that the cyber controls are adequate to risk and complexity
Audit validates that the threat information sharing is adequate to risk and complexity
Internal audit unit has resources and expertise to audit cyber
0%
20%
40%
60%
80%
100%
yes
no
N/A

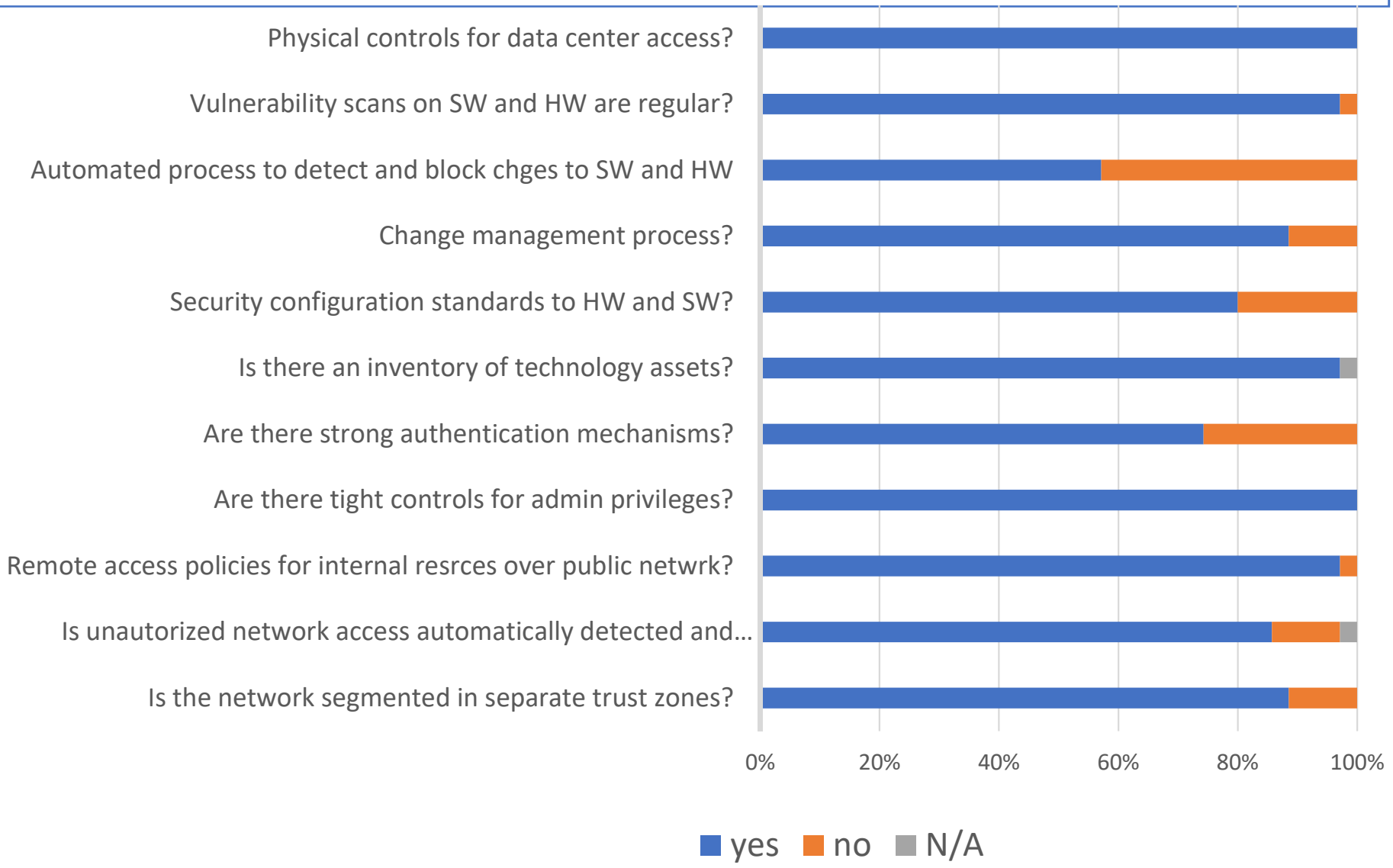
Incident Response Q57- 63



Data Loss prevention Q64- 68



Preventive Controls Q69- 79



POLICY CONSIDERATIONS

- Authorities need to consider:
  - Implementing and/or enhancing **cyber laws and regulations**.
  - Developing **national and/or sector-wide cybersecurity strategies and frameworks**.
  - Implementing **practices or standards that promote the strengthening of cyber governance** by CRSPs.
  - Requiring CRSPs to develop detailed **programs for training** their boards of directors.
  - Issue **guidance on the level and extent of disclosures of security and data breaches**.
  - Ensure that CRSPs implement **sound outsourcing procedures** that detail the controls and processes to be followed when evaluating and managing relationships with third parties.
  - **Subjecting third parties that service CRSPs with the same level of risk management practices** expected of the entities themselves.

POLICY CONSIDERATIONS

- Conducting **annual cybersecurity risk assessments** of critical infrastructure players.
- Encouraging CRSPs to conduct their **own internal assessments** on a periodic basis.
- Promoting **regular cyber audits** of cyber functions.
- Developing **mechanisms that foster and enforce cyber information sharing and collaboration** among parties.
- **Publishing or promote publication of redacted reports** on cybersecurity issues on a semi-annually (half yearly) basis.
- Ensuring that CRSPs **actively participate and collaborate with national cybersecurity actors** such as CERTs.

ICCR
INTERNATIONAL COMMITTEE ON CREDIT REPORTING

SUGGESTED WAY FORWARD

- The Committee will be working on:
  - dissemination of the guideline through workshops.
  - participating in the development of assessment toolkit.
  - conducting country assessments with a view of promoting technical assistance.
  - administering periodic surveys of state of cybersecurity.

ICCR
INTERNATIONAL COMMITTEE ON CREDIT REPORTING


ICCR
INTERNATIONAL COMMITTEE
ON CREDIT REPORTING