Mobile Data Security Survey for Federal Computer Week

May 2007

Survey Summary -1

- 183 responses – mostly federal employees and mostly from civilian agencies
- Most had policies and procedures in place prior to the VA data theft, though military personnel seemed more likely to have those policies and procedures.
- Most agencies have taken additional steps to improve security. 83% of those who already had procedures in place took additional steps over this past year, while 70% of those who said there were no policies/procedures in place noted that they have taken additional steps.
- When asked to select all the steps their agencies have taken, 50% or more report that their agencies had implemented new security policies, procedures and technologies. 46% had invested in training and about a third had allocated and/or requested new resources.

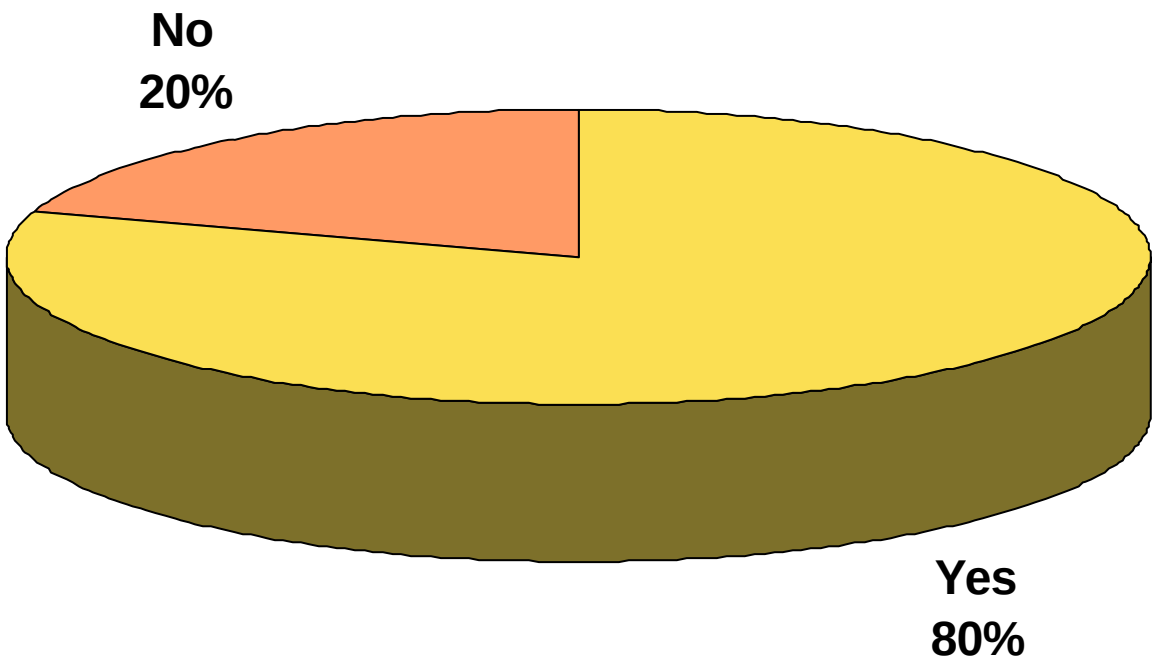
Survey Summary - 2

- Respondents are working to secure thousands of mobile devices of various kinds, a daunting challenge.
  - 47% are working to secure over 1,000 devices
  - A higher percentage of military respondents than civilian respondents are trying to secure more than 25,000 devices (they also have a higher percentage of respondents trying to secure less than 100 devices)\
- Most agencies are trying to secure their laptops, PDAs and mobile data, but about 1/3 are also trying to secure mobile phones.
  - A slightly greater percentage of military respondents reported that they are working to secure mobile data drives and phones.
  - Significantly more military respondents are focusing on PDAs, and though laptops and mobile data devices are also important to military respondents, they reported this concern at a slightly lower rate than civilian respondents.

Survey Summary - 3

- In response to OMB's recommendations on how to address data breaches that could lead to identity theft, most respondents report that their agencies have taken at least some of the steps, however 23% report no progress on this.
- In rating the importance of various aspects of mobile data security to their organizations, respondents were most worried about system integrity, followed by national security. Cost to the organization seems to have been of least concern.

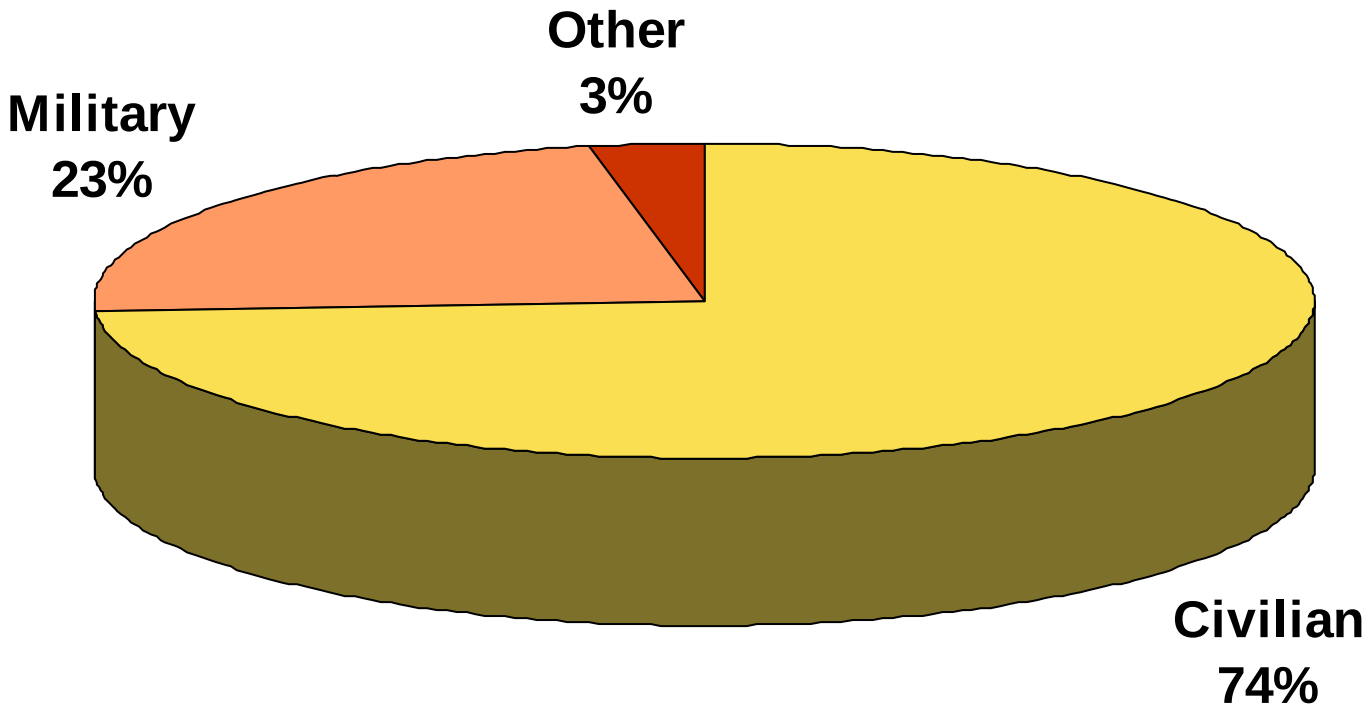
Are you a federal employee?



Are you a federal employee?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Yes	147	80.3%	80.3%	80.3%
No	36	19.7%	19.7%	19.7%

Do you work in a civilian or a military agency?



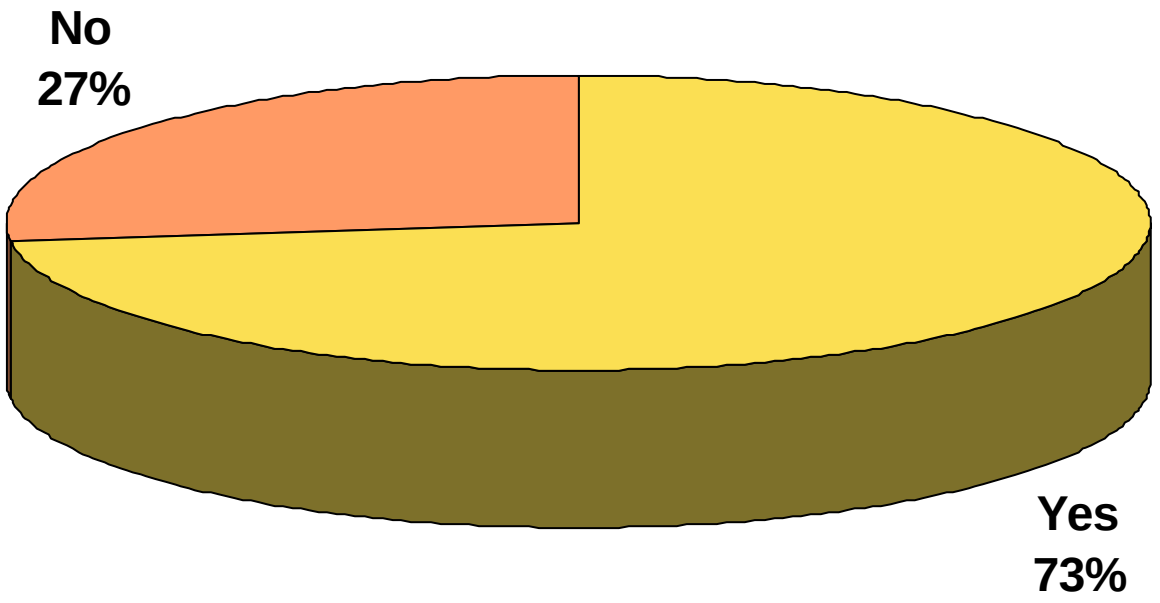
Do you work in a civilian or a military agency?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Civilian	135	73.8%	73.8%	73.8%
Military	42	23.0%	23.0%	23.0%
Other(please specify)	6	3.3%	3.3%	3.3%

Do you work in a civilian or a military agency? - Other(please specify)

- Contractor in DoD support
- contractor
- Industry
- Tribal
- industry
- FFRDC

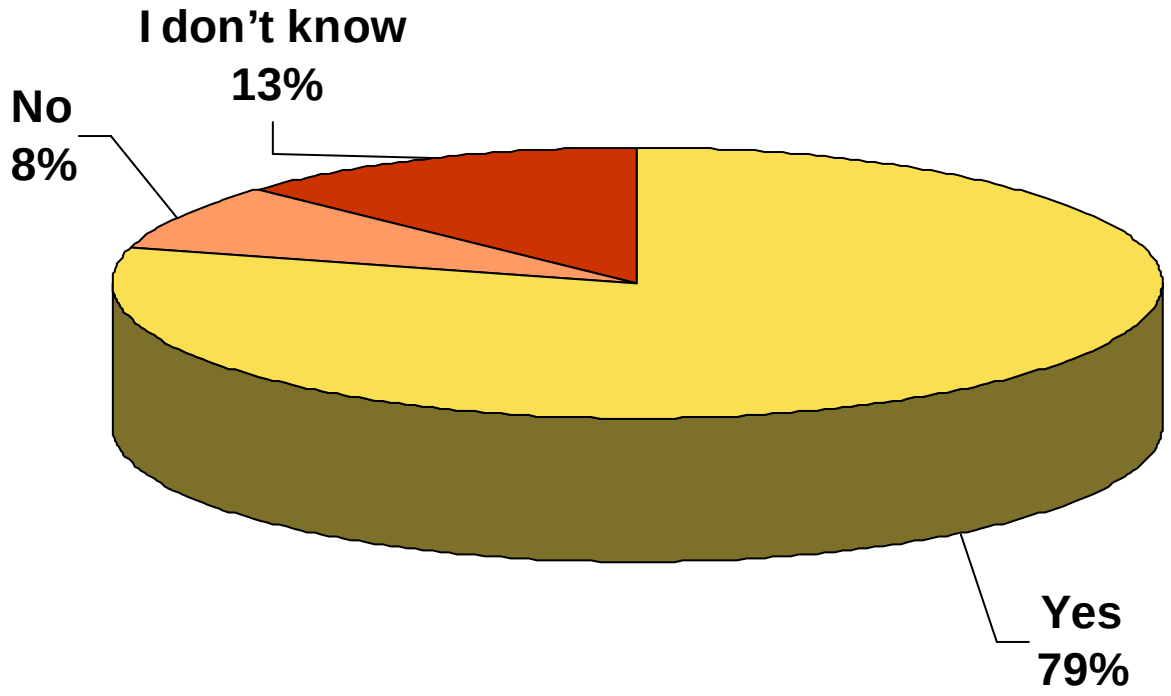
Did you have policies and procedures in place before May 2006 to address mobile data security?



Did you have policies and procedures in place before May 2006 to address mobile data security?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Yes	133	72.7%	72.7%	72.7%
No	50	27.3%	27.3%	27.3%

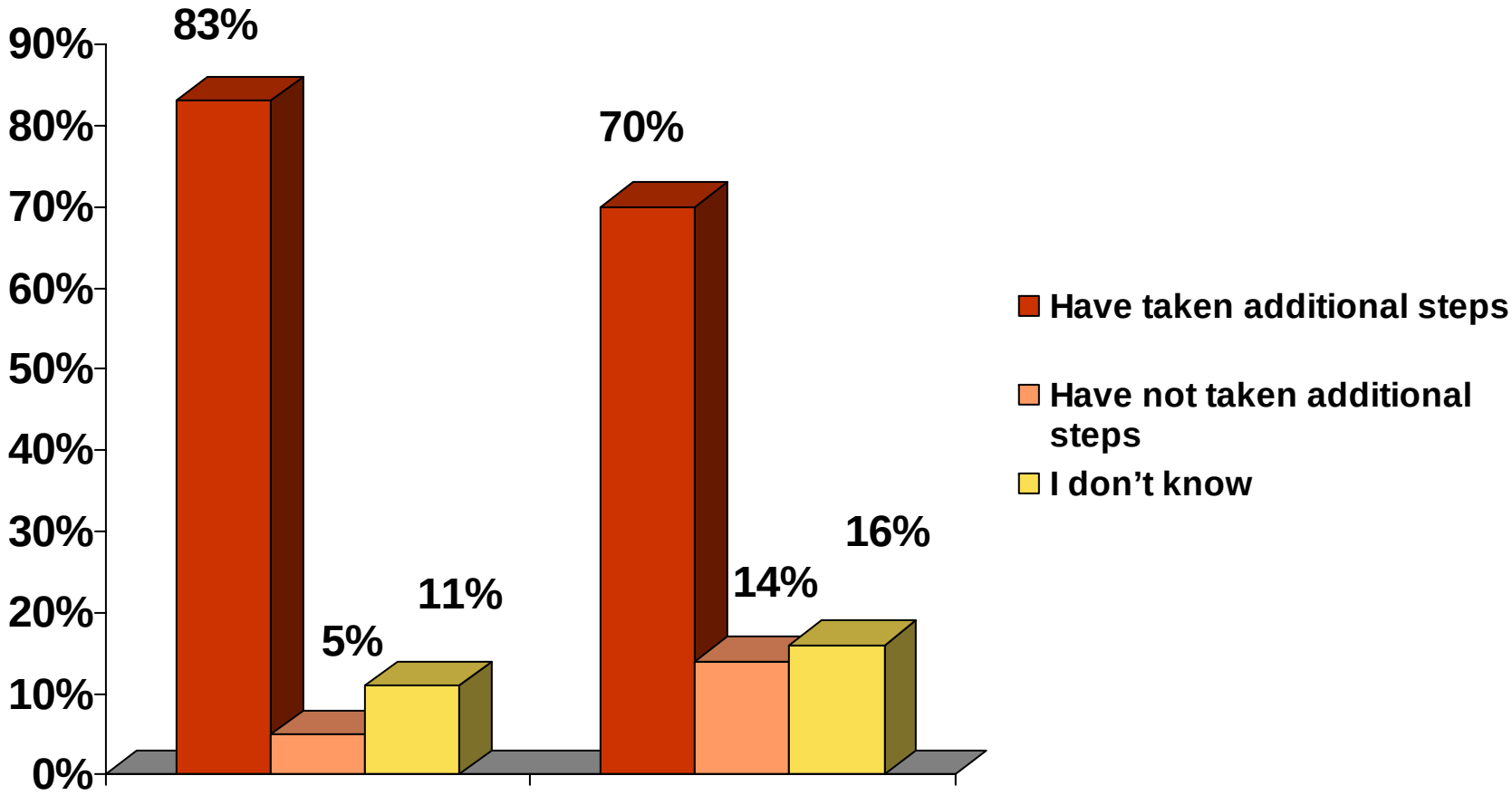
Has your organization taken steps to improve mobile data security over the last twelve months?



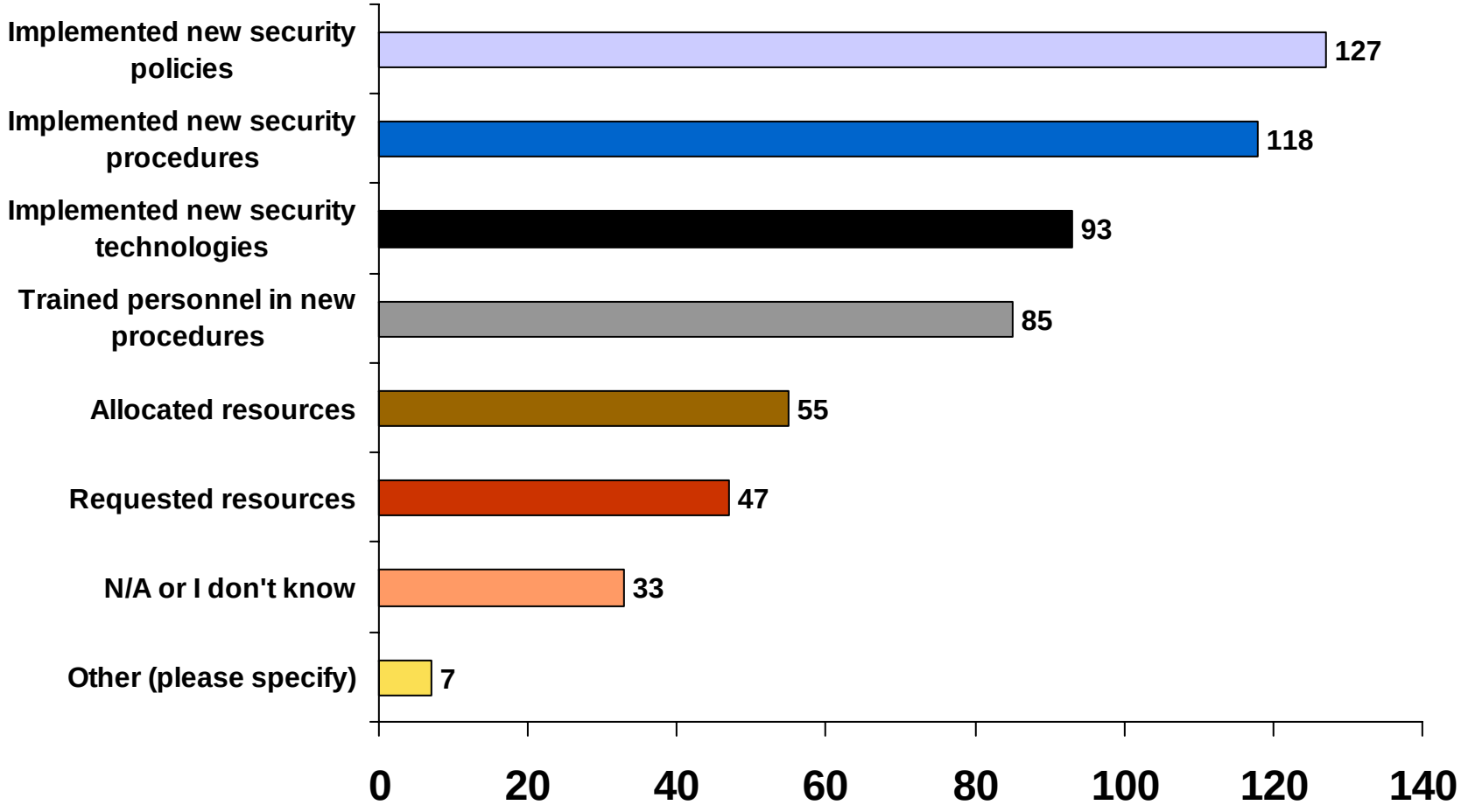
Has your organization taken steps to improve mobile data security over the last twelve months?

Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Yes	146	79.8%	79.8%	79.8%
No	14	7.7%	7.7%	7.7%
I don’t know	23	12.6%	12.6%	12.6%

Changes in policies/procedures over the past year



Please specify these steps (check all that apply):



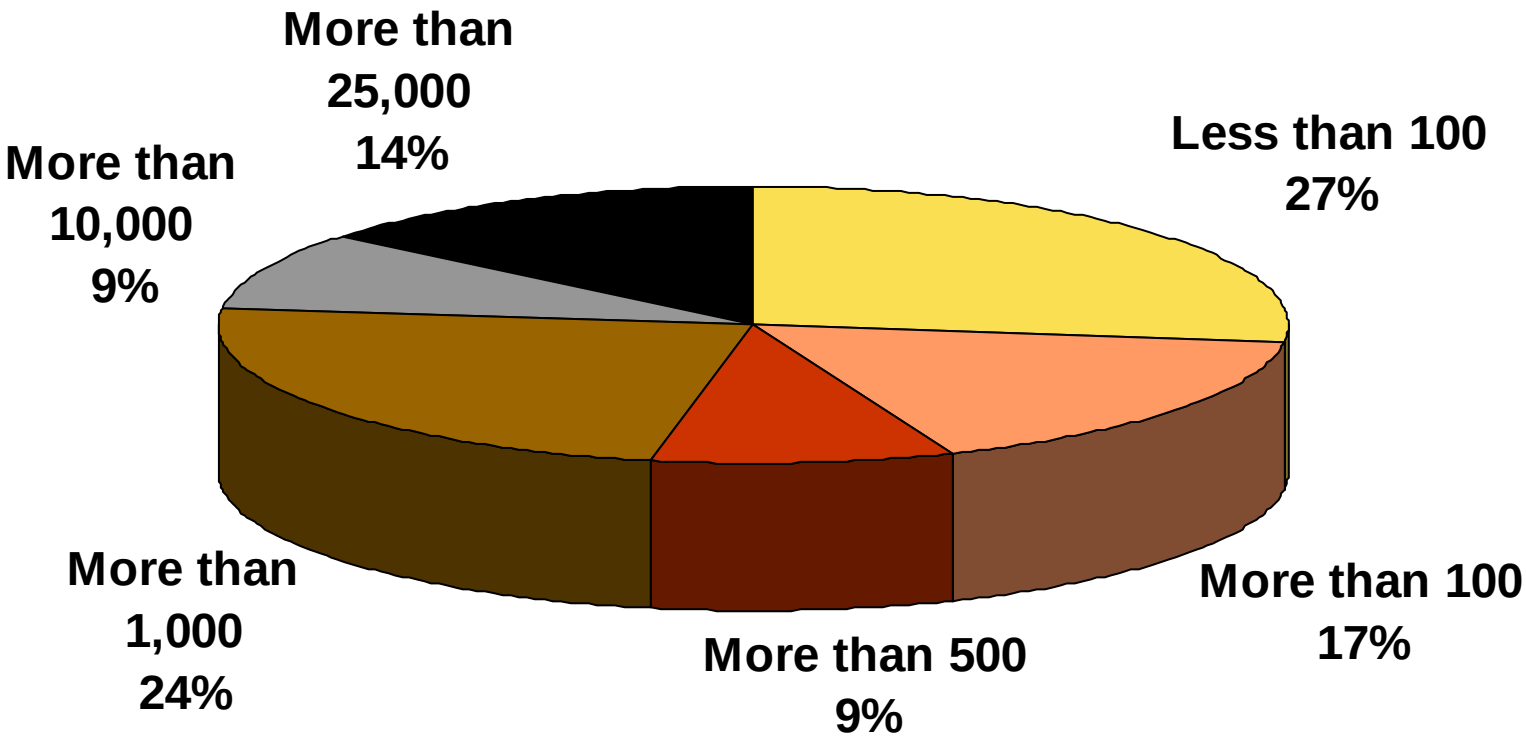
Please specify these steps (check all that apply):

Choice	Count	Percent of Sample Asked	Percent of Total Sample
Implemented new security policies	127	69.4%	69.4%
Requested resources	47	25.7%	25.7%
Allocated resources	55	30.1%	30.1%
Trained personnel in new procedures	85	46.4%	46.4%
Implemented new security procedures	118	64.5%	64.5%
Implemented new security technologies	93	50.8%	50.8%
N/A or I don't know	33	18.0%	18.0%
Other (please specify)	7	3.8%	3.8%

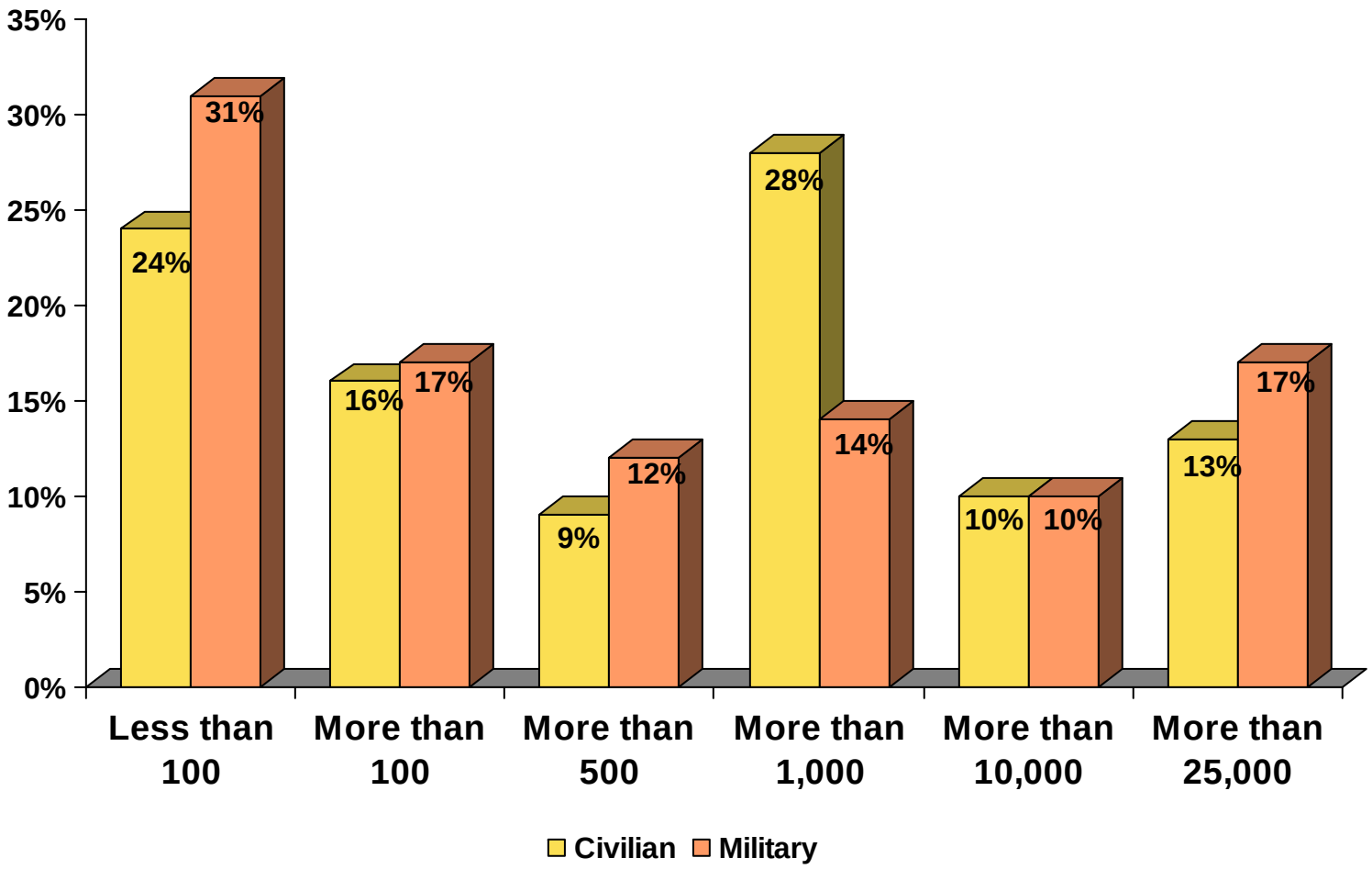
Please specify these steps (check all that apply): - Other

- Provisioned all devices OTA with Trust Digital security software
- No Mobile Units
- restricted VPN access
- Encrypted notebook hard drives
- Refreshed personnel in current security procedures

How many devices are you trying to secure? (select one)



Number of devices to secure, by percentage and sector

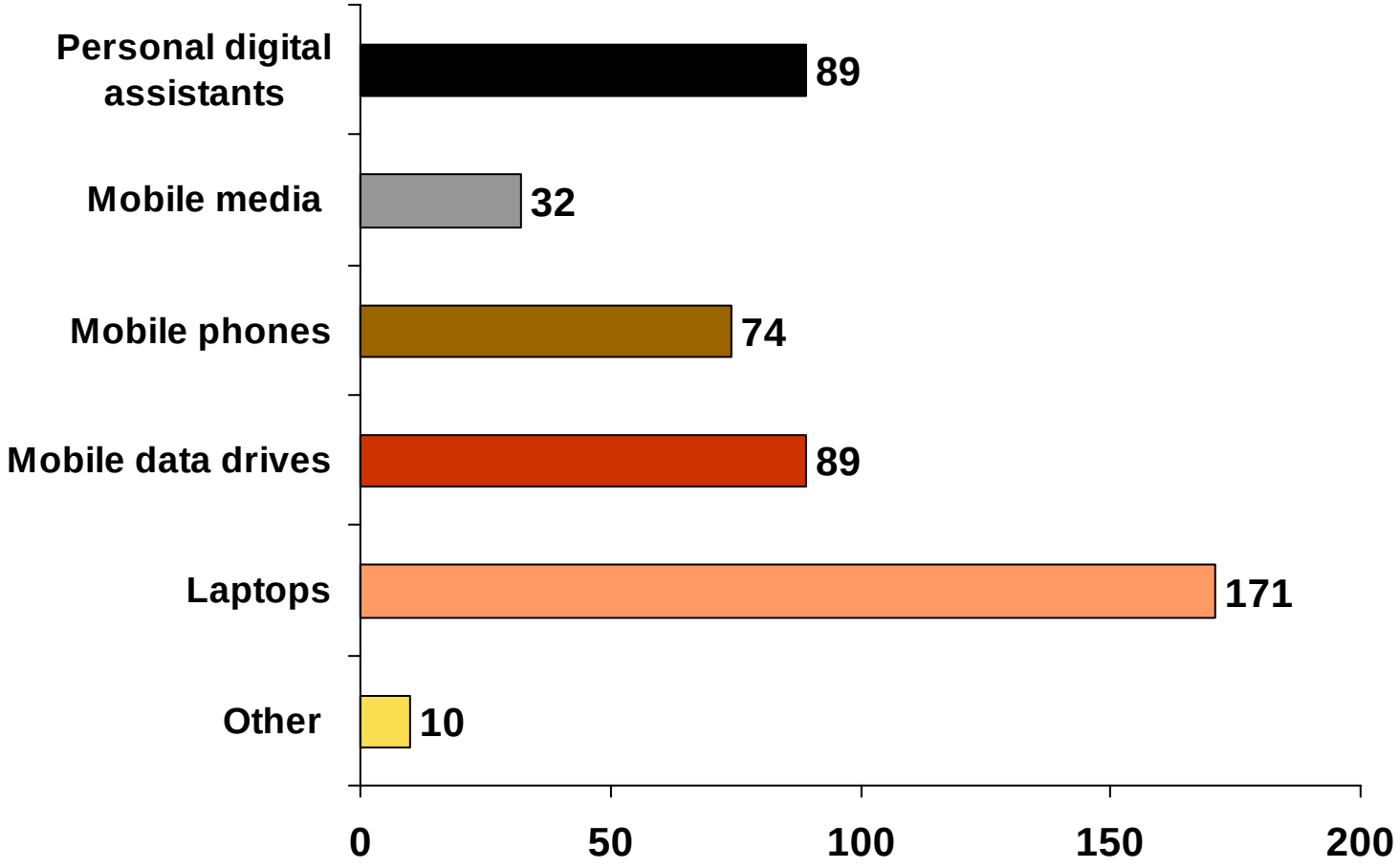


How many devices are you trying to secure? (select one)

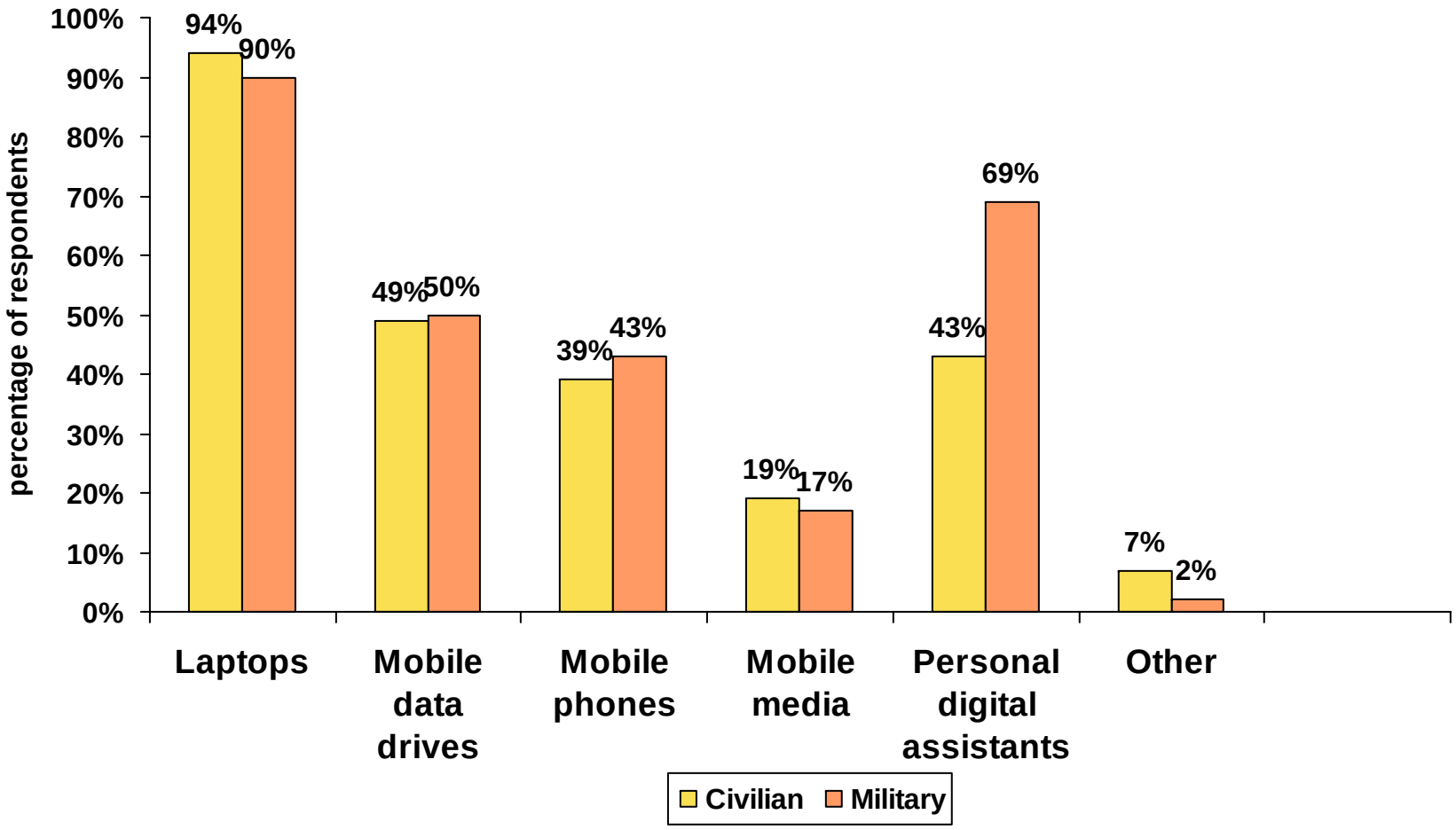
Choice	Count	Percentage of Sample Answering	Percentage of Sample Asked	Percentage of Total Sample
Less than 100	49	26.8%	26.8%	26.8%
More than 100	31	16.9%	16.9%	16.9%
More than 500	17	9.3%	9.3%	9.3%
More than 1,000	44	24.0%	24.0%	24.0%
More than 10,000	17	9.3%	9.3%	9.3%
More than 25,000	25	13.7%	13.7%	13.7%

Choice	Civilian	Military	Other(please specify)
Less than 100	33	13	3
More than 100	22	7	2
More than 500	12	5	0
More than 1,000	38	6	0
More than 10,000	13	4	0
More than 25,000	17	7	1

Which types of devices are you trying to secure? (select all that apply)



Military and civilian respondents have slight differences in the types of devices they are securing



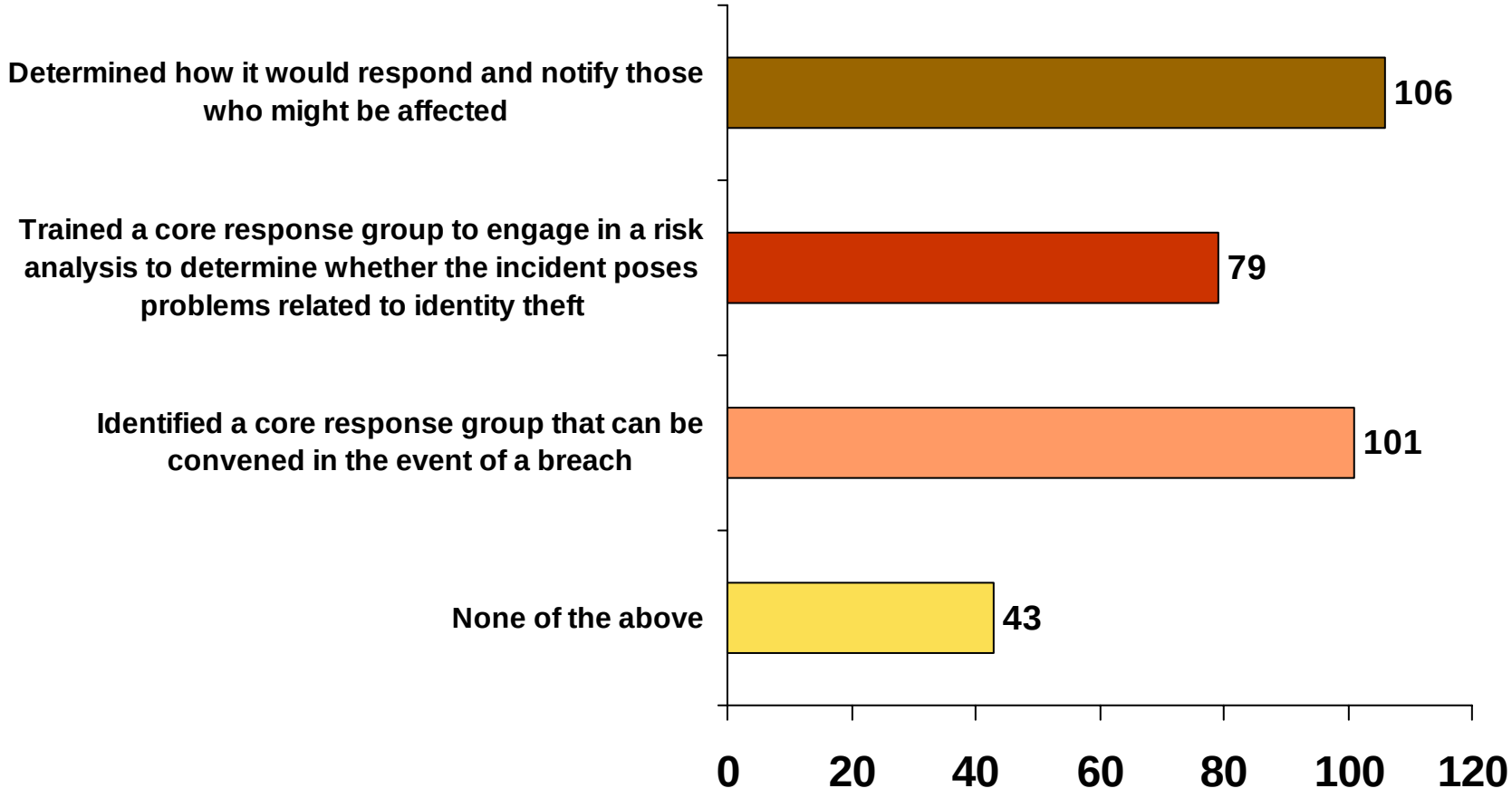
Which types of devices are you trying to secure? (select all that apply)

Choice	Count	Percent of Sample Asked	Percent of Total Sample
Laptops	171	93.4%	93.4%
Mobile data drives	89	48.6%	48.6%
Mobile phones	74	40.4%	40.4%
Mobile media (e.g., music players that also store data)	32	17.5%	17.5%
Personal digital assistants	89	48.6%	48.6%
Other (please explain)	10	5.5%	5.5%

Which types of devices are you trying to secure? (select all that apply) - Other (please explain)

- Blackberries
- Desktop
- storage media
- Servers and Removable Storage Media (all types)
- building property
- No mobile units allowed
- my LAPTOP
- plan to secure addtl types in future
- smart phones

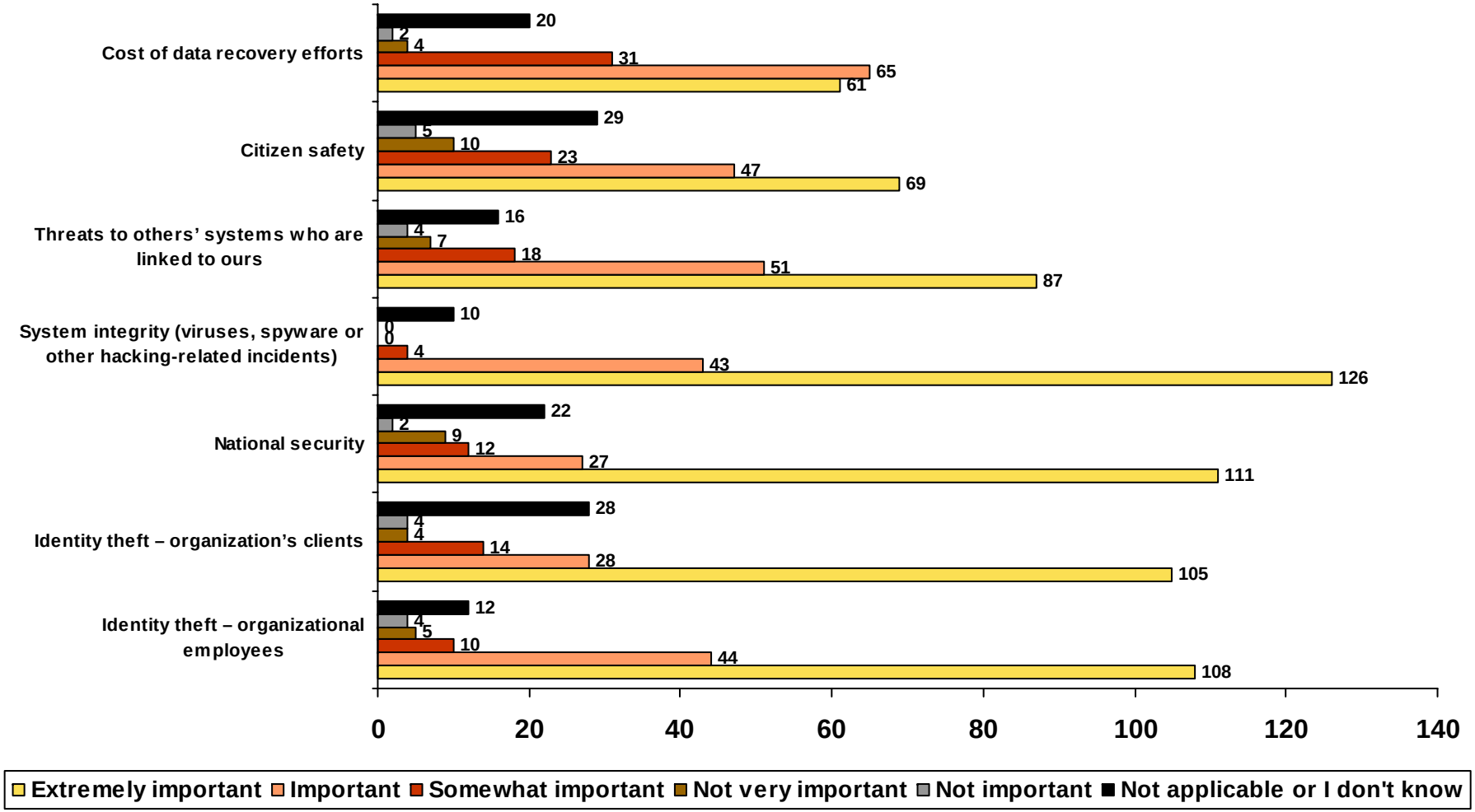
In accordance with OMB's recommendations for responding to data breaches that could lead to identity theft, has your agency (select all that apply):



In accordance with OMB's recommendations for responding to data breaches that could lead to identity theft, has your agency (select all that apply):

Choice	Count	Percent of Sample Asked	Percent of Total Sample
Identified a core response group that can be convened in the event of a breach	101	55.2%	55.2%
Trained a core response group to engage in a risk analysis to determine whether the incident poses problems related to identity theft	79	43.2%	43.2%
Determined how it would respond and notify those who might be affected	106	57.9%	57.9%
None of the above	43	23.5%	23.5%

Please rate the importance of the following implications for breaches in data security at your organization:



Please rate the importance of the following implications for breaches in data security at your organization: - Insert Category

Topic	Extremely important	Important	Somewhat important	Not very important	Not important	Not applicable or I don't know
Identity theft – organizational employees	108	44	10	5	4	12
Identity theft – organization's clients	105	28	14	4	4	28
National security	111	27	12	9	2	22
System integrity (viruses, spyware or other hacking-related incidents)	126	43	4	0	0	10
Threats to others' systems who are linked to ours	87	51	18	7	4	16
Citizen safety	69	47	23	10	5	29
Cost of data recovery efforts	61	65	31	4	2	20