



Cybersecurity

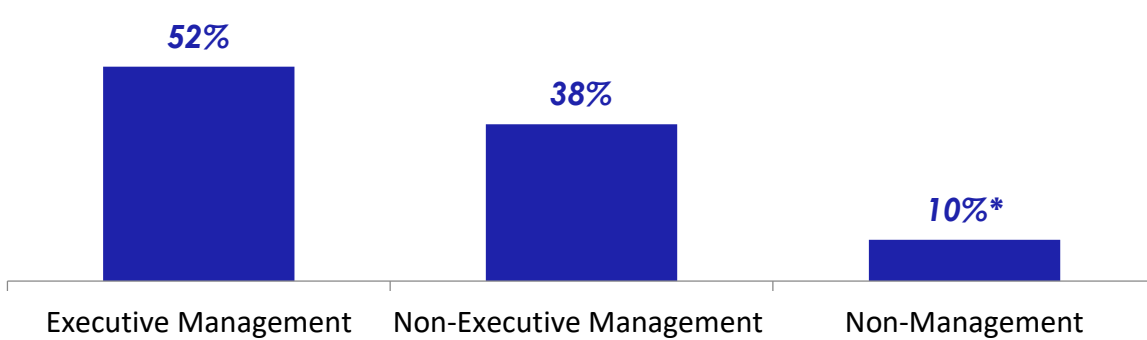
January 2022



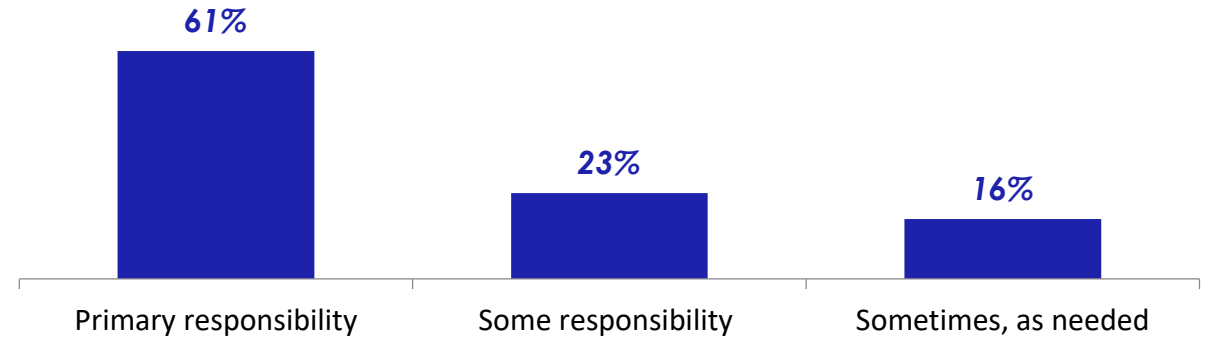
Research Overview

Respondent Profile

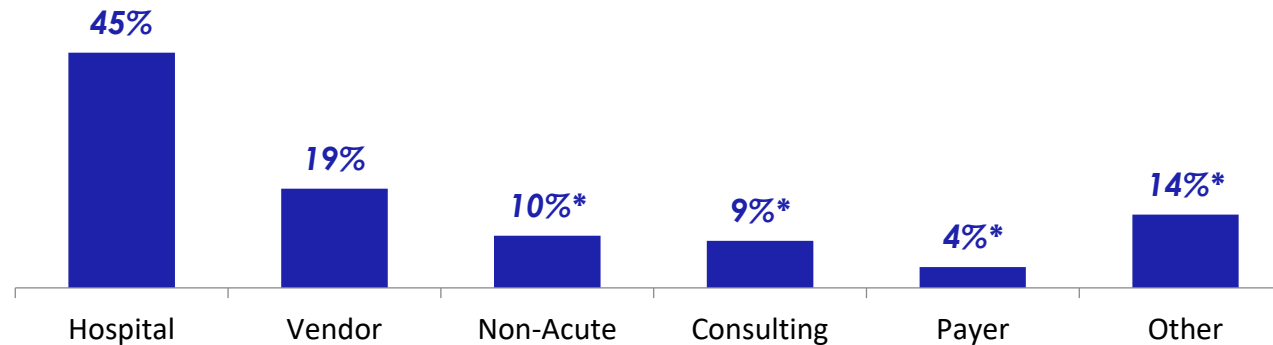
Job Role



Responsibility in Cybersecurity



Organization Type



**Small base sizes, insight is directional*

Percentages may not add up to 100% due to rounding.

Which of the following best describes the role that you hold at your organization?
To what extent are you responsible for oversight or day-to-day-operations of the cybersecurity program at your organization?

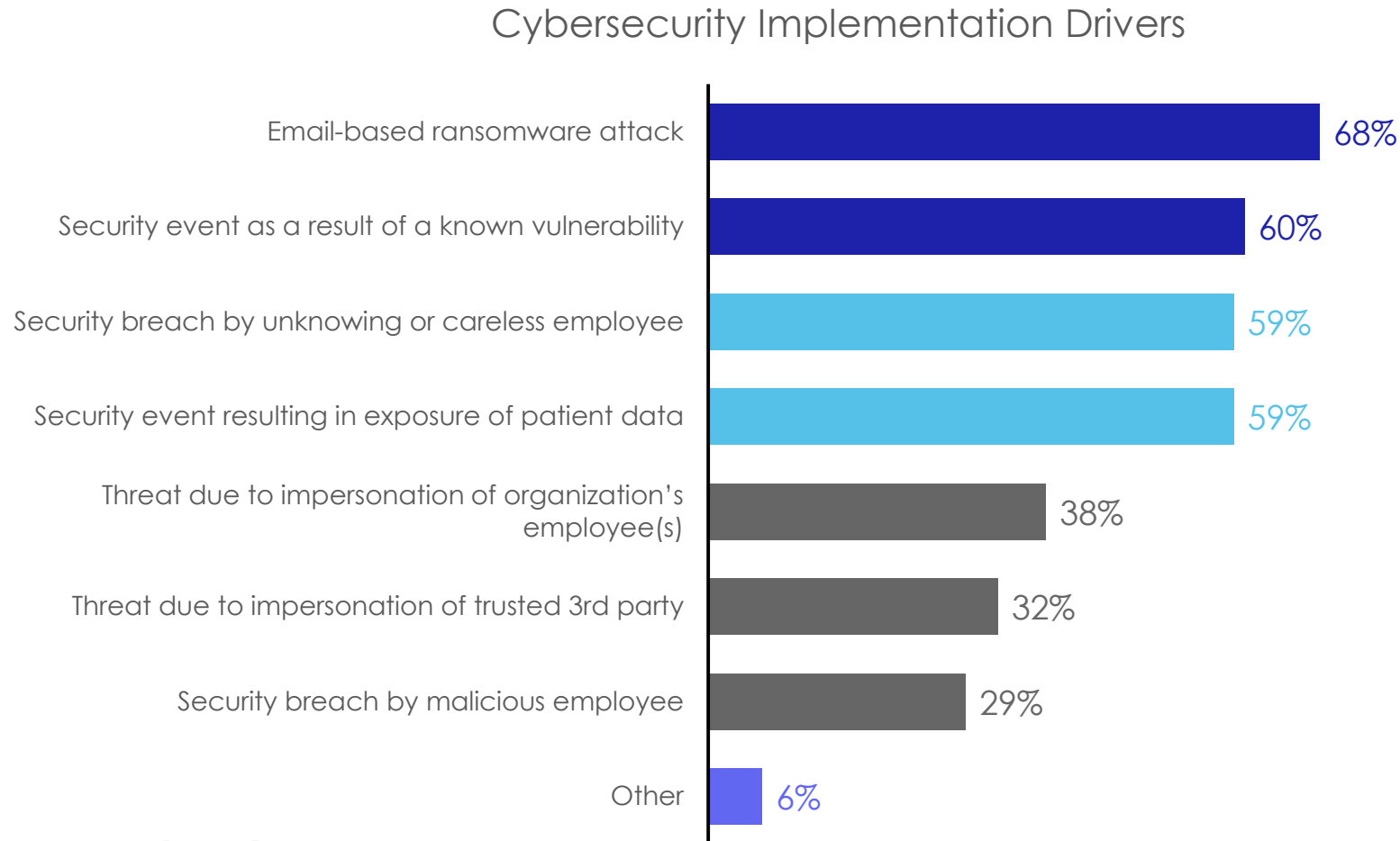
Which of the following best describes the type of organization at which you work?
Base: Total Respondents; n = 167



Detailed Findings

Nearly 7-in-10 are motivated to implement cybersecurity tools / technology due to email - based ransomware attacks, while approximately 60% have seen a security event or breach

Which, if any, of the below factors currently drive your implementation of cybersecurity tools / technology?

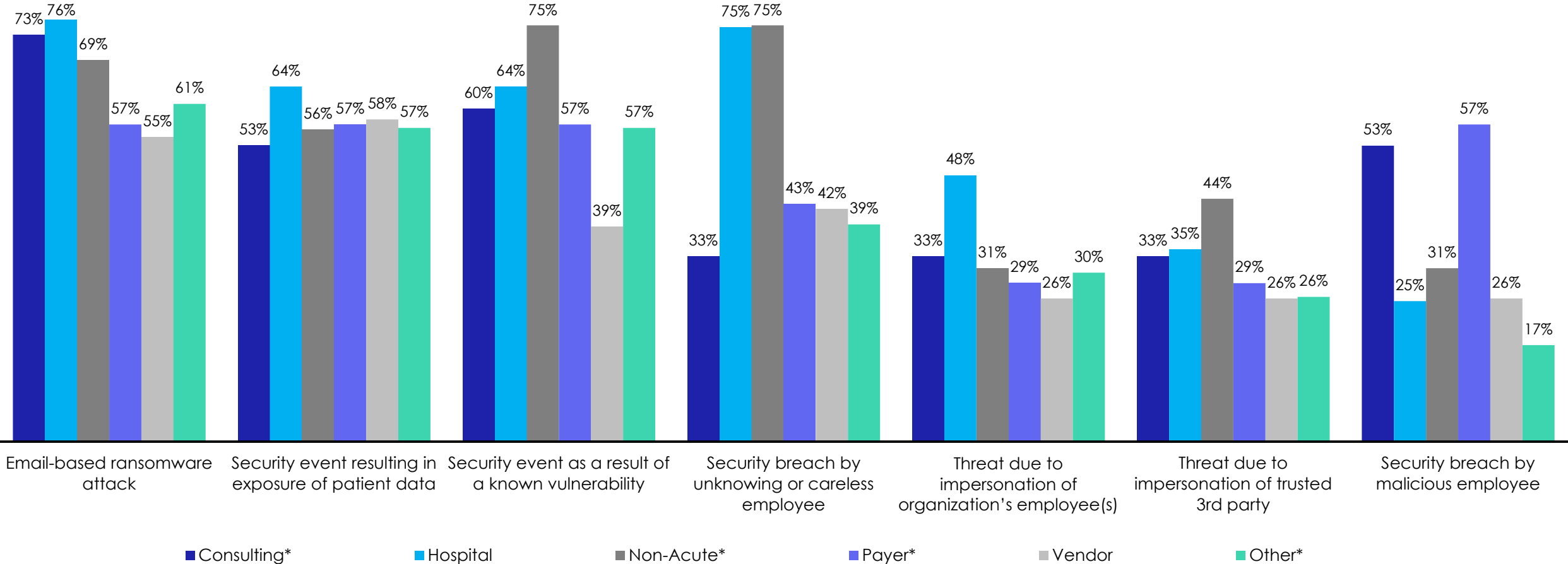


3.5
average
number of
factors

With 3-in-4 hospitals and non-acute care worksites more highly motivated by security breaches by unknowing / careless employees vs other worksites

Which, if any, of the below factors currently drive your implementation of cybersecurity tools / technology?

Implementation Drivers by Worksite



*"Other" Motivators (0%-10%) not shown

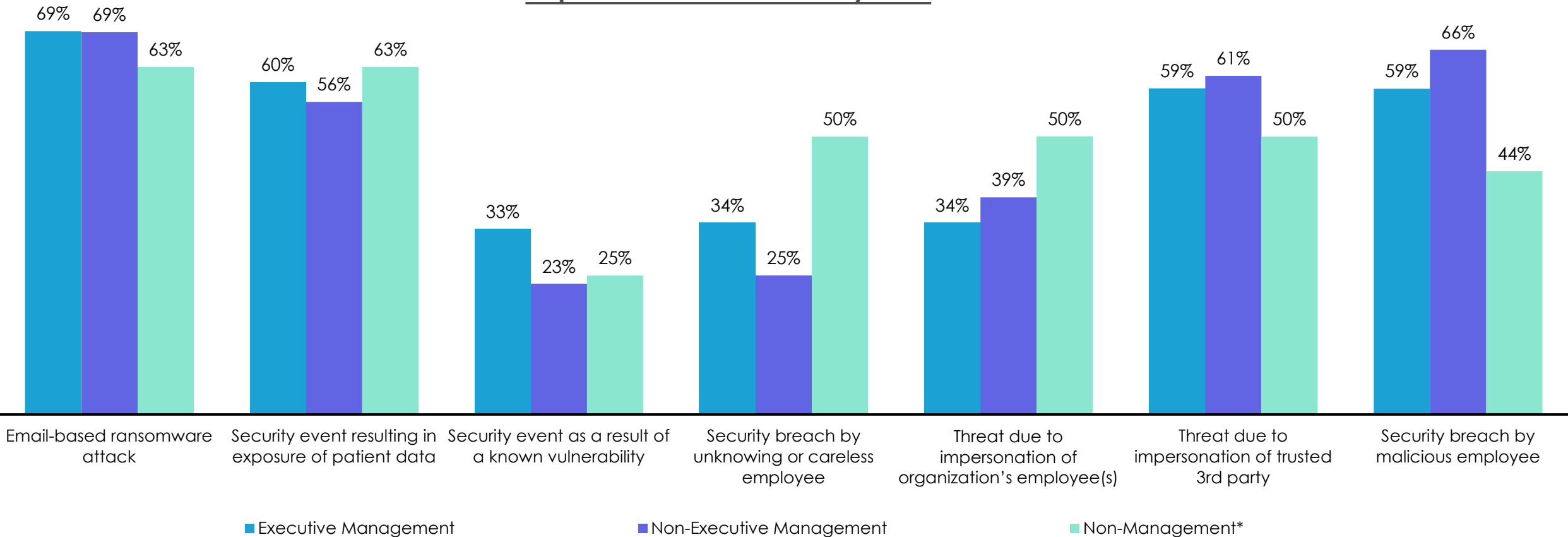
Which, if any, of the below factors currently drive your implementation of cybersecurity tools / technology?
Base: Total Respondents; n=167

*Small base sizes, insight is directional

And, nearly 60% of executives are motivated to implement because of a threat due to impersonation of trusted 3rd party and security break by malicious employee

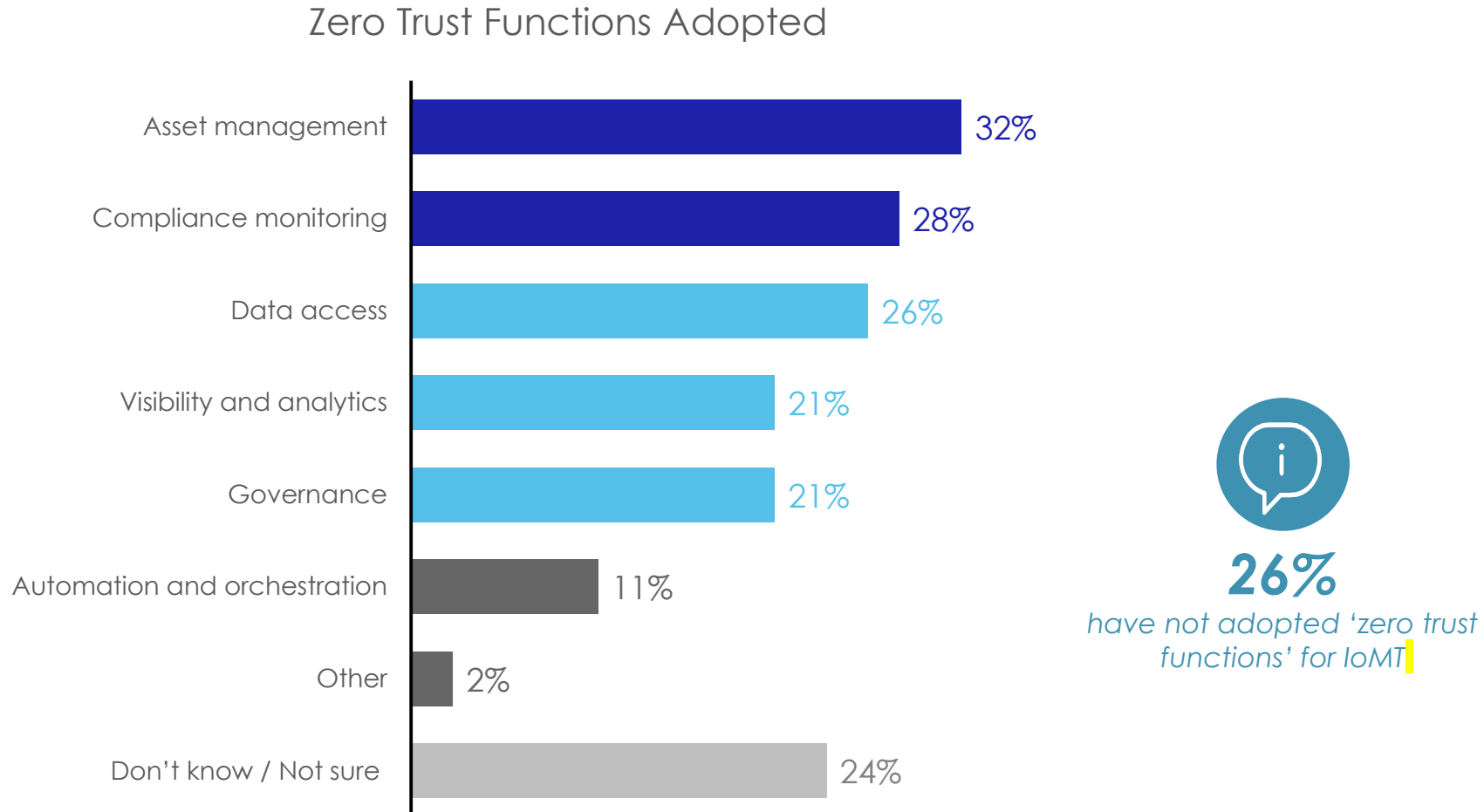
Which, if any, of the below factors currently drive your implementation of cybersecurity tools / technology?

Implementation Drivers by Role



Asset management is the top adopted zero trust function, while more than a quarter state they have not adopted a 'zero trust function'

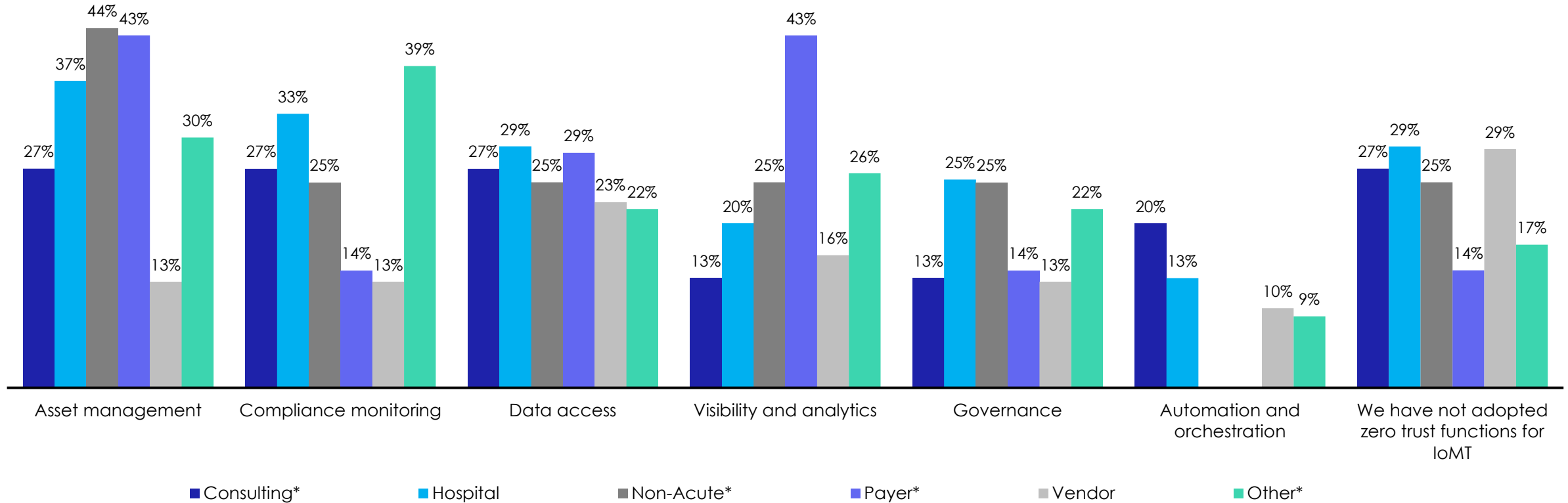
Which zero trust functions have you adopted for the Internet of Medical Things (e.g., connected medical devices)?



Hospital adoptions are across functions, with the highest adoption being Asset Management, and the lowest adoption being Automation and orchestration

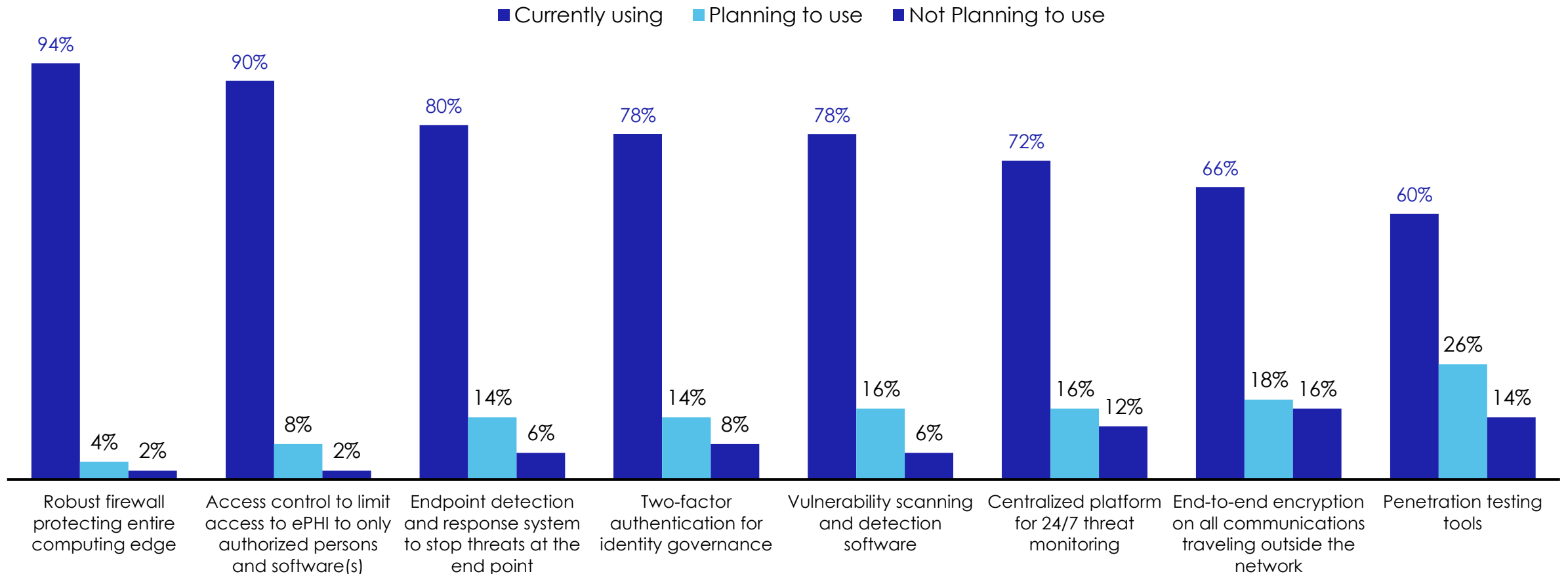
Which zero trust functions have you adopted for the Internet of Medical Things (e.g., connected medical devices)?

Zero Trust Functions by Worksite



9-in-10 currently use a robust firewall protecting entire computing edge and Access control to limit access to ePHI to only authorized persons and software(s)

Please tell us, of the following tools, technology, and education, which your organization is currently using and will be using in 2 years to continue to be secure, effective, and compliant?



Key Takeaways

1

Email-based ransomware attacks is the top driver for cybersecurity implementation

(68%), followed by a security event as a result of a known vulnerability (60%) as a driver for implementation. Those in a hospital (75%) or a non-acute care (75%) worksite, also being more motivated to implement cybersecurity due to security breaches by unknowing / careless employees vs other worksites (33%-43%). With executives also being motivated by a threat due to impersonation of trusted 3rd party (59%) and security break by malicious employee (59%).

2

A quarter of respondents have not adopted any type of zero trust function

Asset management has been adopted most often as a zero trust function for IoMT (32%). Hospitals have also adopted compliance monitoring (33%) and data access (29%).

3

A variety of tools are currently being used to ensure security, effectiveness and compliance

Robust firewall protecting entire computing edge (94%) and access control to limit access to ePHI to only authorized persons and software/s (90%) are the top tools used. Penetration testing tools (26%) and end-to-end encryption on all communications traveling outside the network (18%) are the top tools that have plans to be used within the next two years.



Thank You

For more information on Carahsoft's healthcare IT solutions, please visit our website at carah.io/healthcare.

For inquiries, please contact:

Tim Boltz

Sales Director

Tim.Boltz@Carahsoft.com