Insight

Cybersecurity at a Crossroads:

The Insight 2021 Report

IDG

Table of contents

IT complexity and COVID-19 intensify cybersecurity challenges

Cybersecurity is in the spotlight now more than ever. Staying ahead of an evolving threatscape is a never-ending challenge requiring a proactive approach. But when unexpected circumstances endanger business operations, shifting to a reactive strategy can become necessary.

Entering 2020, organisations were in the midst of addressing growing security challenges associated with distributed IT environments spanning cloud, edge, and on-premises infrastructures. Data is everywhere, moving between and stored in multiple locations, making it more complex to assess and address. Legacy security and data protection and recovery technologies may not support new cloud environments. Compliance regulations make platform choices more complicated. And governance and processes for evolving IT environments need to be modernised. On top of these challenges, skilled security personnel have been in short supply, and cybersecurity attacks have been on the rise.

These challenges intensified with the new demands and security risks introduced by the sudden expansion of remote work brought on by the pandemic. Priorities had to shift in 2020 as employers enabled new work-from-home environments and plugged the gaps left from rapid implementation.

To help us understand how IT leaders are adapting strategies, priorities, and initiatives to address the rapid evolution of the cybersecurity landscape, we commissioned IDG to survey more than 200 executives (CIOs, CTOs, CSOs, IT directors) working at organisations with an average of 21,300 employees in December 2020.

This survey was designed to measure confidence levels in current enterprise security postures and identify roadblocks to improved cybersecurity, as well as identify emerging security modernisation priorities and gaps to be addressed moving forward. These findings are clearly framed within the defining challenges of 2020: scaling distributed IT environments and transitioning to work-from-home models during the pandemic.

One of our most significant findings is that

nearly 80% of IT leaders surveyed

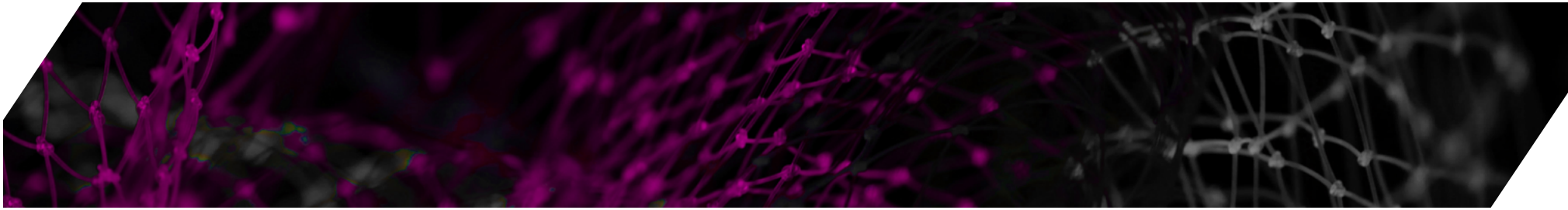
expressed a lack of confidence in their company's IT security posture and saw room for improvement[1] — **despite a significant increase in IT security investments (96% boosted IT security spending in 2020)**.[2]

As a result,

91% of organisations

plan to increase their cybersecurity budgets again in 2021.[2]

Continue reading to learn key factors behind these trends and how we expect to see cybersecurity initiatives change moving forward.



[1] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 10. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.
[2] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 29. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.

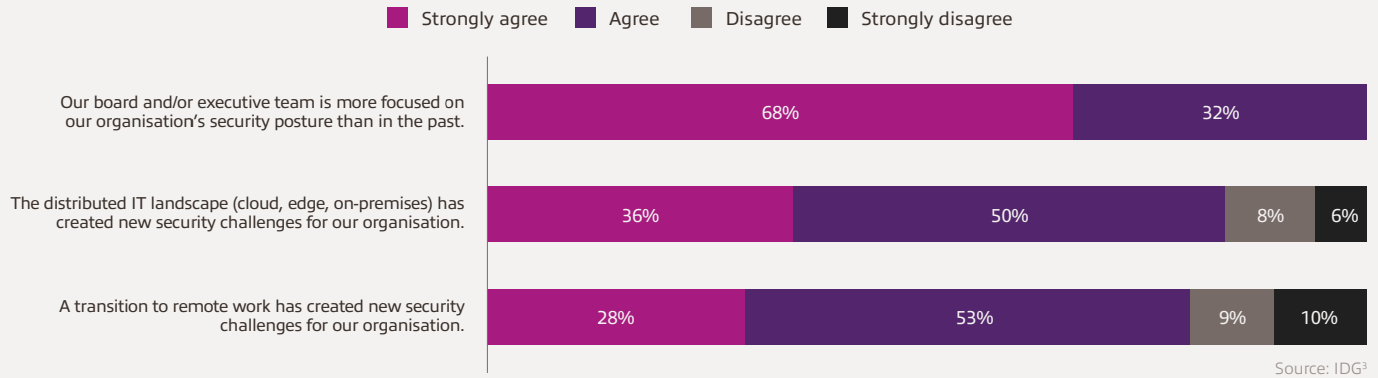
PART 1

IT leaders react as 2020 raises security stakes and budgets

Against the background of preexisting challenges like scaling distributed IT environments and securing organisations against a new surge of sophisticated cyberattacks (e.g., ransomware, phishing, etc.), when the pandemic hit, organisations were left scrambling to meet the new challenge of enabling remote work environments, which introduced a host of new security concerns across networks, endpoints, the cloud, and the edge. As a result, we've seen a clear increase in awareness of enterprise security postures and cybersecurity risks leading to increased spending in both 2020 and 2021.

Of the organisations surveyed, each indicated an increased focus on enterprise security posture at the executive level. This overwhelming response is tied to the clear spike in challenges led by the distributed IT landscape and transition to remote work.

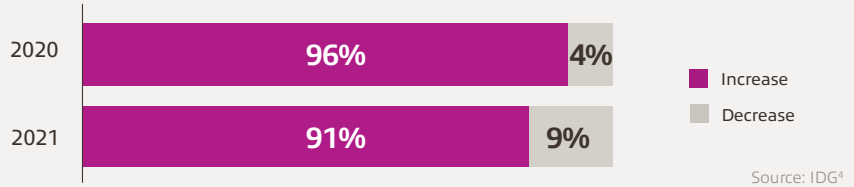
Q: Please rate your agreement with the following statements:



Source: IDG[3]

As a result of the increased pressure on IT leaders to fortify security against these evolving threats, 96% increased their cybersecurity budgets in 2020, and 91% plan to do so again in 2021.

Q: How will your cybersecurity budget change in 2021 compared to 2020?



Source: IDG[4]

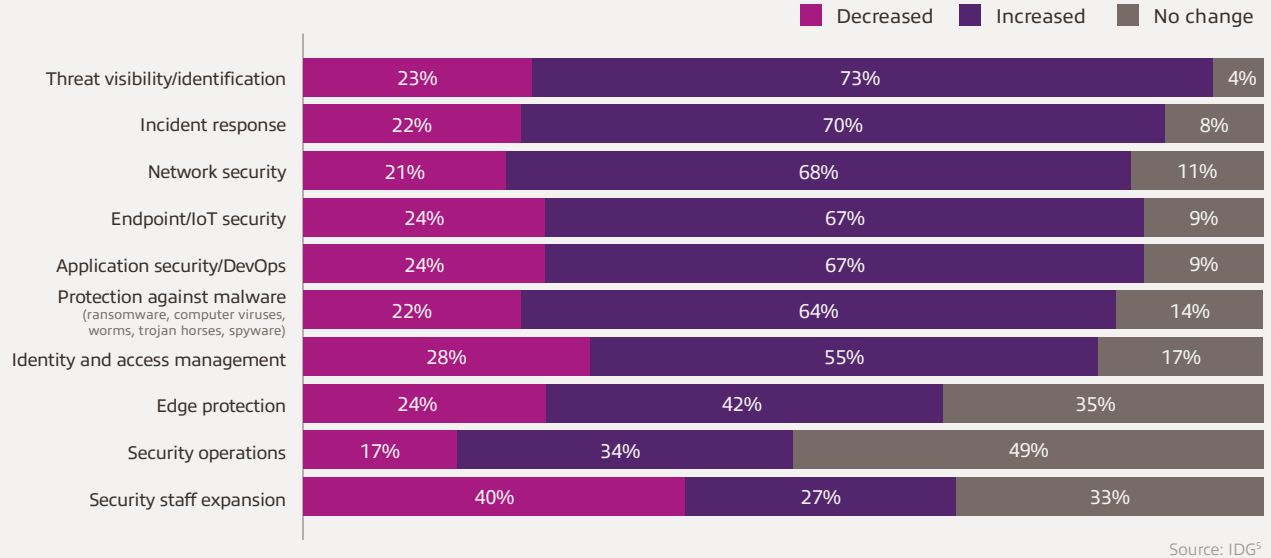
[3] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 9. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.
[4] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 29. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.

PART 2

Despite increased efforts, security confidence is low

The number of new or accelerated security initiatives undertaken in 2020 reflects the complexity of the challenges organisations faced in filling security gaps. In 2020, more than two out of three organisations accelerated between 5–6 different cybersecurity initiatives across several defense levels (endpoint security, threat visibility, incident response, identity management, edge protection), while priorities like security operations and staff expansion were lowered. However, despite increased efforts, survey results show security leaders are not feeling more confident about their security stance.

Q: How did the sudden expansion of work-from-home/distributed IT environment that accompanied the pandemic in 2020 impact your cybersecurity modernisation priorities?



Source: IDG[5]

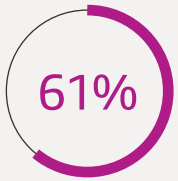
[5] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 14. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.

In addition, organisations are indicating a stronger understanding of cybersecurity's growing threat to company operations. Collaborative integration of security efforts into business continuity, infrastructure, and business operations decisions has long been a pain point for many organisations, with security strategies typically relegated to dedicated security teams and personnel. As the IT environment has grown more complex and dispersed, cross-functional security integration has proven a necessary endeavor, but one that many organisations have found difficult to achieve.

Likely out of necessity arising from the year's challenges, 2020 saw IT leaders increase their efforts to weave security considerations into operations, infrastructure, DevOps, and business continuity plans to help mitigate risk and improve security postures. This is a very strong move in the right direction, and one that will likely continue to gain momentum.

Organisations worked more than ever to integrate cybersecurity across the entire organisation.

integrated incident response into companywide business continuity plan.[6]



integrated cybersecurity into infrastructure (data protection, storage, etc.) and DevOps decisions.[7]

integrated cybersecurity into broader business operations decisions.[7]

But although security efforts increased, organisations' overall confidence in their security posture remains remarkably low. The vast majority (78%) expressed a lack of confidence in their company's current IT security posture and saw room for improvement. Only 22% felt very confident.[8]

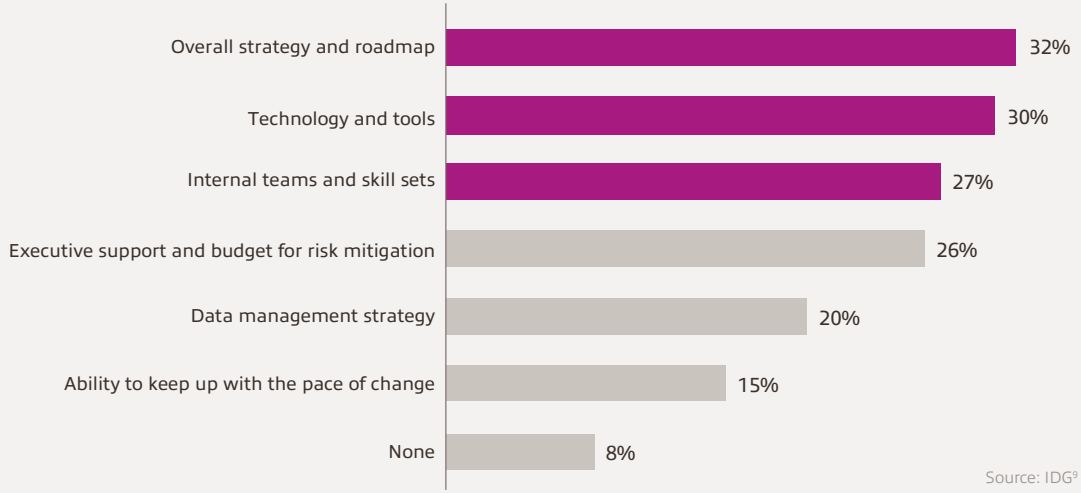
Three in four respondents (78%) expressed a lack of confidence in their company's IT security posture and saw room for improvement.

Source: IDG[8]

[6] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 18. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.
[7] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 25. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.
[8] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 10. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.

Respondents were asked to identify which areas of their security posture they felt least confident in, with the option to select up to two choices. The results showed that the aspect of security respondents felt the least confident about was their overall strategy and roadmap, followed closely by technology and tools, then internal teams and skill sets.

Q: What aspects of your security posture do you feel the least confident about?



Source: IDG[9]

Compounding this absence of reliable technologies and tools is the finding that 27% lacked confidence in their internal teams and skill sets. Security is a specialised field, and finding skilled personnel to fill needs within the security team can be a difficult challenge. Organisations that struggle to acquire the resources they need can adapt by providing or acquiring cybersecurity training for existing staff and/or leveraging professional service providers to fill the gaps in the meantime.

[9] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 11. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.

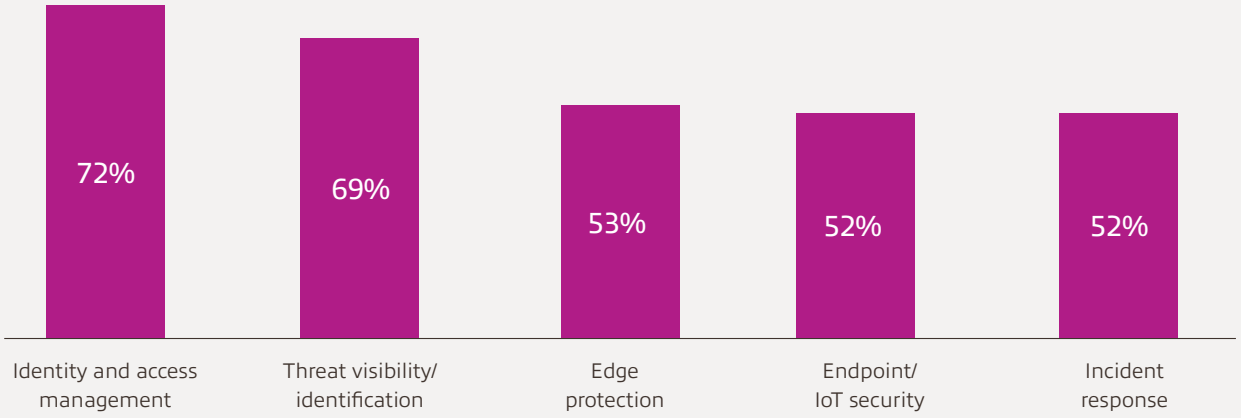
PART 3

Many critical security projects take a back seat

Rapid cloud adoption and distributed IT environments brought new considerations and challenges to organisations' cybersecurity efforts. Whereas before, IT leaders may have felt more confident with on-premises security strategies and clearly defined perimeters, the extended perimeters of distributed IT environments and work-from-home scenarios introduced several new layers of complexity.

Adding the necessity to deploy new remote work scenarios quickly and effectively invited a host of unfamiliar risks that had to be mitigated on a dime. As a result, 2020 security modernisation priorities shifted, with a major focus on identity and access management to address the new remote work security challenges.

Q: Whether or not your priorities changed, what areas of cybersecurity did your organisation work to modernise in 2020?



Source: IDG[10]

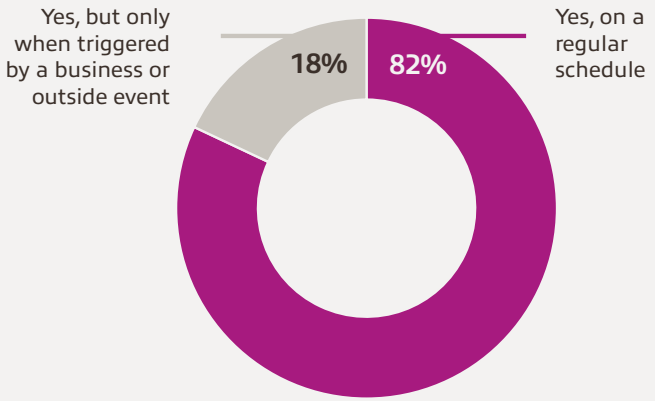
Most organisations focused efforts on closing immediate gaps using basic technologies that were easy to deploy and largely cloud-based, such as Cloud Access Security Broker (CASB), cloud-based Security Information and Event Management (SIEM), and Security Orchestration Automation and Response (SOAR). Many complex, long-range security projects took a back seat to more urgent block-and-tackle activities such as anti-malware and anti-virus upgrades, Multi-Factor Authentication (MFA), and Firewall as a Services (FWaaS) deployments. As a result, relatively few organisations initiated or executed projects in critical areas such as identity governance, Zero Trust, data analytics, and Secure Access Service Edge (SASE) implementations.

[10] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 15. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.

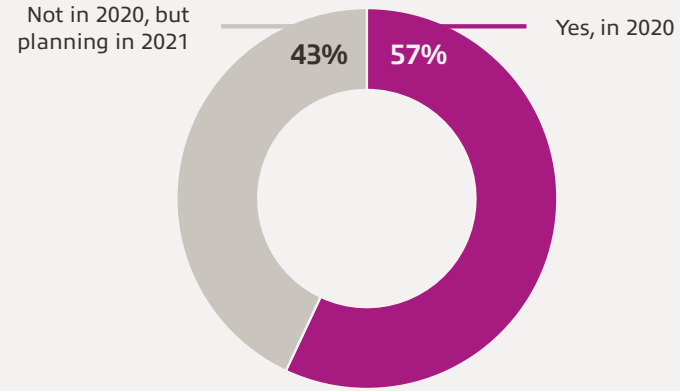
PART 3: MANY CRITICAL SECURITY PROJECTS TAKE A BACK SEAT

To the same end, it wasn't only long-range projects that took a back seat — foundational activities like data security risk assessments fell behind as well. Risk assessments are a critical component of an organisation's security strategy, and most conduct a risk assessment on a regular basis. However, in 2020, only 57% of businesses conducted a data security risk assessment despite the new threats that arose, suggesting the time and resources that would have otherwise been used for annual risk assessments were engaged in managing the new challenges 2020 introduced.

Q: Does your organisation conduct data security risk assessments?



Q: Did your organisation conduct a data security risk assessment in 2020, or are you planning to do so in 2021?



Source: IDG[11]

[11] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 22. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.

PART 4

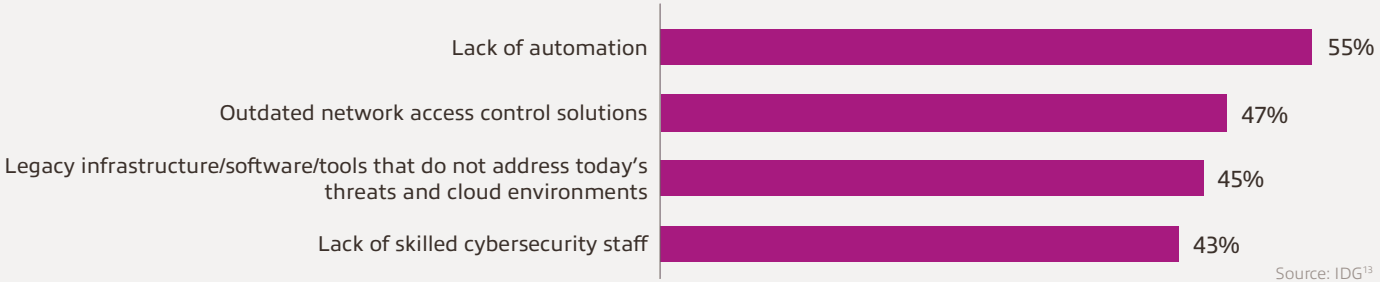
Comprehensive cybersecurity requires robust resources

The fact of the matter is that many organisations simply lack the resources necessary to develop, implement, test, and optimise the comprehensive, integrative, long-term approach to cybersecurity that's required of today's increasing threatscape.

Despite the increase in security budgets and the large number of security projects undertaken in 2020, only 27% of respondents reported expanding security staff in 2020. In fact, 40% decreased their focus on security staff expansion.[12] This left IT teams overburdened, understaffed, and without many of the specialists needed to execute the wide range of security efforts necessitated by the year's evolving threats.

And the challenges facing security operations and management corroborate this notion of the overburdened, understaffed team as lack of automation, modern resources, and skilled personnel top the list.

Q: What are your organisation's major security operations and management challenges?



Source: IDG[13]

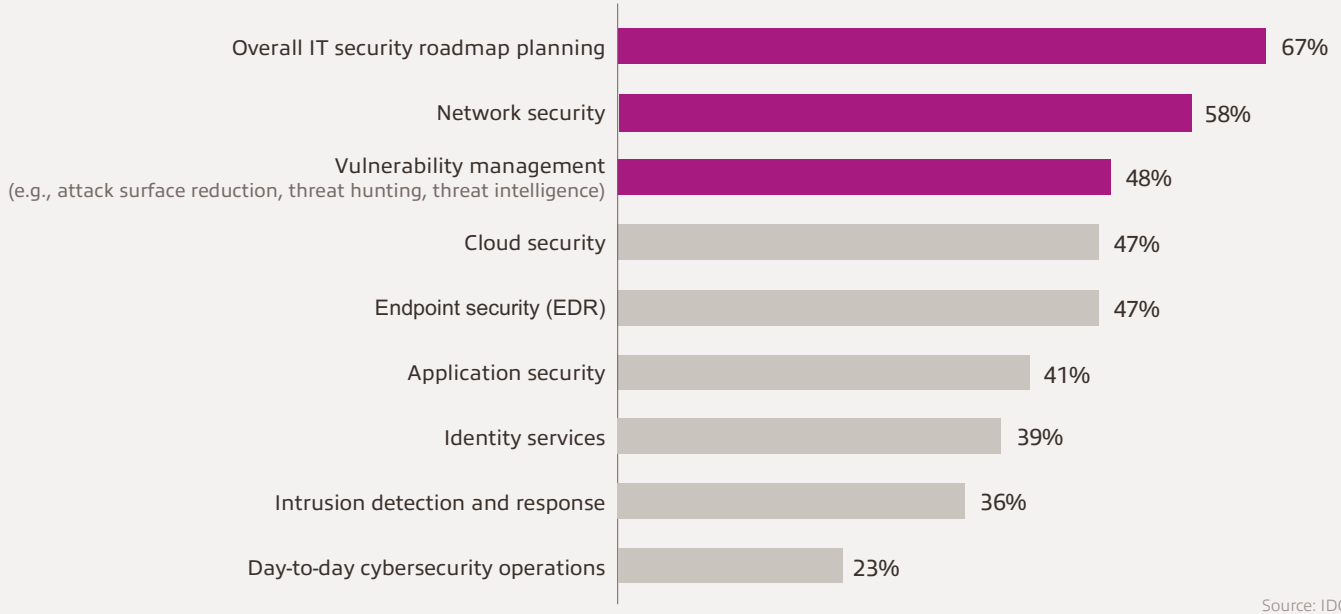
Organisation's struggle with lack of automation reflects the increasing need to simplify management of the flood of notifications and events generated by today's increasingly complex security infrastructure. This problem is exacerbated by factors including the disparate toolsets involved, outdated technology lacking the APIs to support automation, and the time and advanced skill sets required to implement such automated processes.

[12] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 14. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.
[13] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 24. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.

Between the constantly evolving IT landscape, the complexity of distributed IT environments, the growing threatscape, and the difficulty organisations have in attracting and maintaining skilled personnel, it's clear that comprehensive security is a team effort requiring growing amounts of resources.

Recognising the gaps in their resource bases, organisations will not only be increasing cybersecurity budgets in 2021, but also looking to outside experts for support in a variety of areas. While the majority of respondents plan to engage third-party support for functions including security roadmap planning, network security, and vulnerability management, many plan to engage outside support for a host of other tasks, as well, from cloud security to day-to-day operations.

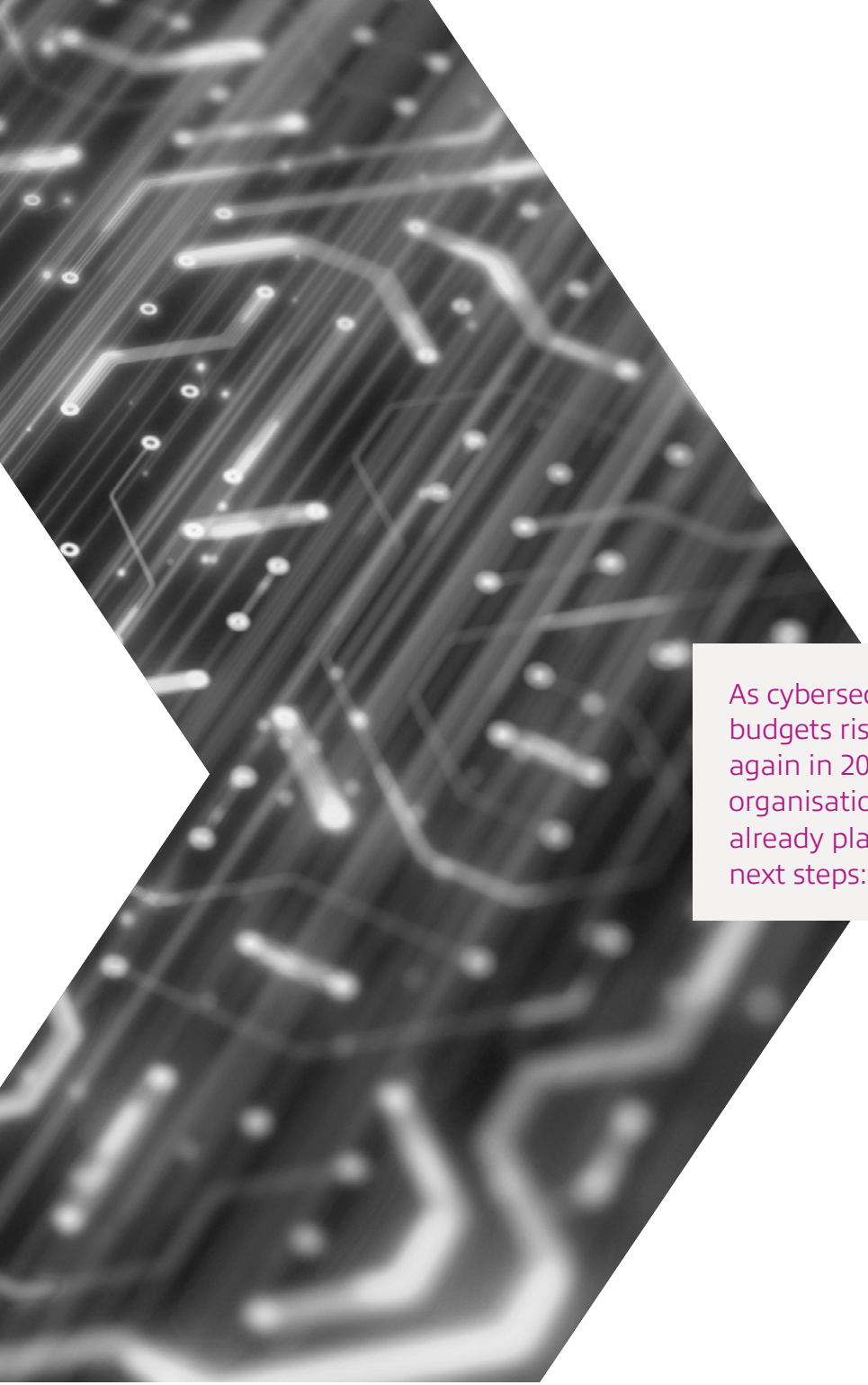
Q: For what cybersecurity functions are you currently engaging or planning to engage a third-party service provider?



Source: IDG[14]

The variety of cybersecurity functions in which organisations plan to seek support illustrates the ongoing need for skilled security specialists.

[14] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 30. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.

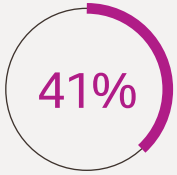


PART 5

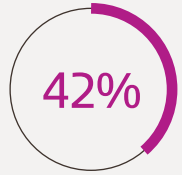
Cybersecurity modernisation is a top priority moving forward

The survey shows that organisations made strides to address gaps and integrate cybersecurity into business, operational, and IT infrastructure decisions. But the work never ends. Bolstering security postures is a complex and continual effort. Implementing and maintaining effective enterprisewide security will require increased time, resources, and skilled support as the threatscape continues to evolve.

As cybersecurity budgets rise again in 2021, organisations are already planning next steps:



plan to begin or resume staff expansion in 2021.



plan to begin modernising security operations in 2021.

Source: IDG[15]

Based on the challenges and roadblocks highlighted in the 2020 survey, it's clear that cybersecurity efforts moving forward will need to shift focus to stronger strategic planning, modernisation of IT, optimisation of security operations, and investments in skilled cybersecurity staff to support comprehensive and long-range security efforts businesswide.

[15] Cybersecurity at a Crossroads: The Insight 2021 Report. Slide 15. (February 2021). Marketpulse Research by IDG Research Services, commissioned by Insight.

Insight

When you're ready to strengthen your security posture, Insight can help.

At Insight, we have helped organisations secure their data and networks for more than 30 years. We assist IT leaders in every aspect of cybersecurity, helping to assess risk, fortify security postures, manage day-to-day security operations, and plan future efforts to ensure their organisations are prepared for future challenges. Mitigating risk and protecting your organisation against an increasingly complex threatscape requires a holistic, multifaceted approach to secure every layer of your IT environment. Insight has the expertise to guide your strategy and roadmap development and the skilled technical resources for identifying and implementing the tools and technologies you need to support a holistic security program.

IDG