Deloitte.

2012 Deloitte-NASCIO Cybersecurity Study

State Officials Questionnaire - Aggregate Results (NASACT)

November, 2012

Note: This document has been produced for the sole use of National Association of State Chief Information Officers (NASCIO) and National Association of State Auditors, Comptrollers and Treasurers(NASACT) to provide a view of NASACT's affiliated members' aggregated response for the 2012 Deloitte-NASCIO cybersecurity survey.

The 2012 Deloitte-NASCIO cybersecurity study – An overview

Objectives

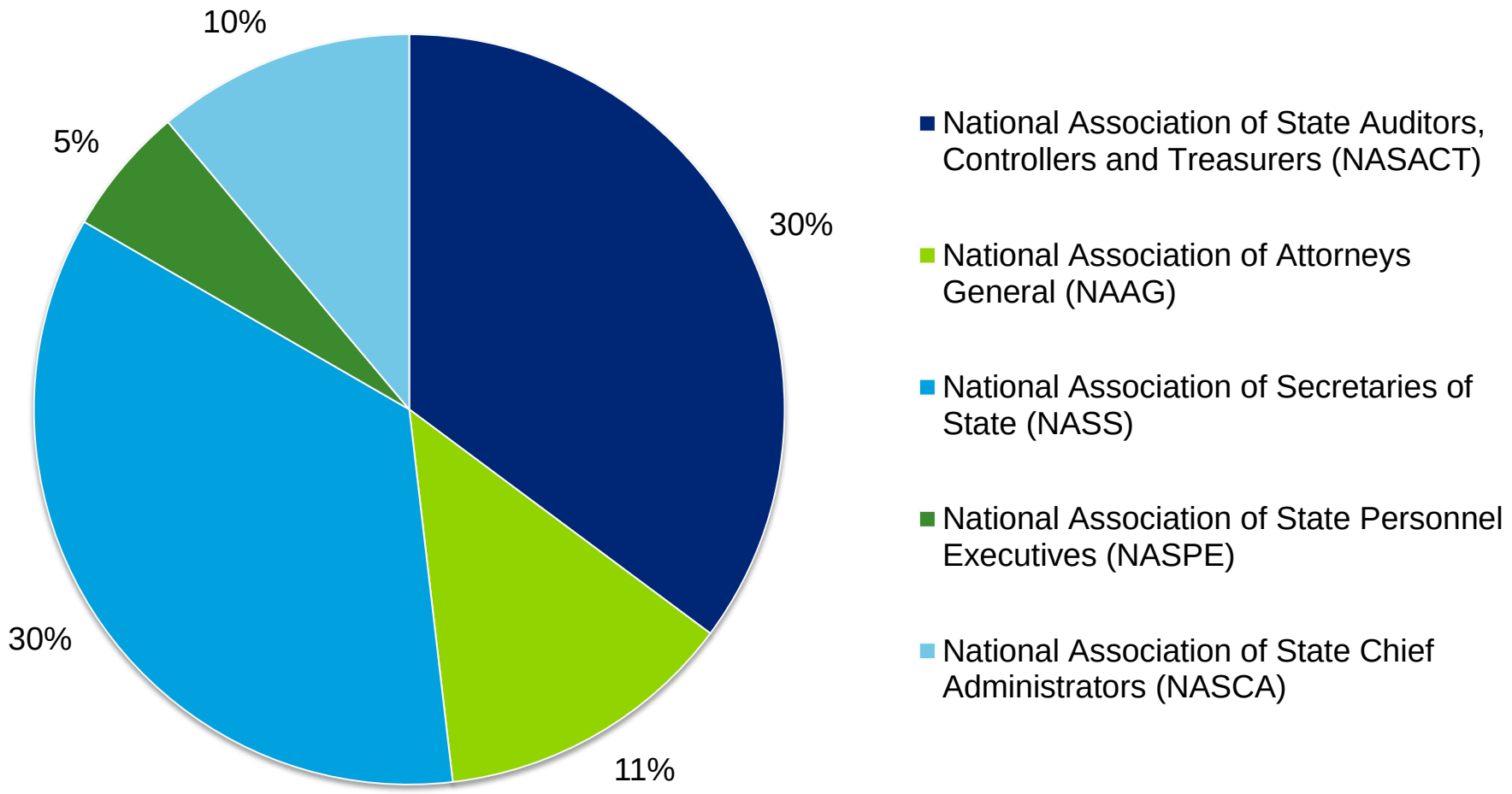
- Assess state of enterprise cybersecurity programs. Compare with:
  - 2010 Deloitte-NASCIO cybersecurity study.
  - Deloitte's 2012 Global Financial Services Industry security study.
- Identify additional trends in the states
  - Preparedness to secure emerging Mobile and Cloud adoption.
  - NASCIO security services taxonomy1 based maturity model.
- Provide state leadership with insights and identify trends to help them in making informed, strategic cybersecurity decisions.
- Assess awareness level with an expanded business survey respondents.

Participation

- 50 state CISOs (or equivalents) responded to the CISO version of the survey, which consisted of 64 questions.
- 63 state officials provided insight with business stakeholders' perspectives on cybersecurity. The participant affiliations included:
  - National Association of State Auditors, Controllers and Treasurers (NASACT).
  - National Association of Attorneys General (NAAG).
  - National Association of Secretaries of State (NASS).
  - National Association of State Personnel Executives (NASPE).
  - National Association of State Chief Administrators (NASCA).

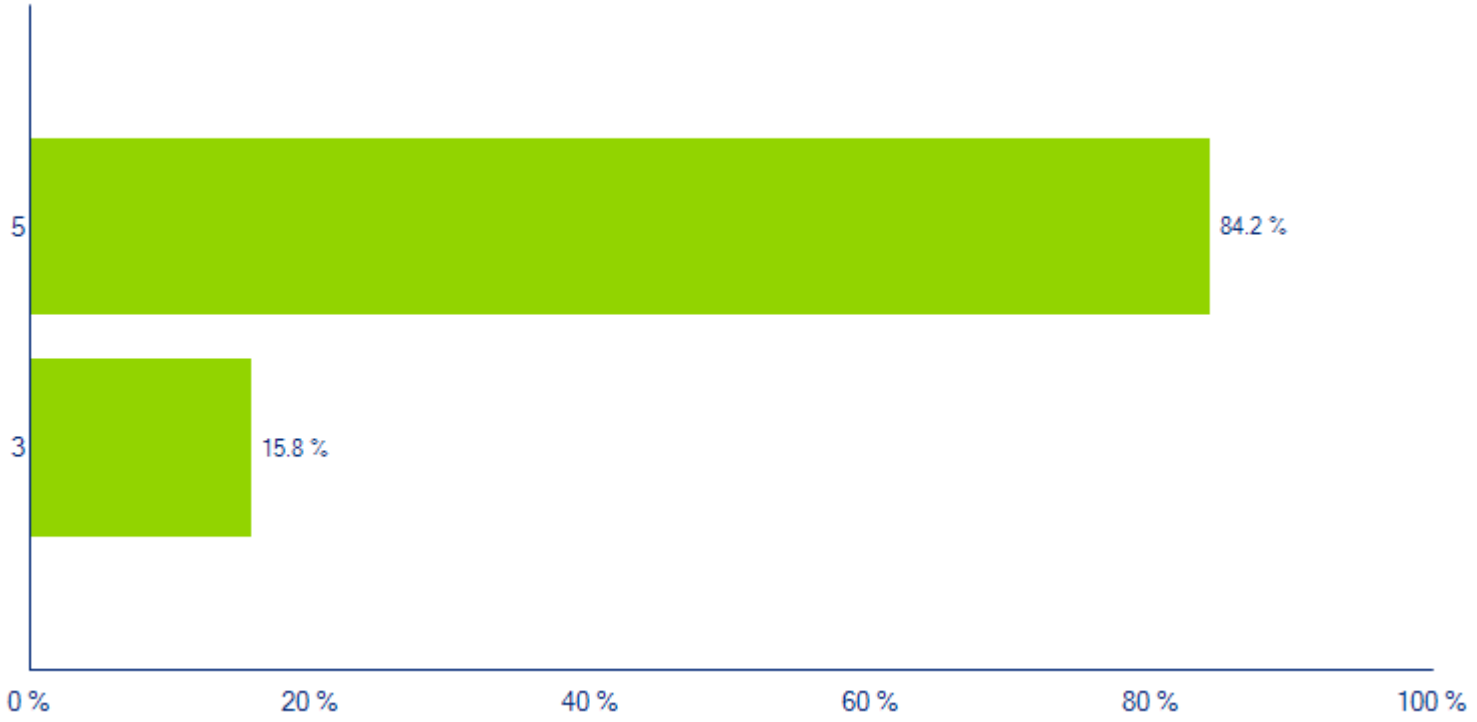
Note: This aggregate report provides a high level comparison of similar questions between the State Officials and the CISO versions of the 2012 Deloitte-NASCIO cybersecurity study.

Q4 Please indicate if you are affiliated with one of the following associations.



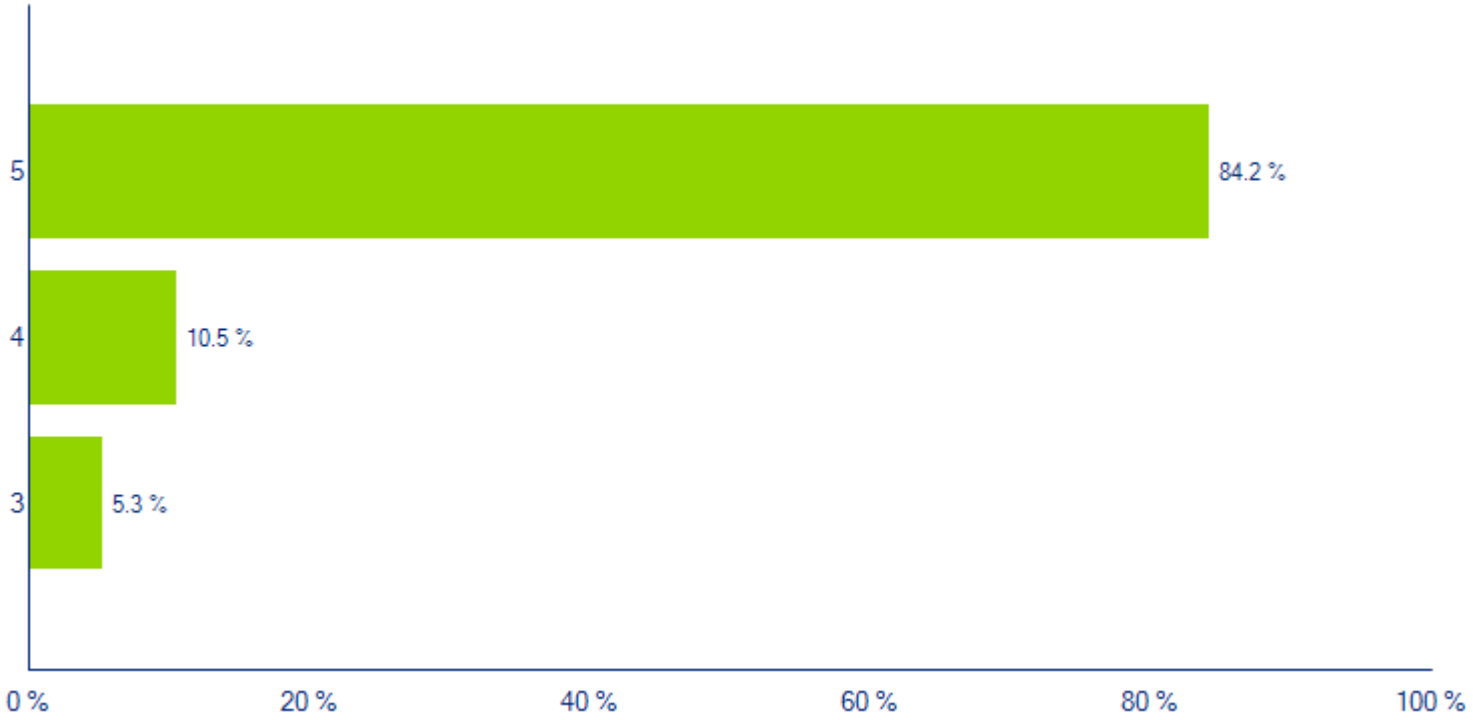
63 state officials participated in the 2012 Deloitte-NASCIO cybersecurity study.

Q5 On a scale of 1 to 5, please indicate how you consider the importance of information security to your **state government**? (1 = Least Important, 5 = Most Important).



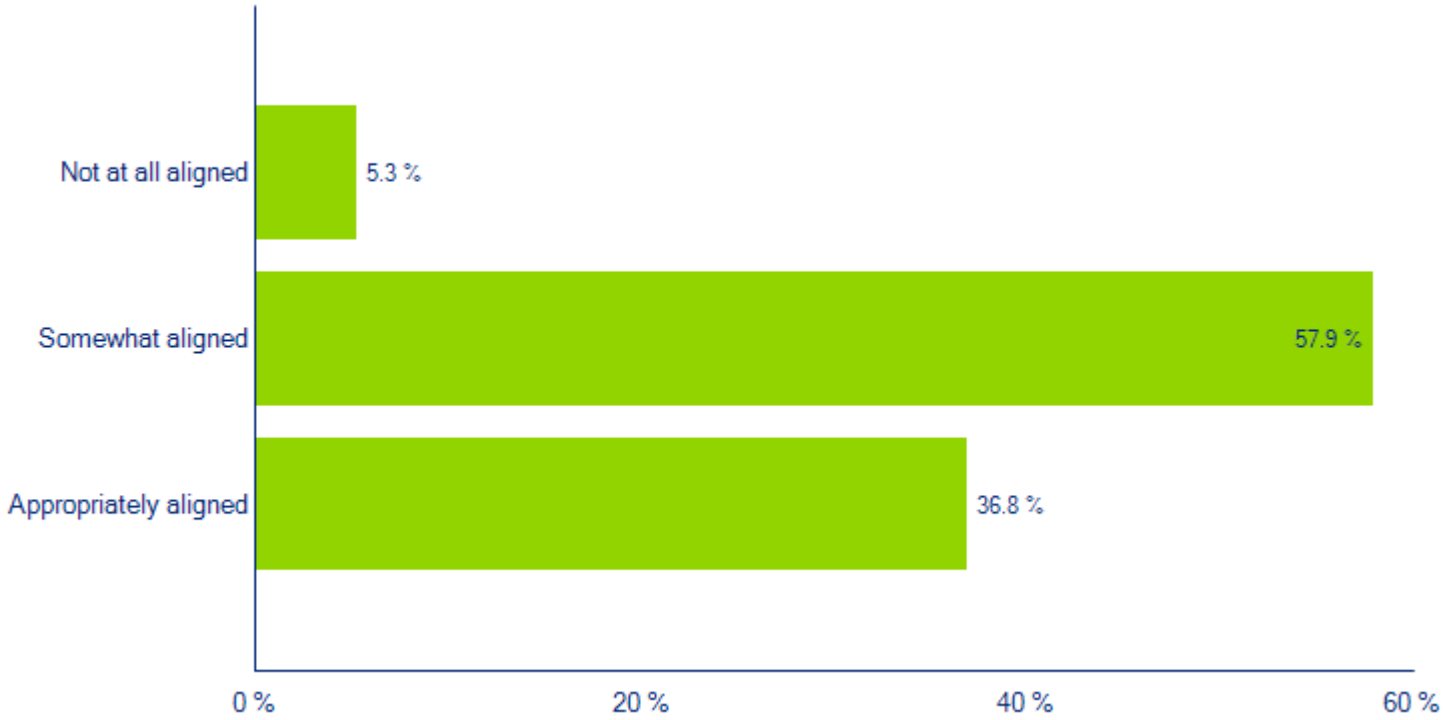
92% of state officials feel that cybersecurity is very important for the state (4 or 5).

Q6 On a scale of 1 to 5, please indicate how you consider the importance of information security to your **agency/office?** (1 = Least Important, 5 = Most Important).



92% of state officials feel that cybersecurity is very important for the agency/office (4 or 5).

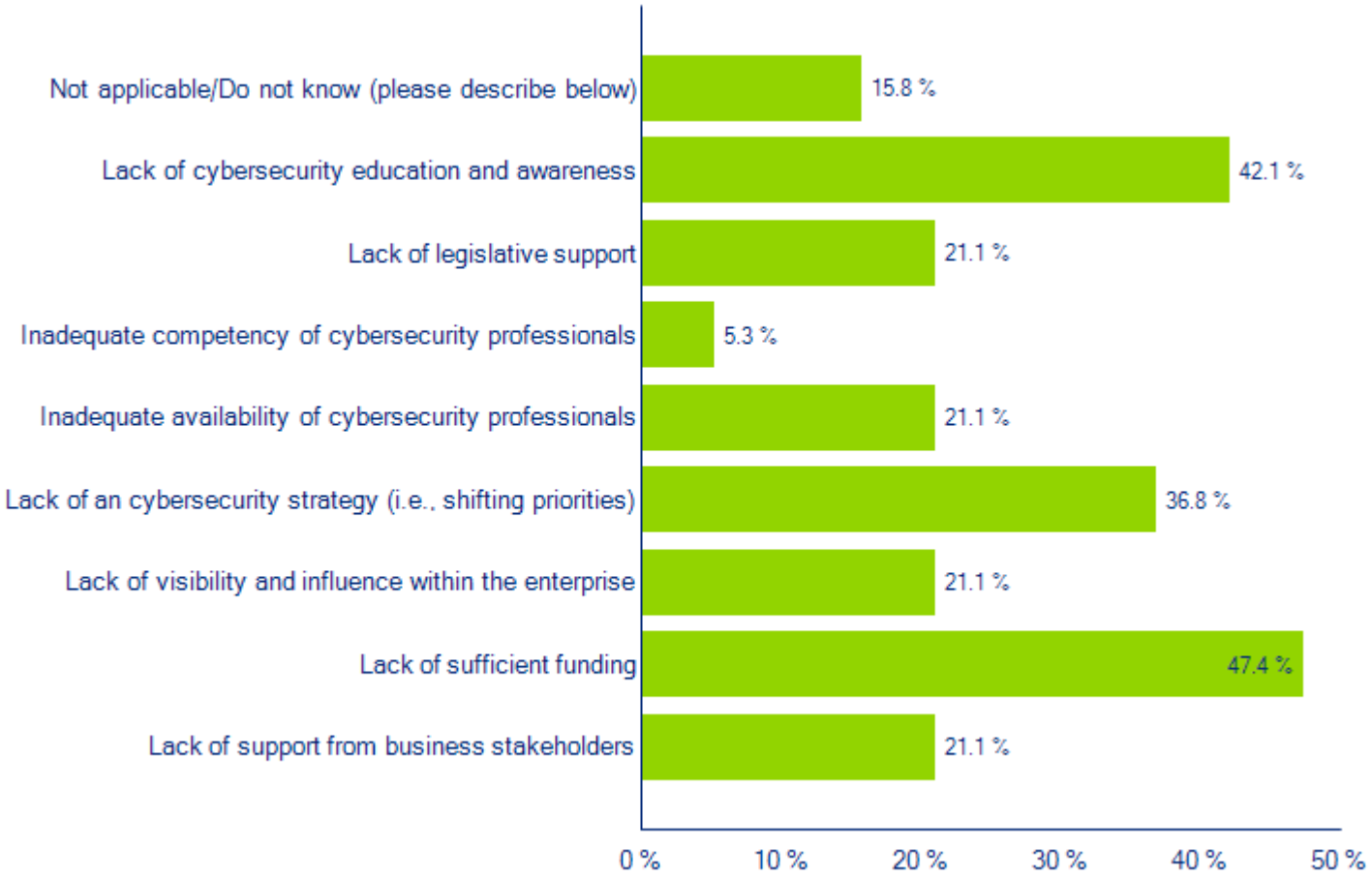
Q7 In your opinion, are business and cybersecurity initiatives aligned with each other in your agency/office?



74% of the Chief Information Security Officers (CISOs) and 52% of the state officials indicated that their business and cybersecurity initiatives are somewhat aligned.

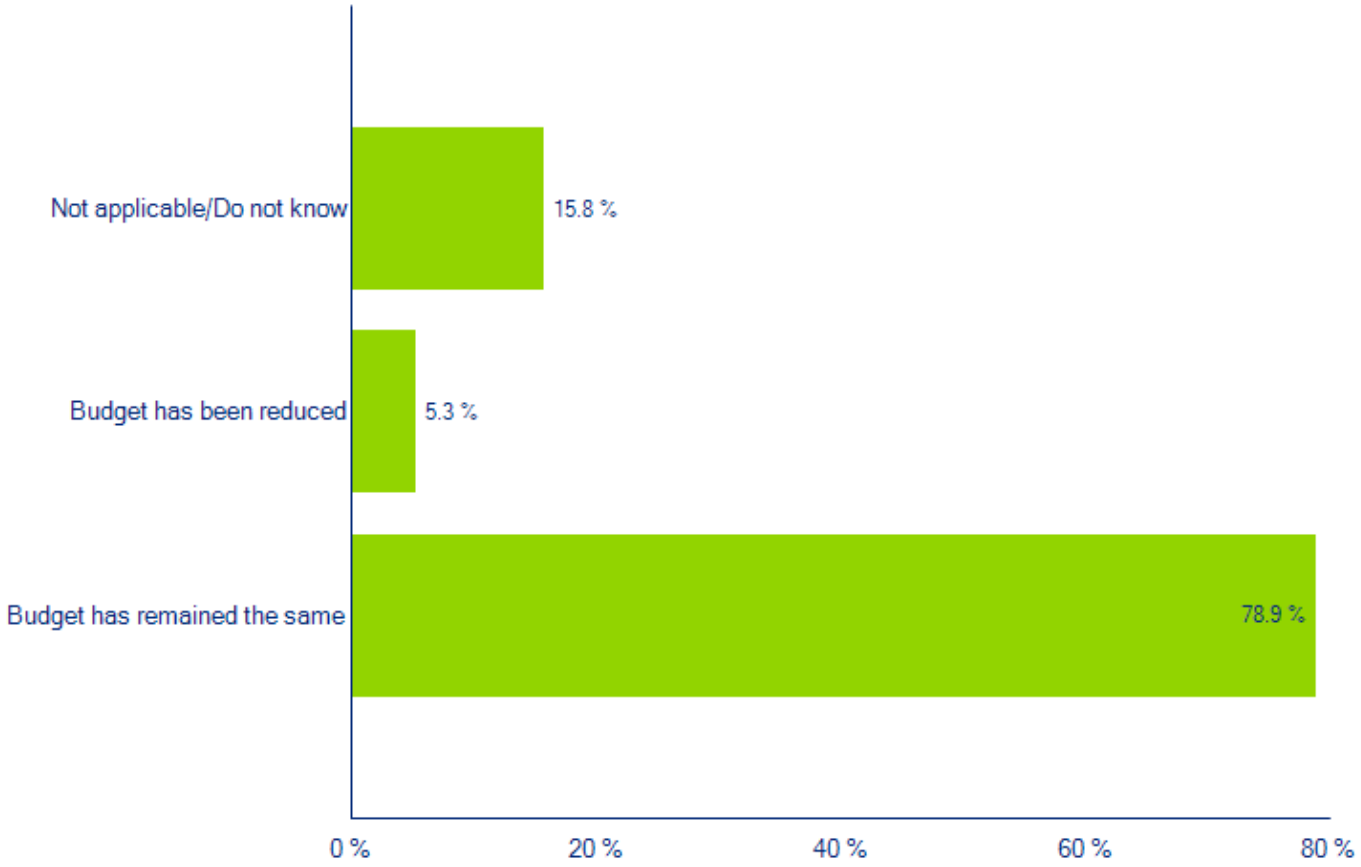
16% of the CISOs and 37% of the state officials indicated that the initiatives are appropriately aligned.

Q8 What major barriers does your agency/office face in addressing cybersecurity?



The CISOs (86%) and state officials (54%) indicated that their major barrier in addressing cybersecurity is lack of sufficient funding.

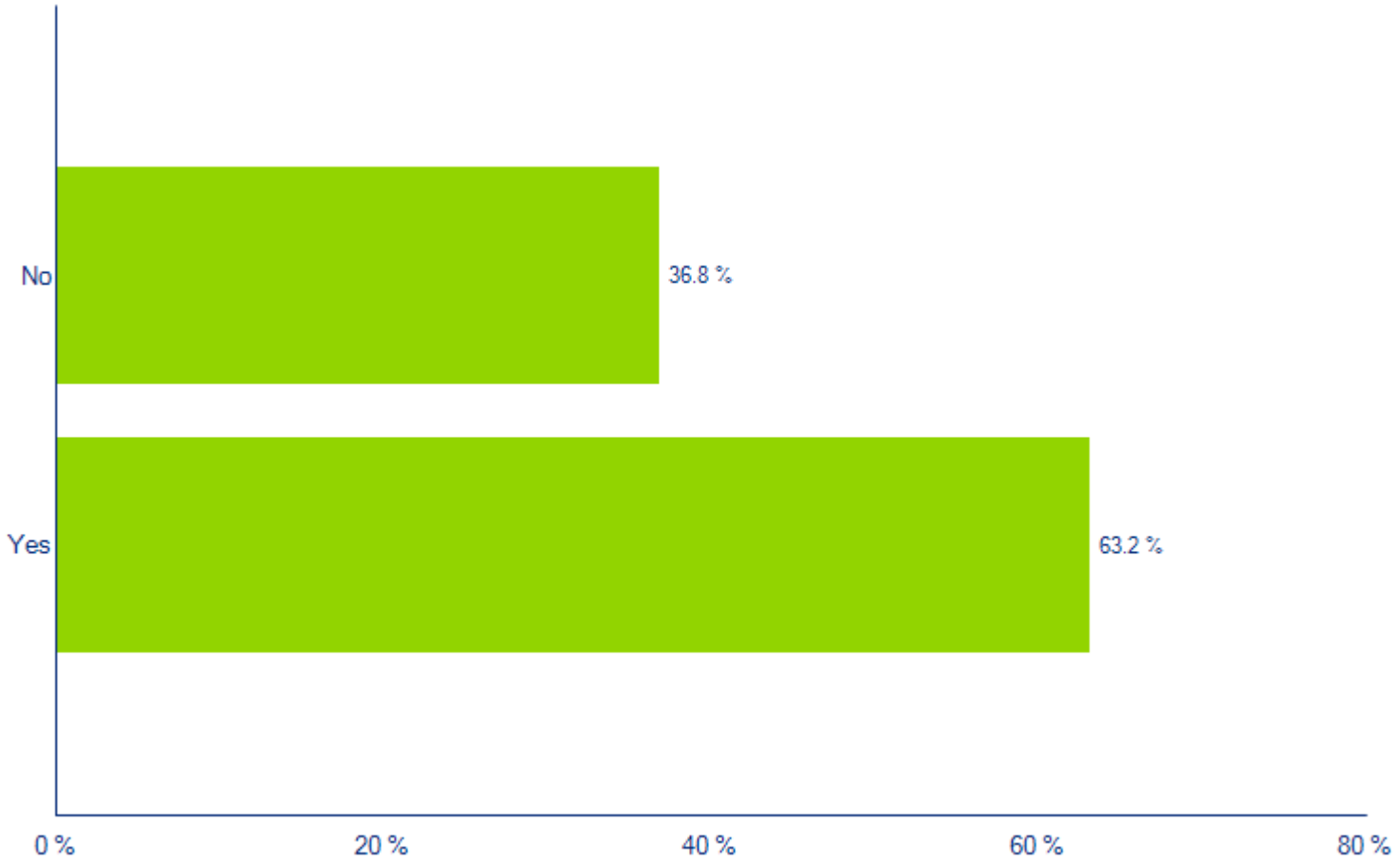
Q9 To the extent of your visibility, please characterize the year-over-year trending in your cybersecurity budget for your agency/office for the years 2010 and 2011.



44% of the CISOs and 54% of the state officials indicated that the cybersecurity budget has remained the same year-over-year.

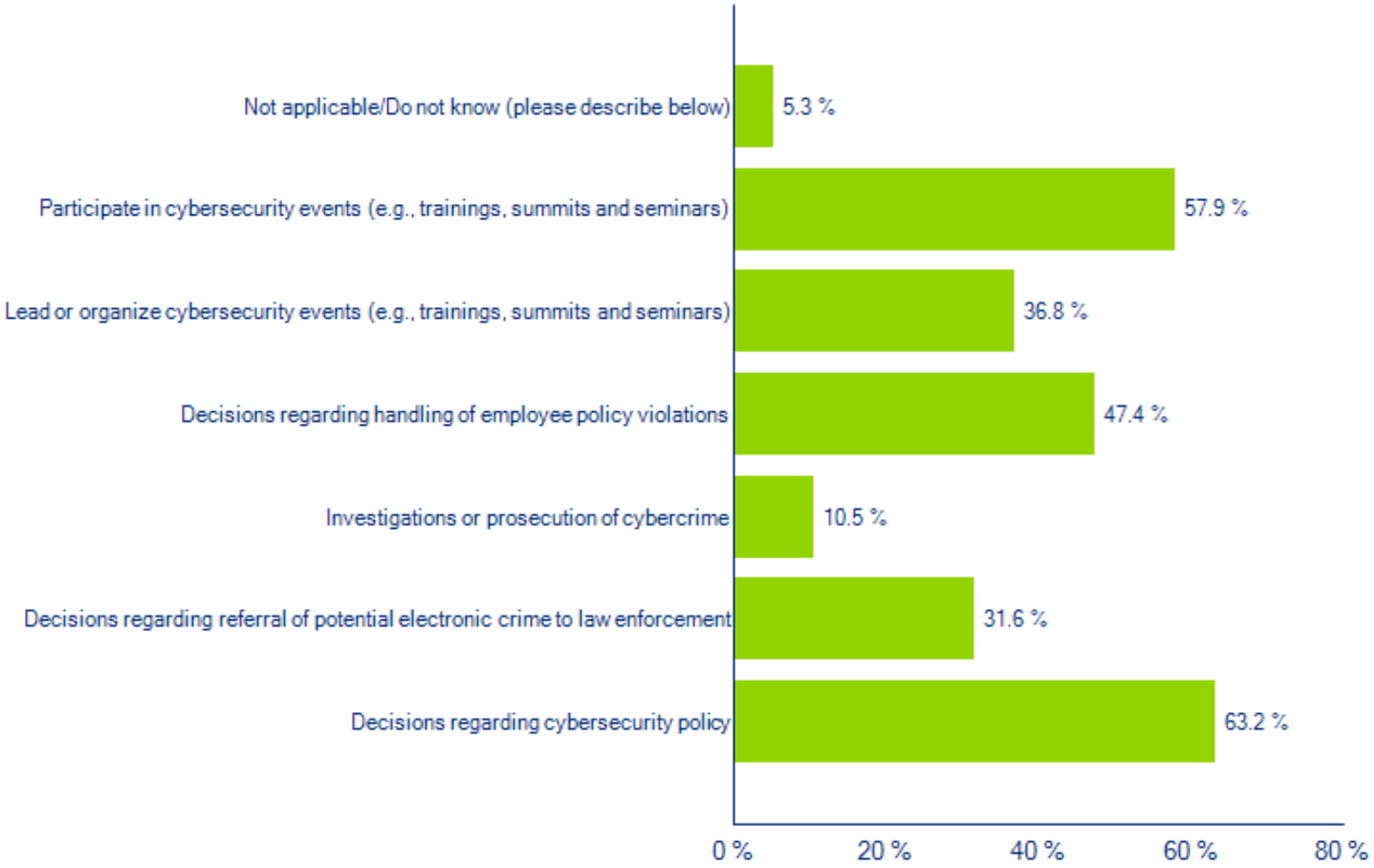
34% of the CISOs and 13% of the state officials indicated a reduction in the cybersecurity budget.

Q10 Do your employees and contractors receive cybersecurity education or awareness training at least annually?



51% of the CISOs and 48% of the state officials indicated that they provide cybersecurity training (at least annually) for employees and contractors.

Q11 Are you personally involved in any of the following in your agency/office?

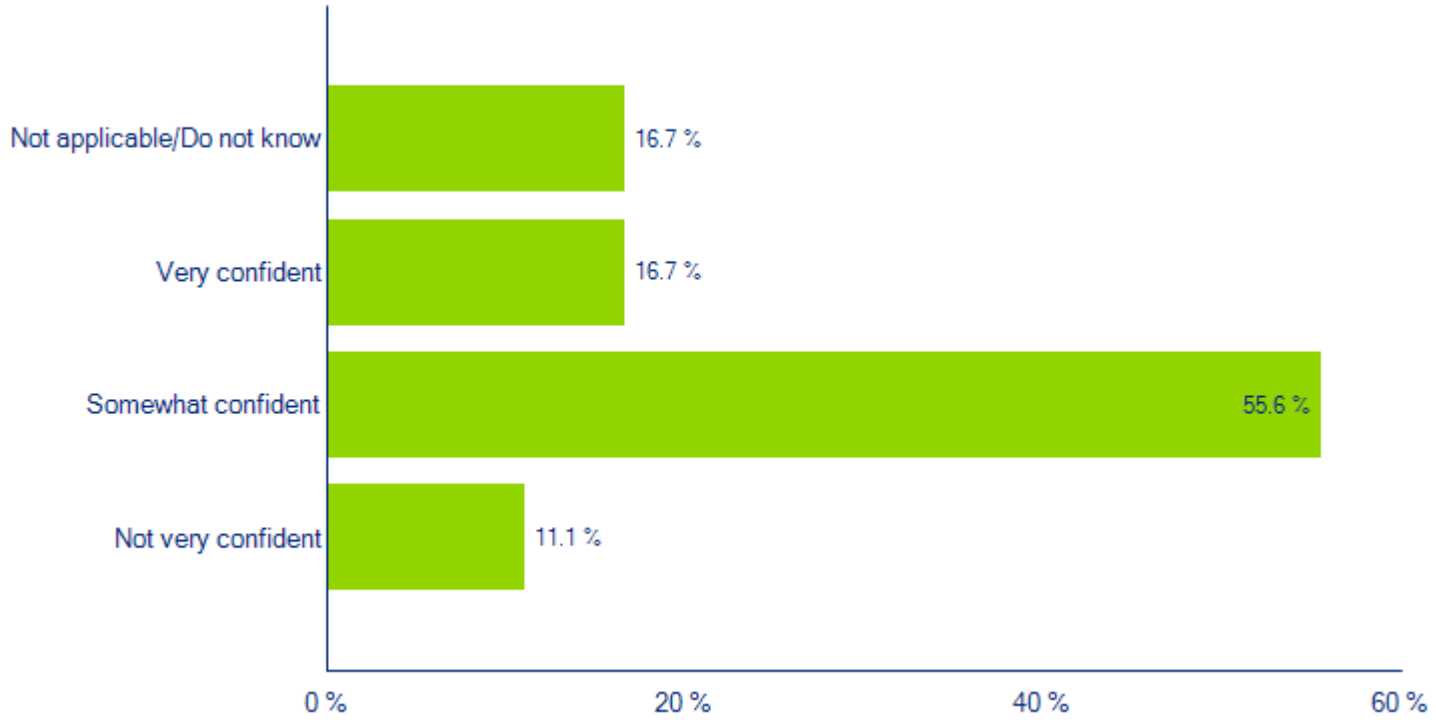


68% of the state officials indicated that the are involved in decisions regarding cybersecurity policy.

Q12 Which of the following are the top three privacy concerns to your agency/office?

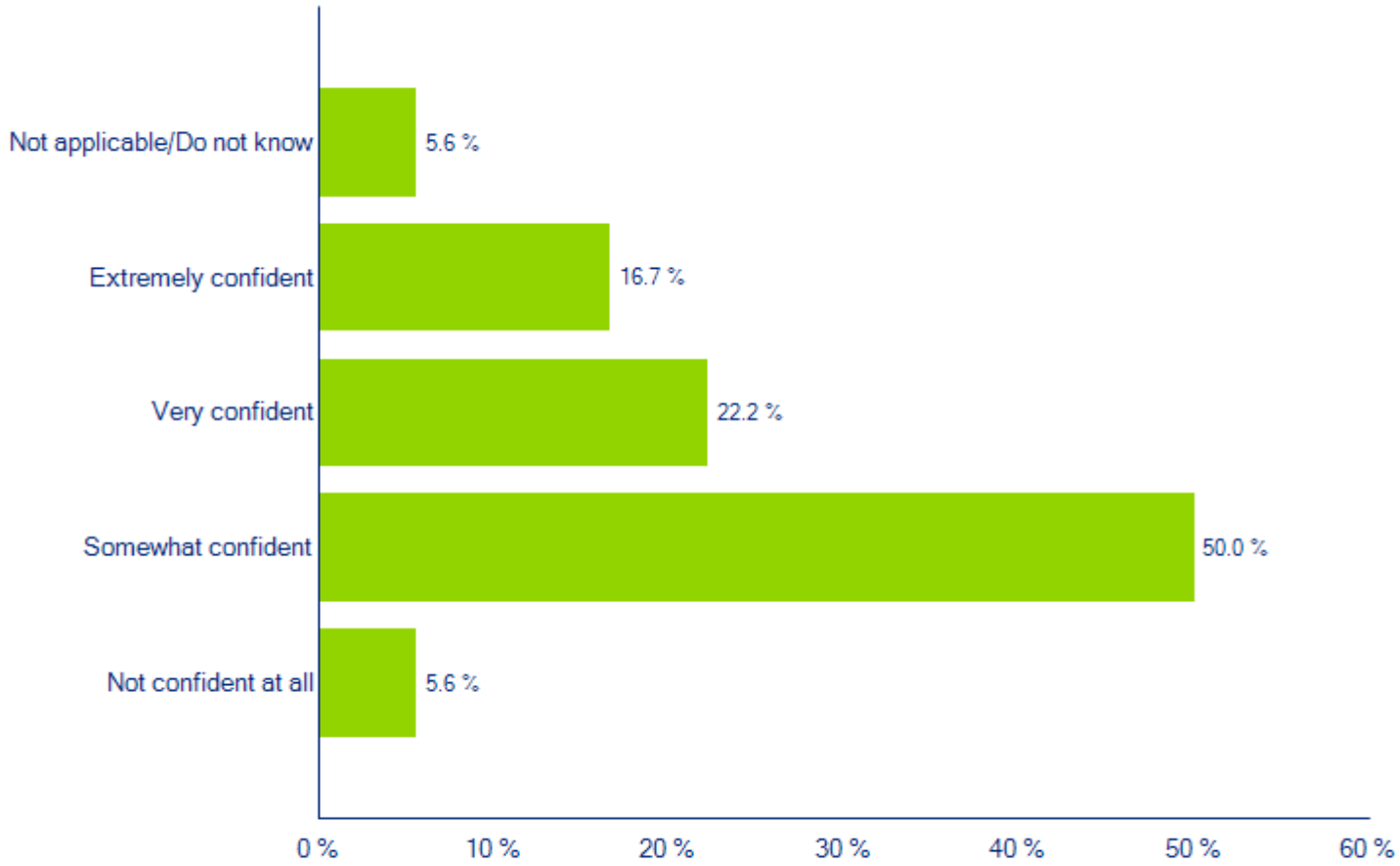
CISOs (86%) and state officials (82.5%) indicated that their top privacy concern is the unauthorized access to personal information.

Q13 How confident are you in the cybersecurity practices of your third parties (contractors, service providers, business partners)?



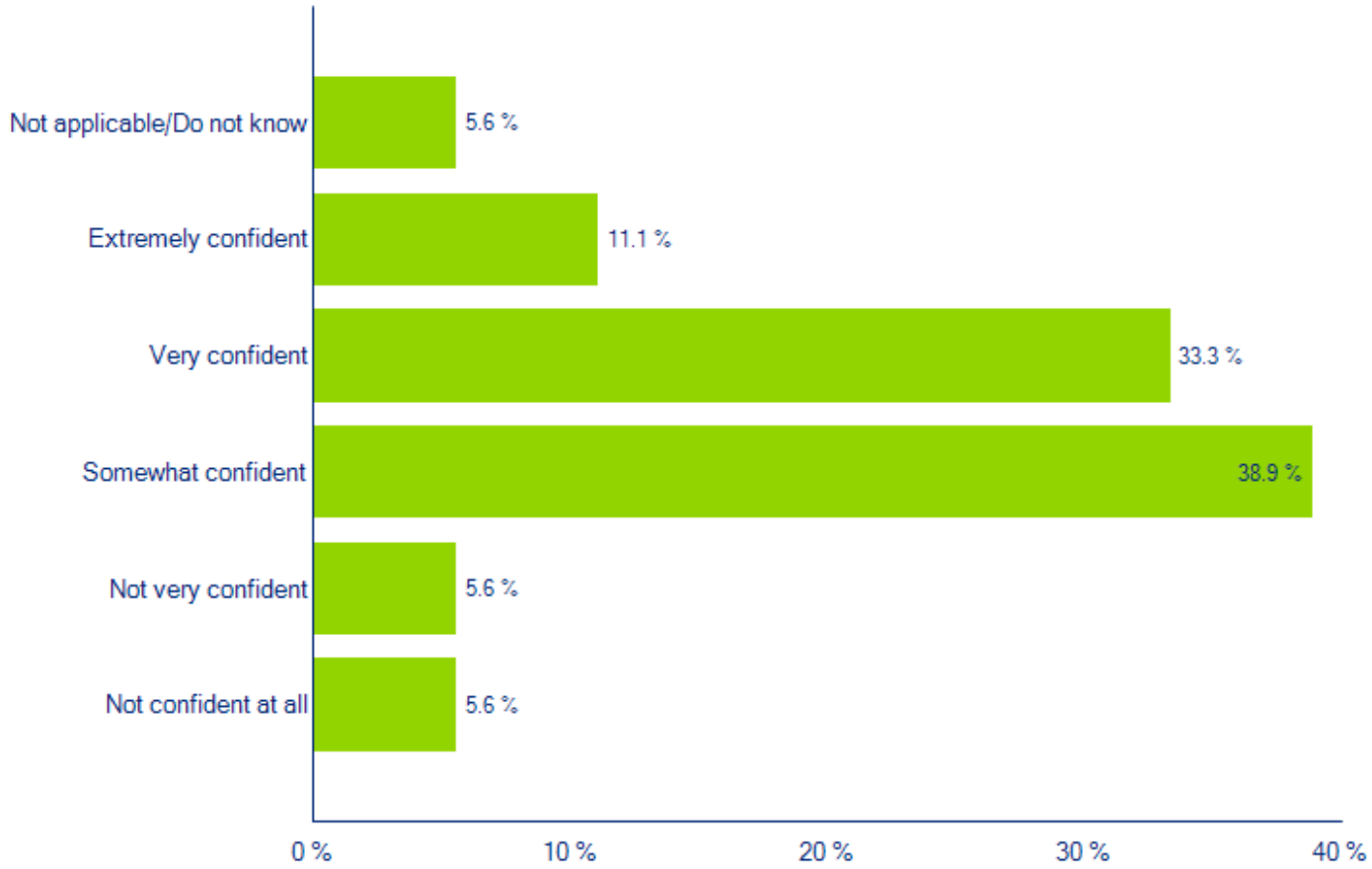
74% of the CISOs and only 53% of the state officials indicated they are somewhat confident in the cybersecurity practices of their third parties.

Q14a Indicate your level of confidence of your agency/office's measures to protect information assets from threats originating internally.



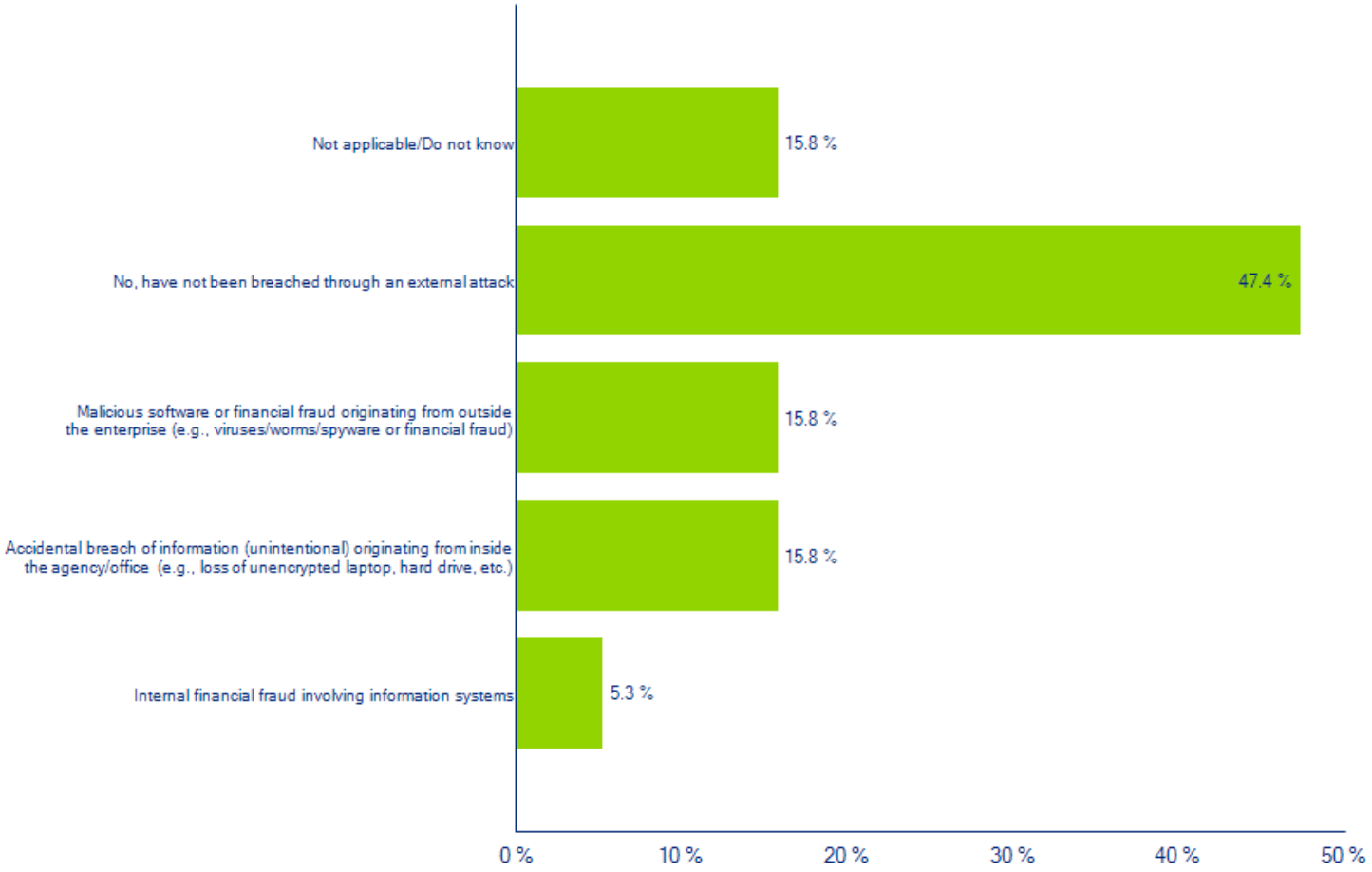
Only 10% of the CISOs are very confident in protecting state's assets against internal threats whereas 29% of the State Officials very confident of their agency's measures to protect against internal threats.

Q14b Indicate your level of confidence of your agency/office's measures to protect information assets from threats originating externally.



Only 24% of the CISOs are very confident in protecting state's assets against external threats whereas 37% of the State Officials very confident of their agency's measures to protect against external threats.

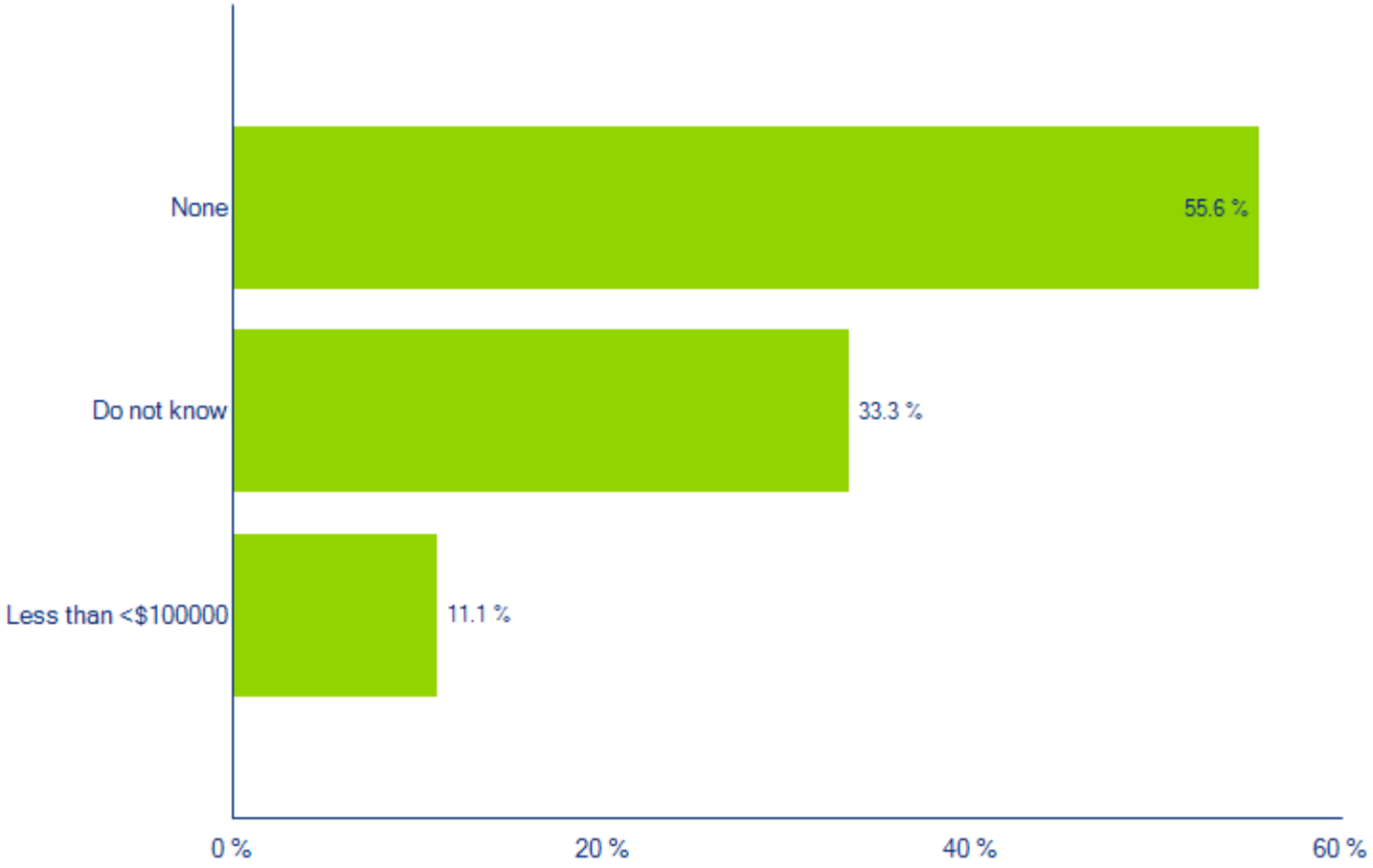
Q15 Please indicate the types of security breaches that has impacted your agency in the past 12 months?



58% of the CISOs and 22% of the state officials indicated that the primary cause of external breaches was due to malicious software originating from outside the enterprise.

44% of the state officials and only 18% of the CISOs indicated that their agency has not been breached by external attacks in the past 12 months.

Q16 Over the past 12 months, please provide an estimate of the cost of handling security breaches in your organization.



Contacts

NASCIO

Doug Robinson

Executive Director

+1 859-514-9153

drobinson@AMRms.com

Charles Robb

Senior Policy Analyst

+1 859-514-9209

crobb@AMRms.com

Deloitte

Srini Subramanian

Principal

Security & Privacy

Deloitte & Touche LLP

+1 717-651-6277

ssubramanian@deloitte.com

Deloitte.

About NASCIO

The National Association of States CIOs is the premier network and resource for state CIOs and an effective advocate for technology policies at all levels of government. State members are senior officials from any of the three branches of state government who have executive-level and statewide responsibility for information resource management. Representatives from federal, municipal, and international governments and other state officials participate in the organization as associate members. Private-sector firms and non-profit organizations may join as corporate members.

AMR Management Services provides NASCIO's executive staff. For more information about AMR visit www.AMRms.com.

NASCIO represents state chief information officers and information
Technology executives and managers from state governments across the United States.

For more information visit www.nascio.org.