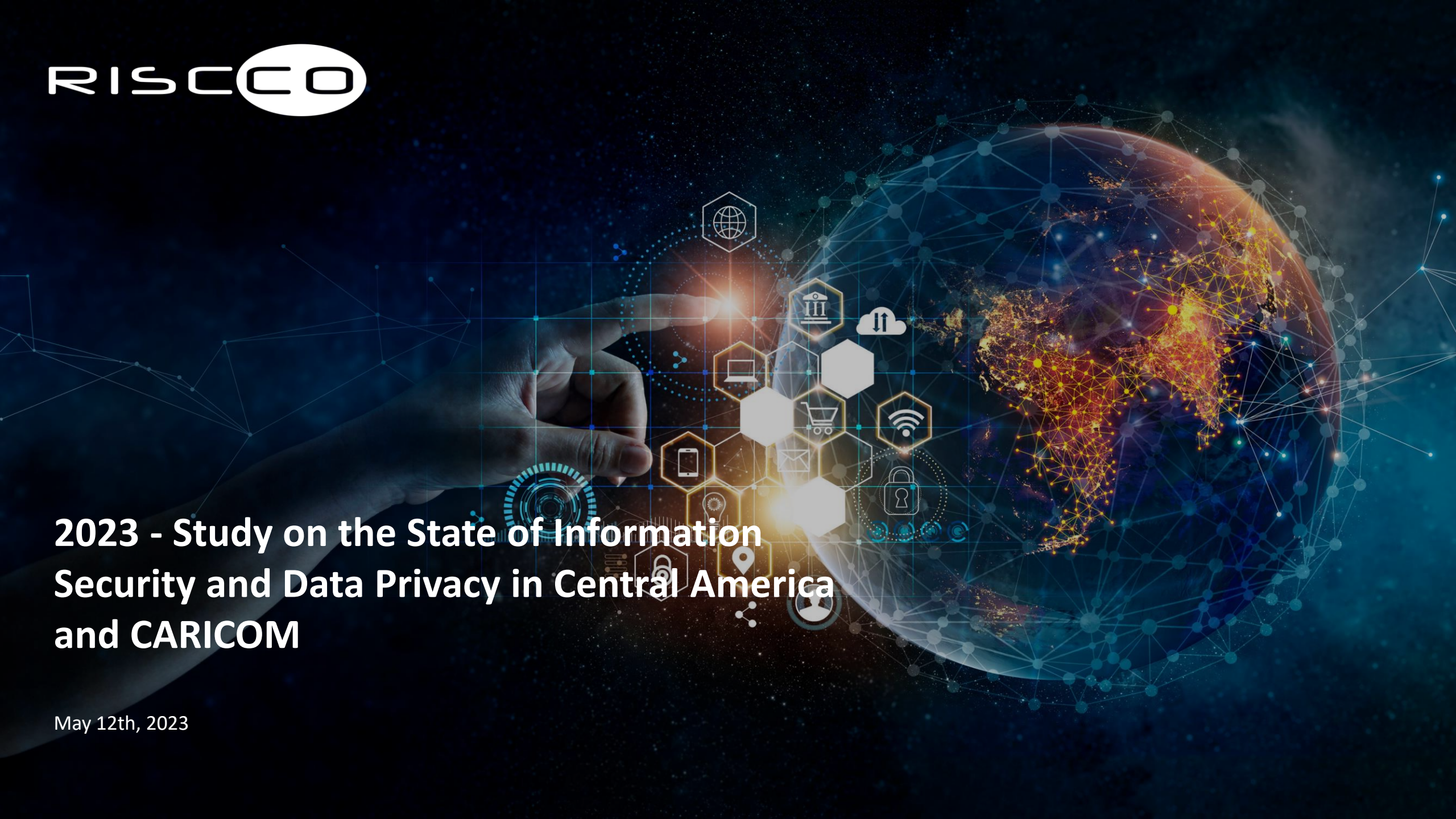


2023 - Study on the State of Information Security and Data Privacy in Central America and CARICOM

May 12th, 2023

CONTENTS

RISCCO

EXECUTIVE SUMMARY

The “2023 - Study on the State of Information Security and Data Privacy in Central America and CARICOM" was conducted from March 1 to April 28, 2023 with 163 participants from Central America, CARICOM and the Dominican Republic. The study aims to show the maturity of information security initiatives in the region.

While it is true that the study shows an important evolution in the adoption of technologies for the protection of information and networks, it reflects that the efforts of organizations to maintain a mature level of security are far from the degree of complexity, sophistication and frequency of threats and technological risks faced by organizations today. This statement is supported due to the following:

- Limited existence of an Information Security, Cybersecurity or Technological Risk Committee among the participants. Only 42% confirmed its existence. Its absence would greatly limit senior executives, regulators and stakeholders from knowing the technological risks and threats to which the organization is exposed, understanding the level of effectiveness of controls and effective decision making for the protection of technological resources.

EXECUTIVE SUMMARY

- 88% of the participants stated that they use obsolete and not very avant-garde strategies to raise awareness of information security among end users. This is worrying, since end users are the weakest link in the information security chain.

- 62% of the participants indicated that they do not have an updated risk map showing the impact and probability of technological risks that may affect the organization's operations.

- The use of cutting-edge technological tools that include artificial intelligence or machine learning to strengthen information security strategies is low. Only 22% indicated using this type of technology.

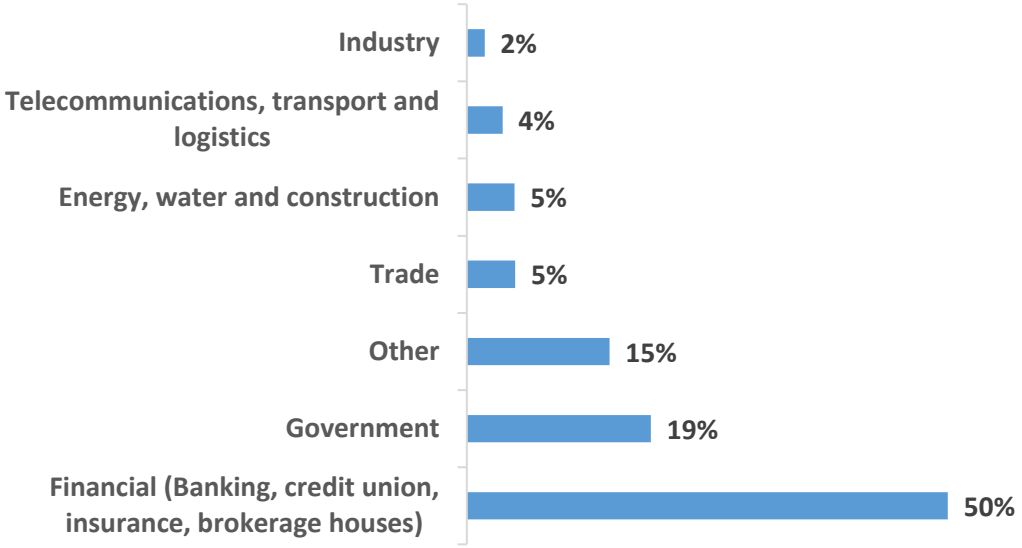
The study reflects some positive information security initiatives among the participants. However, they are not enough.

We respectfully invited participants to do their benchmarking to identify areas that need attention in their organization.

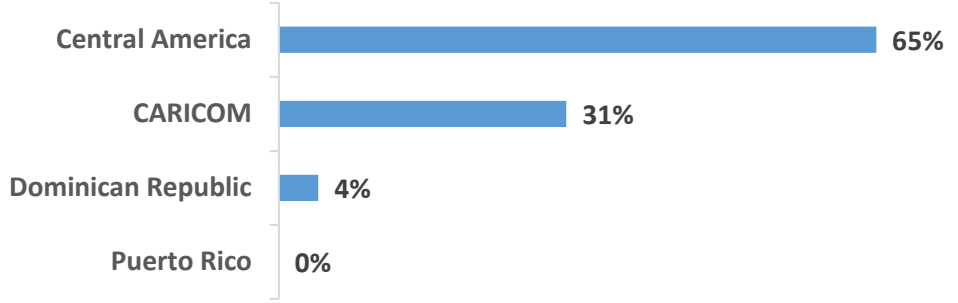
DISTRIBUTION OF PARTICIPANTS

DISTRIBUTION OF PARTICIPANTS

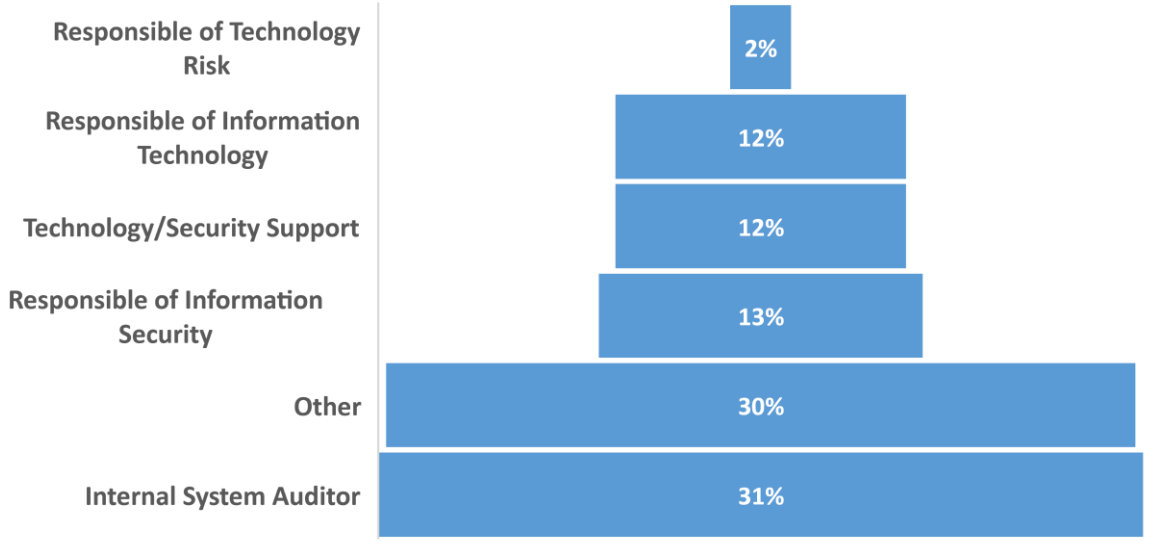
Economic Sector



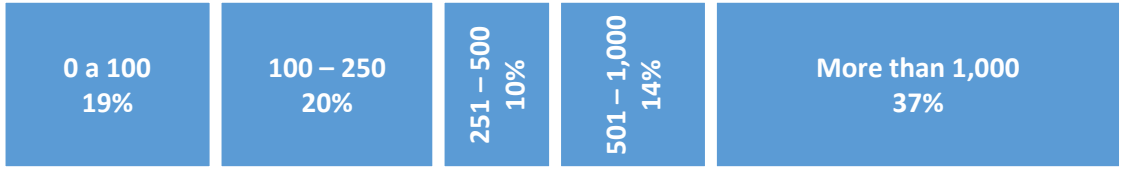
Region



Role within the organization



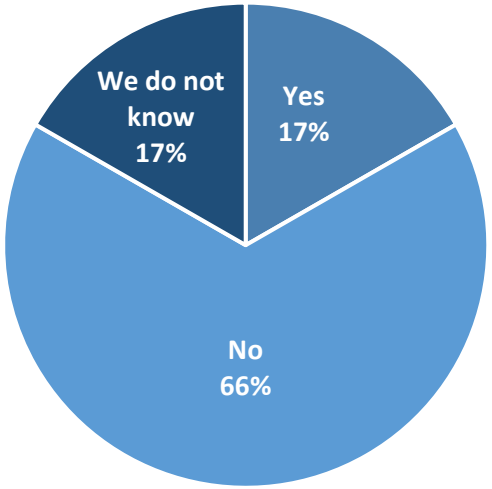
Number of Collaborators




SECURITY
MANAGEMENT
AND
GOVERNANCE

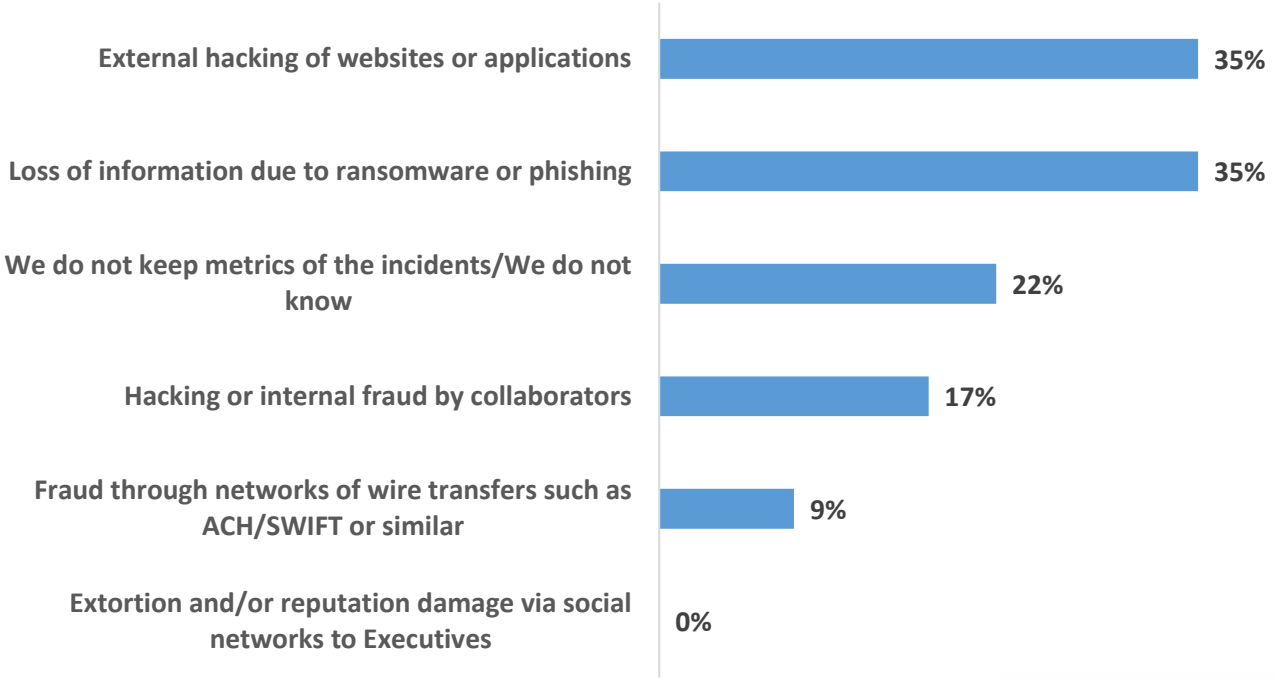
INFORMATION SECURITY AND INCIDENT MANAGEMENT

Has your organization suffered a security incident in the last 12 months?

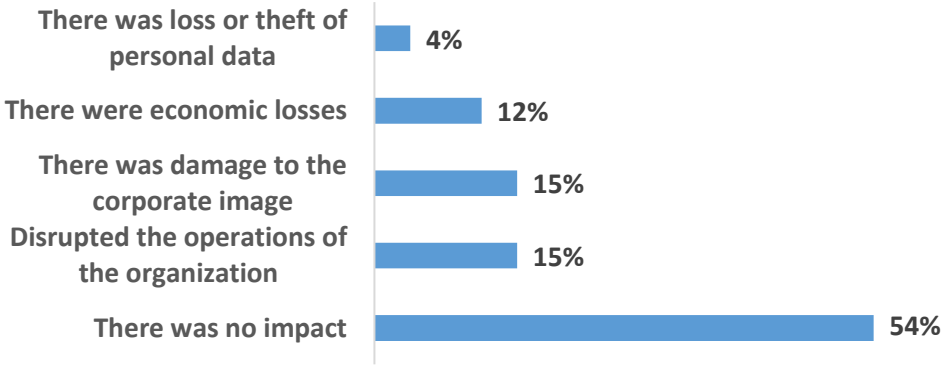


- It is of concern that 17% indicate that they do not know if they have experienced a security incident.
- Of the participants who suffered an incident, 31% suffered damage to image or disruption to operations.

What type of incidents has your organization experienced in the last 12 months?

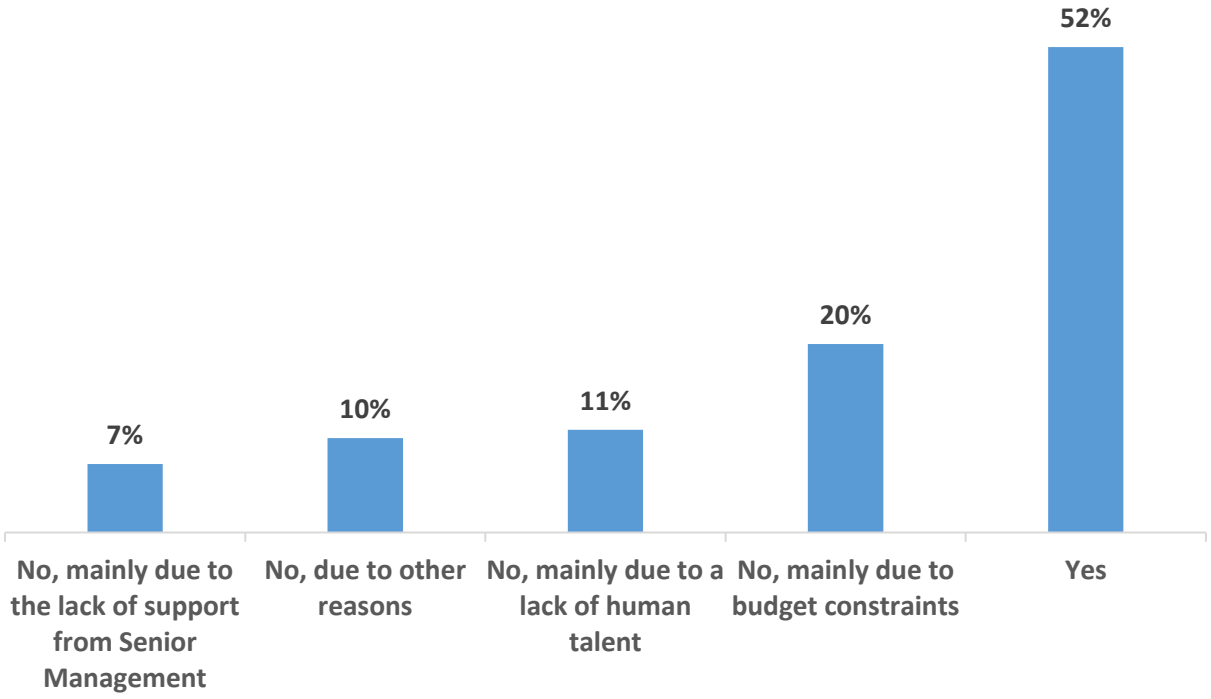


If a critical security incident occurred in your organization in the last 12 months, what was its impact?

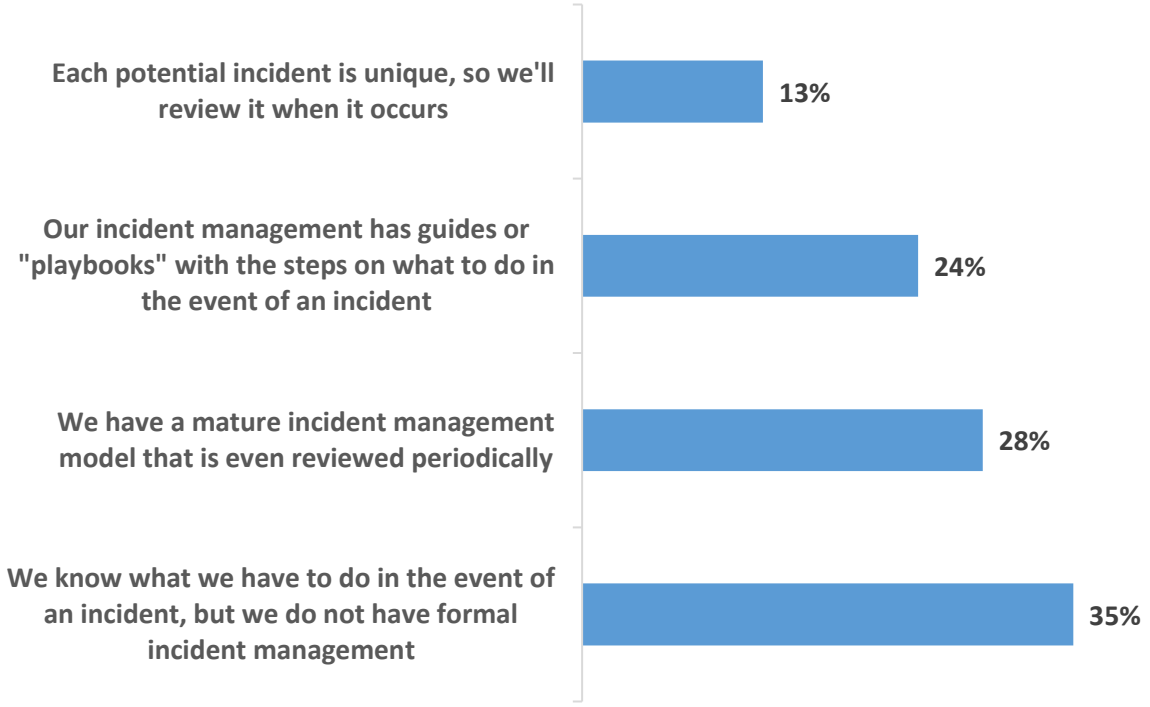


INFORMATION SECURITY AND INCIDENT MANAGEMENT

Do you feel that the information security function is meeting the needs of your organization?



Which of the following statements would best describe your organization's security incident management strategy?

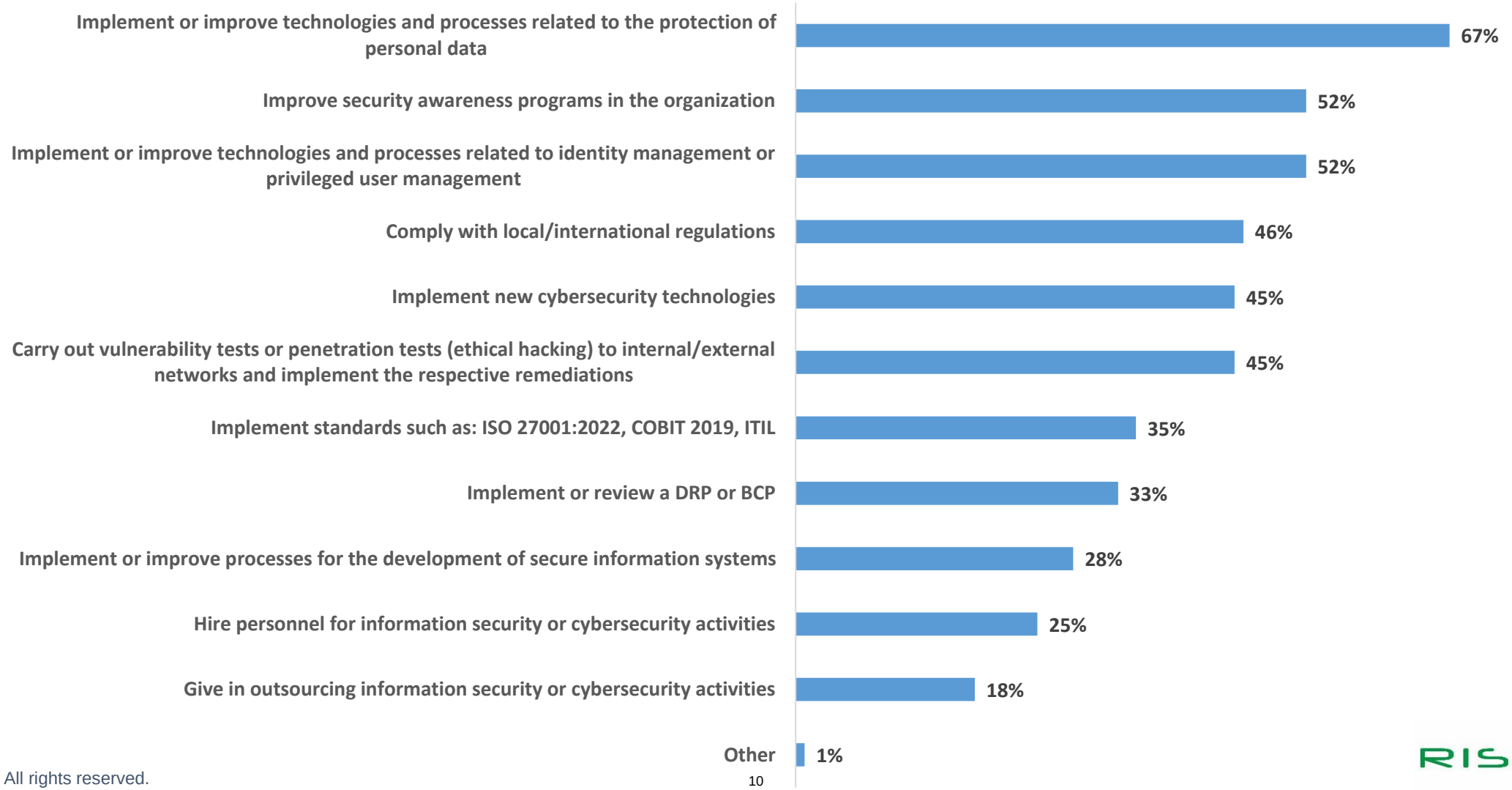


In a digitally interconnected society where cyberattacks occur on a daily basis, this is of concern:

- That 48% feel that information security does not meet the organization's needs.
- That only 28% have a security incident management model.

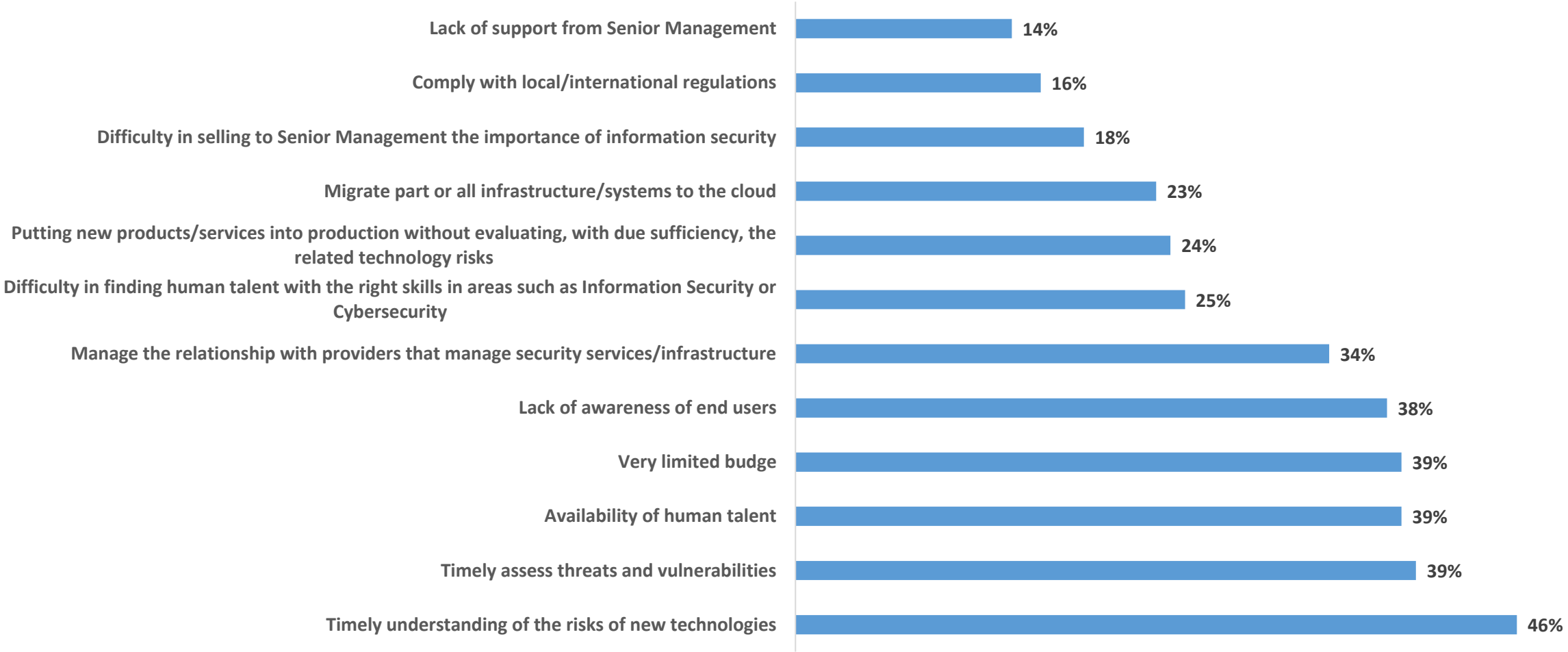
GOVERNANCE

In 2023, what do you think will be the main information security priorities in your organization



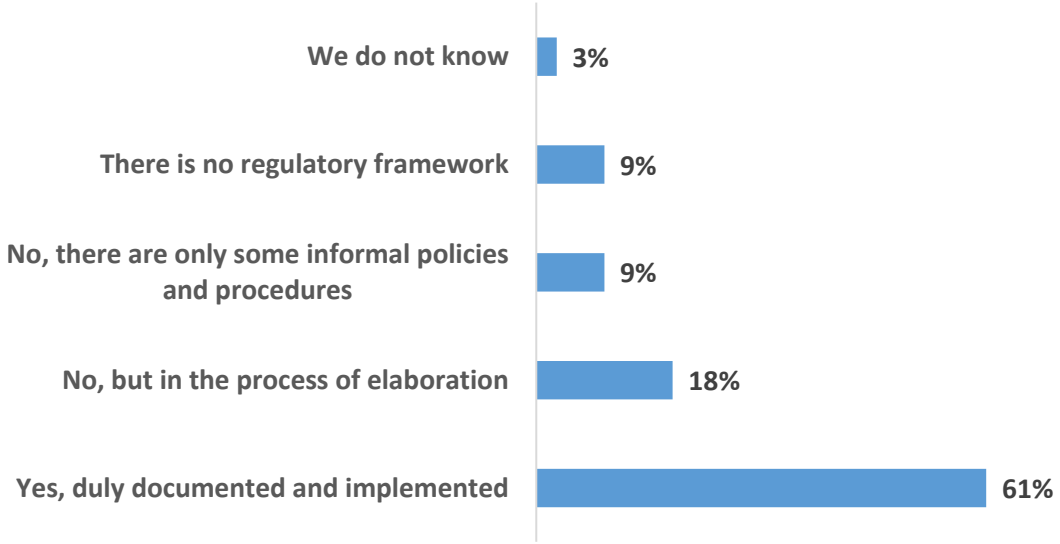
GOVERNANCE

In 2023, what do you consider will be the main challenges to improve information security in the organization?

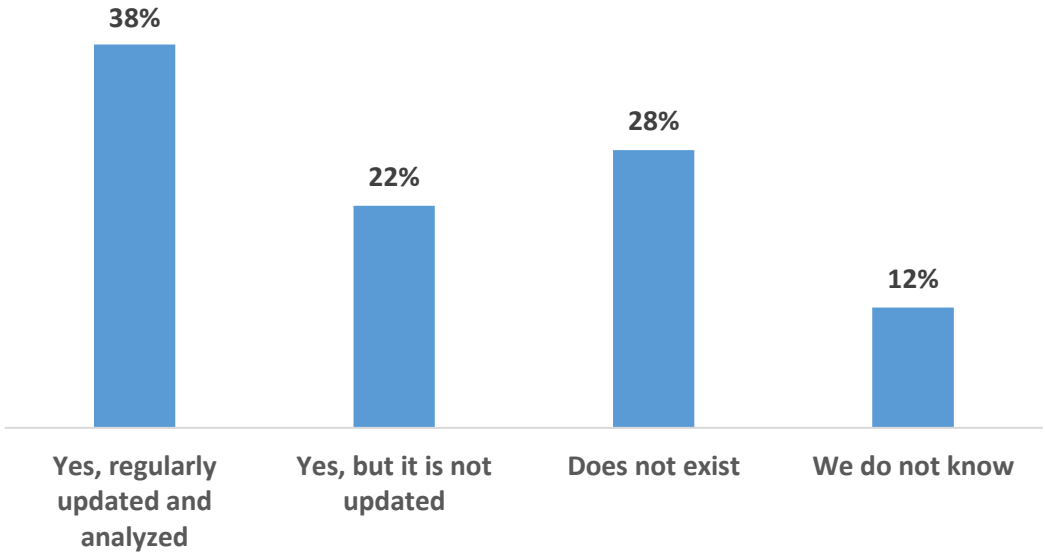


GOVERNANCE

Does your organization have a regulatory framework (policies, processes and procedures) to manage information security in order to mitigate the risks derived from the use of information technology?



There is a risk map that shows the impact and probability of technological risks that may affect the operation of the organization

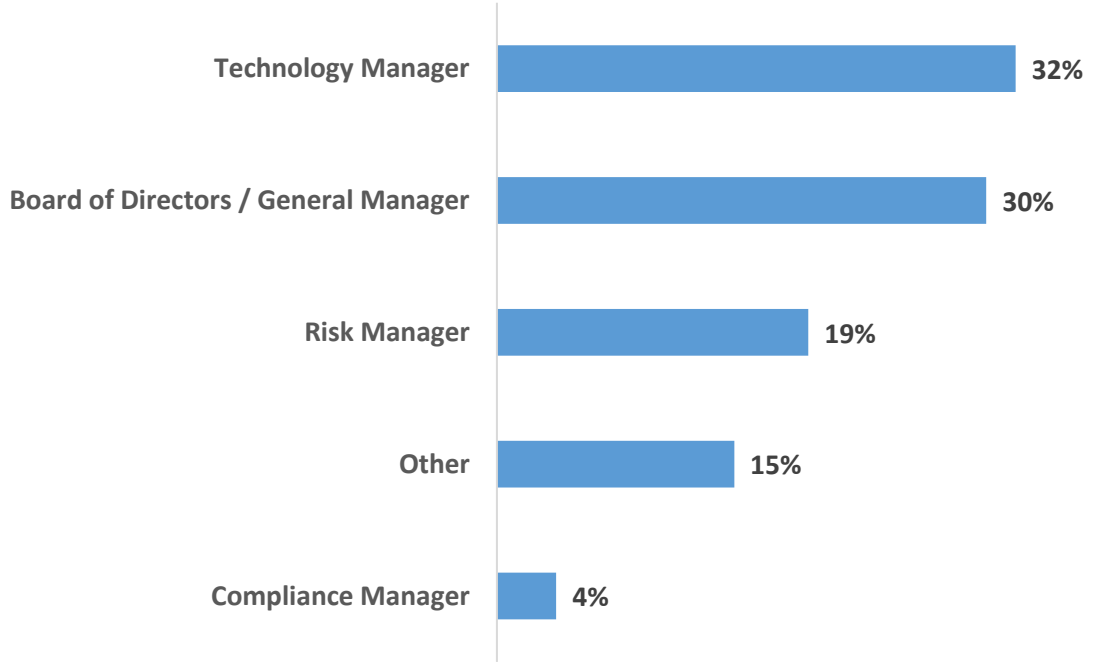


That only 39% of the participants claim not to have a documented framework for security management demands the attention of the organizations. This is compounded by the fact that only 38% reported having an updated technology risk map.

GOVERNANCE

Does the organization have human talent for any of the following functions?

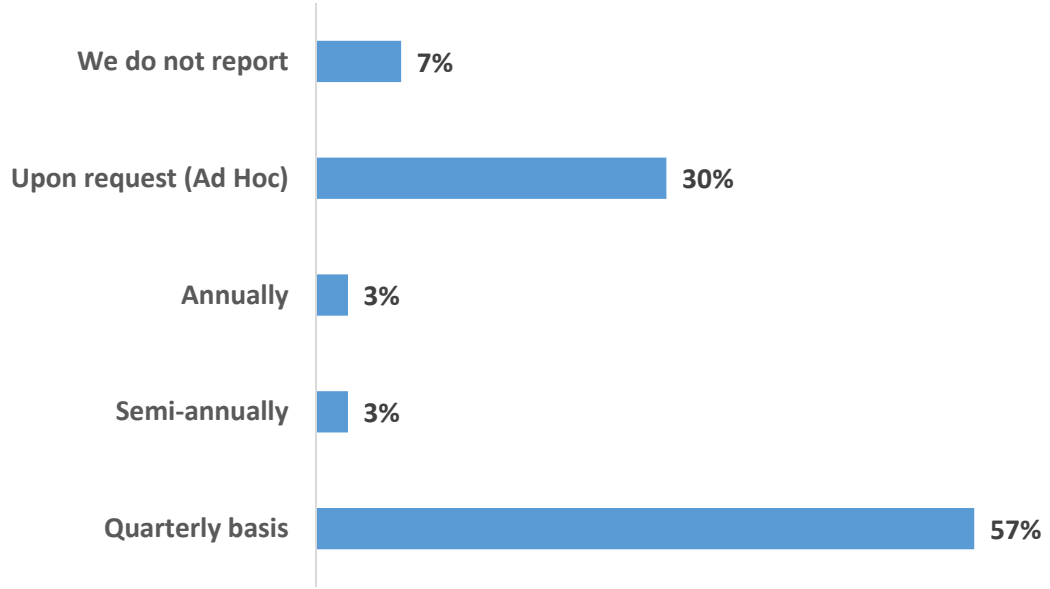
Who does the Information Security Officer report to?



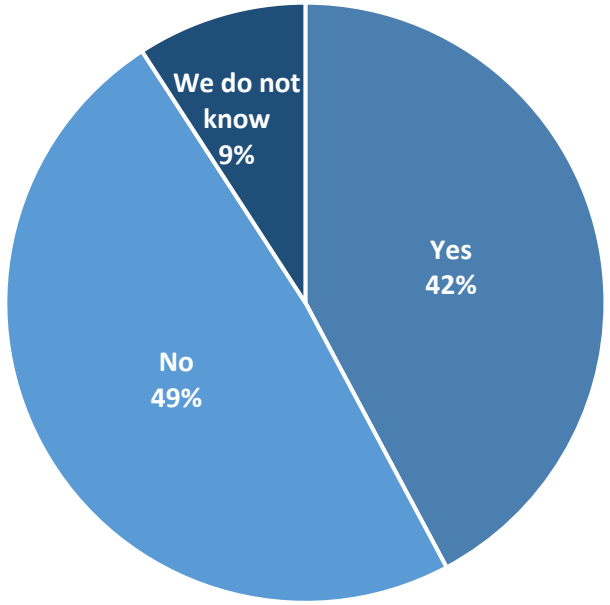
The absence of control areas in 14% of the respondents is worrying with the growing number of threats to which organizations are exposed.

GOVERNANCE

How often are higher levels (for example, General Manager, Vice Presidents, Committees, Board of Directors, Ministers of State) informed about the security level of the organization?



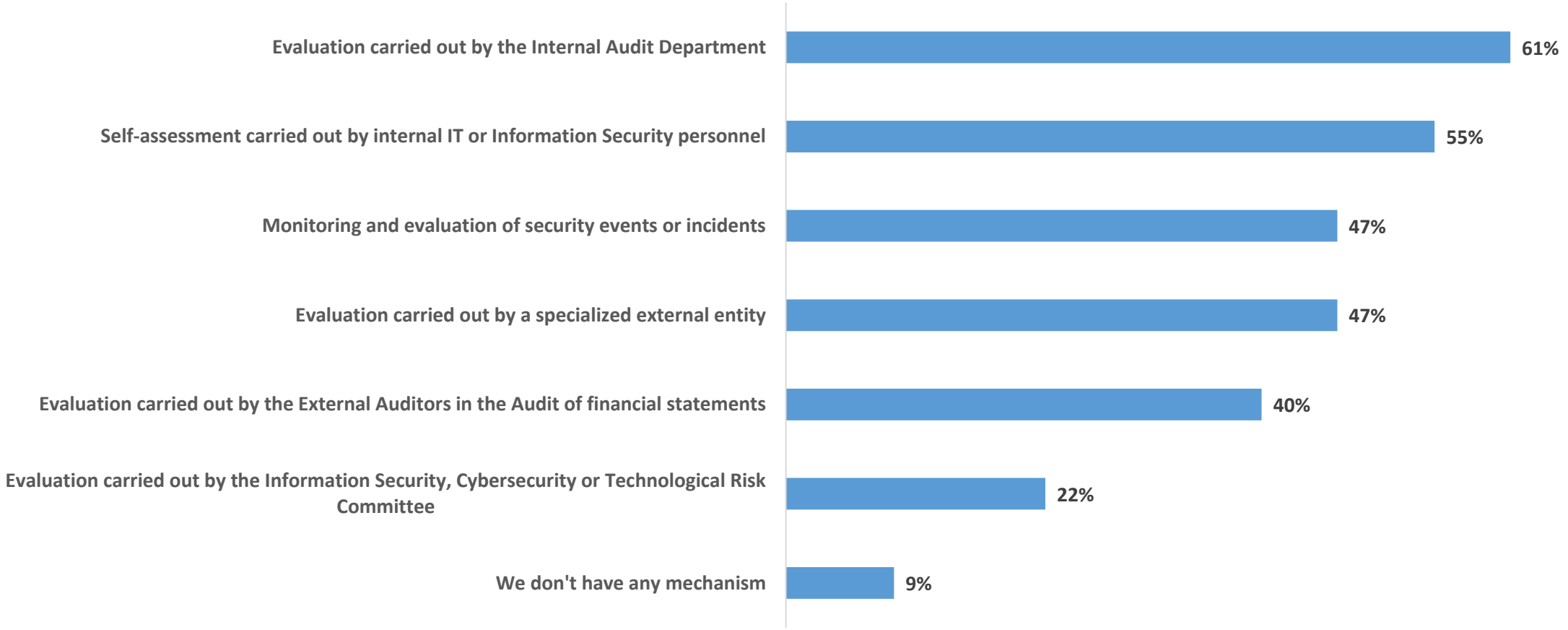
Does your organization have an Information Security, Cybersecurity or Technological Risk Committee?



The study shows that the Boards of Directors and/or "C-Levels" are not documented on a recurring basis on the state of information security in the organization. Thirteen percent receive no information or rarely receive any.

GOVERNANCE

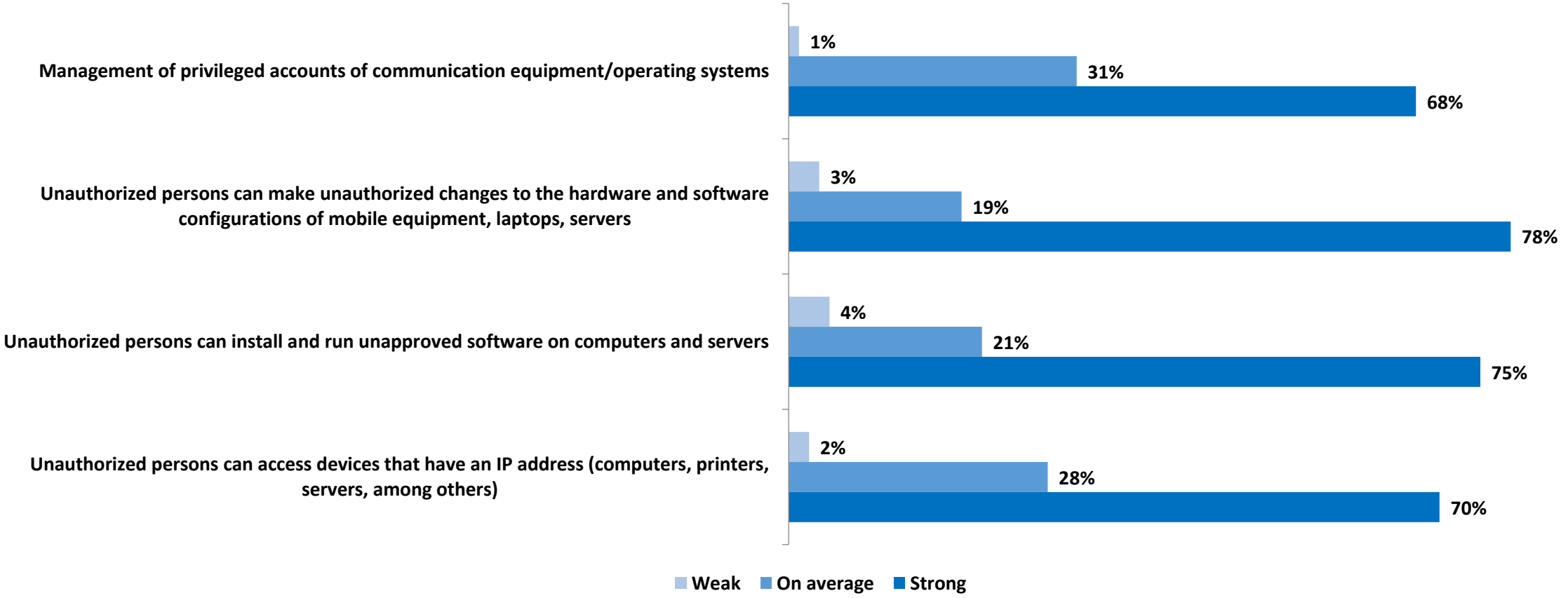
What mechanisms are used in the organization to evaluate the effectiveness of the information security strategy?




SECURITY
OPERATIONS AND
TECHNOLOGIES
RISCEO

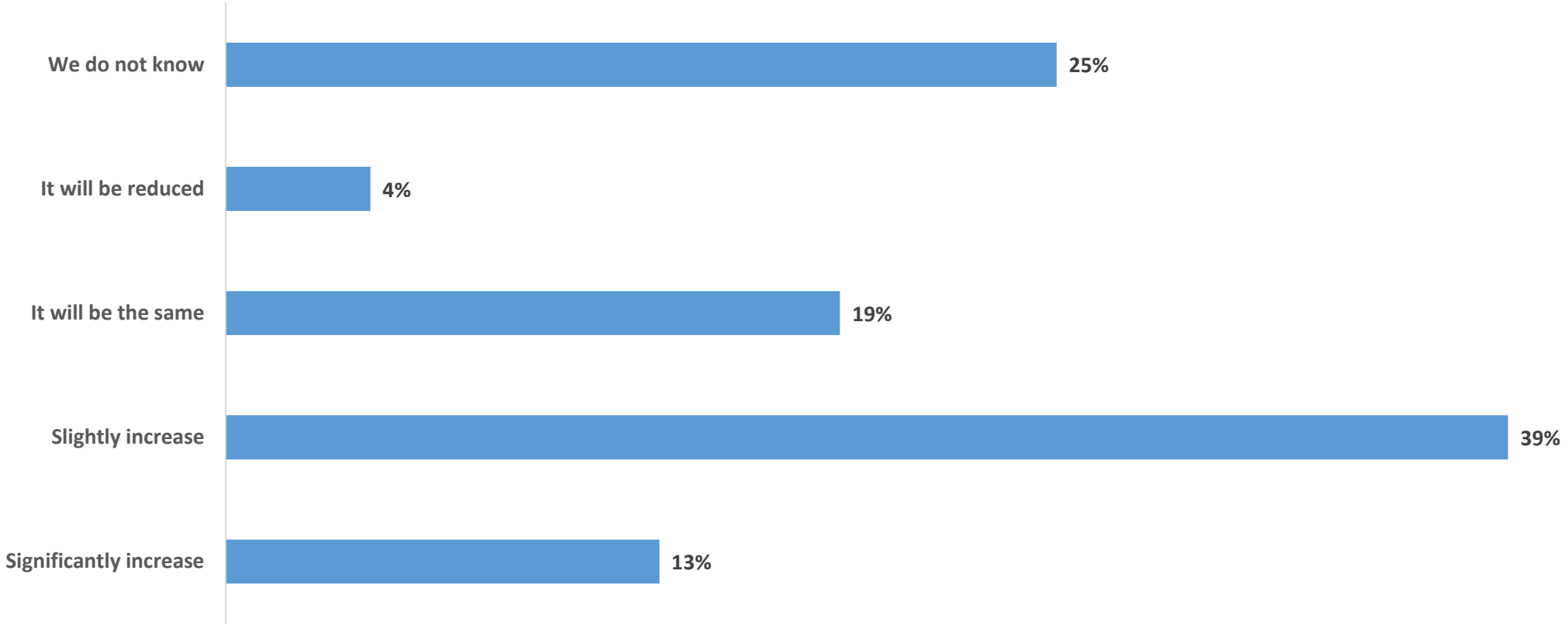
SECURITY OPERATIONS AND TECHNOLOGIES

Do you consider that the controls implemented in your organization, to mitigate the risks described below, are?



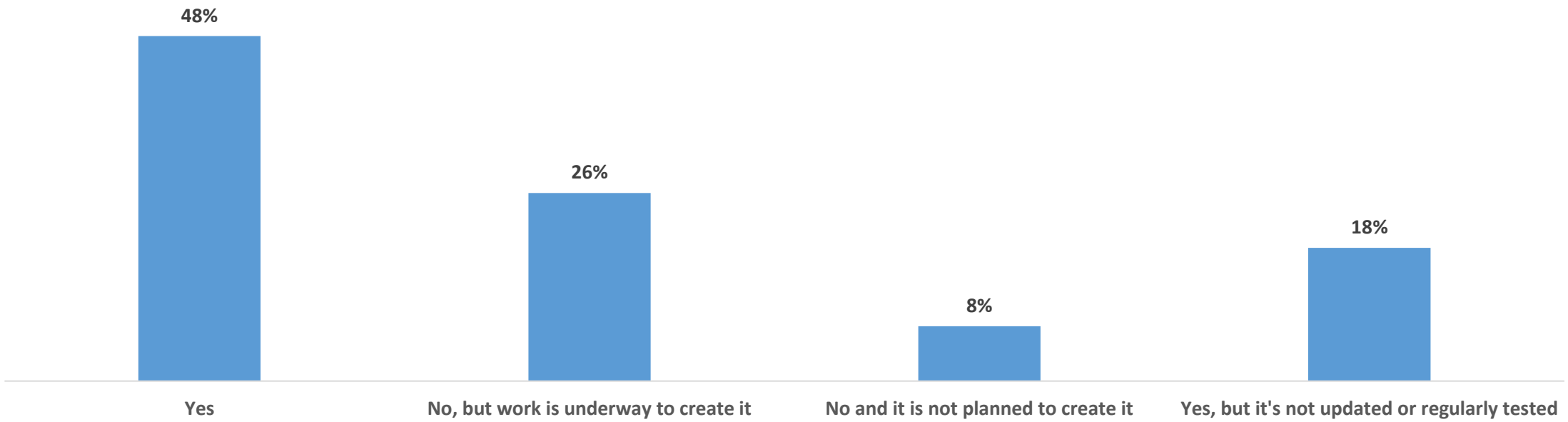
SECURITY OPERATIONS AND TECHNOLOGIES

Do you consider that the budget allocated to information security for 2023 and compared to that of 2022 will?



SECURITY OPERATIONS AND TECHNOLOGIES

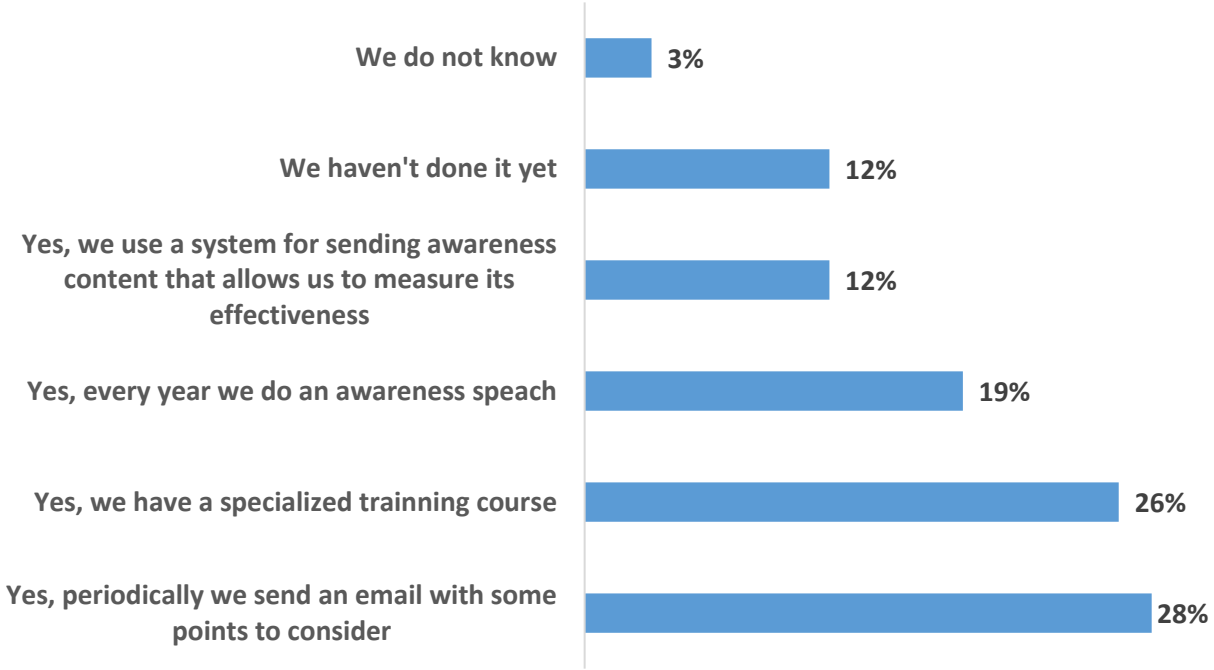
Does the organization have a disaster recovery plan, properly documented and regularly tested?



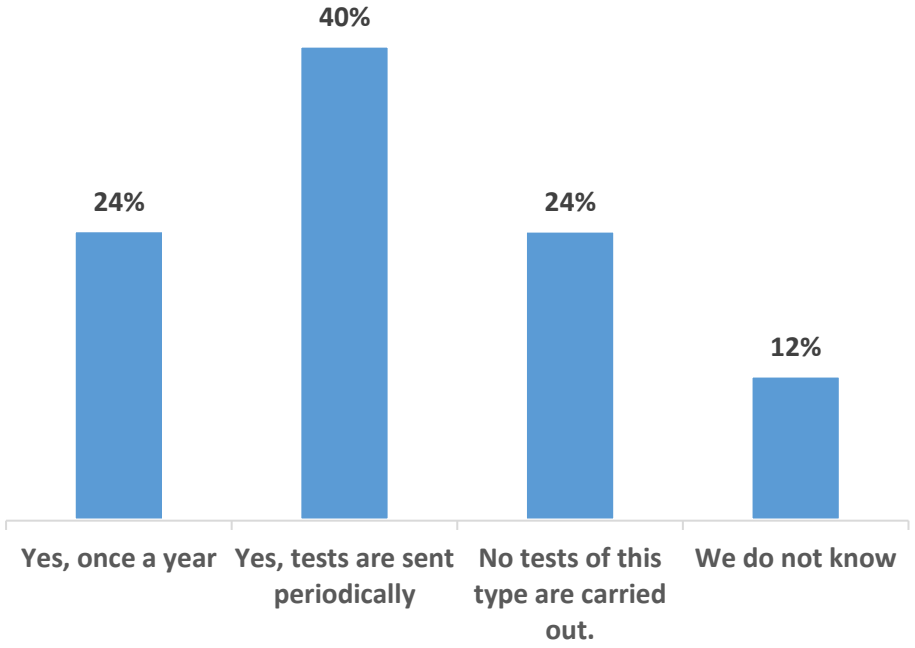
Although 48% report having a disaster recovery plan, it is disturbing that the remaining 52% of respondents do not have a plan or that it is not updated.

SECURITY OPERATIONS AND TECHNOLOGIES

Does the organization have a strategy to reinforce information security awareness of end users?



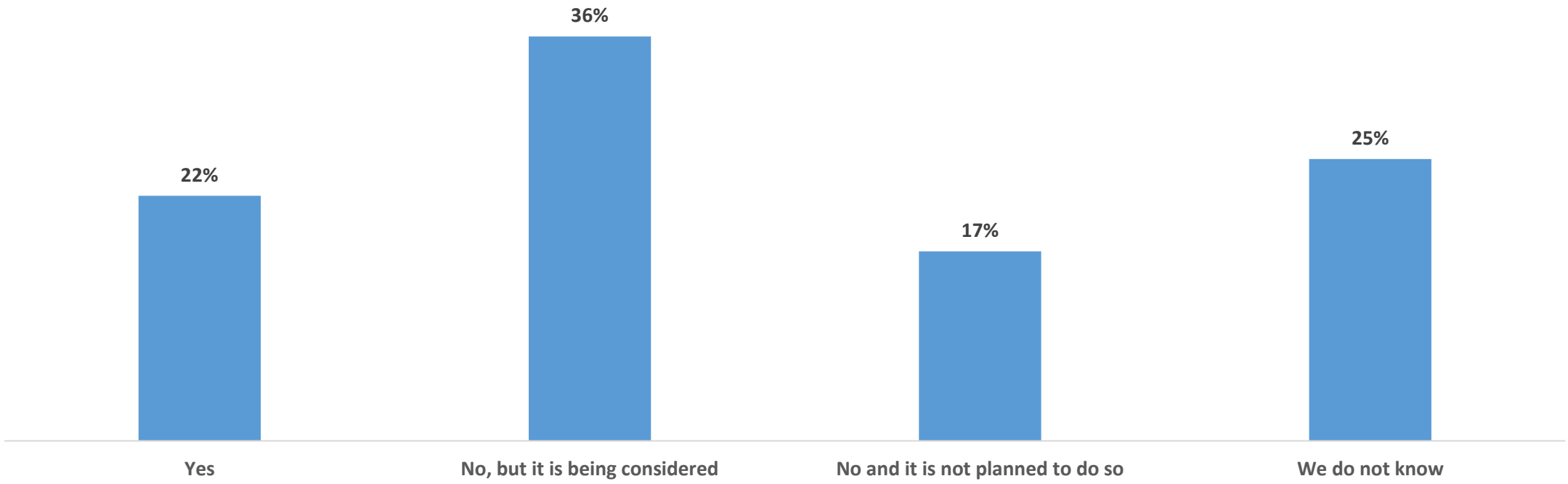
Does your organization regularly conduct phishing or ransomware tests or simulations?



It is clear that user awareness is a fundamental part of the information security strategy, but 73% use mechanisms that are not very measurable or that do not effectively reinforce user awareness.

SECURITY OPERATIONS AND TECHNOLOGIES

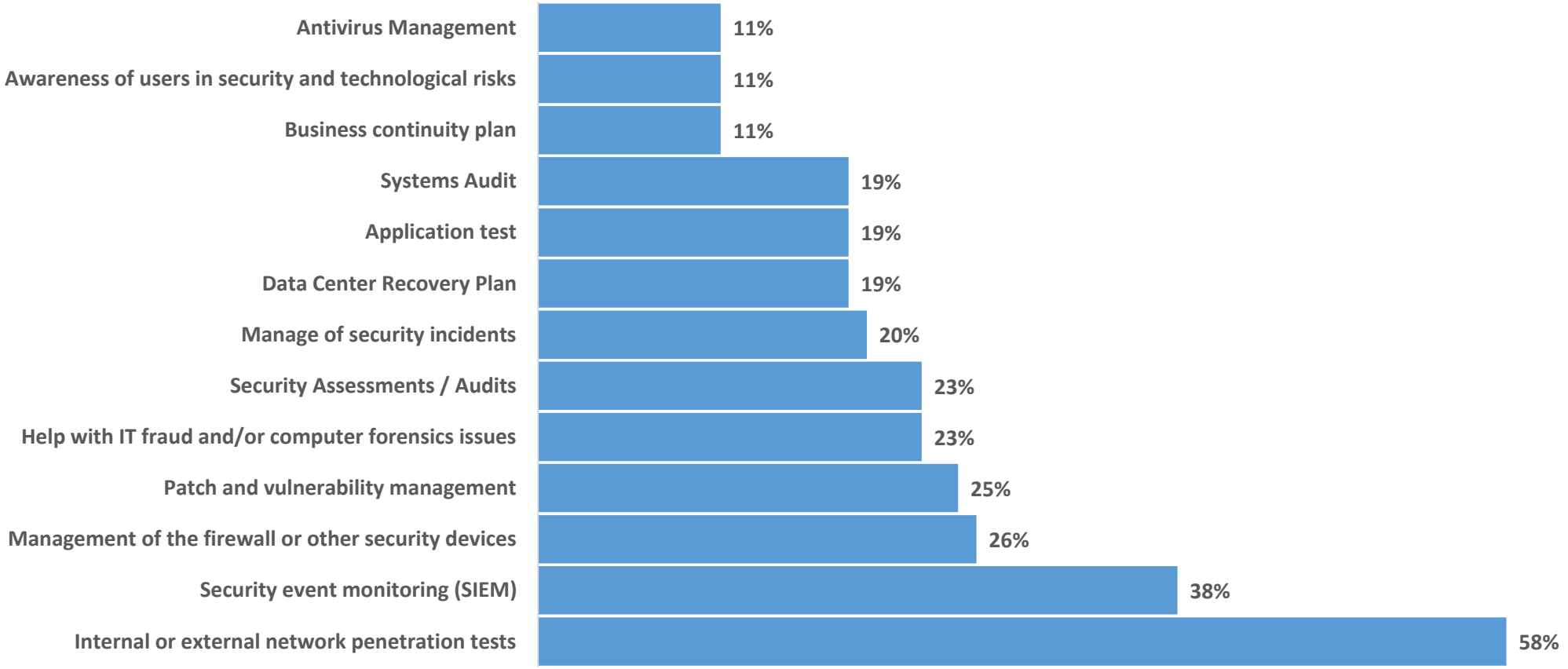
Does the information security and cybersecurity strategy in the organization include software that incorporates artificial intelligence or "machine learning" techniques?



It is a fact that more and more information is becoming available both for the identification of security incidents and for decision making. The use of new technologies to help us manage this volume becomes critical.

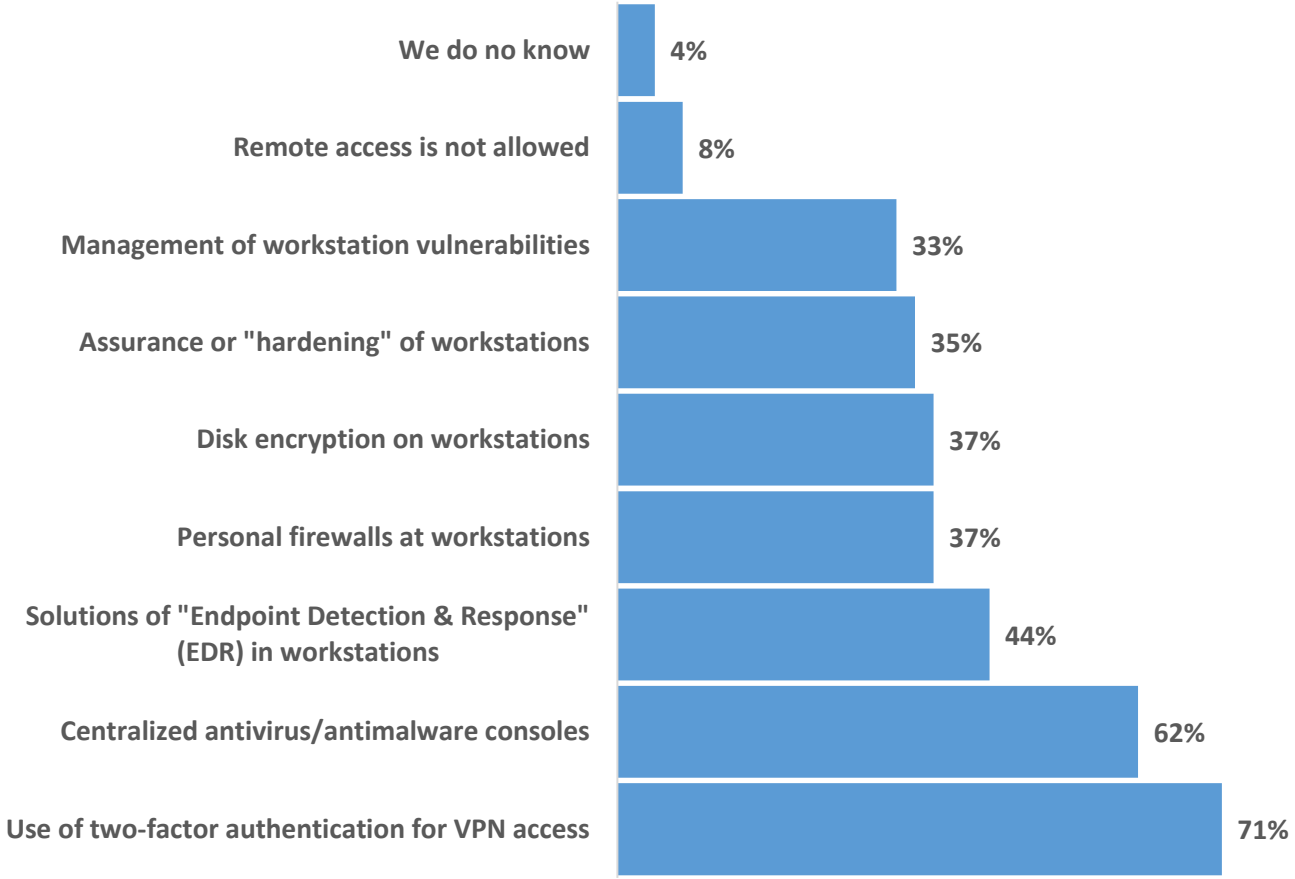
SECURITY OPERATIONS AND TECHNOLOGIES

Which of the following activities related to information security have been or are being considered for outsourcing?

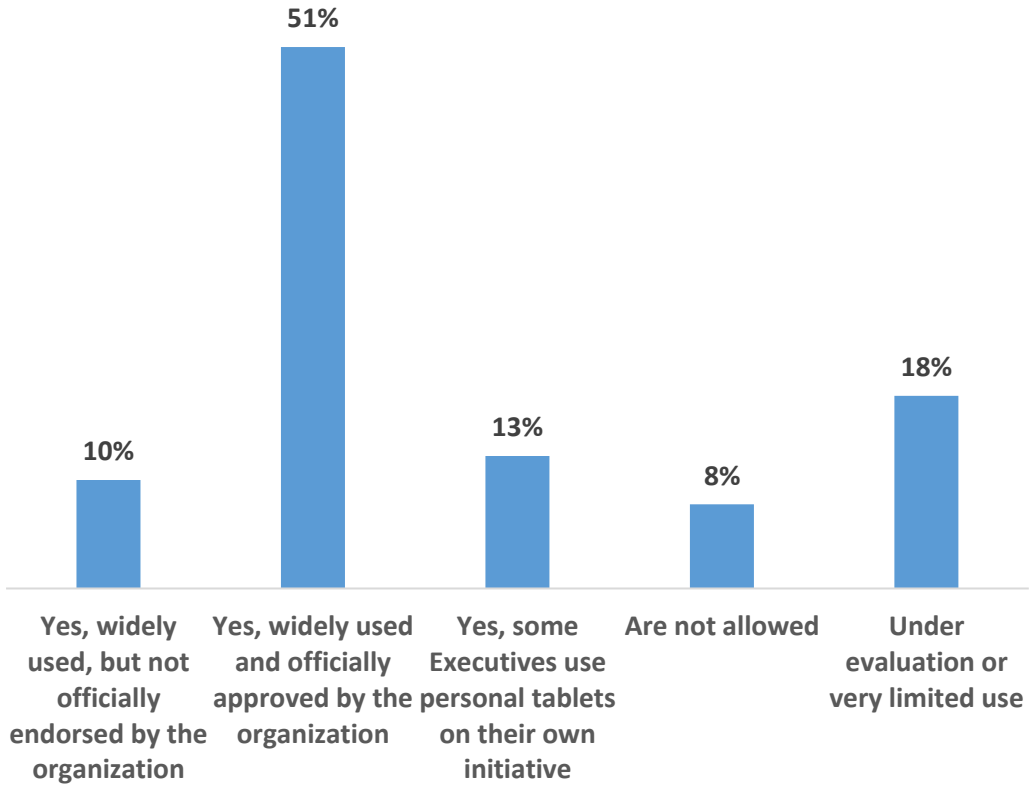


SECURITY OPERATIONS AND TECHNOLOGIES

As remote work has become a part of many organizations, what security controls has your organization implemented to reduce the risks related to this technology?

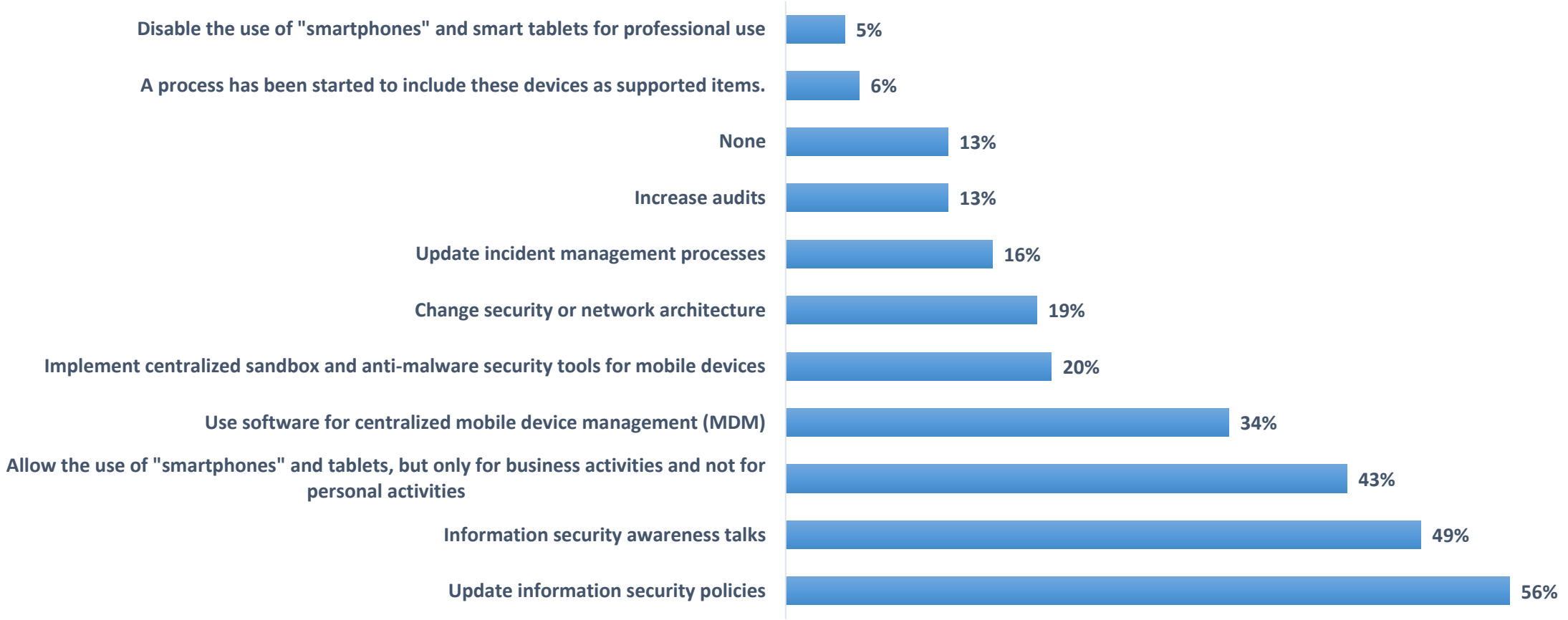


Does your organization currently allow the use of mobile devices such as smartphones or tablets, for business activities?



MOBILE DEVICES

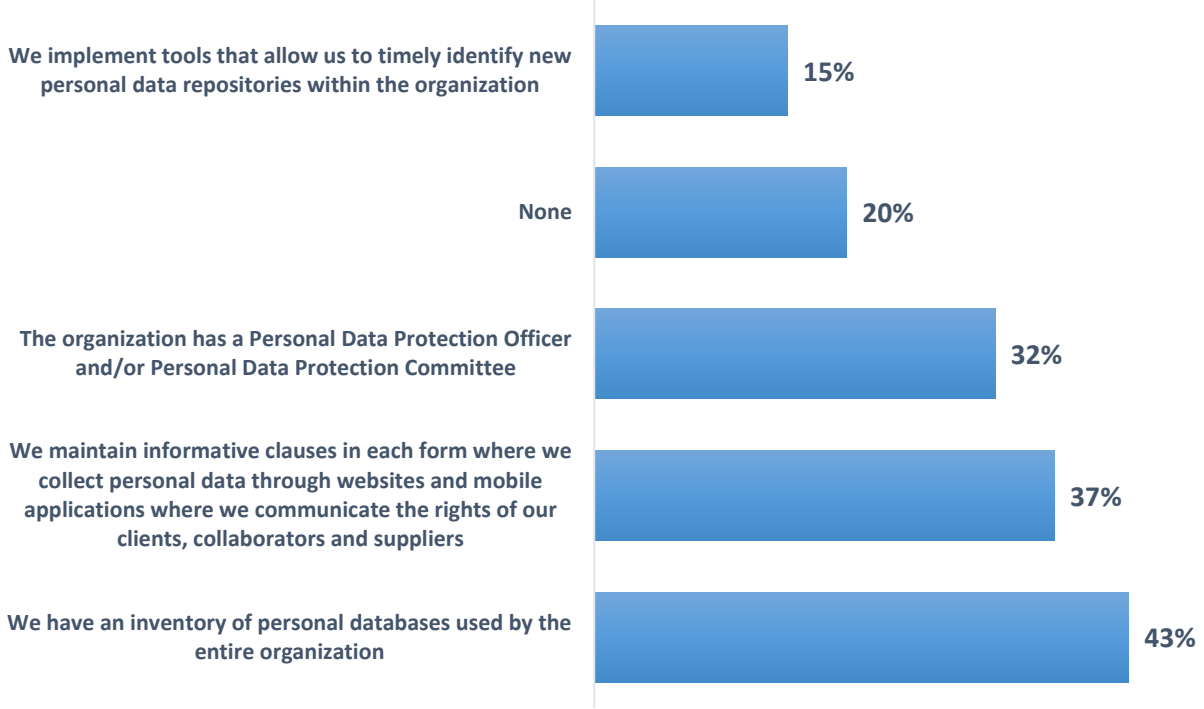
Which of the following controls has your organization implemented to mitigate the risks associated with the use of mobile devices by employees (eg, smartphones and tablets)?



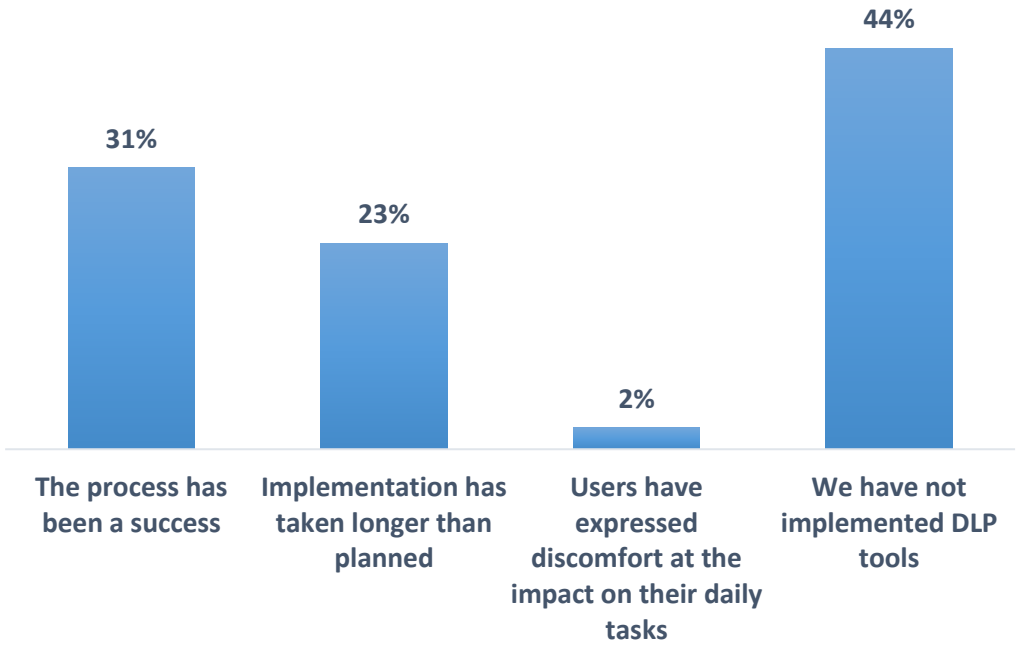

DATA
PRIVACY

DATA PRIVACY

What actions has your organization implemented to maintain proper management of the personal data of clients, collaborators and suppliers?



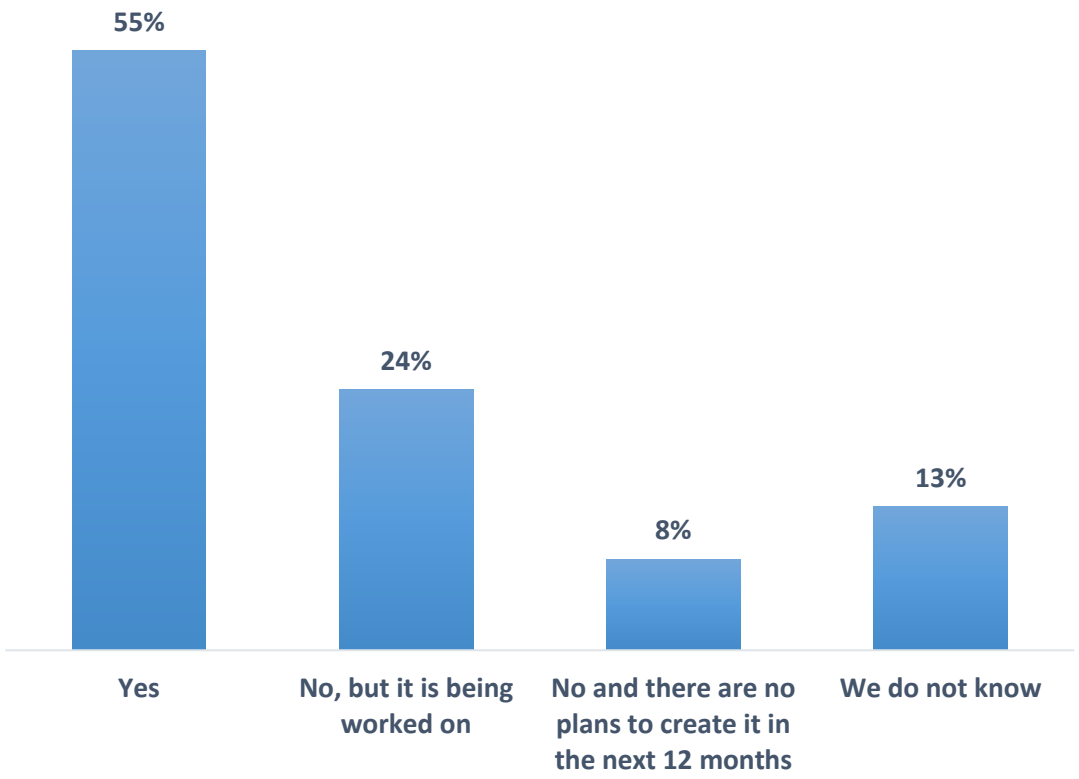
Regarding the implementation of Data Loss Prevention (DLP) or similar tools in your organization, how would you describe this process?



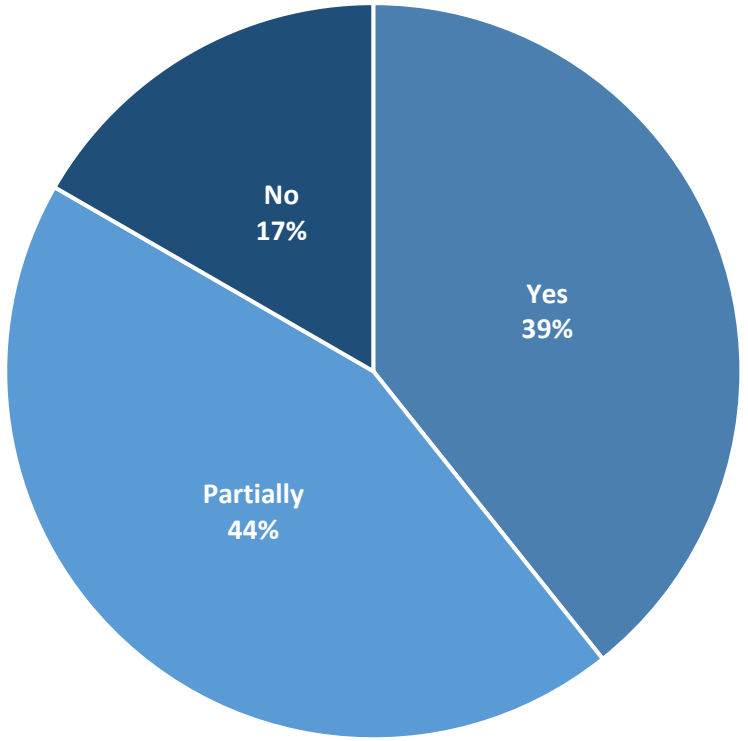
Although personal data is a relevant information asset, only 31% have tools to monitor the manipulation or theft of data, including personal data. This situation is even more relevant since 20% of the participants indicate that they have no mechanisms or tools for the protection of such personal data.

DATA PRIVACY

Is there a formal strategy at management level, to establish controls and procedures to protect the personal data of your clients?



Is there a process for classifying data (public, confidential, etc.) that makes it possible to define control mechanisms to protect personal customer data?



CONTACTS

Panama and CARICOM

Antonio Ayala I.
aayala@riscco.com

Roberto Delgado
rdelgado@riscco.com

Rubén Fernández
rfernámdez@riscco.com

Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica

Maria Cristina Marroquín
mmarroquin@riscco.com

External Advisor

Dr. Modaldo Tuñon (Universidad Tecnológica de Panamá)
modaldotunon@gmail.com

riscco.com

It is an independent regional company dedicated exclusively to helping organizations meet their challenges in GRC (Governance, Risk & Compliance) and ESG (Environmental, Social & Governance); composed of professionals with the knowledge and credibility necessary to translate very technical aspects into a simple language with business sense. With fourteen (14) years of having started operations, RISCCO has in its client portfolio private companies and Government Institutions in the region leaders in their field.