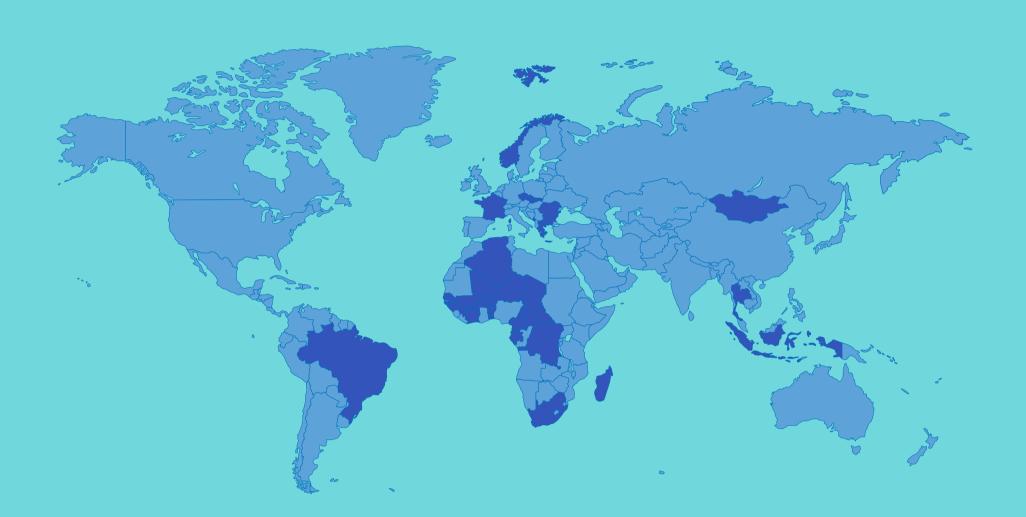


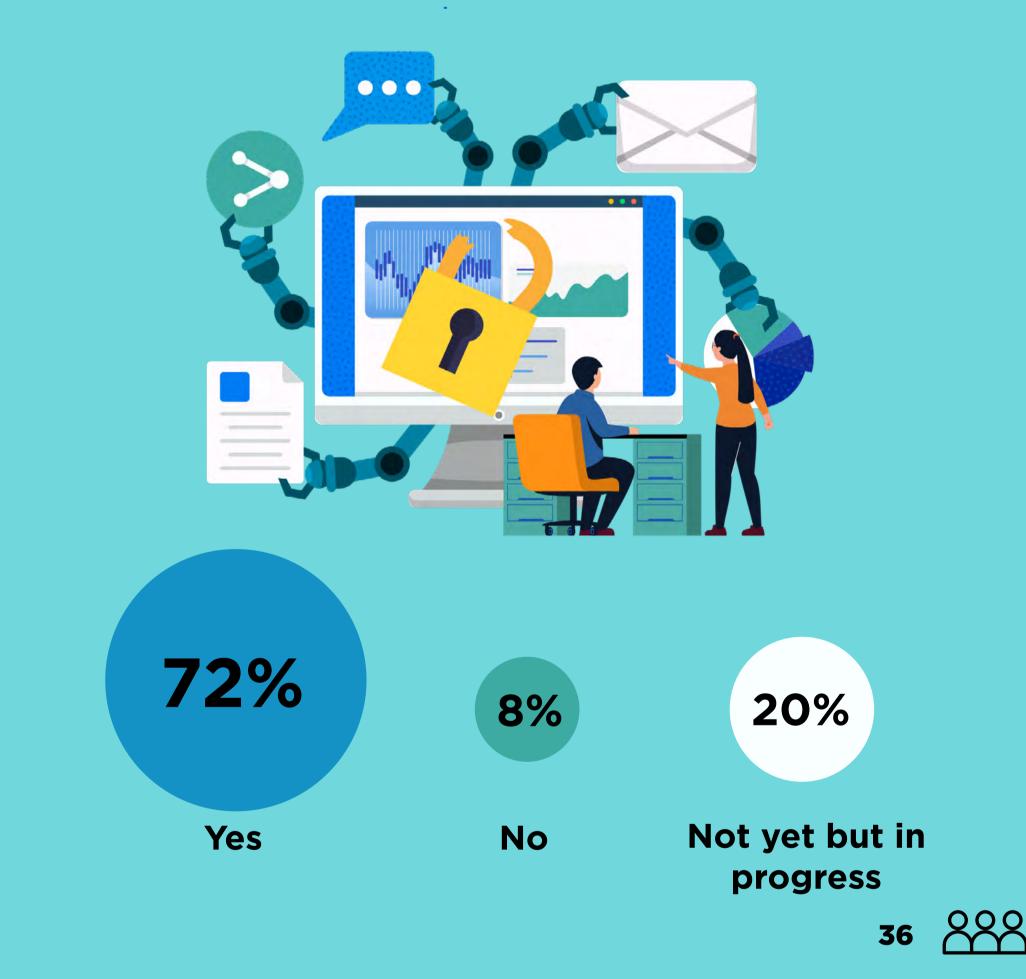
2023 Benchmark



ALGERIA, BELGIUM, BRAZIL, BULGARIA, CAMEROON-BEAC, CZECH REPUBLIC, FRANCE, GREECE, HAITI, INDONESIA, KOSOVO, LATVIA, MAURITIUS, MADAGASCAR, MOLDOVA MONGOLIA, MONTENEGRO, NORTHERN MACEDONIA, NORWAY, **REPUBLIC OF GUINEA, ROMANIA, SENEGAL-BCEAO, SINGAPORE,** SLOVAKIA, SLOVENIA, SOUTH AFRICA, TAIWAN, THAILAND

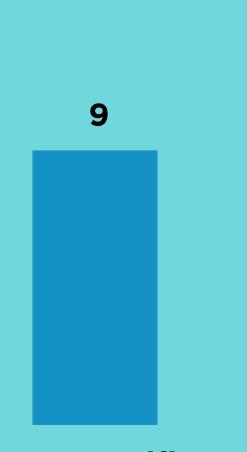


DOES YOUR INSTITUTION HAVE A MANAGEMENT PROTOCOL FOR CYBER CRISES ?

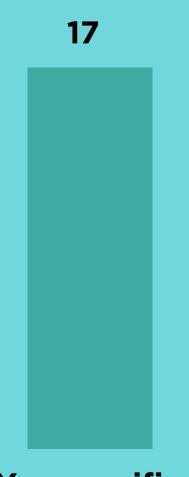


DO YOU HAVE COMMUNICATION

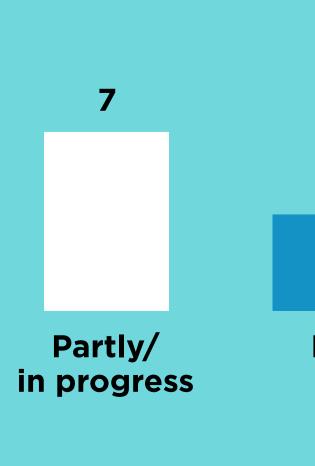
TOOLS AND/OR PROCEDURES, DISTINCT FROM THE STANDARD ONES, ENSURING THAT ACTORS MOBILISED IN A CRISES ARE CONNECTED



Yes specific tools



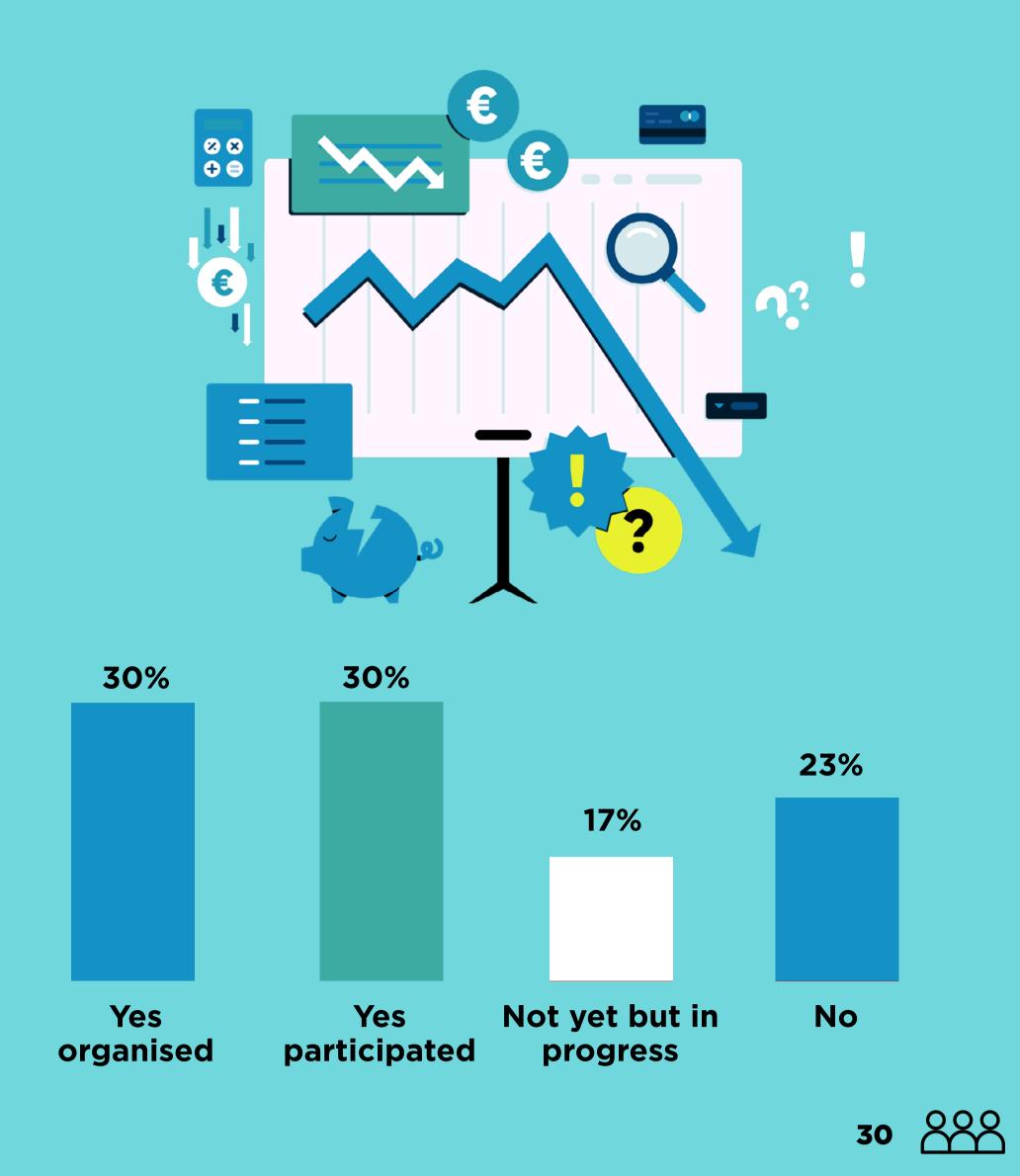
Yes specific procedures



No 33

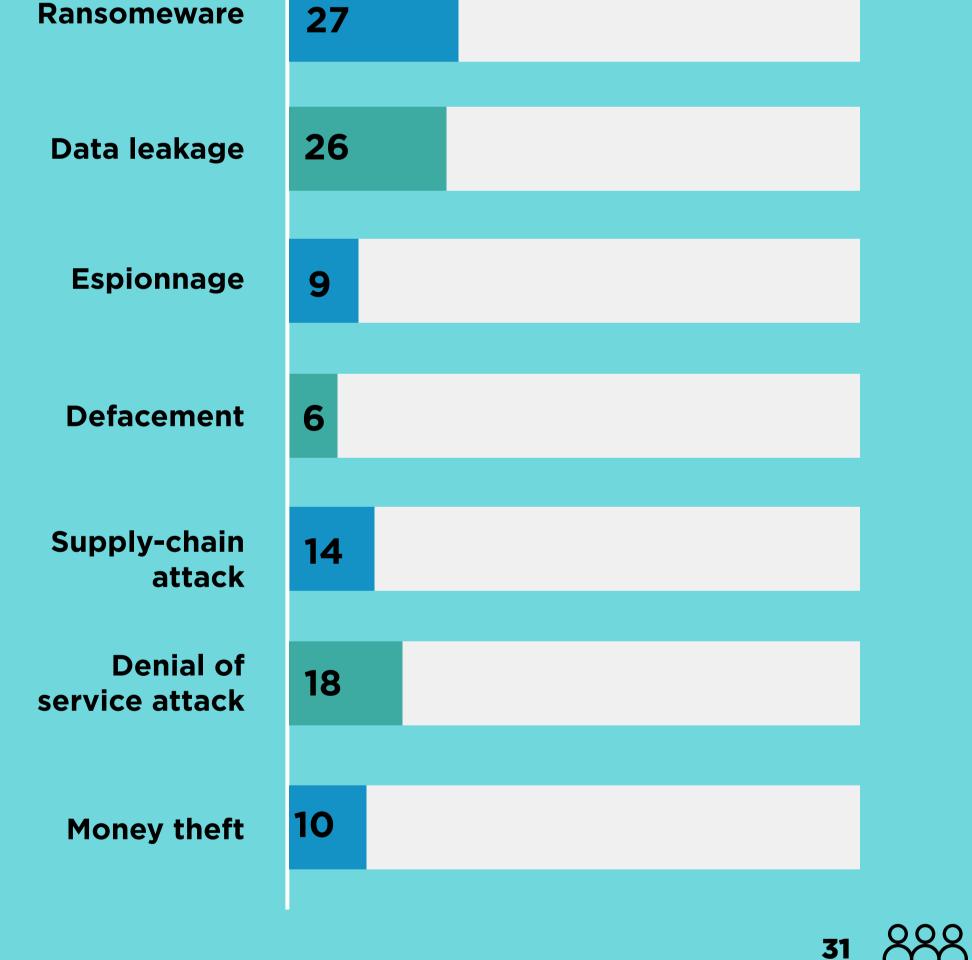
6

HAS YOUR INSTITUTION ALREADY **ORGANISED OR PARTICIPED TO CYBER CRISIS MANAGEMENT EXERCICES?**

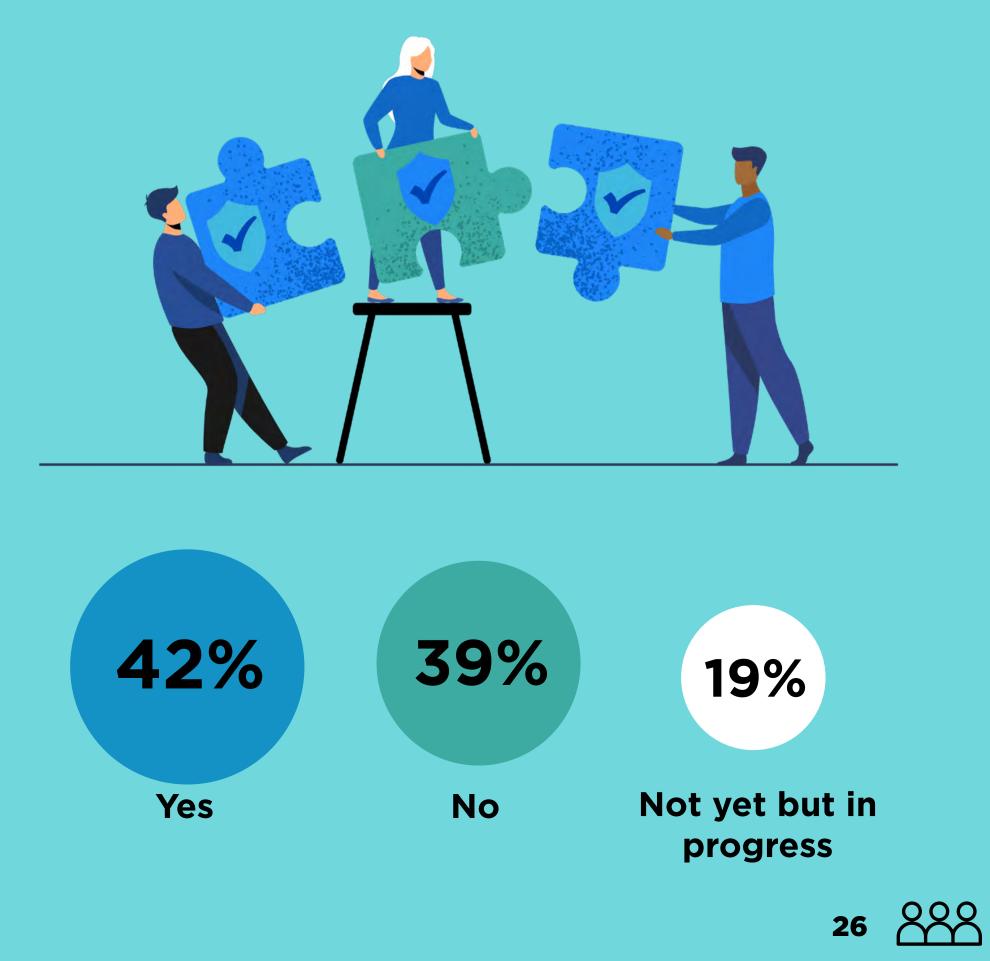


ACCORDING TO YOU, THE MAJOR CYBER THREATS ARE (MULTIPLE CHOICE POSSIBLE)

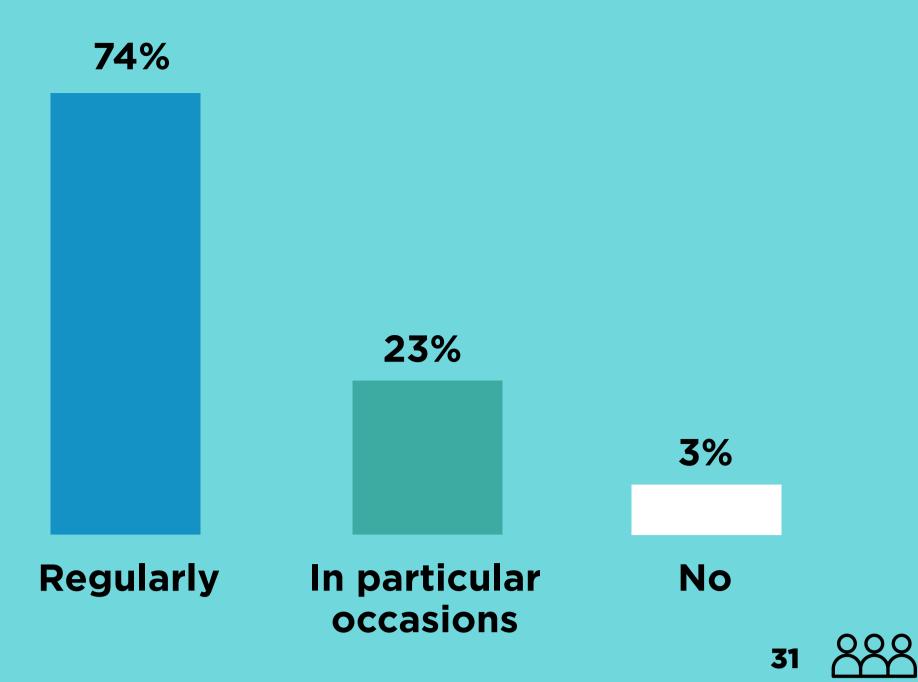




DO YOU SHARE WITH OTHER CENTRAL BANKS OR INSTITUTIONS FEEDBACK AND/OR CYBER-RESILIENCE TESTS (ROBUTNESS GROUP)?



DOES YOUR INSTITUTION RAISE AWARENESS OF GOOD CYBERSECURITY PRACTICES AMONG ITS EMPLOYEES?



HOW OFTEN DO YOU CONDUCT HIGH LEVEL (EXECUTIVE COMMITTEE INCLUDING GOVERNOR) CRISIS SIMULATION EXERCICES?

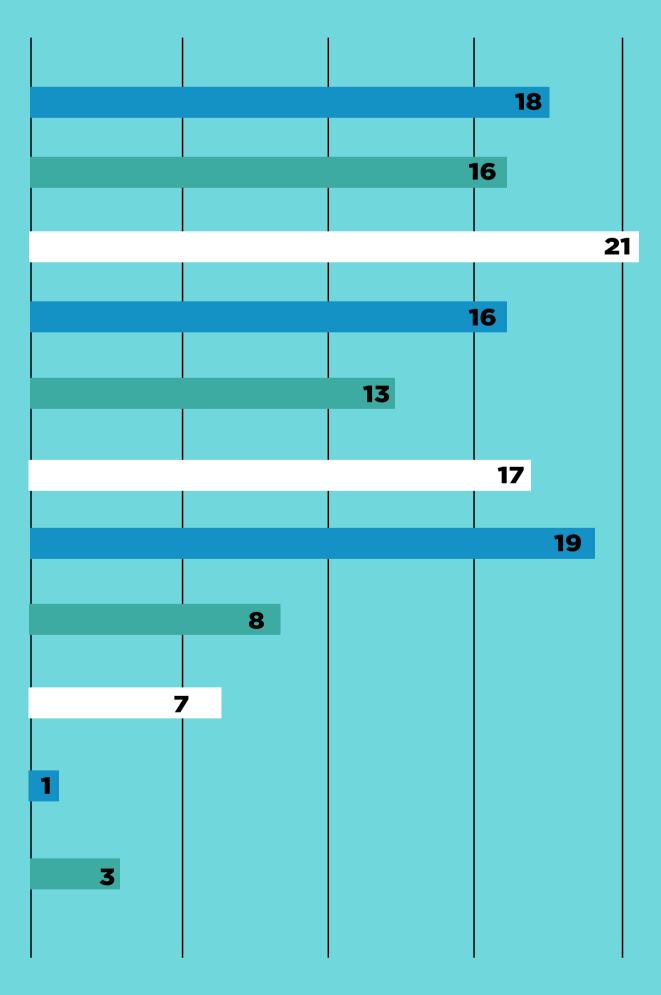


None

30

WHAT ARE YOUR MAIN PROJECTS **IN TERMS OF CYBERSECURITY?** (MULTIPLE CHOICE POSSIBLE)

once a year



VULNERABILITY / PATCH MANAGEMENT

Once a year

or more

USER AWARENESS PROGRAM

DATA LOSS PREVENTION

IDENTITY AND ACCESS MANAGEMENT

CLOUD SECURITY

END POINT DETECTION AND RESPONSE

PRIVILEGED ACCOUNT MANAGEMENT

ACTIVE DIRECTORY SECURITY

ZERO TRUST

AGILE METHODOLOGY (DEVSECOPS)

OTHER

32

DATA CONTAINED IN THIS DOCUMENT ARE CALCULATED FROM PARTICIPANTS' **RESPONSES TO A QUESTIONNAIRE CIRCULATED PRIOR TO THE CONFERENCE.** NO ATTEMPT HAS BEEN MADE TO VERIFY ACCURACY. DEFINITIONS AND METHODOLOGIES DIFFER ACROSS JURISDICTIONS.



