

Kaseya®

2026 REPORT

Cybersecurity report: Building security that survives human error



Table of contents

Foreword	3
Five critical findings from the survey	4
Human error remains the biggest security risk	5
Being audit-ready doesn't make compliance easy	9
Cybersecurity investment isn't keeping up with risk	12
Security teams are bogged down by friction	14
As security skills grow scarce, AI helps fill the gap	19
Your cyber resilience playbook: Engineering around human error	22
Who we surveyed	25
Survey methodology	25

Foreword

At Kaseya, we speak with security leaders every day about the challenges they're facing. They're all carrying the same weight: managing more threats with tighter budgets and teams that are stretched to the limits.

We hear about how they're being asked to make high-stakes security decisions every day, from where to invest to which alerts to prioritize and when to act. What's more, they're often forced to make these decisions with incomplete information and no room for error.

And yet, most security strategies still depend on everything going right.

When we set out to conduct this research, we wanted to understand what's really getting in the way of cybersecurity and true resilience. Our survey of over 1,100 MSPs and IT professionals uncovered an uncomfortable truth: many organizations' security programs are not built for the realities they face.

Many security strategies still depend on employees recognizing when an email is malicious, knowing where your limited security budgets will have the greatest impact and having the right expertise on your team when an incident hits. These are all variables that can't be perfectly controlled or guaranteed. People make mistakes, budgets get cut, skilled talent is harder to find than ever and cybercriminals get more sophisticated every day.



The answer isn't to eliminate human error. It's to build security strategies that engineer for the eventuality of it. The organizations that set the pace in IT are building systems, processes and layers of protection that are designed to withstand imperfection. That means automating routine work, so your best people are working on solving complex challenges. It means testing your defenses before an attacker does and building recovery capabilities that expect a breach to happen. Most importantly, it means measuring your actual readiness, not just your confidence in it.

We hope the findings and the playbook that follows will help you make a fundamental shift in your security strategy.

Five critical findings from the survey

1 Human error remains the biggest security risk

About 68% of respondents identify human error as the threat vector they are most concerned about. They also point to people-related issues, including poor user practices, lack of cybersecurity training, and weak passwords, as leading contributors to cybersecurity incidents.

2 Being audit-ready doesn't make compliance easy

About 65% of respondents say they could pass an audit today without preparation, but being audit-ready today does not mean staying audit-ready over time. Changing regulations, limited resources and the ongoing work of keeping controls and evidence current can make compliance harder to sustain.

3 Cybersecurity investment is not keeping up with risk

About 77% of IT department respondents say their cybersecurity investment is falling behind risk. Nearly 65% of MSPs say the same about their clients, and that much of the investment happens after only incidents or compliance demands force it.

4 Security teams are bogged down by friction

Security teams are being pulled away from higher-value work by day-to-day friction. For 38% of respondents, end-user requests are the most common interruption, while controls such as MFA, privileged access management, and email security add further operational demands. The pressure also causes tough trade-offs, from sacrificing IT budget to maintain security to compromising user experience or technician capacity.

5 As security skills grow scarce, AI helps fill the gap

Security automation and AI specialists are the hardest skills to find or retain, cited by 32% of respondents. Yet AI is already helping fill some of the gap, with 44% using it for threat detection and monitoring and 29% for alert reduction and triage.

The threat landscape

What's hitting organizations right now

Phishing tops the threat list for both MSPs and IT departments — and it leads directly into our first finding. It works not by breaking systems, but by getting past people. That's what makes it so hard to defend against.

Top threats faced in the last three years

- Phishing
- Business email compromise
- Malware
- Ransomware
- Identity & credential compromise
- AI-enabled attacks

Finding One

Human error remains the biggest security risk

Human error, including social engineering and distraction, is the top threat vector respondents are concerned about. About 68% say it could be a gateway to a successful attack in the next 12 months, followed by email at 55%. The connection between the top two vectors is direct: email delivers the threat, but the person receiving it determines whether it succeeds.



*Percentages may not add up to 100% because respondents could select more than one answer. In some cases, response options that accounted for a negligible share of responses, such as "Other," have been omitted from the data and are not shown.

The human factor is already behind many attacks

Among organizations that experienced an incident in the past three years, four of the top five contributing factors were people related. Poor user practices or gullibility ranked first at 41%, followed by a lack of end-user cybersecurity training at 40%. By comparison, just 8% cited outdated security patches and 15% cited a lack of advanced security solutions such as EDR or MDR.

Attackers do not need to defeat every security control. They need to convince one person to click a link, share credentials or approve a payment. That makes people one of the hardest parts of the attack surface to control.

*These factors describe how attacks occurred, not necessarily whether they were successful.

Primary factors that contributed to cybersecurity incidents



When recovery goes wrong, humans are still part of the equation

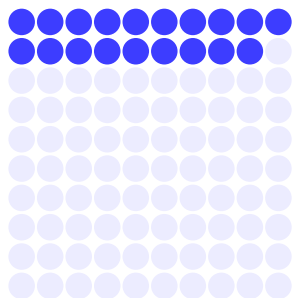
The human factor also affects recovery. Among organizations that experienced slower-than-expected recovery after an incident, 19% attributed the delay to manual or complex recovery processes.

The more recovery depends on manual steps, coordination and individual knowledge, the more room there is for delay when teams are already under pressure. Automation can help by standardizing recovery and reducing the number of steps that depend on people getting everything right.

People are busy, distracted and often facing threats specifically designed to look legitimate. Organizations don't need perfect users. They need security systems, training and recovery plans built around the reality that mistakes happen, and that when they do, a moment of human error should stay a contained incident rather than a full-blown crisis.

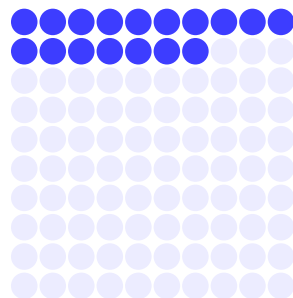
What slowed recovery

19%



Manual or complex recovery processes

17%



Dependence on third-party vendors

10%

Limited IT or security staff / expertise

10%

Difficulty identifying affected systems

10%

Lack of a clearly defined or tested recovery plan

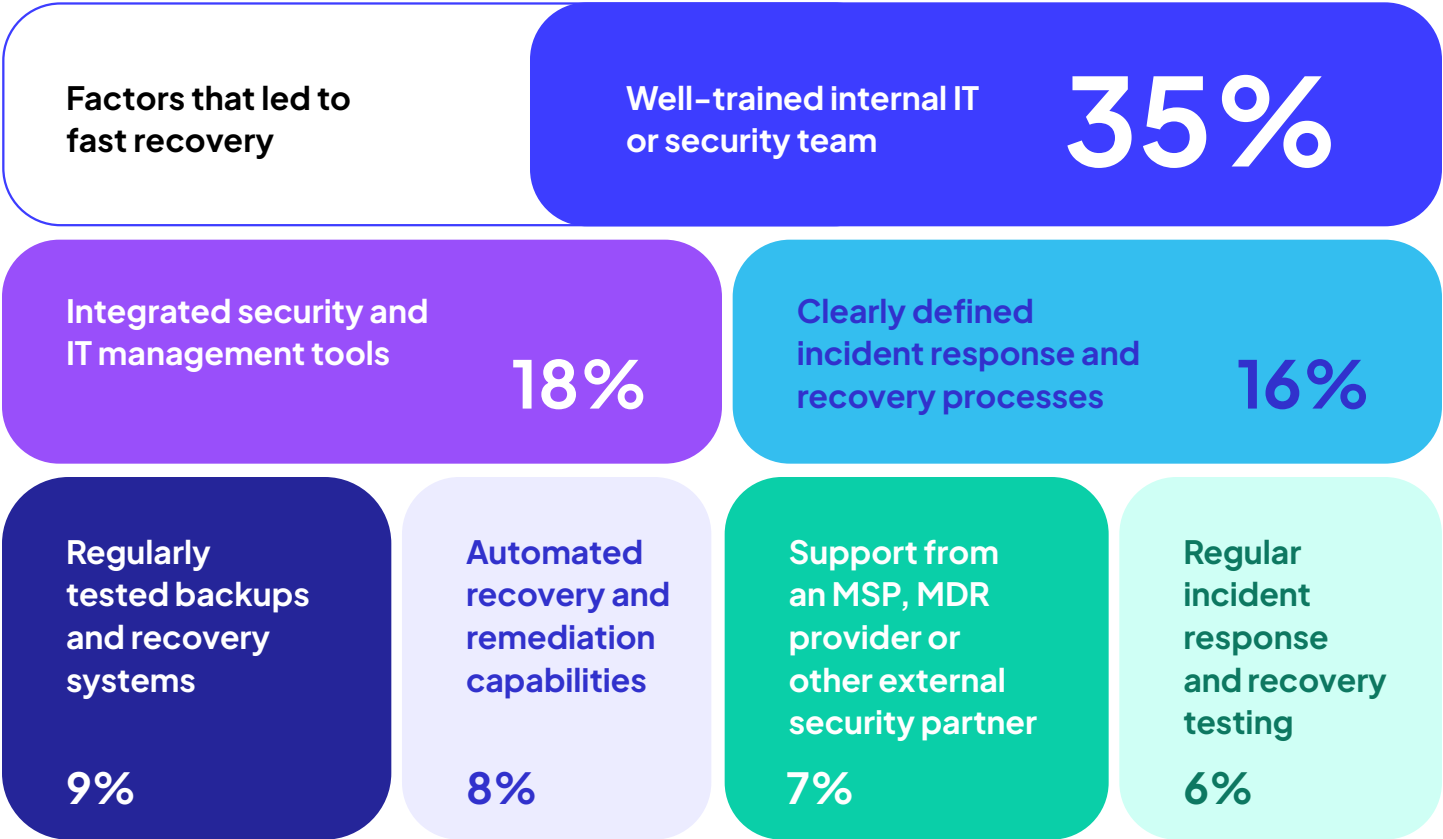
The key ingredients to faster recovery

Looking at organizations that recovered quickly from an incident, which we defined as within two hours, some useful patterns emerged. A well-trained internal IT or security team was the biggest factor, cited by 35% of respondents. Integrated security and IT management tools followed at 18%, pointing to the value of having connected tools that help teams see, manage and respond to an incident quickly.

Preparation also plays a role. About 16% pointed to clearly defined incident response and recovery processes, while 9% cited regularly tested backups and recovery systems. Together, these findings show that faster recovery depends on having the right people, tools and processes in place before an incident happens.

68%

of respondents see human error as the biggest potential gateway for attackers. It is also one of the leading contributors to successful cyber incidents.



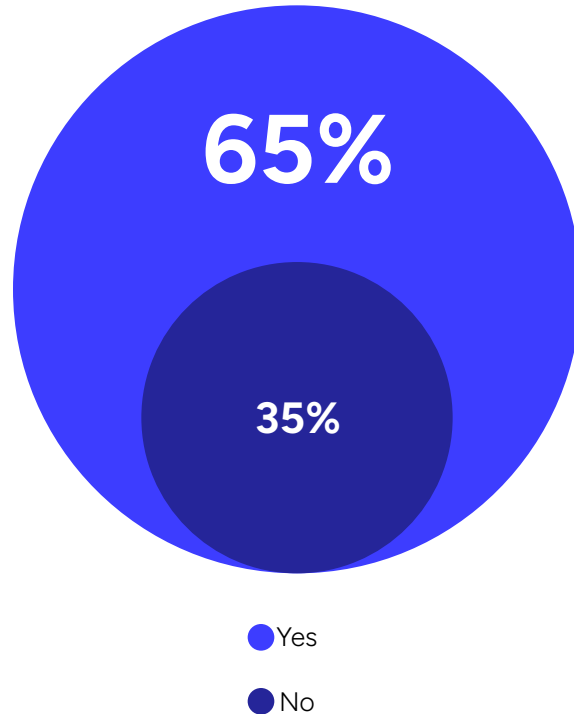
Finding Two

Being audit-ready doesn't make compliance easy

About 65% of respondents say they could pass a compliance audit today without preparation, suggesting strong confidence in their current readiness. But passing an audit and maintaining compliance are different challenges. An audit is a point-in-time test, while compliance requires organizations to keep controls, documentation, processes and employee practices up to date.



Could you pass a compliance audit today, with no preparation time?



What can get in the way of audit readiness

The findings suggest that even organizations that feel confident about their overall readiness can have gaps in the evidence, controls or people needed to demonstrate compliance.

When asked what could create problems during an audit, incomplete documentation or policies ranked highest at 49%. Another 34% pointed to security controls that are not fully implemented, while 33% cited a lack of employee security awareness or training.

Areas most likely to create audit challenges

49% Incomplete documentation or policies

18% Vulnerability management or patching gaps

34% Security controls are not fully implemented

17% Incident response plan has not been tested

33% Lack of employee security awareness or training

16% Weak identity and access management

24% Third-party / vendor security gaps

11% Backup and recovery processes are not regularly tested

21% Insufficient logging, monitoring or audit trails

8% We do not anticipate any major issues

Compliance takes ongoing work

The broader compliance data highlights the practical challenges of maintaining that readiness over time. Budget constraints are the biggest concern at 47%, followed by keeping up with changing regulations at 42% and limited staff or expertise at 41%. Another 33% struggle to maintain documentation and evidence.

Unlike an audit, compliance does not have a finish line. Requirements change, controls need to be maintained, evidence needs to stay current and employees need ongoing training. Being able to demonstrate compliance today does not necessarily mean the organization will be ready tomorrow.

The practical goal is to make compliance part of everyday security operations rather than something that needs to be prepared for when an audit arrives.

65% say they could pass a compliance audit today without preparation, yet 49% cite incomplete documentation as their biggest audit risk.



Areas most likely to create audit challenges

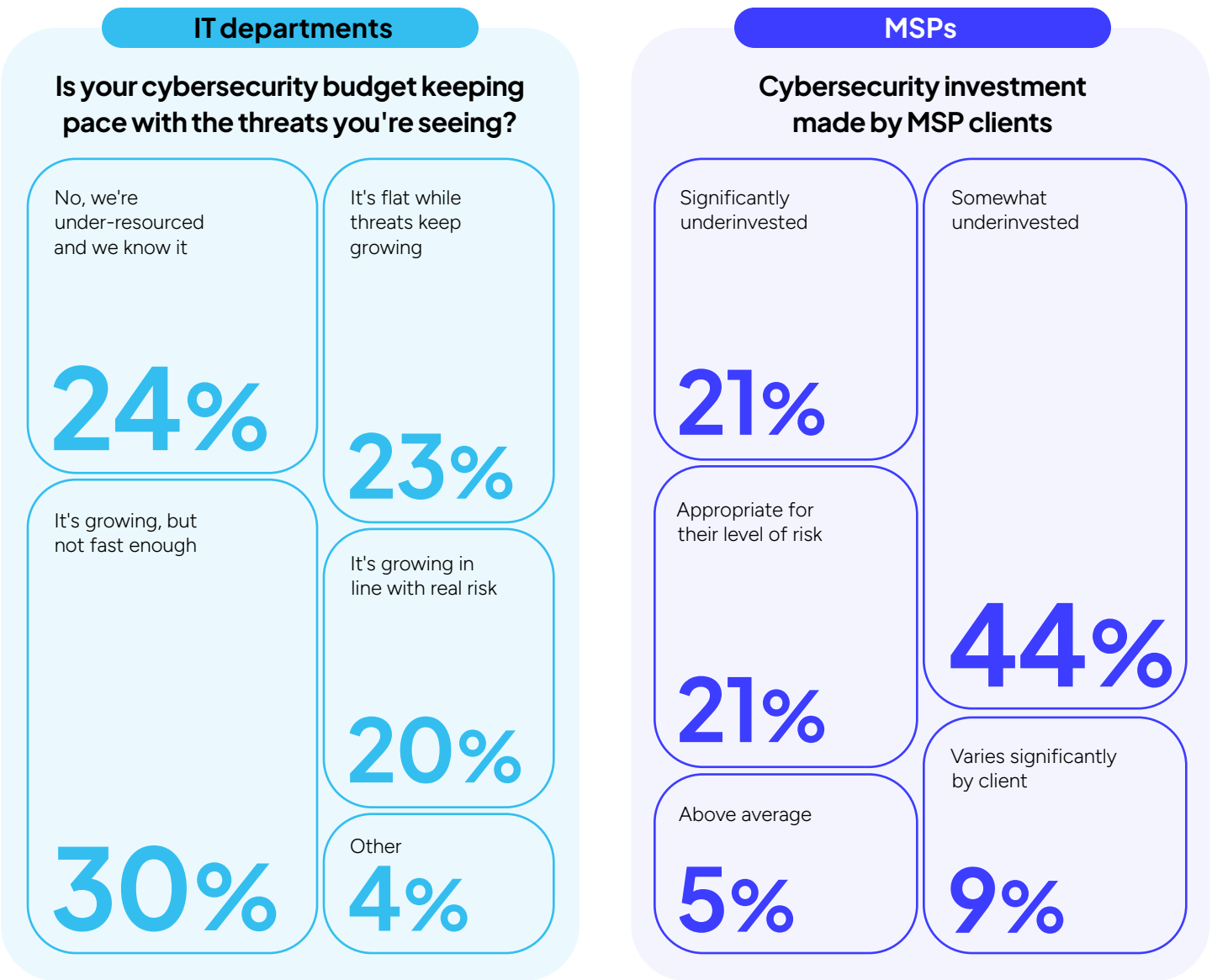


Finding Three

Cybersecurity investment isn't keeping up with risk

Most organizations recognize the risk they face, but their security budgets are struggling to keep pace. Only 20% of IT departments say their cybersecurity budget is growing in line with risk. The other 77% say they are under-resourced, keeping spending flat as threats grow or increasing their budget too slowly.

MSPs see the same pattern across their clients. About 65% say their clients are underinvested in cybersecurity, with 44% somewhat underinvested and 21% significantly underinvested.



Why investment falls behind

Cost remains the biggest barrier. Nearly four in 10 MSPs say available budget is the main factor determining whether clients invest in recommended security solutions.

Security investment is also often triggered by events rather than risk. One-fifth of respondents said a recent incident or near miss drove clients' investment, while the same number cited compliance or cyber insurance requirements the second most common driver. Only 11% say clients invest based on clear evidence of business impact, while just 9% point to demonstrated risk reduction.

The result is a reactive cycle: security investment becomes a priority when something happens, rather than before it. By then, the cost of responding can be far higher than the cost of getting ahead of the risk.

77% of IT departments say their cybersecurity investment is falling behind the risk they face.

65% of MSPs say their clients are underinvested.

What drives MSPs clients to invest in cybersecurity

Cost and available budget

39%

A recent cybersecurity incident or near miss

20%

Compliance or cyber insurance requirements

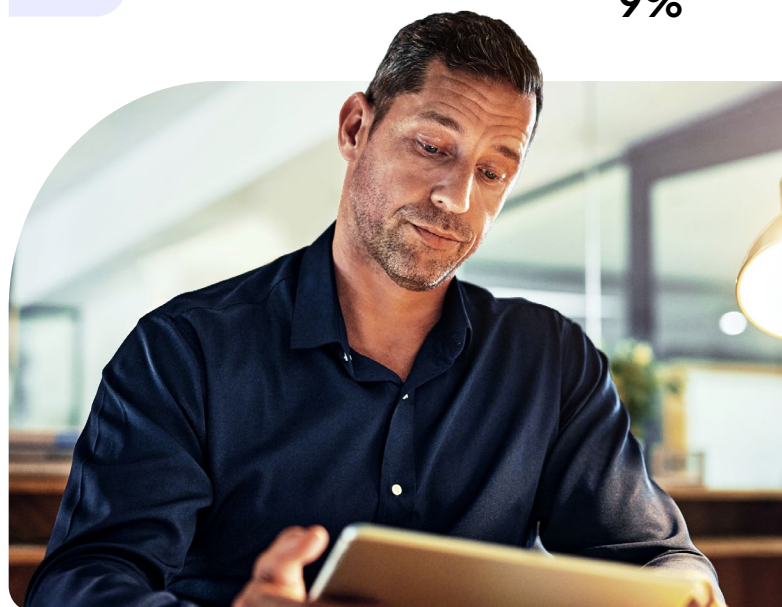
20%

Clear evidence of business impact

11%

Demonstrated reduction in cybersecurity risk

9%



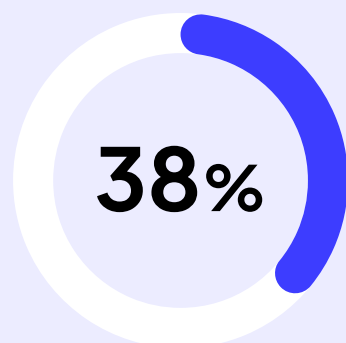
Finding Four

Security teams are bogged down by friction

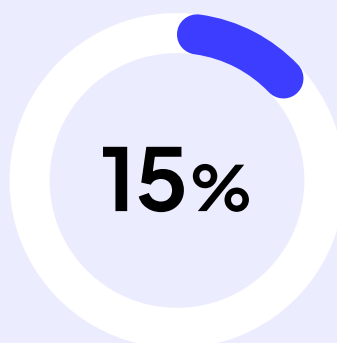
The gap between knowing what needs to be done and having the capacity to do it shows up in the daily work of security teams. Routine requests, tool management and competing IT priorities consume time that could otherwise go toward investigating threats, improving defenses and preparing for incidents.

Demands like end-user requests, unexpected outages and password resets may be routine, but they compete directly with the work needed to strengthen security over time.

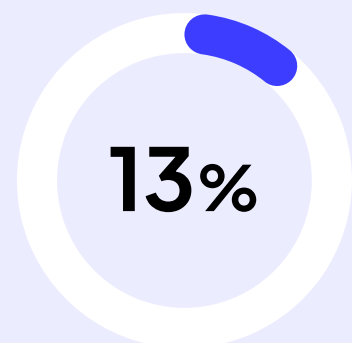
Tasks that most commonly interrupt security work



End-user requests



Unexpected outages



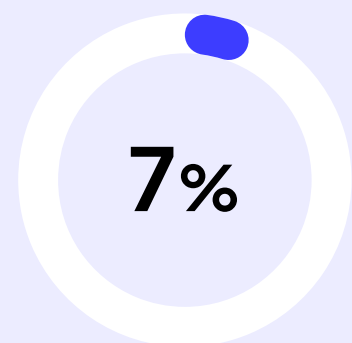
Password resets



Meetings



Compliance work



Device onboarding

The security stack is adding to the workload

The friction also comes from the controls teams put in place to reduce risk.

These controls play an important role in protecting organizations, but they still require day-to-day management. Policies need to be maintained, access exceptions handled and users supported. As security environments become more complex, the workload grows alongside the number of controls teams must manage.

A security control only helps if teams have the capacity to operate it effectively. When managing security consumes too much time, there is less capacity for the work that strengthens the organization against future threats.



Security practices that create the most operational friction

Multifactor authentication (MFA)



Privileged access management



Email security



Compliance documentation



Patch management



Vulnerability remediation



Endpoint management



Security demands create trade-offs elsewhere

Security does not operate in isolation. The demands of maintaining a strong security posture can affect budgets, employee experience and the time technicians have for other IT priorities. About 30% of respondents say they most often trade off IT budget to maintain security, while 28% point to end-user experience and 15% to technician productivity.

In practice, this can show up as less budget for other IT priorities, extra steps or restrictions for employees and technicians spending more time on mundane security tasks instead of projects and user support.

For businesses and MSPs, the practical step is to make these trade-offs clear. Identify where security is consuming budget, time or user capacity, then decide which areas can be reduced, automated or handled differently without increasing risk. This helps teams stay secure without letting security demands slow down the rest of the business.

What security teams trade off to stay secure

30%

IT budget

28%

End-user experience

15%

Technician productivity

9%

Automation opportunities

8%

Project delivery timelines

7%

Customer satisfaction

When security gets complex, decisions get harder

The pressure also affects the decisions security teams make every day. Budget decisions rank highest, with 27% of respondents saying they feel least confident making them. This connects directly to the investment gap in Finding Three. When budgets already lag behind risk, deciding what to fund becomes one of the most important and difficult security decisions teams face.

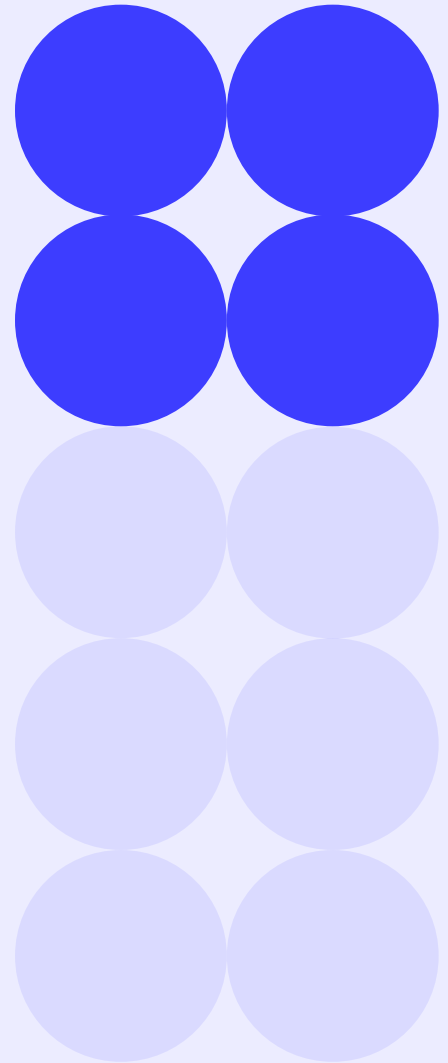
About 18% of respondents are least confident determining whether an alert is a real threat, while 16% struggle most with prioritizing vulnerabilities.

The issue is that security teams must make these decisions quickly and getting them wrong has consequences. If a team cannot confidently distinguish a real threat from a false alarm, it can waste time investigating noise or miss something that needs immediate action. Similarly, poor vulnerability prioritization can mean spending limited time on lower-risk issues while more serious exposures remain unaddressed.



4 in 10

organizations trade off user experience or technician productivity to stay secure.



38% of respondents say end-user requests are the biggest interruption to security work.

Security decisions respondents feel least confident making

27% Budget decisions

13% Configuring policies

18% Determining if an alert is real

12% Responding to ransomware

16% Prioritizing vulnerabilities

10% Recovering after an incident



Finding Five

As security skills grow scarce, AI helps fill the gap

Security teams are struggling to find the skills they need most. Security automation and AI specialists are the hardest to find or retain, cited by 32% of respondents, followed by security operations and incident response at 30%.

Demands like end-user requests, unexpected outages and password resets may be routine, but they compete directly with the work needed to strengthen security over time.

This is significant because, as we saw in Finding One, having a well-trained internal security or IT team and clear incident response processes are among the factors associated with faster recovery after an incident.

Security skills organizations struggle to find or retain



AI is already doing more of the day-to-day security work

At the same time, AI is helping teams stretch the skills they have. Rather than replacing security professionals, it is increasingly taking on high-volume work that can be difficult to manage manually.

Threat detection and monitoring is the most common use of AI in cybersecurity, cited by 44% of respondents. Email security and phishing protection follows at 33%, while 29% use AI for alert reduction or triage.

These are areas where AI can help teams process more information, reduce repetitive work and respond faster. For teams already stretched by limited skills and growing security demands, that additional capacity can make a meaningful difference.

How AI is currently being used in cybersecurity

44% Threat detection and monitoring

33% Email security and phishing protection

29% Alert reduction or triage

28% Automated response or remediation

24% Security reporting and analytics

21% Vulnerability management and risk assessment

21% We are evaluating AI but have not yet implemented it

18% Reporting and compliance

14% Security awareness and training

11% We are not currently using AI to enhance our cybersecurity posture

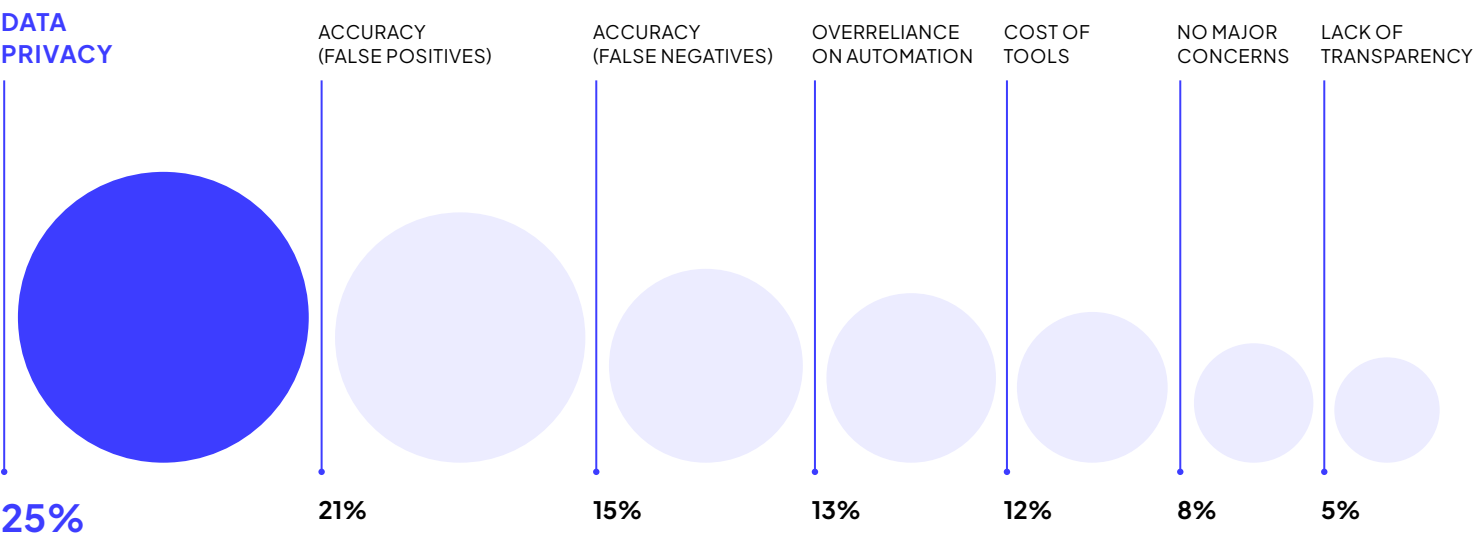
AI helps extend security teams

For security teams facing growing workloads and limited capacity, AI can help take on routine and time-consuming tasks.

Respondents also see areas where careful oversight matters. Data privacy ranks as the biggest concern at 25%, reflecting the risks of using AI with sensitive security data. About 21% of respondents worry about false positives and 15% about false negatives.

The opportunity is to make AI a valuable part of the security workforce. Used with the right oversight, it can help teams work more efficiently, improve accuracy and strengthen human decision-making. It can also help extend the capacity of teams facing skills shortages, while leaving people in control of the decisions that matter most.

Biggest concerns about using AI in cybersecurity



32% respondents said security automation and AI specialists are the hardest skills to find.

Your cyber resilience playbook: Engineering around human error

The research points to five pressure points that repeatedly make security harder to manage: people make mistakes, investment falls behind risk, routine work consumes security capacity, critical skills are hard to find and compliance takes more ongoing effort than an audit alone can show.

The answer is not to add more work to already stretched teams. It's to make security easier to operate, more resilient when things go wrong and better aligned with the resources teams have.

Human risk: Build for the mistake you know will happen

Training matters, but people will still make mistakes. The stronger approach is to build layers of protection so one mistake does not become a major incident.

Use controls such as email protection, MFA, least-privilege access and tested recovery. Then look at what happens when those controls are challenged. Where do users get stuck? Where do technicians have to intervene manually? Where could one mistake still spread?

The goal is not perfect behavior. It's about limiting the impact when behavior falls short and making recovery faster when an incident occurs.





Cybersecurity investments: Stop waiting for an incident to create urgency

Security investment is often triggered by an incident, audit finding or compliance requirement. That makes it reactive by design.

Instead, build the case before the trigger arrives. Connect specific security gaps to business impact, including downtime, recovery costs, regulatory exposure and lost revenue. For MSPs, make that risk visible to clients before an incident makes the conversation urgent.

Operational friction: Make security easier to operate

Routine requests already consume a significant amount of security team capacity. Identify what repeatedly pulls security professionals away from higher-value work, then simplify and automate.

The same applies to user-facing controls. Security measures that are difficult to use can create more support requests, reduce productivity and put pressure on teams to weaken them. The goal is to make secure behavior the easier path.

Security teams also need a clearer way to make trade-offs. When resources are limited, identify which risks need immediate attention, which can be reduced through automation or process changes and where additional investment will have the greatest impact.

Skills and AI: Extend the team you have

Hiring alone will not close the security skills gap. Security automation and AI specialists are among the hardest skills to find, while security operations and incident response are also in short supply.

AI can help fill some of that capacity gap. Teams are already using it for threat detection, alert triage, and automated response, particularly where the volume of work is difficult to manage manually.

Use AI for repetitive, high-volume tasks, but build the skills needed to oversee it. Security professionals still need to validate AI output, identify false positives and false negatives, and know when human judgment is required.

The goal is not to replace expertise with AI. It is to give a stretched team more capacity while keeping people accountable for the decisions that matter.



Compliance: Make readiness part of the work

Being able to pass an audit today does not mean compliance will stay on track tomorrow. Regulations change, controls evolve, employees change and documentation becomes outdated.

Instead of treating an audit as a deadline, build compliance into everyday security operations. Assign clear owners, review requirements regularly, maintain evidence as work happens and make sure controls are being used rather than simply documented.

Putting it into practice

Good security depends on having the right protections in place and making them workable for the people managing them. Kaseya offers a range of IT security solutions designed to help organizations strengthen protection across users, endpoints, email and more.

[Explore Kaseya's IT security solutions](#)

Who we surveyed

1,132

Total respondents

55%

MSPs

45%

IT departments

63

Countries and territories represented across four global regions: the Americas, LATAM, EMEA and APAC

59%

Technicians represented across the survey, alongside 41% executives

Survey methodology

Kaseya conducted the survey in August 2026 using structured questionnaires. The questionnaire included a mix of quantitative and qualitative questions, with respondents selecting from provided answer choices as well as sharing responses in their own words where appropriate. Where questions allowed multiple responses, percentages may total more than 100%. The report presents the findings in a format designed to highlight the trends, challenges and practical priorities most relevant to cybersecurity and IT teams.





Kaseya is the leading global provider of AI-powered IT management and cybersecurity software. Kaseya delivers a unified technology platform to manage infrastructure, secure endpoints, back up critical data, and streamline operations for more than 40,000 MSP and SMB customers around the globe. To learn more, visit www.kaseya.com.

[kaseya.com](https://www.kaseya.com)