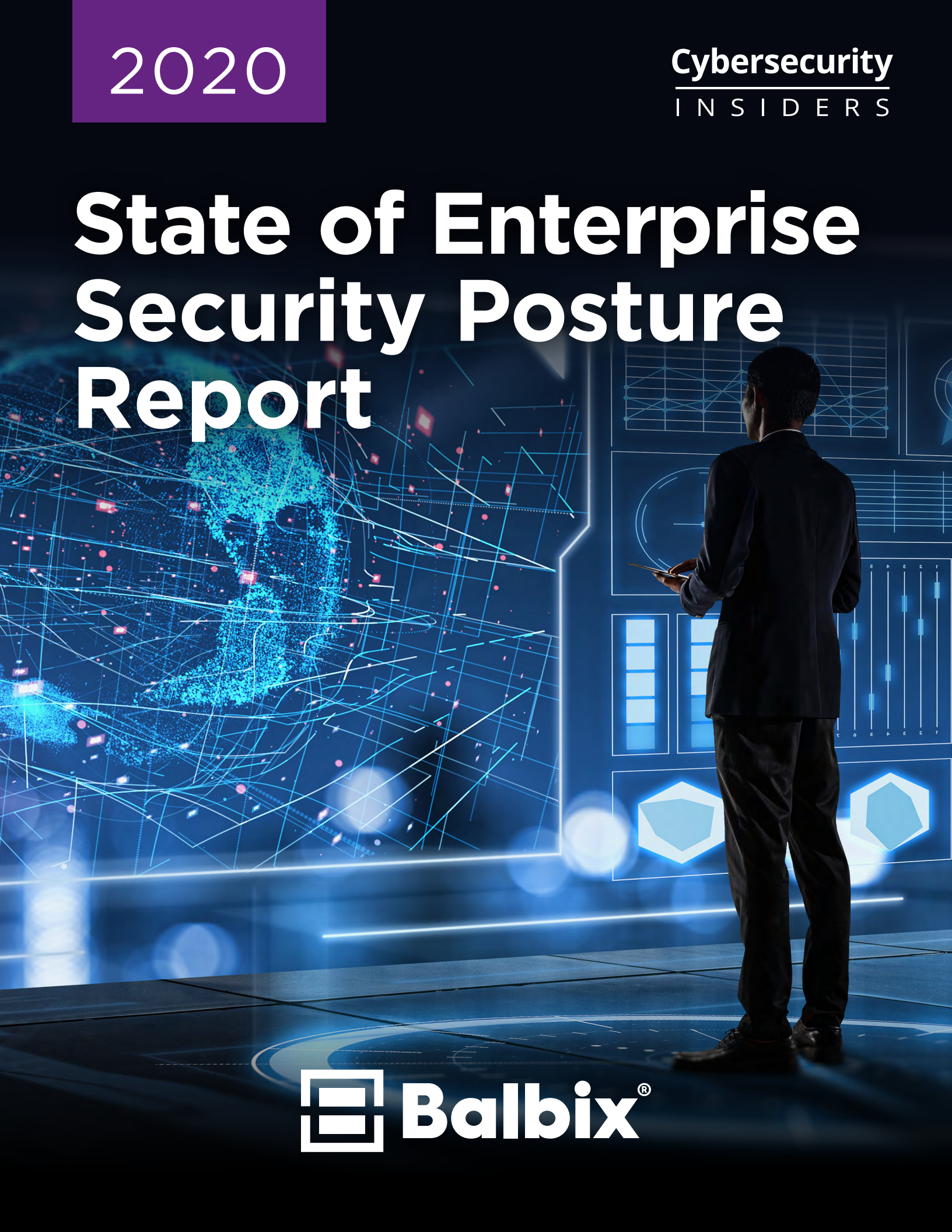
2020

Cybersecurity INSIDERS

State of Enterprise Security Posture Report



Balbix®

OVERVIEW

The 2020 State of Enterprise Security Posture Report reveals that cybersecurity teams are struggling with a lack of visibility into threats, endpoint devices, access privileges, and other key security controls necessary for a robust cybersecurity posture.

The report has been produced by Cybersecurity Insiders, the 400,000 member information security community, to explore the latest trends, key challenges, gaps, and solution preferences for cybersecurity operations.

Key findings include:

- A 64% majority of organizations are lacking confidence in the state of their security posture. This is driven by inadequate visibility.
- 90% of organizations believe that phishing and ransomware are the top threats facing their organization, but only half have sufficient visibility into these challenges.
- 60% of organizations are aware of fewer than 75% of the devices on their network. This lack of asset awareness makes it difficult to improve security posture.
- 80% of organizations provide more access privileges than are necessary for users to do their jobs; 17% even say most or all users have too many privileges.
- Cybersecurity leaders struggle to communicate their security posture to the board and senior management.

We would like to thank Balbix for supporting this important industry research project. We hope you find this report informative and helpful as you continue your efforts in securing your organizations against evolving threats and during challenging times.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

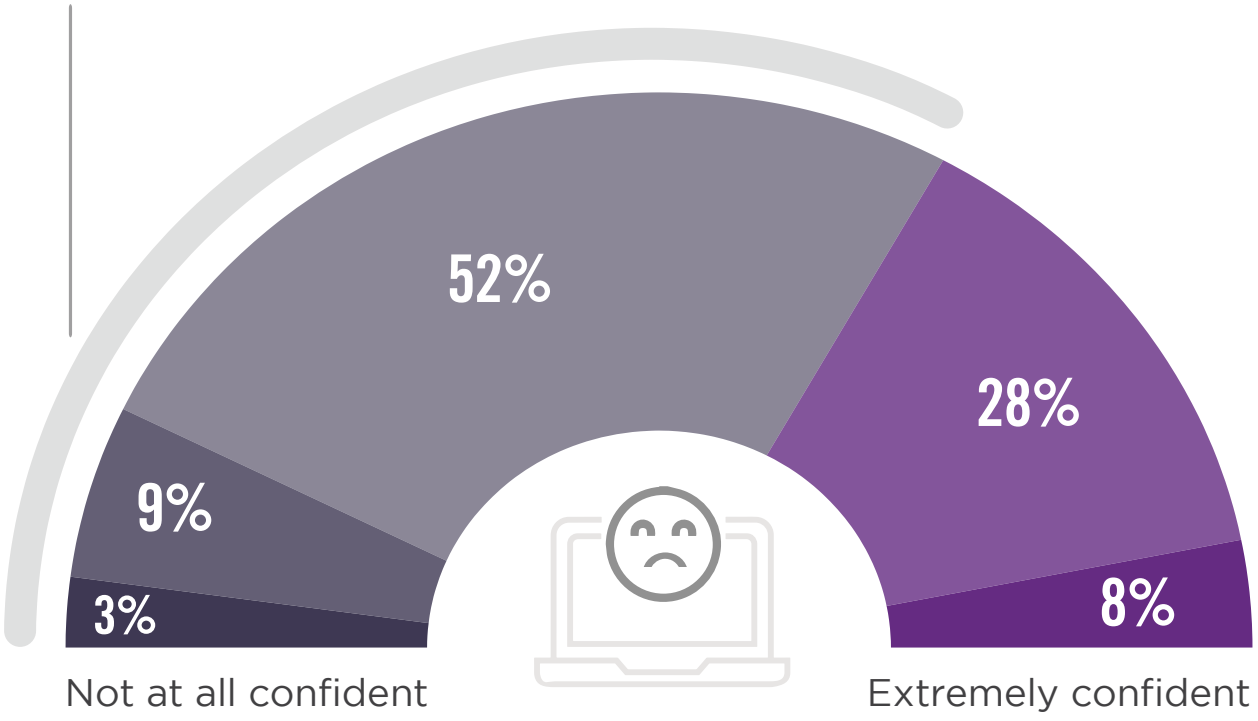
Cybersecurity
INSIDERS

(LACK OF) SECURITY POSTURE CONFIDENCE

We asked organizations about their level of confidence in their overall security posture. 64% say they are, at best, somewhat confident in their security posture.

How confident are you in your organization's overall security posture?

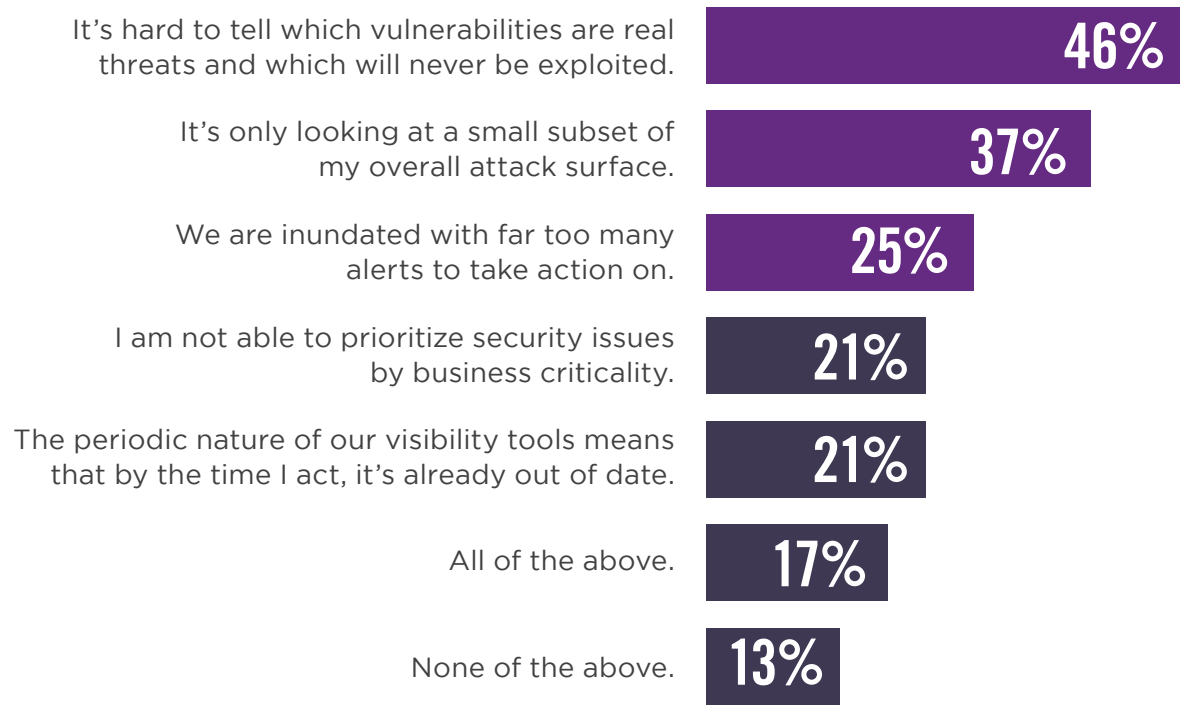
64% of organizations says they are, at best, somewhat confident in their security posture.



FUZZY SECURITY VISIBILITY

Limited visibility and inability to prioritize are inhibiting the effectiveness of vulnerability management programs. 46% of respondents find it hard to tell which vulnerabilities are real threats versus ones that will never be exploited. This is followed by 37% who say their visibility only extends to a small subset of the overall attack surface and 25% who feel they are inundated with far too many alerts to take action.

Which of the following are concerns that you have about your current security visibility?

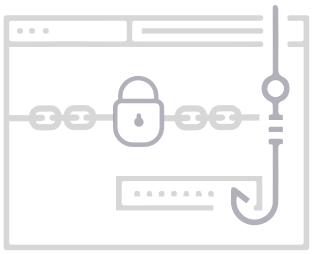


Other 8%

PHISHING DOMINATES THE BIGGEST RISKS

When asked about the biggest security threats facing organizations, 89% are most concerned about phishing, web and ransomware attacks. This is followed by exploitation of vulnerabilities created by unpatched systems (53%) and misconfigurations (47%).

Which of the following areas do you believe are driving the most risk to your organization?



89%

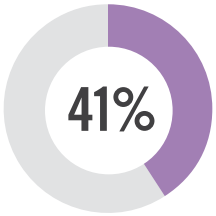
Phishing, web and ransomware

53%

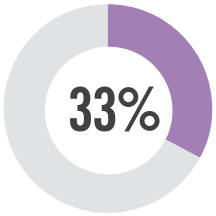
Unpatched systems

47%

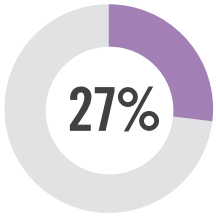
Misconfigurations



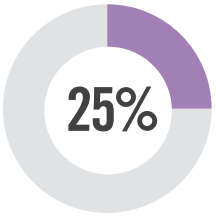
Identity and access management



Password issues



Malicious insiders



Asset inventory

Denial of service attacks 22% | Flat networks 17% | Encryption issues 16% | Other 3%

LITTLE VISIBILITY FOR BIGGEST RISKS

We asked what risk areas organizations have continuous visibility into. 68% list unpatched systems, followed by identity and access management (59%), and phishing, web and ransomware (48%).

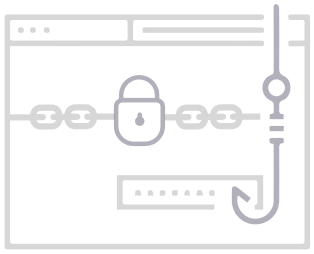
Which of the following risk areas do you have continuous visibility into?

68%

Unpatched systems

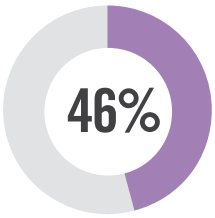
59%

Identity and access management

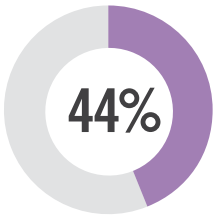


48%

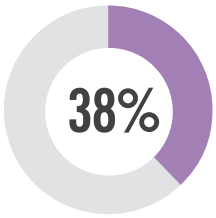
Phishing, web and ransomware



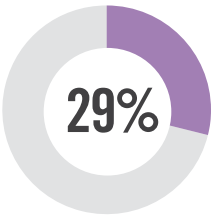
Password issues



Asset inventory



Denial of service attacks



Encryption issues

Misconfigurations 29% | Flat networks 24% | Malicious insiders 24% | Other 3%

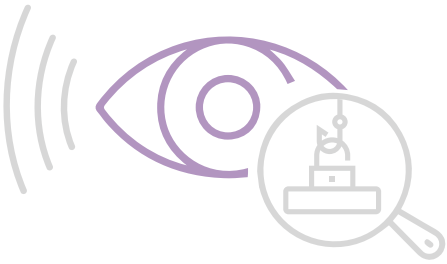
LACK OF VISIBILITY INTO PHISHING RISK

Employees being phished is a large source of risk for organizations of all sizes, as adversaries target users with malicious emails and websites. Although 89% of organizations say phishing is their greatest area of risk, only 48% report having sufficient visibility into it.

89%

Believe that phishing is the highest risk area

BUT ONLY



48%

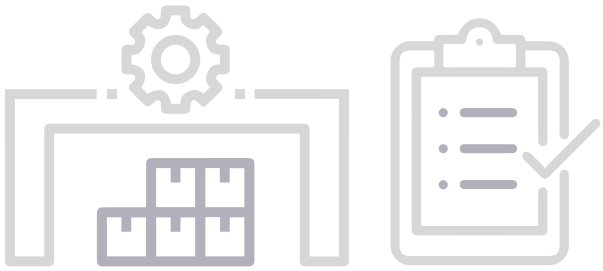
Have adequate visibility into phishing risk

YOU CAN'T IMPROVE WHAT YOU CAN'T MEASURE

60% of organizations are aware of fewer than 75% of the devices on their network. 83% of organizations confirm they have at least 50% asset coverage, knowing roughly how many assets they have, but with only spotty coverage for business criticality and categorization.

This is a significant issue because without an accurate and up-to-date inventory, organizations will struggle to improve security.

Which of the following best describes your organization's handle on asset inventory?



> 75% asset coverage
We know exactly how many assets we have, with business criticality and categorization for all of them.

50-75% asset coverage
We know roughly how many assets we have, but have spotty coverage for business criticality and categorization.

25-50% asset coverage
We have a general idea of the number of assets on our network, but are unable to accurately categorize or determine their business criticality.

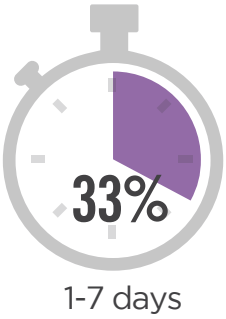
< 25% asset coverage
We do not have any real processes around asset inventory in our organization.

THREAT RESPONSE TIMES VARY

Only 58% say they can determine within 24 hours every vulnerable asset in their organization, following news of critical exploits. More than 40% take 24 hours or longer to identify vulnerable systems, making it nearly impossible to thwart fast moving ransomware or malware outbreaks.

If a new critical exploit hits the news, how long does it take you to determine every asset that is vulnerable?

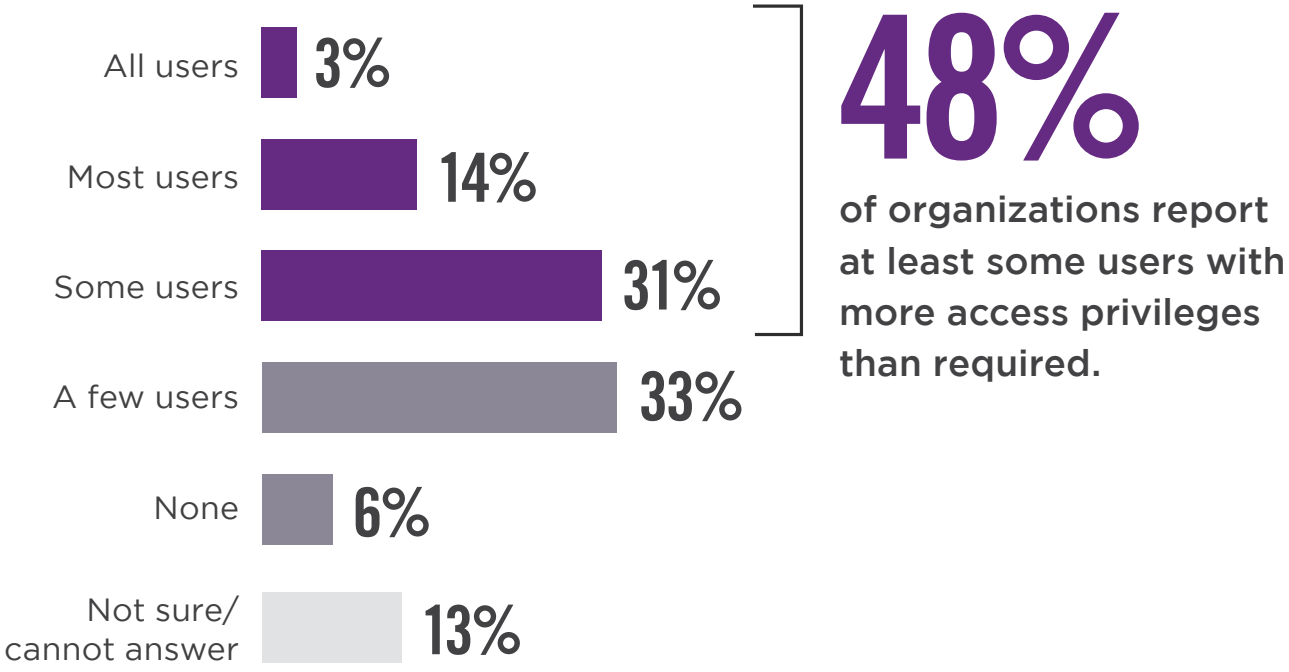
58% say they can determine within 24 hours every vulnerable asset in their organization.



EXCESSIVE ACCESS PRIVILEGES

Nearly 1 in 5 organizations report that most or all users have more access privileges than required for their job. Overall, 81% of organizations provide more access privileges than are necessary for users to do their jobs.

How many users in your organization might have more access privileges than required for their job?



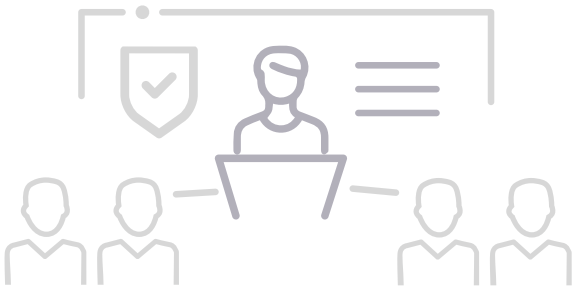
48%

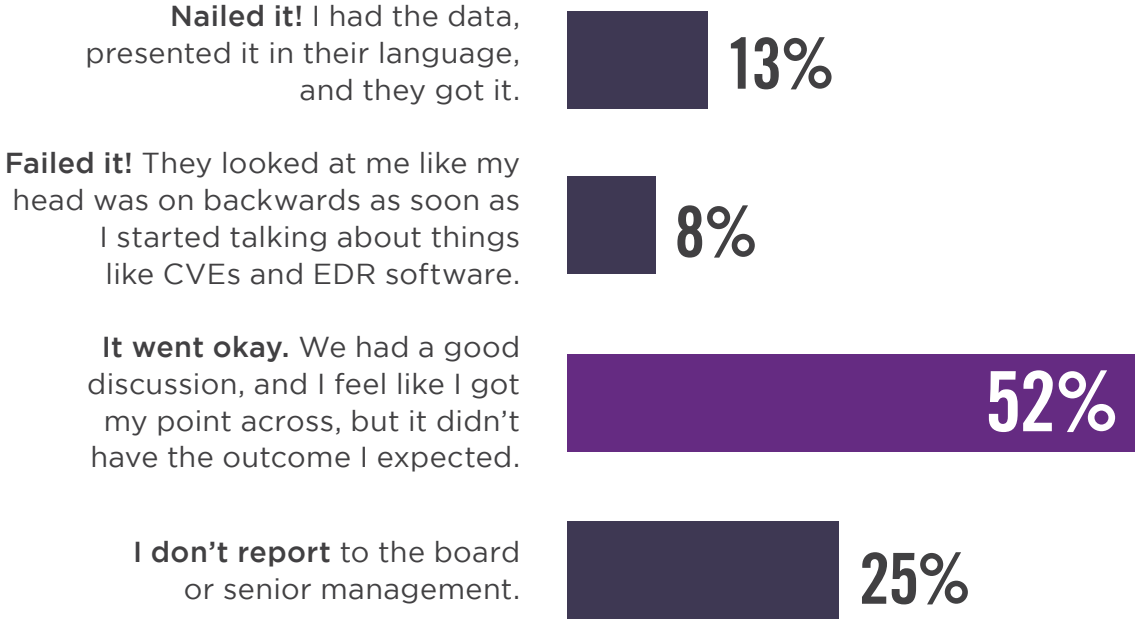
of organizations report at least some users with more access privileges than required.

BOARD PRESENTATIONS ON CYBERSECURITY ARE "OKAY"

Cybersecurity leaders struggle to communicate their security posture to the board and senior management. When asked to characterize their most recent board or senior management presentation on cybersecurity, most frequently (52%) respondents say that they have a good discussion and get their points across but that the outcome was not as expected. Only 13% feel like presentations go very well and the board understands the security situation.

Which of the following most closely characterizes your most recent board or senior management presentation on cybersecurity?



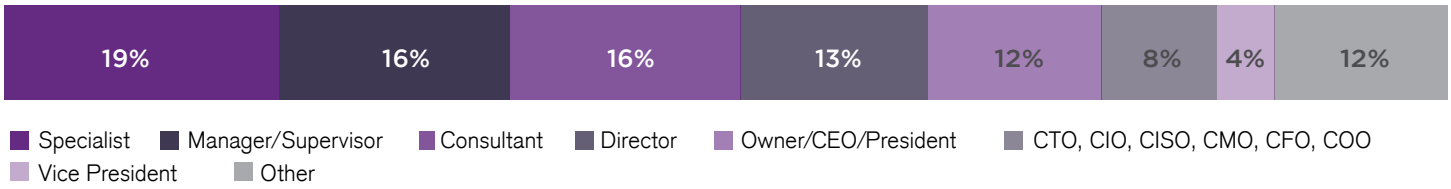


Other 2%

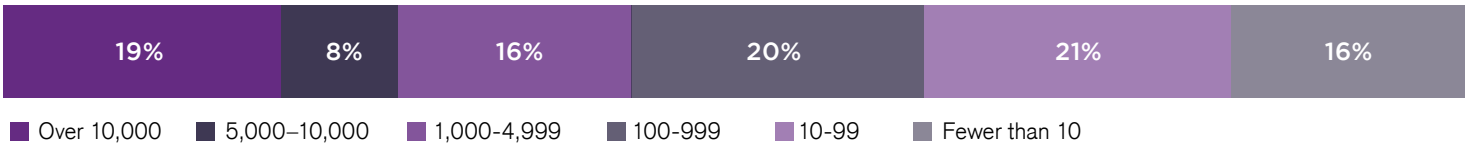
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 372 IT and cybersecurity professionals in the US, conducted in June 2020 to explore the latest trends, key challenges, gaps, and solution preferences for cybersecurity operations. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

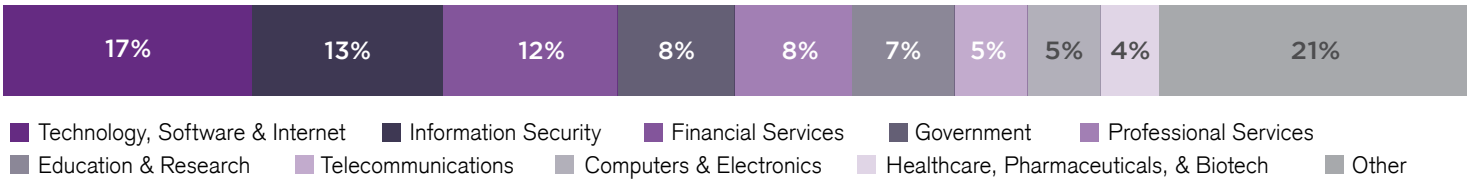
CAREER LEVEL



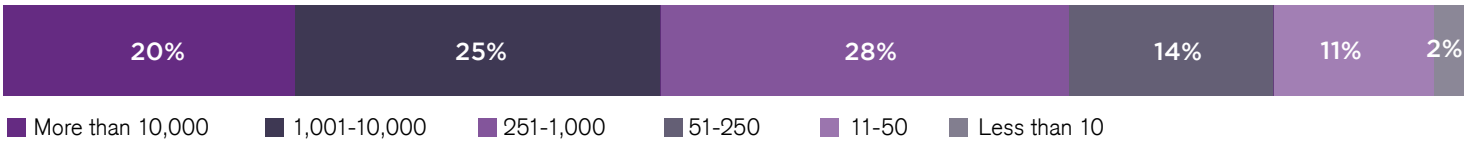
COMPANY SIZE



INDUSTRY



NETWORK-CONNECTED ENDPOINTS



ADDRESSING SECURITY POSTURE CHALLENGES

INADEQUATE VISIBILITY

Only 13% of respondents do not face issues with their security visibility. Infosec teams need visibility into all the devices and applications on their network, as well as the 100s of attack vectors they are susceptible to. This visibility should be continuous, as periodic scans go quickly out of date. Lastly, infosec teams should have visibility into the severity of vulnerabilities to know if they are real threats or just noise.

INVENTORY BLINDSPOTS

The majority of respondents are not accounting for 25% or more of their devices in their inventory. This creates huge blindspots in security posture and serious risks. Enterprises must have a continuous, real-time view of their inventory that includes all devices, apps, and services. This means managed and unmanaged infrastructure, on-prem and cloud, and fixed and mobile. They should also have intel on how devices are being used.

RISK FROM PRIVILEGED USERS

With 80% of organizations providing more access privileges than necessary for their users, it is critical to have visibility into the threats affecting these users. Vulnerabilities on privileged user assets should be treated with urgency and given high priority, since exploitation will result in an accelerated breach. Organizations should also take steps to limit access privileges where possible.

COMMUNICATING TO THE BOARD

52% of cybersecurity leaders are settling for "okay" board presentations when they could be nailing it. Effective board-level presentations start with quantifiable risk metrics and intuitive visualizations. They should focus on business objectives and help stakeholders understand where the company is on cyber risk, where it should be, and how it can get there.

Balbix helps CISOs and security teams assess and report on breach risk, and optimizes security posture transformation by providing visibility across all assets and 100+ attack vectors. Balbix prioritizes security team efforts, reducing breach risk by 95%, improving security team efficiency 10x, and providing risk-based reporting to the board of directors. Numerous Fortune 500 enterprises use Balbix to increase cyber-resilience.

www.balbix.com