Computer Security in the States

An Assessment of Resilience and Current Practices in Local and State Government IT

Underwritten by

elastic

July 2020

Table of Contents

Overview

Purpose

State government networks continue to be pummeled by wave after wave of cybersecurity attacks, with over 230 known ransomware infiltrations recorded since early 2018 alone.[1] These attacks cripple operations, shutter websites, reap financial havoc, and sever essential lines of service between states and their citizens.

While some state and local institutions have reacted by evolving their cybersecurity posture, many others remain unequipped or unable to provision such resources toward the effort. The concerns have even reached the attention of federal legislators: pending House and Senate approval, the State and Local Cybersecurity Improvement Act recently introduced to Congress would authorize the Department of Homeland Security to establish a new grant program dedicated to plugging vulnerabilities in state and local networks.[2]

For state and local organizations in the crosshairs, what measures can they employ to protect themselves? What resources can they call on to transform their cybersecurity policies effectively? To answer these questions and others, Government Business Council (GBC) undertook an in-depth research study in April and May of 2020.

Methodology

To assess the perceptions and attitudes that state and local officials have regarding cyber vulnerabilities, GBC deployed a survey to a random sample of government respondents in April and May 2020. While over 400 state and local employees took part, the data presented herein reflect a subset of 215 respondents with involvement and insight into their agency's IT decision-making. 17% of respondents are IT leadership, project managers, and administration. Two-thirds work in a role related to the IT decision-making process or in a capacity where they are required to understand IT policies and processes.

1. StateScoop."Ransomware Attacks Map." May 2020. https://statescoop.com/Ransomware-Map/
2. Department of Homeland Security. "The "State and Local Cybersecurity Improvement Act" Accessed May 14, 2020. https://homeland.house.gov/download/state-and-local-cybersecurity-improvement-act-fact-sheet

Executive Summary

Internal IT expertise, more critical than ever, is insufficient

47% of respondents say that people are their greatest organizational vulnerability. In response, three quarters of organizations have invested in increased training and awareness campaigns for staff. However, as 29% of respondents cite lack of in-house expertise as a major barrier to cybersecurity improvement, this reveals the need for better top-down IT decision-making capabilities. Training and awareness campaigns are only as strong as the leaders who craft them.

Managed Service Providers could fill workforce gaps, but limited MSP visibility may be dangerous

As a lack of in-house expertise is a major concern for organizations, many contract out cybersecurity-related work to managed service providers (MSPs). 85% outsource tasks to MSPs, and a majority of this group say they have very little visibility into how the MSPs use their information. Of those who say they've experienced a recent cyberattack, 22% say it was linked to an MSP whereas 55% do not know if an MSP was involved. The inability to diagnose vulnerabilities and where they emerge is increasingly a concern for state and local IT leadership.

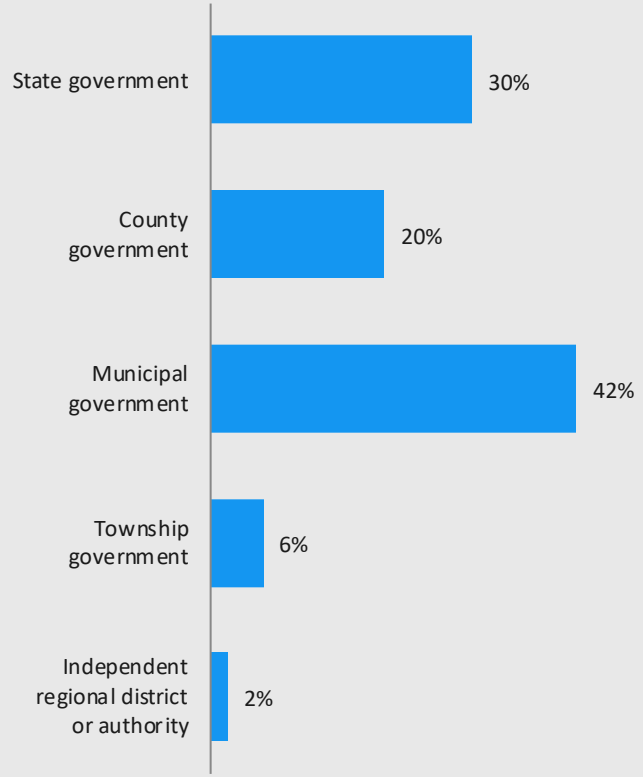
Organizations must focus on improved attack surface visibility to mitigate risk of blind spots

The most potent solutions prioritize vulnerability mitigation and improved visibility of an organization's attack surface–including all physical and digital IT assets on-premise, in the cloud, or hosted by a third-party provider. Only 15% say their organization has full visibility of its attack surface. 34% say they have moderate visibility, and 18% say they have limited to no visibility. While cybersecurity investment and confidence has increased in 2020 from 2019, 61% of respondents say their organization is still unable to prevent at least 25% of cyberattacks.

Respondent Profile

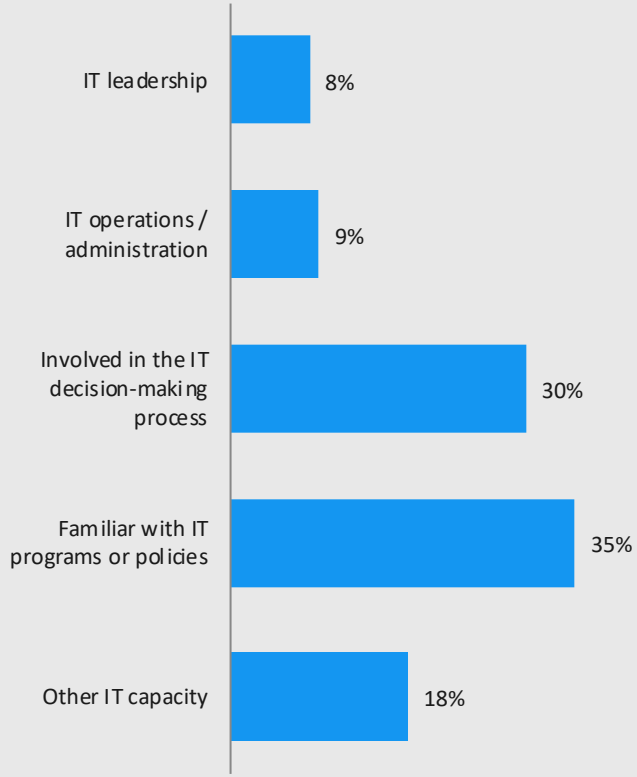
Respondents represent a targeted cohort involved in IT decisions, operations, and programs

Employer



Percentage of respondents, n=210
Note: Percentages may not add up to 100% due to rounding

Level of IT Influence

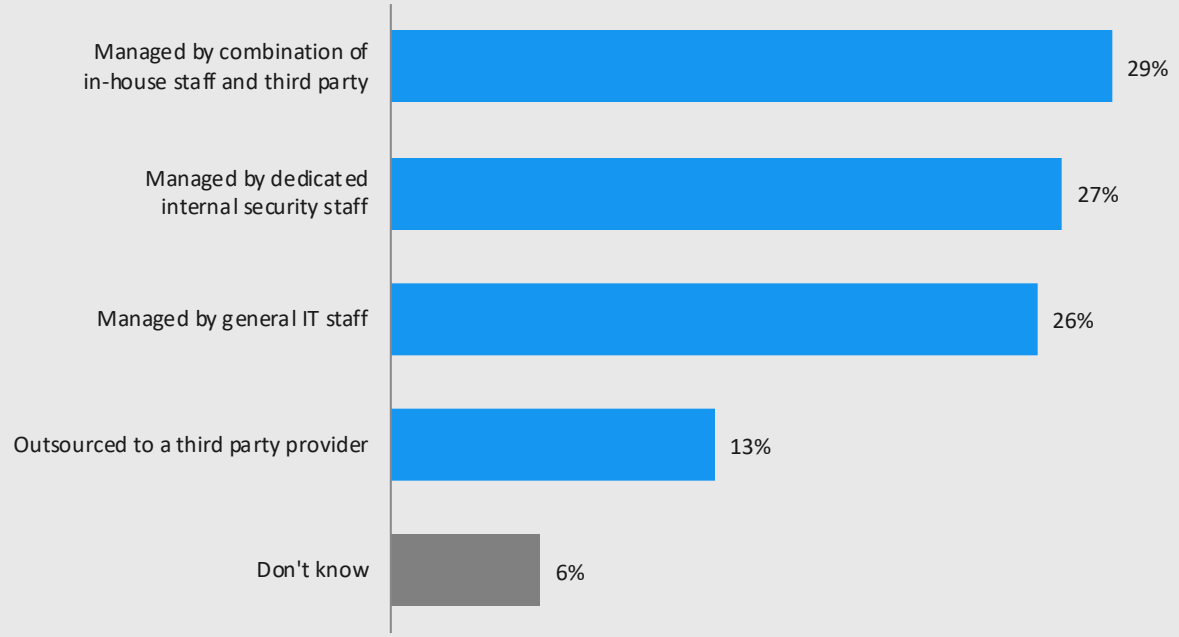


Percentage of respondents, n= 210
Note: Percentages may not add up to 100% due to rounding

Research Findings

Several types of IT staffing options are equally popular among respondents' organizations

What best describes your organization's IT security staffing?



Percentage of respondents, n=210
Note: Percentages may not add up to 100% due to rounding

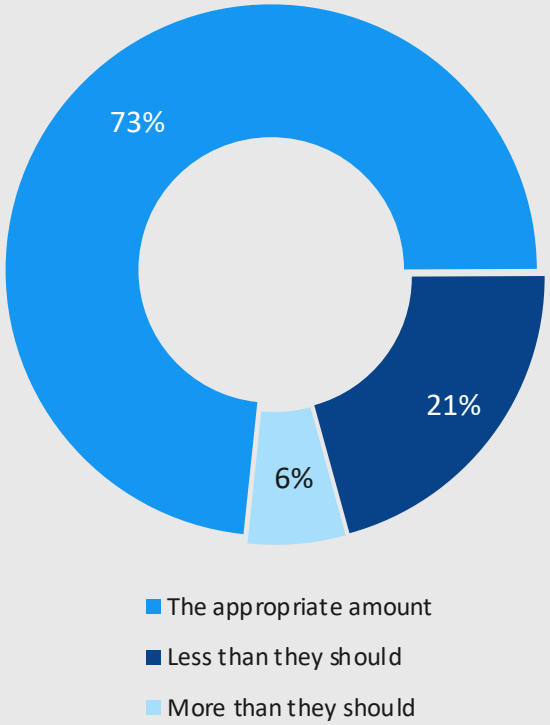
IT experts surveyed report that several strategies are commonly used for IT security staffing. 53% use an internal staff, half of which dedicate a team specifically for security. The other half lean on general IT staff. The use of a combination of in-house and external third-party experts is equally as popular as the two internal staffing options. Just one in ten exclusively use a third party.

53%

of respondents indicate that their security is managed solely by a team of internal employees.

A majority feel that their organization's leadership prioritizes IT the appropriate amount

"My organization's senior leadership prioritizes cybersecurity _____."



Percentage of all respondents, n=206
Note: Percentages may not add up to 100% due to rounding

Almost 3 in 4

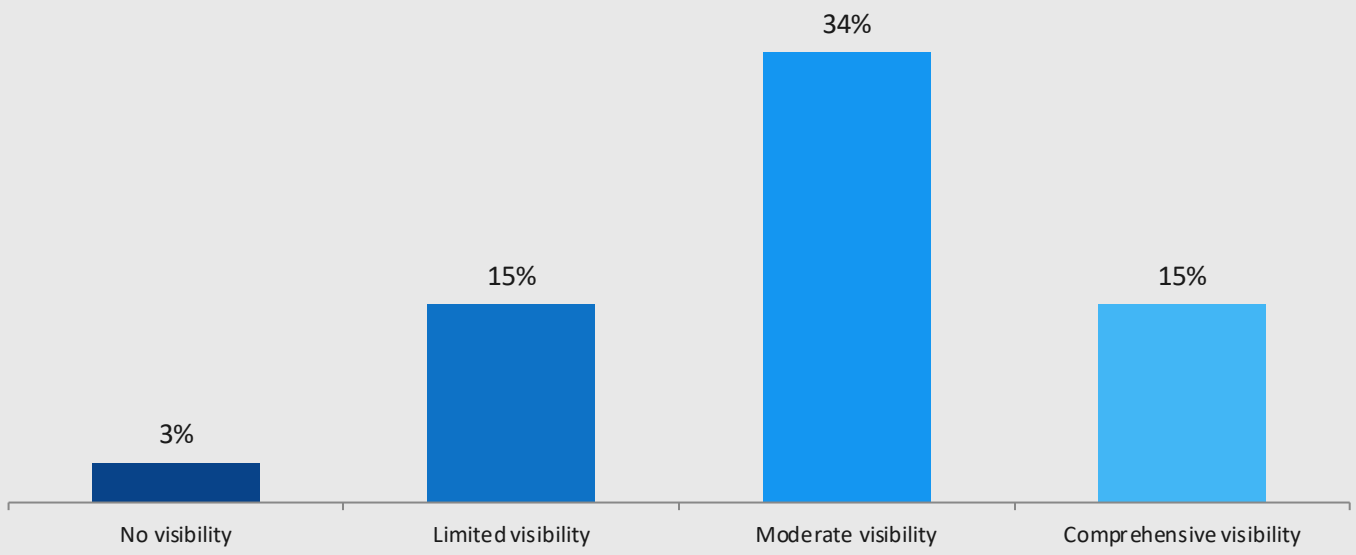
respondents feel that their organization's senior leadership prioritizes cybersecurity the appropriate amount.

21% of respondents say their leadership prioritizes cybersecurity less than they should.

6% of respondents say they prioritize cybersecurity more than they should.

Only 15% of employees say their organization has comprehensive visibility into its attack surface

What level of visibility do you believe your organization has into its attack surface?



Percentage of respondents, n= 198
Note: Percentages may not add up to 100% due to rounding
Not shown are 32% who selected "Don't Know"

An organization's attack surface refers to all the possible vulnerabilities across software, hardware, networks, and the people engaging these technologies.

While respondents possess higher awareness of their organization's IT procedures, 1 in 3 of those surveyed did not know what level of visibility their organization had into its attack surface. This may speak to the strength of internal security protocols or possibly a lack of clear communication with staff about cybersecurity capabilities.

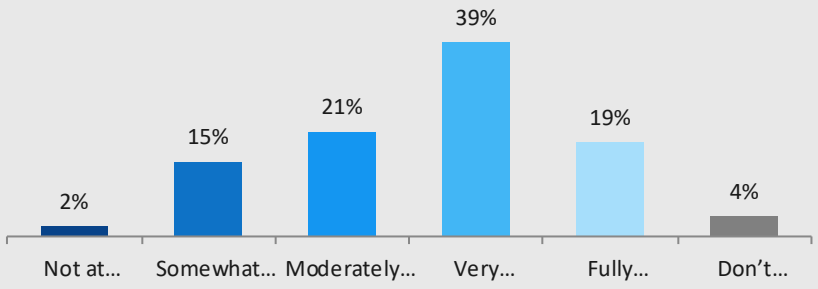
Of those who understood their organization's visibility, most felt they had moderate visibility, while 15% believe their organization has comprehensive visibility.

18%

feel that their organization has limited to no visibility into its attack surface.

Most say their organization recognizes its security vulnerabilities and considers them while making decisions

How aware do you think your organization is of its security vulnerabilities?



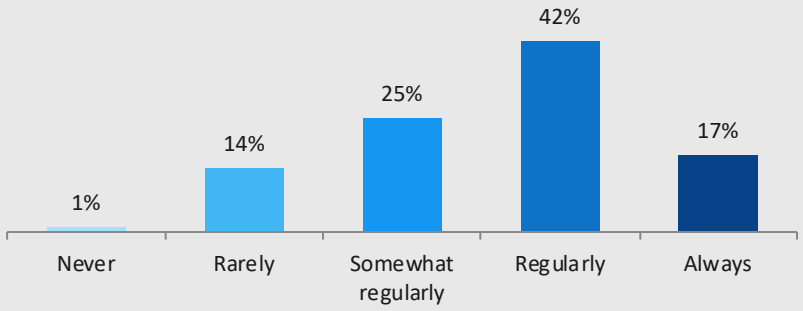
Percentage of respondents, n=198
Note: Percentages may not add up to 100% due to rounding

58%

of respondents believe that their organization is very aware or fully aware of its security vulnerabilities.

At the same time, 36% of respondents indicate that their organization is only moderately or somewhat aware of its vulnerabilities. And 2% of respondents say that their organization is not at all aware of vulnerabilities.

How frequently does your organization's leadership take these vulnerabilities into consideration when making decisions?



Percentage of respondents, n=197
Note: Percentages may not add up to 100% due to rounding

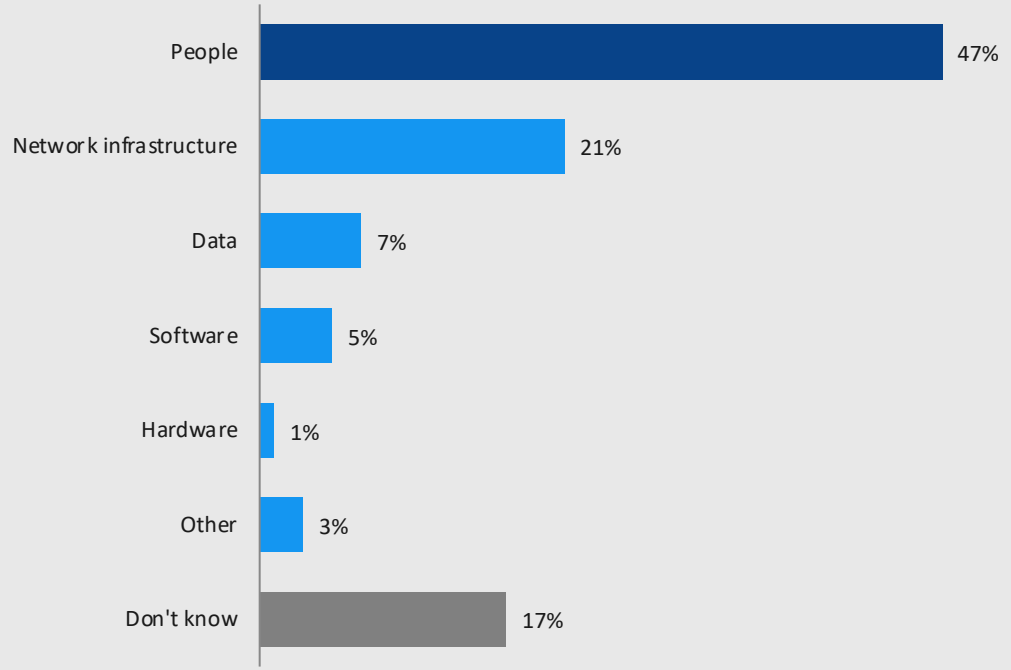
59%

of respondents say that vulnerabilities are regularly or always taken into consideration when making decisions.

Respondents say that *people* are their IT systems' greatest vulnerability

While the tangible aspects of an IT strategy such as infrastructure, hardware, and software are key, investing in cyber hygiene awareness through recruiting and training is just as important. Almost half of respondents considered human vulnerabilities to be the top IT security liability.

Which element of your organization's IT system do you think is the most vulnerable?



Percentage of respondents, n=196
Note: Percentages may not add up to 100% due to rounding

Network infrastructure follows *People* as the most vulnerable element of an IT system. Data, software, and hardware trail the list of greatest vulnerabilities, possibly because they have been major objectives of IT cybersecurity strategies in recent years. Investing in workforce training, expertise, and clear technology protocols for employees who may not be tech-savvy will be important to safeguard IT systems.

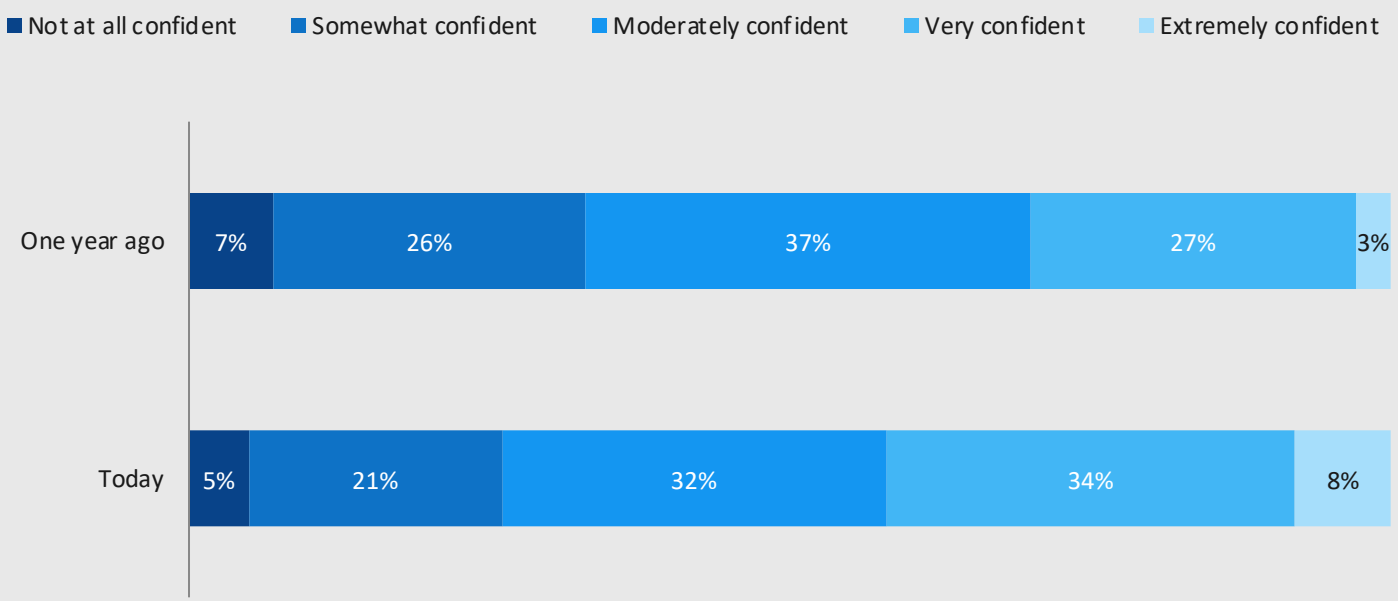
47%

of respondents cite people as their IT system's greatest vulnerability.

Confidence in organizational security capabilities has increased since 2019

Employees are increasingly more confident in their organization's ability to fend off cyber threats. The number of respondents who said they are moderately to extremely confident in their organization's security posture has increased from 67% to 74% in the past 12 months. However, 26% are still not at all or only somewhat confident in their organization.

Respondent Confidence in Cybersecurity Capability



Percentage of respondents, n=187
Note: Percentages may not add up to 100% due to rounding

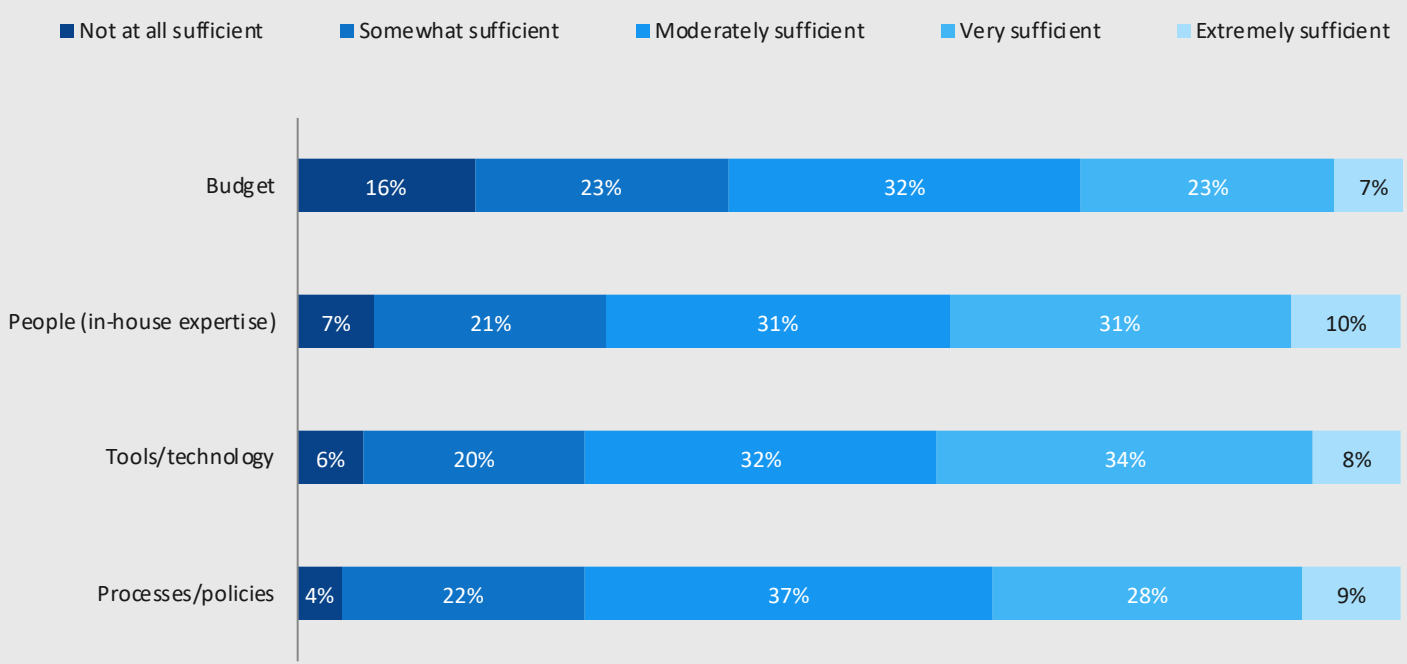
The number of employees who are extremely confident in their organization's security posture has increased by almost 3 times its former levels in the past year.

74%

of respondents are moderately to extremely confident in their organization's security posture.

Budget tops the list of insufficiencies, with 39% claiming their budget is not at all or only somewhat sufficient

How sufficient are each of the following at helping your agency minimize risk of infection or compromise?



Percentage of respondents, n=178
Note: Percentages may not add up to 100% due to rounding

Respondents indicated that budget insufficiencies are a common problem in helping their agencies minimize risk of infection or compromise. Almost 2 in 5 respondents say that their budget for cybersecurity is not at all or only somewhat sufficient. This finding underscores a recent report showing that most state budgets allot 0-3% of their IT budget for cybersecurity, compared to private industry which generally allots 10% of its IT resources for cyber.[3]

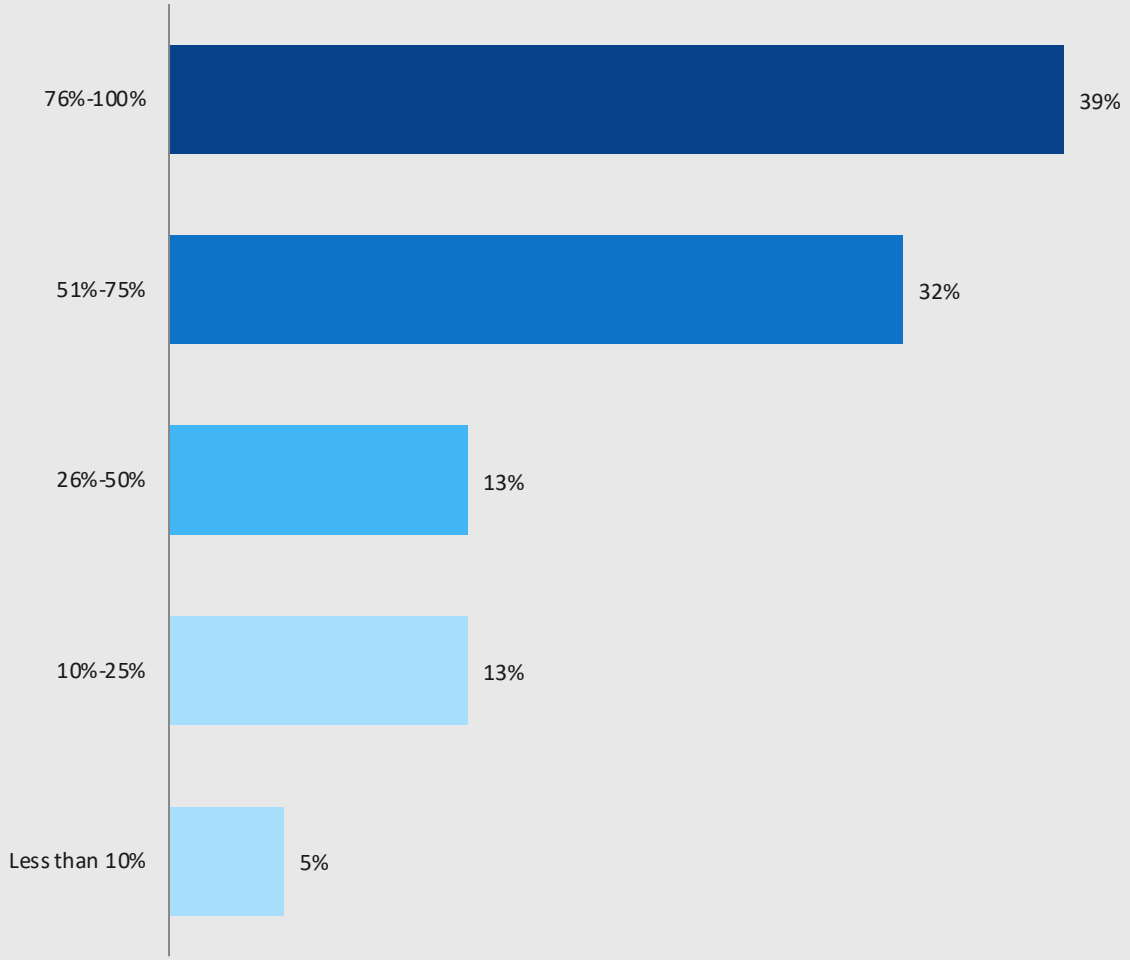
Only 30%

of respondents say their agency's budget is very or extremely sufficient for protecting their agency from cyberattacks.

3. NASCIO. "Ensure Dedicated Cybersecurity Funding for State and Local Governments with CIOs as Key Decisionmakers." https://www.nascio.org/wp-content/uploads/2020/01/NASCIO-Dedicated-Cyber-Funding-2020.pdf

39% believe their organization stops most attacks, while 31% say they miss more than half

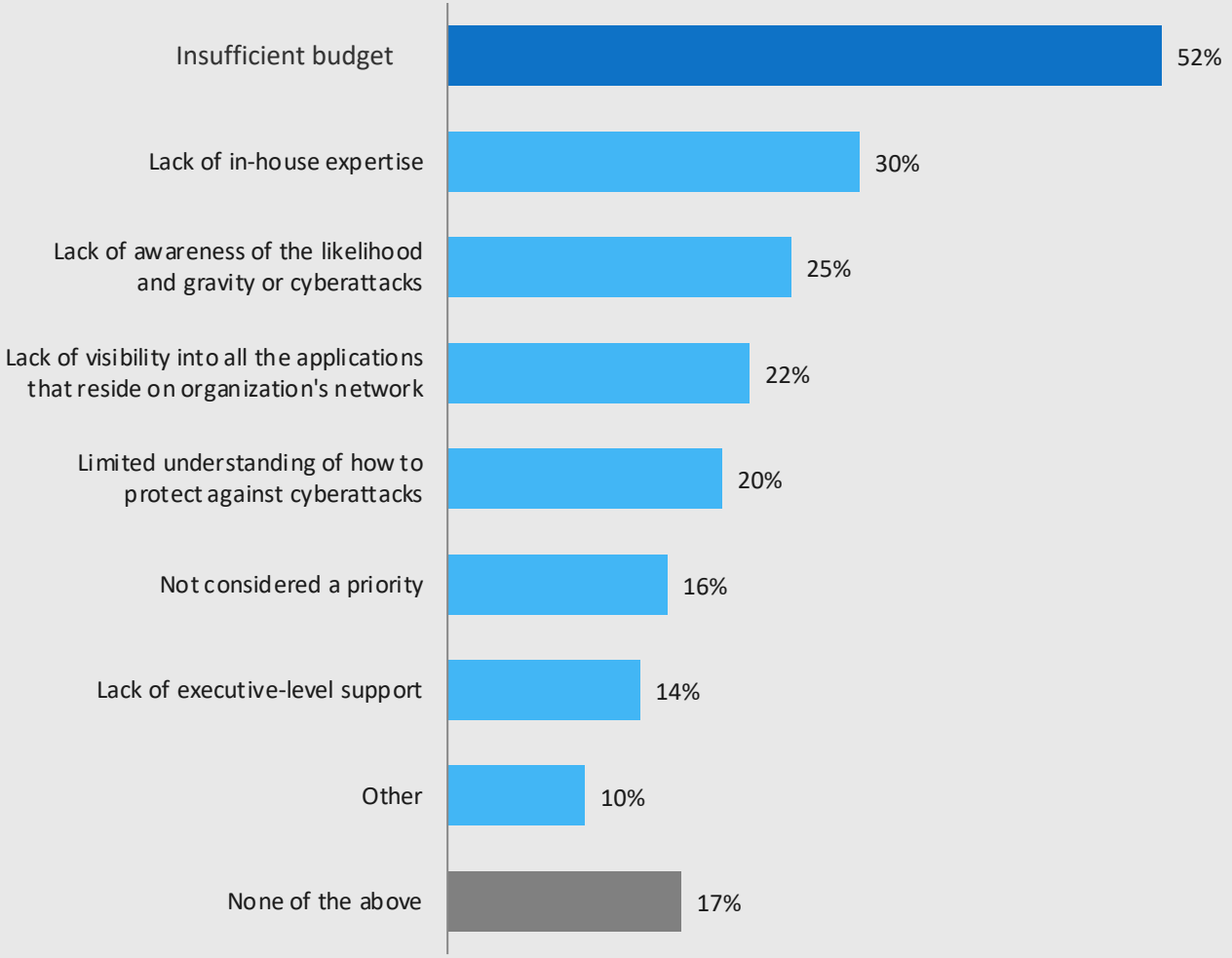
When thinking about your organization's current technologies, processes, and in-house expertise, what percentage of cyberattacks do you think your organization can realistically stop?



Percentage of respondents, n=176
Note: Percentages may not add up to 100% due to rounding

Budget insufficiencies and lack of in-house expertise are the greatest cybersecurity barriers

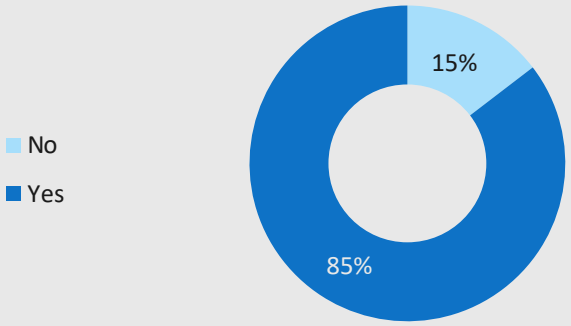
What are the prohibiting factors (if any) keeping your organization from improving its cybersecurity? Please select all that apply.



Percentage of respondents, n=174
Respondents were asked to select all that apply

Most say third parties provide some IT services, but they have little visibility into the operations of these providers

Does your organization rely on third parties or any kind of managed professional service or software maintenance?

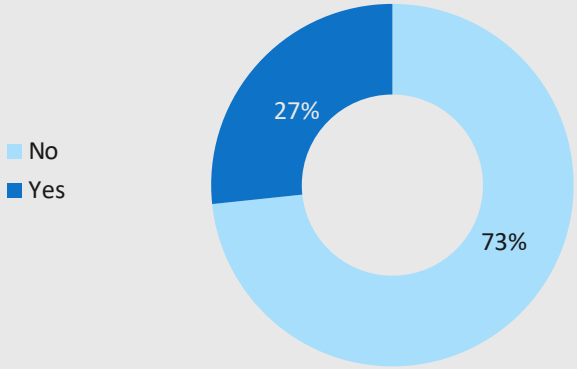


Percentage of all respondents, n=137
38 responded "Don't know"
Note: Percentages may not add up to 100% due to rounding

85%

of those who are informed on the matter report that their organization relies on third party providers.

Does your organization have real-time visibility into its managed service providers?



Percentage of respondents, n=73
41 responded "Don't know"
Note: Percentages may not add up to 100% due to rounding

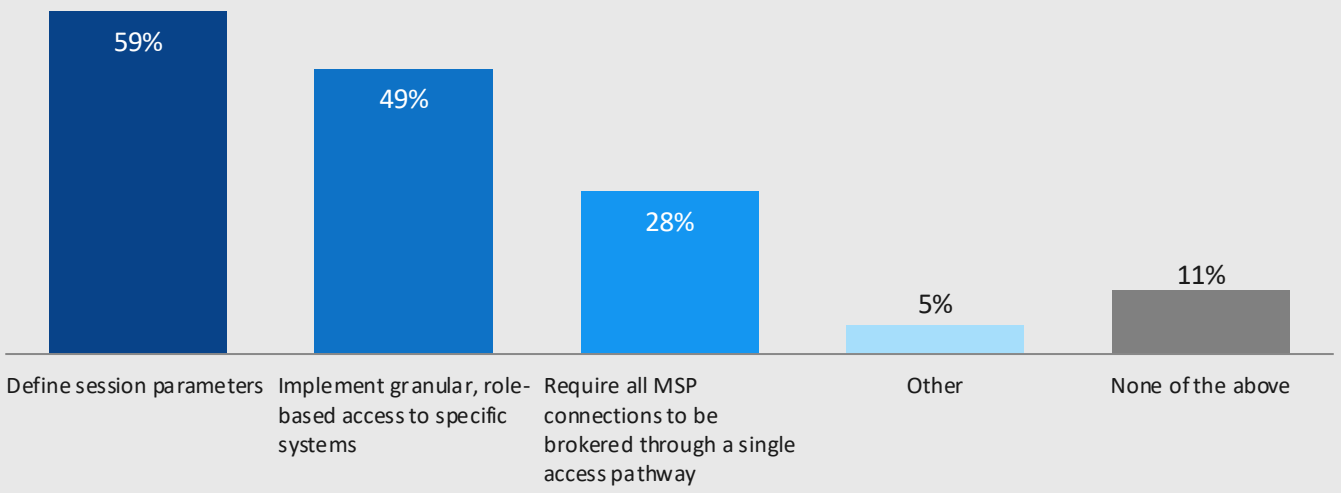
73%

have no real-time access into those MSPs. While 85% of employees report that their organization uses third party providers, almost three quarters of those respondents have very little visibility into the activities of those managed service providers.

Most respondents say their agencies define the session parameters of their MSPs

While several strategies are employed to give managed service providers some, but not *too* much access to systems, the most popular method is the definition of session parameters. These rules restrict who, when, and over what systems MSPs can give organizations visibility and control of their capabilities.

Which, if any, of the following practices does your organization implement to ensure the security of its MSPs?



Percentage of respondents, n=61
Respondents were asked to select all that apply

Defining session parameters allows vendors or internal users access to specific systems for an allotted time for a specific purpose. Role-based access is a different approach that restricts MSPs by only allowing certain authorized users to access a system. Just over a quarter of MSPs are required to use a single access pathway to operate systems in local and state governments.

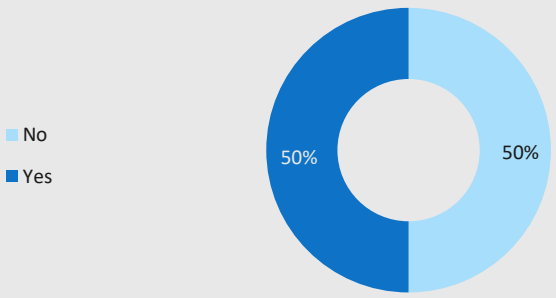
As 41% do not yet define session parameters, and over half do not implement role-based access systems, adopting these these protocols could greatly improve dynamic control over MSP access for many organizations.

59%

of respondents describe the most common MSP security practice as defining session parameters

Of those who experienced a recent compromise, almost half were tied to a third-party MSP

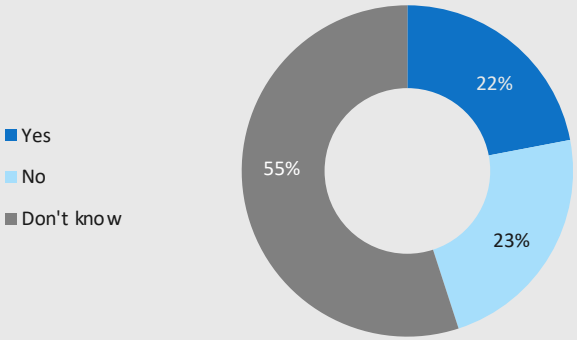
To the best of your knowledge, has your organization suspected or confirmed a compromise to any component in its network (i.e., data assets and/or infrastructure) in the last 12-18 months?



Percentage of all respondents, n=128
48 responded "Don't know"

50%
of all respondents report a compromise in the past year and a half.

Has your organization found evidence of a connection to a third party in relation to the compromise?



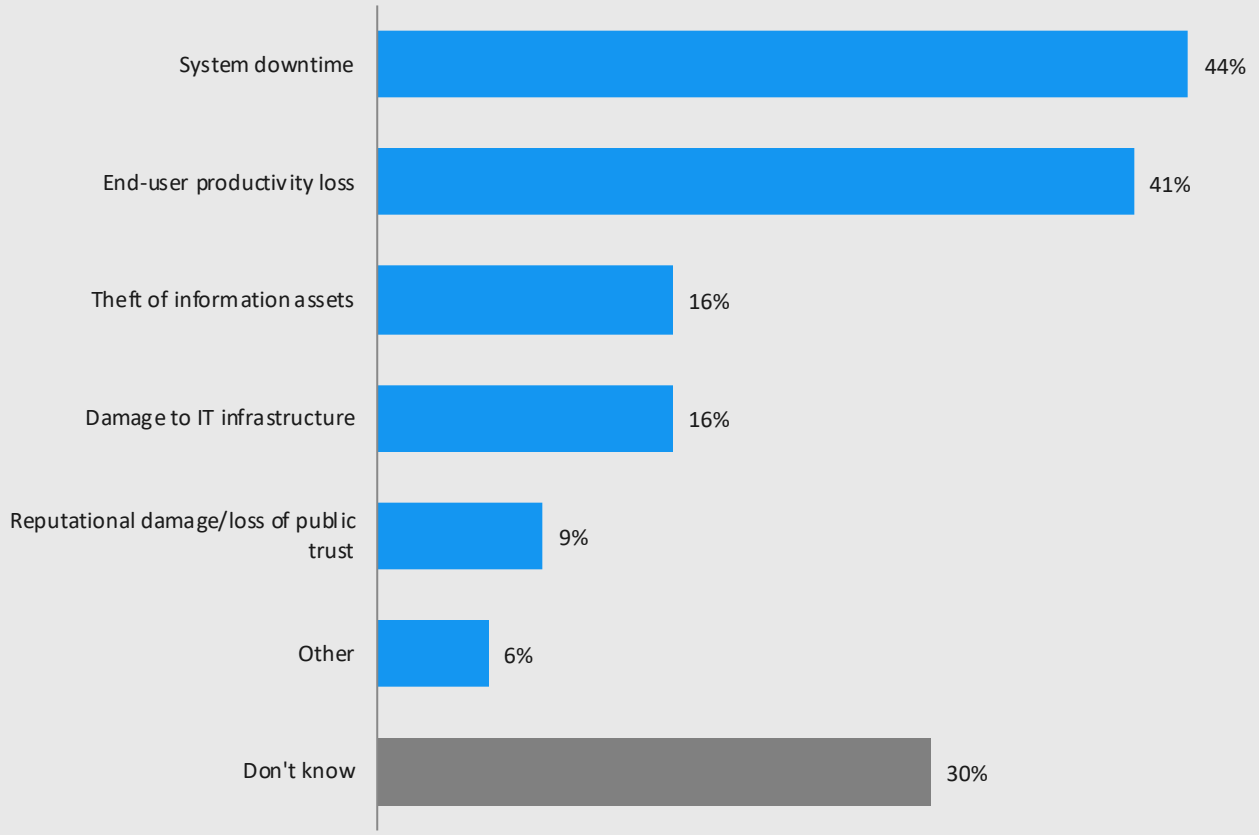
Percentage of respondents, n= 64
Note: Percentages may not add up to 100% due to rounding

GBC asked its respondents who responded that their organization had suspected or confirmed a compromise whether it was tied to a third-party vendor.

22%
of attacks were known to be related to third party providers.

Downtime and productivity loss were common consequences of cyberattacks

What were the consequences of the attack?



Percentage of respondents, n=64
Note: Percentages may not add up to 100% due to rounding

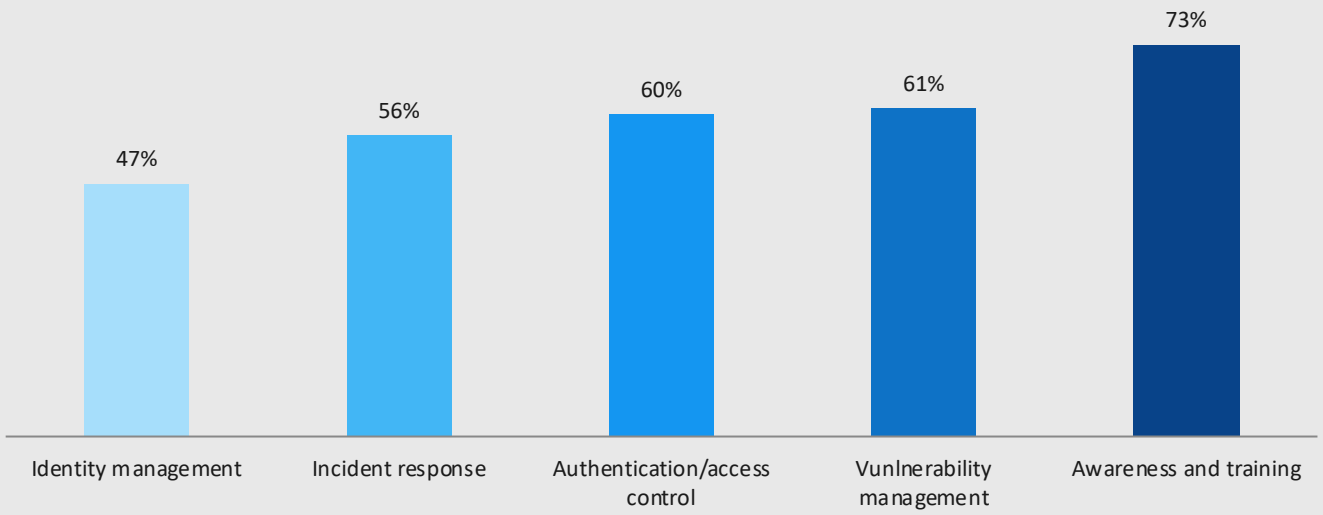
44%

of respondents say their organization experienced system downtime as a result of the attack. Additionally 41% experienced a productivity loss. 16% experienced theft of IT assets or suffered damage to IT infrastructure. 1 in 10 suffered reputational damage.

While the most common consequences were loss of time and productivity, about 1 in 6 saw tangible losses such as information theft and IT infrastructure damage.

After a cyberattack, employees report the most investment in increased awareness and training

Following an attack, which of the following initiatives has your organization prioritized more than they did before the attack?



Percentage of respondents, n= 62,
Note: Percentages may not add up to 100% due to rounding

Of respondents who indicated that their organization had suffered a security compromise, almost half say all security strategies listed were given more investment. Awareness and training outreach to employees increased according to 73% of respondents. Vulnerability management and authentication/access control received more time and resource post-cyberattack according to 3 out of 5 employees.

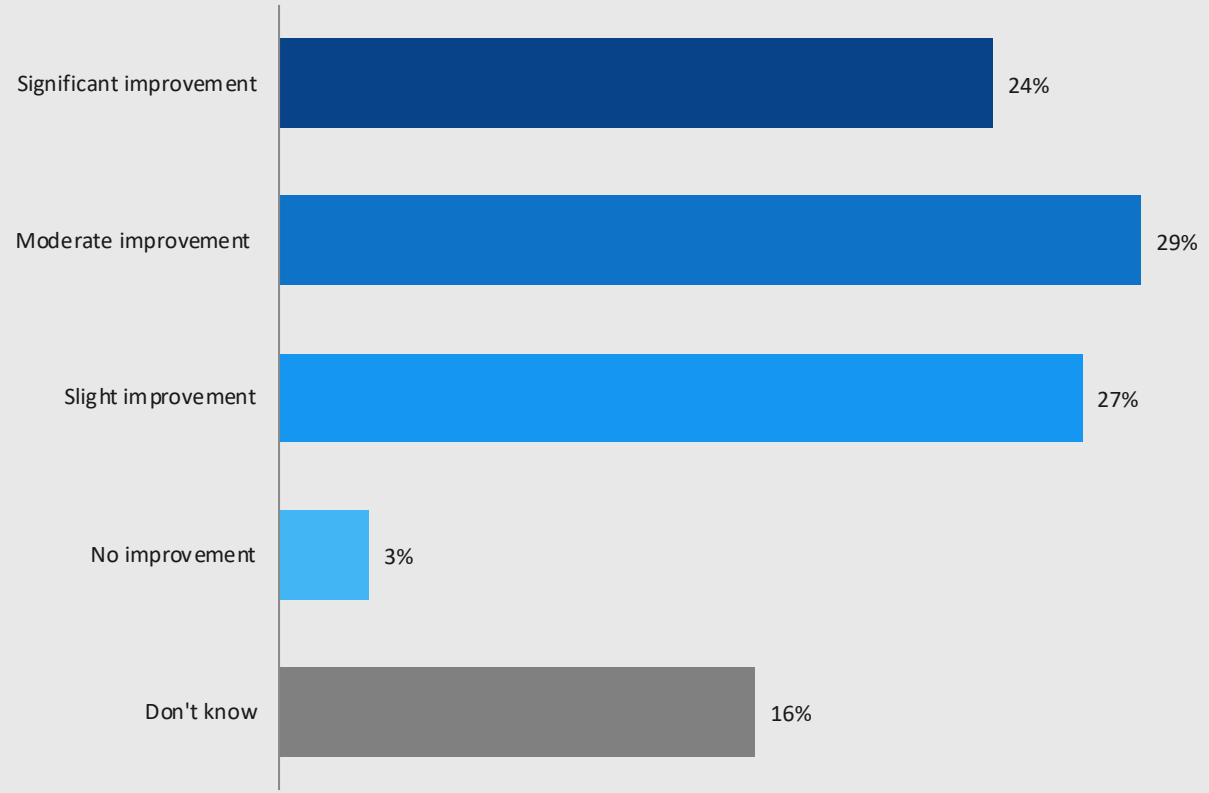
Only 56% of respondents say their organization invested more in incident response, less than training, vulnerability management, and authentication control. Lack of investment from 44% may prove to be dangerous, as incident response is important for security systems to learn and adapt over time.

Only 47%

of respondents say their organization invested more in identity management solutions after the attack.

Just over half cite moderate to significant improvement in their organization's cybersecurity detection capabilities after an attack

To what extent has your organization's ability to detect and respond to cyberattacks changed since the attack?



Percentage of respondents, n=62
Note: Percentages may not add up to 100% due to rounding

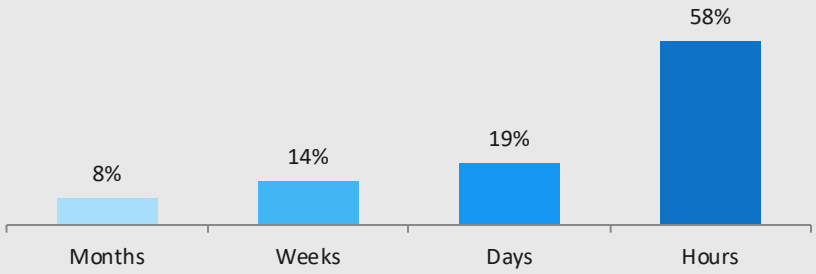
53%

of respondents say their organization's ability to respond to cyber attacks has significantly or moderately improved since the attack.

Although, 1 in 3 say there has been slight or no improvement.

While some organizations experienced loss, cyberattacks ultimately make their systems more resilient and improved the speed of incident detection.

Prior to the security incident, how long did it take your organization to detect an active attacker?

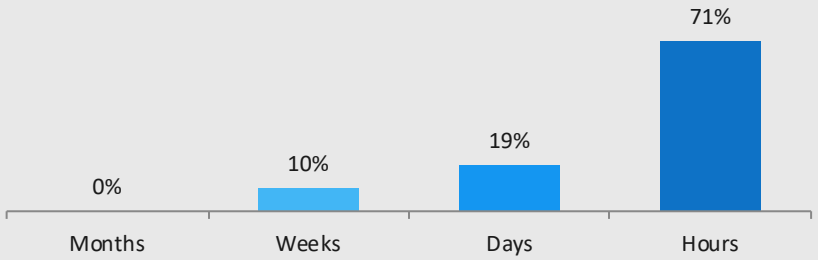


Percentage of respondents, n=36
23 responded "Don't Know"
Note: Percentages may not add up to 100% due to rounding

22%

of respondents say it took their organization weeks to month prior to their security incident to detect an active hacker.

Since discovering the security incident, how long does it take your organization to detect an active hacker?



Percentage of respondents, n=31
29 responded "Don't know"
Note: Percentages may not add up to 100% due to rounding

71%

of respondents now say it would take just hours to detect an active hacker post cyberattack, up from 58% before the security incident.

Still 10% say the incident would take weeks to discover.

Final Considerations

Protecting agencies from cyberattacks in the future will require:

Better comprehension of attack spaces

Respondents have signaled that investment in cybersecurity measures is increasing, and that their organizations have some level of visibility over their vulnerabilities. However, there is room for improvement. Solutions that give IT staff a comprehensive map of their data and abnormal events will provide leaders with a better view of their security landscape and vulnerabilities.

Dynamic control of access for Managed Service Providers

The ability to leverage expertise from MSPs is important. 60% report setting defined parameters around the sessions of MSPs, and 48% assign role-based system access rules, yet almost a fifth of reported security compromises were tied to MSPs. Organizations should seek to expand the use of defined parameters and other access controls. With less than a quarter citing significant improvement to their organization's cybersecurity capabilities since the attack, MSP access control is the imperative next step for many government security programs.

Insights from Elastic

Eliminate blind spots and get full visibility. Whether you're tracking MSP activity or monitoring your own networks, you need to be able to ingest, store, and search across large volumes of disparate data sources. Full visibility into network, threat hunting, analysis, and threat discovery provide a detailed landscape of your cyber environment, including vulnerable attack surfaces.

Look for a comprehensive security solution. It's not enough to only protect the perimeter; security must happen across the entire attack surface. Anti-malware, role- and attribute-based access controls, endpoint protection, SIEM capabilities, and machine learning-powered threat hunting are critical for effective threat prevention, detection, and response.

Arm every analyst to succeed. Empower practitioners with intuitive UIs that minimizes context switching. Look for visualizations rendering the origin, extent, and timeline of an attack. Utilize embedded case management and automated actions to accelerate response with. Quickly gather and analyze information to determine root cause and enable rapid action.

Start with open and deploy quickly. With free and open Elastic SIEM, you can quickly start building prototypes and test out solutions to meet your cybersecurity needs without having to rip and replace legacy systems. Visit elastic.co/security to learn more.

About

Government Business Council

Government Business Council (GBC), the research arm of Government Executive Media Group, is dedicated to advancing the business of government through analysis and insight. GBC partners with industry to share best practices with top government decision makers, understanding the deep value inherent in industry's experience engaging and supporting federal agencies.

Report Author: Molloy Sheehan

Contact

Daniel Thomas
Director, Research & Content Services
Government Executive Media Group

govexec.com/insights
@GovExecInsights

Elastic

Elastic is a search company. As the creators of the Elastic Stack (Elasticsearch, Kibana, Beats, and Logstash), Elastic builds self-managed and SaaS offerings that make data usable in real time and at scale for search, logging, security, and analytics use cases. Learn more at elastic.co