Cybersecurity

July 2021

HIMSS auth0

Research Overview

HIMSS auth0

Research Overview

HIMSS Market Intelligence conducted this research in May to June 2021. The research was conducted among medical IT practitioners to understand cybersecurity awareness in a hospital / health system setting. Topics included:

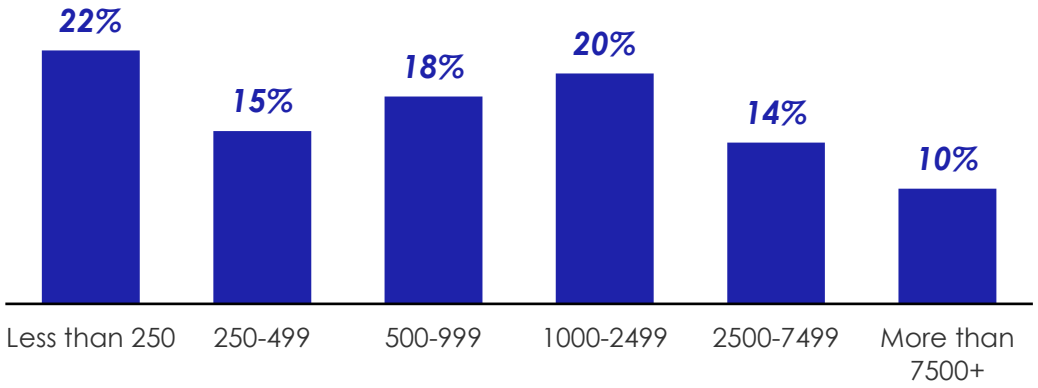
- Gauging baseline for security awareness
- Cybersecurity training
- Cybersecurity budgets and allocations
- Understanding what healthcare cybersecurity professionals are most concerned about

Methodology

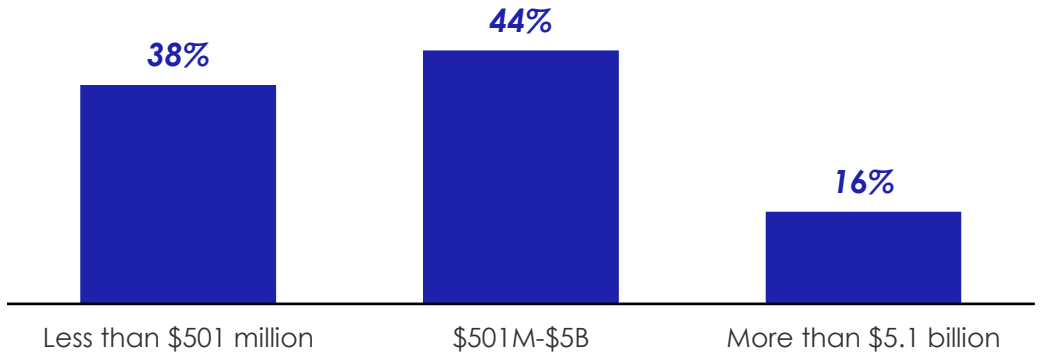
- This research was conducted online amongst IT practitioner leaders in healthcare in the United States.
- Respondents were screened for working in a relevant function (IT / Technology, IT security / Cybersecurity or Executive Leadership) and for having a role in decision making regarding cybersecurity at their organization.
- A total of 250 qualified respondents participated in this research.
- This was a blind data collection effort, Auth0 was not identified as a sponsor of the research.

Organizational Profile

Number of Hospital Beds

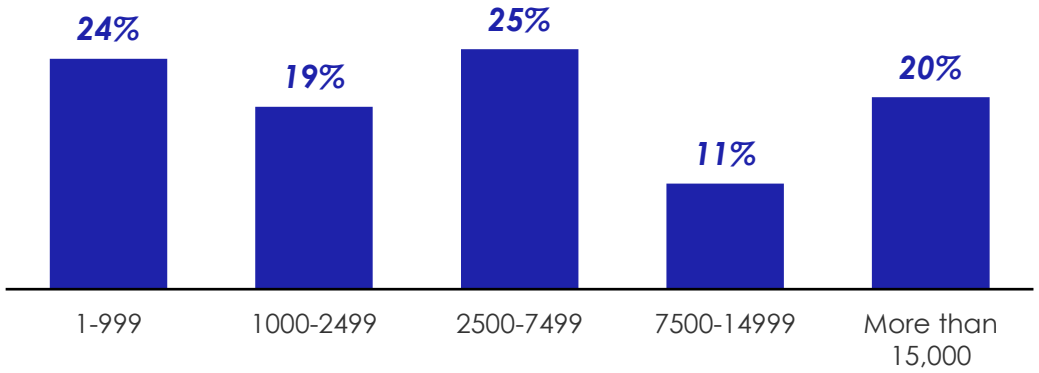


Annual Revenue



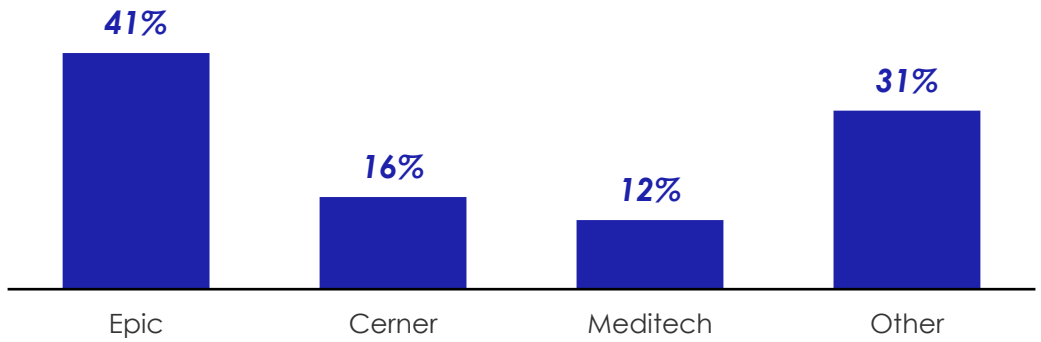
*Unsure/Can't discuss, 2%, not shown

Number of Employees



*Unknown, 1%, not shown

Primary EHR Platform

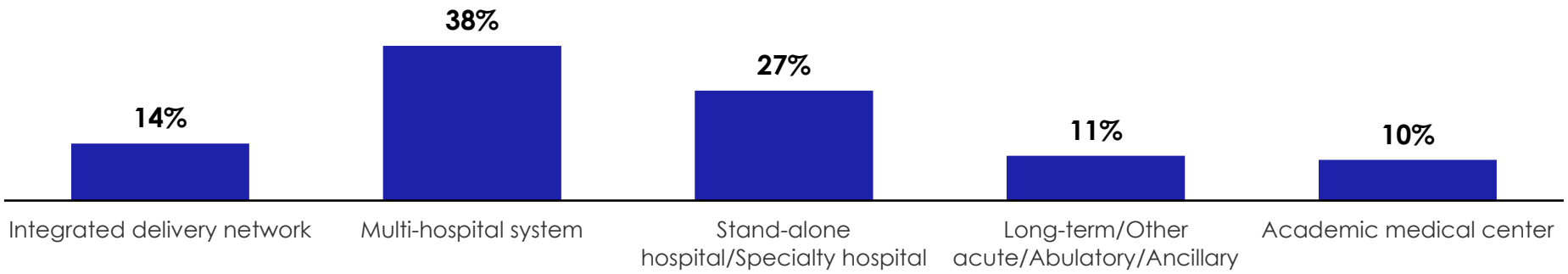


HIMSS auth0

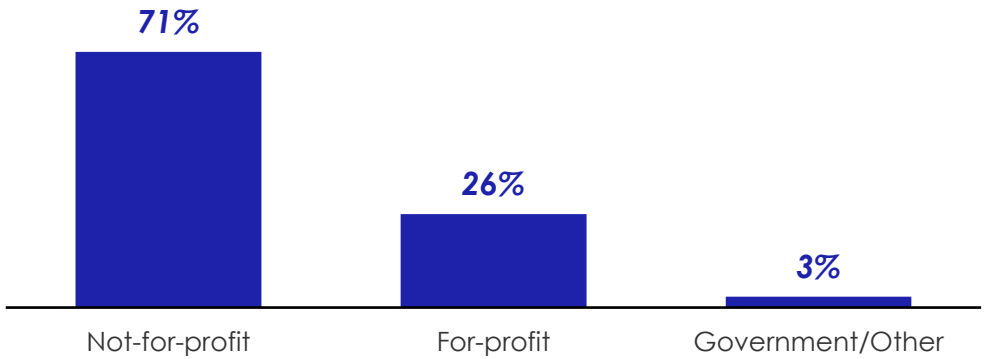
Please tell us the total number of hospital beds in your organization.
What is your organization's annual net revenue?
Please tell us the total number of employees in your organization.
What is your organization's primary EHR (electronic health records) platform?
Base: Total Respondents; n=250

Organizational Profile

Worksite



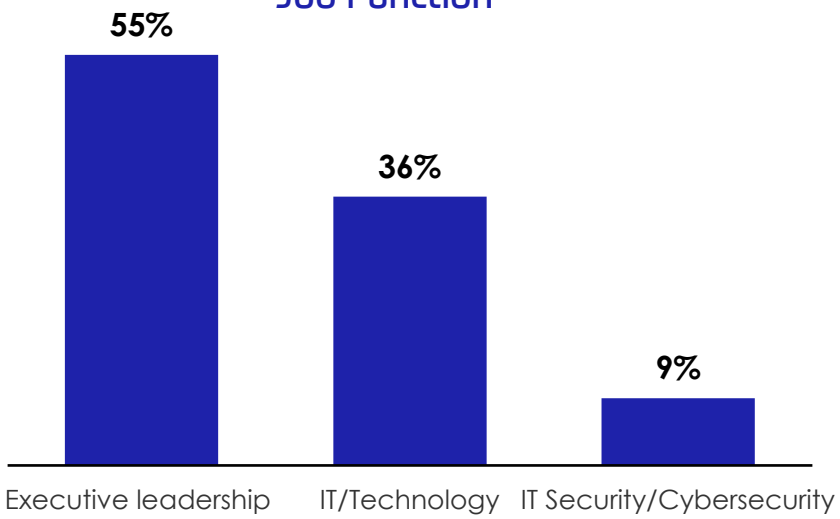
Ownership



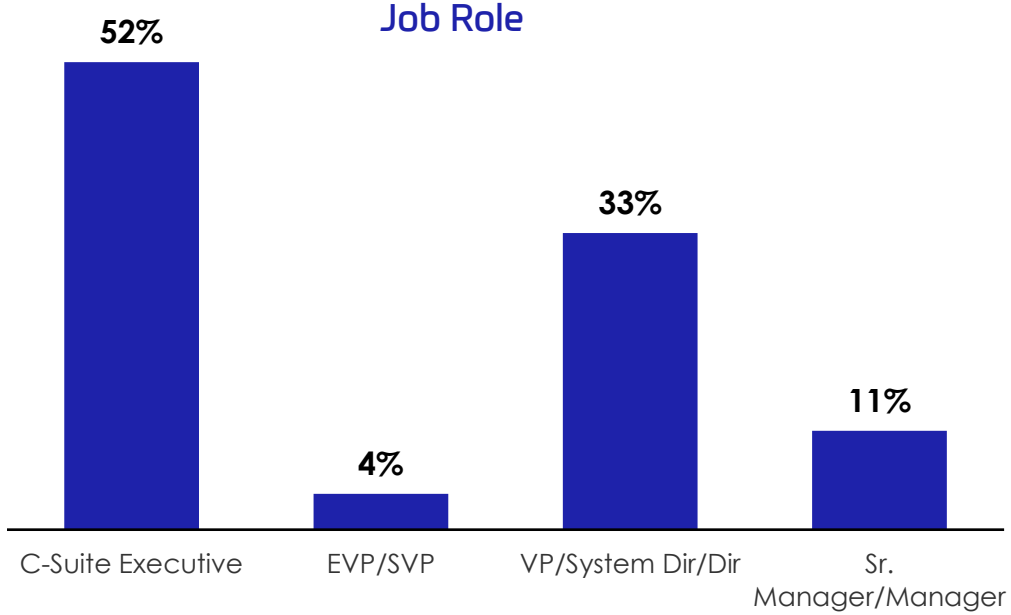
Which of the following best describes your health system/hospital ownership?
Which of the following best describes your worksite?
Base: Total Respondents; n=250

Respondent Profile

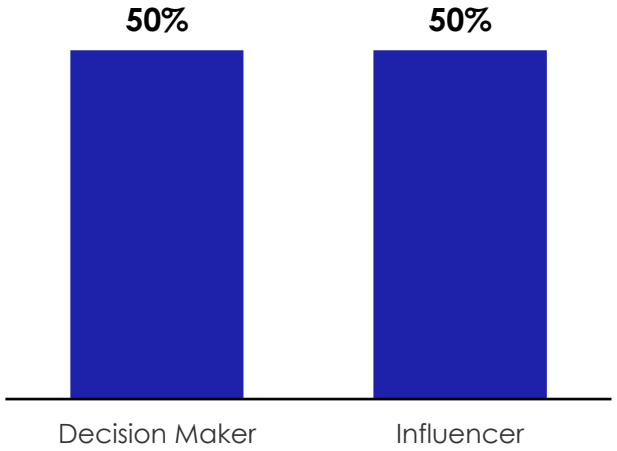
Job Function



Job Role



Role Regarding Cybersecurity



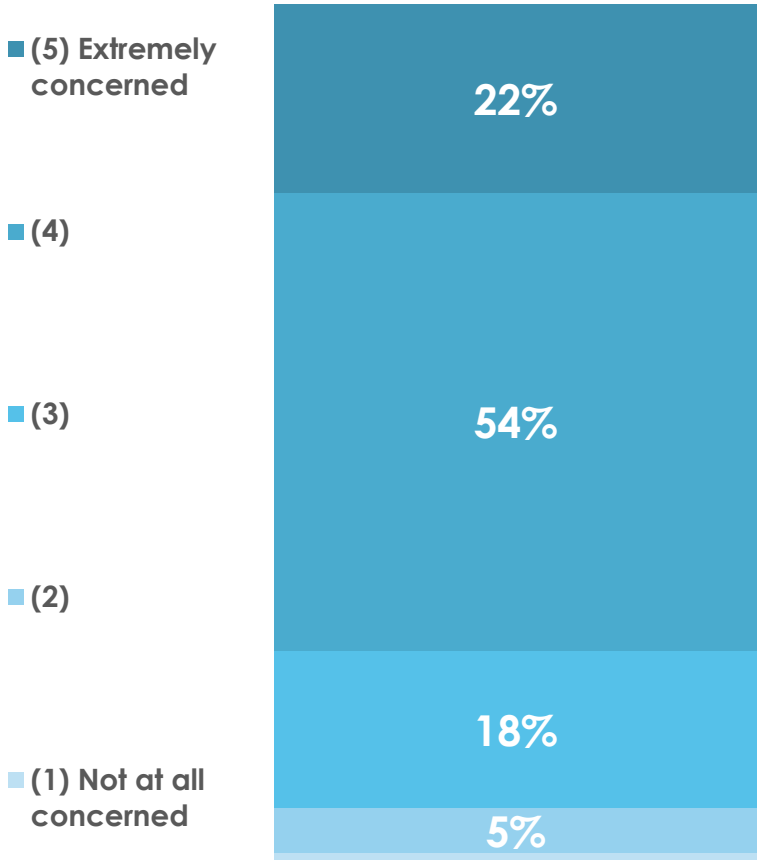
How would you characterize your job role or function?
What is your current role?
Which of the following best describes your role regarding cybersecurity at your organization?
Base: Total Respondents; n=250

Detailed Findings

HIMSS auth0

3-in-4 are concerned about the possibility of a security breach on their organization's network connected medical devices

Tell us your level of concern when thinking of your organization's network connected medical devices and the possibility of a security breach



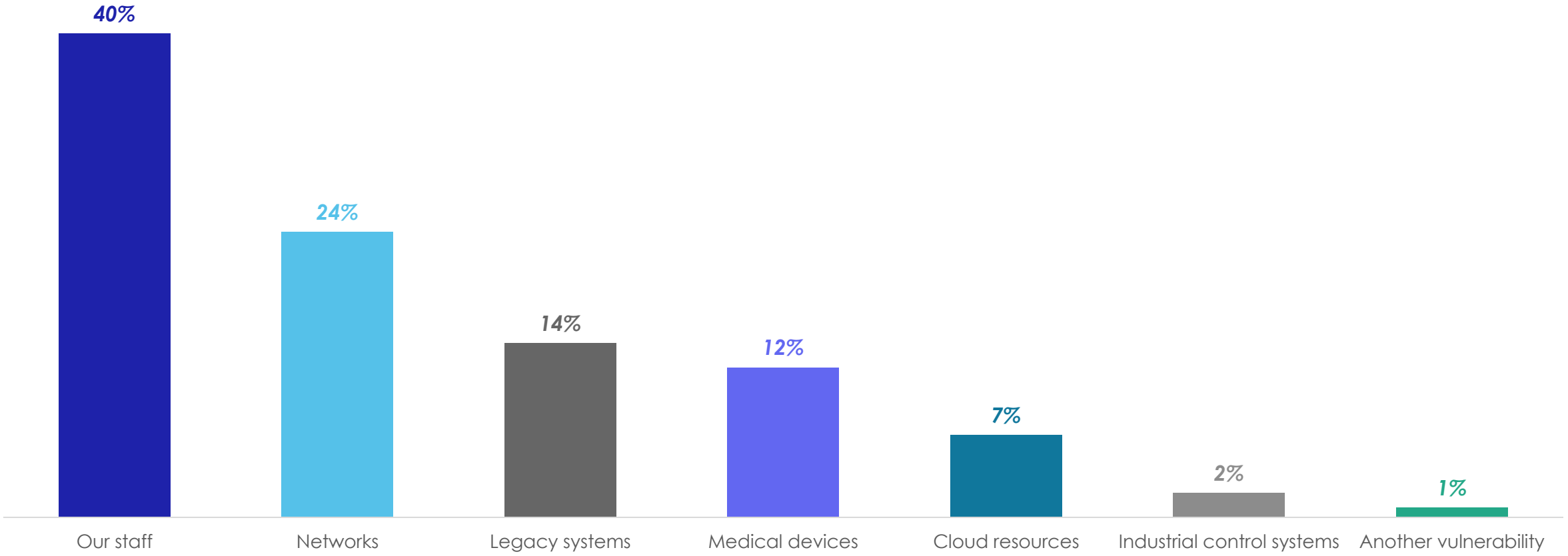
76% of participants are concerned about the possibility of a security breach

Data labels under 5% not shown

On a scale of 1-5 where 1=Not at all concerned and 5=Extremely concerned, please tell us your level of concern when thinking of your organization's network connected medical devices and the possibility of a security breach i.e.: a security attack.
Base: Total Respondents: n=250

The staff at organizations is seen as the biggest cybersecurity vulnerability

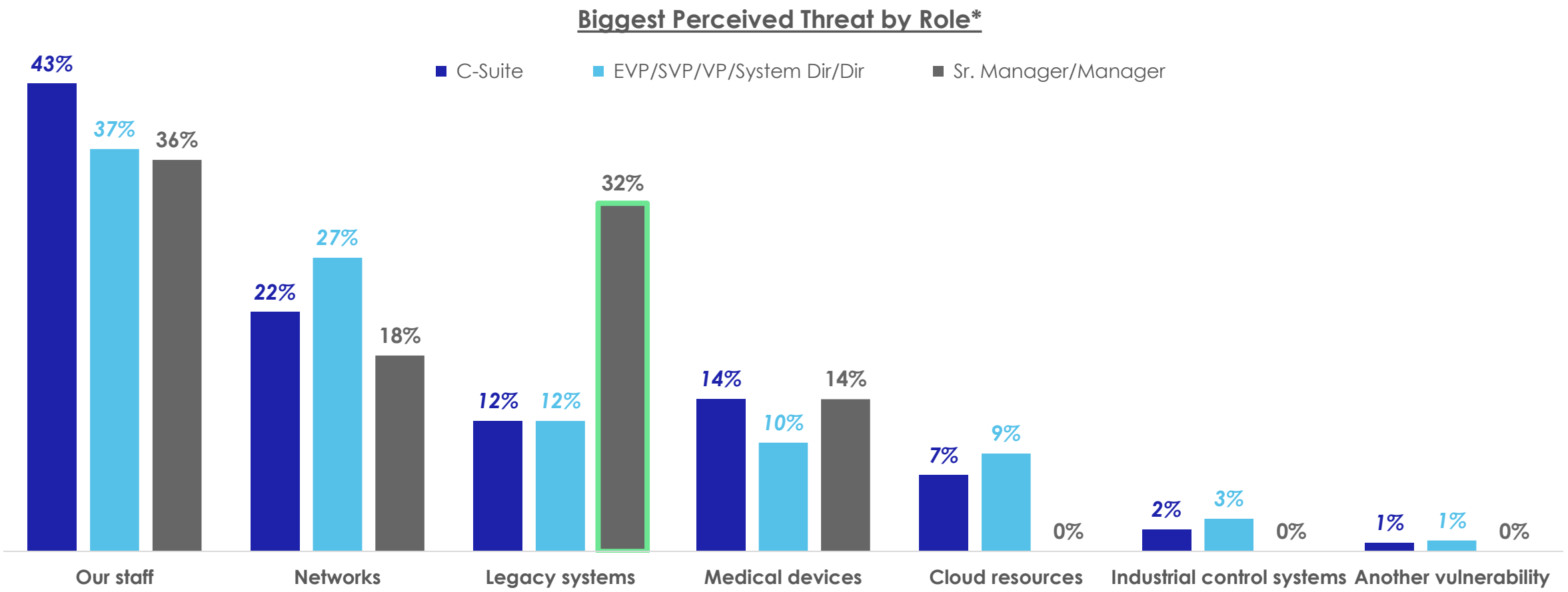
What do you perceive as the biggest cybersecurity vulnerability at your organization?



What do you perceive as the biggest cybersecurity vulnerability at your organization?
Base: Total respondents; n=250

Managers see legacy systems as a significantly bigger threat compared to those in a higher role

What do you perceive as the biggest cybersecurity vulnerability at your organization?



*Small base size, insight is directional

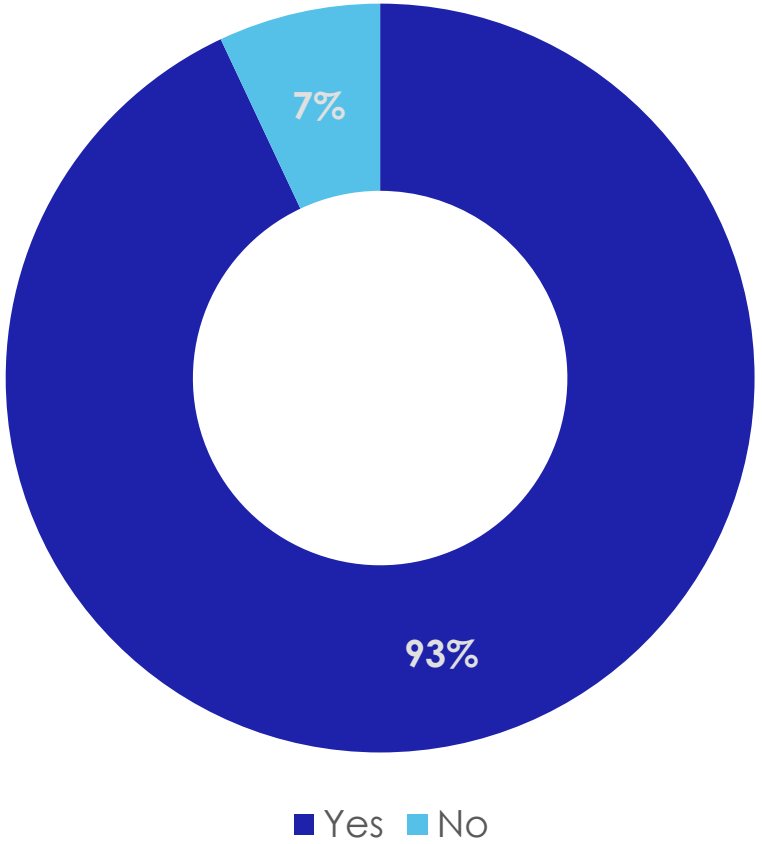
HIMSS auth0

Denotes statistically significant difference at the 95% confidence level.

What do you perceive as the biggest cybersecurity vulnerability at your organization?
Base: Total respondents; n=250

The majority are conducting cybersecurity training within their organization

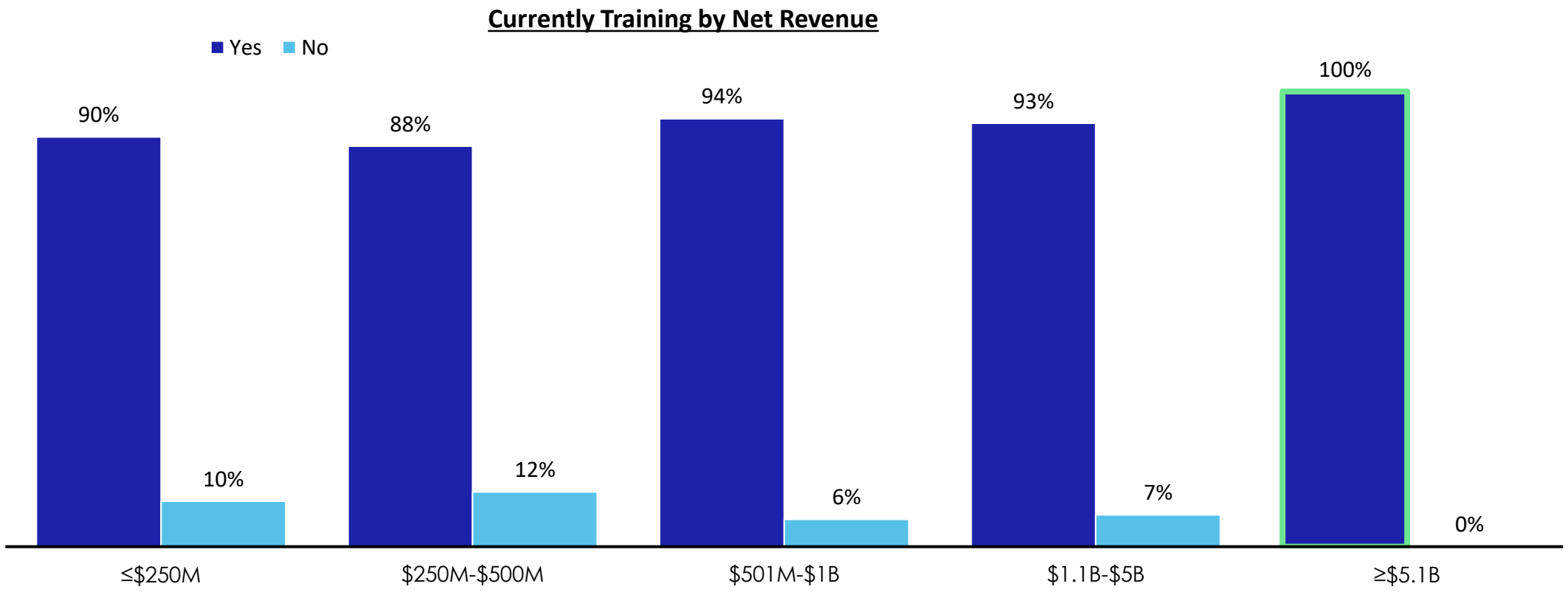
Do you currently train on cybersecurity within your organization?



Do you currently train on cybersecurity within your organization?
Base: Total Respondents; n=250

All respondents in organizations with a annual net revenue of ≥$5.1B are currently training on cybersecurity

Do you currently train on cybersecurity within your organization?

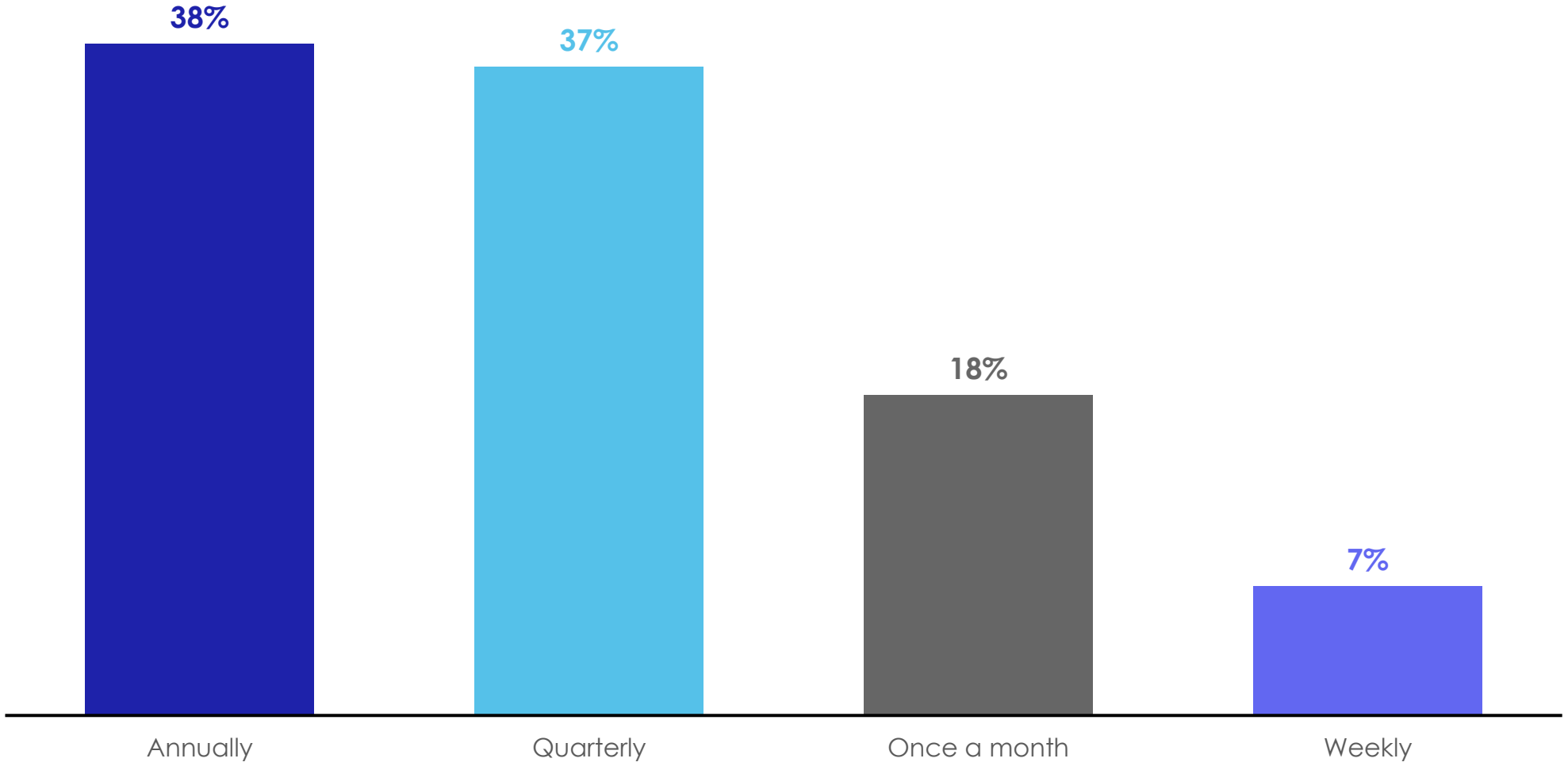


Denotes statistically significant difference at the 95% confidence level.

Do you currently train on cybersecurity within your organization?
Base: Total Respondents; n=250

With 3-in-4 conducting cybersecurity awareness training at least quarterly on average

On average, how often does your organization conduct cybersecurity awareness training?

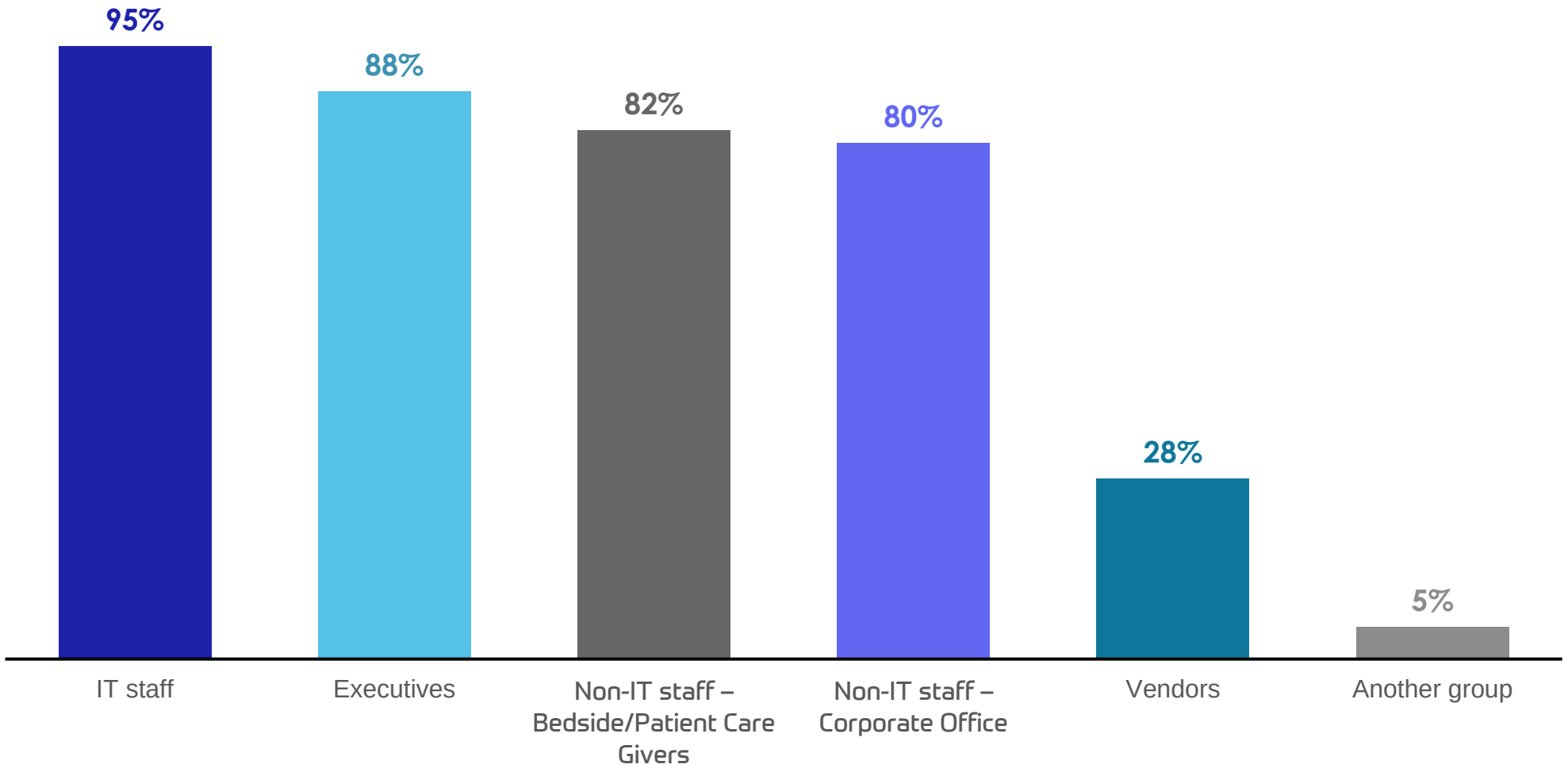


HIMSS auth0

On average, how often does your organization conduct cybersecurity awareness training?
Base: Currently train on cybersecurity; n=232

8-in-10 Non-IT staff are trained on cybersecurity awareness, with only nearly a third of their vendors being trained

Which groups do you currently train on cybersecurity awareness?

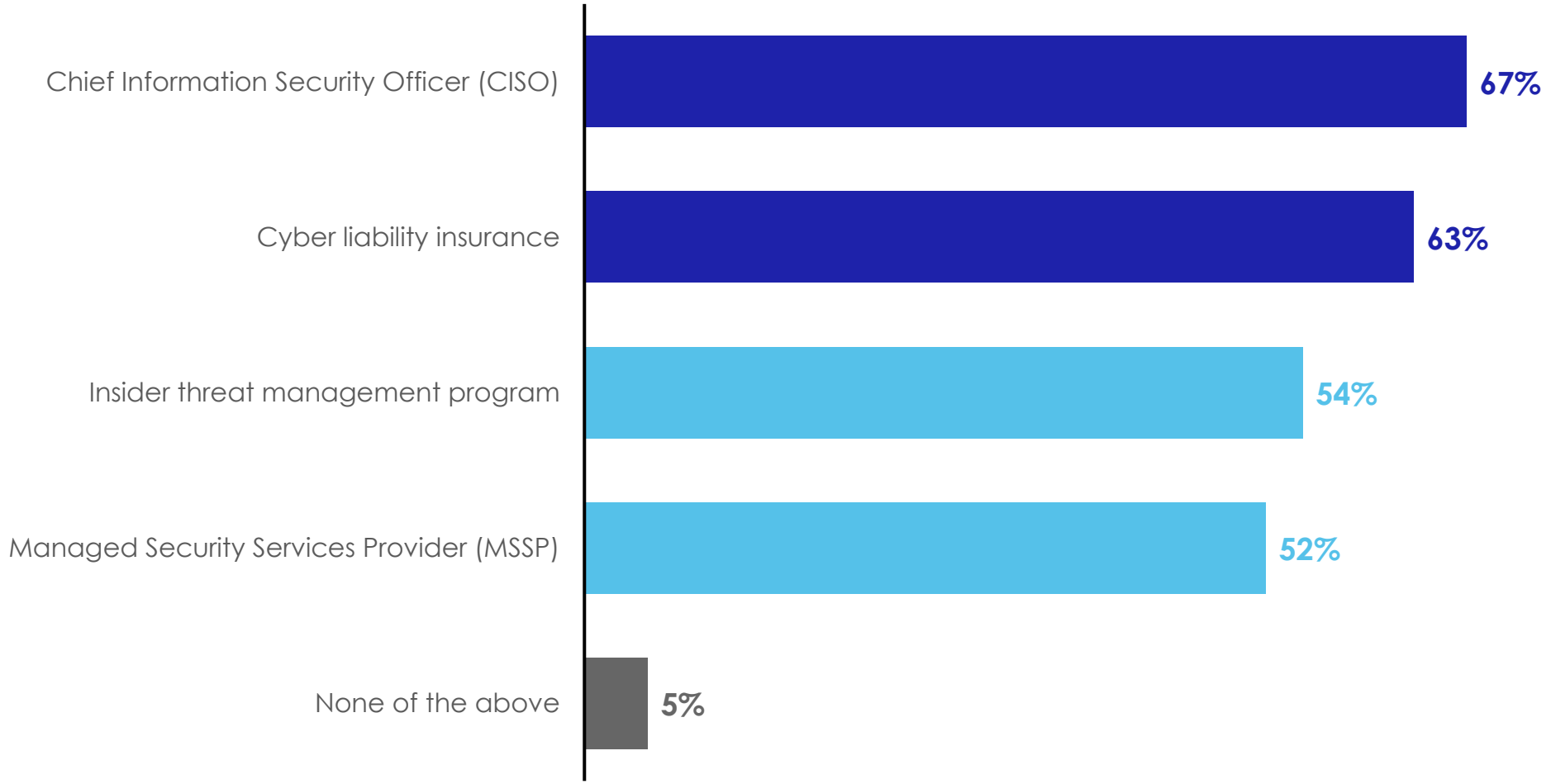


HIMSS auth0

Which groups do you currently train on cybersecurity awareness?
Base: Currently train on cybersecurity; n=232

Over 6-in-10 organizations have a CISO or use Cyber liability insurance, with half having an Insider threat mgmt program and MSSP

Which, if any, of the following does your organization have and/or use?

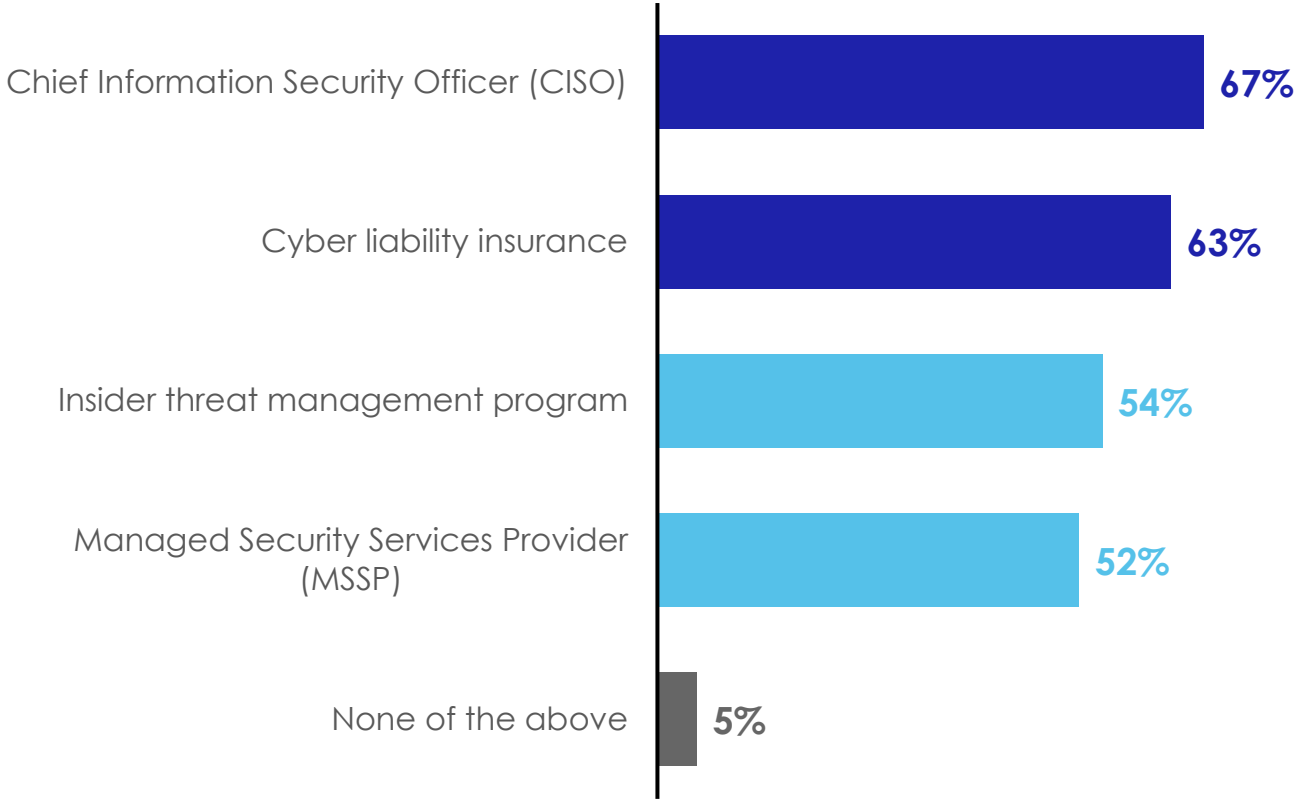


HIMSS auth0

Which, if any, of the following does your organization have and/or use?
Base: Total Respondents; n=250

The majority of organizations with a net revenue of ≥$5.1B have a CISO

Which, if any, of the following does your organization have and/or use?



Organizations with a net revenue of ≥$5.1B have a CISO significantly more compared to those with a net revenue of <$5B

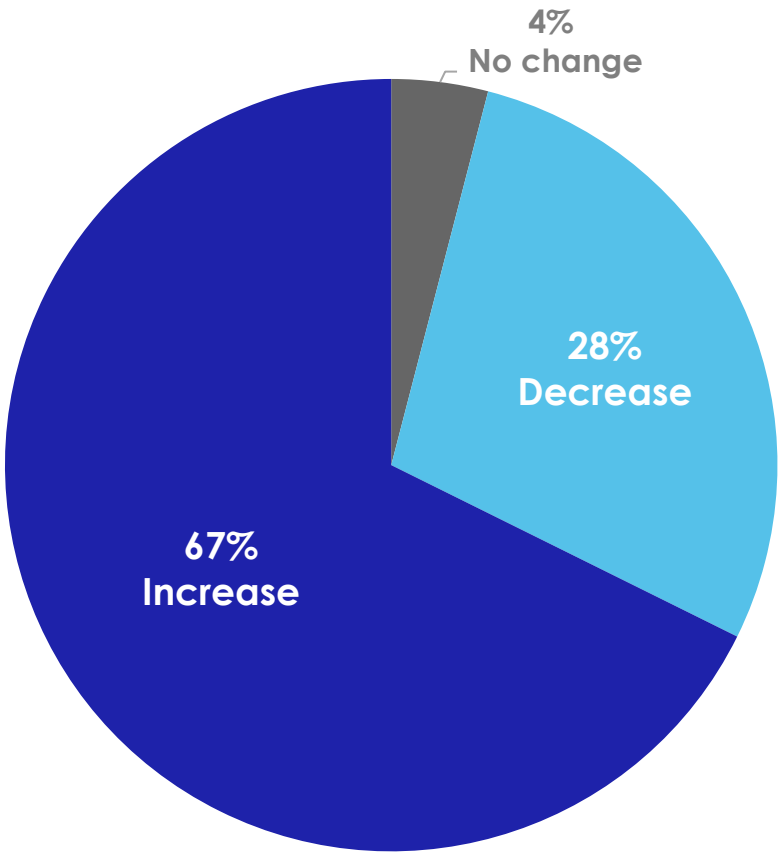
93% v. 72%-41%

HIMSS auth0

Which, if any, of the following does your organization have and/or use?
Base: Total Respondents; n=250

Nearly 7-in-10 have seen an increase in their cybersecurity budget in the last 12 months

How has your cybersecurity budget changed in the last 12 months?

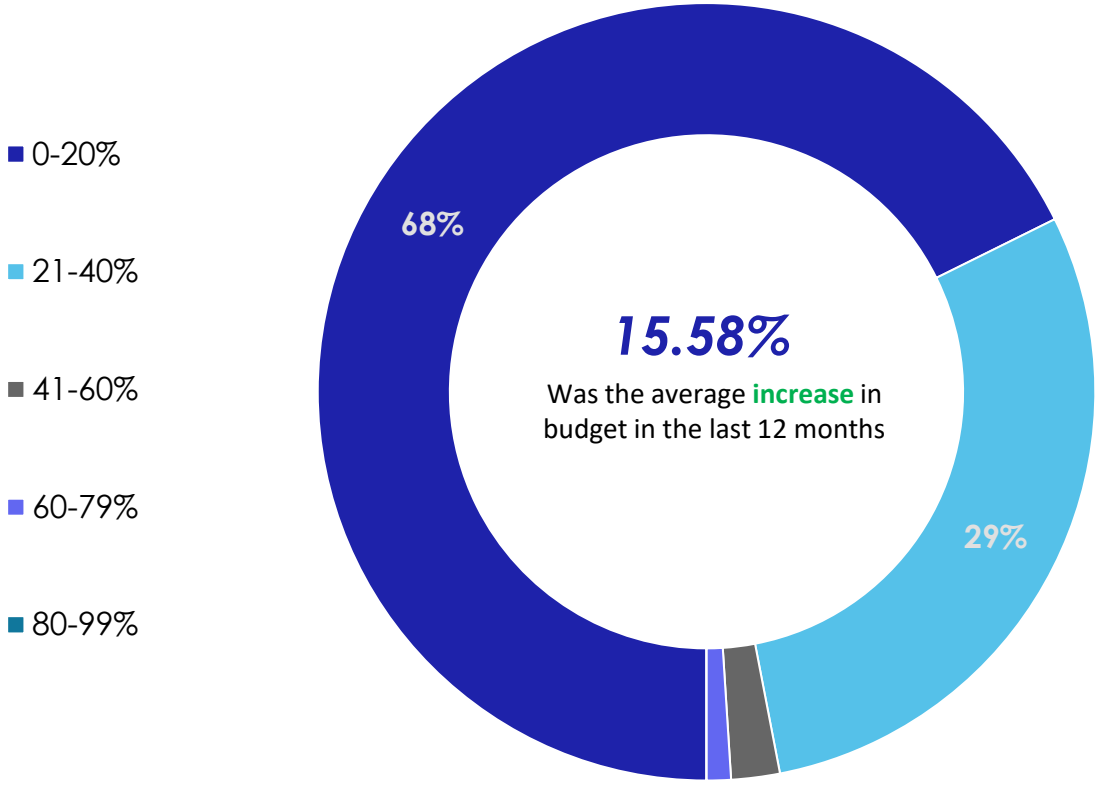


Don't know, 2%, not shown

How has your cybersecurity budget changed in the last 12 months?
Base: Total Respondents: n=250

Although, 7-in-10 only saw a budget increase of 20% or less

Estimate the percent your budget has increased/decreased in the last 12 months.



Of those that confirmed they had an increase or decrease in budget, the majority stated an increase in the cybersecurity budget occurred.

95% v. 5%

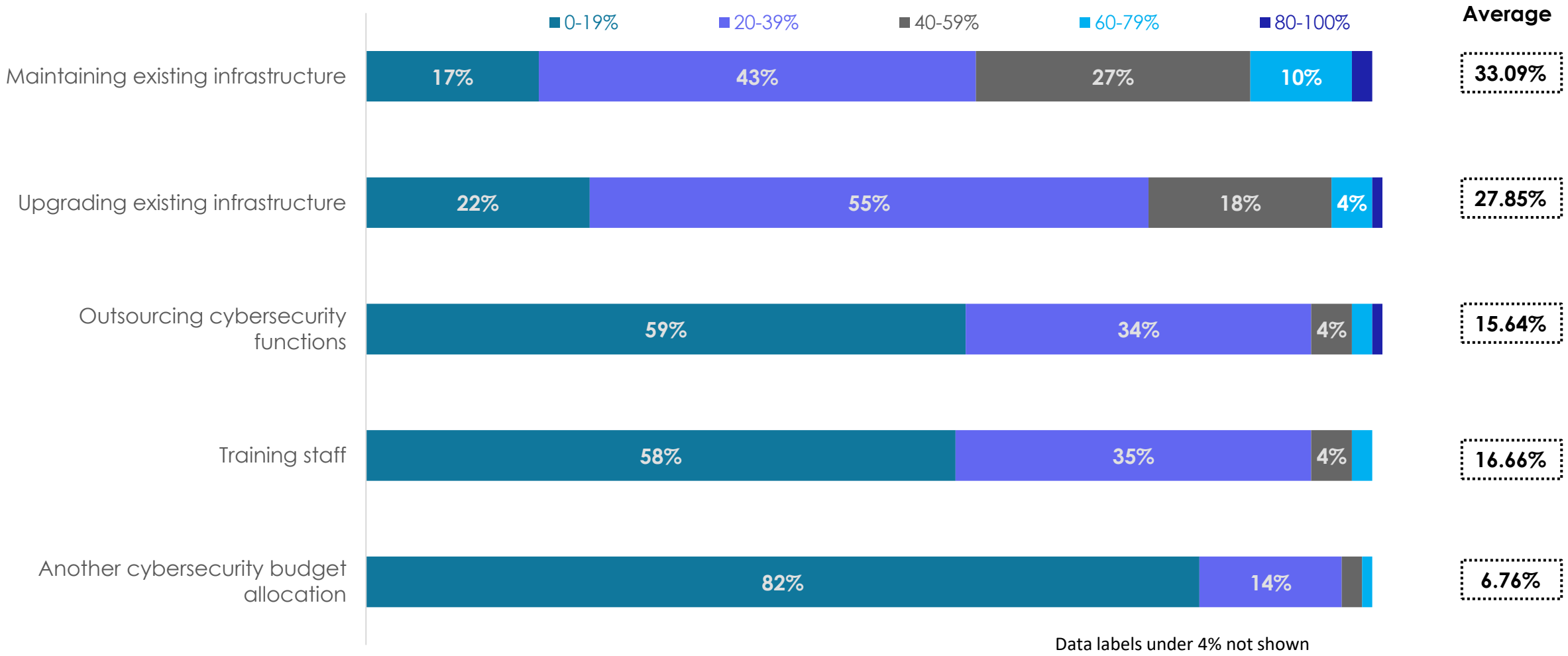
Data labels less than 4% not shown

HIMSS auth0

And, please estimate the percent your budget has increased/decreased in the last 12 months.
Base: Percent business has increased/decreased in the last 12 months; Increase n=167

With the largest percent of the cybersecurity budgets being invested in maintaining / upgrading existing infrastructure

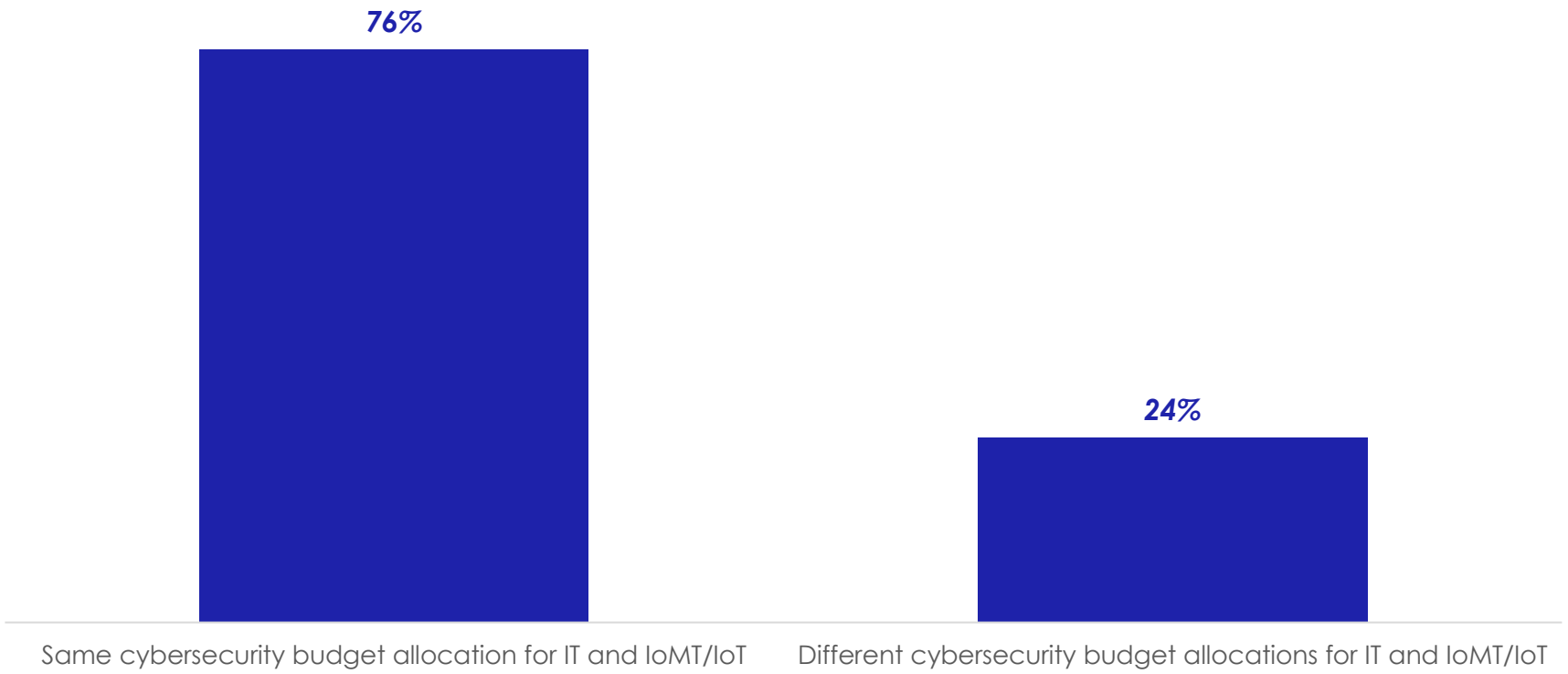
By percentage, please tell us, on average, the relative cybersecurity budget allocation for…?



By percentage, please tell us, on average, the relative cybersecurity budget allocation for…?
Base: Total Respondents; n=250

Only 1-in-4 currently have a different cybersecurity budget allocation for IT and IoMT/IoT

My organization has the…



Which of the following best describes your organization?
Base: Total respondents; n=250

Key Takeaways

1 3-in-4 are concerned about the possibility of a security breach

Over 60% of organizations have a CISO (67%) and/or use cyber liability insurance (63%). The majority (93%) with a net revenue of ≥$5.1B, have a CISO.

2 Staff is seen as the biggest cybersecurity vulnerability

The majority (93%) are conducting cybersecurity training within their organization and those with a net revenue of ≥$5.1B, having 100% currently training on cybersecurity. On average, cybersecurity training is occurring at least quarterly (75%). While the majority of Non-IT staff (80%-82%) are being trained, vendors (28%) are not.

3 Nearly 7-in-10 have seen an increase in their cybersecurity budget in the last 12 months

Majority (82%) only seeing an increase of 20% or less. The largest percent of the cybersecurity budget being invested in maintaining (33%) and upgrading (28%) existing infrastructure. Not many have a different cybersecurity budget allocations for IT and IoMT/IoT (24%). HIPAA violations (87%) and patient safety (82%) are top of mind as cybersecurity budgets are created.

4 Only half have security technologies in place for their employees

Although staff is deemed to be the biggest cyber security vulnerability, encryption for archived files/data (50%), anti-theft devices (54%), digital forensics (54%)or a business continuity/disaster recovery plan (55%) is stated to only be enabled for employees at half of the organizations. Nearly a third are planning to implement biometrics (29%), digital forensics (28%), or penetration testing (28%) within the next 24 months. With larger organizations (*28% at a net rev. of $1.1B-$5B; 32% at a net rev. of ≥$5.1B*) significantly more likely to implement biometrics in less than 12 months.

About Auth0

The Auth0 Identity Platform, a product unit within Okta, takes a modern approach to identity and enables organizations to provide secure access to any application, for any user. Auth0 is a highly customizable platform that is as simple as development teams want, and as flexible as they need. Safeguarding billions of login transactions each month, Auth0 delivers convenience, privacy, and security so customers can focus on innovation. For more information, visit https://auth0.com.

Thank You

For more information please contact:

Nicole Ramage
Market Intelligence Manager
Nicole.Ramage@himss.org