Cybersecurity at a Crossroads:

The Insight 2021 Report

In 2020, the cybersecurity landscape was shaped by the challenges of scaling distributed IT environments and transitioning to work-from-home models during the pandemic. How did these hurdles impact corporate security strategies and initiatives? What are the main challenges security leaders face moving forward?

We asked hundreds of IT and security leaders in an Insight-commissioned IDG survey. Here's what we learned:

Cybersecurity awareness and budgets have grown.

As a result of increasingly complex IT environments, security teams have been tasked with addressing new vulnerabilities and evolving risks in their environments.
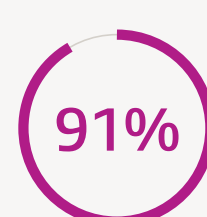
Companies accelerated
5–6 different
cybersecurity initiatives on average.

100% of respondents agree that boards and executive teams are now **more focused on the company's security posture than in the past.**

96% increased their cybersecurity budgets in 2020.

91% plan to do so again in 2021.

And yet, despite increased investments in cybersecurity in 2020, **three in four respondents (78%) expressed a lack of confidence** in their company's IT security posture and saw room for improvement.

Security leaders suffer from a lack of resources.

Companies shifted cybersecurity modernization priorities in response to challenges presented by the pandemic, focusing on closing security gaps caused by a rapid move to work-from-home environments.

Although most companies completed a number of short-range, block-and-tackle initiatives, security confidence remains low — likely due to teams lacking the resources for executing a wider range of foundational and long-term security efforts.
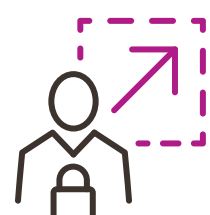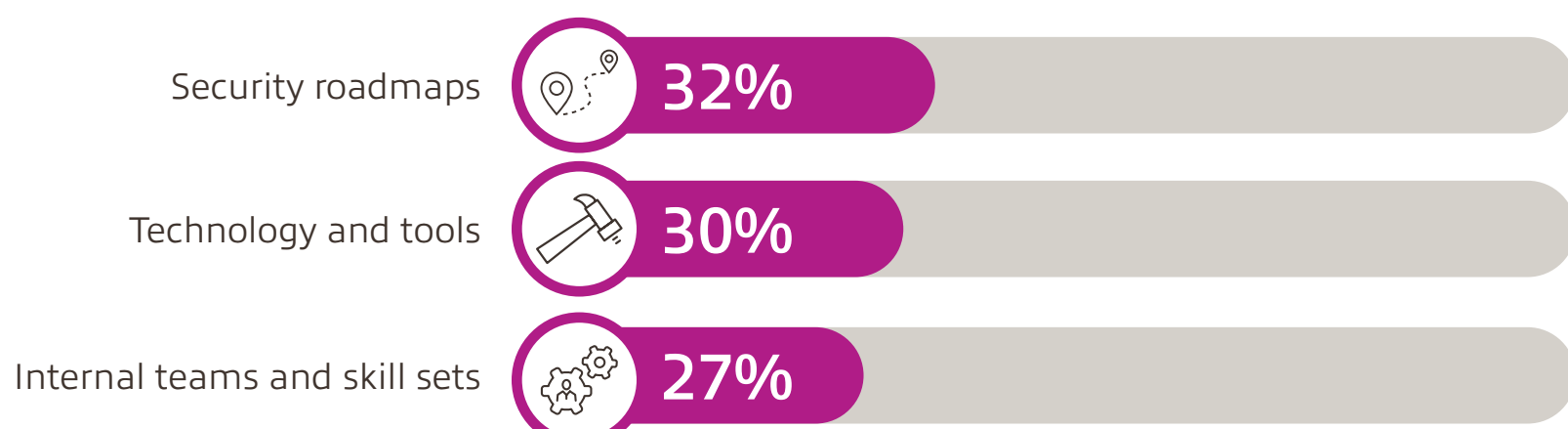
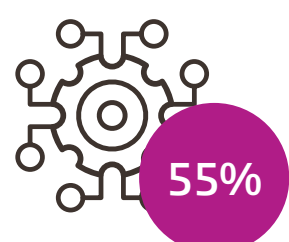**Only 27%** of respondents expanded security staff in 2020.
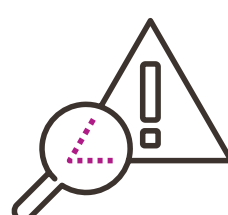
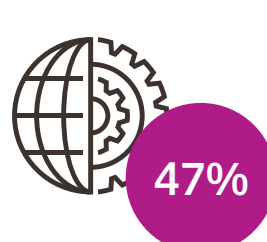**Only 57%** of businesses conducted a data security risk assessment.

Security leaders have the least confidence in their organizations':

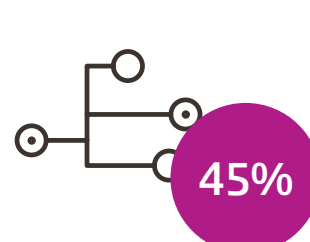|	
Security roadmaps	**32%**
Technology and tools	**30%**
Internal teams and skill sets	**27%**

The key challenges security teams face in strengthening security postures:
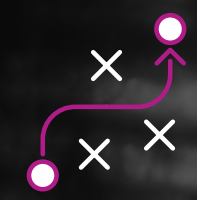
55% Lack of automation

47% Outdated network access control solutions
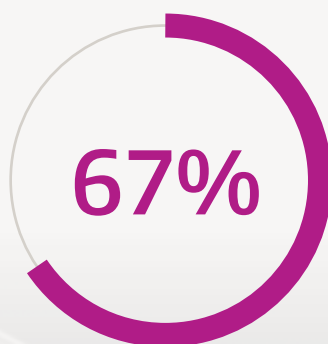
45% Legacy infrastructure and tools

43% Lack of skilled cybersecurity staff

Organizations need skilled resources and strategic support.

Looking to the future, organizations plan to spend some of their increased cybersecurity budgets on expanding security teams, modernizing operations, and engaging with outside specialists for strategic support.

67% are seeking assistance in developing an overall IT security strategy.
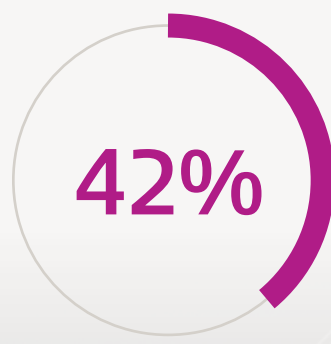
42% plan to modernize security operations.

41% plan to begin or resume staff expansion.

Security is a team effort.

Organizations made enormous strides to address gaps and reduce cybersecurity risks against new challenges in 2020. But bolstering security postures is a complex and continual effort requiring varied and specialized resources. From strategic planning to day-to-day managed security, we're here to help you minimize risk, maximize your resources, and make every challenge a step toward stronger defenses.

Get the partnership you need for a stronger security posture.

CONTACT US

To learn more about our 2021 cybersecurity report, view the full survey results here:
insightCDCT.com/cybersecurity2021