

Report on the Risk Assessment Tool - Short Survey



General Information about the Questionnaire

This report provides information obtained through a questionnaire on Cyber-risk self-assessment. The survey is available on the cybersecurity observatory website ¹.

The main goal of the survey is to provide a simple and quick tool for cyber risk self-assessment. The tool requires two types of input: information about security measures and information about key assets of the enterprise. When all inputs are provided, the tool estimates the expected annual losses for every relevant threat and a total one. The survey has 34 multiple choice questions, divided into 7 categories. For each question, we report the distribution of answers among all the possible choices.

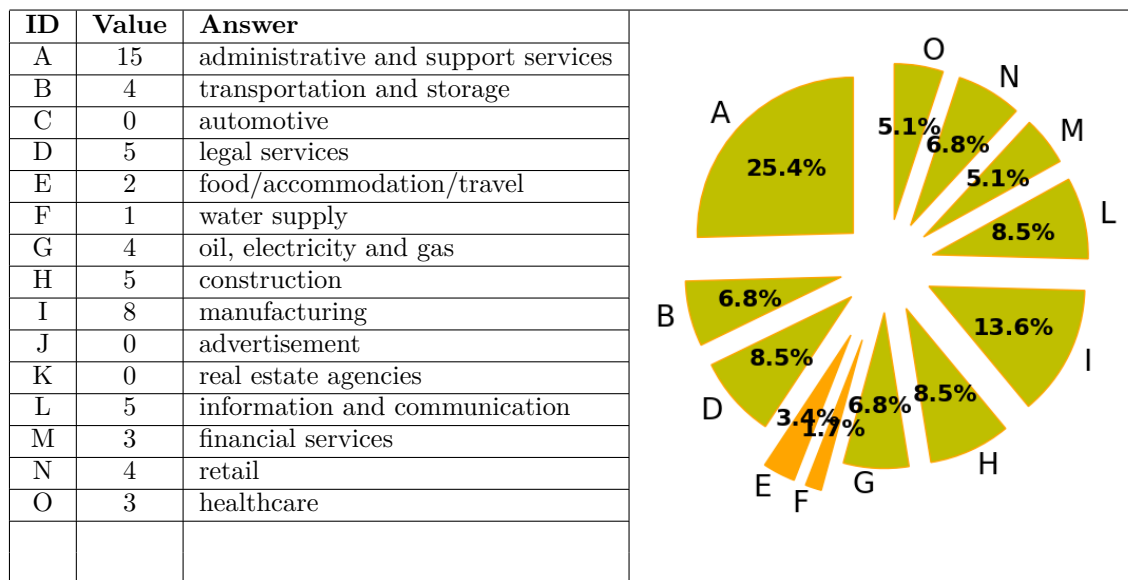
In numbers, the data collected in this report comes from:

Number of Participants: 59

Data collected between: 08/07/2019 and 19/11/2019

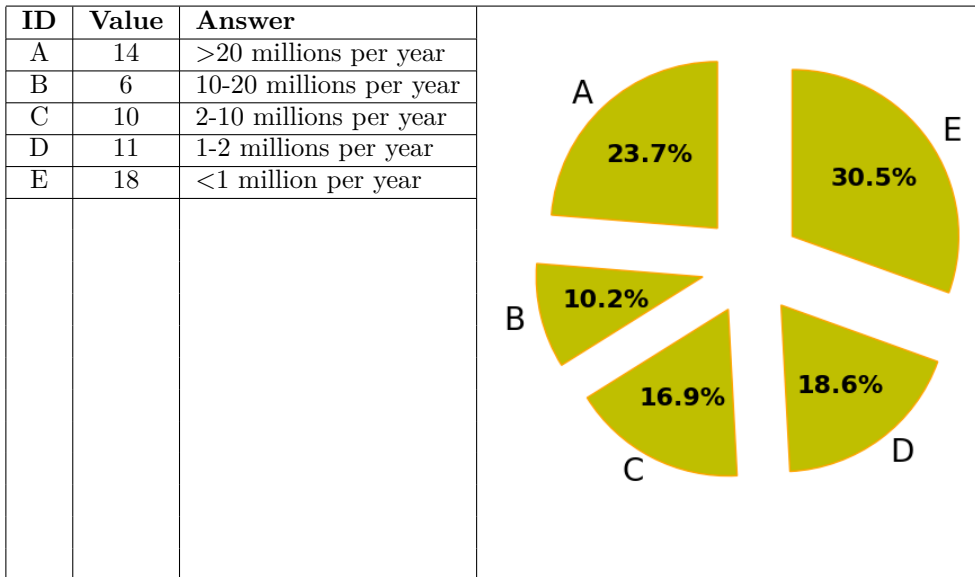
1 The Organizations

Sector:

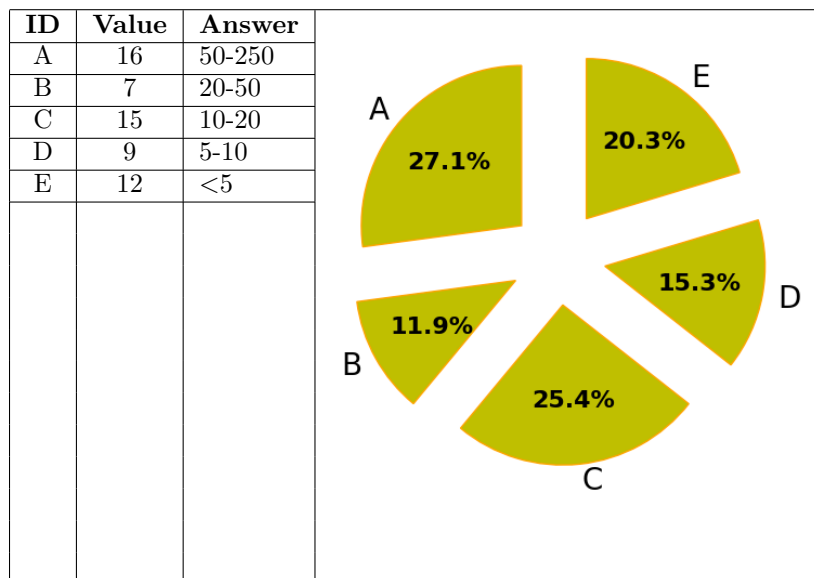


¹<https://www.cybersecurityosservatorio.it/Services/survey.jsp>

Turnover:

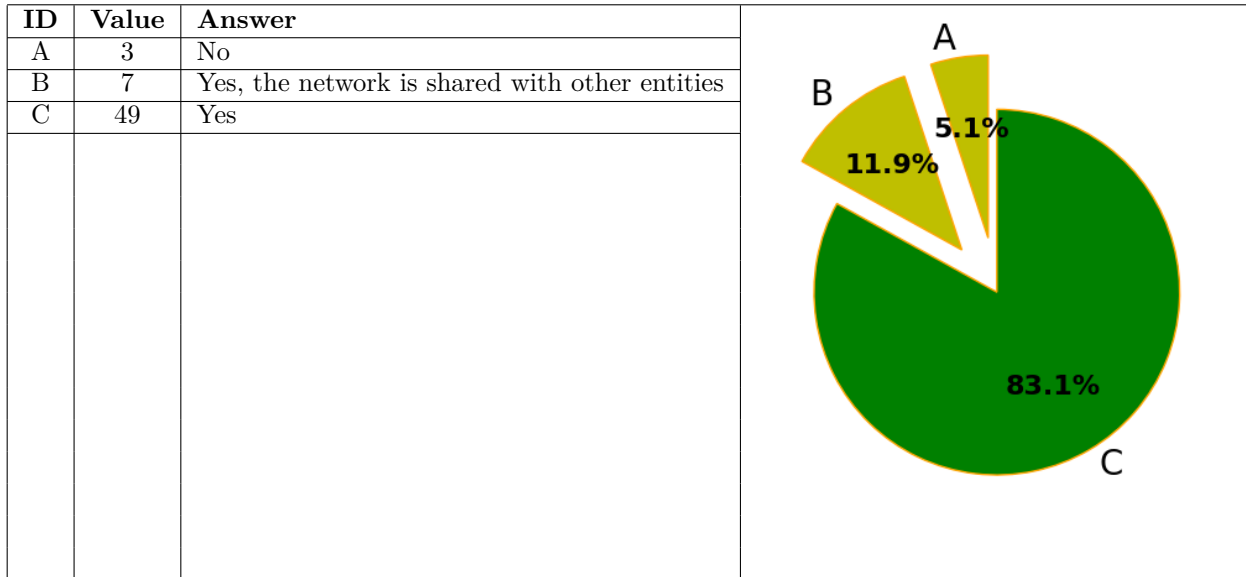


Amount of employees:

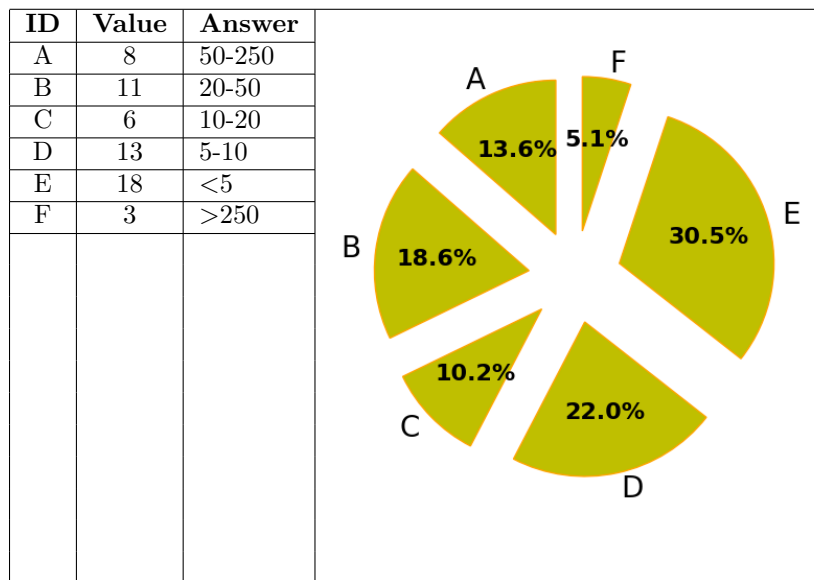


2 The Networks

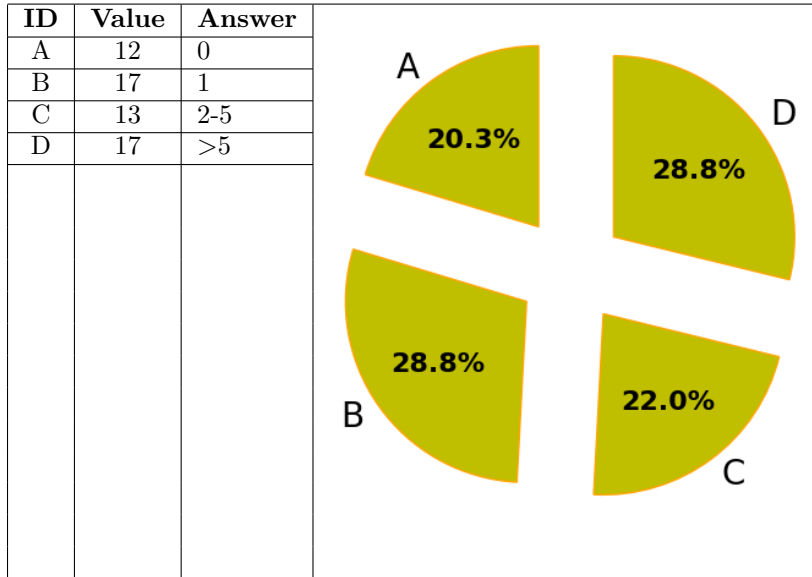
Does the organization has its own IT network:



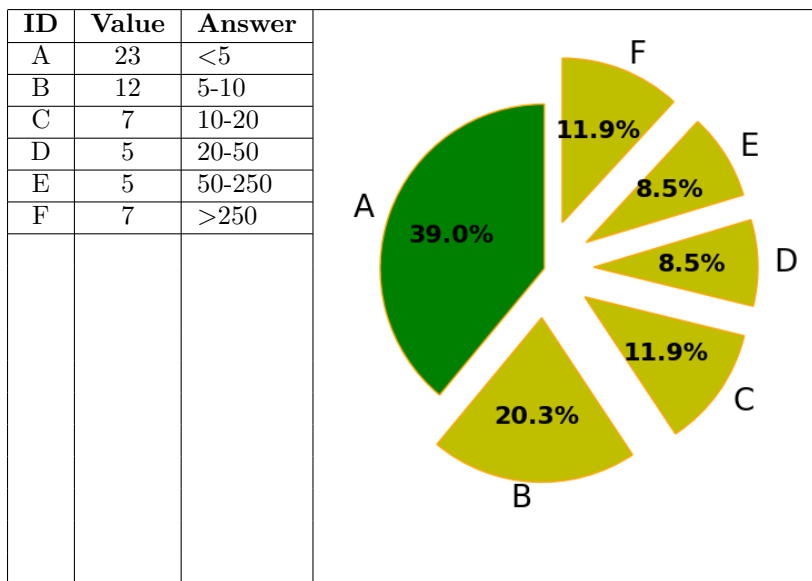
Computers/workstations:



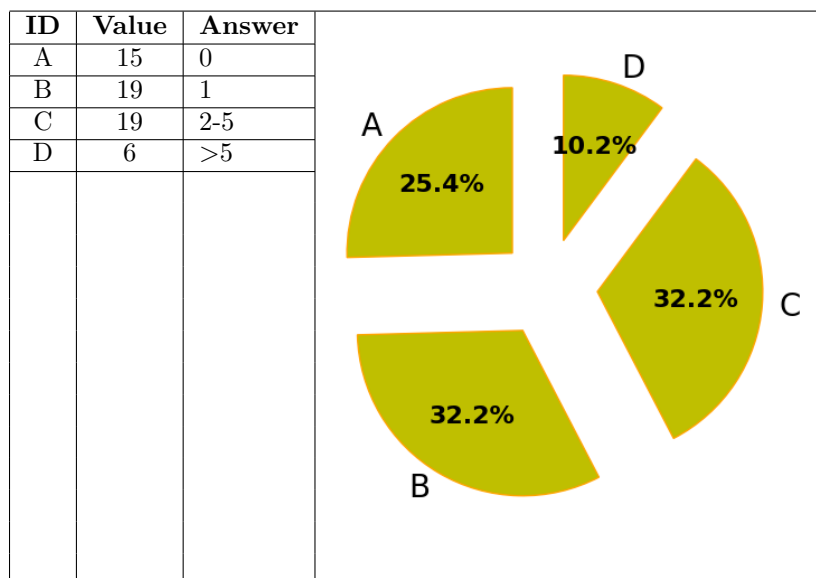
Servers:



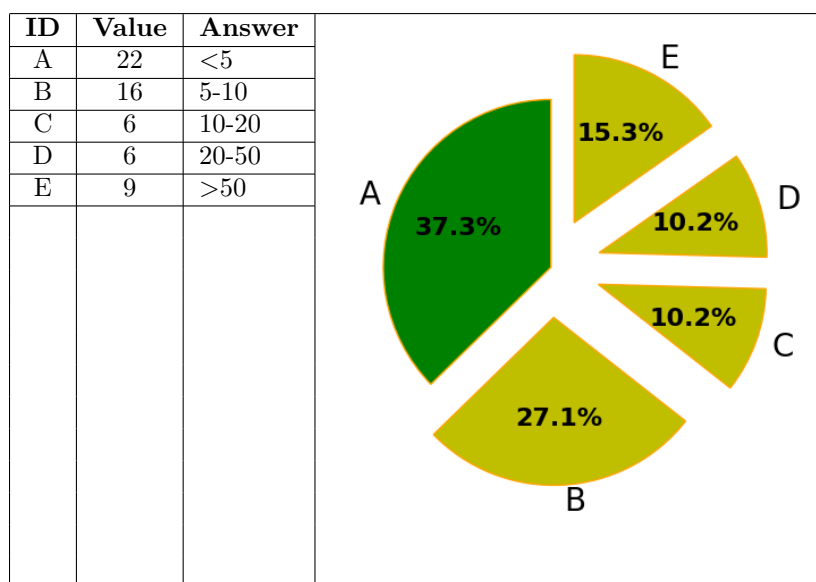
Mobile devices (smartphones, laptops, tablets, etc.):



Cloud services:

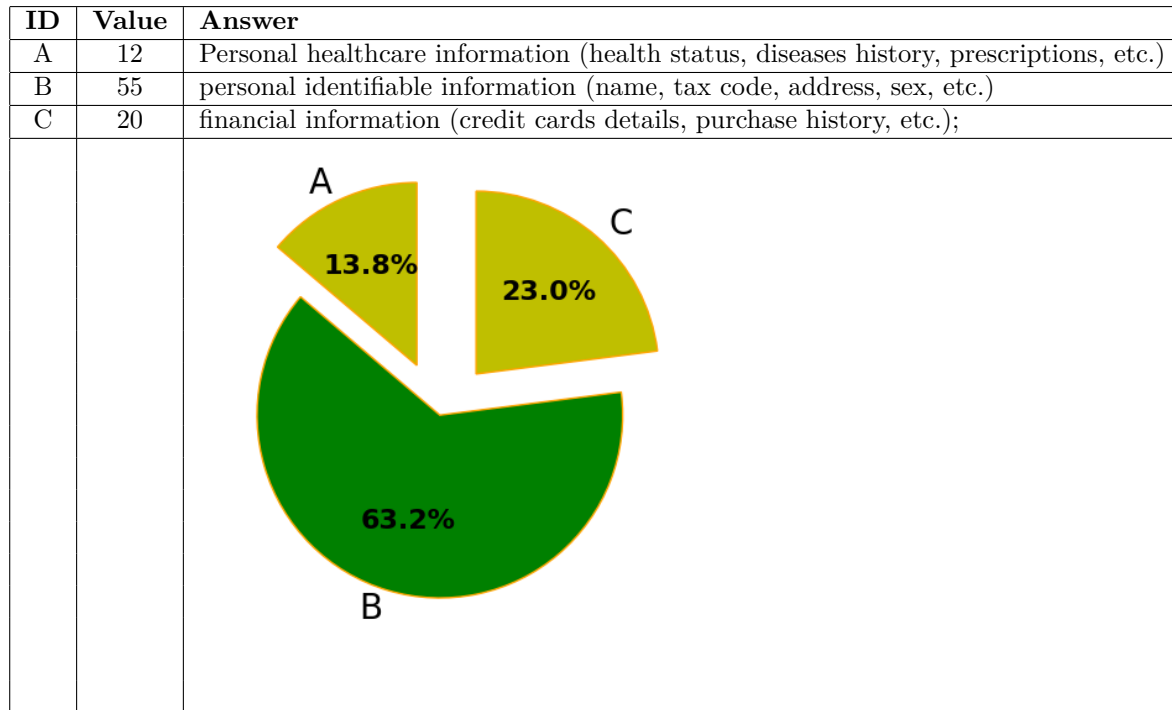


Special electronic devices (connected to the network):

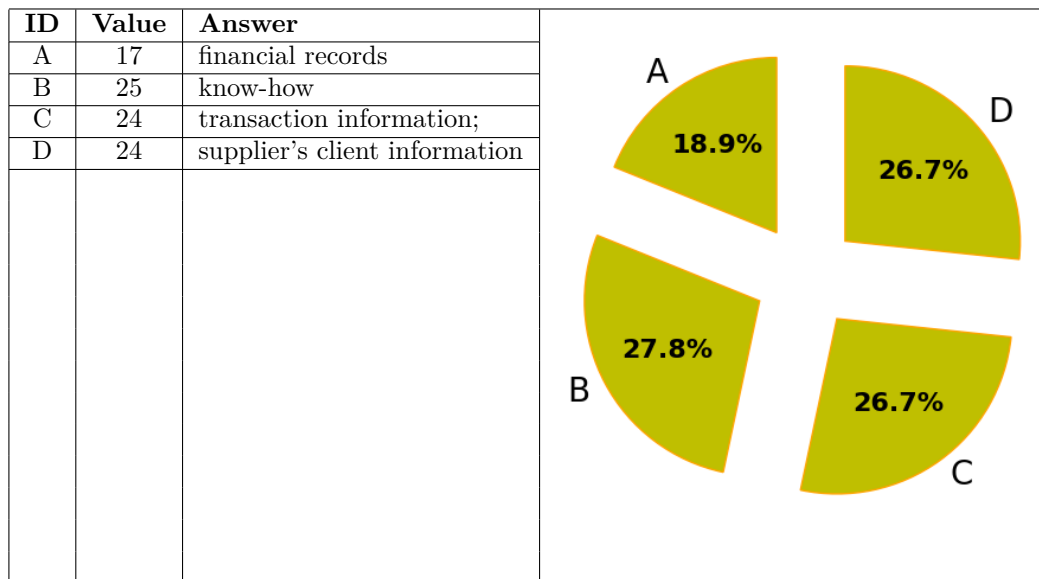


3 The Assets

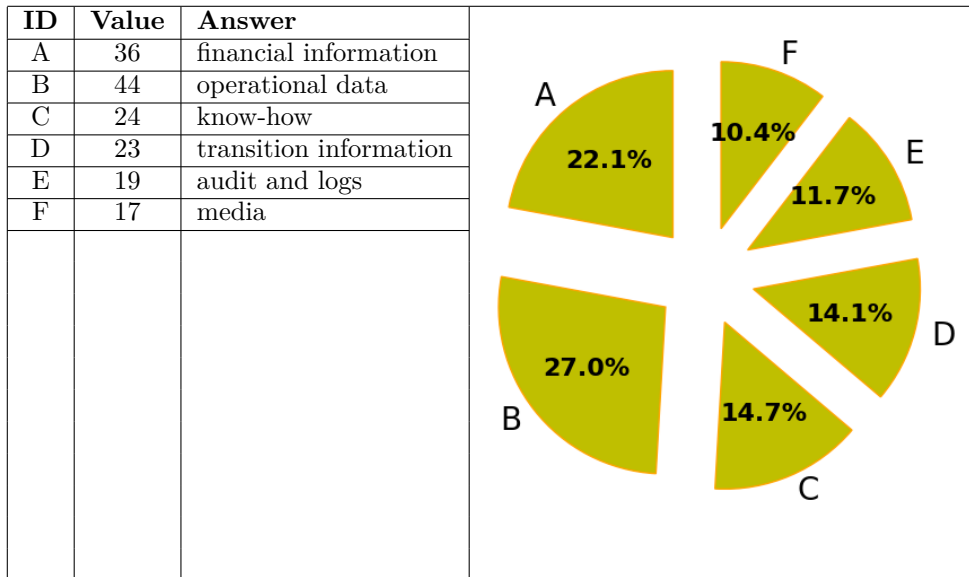
Client's info:



Supplier info:

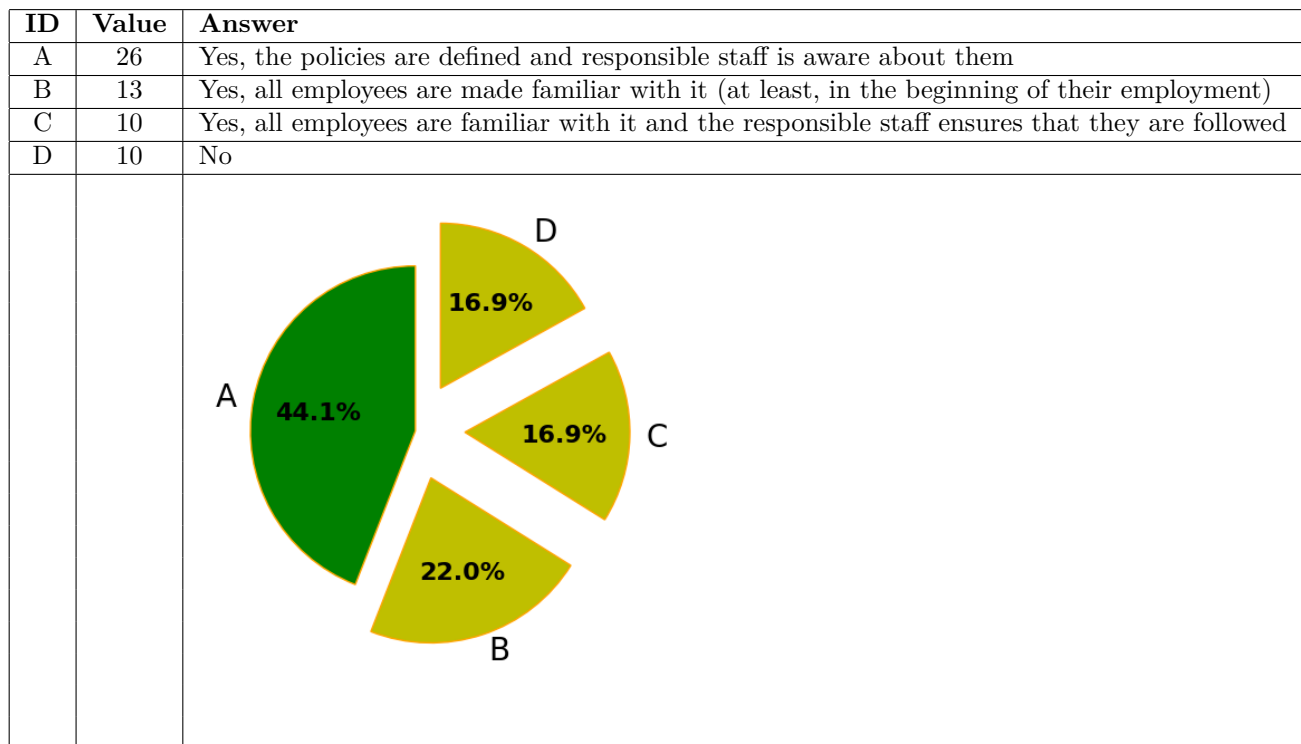


Data of the organisation:

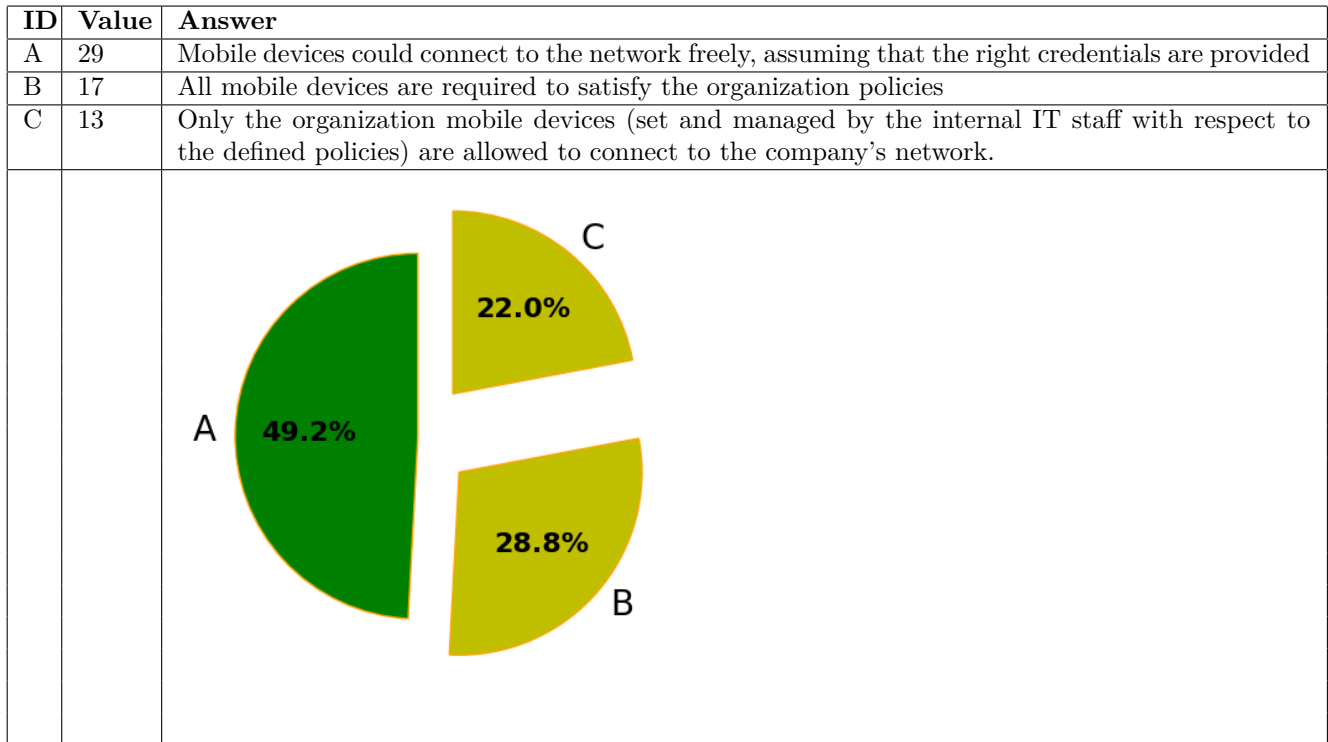


4 Cyber Protection - Management

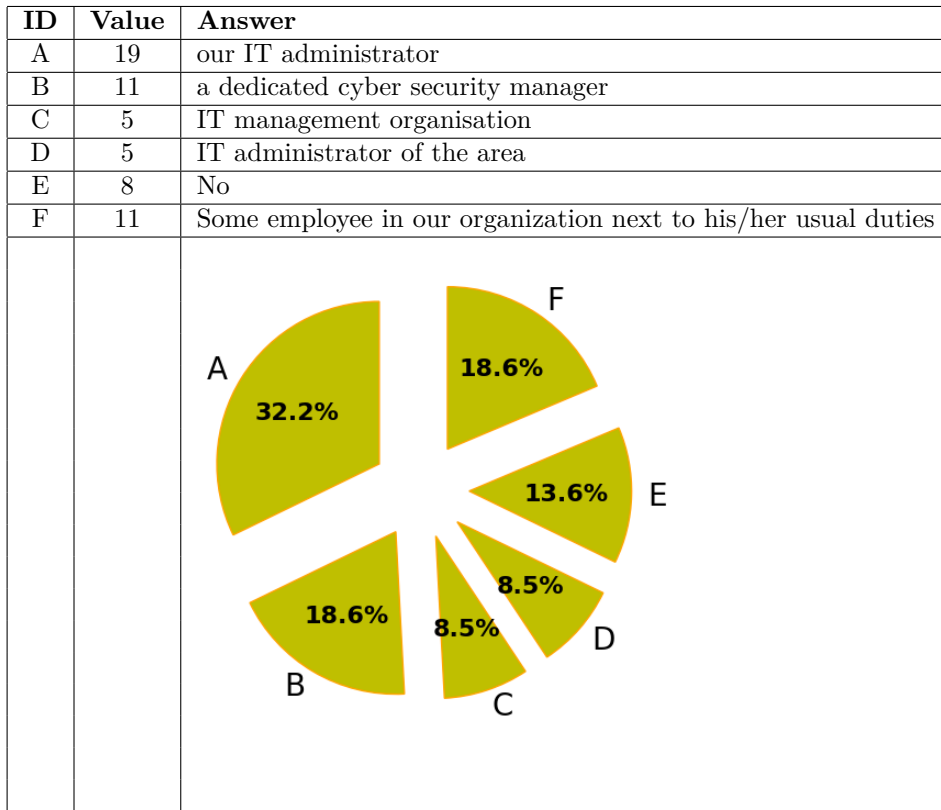
Does the organisation have formally defined security policies:



Mobile device policies (assuming, that the previous answer is YES)

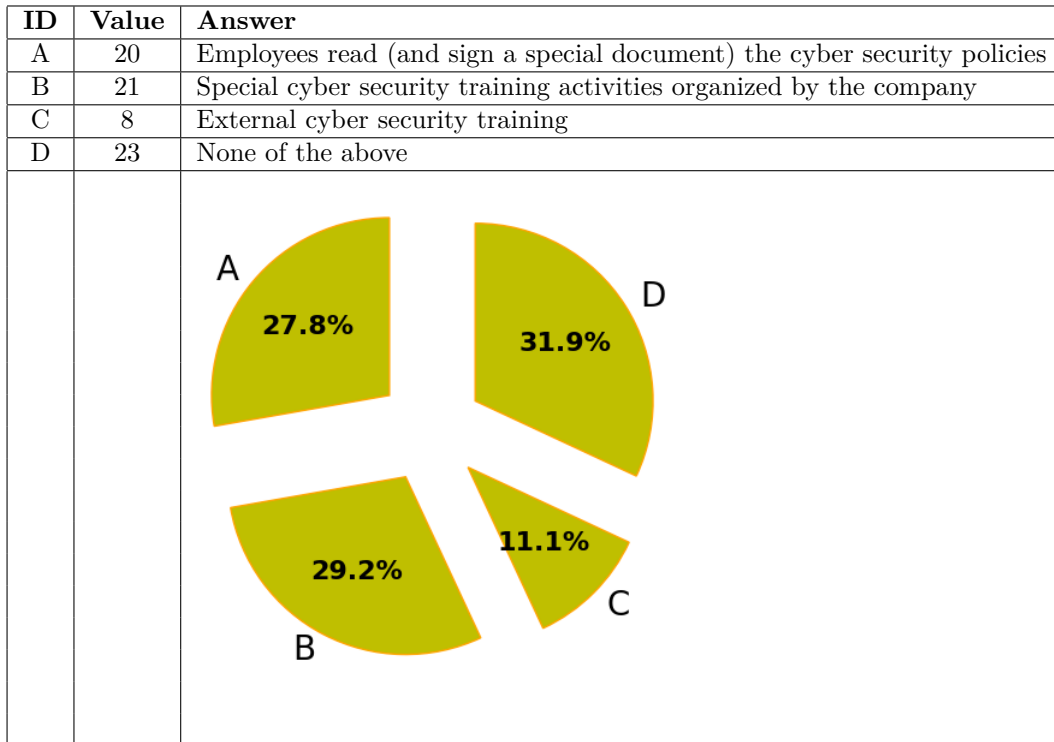


Does your organization has a person officially responsible for cyber security
(the one reporting to the board/owner, distributing cyber security budget,
setting up the strategic goals and defining security policies, etc.)

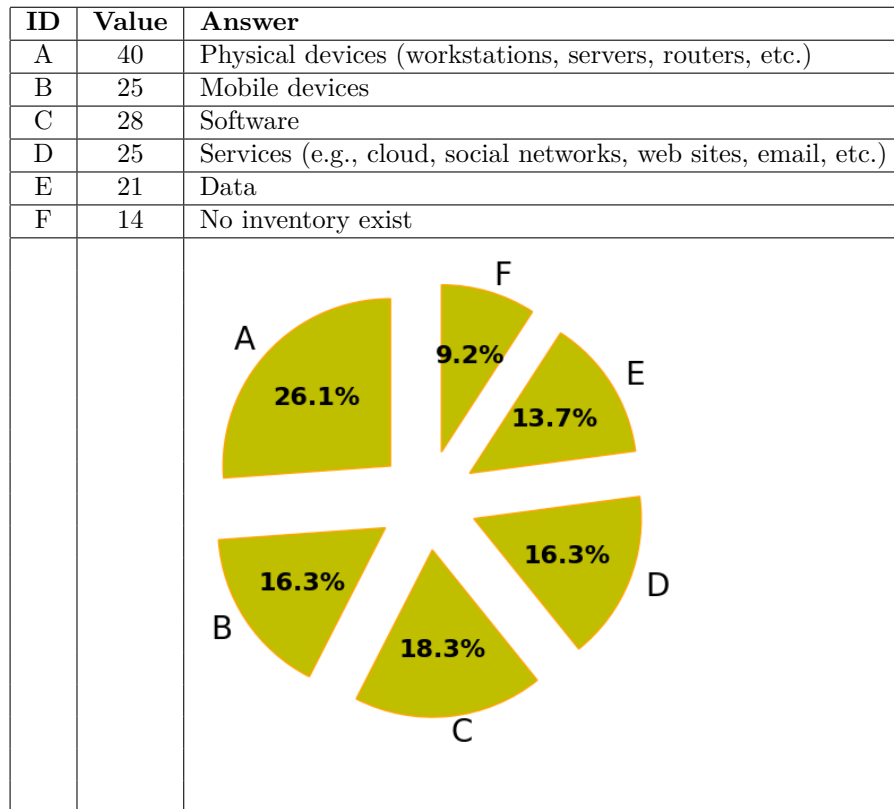


5 Cyber Protection - Non technical questions

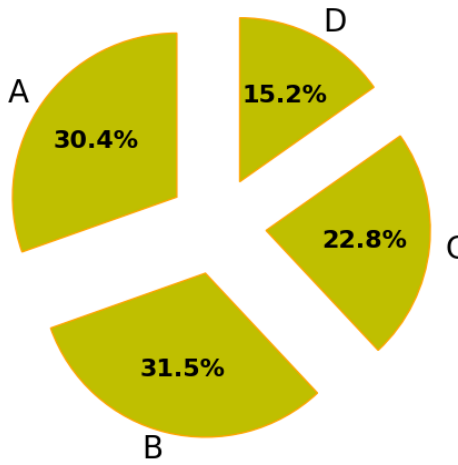
What is the level of cyber security awareness in your organization about employees:



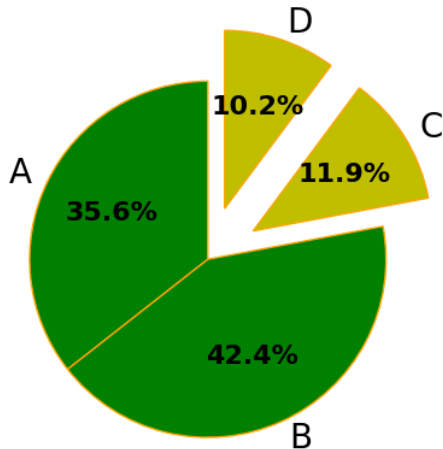
Which asset are included into a maintained inventory: (multiple choices, check boxes)



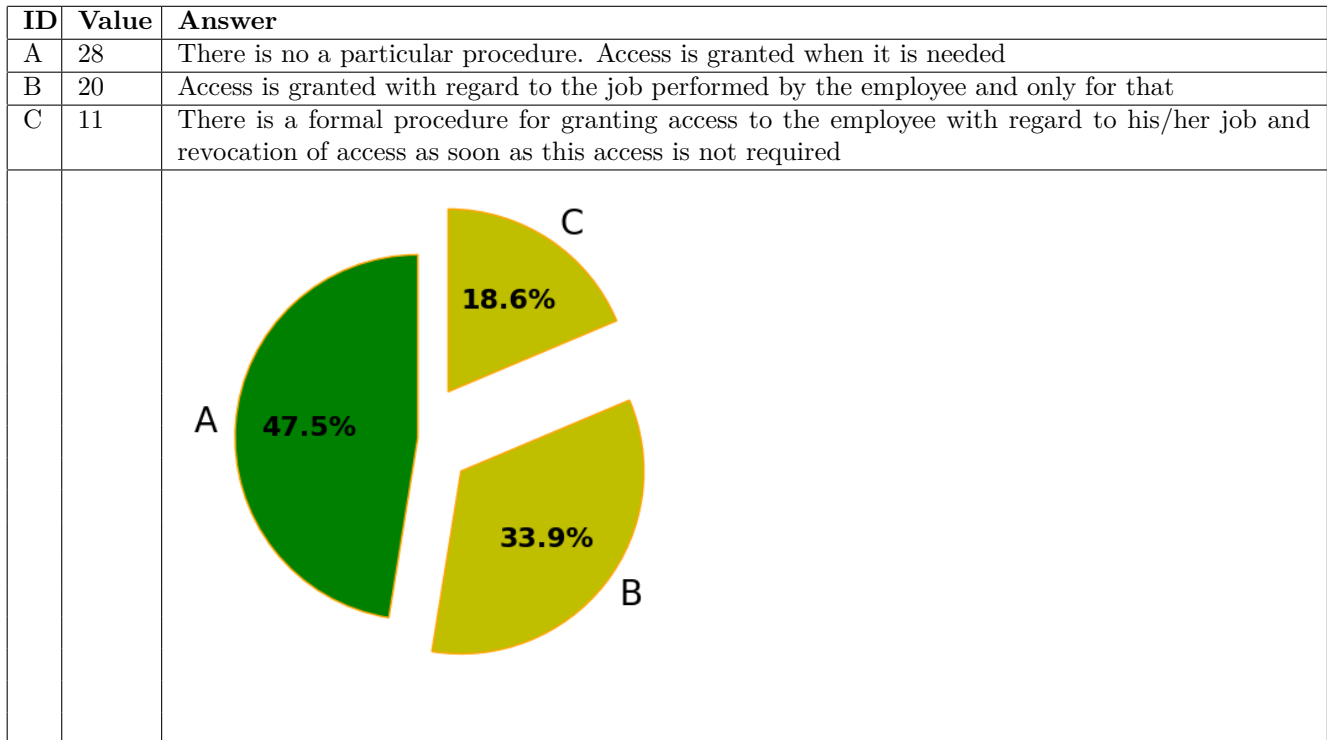
**How is physical access to organization premises protected and controlled
(multiple choice):**

ID	Value	Answer										
A	28	Perimeter. Access to the area is guarded by receptionist and all entries and exits of the external personal is recorded										
B	29	Offices. Access to the main offices is strictly forbidden for external visitors and the offices are locked if no one of the personal is inside										
C	21	Server room is locked and only responsible staff has access to it										
D	14	Access of external visitors is not monitored										
		 <p>A pie chart illustrating the distribution of responses for the question 'How is physical access to organization premises protected and controlled (multiple choice)'. The chart is divided into four segments, each representing a different answer choice. Segment A (Perimeter) accounts for 30.4% of the responses. Segment B (Offices) is the largest segment at 31.5%. Segment C (Server room) accounts for 22.8%, and Segment D (Access not monitored) is the smallest at 15.2%.</p> <table><thead><tr><th>Answer</th><th>Percentage</th></tr></thead><tbody><tr><td>A</td><td>30.4%</td></tr><tr><td>B</td><td>31.5%</td></tr><tr><td>C</td><td>22.8%</td></tr><tr><td>D</td><td>15.2%</td></tr></tbody></table>	Answer	Percentage	A	30.4%	B	31.5%	C	22.8%	D	15.2%
Answer	Percentage											
A	30.4%											
B	31.5%											
C	22.8%											
D	15.2%											

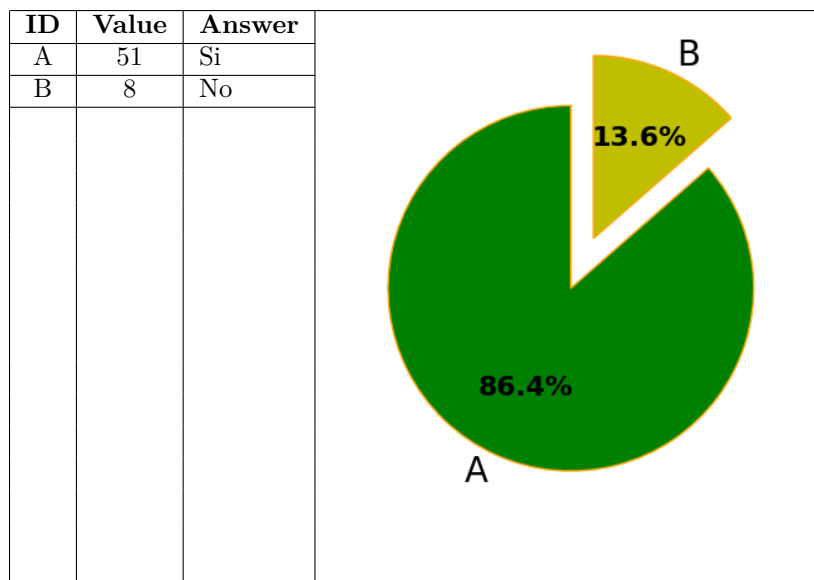
What kind of policies are enforcement with respect to credentials:

ID	Value	Answer												
A	21	Passwords are allowed to be selected by the employees, without any further check of password strength												
B	25	Passwords are allowed to be selected by the employees, but checked and forced to satisfy internal requirements												
C	7	Passwords are issued by the password management personal/software only												
D	6	Multi-factor authorization is enforced												
E	0	Other methods for authentication, than simple login-password pair, are in use (like, smart cards, biometrics, etc.)												
		 <p>A pie chart illustrating the distribution of policy enforcement across five categories (A, B, C, D, E). The chart is divided into five segments: A (35.6%, green), B (42.4%, green), C (11.9%, yellow), D (10.2%, yellow), and E (0%, not visible). The segments are labeled with their respective letters and percentages.</p> <table><thead><tr><th>Category</th><th>Percentage</th></tr></thead><tbody><tr><td>A</td><td>35.6%</td></tr><tr><td>B</td><td>42.4%</td></tr><tr><td>C</td><td>11.9%</td></tr><tr><td>D</td><td>10.2%</td></tr><tr><td>E</td><td>0%</td></tr></tbody></table>	Category	Percentage	A	35.6%	B	42.4%	C	11.9%	D	10.2%	E	0%
Category	Percentage													
A	35.6%													
B	42.4%													
C	11.9%													
D	10.2%													
E	0%													

What is the procedure for granting access to the information resources:

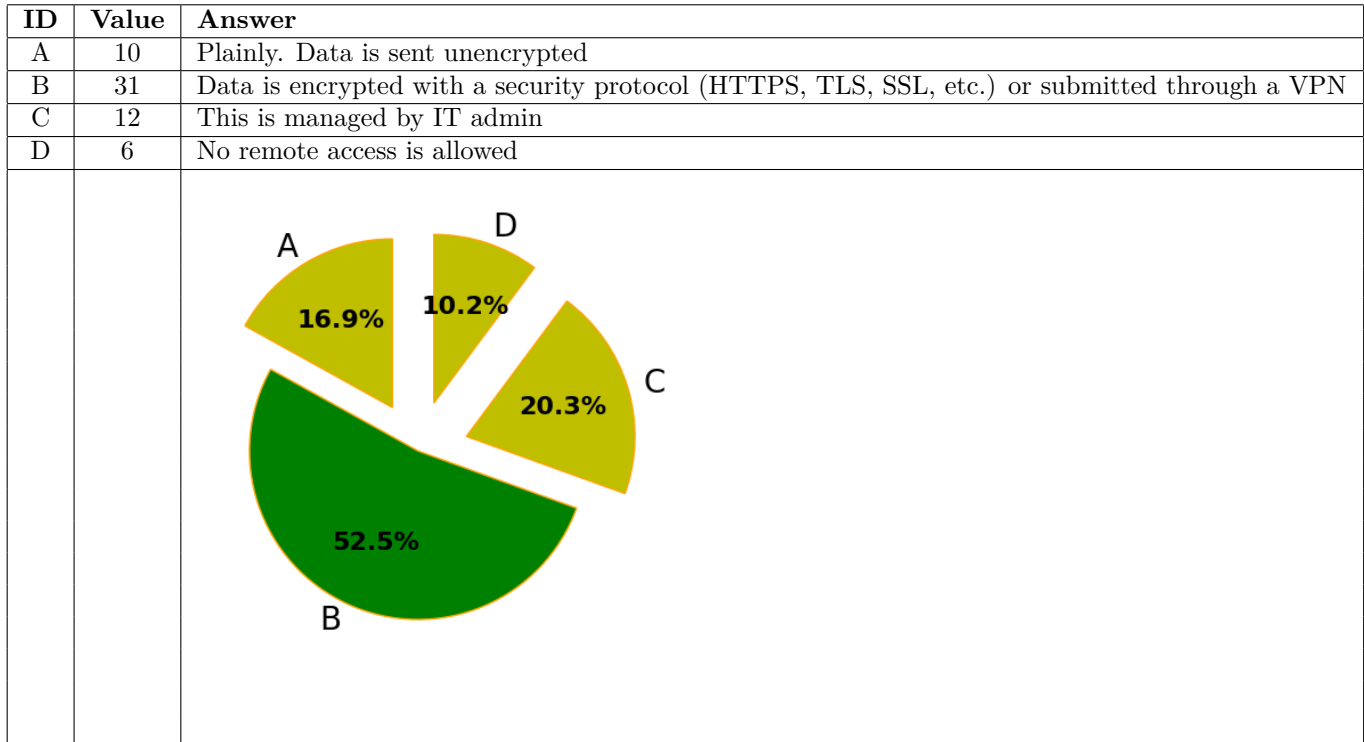


Do you have a centralised credentials management system:

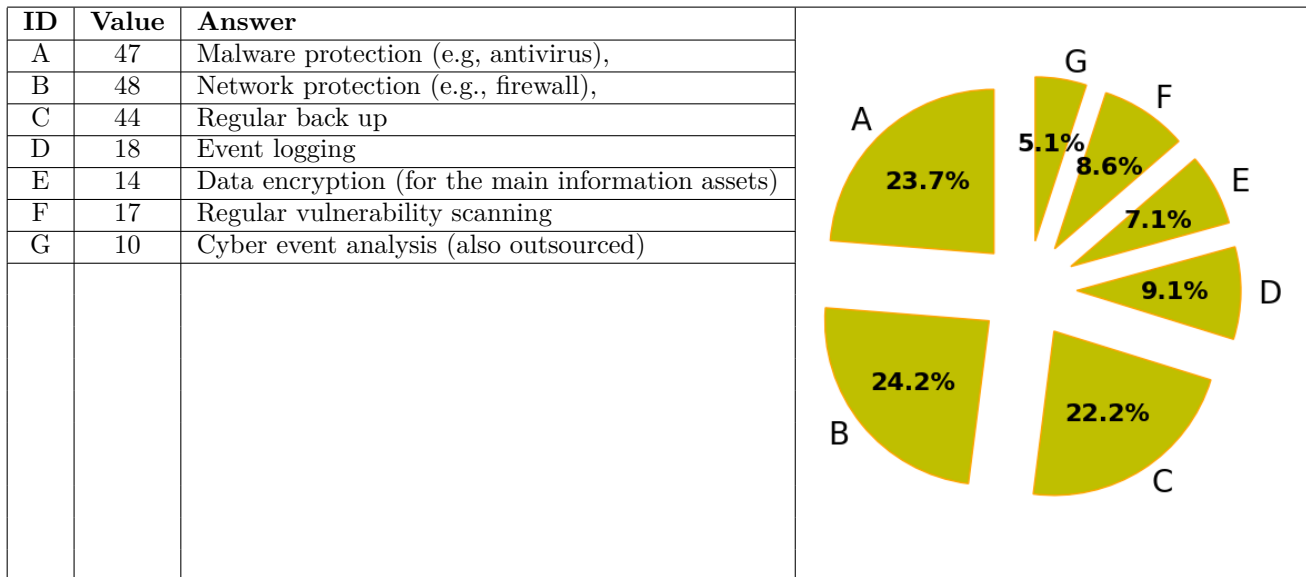


6 Cyber Protection - Technical questions

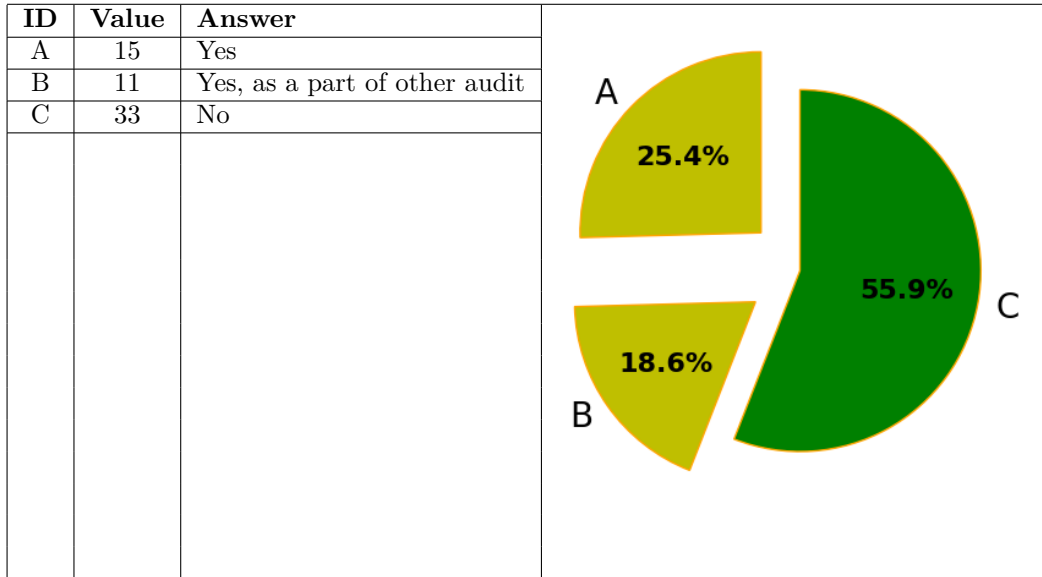
How the remote access to information assets is protected:



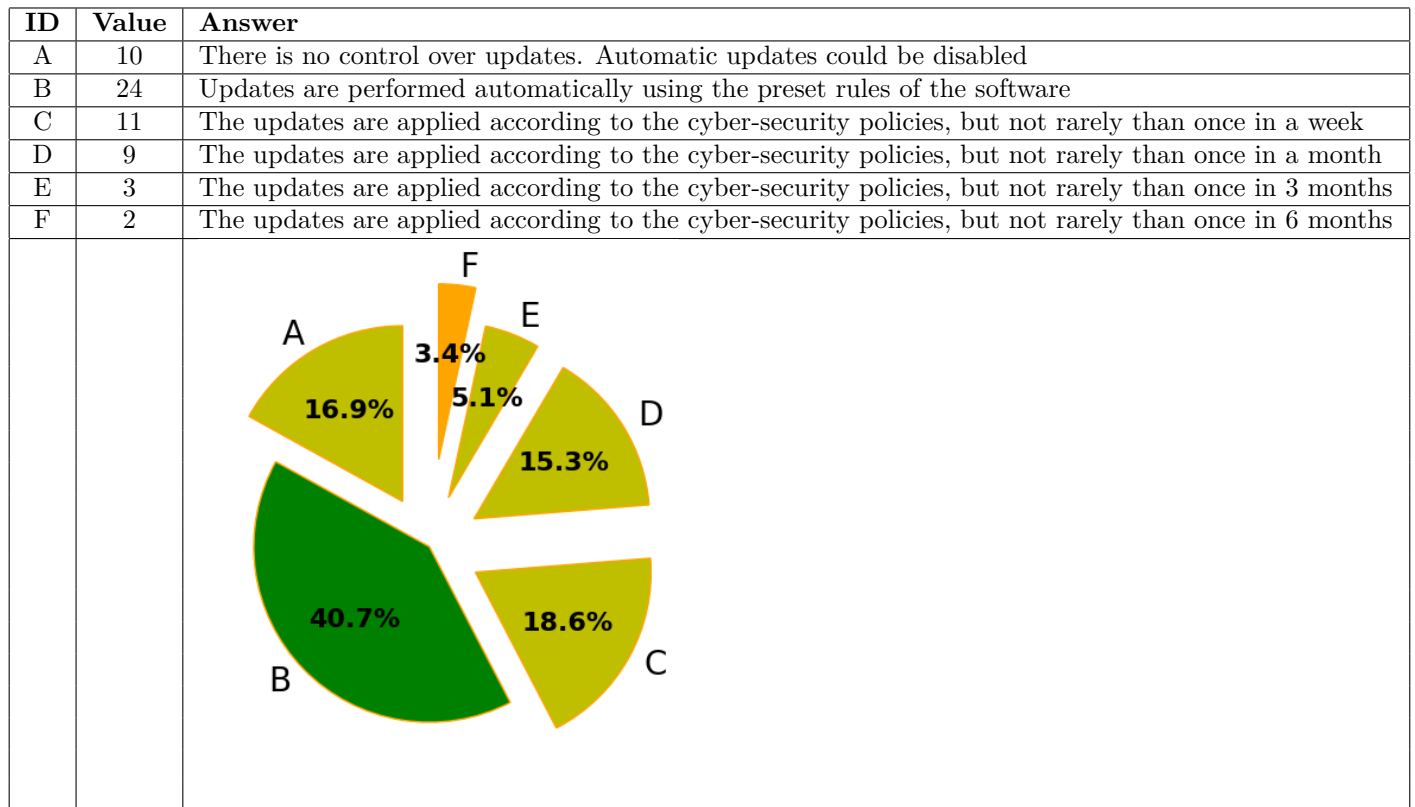
What protection mechanisms are installed:



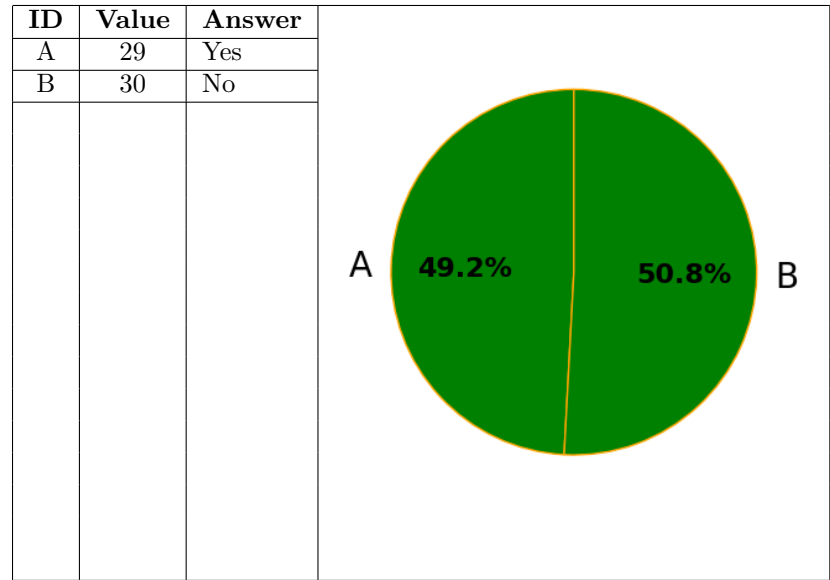
Have you ever passed a cyber security audit:



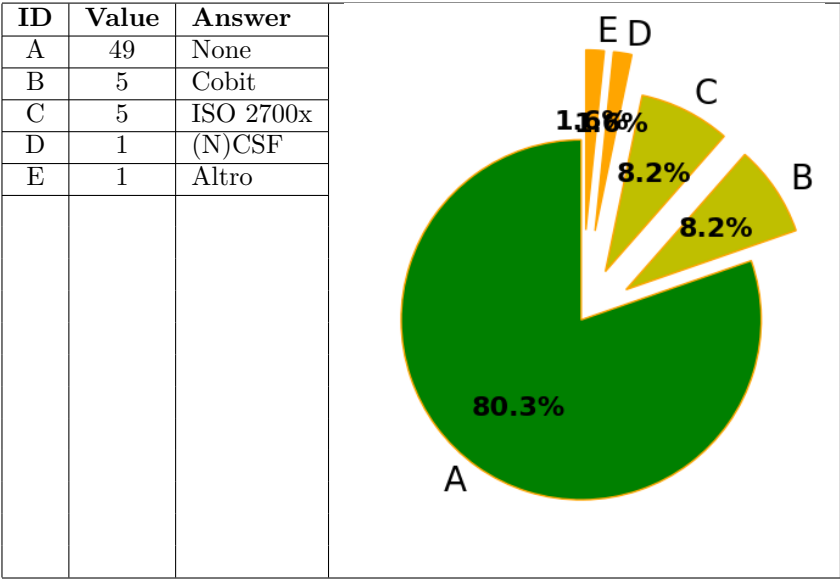
How often do you update your systems (including, operating systems, web services, browsers, database, etc.)



Does the organization have a prescribed set of actions and a list of possible contact points (e.g., cyber security experts) in case a cyber security incident occurs:

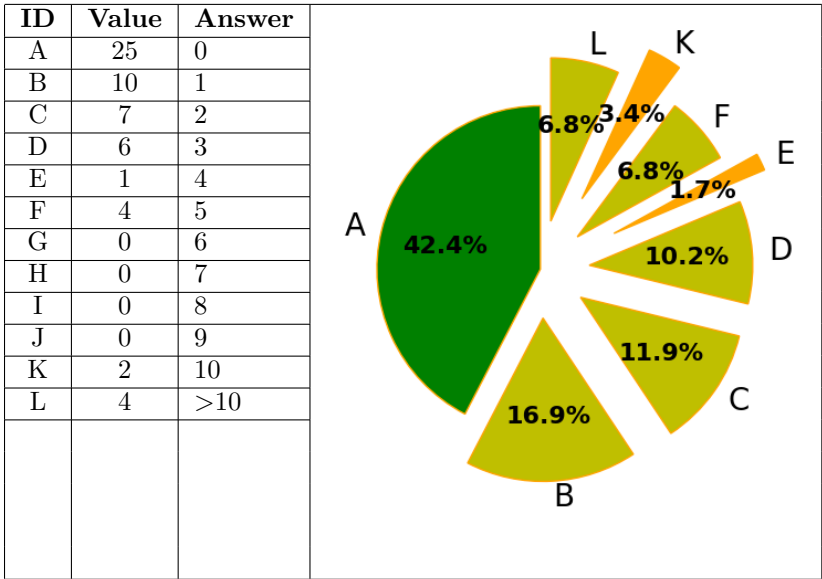


Does the organization has a cyber security certificate:

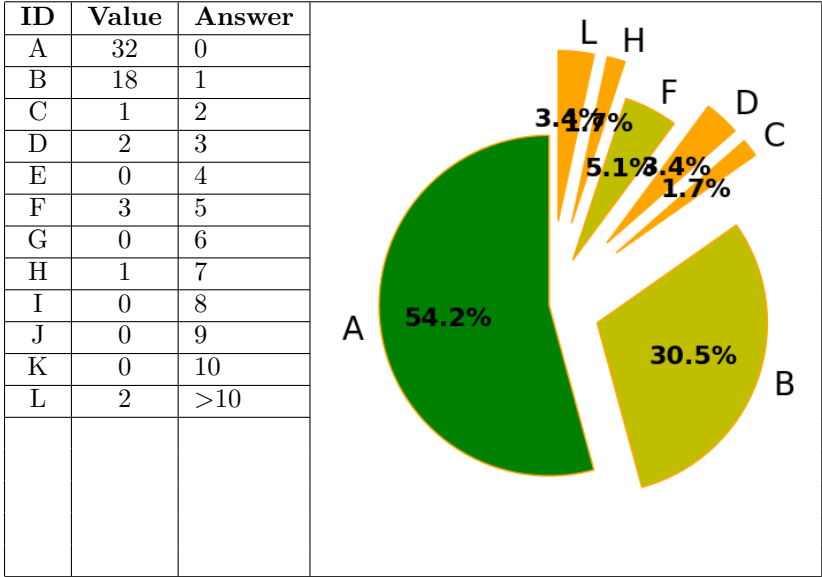


7 Which and how many cyber incidents experienced in the past 3 years

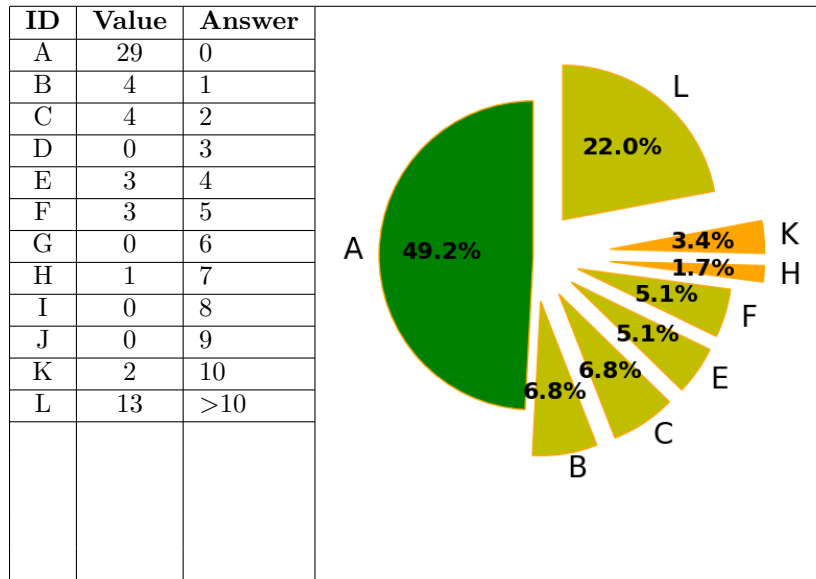
Malware / Hacker



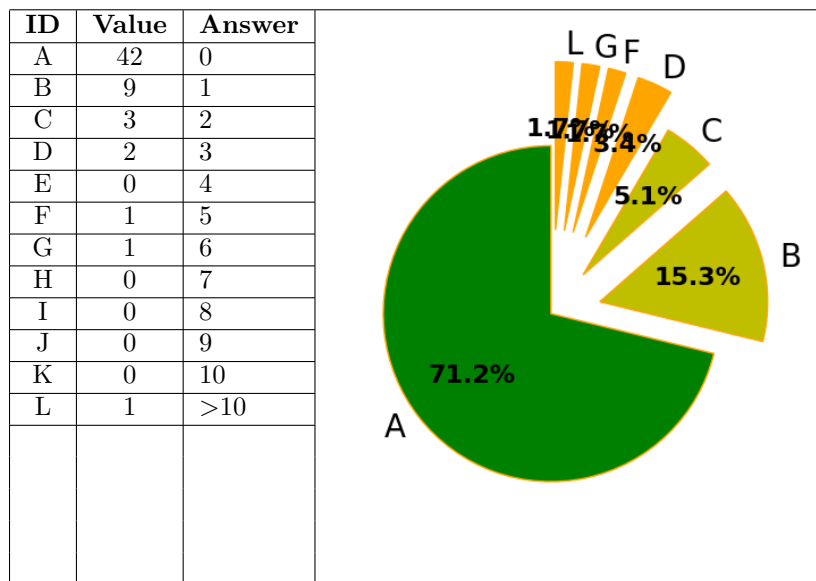
Ransomware



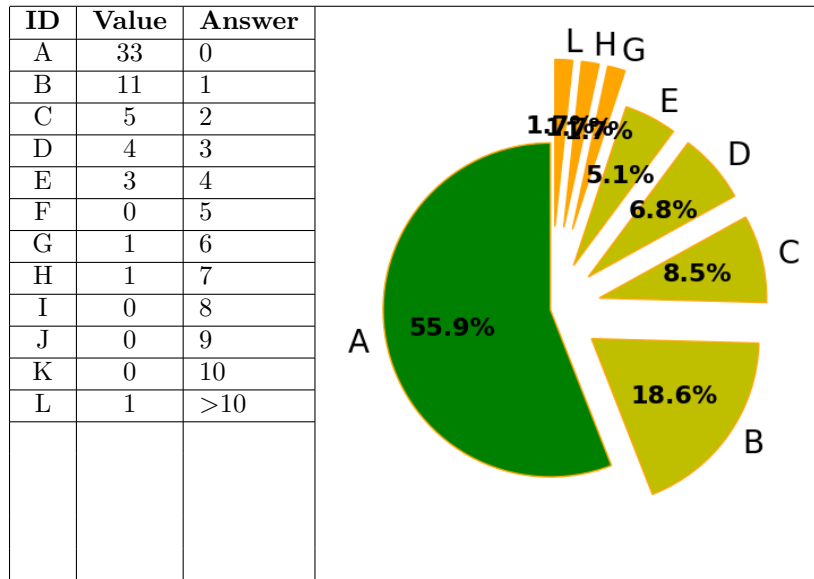
Phishing



Cyber Fraud (money stolen)



Employee misbehavior



If other, please, indicate

ID	Value	Answer
A	0	0
B	0	1
C	0	2
D	0	3
E	0	4
F	0	5
G	0	6
H	0	7
I	0	8
J	0	9
K	0	10
L	0	>10

The number of other incidents:

