nten
CONNECT ▸ LEARN ▸ CHANGE

State of Nonprofit Cybersecurity

November, 2018

An NTEN Report
By Robert Hulshof-Schmidt

Security is critical

for Nonprofits

In a world where news about cyberattacks and hackers regularly make the headlines, we knew it was necessary to better understand how nonprofit organizations were - or were not - managing security and privacy. NTEN and Microsoft surveyed more than 250 nonprofits across the US for the first State of Nonprofit Cybersecurity Report.

There are some bright spots in the findings, including 70% of respondents reporting they have backup policies, and over half have policies for risk, usage, and privacy. And there are many areas for further investment, including less than half of respondents reporting they have policies around cyberattacks and only 40% of respondents reporting they providing regular cybersecurity training for staff.

Our intention with this report is that you can benchmark where your organization is at against others, and start to identify priority areas for your investment and planning.

Amy Sample Ward
CEO, NTEN

Jane Meseck
Senior Director of Global Programs and Partnerships, Microsoft Philanthropies

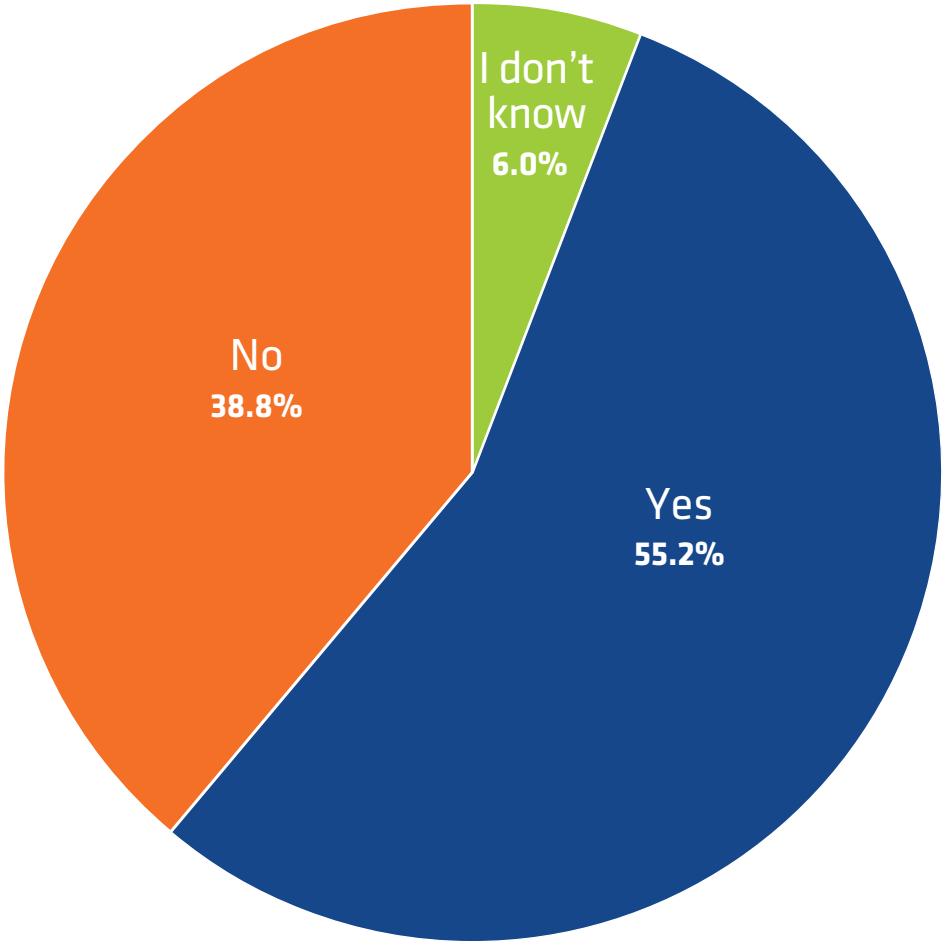
Policies

A critical aspect of effective security is establishing clear policies and ensuring that everyone knows and understands them. Most respondents have at least one of the five cybersecurity policies explored in this report.

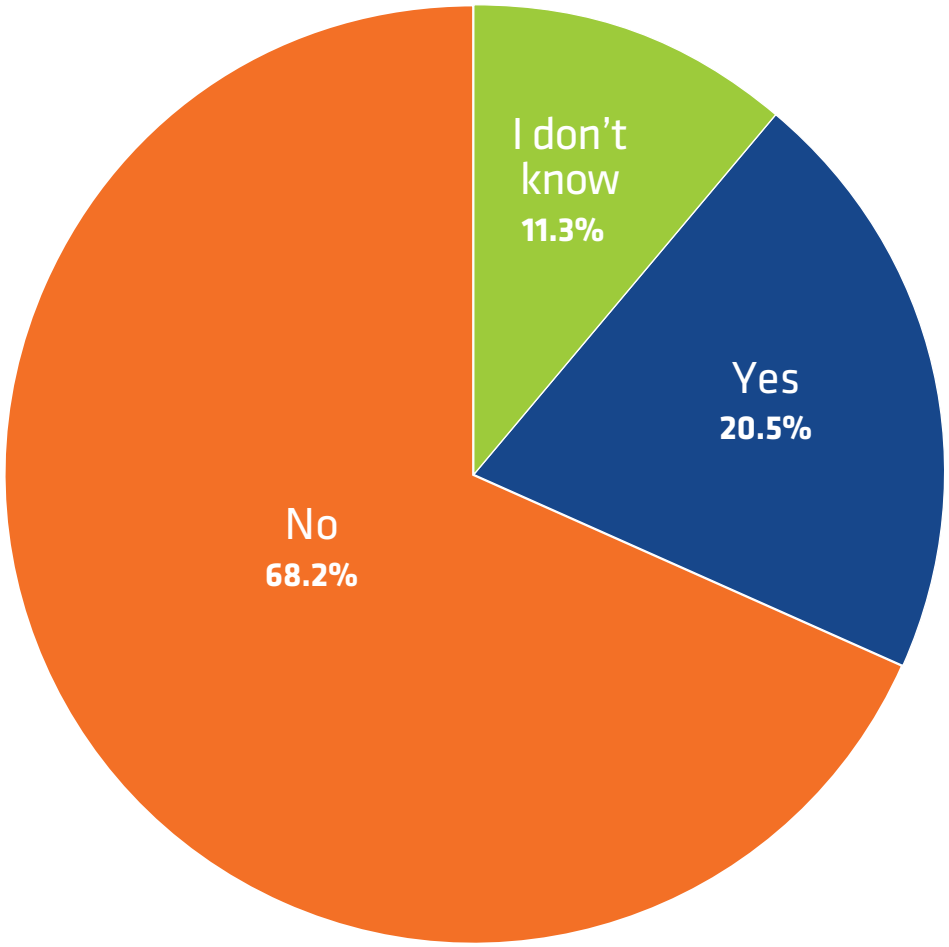
Over 70% of respondents have backup policies, enabling them to get back on their feet after an incident. Over half have specific cybersecurity policies addressing risk, usage, and privacy. Just under half address data sharing or personally identifiable information. The least common policy, at just over 20% of respondents, addresses cyberattacks explicitly.

Surprisingly, there is very little correlation between organizational size (by staff or budget) and the existence of policies. Respondents with larger IT departments are slightly more likely to have a broader variety of policies, but there is not a strong relationship. The best indicator of whether or not a respondent has a range of cybersecurity related policies is the age of the organization; more established respondents were the most likely to have the greatest number of policies in place.

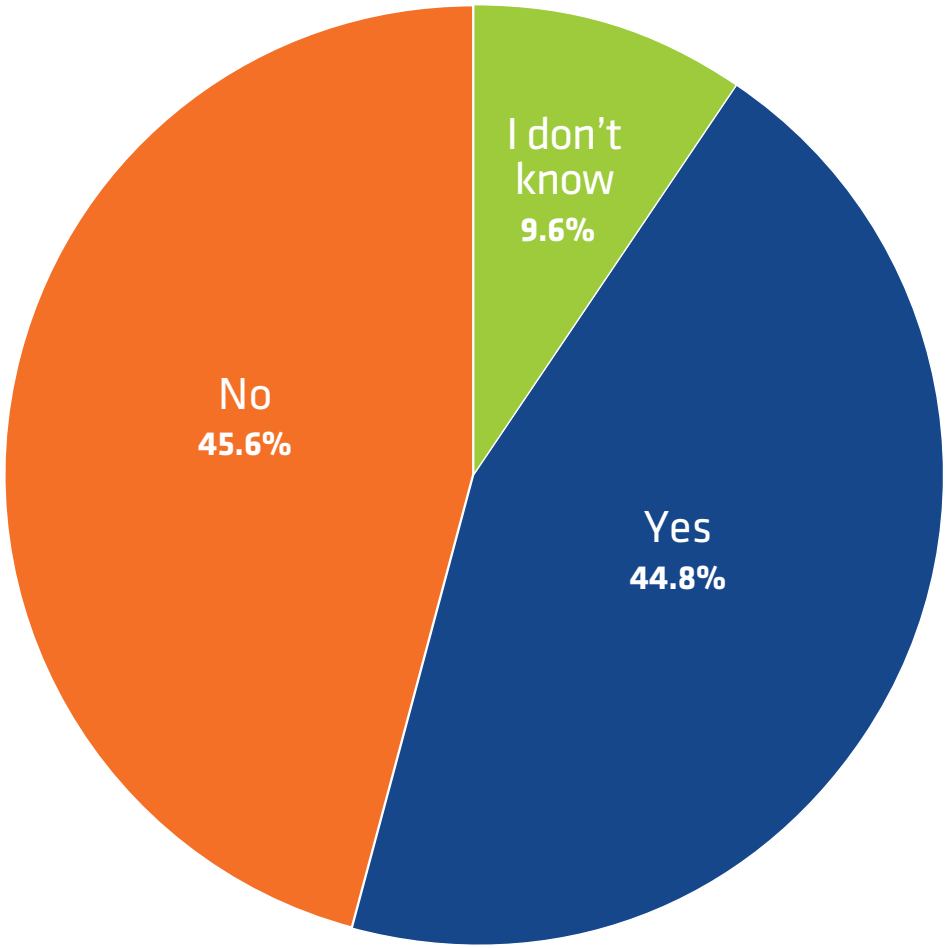
Do you have a policy which identifies how your organization handles cybersecurity risk, equipment usage, and data privacy?



Does your organization have documented policies and procedures in case of a cyberattack?

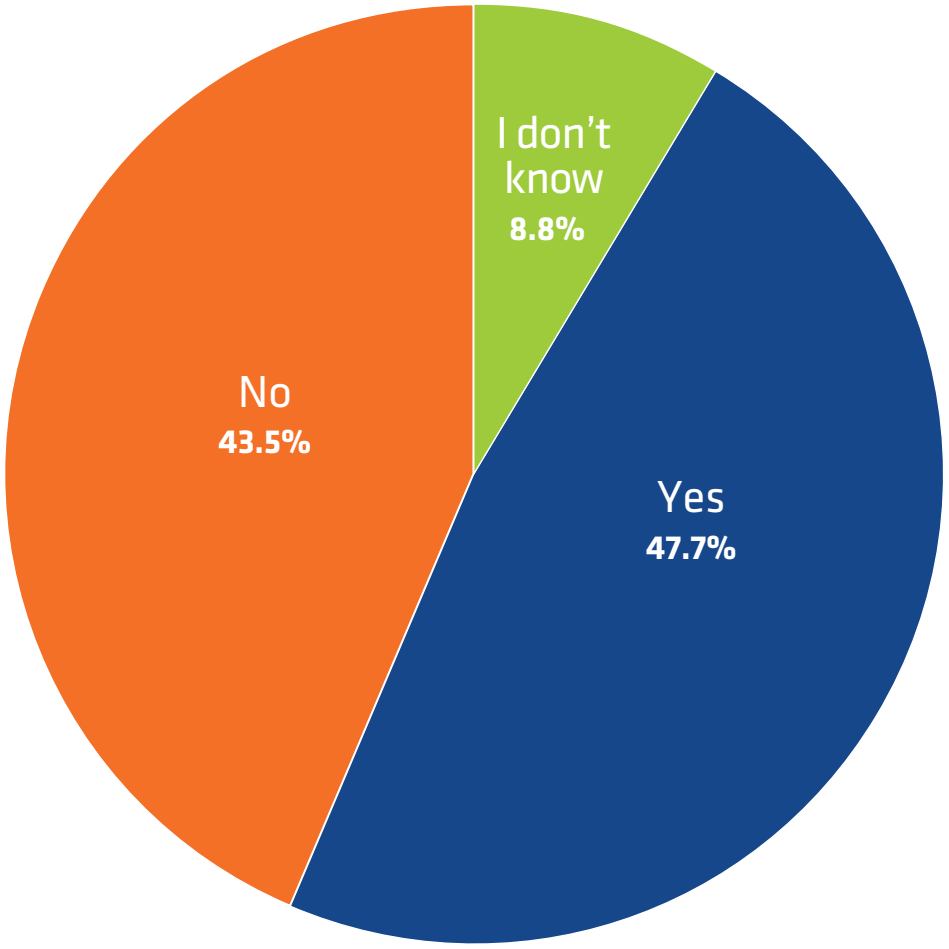


Do you have internal procedures or policies in place to manage how data is shared with external agencies?

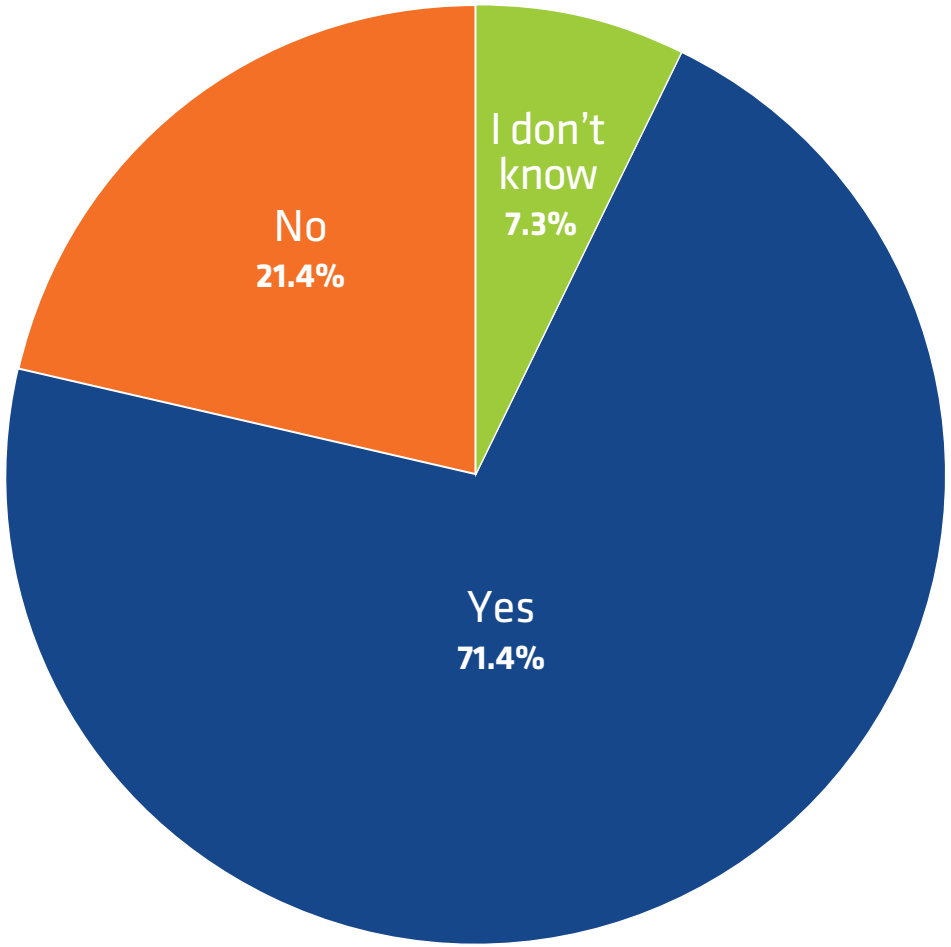


Do you have policies which clearly define what data collected (for both staff and constituents) are considered personally identifiable information (PII)?

Examples of PII include home address, social security number, credit card numbers, and date of birth.



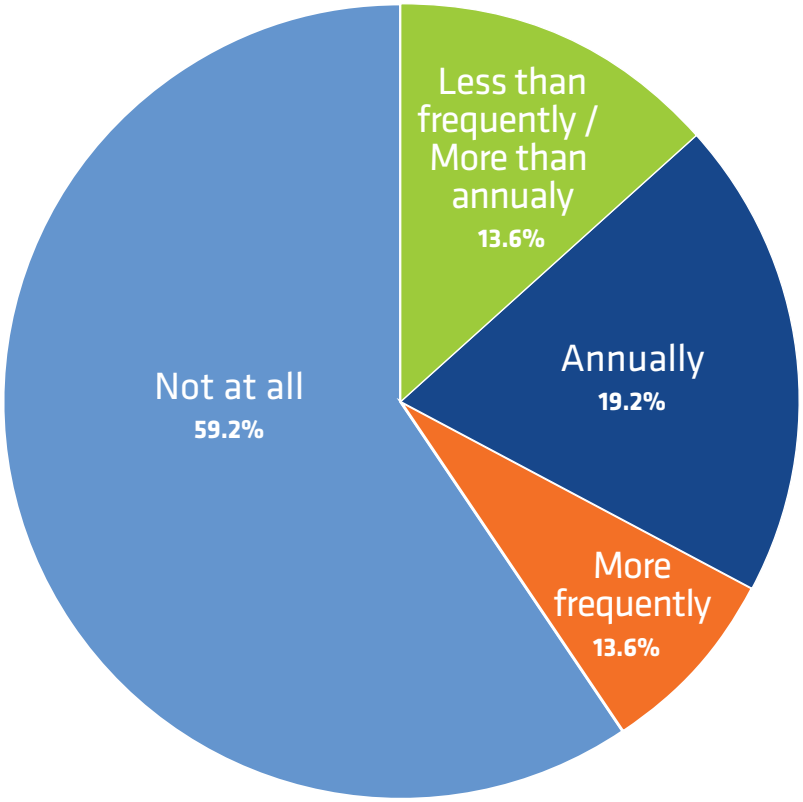
Does your organization have policies and procedures for backing up data, hardware, and software?



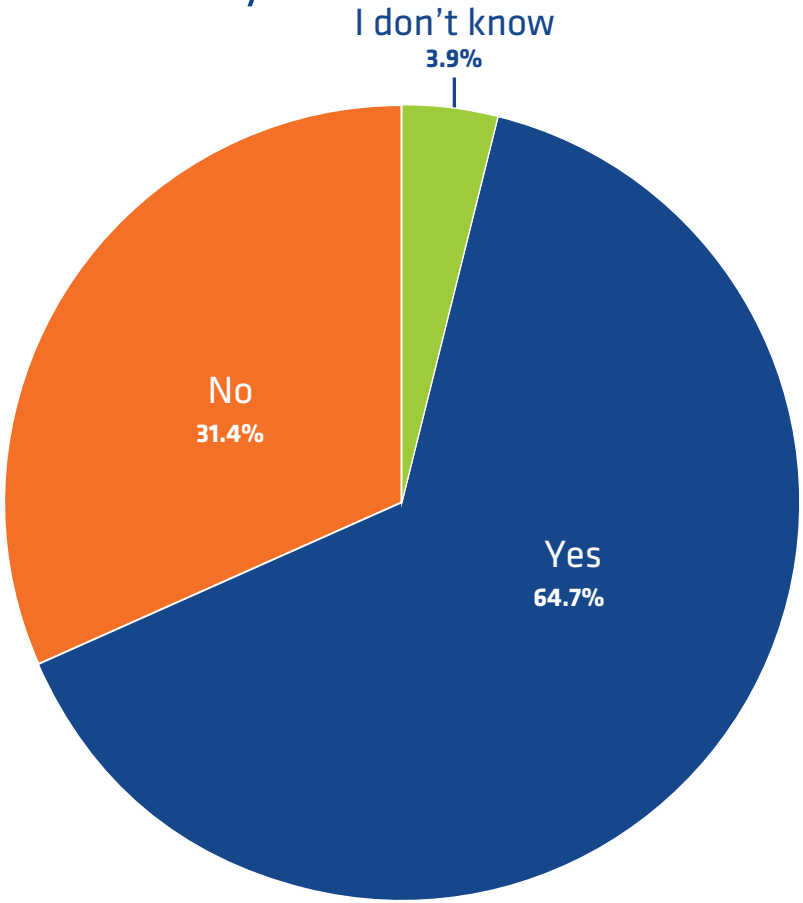
Training

In addition to effective policies, ensuring strong security is easiest when staff have training on critical issues. About 40% of respondents offer cybersecurity training on a regular basis, with half of them ensuring annual trainings. Of those that offer training two-thirds make that training mandatory, mostly those with a regular schedule. Training does not correlate to the size of the organization, but there is a clear relationship to the size of the IT department.

Does your organization provide cybersecurity training to staff on a regular basis?



Is the cybersecurity training mandatory?

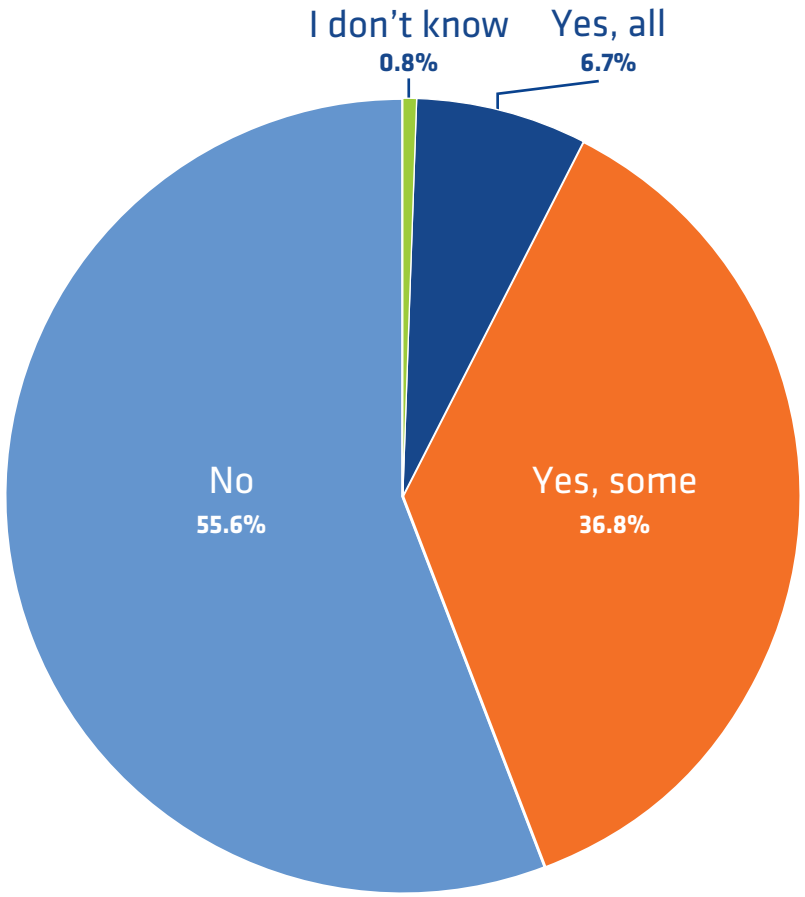


Access

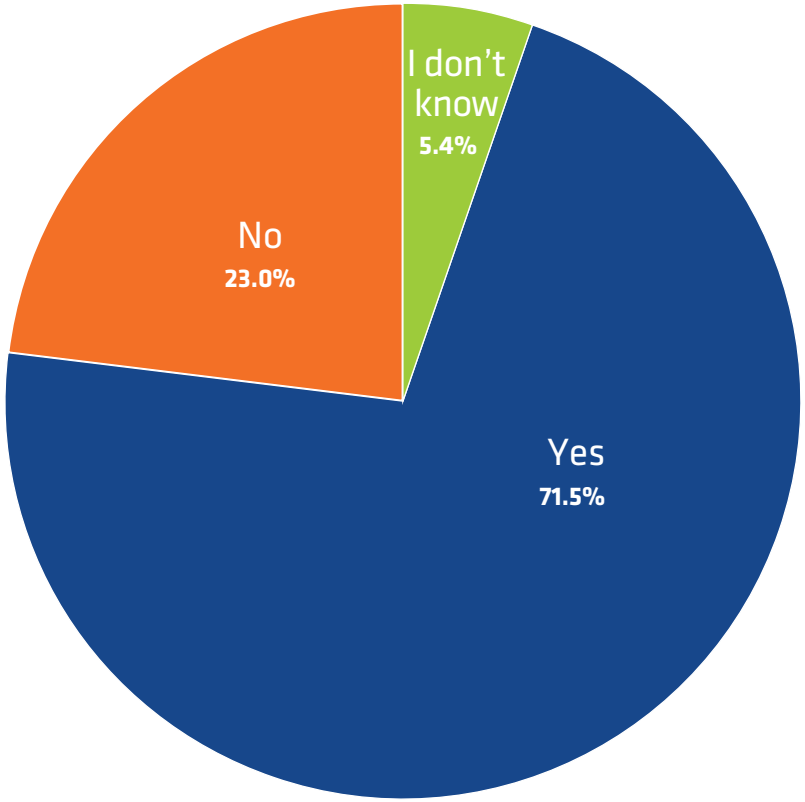
Controlling access is a key component of cybersecurity, but organizations must balance that control with effective and efficient work practices. Over 70% of respondents indicated that they have some form of wireless technology for office devices. A similar number allow unsecured access to some business functions from personal devices. Slightly less than half require multi-factor authentication for online access, and few require it for all functions.

Respondents with more locations were more likely to insist on some level of security or increased authentication, as were those with larger IT departments.

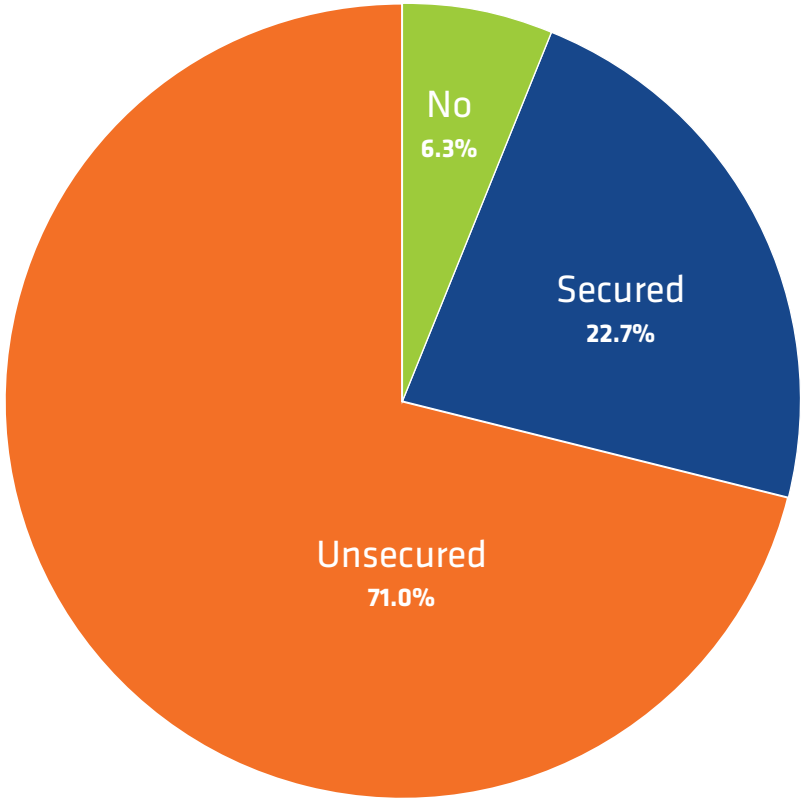
Does your organization require multi-factor authentication (MFA) to log into online accounts? MFA means the use of a password plus another authentication method, such as a rotating PIN, to access email or other online services.



Does your organization use wireless or Bluetooth technology for its printers, phones, or other devices?



Are staff allowed to use their personal devices to access organizational emails and business files?

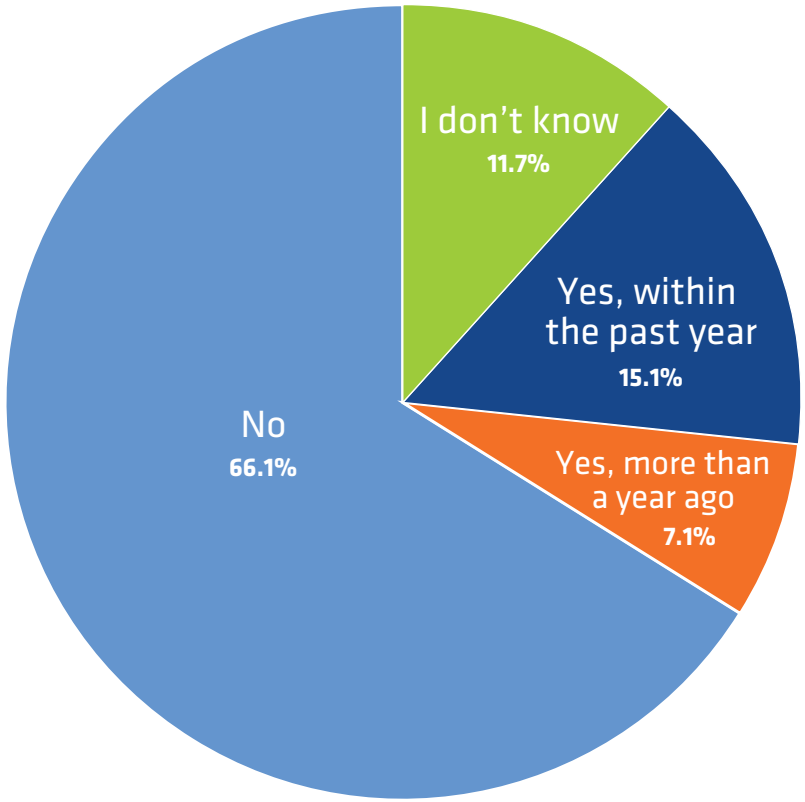


Drills and Exercises

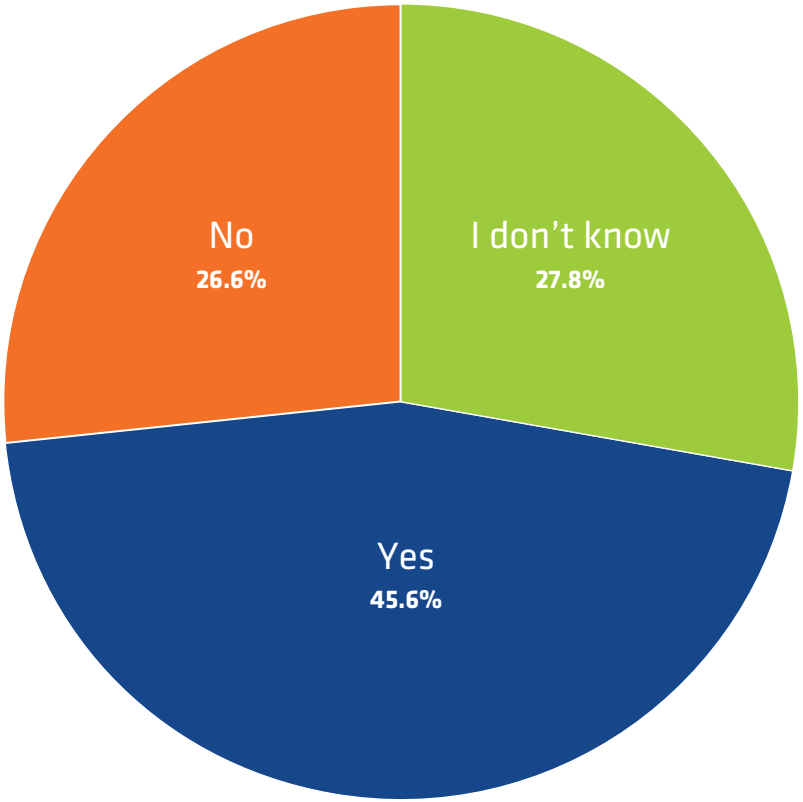
Practice makes perfect. Testing an organization's ability to deal with threats and attacks is a valuable way to ensure that policies and training are effective. Unfortunately, creating exercises and drills is resource intensive.

Only 7% of respondents have ever done a cyberattack simulation. Three times that many have done some sort of threat assessment exercise, but again only 7% have done so recently. Of those who have performed a drill, nearly half ensured that their employees could connect their personal behavior to any risks. Larger and more established organizations are much more likely to have conducted a threat assessment.

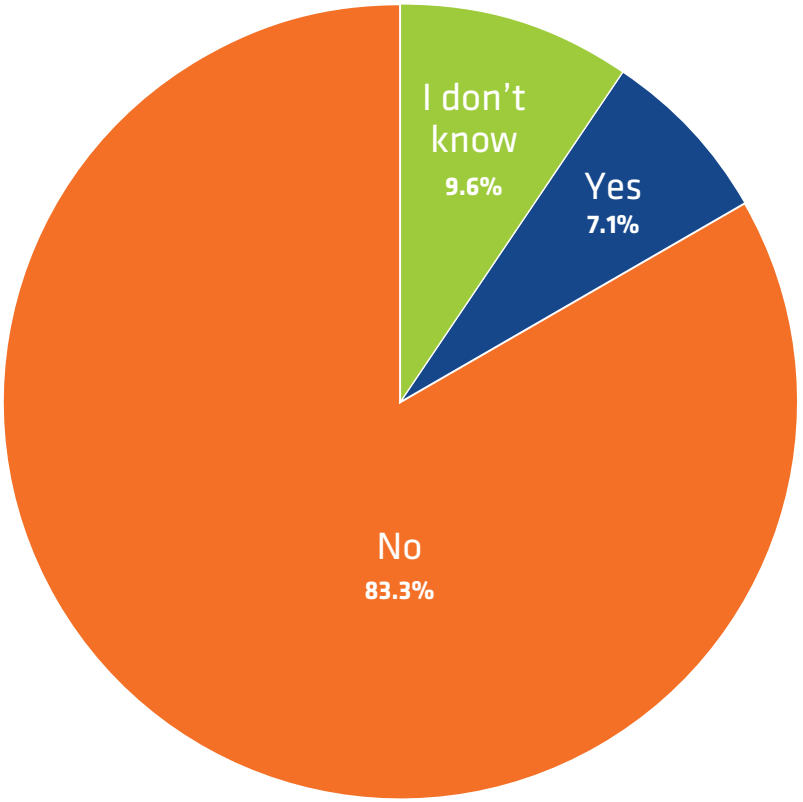
Has your organization undergone a threat assessment exercise or drill?



In the threat assessment exercise, did employees learn about areas in which their behavior is a factor?



Has your organization ever undergone a cyberattack simulation activity?



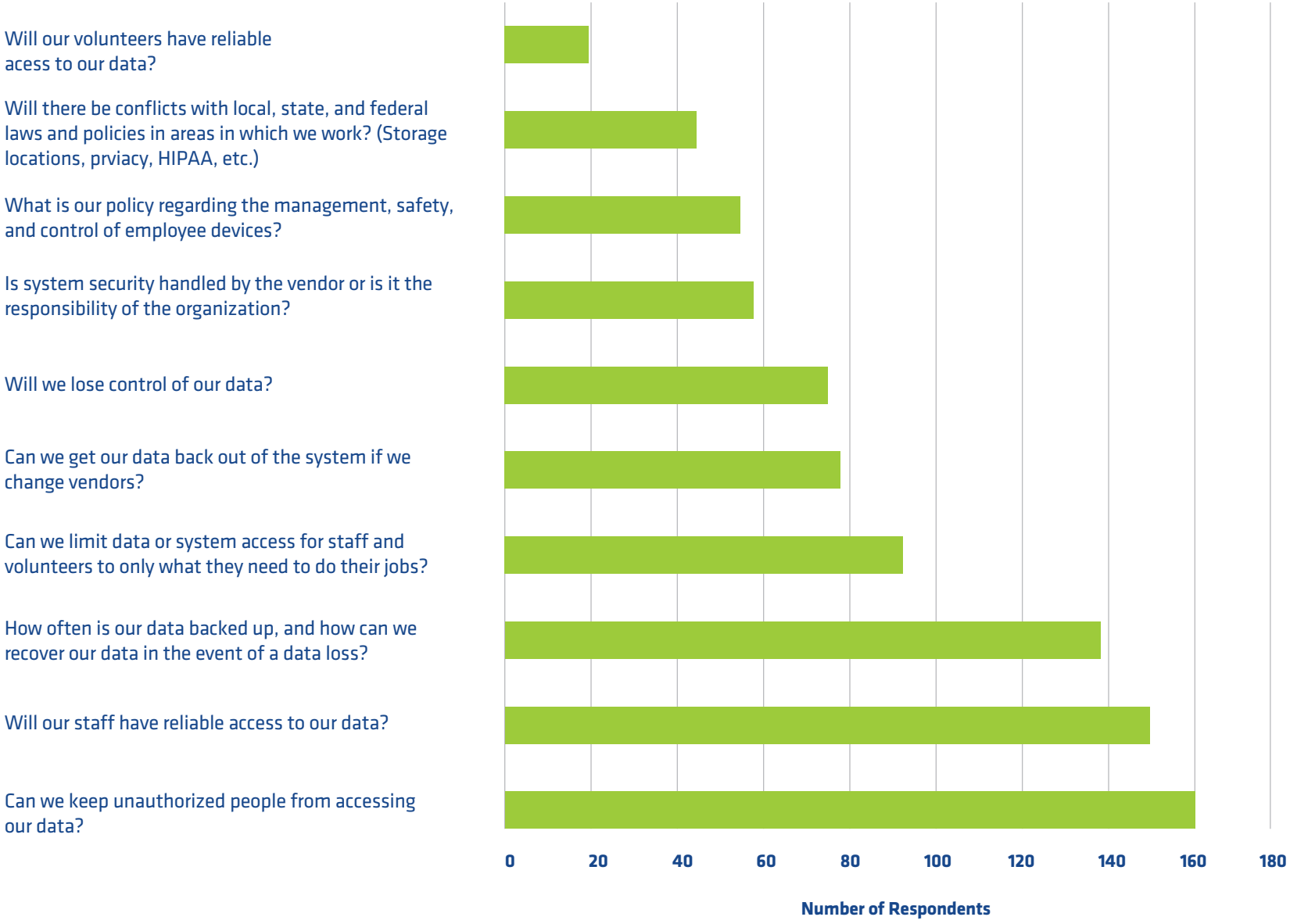
Decision Making

When assessing technology choices, a few security considerations are the most important to respondents. Access, recovery, and control are the key issues.

Access goes both ways: can we keep the wrong people out while allowing the right people in easily? These two related concerns were the largest by far. Coming in third is backup and data recovery. How easily can we recover if something goes wrong? Control issues cluster in the middle. Respondents were concerned about data control, migration, and vendor issues in equal measure.

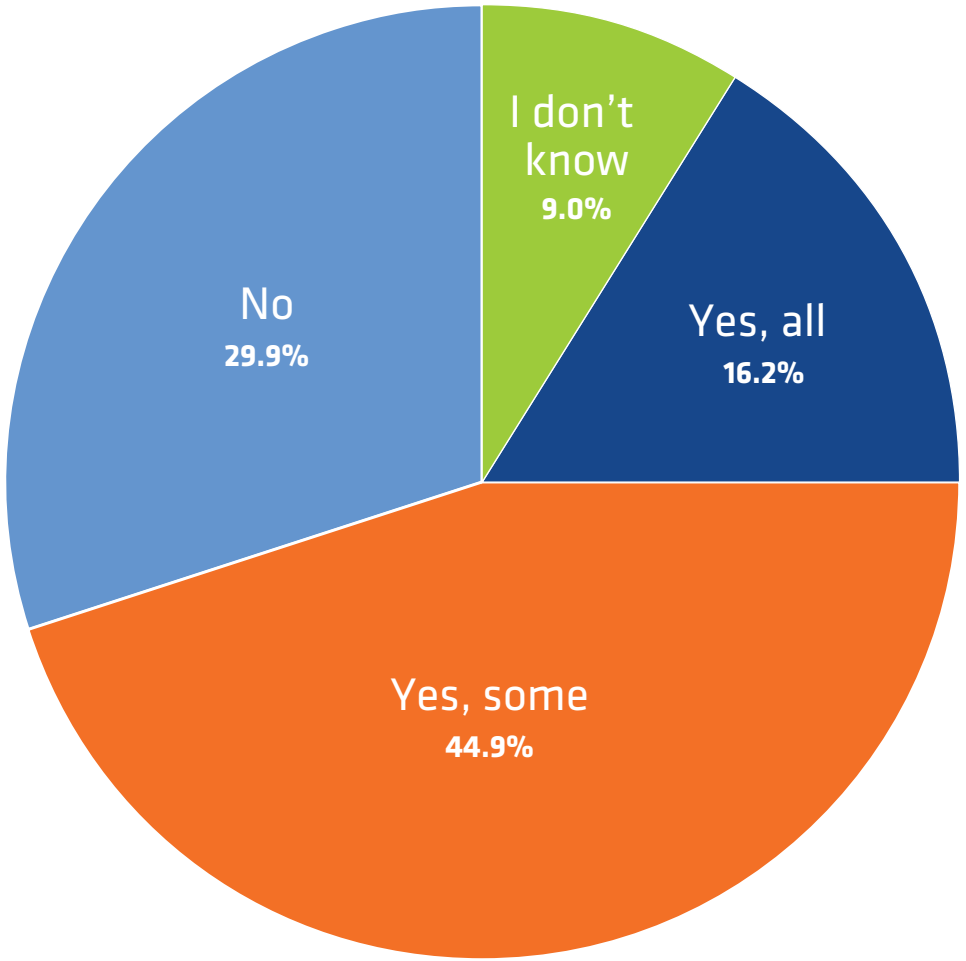
The biggest concerns were shared equally across respondents regardless of size or budget.

When comparing your technology options, how did the following security concerns factor into your decision-making? Participants chose their top three responses.*



Monitoring and Control

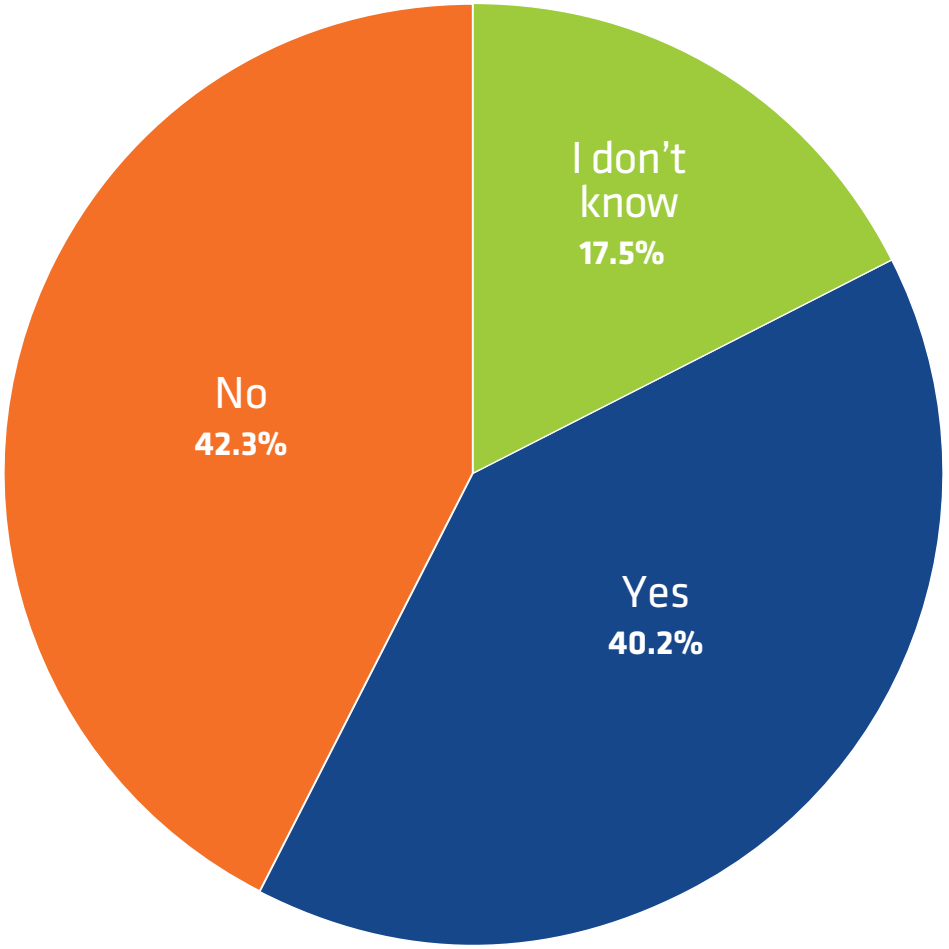
Are you monitoring the use of computer and web applications by your organization?



Do you have an application inventory?

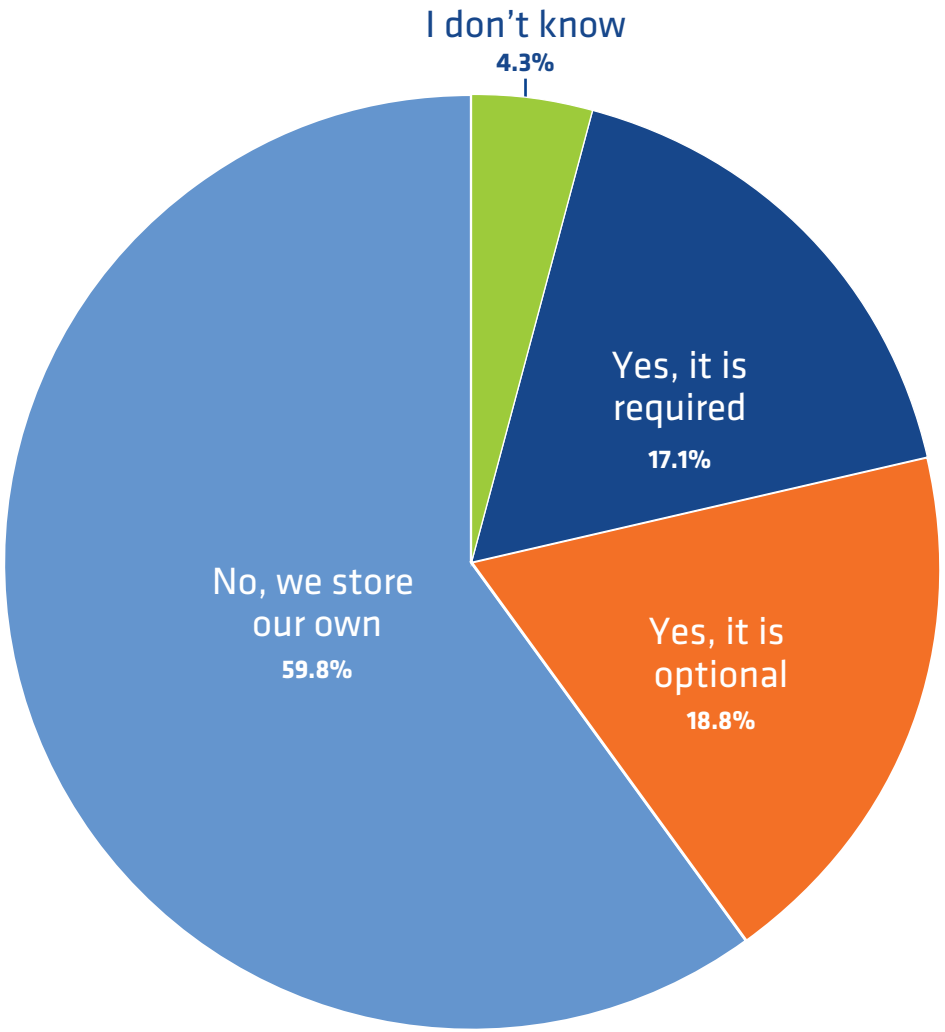
About 60% of respondents perform some application monitoring in the workplace. Only ¼ of these attempt to monitor all applications. The larger the organization and IT department, the more robust the monitoring.

About half of the respondents have an application inventory. The majority of these are also performing application monitoring.



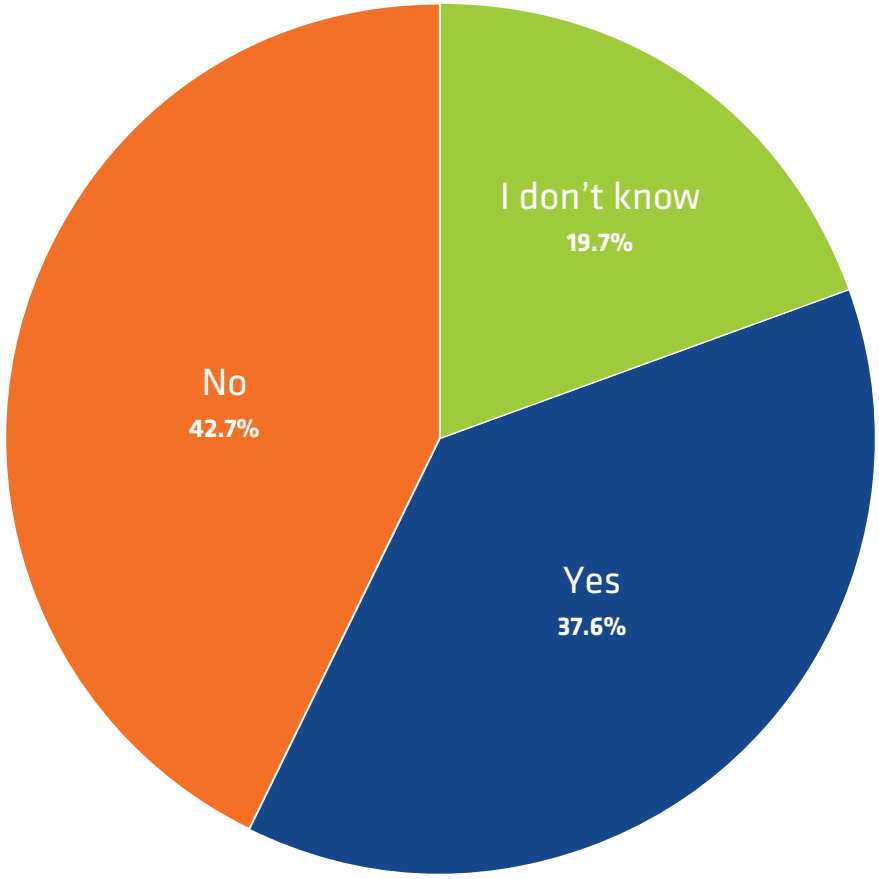
Does your organization use a secure password management tool for storing and sharing user IDs and passwords?

Only about one-third of respondents use a password management tool, and half of those make it optional. Use and requirement are closely related to the size of the IT department.



Have you discovered unauthorized applications, or so-called "shadow IT" being used at your organization? Examples could include software or hardware that was installed without the examination, knowledge, and/or approval of IT staff.

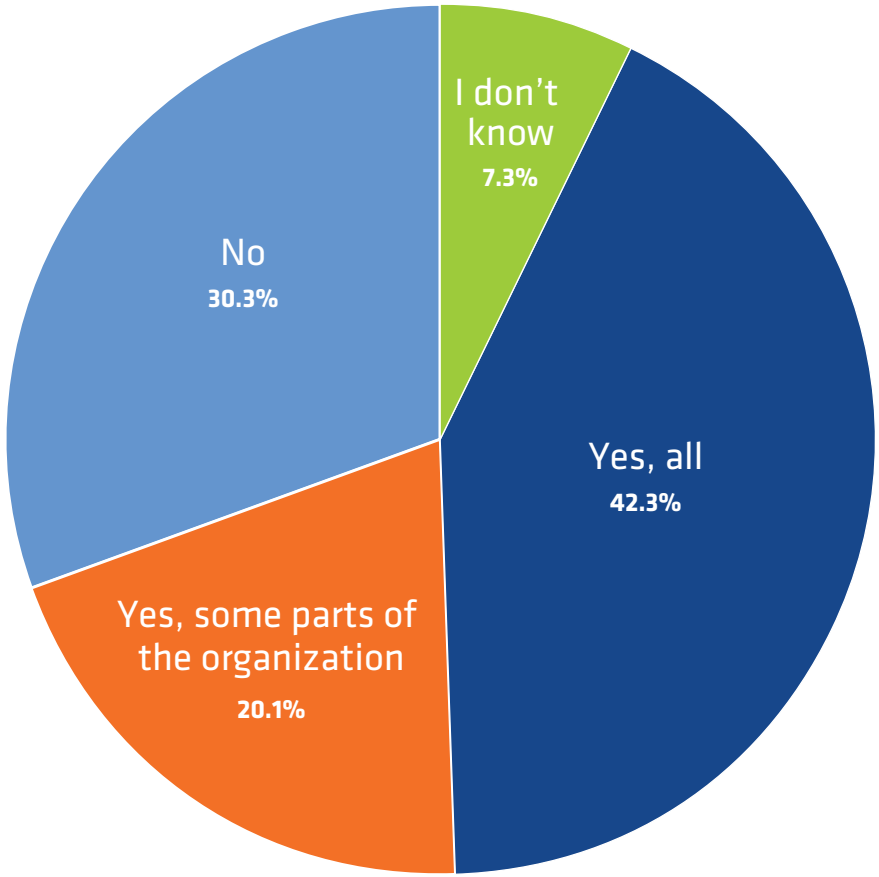
Just over one-third of respondents have identified unauthorized applications in the workplace. Of the 20% that answered “I don’t know,” most have limited IT staff.



Does your organization have an internal network with a virtual private network (VPN) and perimeter security to protect internal-only resources?

For example, if remote and regional staff offices can access files managed at the head office via an internet connection, and that connection is secured by a VPN login.

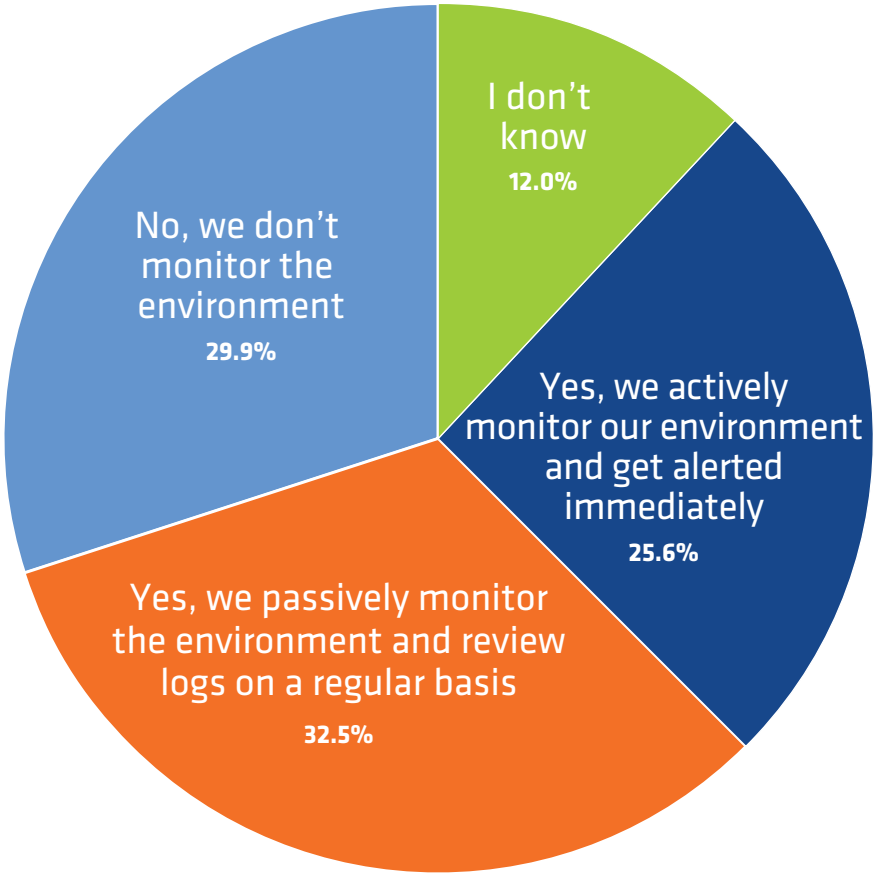
Over 60% of respondents have a secured internal network for critical resources. Nearly ⅔ of those organizations use this security measure for all of their resources. Respondents with larger budgets and IT staff are more likely to have these measures in place.



Does your organization monitor the environment for security events?

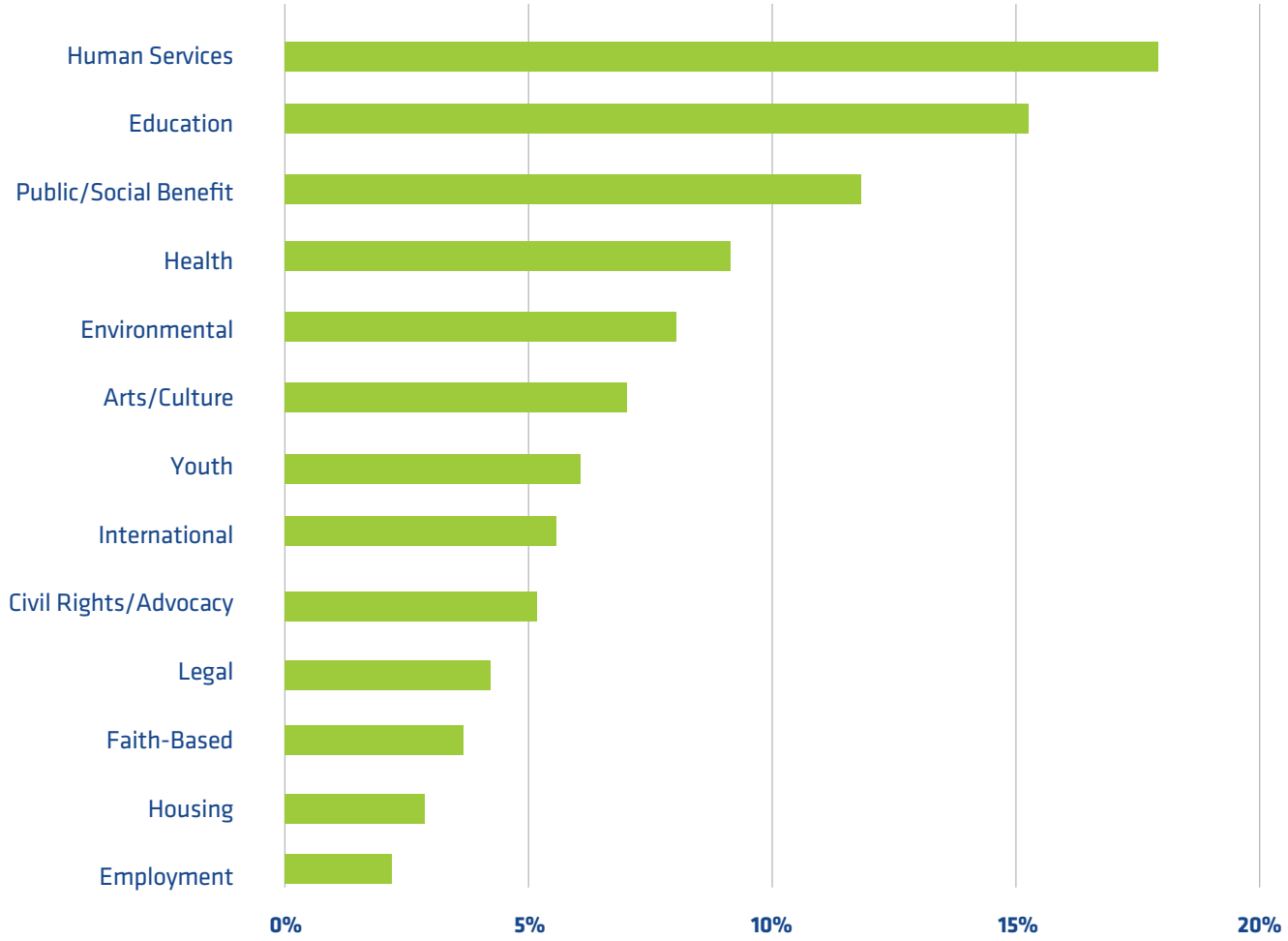
For example, a change in the way your network functions that could indicate a security policy has been violated or a safeguard failed.

Just under 60% of respondents perform some sort of security event monitoring. A slightly larger share of these perform passive monitoring rather than receiving real-time alerts. Organizational size and budget have little impact on these practices, but there is a close relationship with IT size. Larger IT shops are more likely to monitor, and the larger they are, the more active they are likely to be.



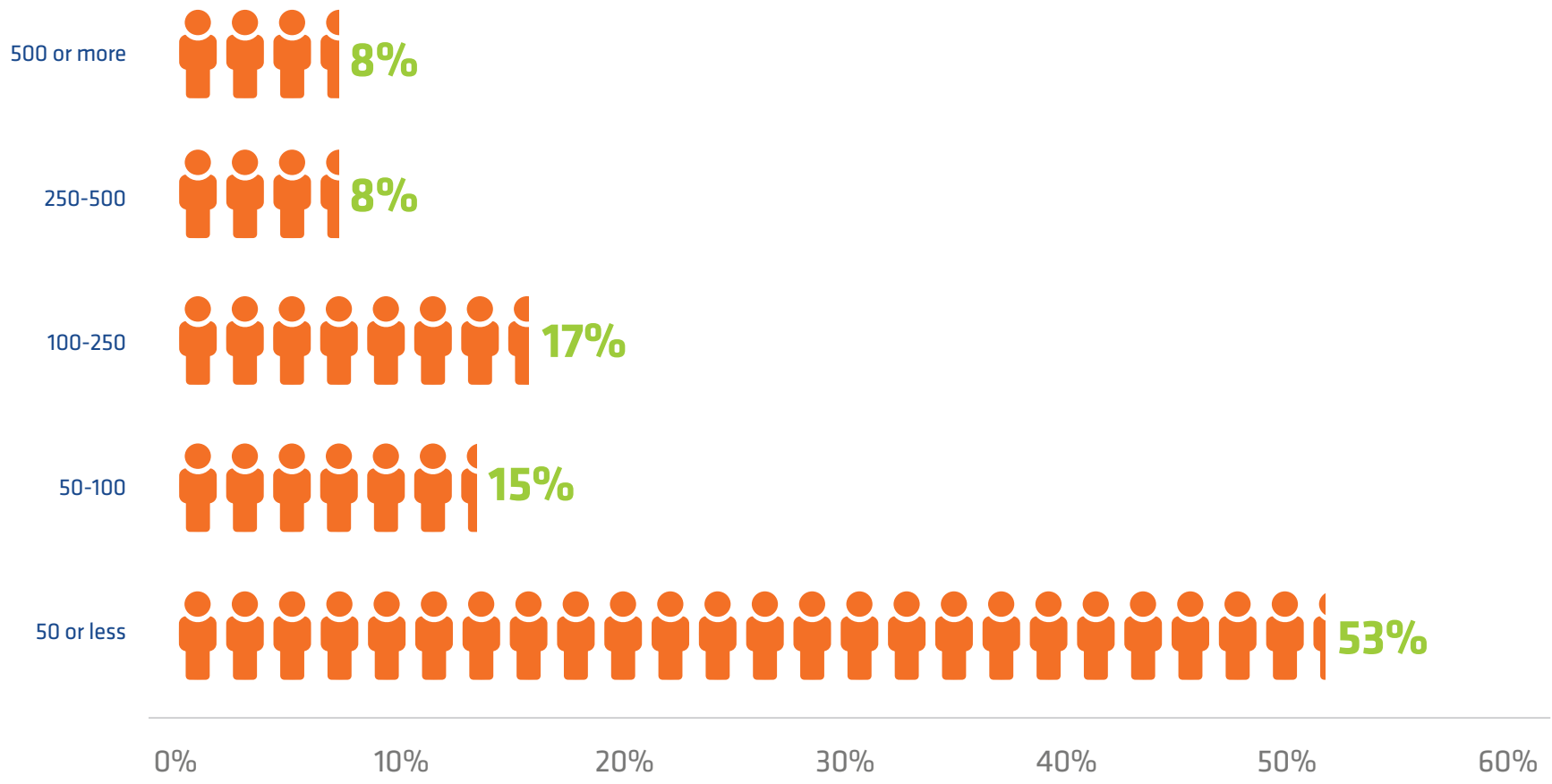
Demographics

What best describes your organization's primary issue area?

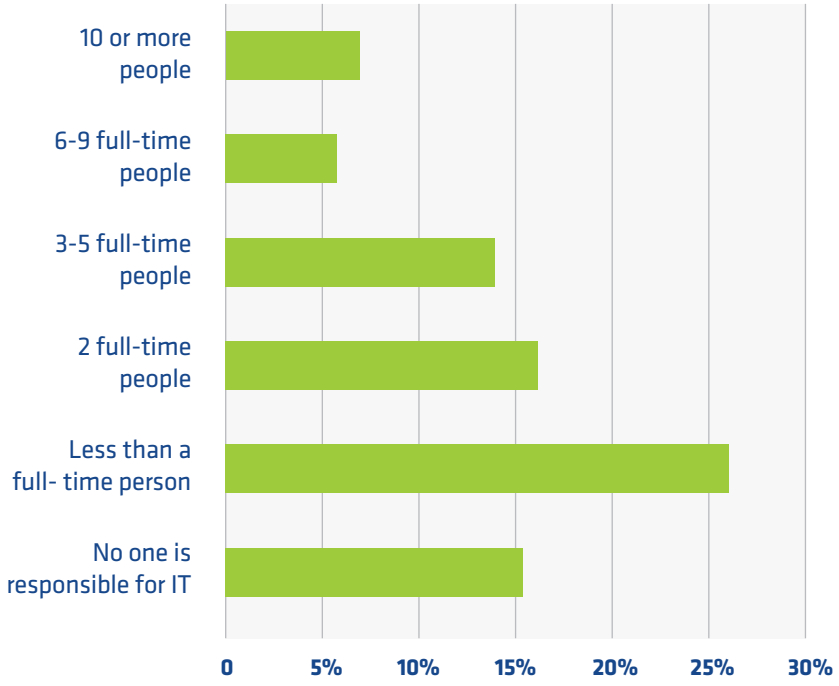


The majority of respondents work in the areas of human and public services, with four categories accounting for over half of the responses.

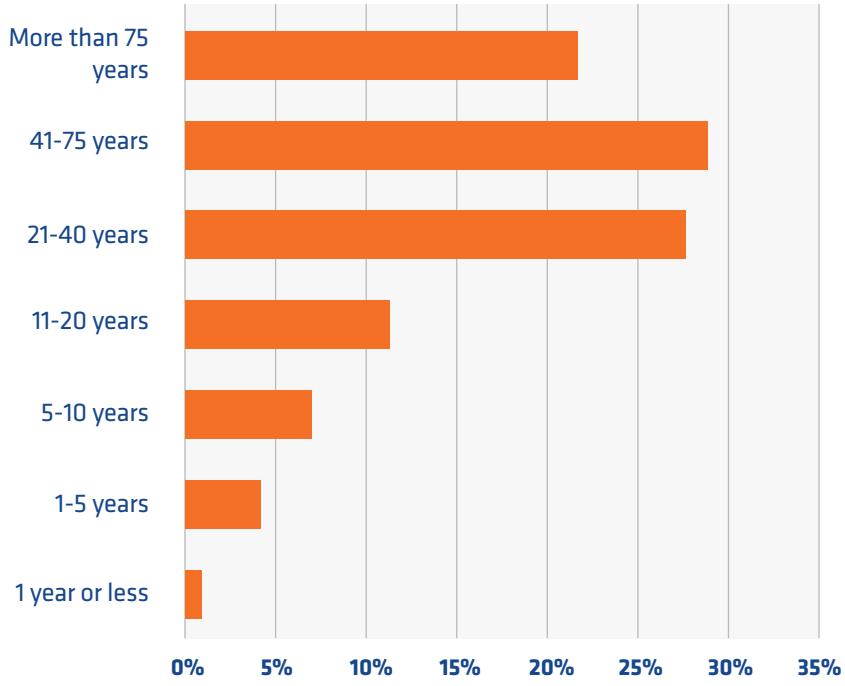
What is the size of your overall organization staff?



About how many IT staff members does your organization have?

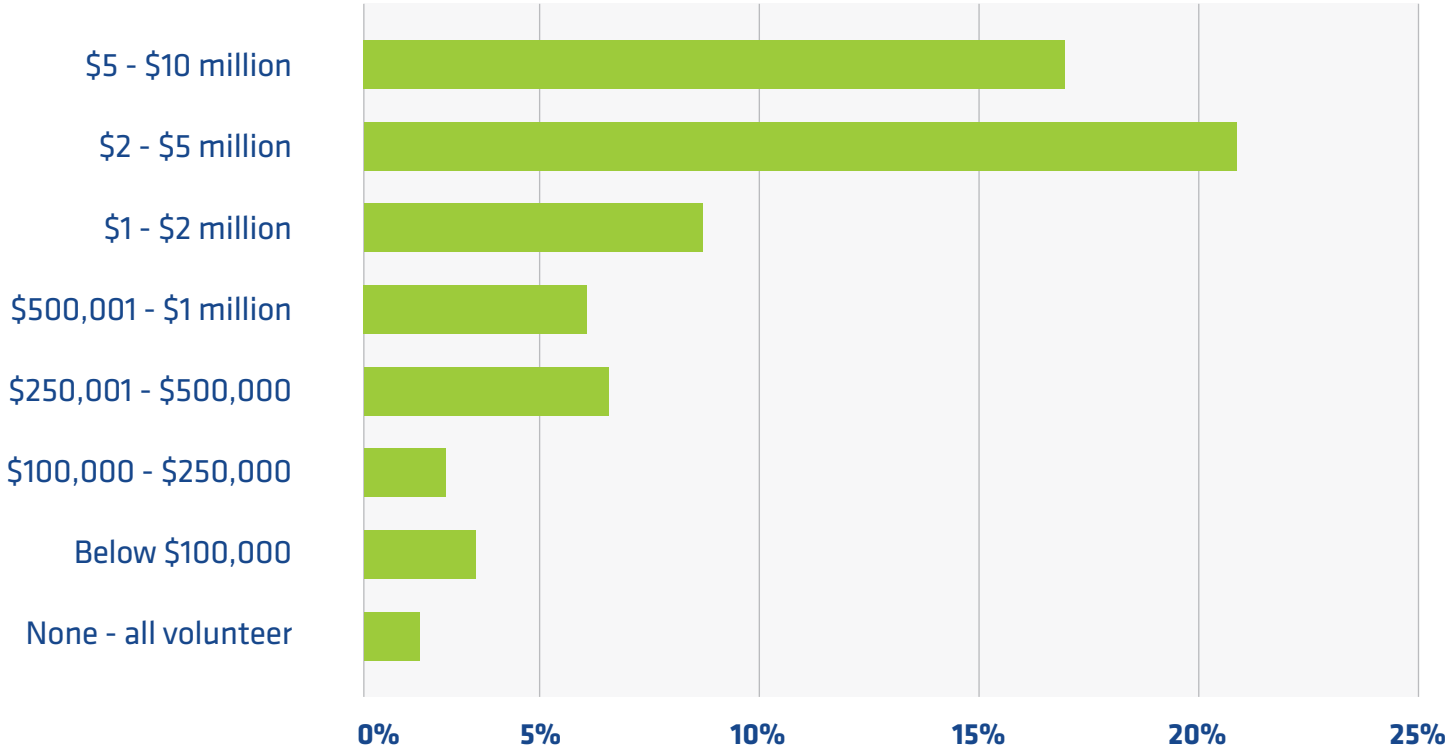


About how long has your organization existed?

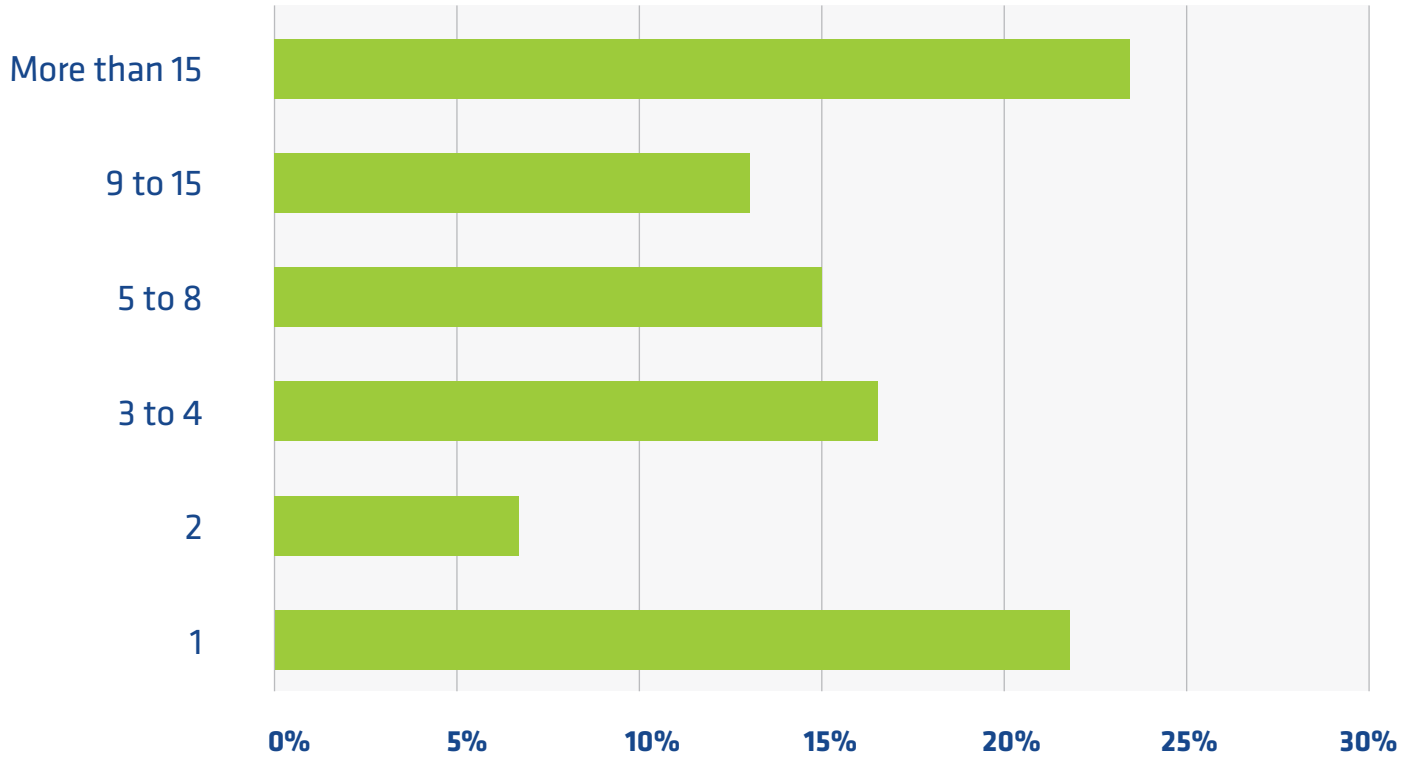


The majority of respondents represented well-established organizations; over two-thirds have operated 20 years or longer. Approximately 7% were relatively new (five years or fewer.)

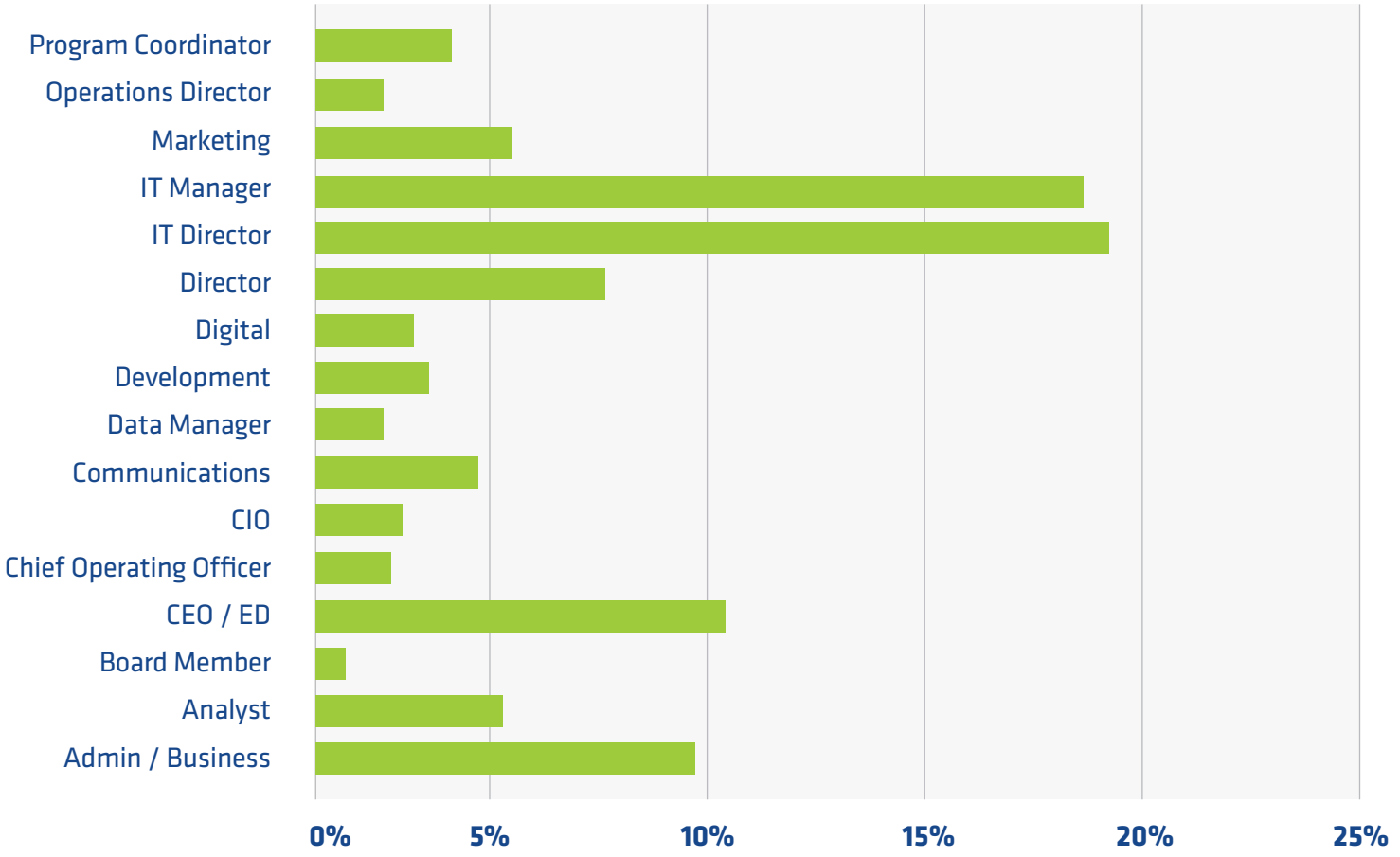
What is the approximate annual budget of your organization?



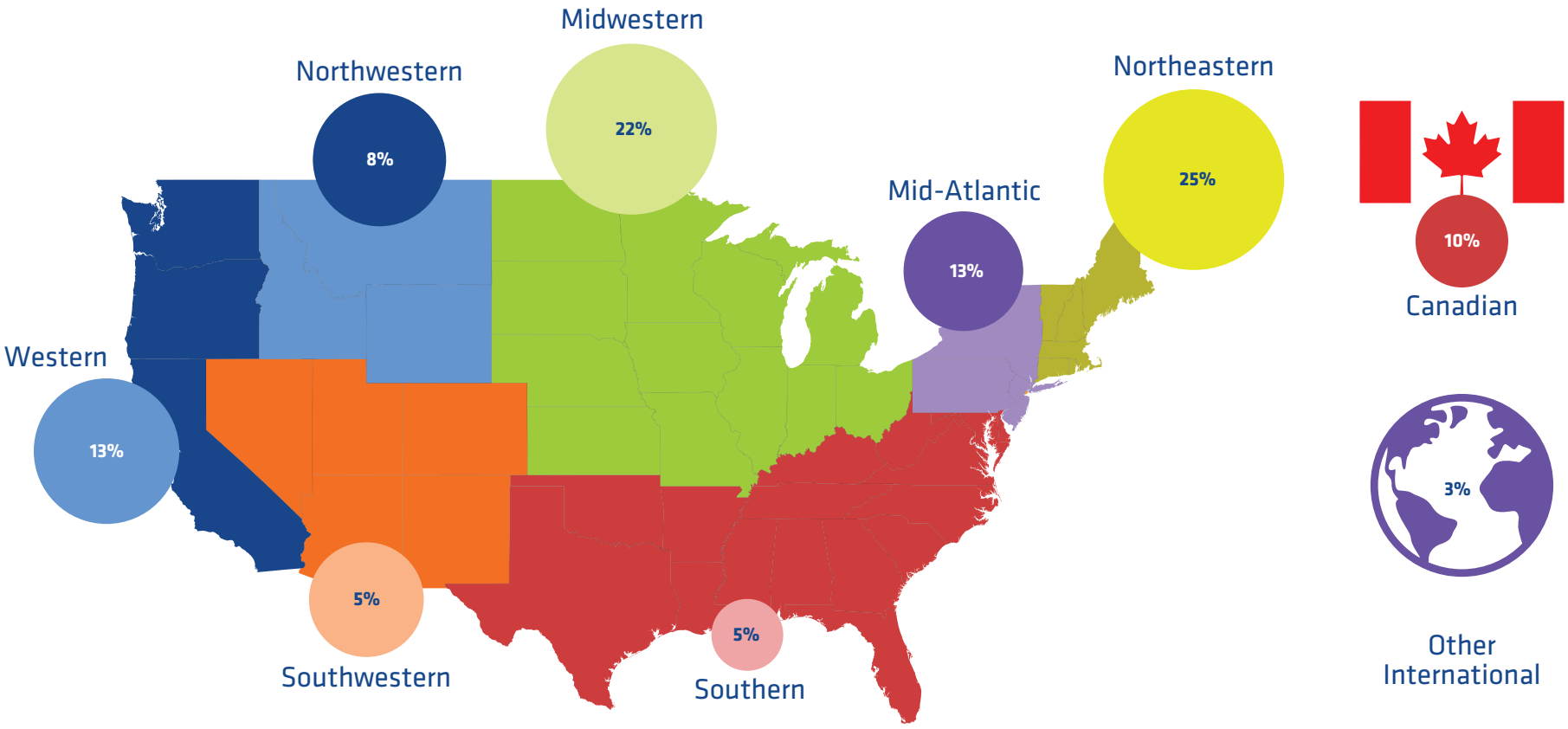
From about how many locations does your organization work? (offices, home, telecommuting)



What is your job title?



Where is your organization located?



nten
CONNECT ▸ LEARN ▸ CHANGE

About NTEN

We envision a more just and engaged world where all nonprofits use technology skillfully and confidently to meet community needs and fulfill their missions. We support organizations by convening the nonprofit community, offering professional credentials and training, and facilitating an open exchange of ideas.

NTEN reports support the growth and development of the sector through benchmarking the technology goals and challenges of nonprofits, and identifying areas of need. For more, visit **nten.org/reports**.

Microsoft

About Microsoft

Microsoft's Tech for Social Impact program empowers nonprofits and humanitarian organizations around the world with technology to advance their missions.

With recognition that many nonprofits have limited IT staff, the program provides solutions and resources that help nonprofits innovate new ways to tackle global issues. For more, visit **microsoft.com/nonprofits.**