The University of Hong Kong Public Opinion Programme

Microsoft Hong Kong Limited

The Hong Kong Council of Social Service

Survey on Local NGOs' Knowledge on "Cloud Solution" and Security Concerns 2012

Dr Robert T. Y. CHUNG

Director of Public Opinion Programme, HKU

May 30, 2012

Research Background

- Objective: To understand the current applications of network security in local NGOs, their views and concerns about "Cloud Solution".

- POP has consulted Microsoft and HKCSS in designing the questionnaire while POP enjoyed full autonomy in fieldwork operation, data collection and data analysis. POP takes full responsibility for all findings reported.

- The research methodology and all survey findings will be open for public consumption.

Contact Information

Date of survey: April 2 to 20, 2012

Target population: Representatives of local NGOs who are involved in decision making of IT policies, contact list was provided by HKCSS

Survey method: HKCSS invited 399 agency members to participate in this survey via email, then the contact list of 101 interested organizations was given to HKUPOP to conduct telephone interviews

Sample size: Representatives of 93 out of the 101 organizations completed the telephone interviews, the cooperation rate is 98.9%, accounting to 23.3% of the total agency members

Standard error: Assuming no response bias, at 95% confidence level, the sampling error of all percentages should be no more than +/-9.1 percentage points
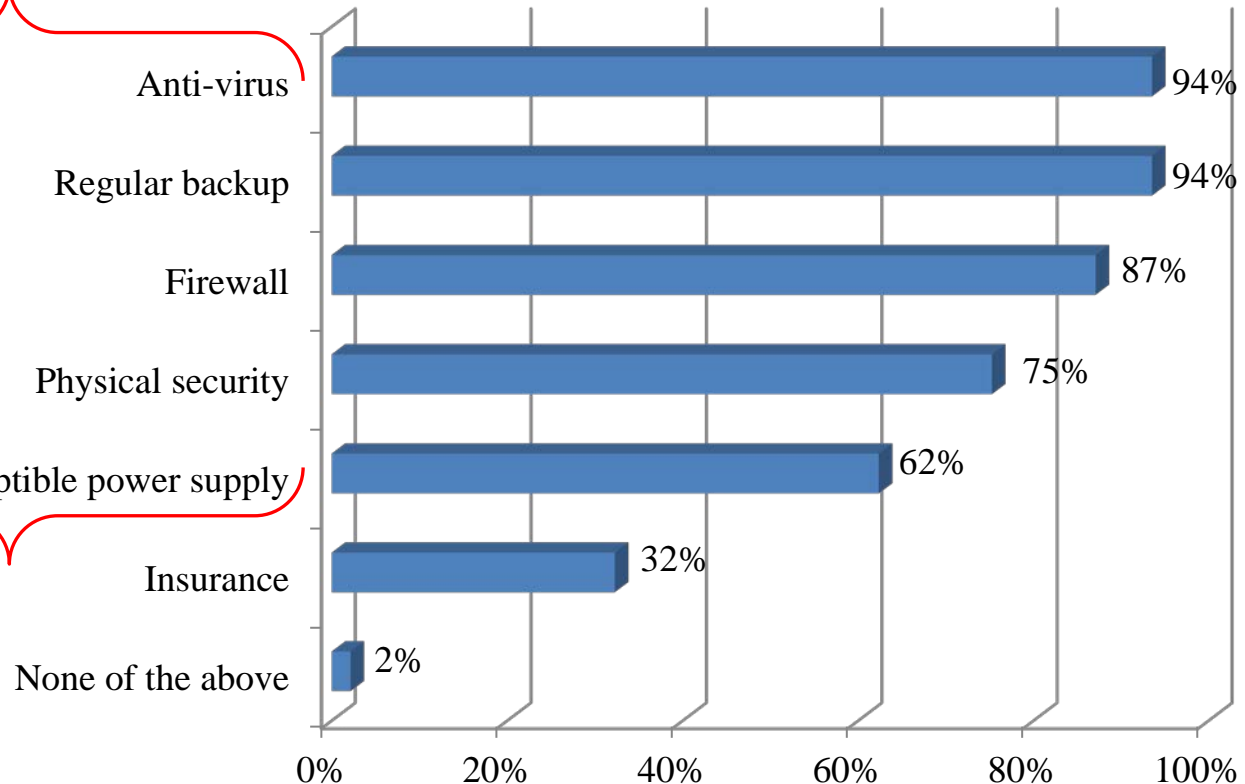
1) Network Security

Almost all organizations use "anti-virus" and "regular backup"
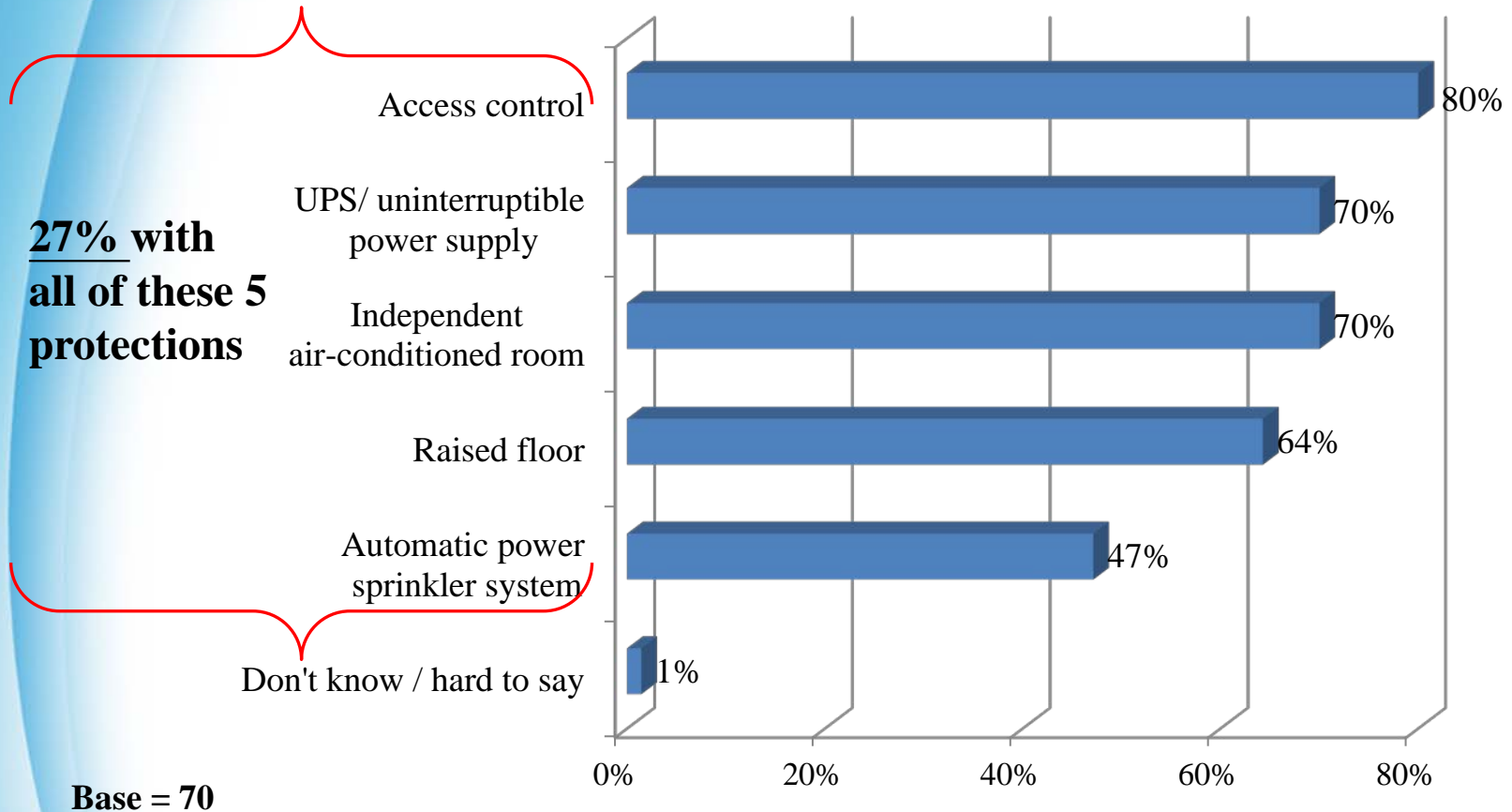
54% have all these 5 measures

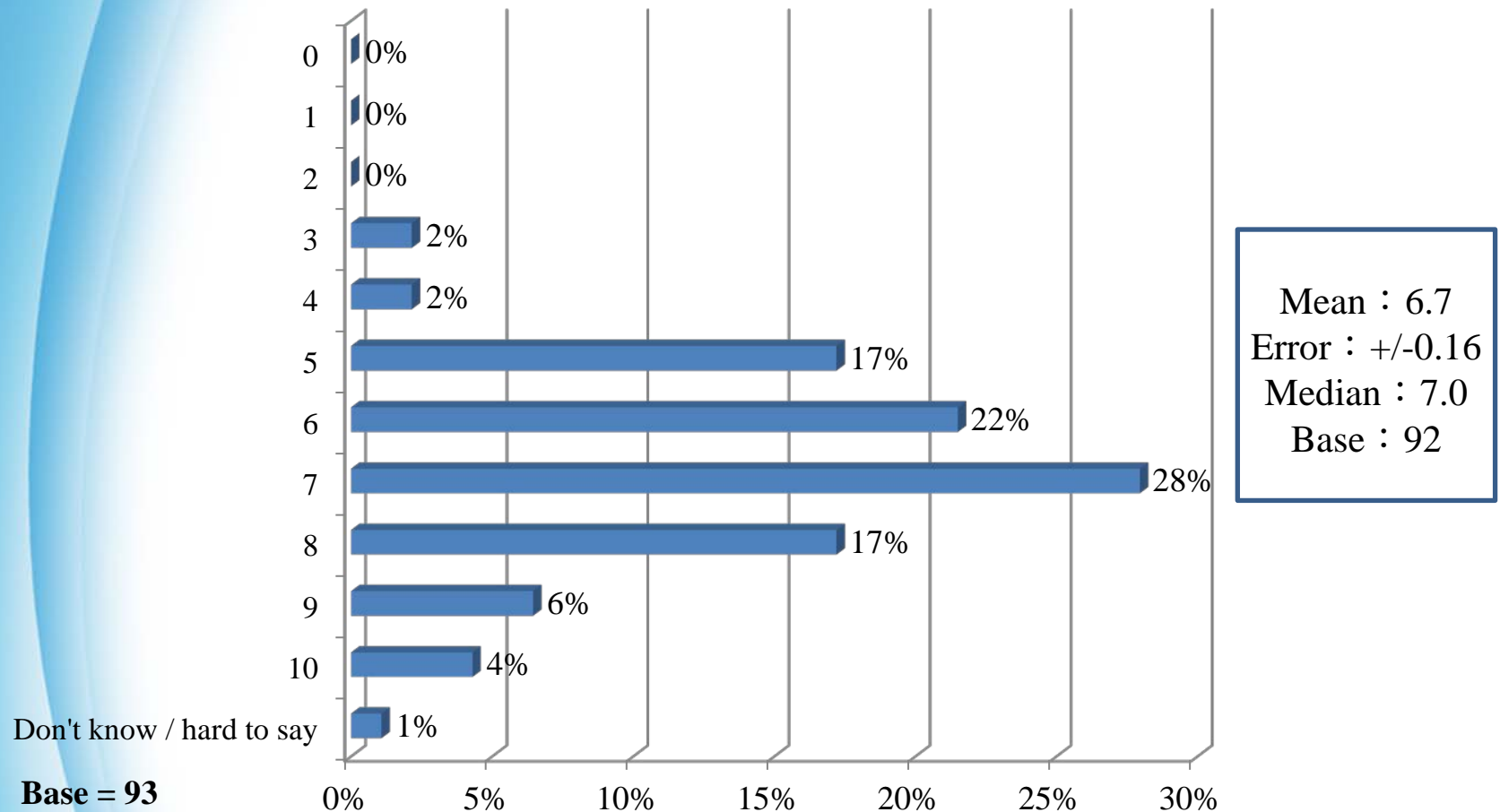| Measure	Percentage
Anti-virus	94%
Regular backup	94%
Firewall	87%
Physical security	75%
UPS / uninterruptible power supply	62%
Insurance	32%
None of the above	2%

Base = 93

[Q1] Which of the following measures does your organization have to protect the servers / application system? [Interviewer to read out items 1-6, order to be randomized, multiple responses allowed]

"Access control" is the most commonly used physical security for servers

27% with all of these 5 protections

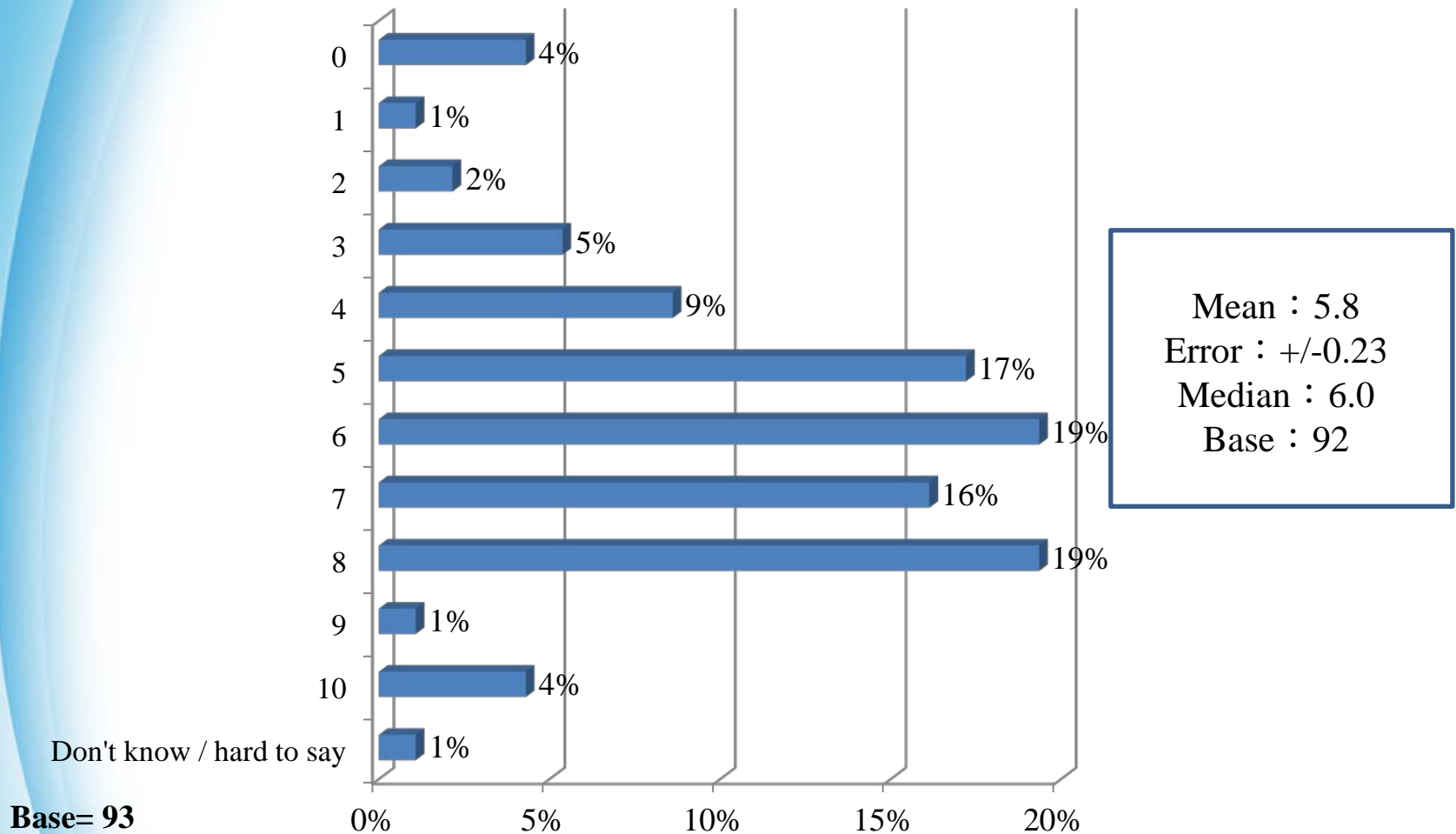| Category	Percentage
Access control	80%
UPS/ uninterruptible power supply	70%
Independent air-conditioned room	70%
Raised floor	64%
Automatic power sprinkler system	47%
Don't know / hard to say	1%

Base = 70

[Q2] [Only ask those who pick "physical security" in Q1] Which of the following physical security does your organization have? [Interviewer to read out items 1-5, order to be randomized, multiple responses allowed]

Organizations' security works of data storage and transfer are perceived to be sufficient

Scale	Percentage
0	0%
1	0%
2	0%
3	2%
4	2%
5	17%
6	22%
7	28%
8	17%
9	6%
10	4%
Don't know / hard to say	1%

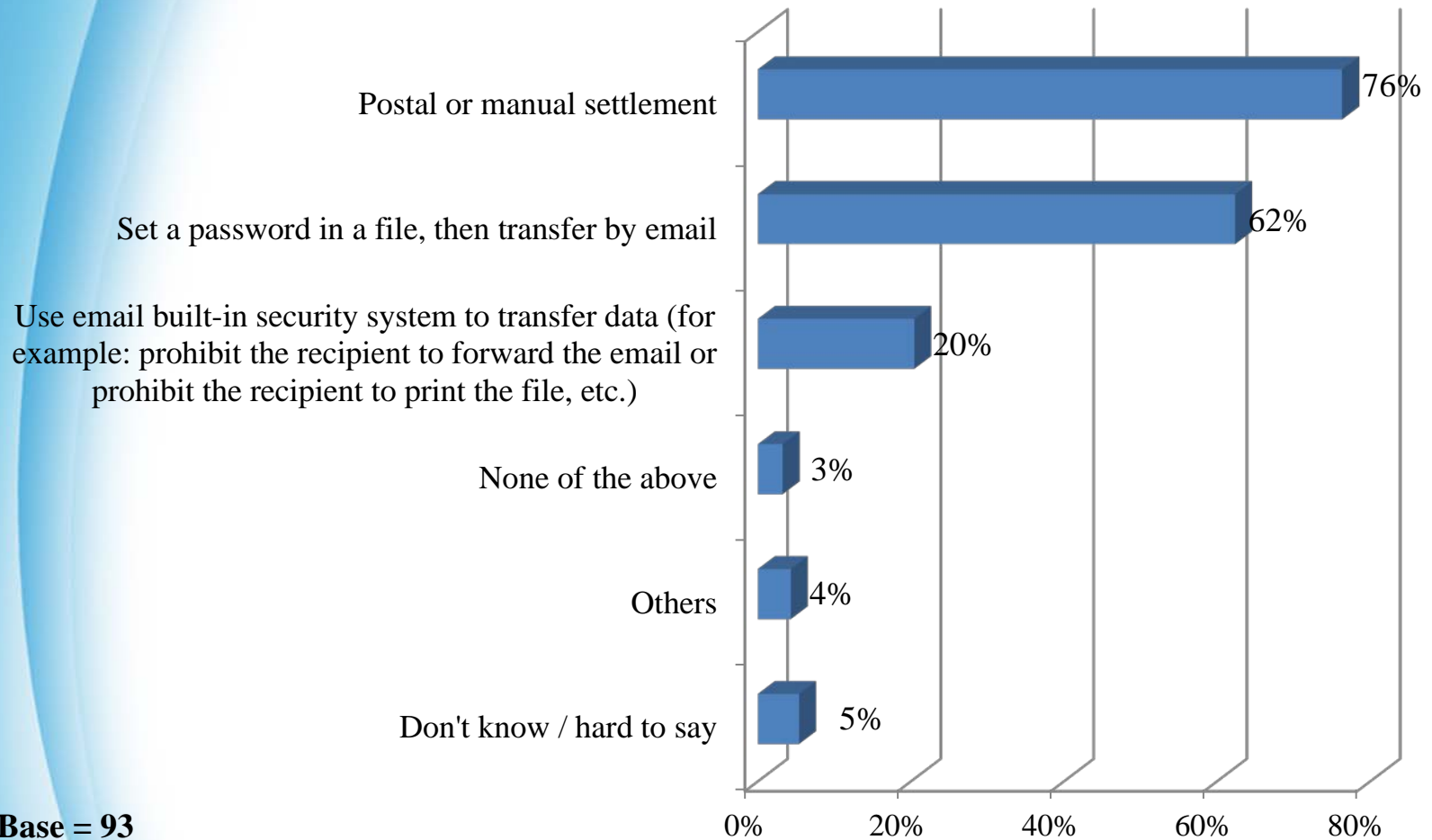Mean：6.7
Error：+/-0.16
Median：7.0
Base：92

Base = 93

[Q3] Do you think the security work of data storage and transfer in your organization is sufficient in the past year? Please use a scale of 0 -10 marks to rate the sufficiency, in which 0 represents totally insufficient, 5 represents half-half, 10 represents very sufficient.

Respondents generally think there is no urgent need to enhance the security works of data storage and transfer

Rating	Percentage
0	4%
1	1%
2	2%
3	5%
4	9%
5	17%
6	19%
7	16%
8	19%
9	1%
10	4%
Don't know / hard to say	1%

Mean：5.8
Error：+/-0.23
Median：6.0
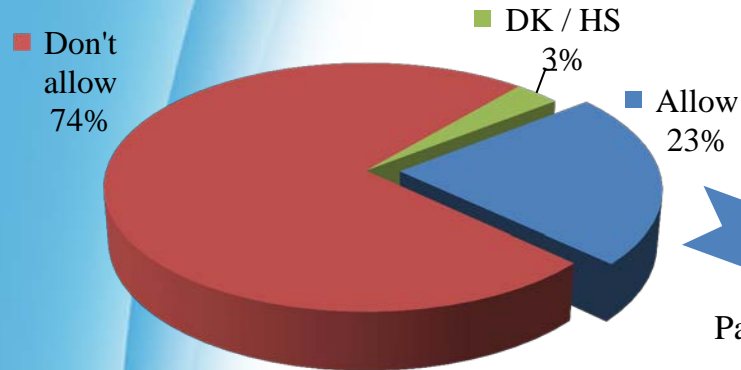Base：92

Base= 93

0%　　5%　　10%　　15%　　20%

[Q4] Do you think your organization is in need to enhance the current security work and/or facilities in data storage and transfer. Please use a scale of 0 -10 marks to rate how much your organization is in such need, in which 0 represents no enhancement is needed at all, 5 represents half-half, 10 represents enhancement is urgently needed.

Most organizations use "postal or manual delivery" to avoid leakage of important/confidential data

Base = 93

- Postal or manual settlement — 76%
- Set a password in a file, then transfer by email — 62%
- Use email built-in security system to transfer data (for example: prohibit the recipient to forward the email or prohibit the recipient to print the file, etc.) — 20%
- None of the above — 3%
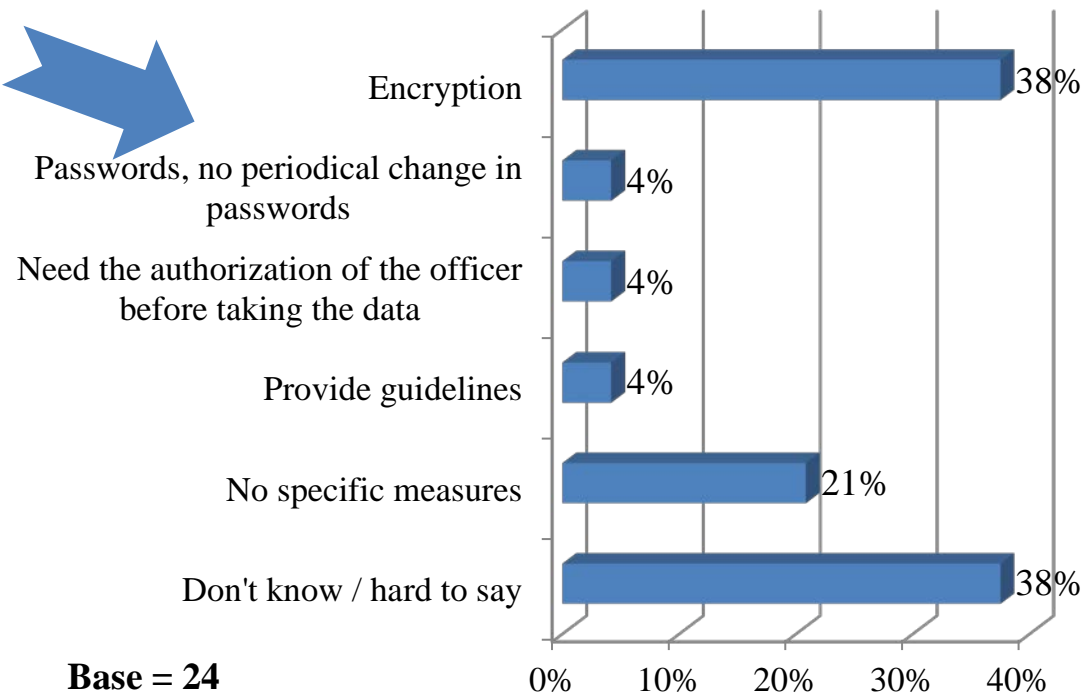- Others — 4%
- Don't know / hard to say — 5%

[Q5] What kind of measures does your organization use to ensure that the data will not be disclosed when transferring important or confidential data / files? [Interviewer to read out items 1-3, order to be randomized, multiple responses allowed]

Nearly 3/4 prohibit employees from taking confidential data out of their premises, where encryption is the most common protective measure used to avoid information leakage

Don't allow 74%

DK / HS 3%

Allow 23%

Base = 93

[Q6] Does your organization allow employees to take confidential data, such as users' personal data, away from the office by using USB or other hardware?
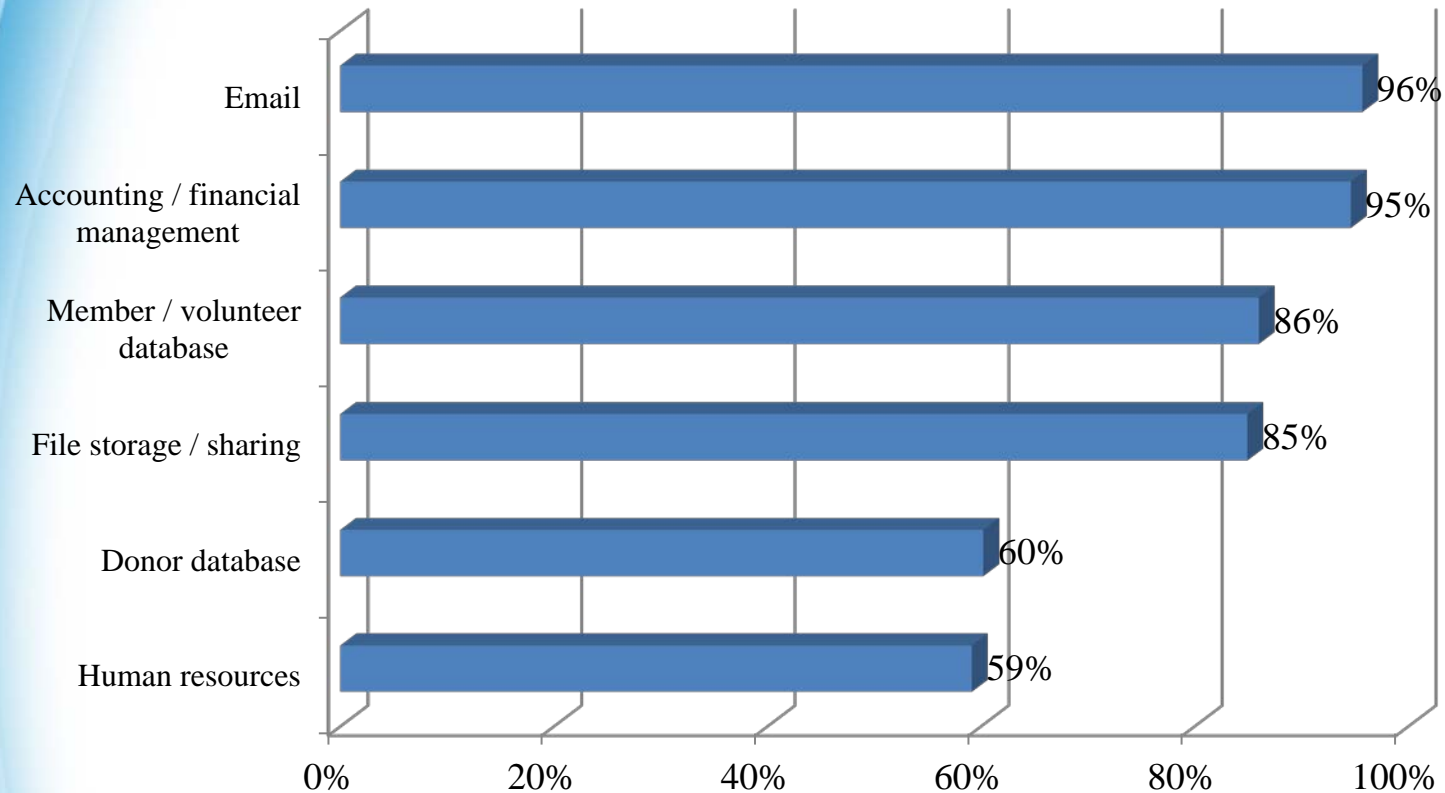
Measure	Percent
Encryption	38%
Passwords, no periodical change in passwords	4%
Need the authorization of the officer before taking the data	4%
Provide guidelines	4%
No specific measures	21%
Don't know / hard to say	38%

Base = 24

[Q7] [Only ask those who answer "allow" or "don't know/hard to say" in Q6, base=24] How does your organization ensure the office data stored in USB or other hardware will not be leaked? [Do not read out answers, multiple responses allowed]

10

2) Cloud Solution

Almost all organizations currently use "email" and "accounting/financial management" programs

Email 96%
Accounting / financial management 95%
Member / volunteer database 86%
File storage / sharing 85%
Donor database 60%
Human resources 59%

Base = 93

[Q8] Which of the following computer program(s) does your organization use currently? [Interviewer to read out items 1-6, order to be randomized, multiple responses allowed]

# 2/3 NGOs are not current users of any "Cloud Solution" systems
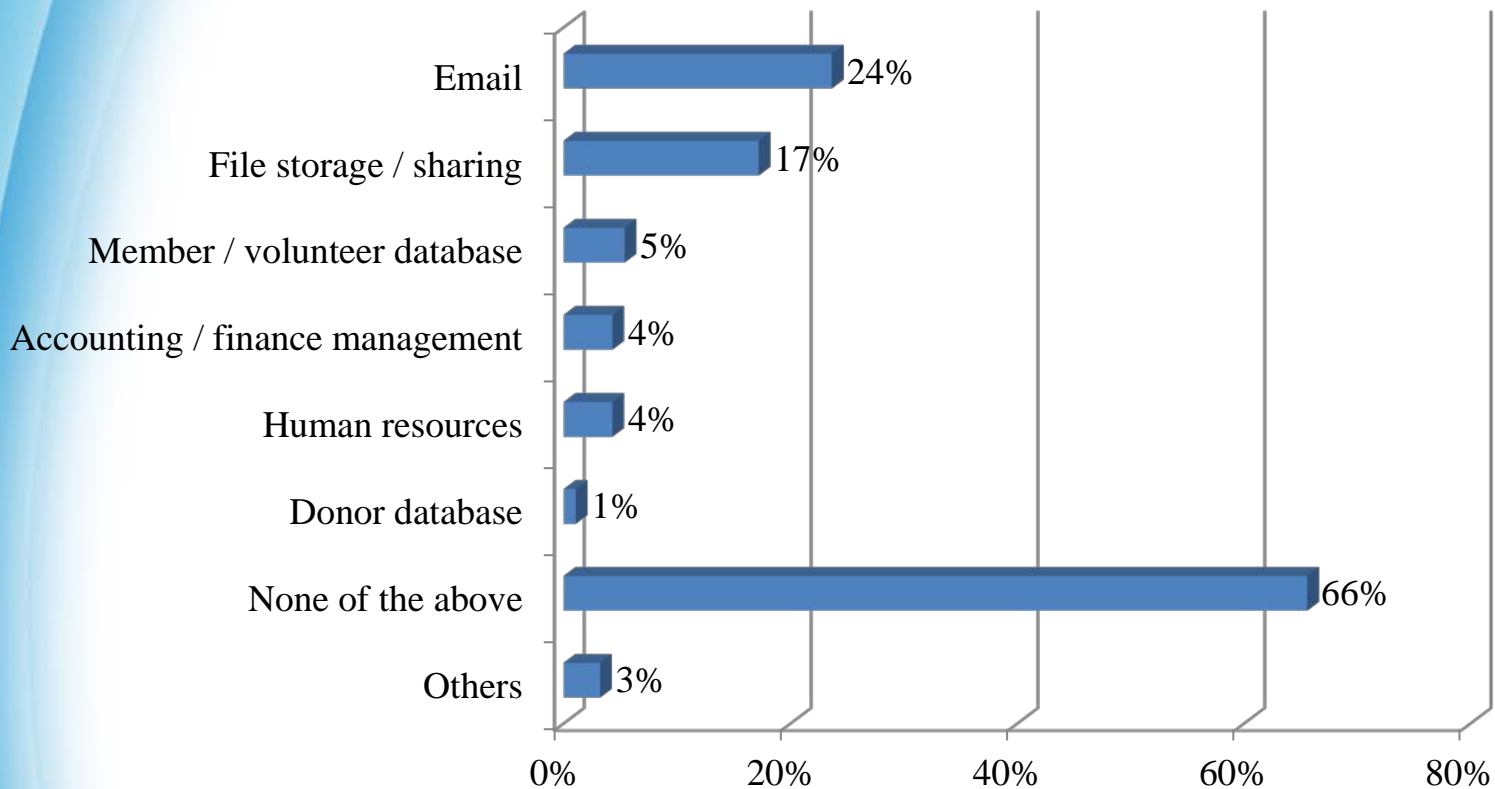
Base = 93

[Read out: "Cloud Solution" basically refers to sharing and storing softwares through the Internet, but not in hardware and local intranet. As a result, once you connect to the Internet, you can use the softwares based in "Cloud Solution". In other words, you are not limited to use the softwares in the office.]

[Q9] Which of the following "Cloud Solution" system(s) does your organization use currently? [Interviewer to read out items 1-6, order to be randomized, multiple responses allowed]

Current situation of using "Cloud Solution" systems
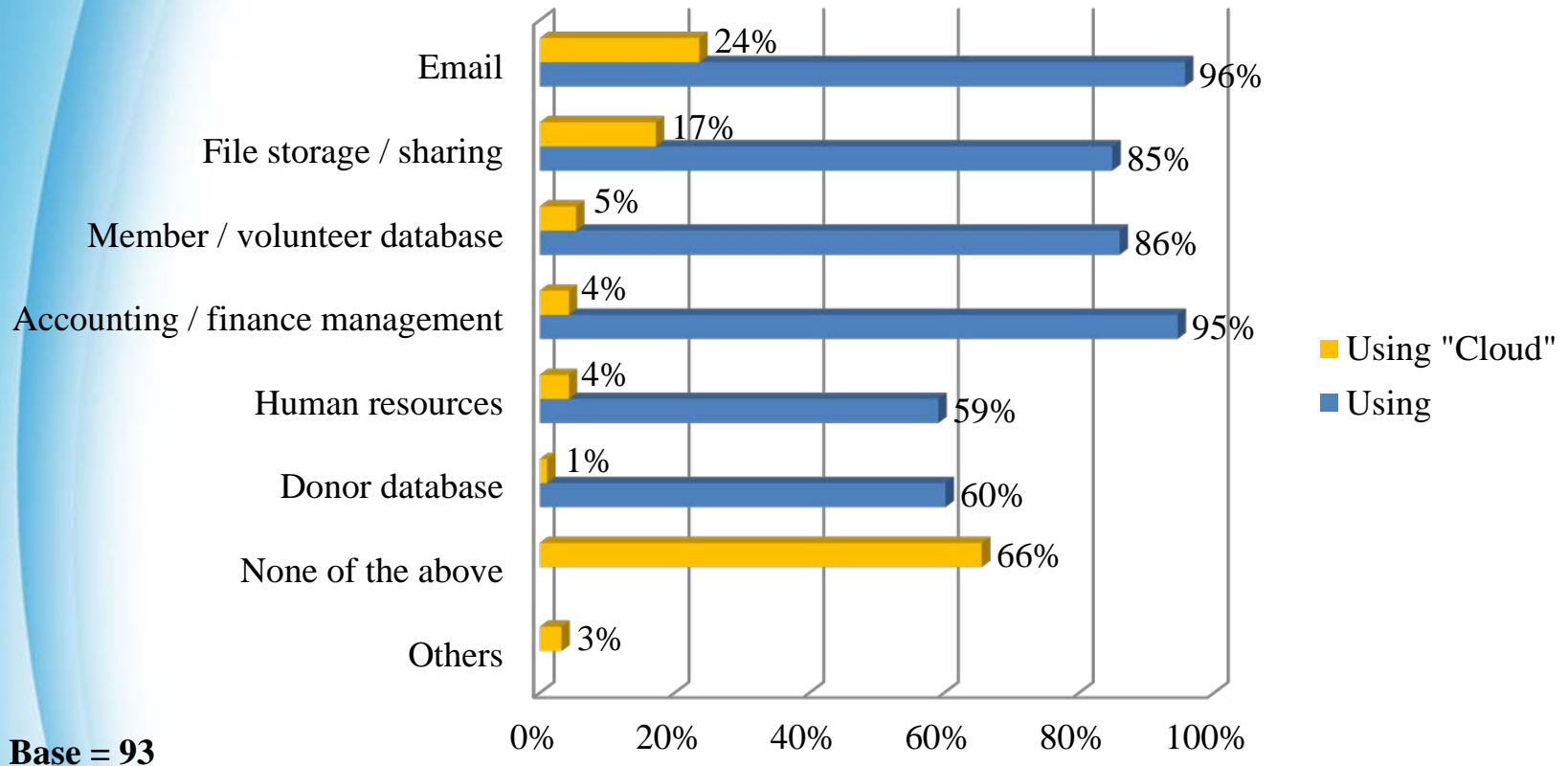
Base = 93

[Q8] Which of the following computer program(s) does your organization use currently? [Interviewer to read out items 1-6, order to be randomized, multiple responses allowed]
[Q9] Which of the following "Cloud Solution" system(s) does your organization use currently? [Interviewer to read out items 1-6, order to be randomized, multiple responses allowed]
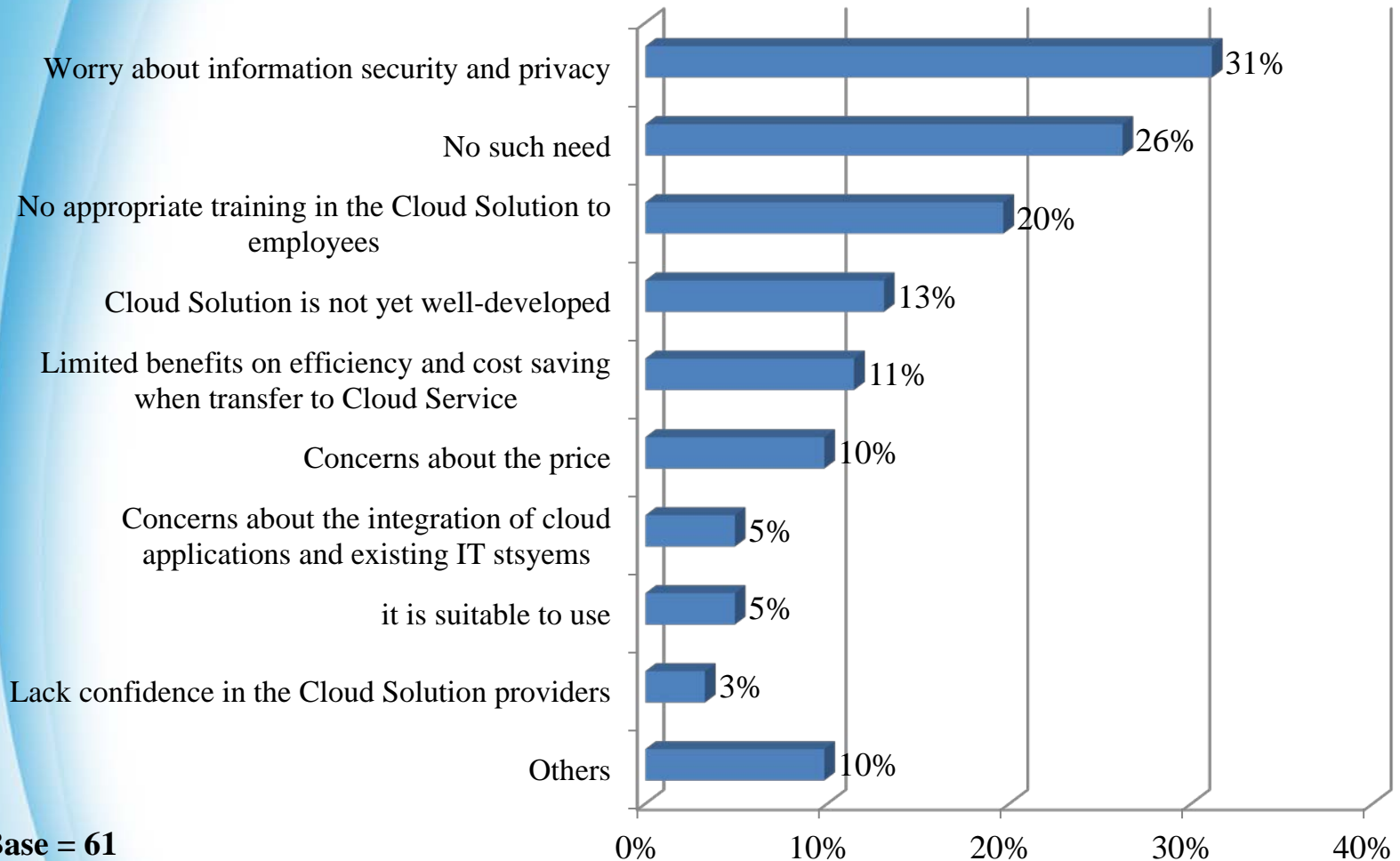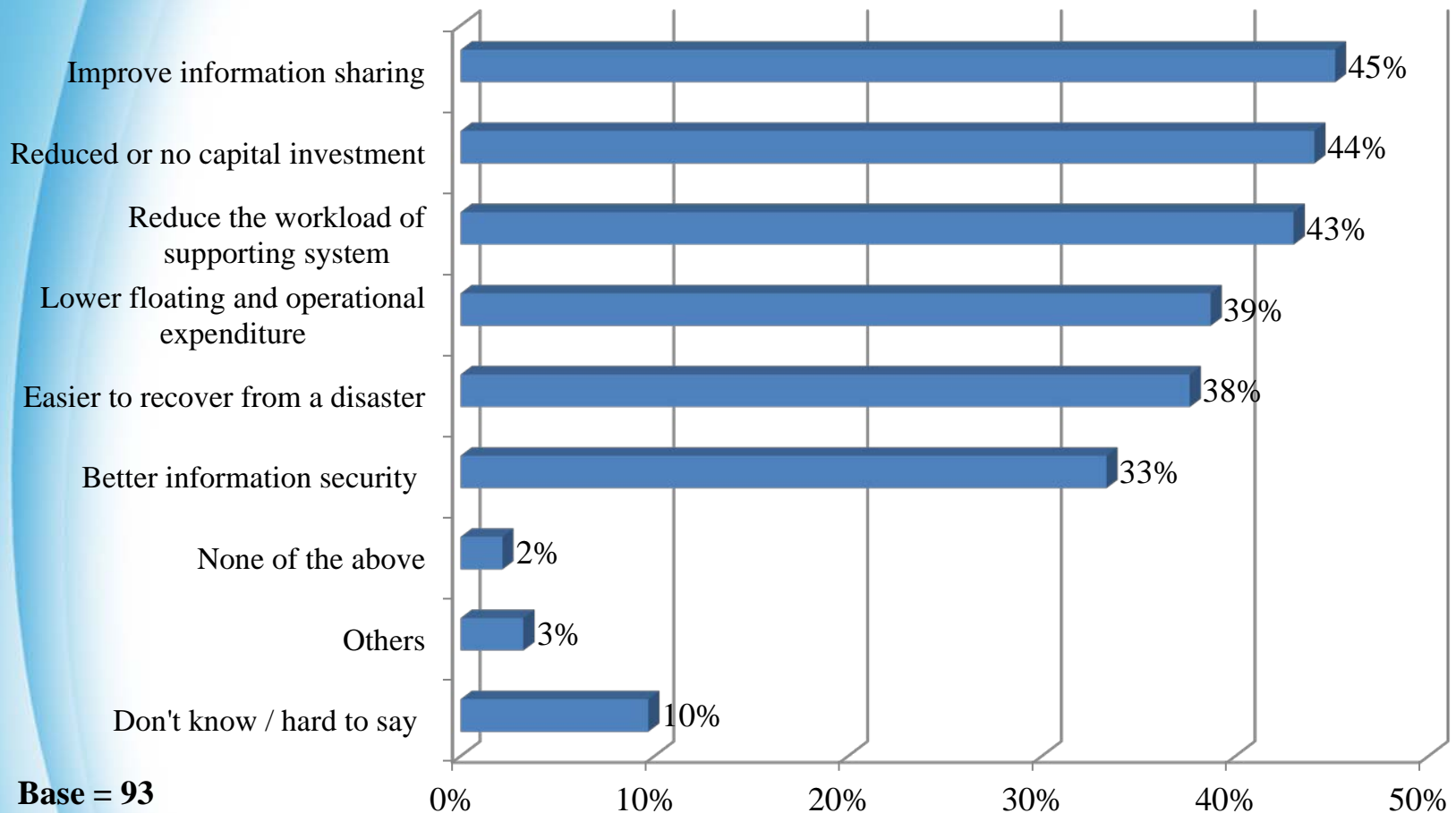
"Worry about information security or privacy" the No.1 reason for not using "Cloud Solution"

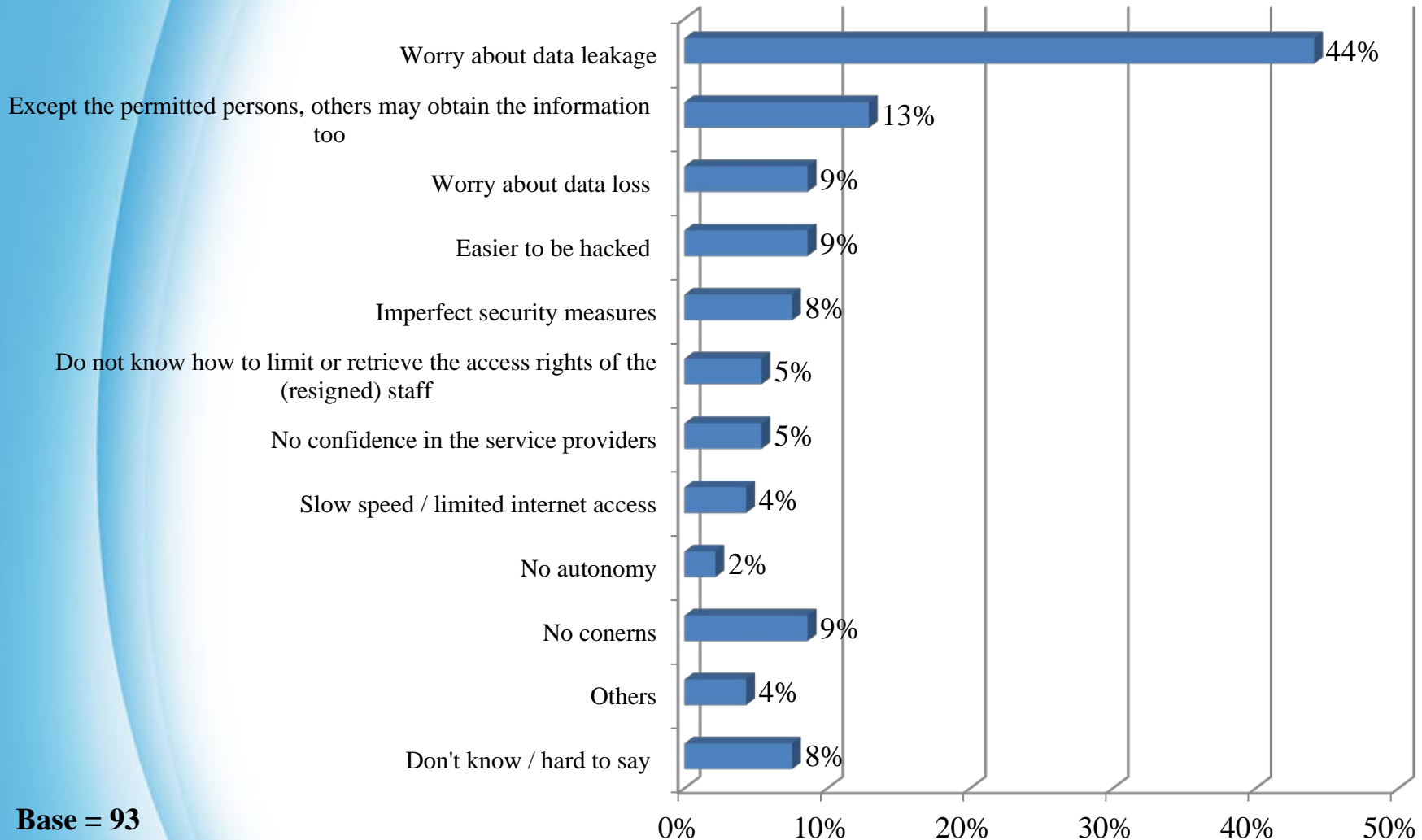| Reason	Percentage
Worry about information security and privacy	31%
No such need	26%
No appropriate training in the Cloud Solution to employees	20%
Cloud Solution is not yet well-developed	13%
Limited benefits on efficiency and cost saving when transfer to Cloud Service	11%
Concerns about the price	10%
Concerns about the integration of cloud applications and existing IT stsyems	5%
it is suitable to use	5%
Lack confidence in the Cloud Solution providers	3%
Others	10%

Base = 61

[Q10] [Only ask those who answered "none of the above" in Q9] What is / are the reason(s) for not using "Cloud Solution" in your organization? [Do not read out answers, multiple responses allowed]

Call for "improvement in information sharing", "reduced or no capital investment" and "reducing the workload or supporting system" to attract users

Category	Percentage
Improve information sharing	45%
Reduced or no capital investment	44%
Reduce the workload of supporting system	43%
Lower floating and operational expenditure	39%
Easier to recover from a disaster	38%
Better information security	33%
None of the above	2%
Others	3%
Don't know / hard to say	10%

Base = 93

[Q11] What reason(s) would you consider to be the most attractive for your organization to transfer IT to Cloud Service? [Interviewer to read out items 1-6, order to be randomized, multiple responses allowed]

Nearly half of the organizations express concern on potential data leakage

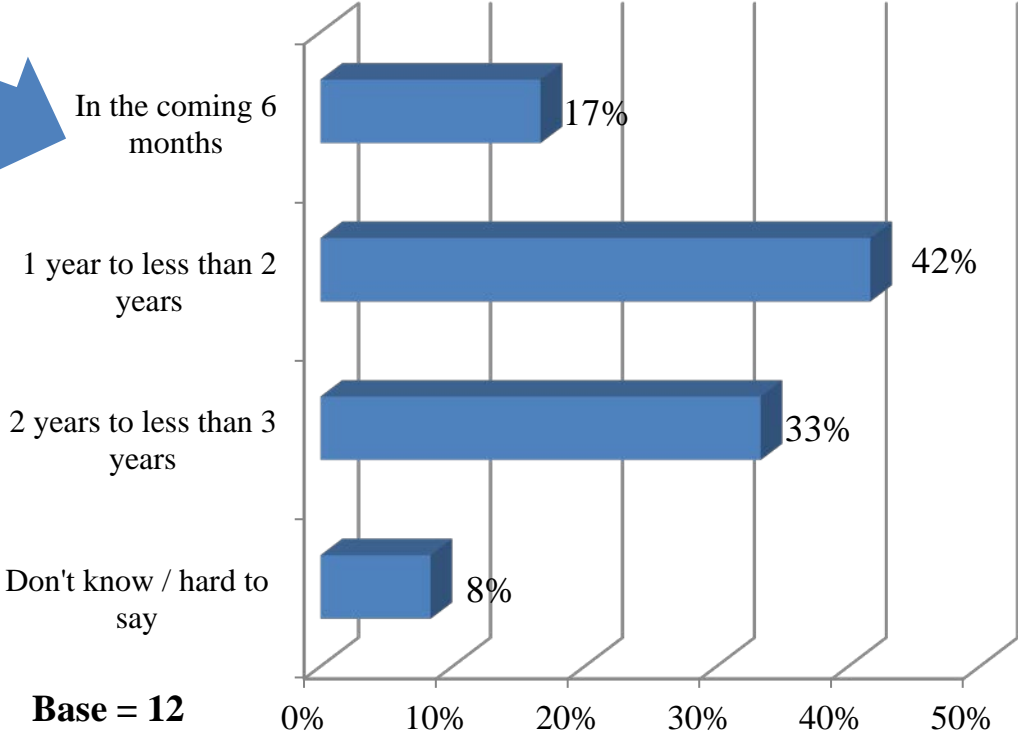| Category	Percentage
Worry about data leakage	44%
Except the permitted persons, others may obtain the information too	13%
Worry about data loss	9%
Easier to be hacked	9%
Imperfect security measures	8%
Do not know how to limit or retrieve the access rights of the (resigned) staff	5%
No confidence in the service providers	5%
Slow speed / limited internet access	4%
No autonomy	2%
No conerns	9%
Others	4%
Don't know / hard to say	8%

Base = 93

[Q12] What is/are your main concern(s) on the information security of "Cloud Solution"? [Do not read out answers, multiple responses allowed]

About 1/8 anticipate they will transfer most of their IT to "Cloud" within the next 3 years

DK / HS 10%
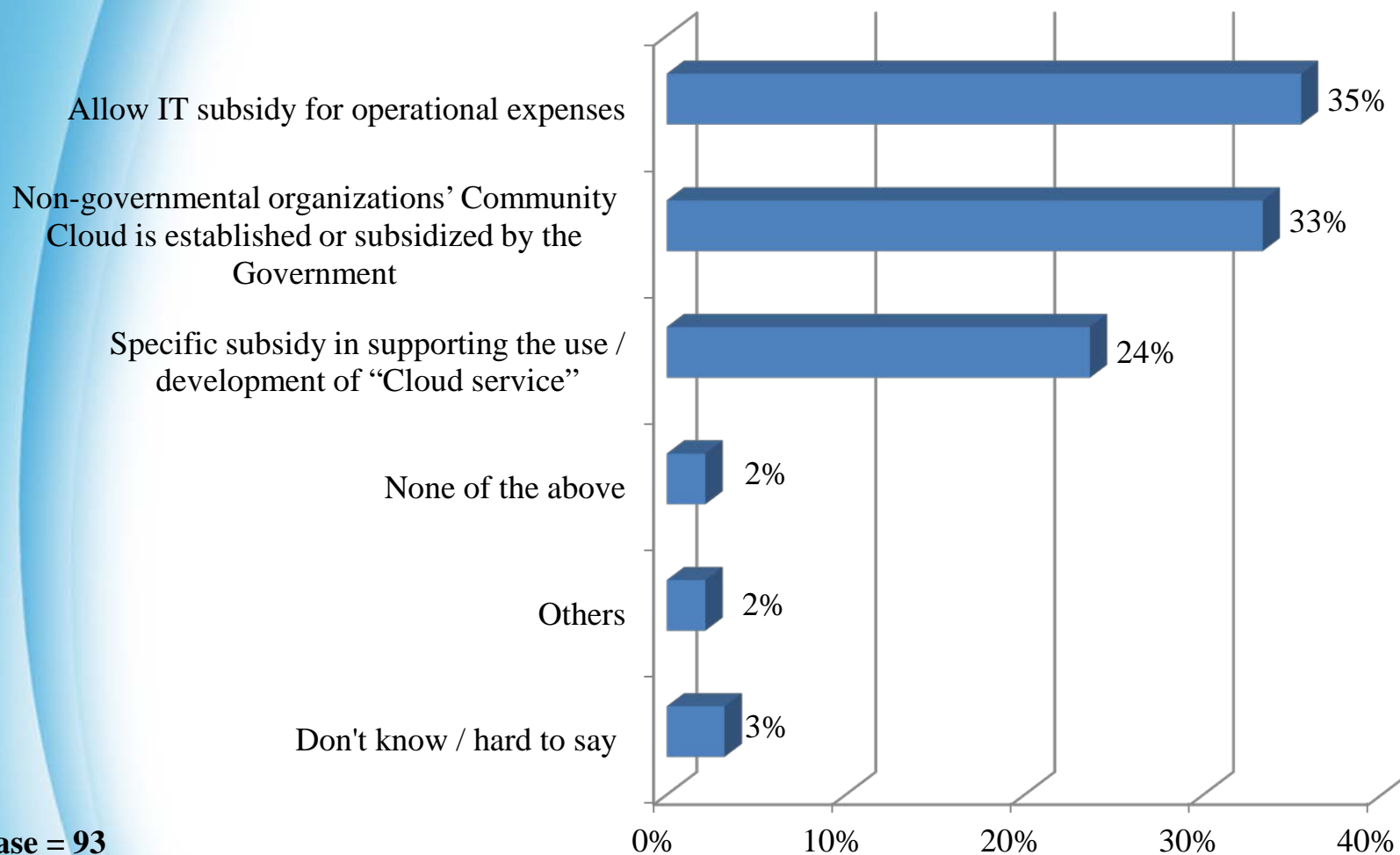
Yes 13%

No 77%
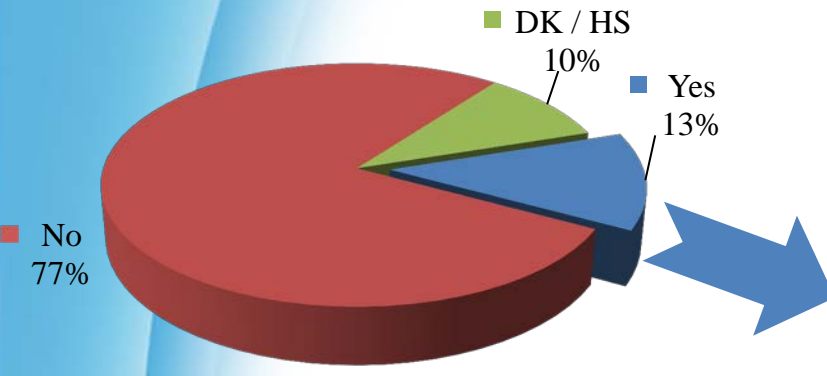
Base= 93

[Q13] Would you expect your organization will transfer most of the IT (databases, e-mail or file storage) to "Cloud" within the next three years? (interviewer can read out: "most" means more than 50% of application system)

In the coming 6 months — 17%

1 year to less than 2 years — 42%

2 years to less than 3 years — 33%

Don't know / hard to say — 8%

Base = 12

0% 10% 20% 30% 40% 50%

[Q14] [Only ask those who answered "yes" in Q13] When will it be?

"Allowing IT subsidy for operational expenses" and "government initiated/subsidied Community Cloud" are perceived as effective means in encouraging local NGOs to use "Cloud Solution" in future

Category	Percentage
Allow IT subsidy for operational expenses	35%
Non-governmental organizations' Community Cloud is established or subsidized by the Government	33%
Specific subsidy in supporting the use / development of "Cloud service"	24%
None of the above	2%
Others	2%
Don't know / hard to say	3%

Base = 93

[Q15] Which of the following mode(s) of subsidy would you consider more effective for the Government to promote non-governmental organizations to use "Cloud Solution"? [Interviewer to read out items 1-3, order to be randomized, one response allowed]

Conclusion

- Only slightly more than half of the NGOs interviewed have used all 5 server protective measures, namely, "**anti-virus**", "**regular backup**", "**firewall**", "**physical security**" and "**uninterruptable power supply**".

- Organizations generally perceived they have **sufficient security works of data storage and transfer**, and they do not see an urgent need to **enhance the corresponding works/facilities**.

- **Postal or manual settlement** is the most common measure to prevent data leakage to outside while most organizations **prohibit their employees to take confidential data away from office premises**.

Conclusion (Cont.)

- **Worry about information security or privacy** is reportedly the top major concern for not using "Cloud Service". **Improvement in information sharing** can best attract local NGOs to subscribe "Cloud Service".

- 70% of the NGOs interviewed say that in the next three years, they **will not transfer most of the IT to "Cloud"**.

- **Allowing IT subsidy for operational expenses** and **government initiated/subsidized Community Cloud** are perceived as most effective in encouraging local NGOs to use "Cloud Solution".
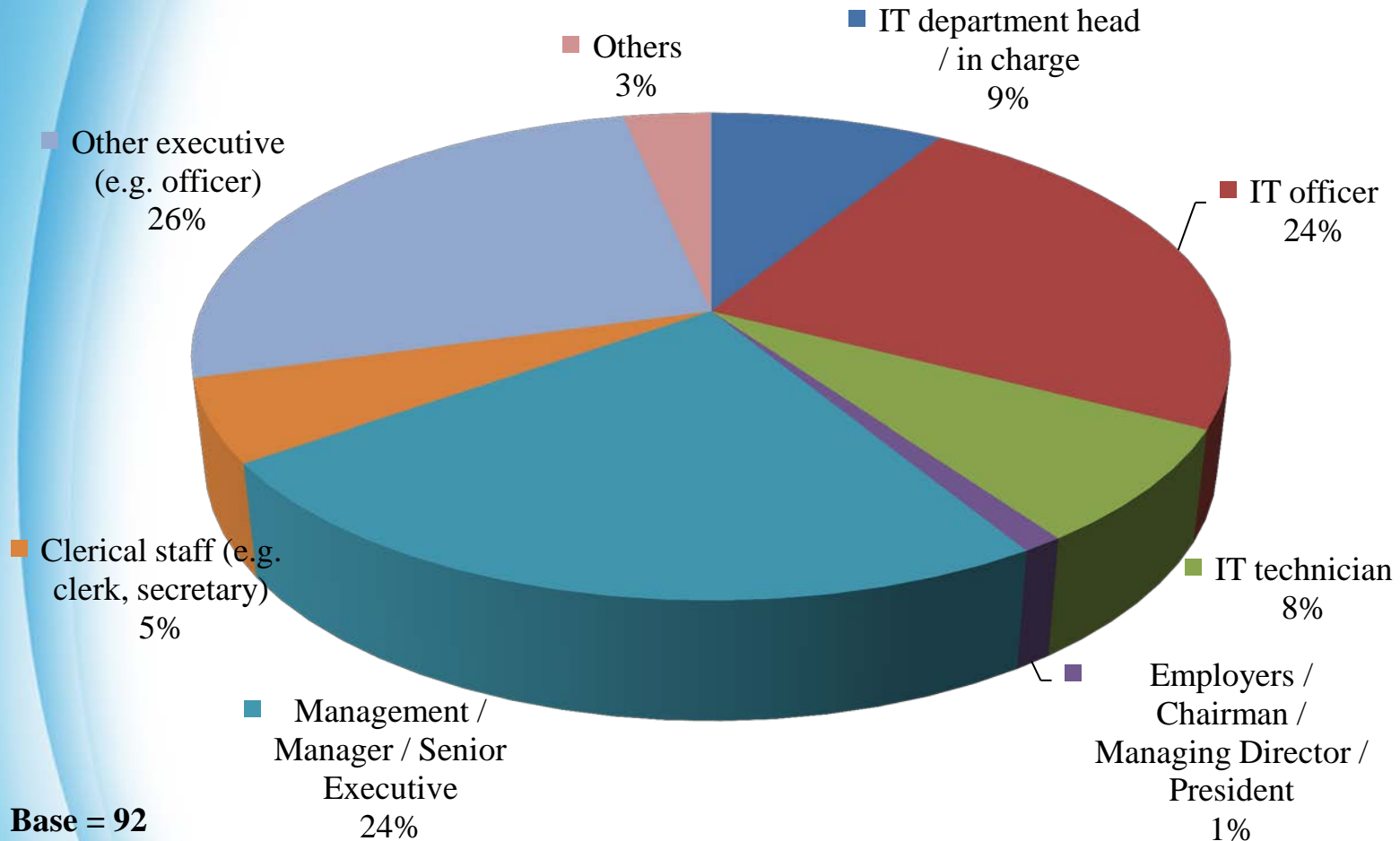
Profile Information of Interviewed Organizations

Categorization of Organizations

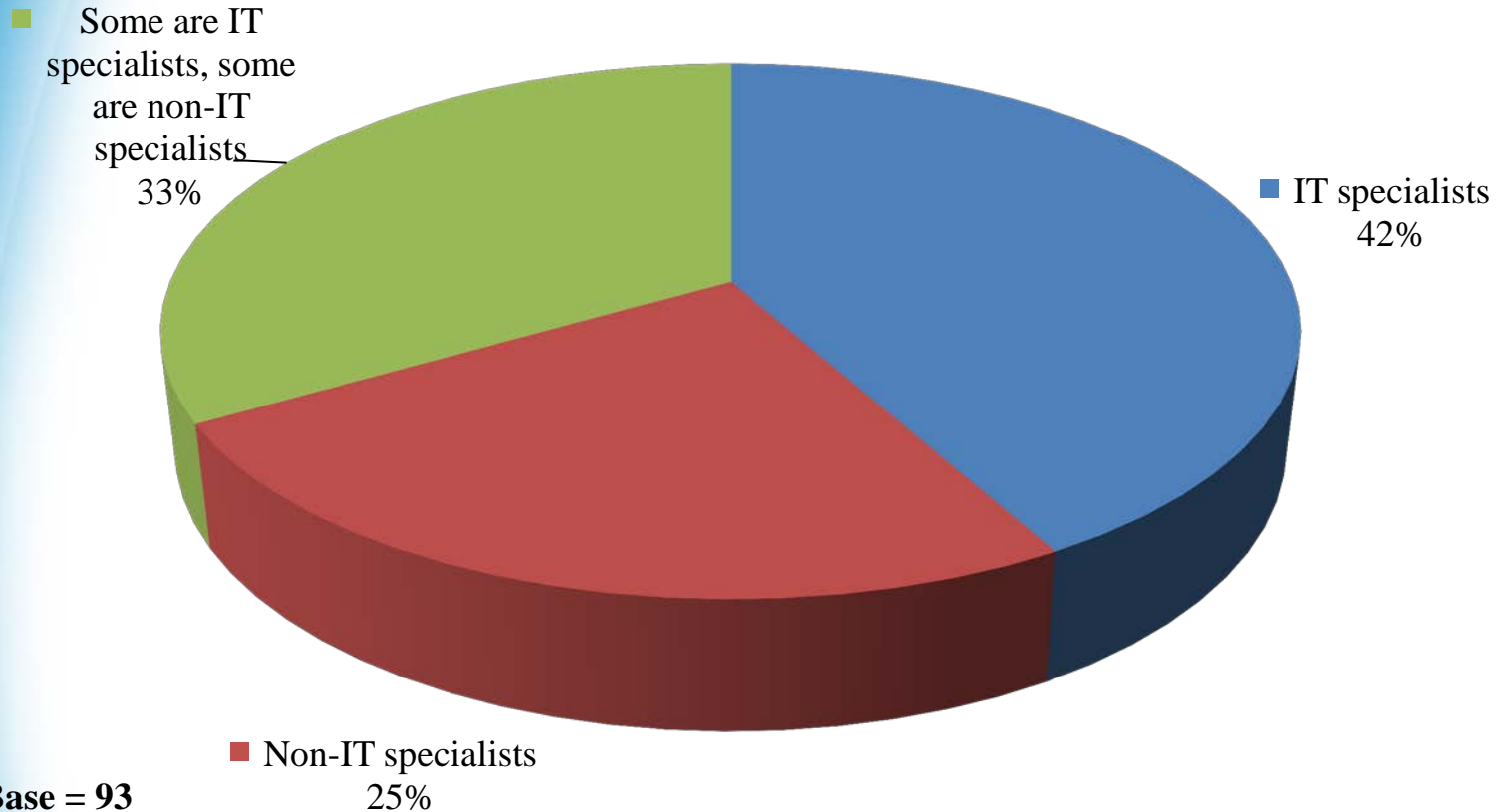| Category	Annual Expenditure* (HK$)	Percentage (number)
Small size organization	Below 1 million	14% (13)
Medium size organization	Between 1 million and 10 millions	45% (42)
Large size organization	More than 10 millions	41% (38)
Total		93

* Categorization was based on the expenditure of Year 2010-11.

Position of Respondents

Others
3%

IT department head
/ in charge
9%

Other executive
(e.g. officer)
26%

IT officer
24%

Clerical staff (e.g.
clerk, secretary)
5%

IT technician
8%

Management /
Manager / Senior
Executive
24%

Employers /
Chairman /
Managing Director /
President
1%

Base = 92

Staff responsible for IT affairs

Some are IT specialists, some are non-IT specialists 33%

IT specialists 42%

Non-IT specialists 25%

Base = 93

[DM1] People who are responsible for IT affairs in your organization are mainly: (IT specialist indicates people who are mainly responsible for IT services and resolve the needs of internal IT services)

Number of IT specialists

Base = 92
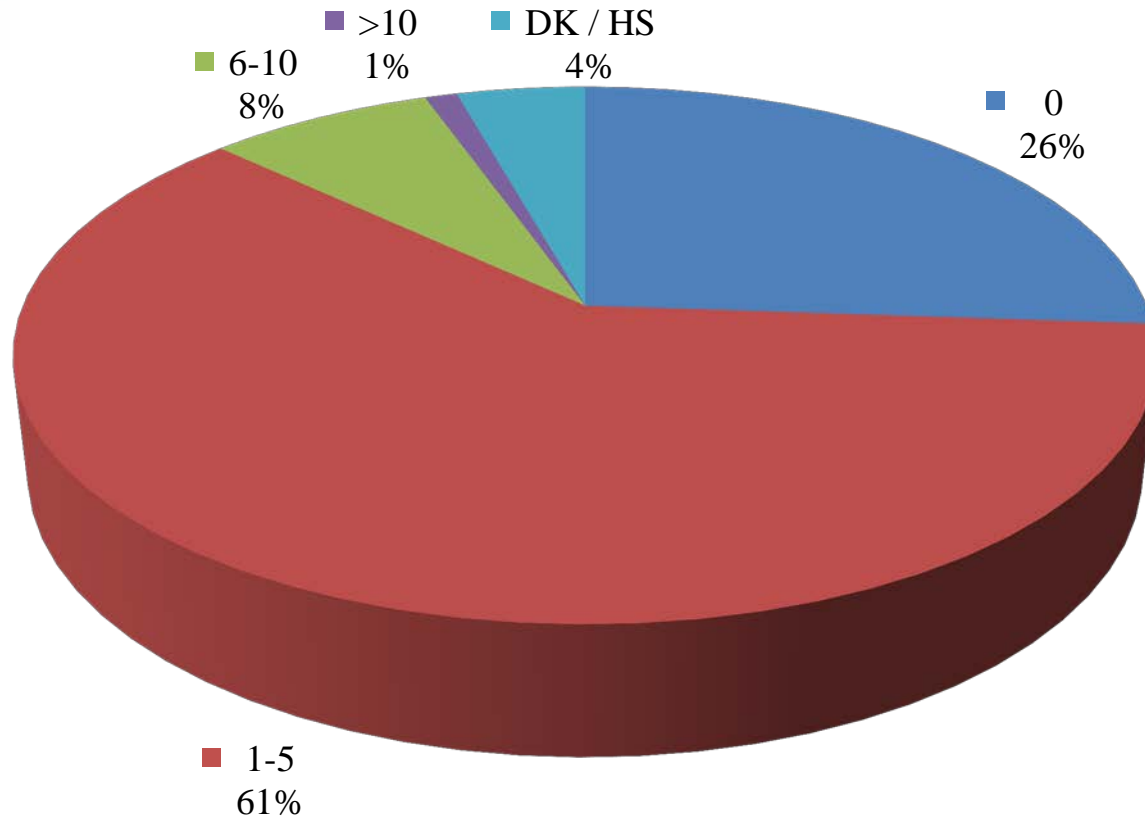
[DM2] How many IT specialists in your organization in total?

The End

For detailed report, please visit
http://hkupop.hku.hk