Cybersecurity Perspectives 2021

The Pandemic, SolarWinds, and the Security Leader State of Mind

Table of Contents

Introduction

2020 was an extraordinary year for businesses, which had to pivot quickly to remote work environments. That meant accelerating cloud migrations and moving data and operations that were still on-premises to the cloud, as well as fortifying employee work-from-home systems and remote connectivity.

Ever the opportunists, cyber criminals took advantage of the chaos, targeting government agencies, schools, healthcare organizations, and other critical industries with ransomware that victims would be desperate to pay to resolve.

> **Phishing and other attacks targeted corporate employees whose home computers and networks fell outside the security team's domain.**

The view from mid-2021 is surprisingly positive, given the uncertainty businesses felt confronting such an unprecedented technology disruption. Most companies weathered the transition and are prepared for remote work environments as a new normal. At a macro level, cyberattacks did not interfere with the election, although ransomware attacks have been unrelenting.

In late 2020 and early 2021, two big cyberattacks impacting hundreds of companies were an important warning against security complacency. Attackers compromised the software update system of SolarWinds, a provider of network management software, used it to distribute malware to thousands of the company's customers, and then activated the backdoor for further hacking in a number of customer networks. This gave attackers inside access to networks of government agencies and targeted private sector companies. Meanwhile, researchers discovered vulnerabilities in Microsoft Exchange that were exploited in a cyber campaign dubbed Hafnium. Before patches were released, tens of thousands of private and public organizations were compromised. These attacks brought a new sense of urgency to businesses across industries.

> **The SolarWinds attack also spurred President Biden to release an executive order aimed at addressing software supply chain attacks.**

For our fifth annual Scale Venture Partners survey, we asked security leaders throughout the U.S. how the events of the past year have influenced them, covering the period from the start of the pandemic to the SolarWinds revelations beginning in late 2020. With the Colonial Pipeline attack just starting to make headlines, those lessons will come to bear on what is already shaping up to be an eventful year for the industry.

Key Findings

Security budgets and staff rose during the pandemic and will grow after SolarWinds too. Organizations have increased security budgets and staff as a result of the pandemic and rise in WFH-related attacks. Meanwhile, SolarWinds is also prompting them to increase budgets and secure software updates. Forty percent increased headcount and 63% increased budget, with 45% nearly doubling the budget.

The rush to remote work increased security risk. The move to work-from-home environments increased risk as cyber criminals exploited unsecured home networks and cloud service weaknesses. More than half (52%) of respondents said cybersecurity incidents involving attacks on compromised data, devices, systems, or networks increased. Thirty-six percent attributed the majority of those attacks to employees working from home.

The chain of command matters for security. Security professionals who perceive they have a "seat at the table" – that is, a direct line to CEOs – appeared to care more about high-level "business-impacting issues," such as data privacy, network security, and regulatory measures. Meanwhile, 94% of respondents who report to the CEO said they are equipped to handle cybersecurity risks, compared with 86% who do not report to the CEO.

Automation can't come soon enough. As the number of security solutions in enterprises has risen, companies are turning to automation tools to help security teams stay on top of alerts and manage new solutions. Of ranked investment priorities, automation climbed to sixth from eighth in 2018; for the first time it was listed among the tools that respondents plan to build in house because they can't find what they need in the market.

Data privacy remains an investment priority. Spending on data privacy solutions now and in the future remains a security investment priority, and is accelerating in importance as companies acclimate to new regulations and market solutions. Data privacy is among the top four security investments and the second highest technology investment for the coming 12 months.

The Impact of the Pandemic and the SolarWinds Cyberattack

Even during "normal" years, there's rarely a dull moment on security teams. But 2020 delivered a one-two punch to security operations: the SolarWinds software supply chain attack and the COVID-19 pandemic. The scale of these two events couldn't help but shake up how security teams manage risk — such as generating more conversations with C-suite executives, boosting budgets, and continuing to invest in cloud infrastructure.

Remote Work Increases Security Risks

The abrupt shift to remote work tested security leaders' ability to manage risks, since end users were scattered far beyond network perimeters, using home networks with potential security gaps. More than half **(52%) of respondents said cybersecurity incidents increased as employees shifted to remote work**; the incidents included attacks on data, devices, systems, and networks. Thirty-six percent attributed **50% or more of those attacks to employees working from home.**

Without the ability to closely manage where and how employees access network and cloud resources, it's not surprising that respondents must grapple with higher risk levels. Security professionals named **lack of adequate security on home devices as their top security challenge (66%).** Other remote work challenges they called out: falling for social engineering attacks, corporate data in the cloud at potential risk due to misconfigurations, inadequate VPN technology, and unsecured home wifi networks.

52%

of respondents said cybersecurity incidents increased as employees shifted to remote work

36%

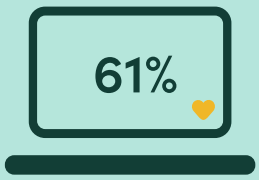
attributed the majority of those attacks to employees working from home

66%

of security professionals named lack of adequate security on home devices as their top security challenge

Security professionals have already been shoring up cloud infrastructure over the past several years, as previous Scale surveys have shown. This year, no doubt partly in response to widespread remote work, **cloud infrastructure topped the list of technologies garnering the most investment** – in last year's Scale survey, cloud infrastructure was fourth on the list. Cloud infrastructure security also topped the list of technologies in which security teams plan to invest more money and resources over the next 12 months, tying with data privacy (28% each).

In spite of the heightened risks associated with remote work, security professionals' job satisfaction increased during the pandemic. **Sixty-one percent of respondents said they were much happier (36%) or somewhat happier (25%) with their current roles since the pandemic began.** It's possible that working from home and avoiding long commutes are the reasons behind this job satisfaction during a tumultuous time, as many employees across industries have reported similar satisfaction in other workplace surveys.



of respondents said they were much happier or somewhat happier with their current roles since the pandemic began

SolarWinds Triggers a Rethink of Security Operations

Simply judging by the continuing amount of trade press and general media coverage of SolarWinds, there's a good deal of concern about strengthening security to avoid similar attacks in the future. The Biden administration issued a federal executive order to bar contractors from working with the government unless they adhere to more stringent cybersecurity requirements. The Scale survey shows respondents too are retooling security operations, adding personnel, and boosting budgets in response to the changing threat environment.

When asked how they've changed security processes over the past 12 months, **57% said they have increased integration with other teams,** like IT and software development. Given the ongoing trend to share data with C-level executives (see page 9) and empower other teams to focus on risk management, it's unsurprising that respondents are working to address SolarWinds-style risks by collaborating with other business functions.

SolarWinds also sharpened respondents' focus on security risks created by third-party vendors whose products play critical roles in business operations. **Thirty-six percent said that they**

expected third-party risks to rise over the next 12 months; 47% of respondents said **third-party risks are a top factor affecting the C-suite's understanding of the business impact of security,** behind data breaches (57%) and remote work (54%).

To address software supply chain risks highlighted by SolarWinds, **52% intend to use technology to manage the security of software updates –** the SolarWinds attackers compromised the software update mechanism to distribute a malicious backdoor to unsuspecting customers. Half (50%) said they would increase security budgets to address the impact of SolarWinds. Meanwhile, 45% said they would turn to technology that manages the security of digital certificates and tokens to help prevent attackers from compromising the code signing keys as was done in the SolarWinds attack.

Asked what steps they take to minimize third-party security risks, **51% said they perform an audit of third-party vendors' procedures.** Forty-eight percent said they rely on third-party risk rating services like CyberGRX or a risk-exchange service; 47% ask vendors to complete self-assessment questionnaires.

Respondents are also augmenting staff and budgets where they can. **Forty percent of respondents said they increased headcount in 2020.** Of those who increased headcount, nearly one-third (32%) said it rose 50% or more.

In terms of budgets, **63% said their security budget increased over the past 12 months.** Of those those who increased their budget, 45% said it had doubled. Thirty-four percent said their budgets stayed the same and only 3% said their budgets had decreased.

When asked how they reorganized the structure of their security teams to address new threats, **59% said they had trained security teams in best practices,** while 48% changed their team's reporting structure.

52%

said they would use technology to manage the security of software updates

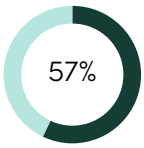
40%

of respondents said they increased headcount in 2020

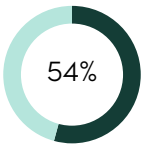
63%

said their security budget increased over the past 12 months

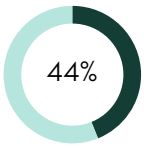
Over the past 12 months, how have you changed your processes/strategy around security?
Select all that apply.



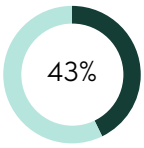
Increased integration of security with other teams



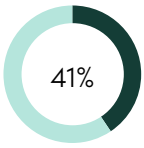
Increased cybersecurity metrics and reporting



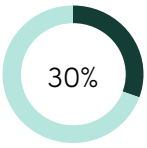
Expanded accountability for security across the business



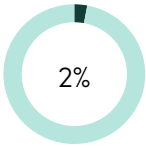
Applied stricter enforcement of security policies



Increased visibility about security within the organization

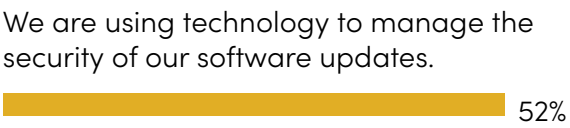


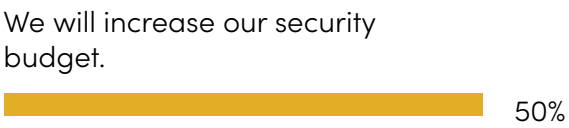
Re-organized security teams

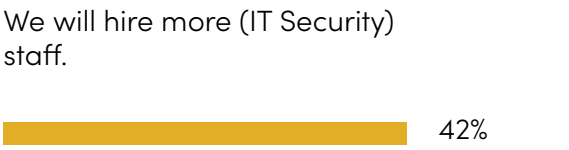


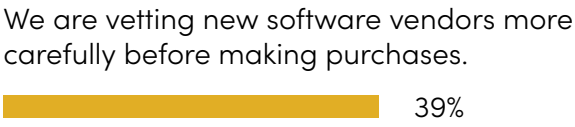
No change

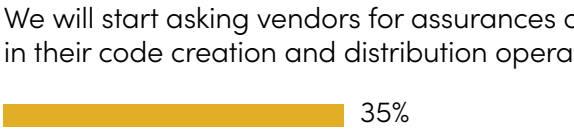
How do you think the SolarWinds attack will influence your company's approach to addressing software supply chain risks?
Select all that apply.

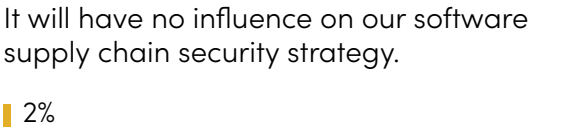










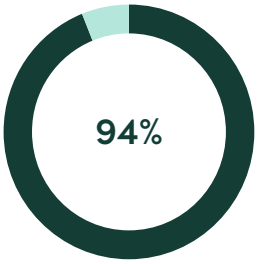


The Value of a Seat at the C-Suite Table

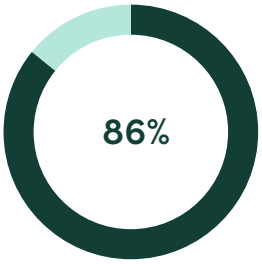
For decades, security teams worked more or less in silos, considered an offshoot of IT instead of a mission-critical function. Thanks to increasing awareness that cyberattacks destroy brand image and customer trust, **enlightened organizations no longer sideline security**. In the process of elevating the security practice, security professionals now seek a "seat at the table," meaning regular communication with leadership about the state of risk management. Frequent conversations between the C-suite and security teams benefit both sides: leadership recognizes the link between security and business value, and security teams are better able to discover new opportunities to deliver value to other business functions like finance and operations.

The higher up the C-suite the conversations go, the greater the changes in the dynamic between security and leadership. For example, survey respondents who report to the CEO focus more on issues with high-level business impact, such as data privacy, network security, and regulatory compliance. On the other hand, **respondents who did not report to the CEO focused more on second-order issues** like defending against specific threats or making sound technical security investments.

Having a seat at the table also appears to affect confidence in the ability to manage risk. **Ninety-four percent of respondents who report to the CEO said they are equipped to handle cybersecurity risks, compared with 86% who do not report to the CEO.** In addition, 94% of all respondents said that, compared to 12 months ago, the C-suite better understands the business impact of security. It's likely that the twin challenges of SolarWinds and COVID-19 have markedly raised the C-suite's awareness of the value of security.



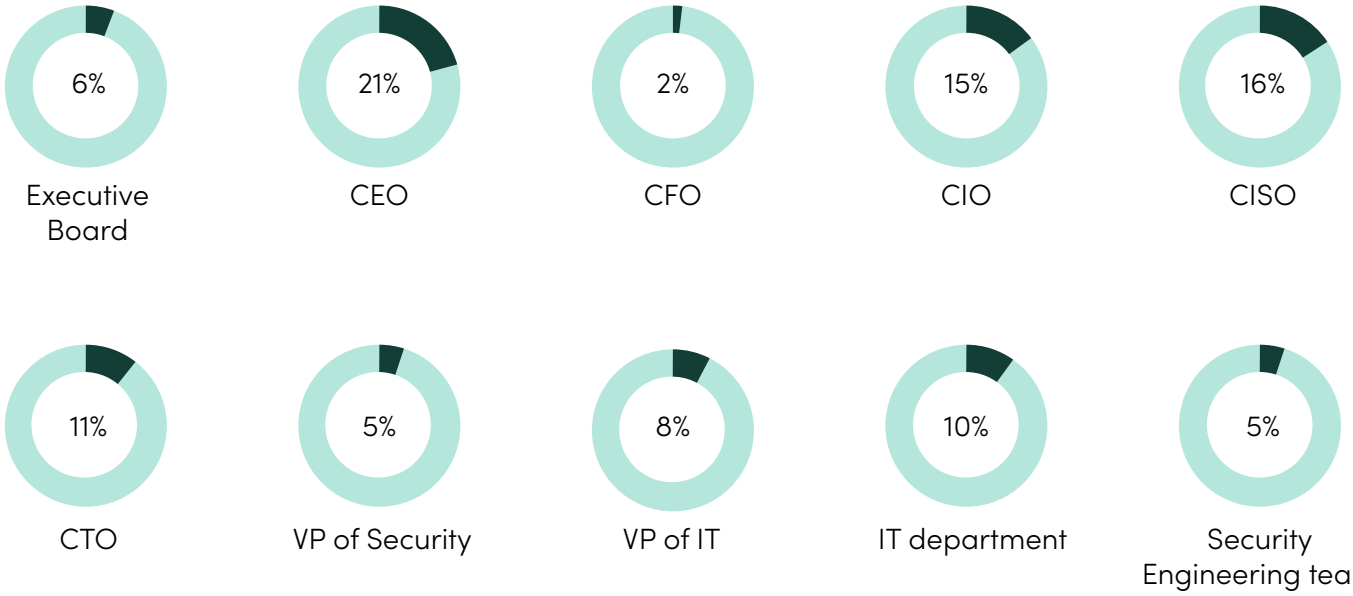
of respondents who report to CEOs said they are more or less equipped to handle cybersecurity risks



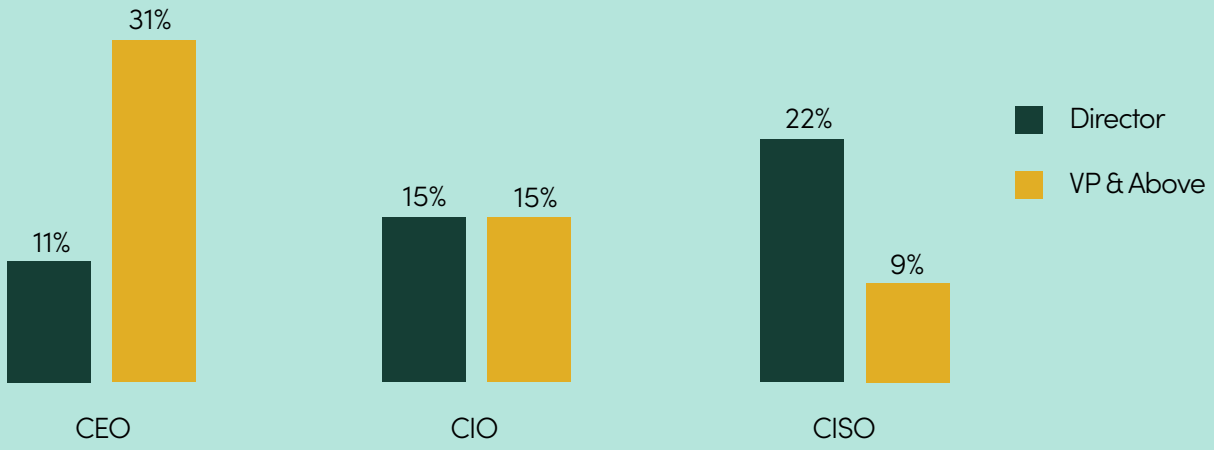
of respondents who **do not** report to CEOs said they are equipped to handle cybersecurity risks

A security professional's position in the organization can also affect views on cybersecurity and its impact — such as whether the CEO is viewed as ultimately accountable for security. For respondents at the VP level and above, **31% said the CEO is accountable for security, while 15% said the CIO is accountable**. By contrast, 22% of respondents at the director level said CISOs are ultimately accountable for security.

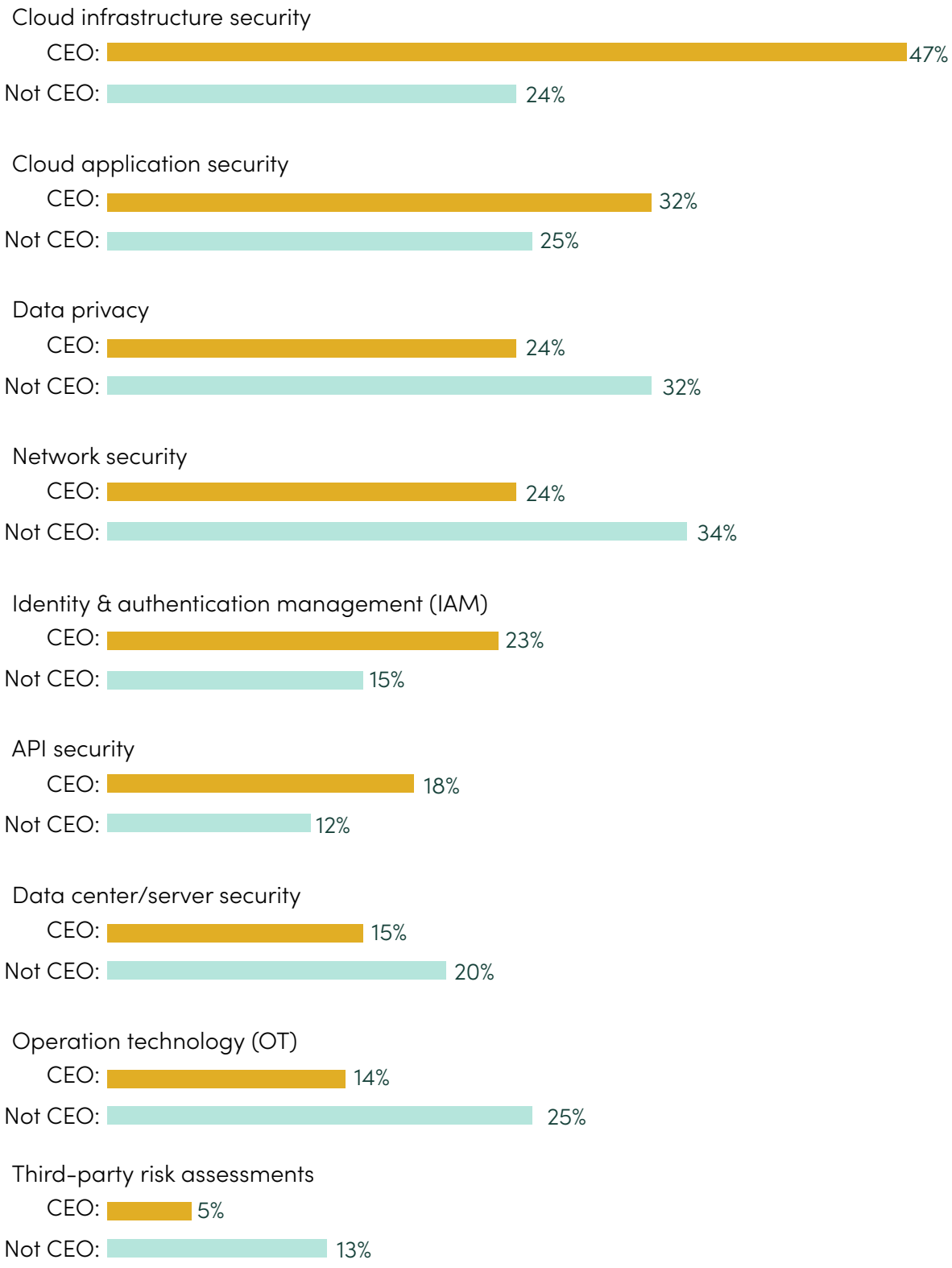
In your organization, who is ultimately accountable for security?



Who is ultimately accountable for security by title?



Security technologies/strategies currently investing in by whom the CISO reports to:



Automation Seen as Key to Managing Sprawling Solutions

"Tool sprawl" — that is, the rapid proliferation of security point solutions, platforms, and services deployed inside a given enterprise — is a growing challenge. A 451 Research report found that 40% of survey respondents use between 11 and 30 monitoring tools alone.

In some environments, multiple tools are deployed to respond to specific security issues like endpoint security or vulnerability scanning. Other tools stand in for shortfalls in headcount, especially in fast-growing organizations. Either way, the solutions deployed to solve problems often end up becoming problems themselves: more tools mean more time spent on managing software by already overburdened security teams. The operational overhead of introducing new security tools is often underestimated.

Automation has come to be seen as the hero that will save organizations from tool sprawl. Companies using a medium to high-level of security automation rose from 39% in 2019 to 47% in 2020, according to a recent SANS survey.

In terms of investment priorities, **security automation has risen steadily in the past two years, climbing from eighth place in 2018 to sixth in 2021.** As the number of security tools continue to expand, the need for automation has increased accordingly.

Automation technologies are also climbing up the list of solutions that security teams build in-house when they can't find the appropriate solution from a third-party vendor. **Of the 51% of respondents who said they created an in-house solution in the past 12 months, 23% said they had built security automation technology.** This marks the first time in our survey that respondents placed security automation technologies on the list of the top 10 security solutions they build in-house, coming in fourth place.

Security automation has risen steadily in the last two years, climbing from eighth place in 2018 to sixth in this year's report

23%

of those that created in-house solutions built security automation technology - its first year on the list

The rise of security automation technology may help organizations address one of their key challenges: managing tool sprawl and configuring individual solutions. The lack of automation can be seen as a barrier to managing risk: **"too much manual labor" is listed as one of the top three obstacles holding organizations back from achieving their desired security posture in the past 12 months.**

Also, in a four-year comparison across all Scale surveys, the obstacle of manual labor jumped slightly, by about 7% — a potential reflection of the increase in tech sprawl.

What are the top 3 security technologies/strategies you are currently investing in?

2018	2019	2020	2021
Cloud infrastructure	Cloud application security	Cloud infrastructure	Cloud infrastructure security
Cloud application security	Cloud infrastructure security	Cloud application	Data privacy
Network security	Network security	Network security	Network security
Data security/data loss prevention	Data security/data loss prevention	Data security/data loss prevention	Cloud application security
Data center / server security	Data center / server security	Data privacy	Data security/data loss prevention
Threat intelligence	Endpoint security	Data center / server security	Security automation technologies
Endpoint security	Threat intelligence	Security automation technologies	Operation technology (OT)
Security automation technologies	Security automation technologies	Endpoint security	Data center / server security
Breach/attack simulation	Breach/attack simulation	Operation technology (OT)	Endpoint security
Insider risk analytics	Quantum encryption	Threat intelligence	Identity & authentication management (IAM)

In what areas did you build an in-house solution?

35%
Network security

28%
Operation technology (OT)

25%
Data privacy

23%
Security automation technologies

22%
Cloud infrastructure security

21%
Data center/ server security

20%
Data security/ data loss prevention

20%
Cloud application security

19%
API security

14%
Threat intelligence

What were the top three obstacles holding your organization back from achieving its desired security posture 12 months ago?

51%
Complex legacy data center infrastructure

49%
Outdated security technology/processes

45%
Too much manual labor associated with security

Data Privacy Remains a Priority

Cyberattacks no longer fly under the radar now that consumers are alerted to how breaches expose their personal data. Heightened consumer awareness joins data privacy regulations in Europe (General Data Protection Regulation), California (California Consumer Privacy Act and its updated version, California Public Records Act), and a growing number of U.S. states to drive ongoing investment in data privacy solutions.

Respondents placed data privacy among the top four security technologies that they are currently investing in. Data privacy saw the largest year-over-year rise in the list of technologies that will be prioritized the next 12 months, moving up from fifth place to second. In the 2020 Scale survey, data privacy placed in the top six security technologies prioritized for investment.

For the rest of 2021, data privacy tops the list of technologies that respondents expect to invest in, tying with cloud infrastructure security (28% each). Even though the regulations have been in place for a few years, enforcement has lagged, giving the industry time to better understand compliance requirements and the solutions available in the market.

Our survey also found that **confidence in managing data privacy risks remains high**. In the 2021 survey, 79% of respondents said they were confident in managing data privacy, compared with 75% in the 2020 survey. All of the work in the years leading up to GDPR and CCPA may be paying dividends alongside maturity in available tools and guidance on how to use them.

Data privacy is a growing priority, climbing from 5th place in 2020

Conclusion

This year's survey is good news for the cybersecurity industry as a whole as well as entrepreneurs pursuing new market opportunities. Security leaders have more resources and support than ever before, and more visibility inside the organization. All of which is reflected in higher confidence in their ability to do their jobs well.

2020 gave CISOs lessons that are very much still in play. The pandemic was the ultimate catalyst for accelerating the move to the cloud. SolarWinds highlighted security cracks in the software supply chain. And the move to remote work created even more openings for cyber attackers to access corporate data and networks, advancing the need for zero-trust architectures. Security professionals responded by increasing budgets and staff and examining how organizational reporting impacts security outcomes.

For startup founders looking for market opportunities, two key areas stand out: security automation and next-gen data privacy. Security teams are overwhelmed by all the security tools they manage and are in need of ways to automate more of their tasks. Meanwhile, neither the pandemic nor SolarWinds distracted security leaders from the ongoing responsibility of complying with regulatory requirements to protect the privacy of customer data. Yet comprehensive security is still very much an unsolved problem.

The coming year will no doubt bring new challenges for CISOs and additional opportunities for security startups as the perennial cat-and-mouse game between defenders and attackers advances. This year's survey paints a picture of organizations coming out of 2020 more resilient and prepared for the next threats.

Methodology

Scale Venture Partners commissioned Market Cube to conduct a survey of 300 security leaders in the United States who are responsible for buying decisions, the success of security deployments, or the overall security of the company. The web-based survey was fielded March 22 through March 30, 2021. The margin of error is plus or minus 5.6 percentage points.

You can view Scale's past Cybersecurity Perspectives reports here:

2020 | 2019 | 2018 | 2017

SCALE

scalevp.com