Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **September 2024**
Sponsored by **Abnormal Security**

Safeguarding Identity Security: We Need to Talk about MFA

Executive summary

Data breaches and ransomware attacks make headlines every day in the mainstream news. These articles routinely comment on the need for multi-factor authentication (MFA), especially if it wasn't used. This emphasis can give the impression of MFA as a silver bullet, and that using it can easily prevent breaches. However, the reality is more complex. It is more accurate to say that while the presence of MFA reduces the likelihood of a breach, not all MFA is created equal, and the risk of data breaches continues to rise even as organizations implement MFA.

Despite these challenges, we strongly advise organizations to continue using MFA. Instead of abandoning it, organizations should focus on improving and strengthening how MFA is implemented—including the types of MFA being used. This should be part of a broader effort to reinforce security measures throughout the entire authentication process, ensuring that every step is as secure as possible given the risks involved.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Identity threats are bad and getting worse**
  79% of the organizations we surveyed for this research have been compromised by one or more types of identity attacks in the past 12 months, and 86% say that cybercriminals are increasingly interested in stealing and abusing compromised credentials. Less than 5% of organizations currently have full MFA coverage across all employees and apps.
- **Most organizations cannot stop an identity attack in real time**
  Most can stop an attack once it has been detected, but not before a threat actor compromises their digital estate and puts them at risk of data theft, the implementation of ransomware, and other forms of loss. Many organizations lack the alerting, monitoring, and detection optics needed. This means that protecting against account takeover in the first place is more important than ever.
- **Many good reasons for using and strengthening MFA processes**
  90% of organizations identify six or more reasons as being highly important for using MFA, led by reducing the likelihood of account takeover. 61% of organizations are transitioning to phishing-resistant, next-generation MFA methods over the next two years including hardware tokens and biometrics.
- **Elevating identity security through new innovations is essential**
  Improving identity security and strengthening MFA processes is a must-do strategy for all organizations. New innovations available in the market include anomaly detection on identity usage, new form factors for MFA hardware devices, and dark web monitoring to detect compromised credentials for proactive remediation.
- **Best practices for identity security include upgrading MFA methods, monitoring for risk and threat patterns, and training users**
  Upgrade to next-generation MFA devices that are phishing-resistant, monitor for attacks across identities, and strengthen MFA protections by training users to detect new and emerging types of MFA bypass and compromise attacks.

Focus on improving and strengthening how MFA is implemented—including the types of MFA being used.

ABOUT THIS WHITE PAPER

This white paper is sponsored by Abnormal Security. Information about Abnormal Security is provided at the end of this paper.

Identity security is under attack

Identities are under relentless attack. Organizations experience these attacks directly and face a range of challenges in addressing them. In this section, we review the evidence.

IDENTITY THREATS ARE ALREADY BAD—AND GETTING WORSE

Most organizations in this research have been compromised by one or more types of identity attacks in the past 12 months (79%)—such as a phishing attack that resulted in credential compromise when the user was—or wasn't—protected by MFA, or the theft and use of an authentication session token. It is not surprising that most have been compromised since:

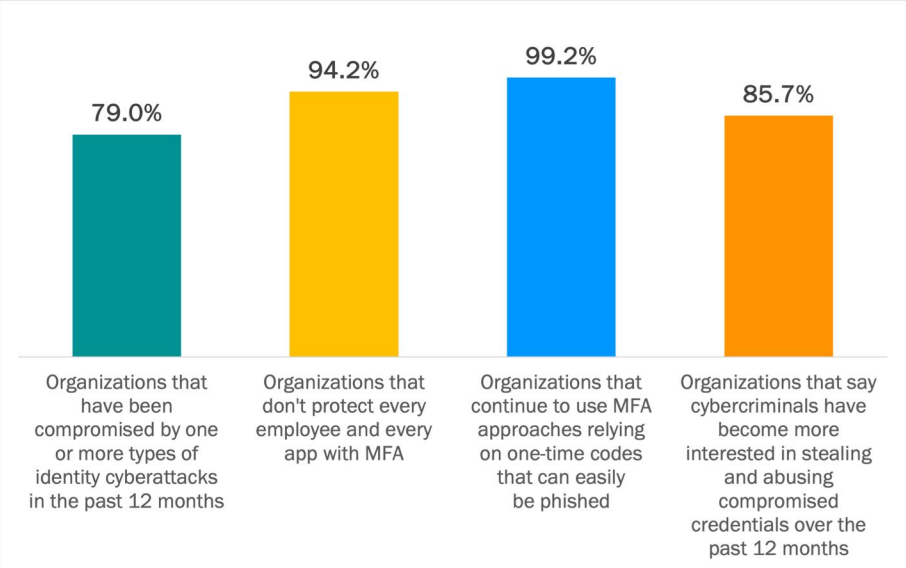
- Almost all organizations don't protect every employee and every app with MFA (94.2%), which immediately opens exposure pathways for threat actors to infiltrate; and
- Almost all organizations continue to have some degree of reliance on weaker forms of MFA, specifically those that use one-time codes (99.2%). Not all forms of MFA are created equal, and those that are easier to bypass through MFA attacks are essentially useless and don't deliver the desired value.

This current state of identity wouldn't be such an issue if threat actors were designing non-identity-based attacks to compromise organizations, but organizations are seeing greater interest from cybercriminals in stealing and abusing compromised credentials by their own admission (85.7%) and their direct experience of account takeover, credential phishing, and other types of identity attacks.

See Figure 1.

It is not surprising that most organizations have been compromised by identity attacks since hardly any protect every employee and every app with MFA.

Figure 1
Statistics on identity cyberattacks, countermeasures, and what's still to come
Percentage of respondents



Source: Osterman Research (2024)

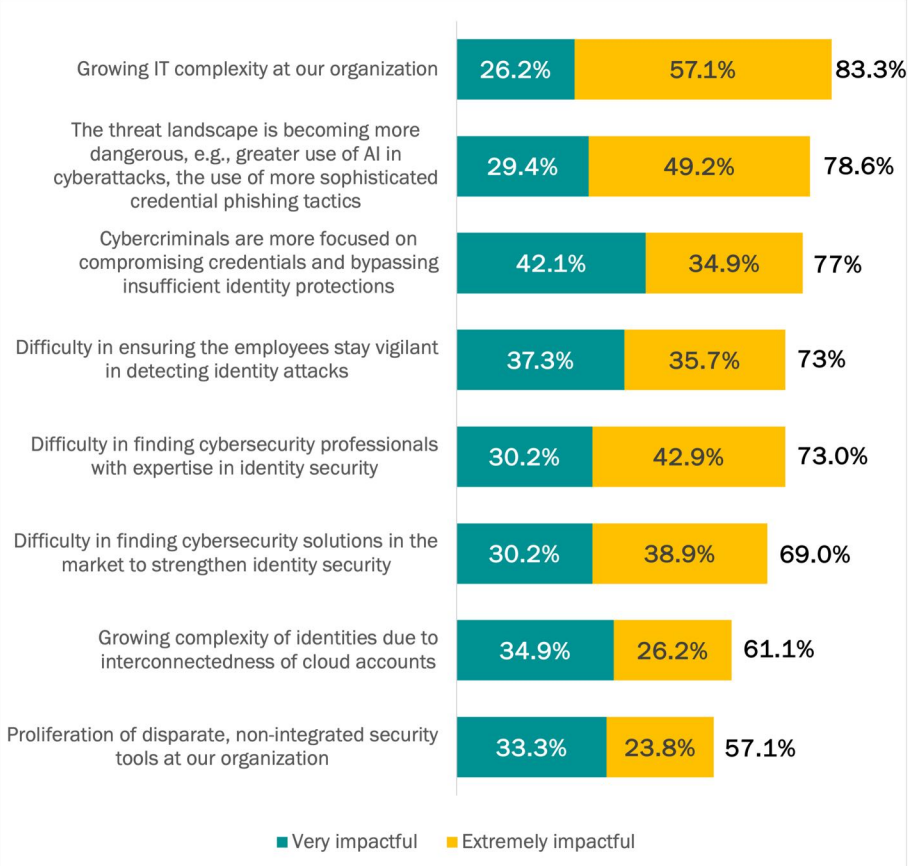
KEY INTERNAL AND EXTERNAL FACTORS MAKE IDENTITY SECURITY MORE DIFFICULT

A mixture of internal and external factors makes identity security more difficult for organizations. Growing IT complexity leads the pack with 83.3% of respondents saying this is "very impactful" or "extremely impactful" to their identity security posture. Additional highly ranked internal factors are employee risks (73%) and difficulty in finding cybersecurity professionals with expertise in identity security (73%). These are tied for fourth place. As well as leading overall, the IT complexity factor has the highest standalone rating of "extremely impactful" out of all the factors we researched (57.1%).

Two external factors rank highly in the top five. A more dangerous threat landscape ranks in second place (78.6%) with cybercriminals more focused on compromising credentials closely following in third (77%).

In summary, organizations face greater IT complexity inside, a more dangerous threat landscape outside, and are uncertain as to how well employees can detect identity threats while not having enough cybersecurity professionals to safeguard identity security. See Figure 2.

Figure 2
Factors making identity security more difficult
Percentage of respondents



Source: Osterman Research (2024)

Organizations face greater IT complexity inside and a more dangerous threat landscape outside.

ORGANIZATIONS KNOW IDENTITY THREATS ARE CHANGING DUE TO DIRECT EXPERIENCE AND CONTEXTUAL DATA

Direct experience with increasing numbers of account takeover attempts and credential phishing attacks is the most frequently cited type of evidence that the cyberthreat environment with identities is changing. Reading about changing cyberthreats with identities is another form of evidence, and while several sources of such data are ranked highly in this research (i.e., cybersecurity industry news and industry reports from cybersecurity vendors), both sources are less commonly cited than direct experience.

In looking at the data, 70% of respondents said they have three or four sources of evidence for the changing cyberthreat environment.

See Figure 3.

Figure 3
How organizations know identity threats are changing
Percentage of respondents with direct experience (the teal bars) and contextual data from reading about changing cyberthreats (the yellow bars)

Source: Osterman Research (2024)

It is more common for organizations to have direct experience with changing identity threats than simply reading about it.

WE'RE NOT THE ONLY ONES SAYING THIS

Other industry research echoes our concerns about identity attacks. For example:

- **Cybercriminals "logging in" versus hacking in**
  IBM's X-Force analysis of cyberattacks in 2023 concluded that cybercriminals were forgoing hacking activities in favor of just "logging in" to a corporate network through valid accounts. These accounts have been compromised in third-party data breaches and are commonly leaked on the dark web. This abuse of valid accounts tied for first place with phishing as the most frequently used initial access vector of attack (both at 30%). This is a substantial change from the year before when phishing was the initial access vector in 41% of attacks and the abuse of valid accounts in only 16%.[1]

- **Email addresses and passwords included in most data breaches**
  Constella Intelligence identified over 151,000 breaches during 2023, containing 39 billion records with personally identifiable information on the deep and dark web.[2] Email addresses were included in 96% of data breaches and leakages, and passwords in 88%. Passwords were most commonly available in plain text or were encrypted with weak encryption algorithms. In other words, the data is out there. Unless organizations have compensating controls for breached credentials—such as strong MFA—cybercriminals have ample opportunities to just log in.

- **Authentication mechanisms can be bypassed due to vulnerabilities**
  Threat actors have proven their ability to leverage vulnerabilities on unpatched servers to bypass authentication mechanisms, craft malicious requests, and gain administrator-level privileges on affected systems for initiating whatever commands they want.[3]

- **Credential phishing increased by 217% in six months**
  During a six-month period from 3Q 2023 to 1Q 2024, credential phishing attacks increased by 217%.[4] Cybercriminals want to get their hands on credentials, as they provide access to email accounts, document repositories, and many other data sources, especially among organizations using Microsoft 365 and Google Workspace. Unless accounts have strong protections, increased attack incidence rates are likely to result in increased breaches.

- **Misuse of valid accounts frequently seen in successful infiltrations**
  Based on its vulnerability assessments, the United States Cybersecurity & Infrastructure Security Agency (CISA) found that the misuse of valid accounts was a commonly occurring phenomenon across multiple stages of cyberattacks, including initial access (54.3%), persistence (56.1%), and privilege escalation (42.9%).[5]

- **Tailored tactics successfully bypass MFA in one out of four attacks**
  Microsoft's analysis of digital defenses in 2023 found that highly sophisticated, deliberate campaigns focused on a specific organization or individual will penetrate MFA defenses in one out of four attacks.[6] Such campaigns generally use tailored tactics and involve extended efforts to infiltrate systems, with the aim of stealing data, obtaining privileged access, or deploying malware.

- **Two-step verification only 50% effective**
  Google analyzed account compromise attacks after auto-enrolling over 150 million users in two-step verification for their Google account. Across all two-step methods in use (the mix of which was not disclosed), targeted accounts were still compromised in 50% of situations.[7] To decrease this further, Google advocated for the adoption of hardware security keys, which based on its own internal deployment, were impervious to phishing attacks.[8]

Cybercriminals are forgoing hacking activities in favor of just "logging in" to a corporate network through compromised accounts.

Organizations struggle to detect and mitigate the use of invalid credentials

The ability to successfully differentiate between valid use of valid identities and malicious use of valid identities is a key test of the efficacy of identity security protections. Many organizations are ill-prepared.

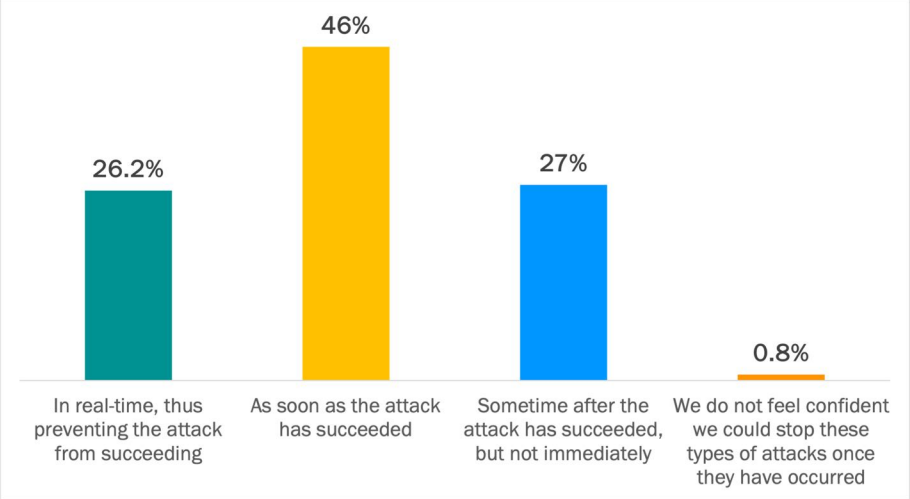
THREE OUT OF FOUR ORGANIZATIONS CANNOT STOP AN IDENTITY ATTACK IN REAL-TIME

Most organizations lack the controls to detect and stop an identity attack in real-time. Of this cohort of organizations, almost all say they can detect and stop the attack as soon as it has succeeded (46%) or sometime after it has succeeded (27%). In the absence of being able to prevent the attack from succeeding altogether, the ability to detect it as soon as it has succeeded is the best of the bad options. Limiting the dwell time of the incursion ideally minimizes the extent of data theft, data corruption (e.g., ransomware), and other forms of digital, reputational, and financial loss.

The final segment of this cohort, albeit a very small one thankfully (0.8%), do not feel confident that they could stop such attacks once they are in flight. This is the worst case of the four options, and any organization in this segment needs to act urgently to acquire the necessary capabilities.

See Figure 4.

Figure 4
Time scale for detecting and stopping identity attacks
Percentage of respondents



Source: Osterman Research (2024)

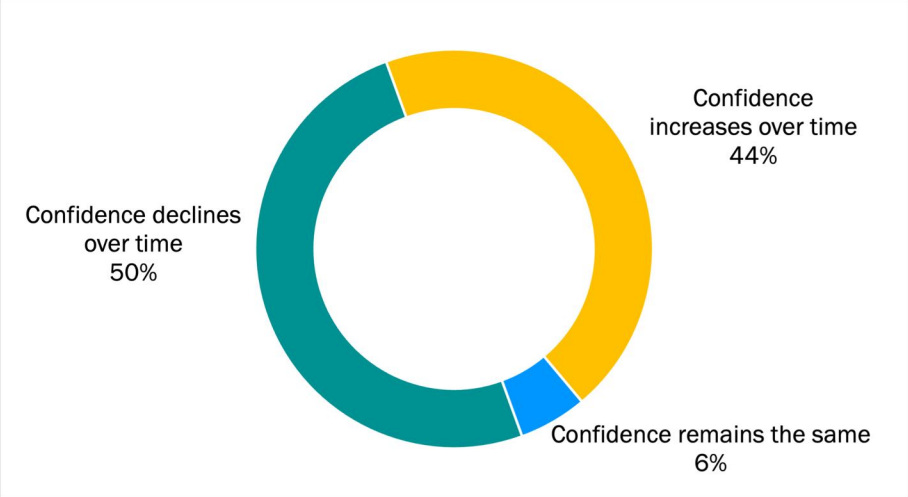
Only organizations that can detect and stop an identity attack in real-time can avoid data theft, data corruption, and other forms of loss that flow from this type of attack.

Only organizations that can detect and stop an identity attack in real-time can avoid data theft, data corruption, and other forms of loss.

CONFIDENCE TO DETECT AND STOP IDENTITY ATTACKS IS DROPPING

Half of organizations have a declining level of confidence in the ability of their systems and processes to protect against identity threats, for example, the ability to detect and stop a threat actor from using valid but compromised credentials for malicious purposes. For some of these organizations, confidence declines year on year across the three time periods we asked about (two years ago, currently, and the expected level of confidence in two years if no changes were made to current systems and processes). For others, confidence was high two years ago but dropped for the current time period or is expected to drop in two years' time. See Figure 5.

Figure 5
Confidence to protect against identity threats
Percentage of respondents



Source: Osterman Research (2024)

The other half of organizations say that their confidence is increasing over time or remaining stable. It is unclear where this greater hope for the future comes from, as the profile of both groups of organizations is very similar in the data. For example, there is only a slight difference in the number of identity attacks across both groups. The average number of types of identity attacks suffered at organizations over the past 12 months with declining confidence is 2.75. At organizations with increasing confidence, it is almost the same at 2.73.

Nonetheless, for all organizations, the changing threat dynamics around identity security mean that organizations need a higher level of assurance for all identity claims.

Confidence in the ability to protect against identity threats is dropping at many organizations.

LESS THAN HALF OF ORGANIZATIONS HAVE THE SYSTEMS TO STOP—OR EVEN DETECT—CYBERATTACKS THAT INCLUDE MFA COMPROMISE

Bypassing of MFA security controls has become a common occurrence across a raft of cyberattack types. Many phishing toolkits include MFA bypass features that nullify the MFA security controls an organization has put in place. For example, a phishing attack that points victims to an impersonated website will request credentials, submit these immediately in the background to the real site, and then ask for the MFA token or wait for that to be approved by the user on their device of choice. This immediate submission of stolen credentials to the real site gives the cybercriminal surreptitious access even though MFA protections were in place.

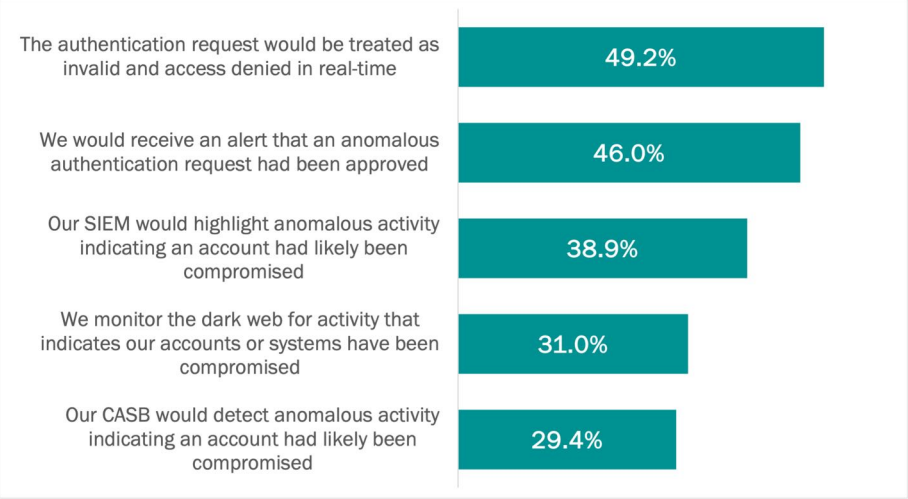
Not all types of MFA suffer from bypass, bombing, or other MFA compromise attacks, but many of the most commonly used approaches do. At particular risk are older legacy approaches that are no longer best practice, such as one-time codes delivered by SMS, email, and even authenticator apps. Newer and more modern MFA approaches—such as those relying on the FIDO (Fast IDentity Online) approaches which use public key cryptography for phishing-resistant authentication—are not susceptible to the types of bypass attacks that undermine older legacy approaches.

In this research, only one half of organizations (49.2%) said they can detect and stop a malicious authentication request in real-time that includes MFA compromise. Less than half have the alerting, monitoring, and detection optics in place across a range of common security systems to know about the anomalous authentication request or that an account has likely been compromised. For example, only 38.9% said their SIEM would highlight the activity, and 29.4% said the same for their CASB. Most organizations are flying blind. This means that protecting against account takeover attempts in the first place through stronger forms of MFA is more important than ever.

See Figure 6.

Many of the most commonly used types of MFA suffer from bypass, bombing, and other MFA compromise attacks.

Figure 6
How an MFA compromise would be detected
Percentage of respondents

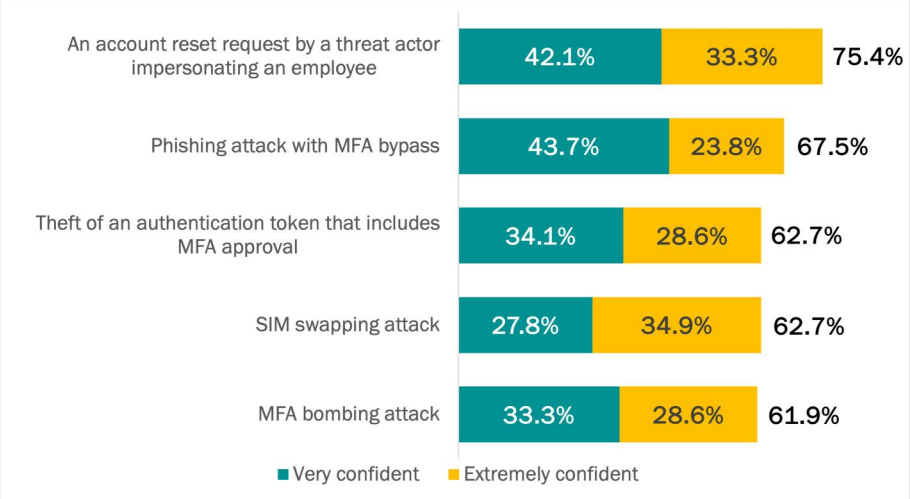


Source: Osterman Research (2024)

FEW ORGANIZATIONS HAVE THE HIGHEST CONFIDENCE IN THEIR ABILITY TO STOP MFA AND IDENTITY ATTACKS

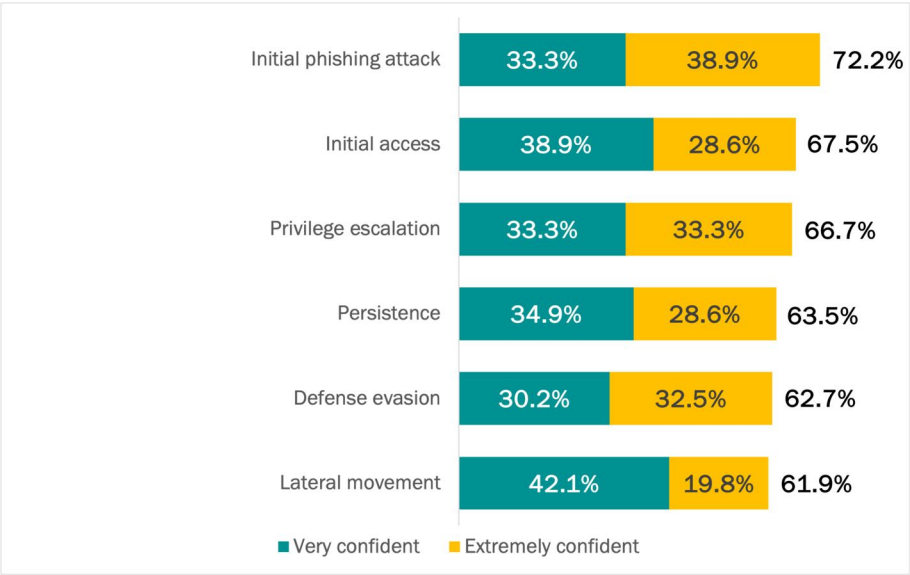
On average, only 30% of organizations have the highest confidence that they currently have the processes and technology to detect and avoid various types of MFA attacks (see Figure 7) and the highest confidence that they can stop identity attacks across different stages of a cyberattack (see Figure 8). For attack types, confidence is lowest for a phishing attack with MFA bypass (23.8%), and for stages, confidence is lowest for stopping lateral movement (19.8%).

Figure 7
Confidence to detect and avoid various types of MFA attacks
Percentage of respondents



Source: Osterman Research (2024)

Figure 8
Confidence to stop identity attacks at various stages of an attack
Percentage of respondents



Source: Osterman Research (2024)

Too few organizations are highly confident in their ability to detect and avoid various types of MFA attacks.

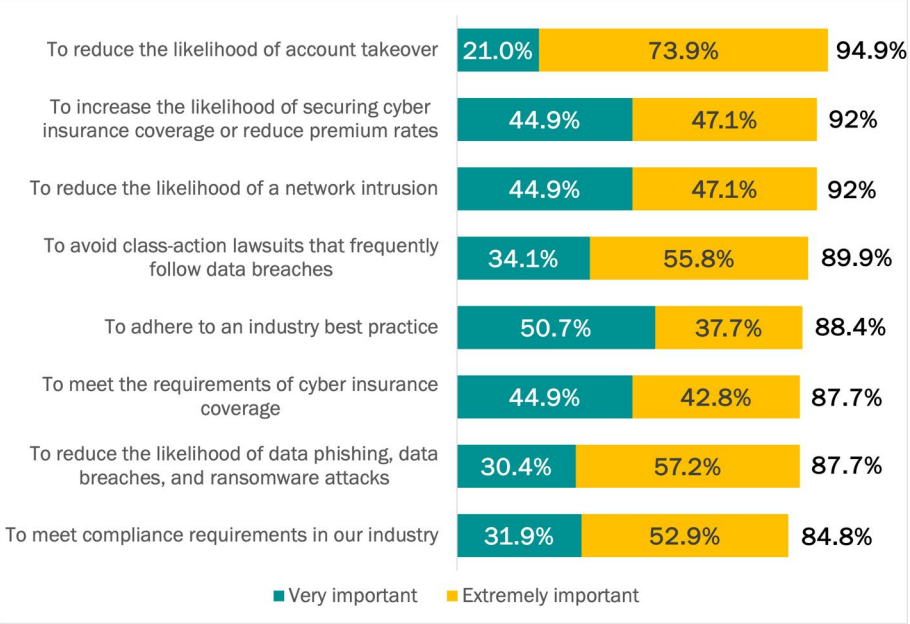
Organizations have good reasons for using and strengthening MFA protections

Strengthening MFA protections is highly important for multiple reasons, and many organizations are moving in the direction of modern methods in the next two years.

MFA IS TIED TO MULTIPLE SECURITY AND BUSINESS DRIVERS

90% of organizations rank six or more reasons as being highly important for using MFA. In first place is reducing the likelihood of account takeover. Increasing the likelihood of securing cyber insurance coverage requirements and reducing network intrusion are tied for second. The data in this research says that all eight reasons we asked about are ranked closely on the importance scale, with only a 10% variation between the highest and lowest ranked reason. For years, Osterman Research has repeatedly said that MFA is a critically important security control, and this criticality is being recognized by organizations. See Figure 9.

Figure 9
Reasons for using MFA
Percentage of respondents



Source: Osterman Research (2024)

Relying on anything but the strongest MFA methods is a recipe for disaster.

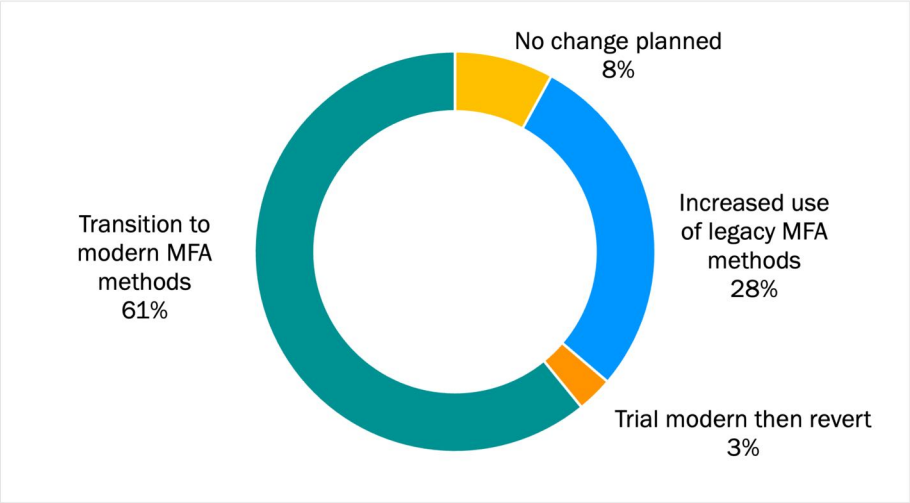
Given the criticality of MFA across multiple security and business drivers, relying on anything but the strongest MFA methods is a recipe for disaster. Organizations need to move with the times—stopping the use of legacy and weak forms of MFA and embracing stronger and more modern next-generation approaches. Account takeover attacks are easily designed with phishing toolkits that include MFA bypass capabilities to ensnare victims not using phishing-resistant next-generation MFA methods. Claiming to use modern MFA approaches on a cyber insurance application when such controls are not in place can lead to the coverage being rescinded as void from inception,[9] as well as suffering from a network intrusion, facing a class-action lawsuit (an increasingly common outcome), and suffering a data breach.

ORGANIZATIONS ARE MOVING TOWARD MODERN MFA METHODS

We compared MFA methods in use two years ago, currently, and the expectation for two years out. Three out of five organizations are transitioning to modern next-generation MFA methods, such as hardware tokens and biometrics. This transition is taking place over multiple years as organizations leave legacy and weak approaches behind. Various sub-patterns are evident within the overall pattern of transitioning to modern MFA methods, such as stepwise increased usage over the three time periods, and a dip in the middle time frame as organizations experiment with new approaches.

See Figure 10.

Figure 10
Transitions in MFA methods in use
Percentage of respondents



Source: Osterman Research (2024)

The second most common pattern is increased use of legacy MFA methods (28%), which is worrisome given the frequency with which these approaches are bypassed with easy-to-obtain phishing and account compromise toolkits. However, directionally appropriate change is still afoot among this group of organizations for the time horizon we enquired about. Fewer are relying on one-time codes delivered by SMS (32% lower usage) and email (41% lower usage). The use of authenticator apps as a way of distributing one-time codes is increasing (48% higher usage). If we do this research again in another two years, ideally even more organizations will be transitioning away from legacy forms of MFA.

Among organizations planning no change in methods (8%) at the level of legacy versus modern, some are still changing within these groupings. For example, some are making higher use of one-time codes by authenticator apps rather than SMS or email. Others are experimenting with newer types of modern MFA to see what best fits their use cases, employees, and workflows. Of this group, however, most make higher use of legacy methods than modern ones, which as above, is dangerous for safeguarding identity.

Three out of five organizations are transitioning to modern next-generation MFA methods over the next two years.

New innovations in identity security

Vendors are actively engaged in looking for new and better ways to enhance identity security for organizations. There is still significant space for new innovations that streamline and strengthen identity security. We look at the most important innovations in this section.

ANOMALY DETECTION ON IDENTITY USAGE

An employee using their identity credentials in the course of their job will evidence certain patterns over time, such as where they log in from, when they do so, what tasks they perform while logged in, and which devices they rely on. Capturing these and other underlying identity signals allows a pattern of normal activity to be created for each individual. Some deviations from normal patterns of activity will be explainable through benign circumstances, such as when an employee is traveling for business or is on vacation. Other deviations will signal malicious activity that needs to be addressed immediately, ideally through autonomous intervention to restrict the access rights of the identity entirely or enforce additional authentication challenges while an investigation is carried out.

The pattern for each individual can also be compared to the patterns of others across the organization, especially those performing a similar set of work tasks. Deviations from the comparative group can signal anomalies that may indicate insider risk from the employee or that an identity has been surreptitiously compromised and is being used for malicious purposes.

Anomaly detection on identity usage will signal malicious activity that needs to be addressed immediately, ideally through autonomous intervention.

NEW FORM FACTORS FOR MFA HARDWARE DEVICES

Over 95% of respondents in this research believe that next-generation MFA solutions will significantly improve the ability of their organization to stop identity threats. In other words, there is almost universal support for exploring new and stronger methods that address the weaknesses of earlier MFA approaches.

The strongest approach for MFA that is currently available in market is a hardware device that ties to an individual via a biometric sensor. These are most frequently deployed as a hardware key to be connected to a keyring and carried in a pocket or purse. Nonetheless, hardware keys run the risk of theft and misplacement.

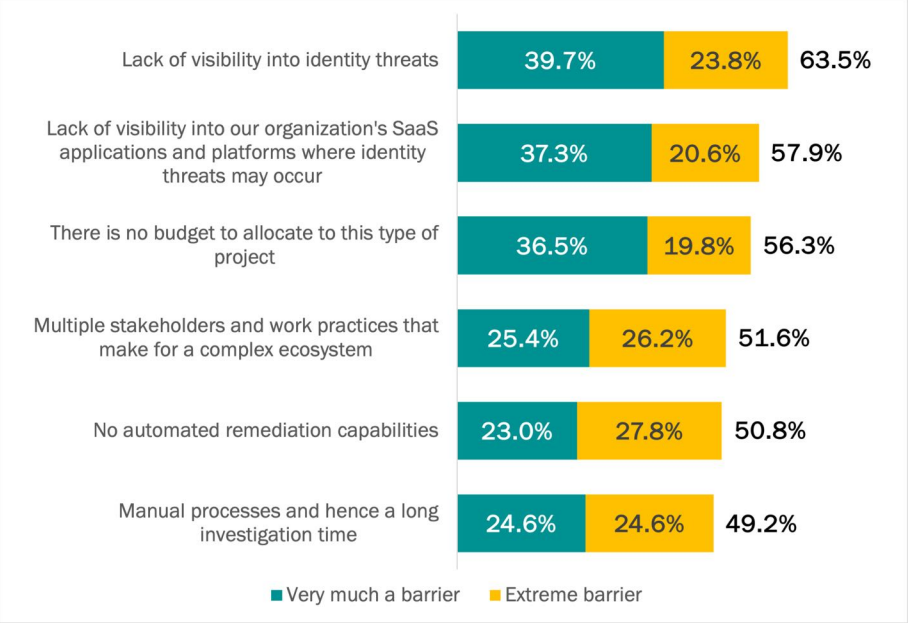
Some vendors are exploring alternate hardware form factors that more closely tie the hardware device to the individual, while not giving away biometric safeguards. These new form factors decrease the threat of device loss, increase convenience of usage by making it a wearable object, and hold out the promise of more universal applicability across multiple MFA use cases.

OPTICS AND VISIBILITY INTO IDENTITY THREATS AND COUNTERMEASURES

A lack of visibility into identity threats in general and across SaaS applications in particular are the two top-rated barriers that organizations face when attempting to stop identity threats (see Figure 11). Visibility means having the ability to see anomalous authentication patterns, users that lack MFA protections, and those that continue to rely on legacy and weak MFA approaches, among others.

Visibility drives change. Identity security and other cybersecurity vendors offer solutions that aggregate identity signals across users, endpoints, servers, networks, and cloud offerings to show what is happening and highlight what looks out of place. Manual—or ideally autonomous—mitigations can then be enacted.

Figure 11
Barriers to stopping identity threats
Percentage of respondents



Source: Osterman Research (2024)

Paying attention to early warning signals of compromised credentials on the dark web can mean the difference between a failed attack and a breach.

EARLY WARNING OF COMPROMISED CREDENTIALS ON THE DARK WEB

Data breaches and data leakages usually result in identity data being available for purchase by threat actors on the dark web. Cybersecurity vendors are also gaining access to this identity data—usually not by paying for it, however. Once acquired, vendors ingest the data into their threat data lakes for analysis, correlation, and processing.

Some vendors offer alerting services to organizations when identities of relevance are detected in new data breaches, for example, when a corporate email address or valid authentication token is discovered in a breach record. Organizations can build manual or automated workflows around such advisories, including temporarily locking an account to prevent login while an investigation is underway, forcing the user to change their password and authentication details, revoking current authentication tokens, or forcing additional MFA security controls on subsequent authentication attempts. Paying attention to these early warning signals can mean the difference between an attack that is stopped and one that becomes a breach.

MODERNIZATION OF IDENTITY FLOWS

Changing to next-generation phishing-resistant MFA devices is a key part of strengthening identity security, but not all systems and processes support these methods. Organizations with legacy applications face the daunting task of modernizing their apps to support modern identity flows. As a manual re-development process, this takes time, is costly, and risks the integrity of the processes enabled by the application. Unless done properly, it also fails to future-proof the organization and its apps for yet-to-come identity approaches.

Various vendors offer solutions that enable identity modernization without the cost and risk of manual re-development of the legacy app in full. Such solutions enable organizations to intercept current identity flows, replace them with more modern alternatives, and provide options for enforcing and updating MFA methods in use. Some solutions can also assess risk factors as part of the authentication request and route the request through elevated MFA procedures for a risk-adjusted stance.

In principle, we encourage organizations to modernize apps and embrace the strongest and most effective forms of MFA and identity security possible. Getting there takes time, and if the choice is to continue to offer only SMS-based MFA with the legacy app versus replacing identity flows with a more modern MFA approach while wider app modernization takes place, we recommend the second approach. Modernize your apps, create the foundation for using the strongest forms of modern MFA possible, and in the meantime, upgrade what's possible using identity modernization solutions.

Identity modernization solutions enable organizations to intercept current identity flows, replace them with more modern alternatives, and provide options for enforcing and updating MFA methods in use.

Best practices for identity security

Organizations elevating identity security are focused on three main strategies: training users, upgrading MFA devices, and monitoring.

HARDEN MFA METHODS AND CONTEXTUAL PROCESSES

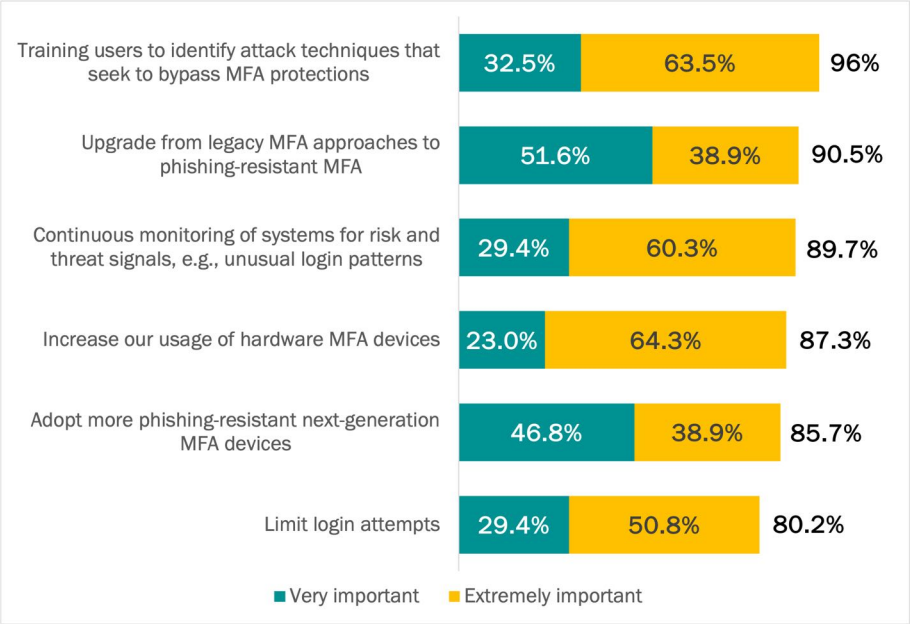
The organizations in this research plan on strengthening a range of processes tied to MFA usage over the next 12 months, with 84.1% of respondents giving the two highest ratings to five or more strategies below. These strategies are not a pick list of either/or but rather a basket of approaches that need to be hardened in lockstep. For example, training users to identify attack techniques that seek to bypass MFA protections is critically important (and ranks in first place overall) but is ultimately undermined if legacy and phishing-prone MFA devices are retained.

The five highest-ranked strategies combine to offer a three-point plan for strengthening MFA protections (see Figure 12):

1. **Training users**
   Train users so they can detect attacks that seek to bypass MFA protections (ranks in first place overall and in second place for "extremely important").
2. **Upgrade MFA devices**
   Stop using legacy MFA approaches. Replace legacy methods with hardware (ranks in first place for "extremely important") and next-generation MFA devices that are phishing-resistant.
3. **Monitor identity security**
   Continuously monitor systems for risk and threat patterns (ranks in third place both overall and for the "extremely important" rating).

Three strategies for strengthening identity security offer a basket of approaches that need to be hardened in lockstep.

Figure 12
Strategies for strengthening MFA: the 12-month outlook
Percentage of respondents



Source: Osterman Research (2024)

This three-point plan was also evident in the answers to an open-ended question on factors that influence confidence in protecting against identity threats. After grouping and categorizing the answers, the top four factors were:

- **Staff competency**
  Staff competency is what staff training seeks to develop in employees, managers, and executives. For all, training on detecting general phishing attacks is essential, along with specialized role-based spear phishing and BEC training. Specifically in terms of MFA, employees must be trained to not approve an MFA request they haven't initiated, the reasons for using stronger and hardened forms of MFA wherever possible, and how to protect themselves (and their organization) against new and emerging types of identity attacks. Future identity threats are likely to include drive-by type attacks where malware or remote execution capabilities are established on a phone or computer. Competency to protect against the threats of today and tomorrow is essential.

- **The use of MFA**
  That employees use MFA of any kind was taken as a sign of confidence in protecting against identity threats. While we agree that some kind of MFA is better than nothing, legacy and weak forms harm identity security posture by giving the impression of security without the reality thereof. Some respondents who mentioned the use of MFA also highlighted the importance of modernizing current approaches.

- **Access limits and controls**
  Limiting what data and systems can be accessed by identities helps to limit the extent of a data breach. In particular, sensitive data needs elevated safeguards to prevent inappropriate access. See the next section for more.

- **Monitoring**
  Comprehensive insight into current identity protections is a source of confidence. Several respondents noted the need to analyze user behaviors for risky signals and include oversight of privileged and third-party users.

Compromised accounts to organizations where openness and transparency reign provide access to a whole lot more data than would otherwise be available.

RECHECK ACCESS CONTROLS

Most organizations find access controls a difficult concept to master in practice. Collaboration systems, team workspaces, and other social business initiatives over the past decade have emphasized openness and transparency. While these are worthwhile employee engagement strategies, they result in threat actors rubbing their hands in glee. Compromised accounts to organizations where openness and transparency reign provide access to a whole lot more data than would otherwise be available. As a rule, if the culture revolves around openness and transparency, compensating security controls must be in place. These include:

- **Regular access reviews**
  Periodically request the owner of each data system or repository to check and certify that current users are valid.

- **Alerting on anomalous access patterns**
  Malicious use of valid credentials can be discovered by looking at the underlying attributes of an authentication request, such as device type, geographical location, network type, and time of day. Having the ability to see these in the context of data access will signal anomalous patterns.

- **Hardening employee offboarding processes**
  Departing employees can retain access to corporate data if their credentials are not fully revoked as soon as they finish employment. Ensure full removal and revocation of access rights for all departing employees as soon as possible.

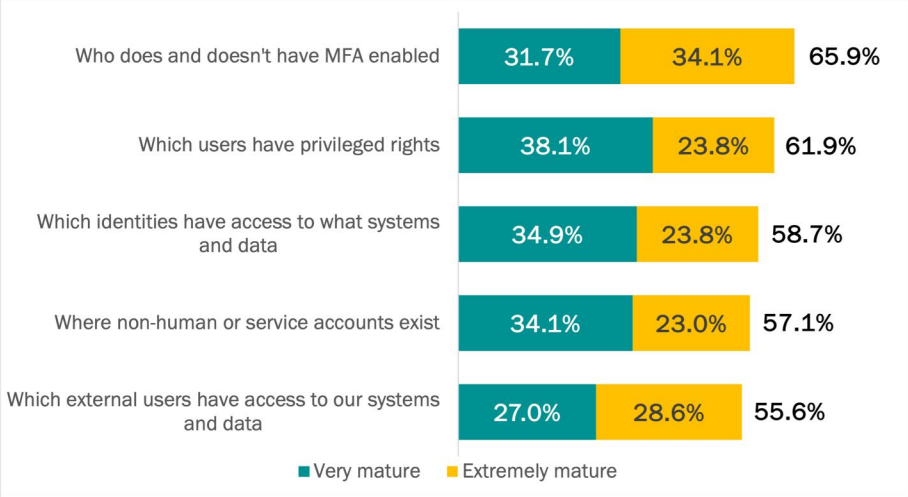
INCREASE MATURITY OF VISIBILITY

Many organizations lack mature systems and processes for providing visibility into identity security posture, such as which employees do and do not have MFA enabled (only 65.9% claim to have mature processes), which users have privileged rights (61.9%), and which identities have access to systems and data (58.7%). When visibility into identity security posture is lacking, people, data, and systems are unknowingly exposed to cyberattack risks.

Organizations with less than extremely mature visibility need to rapidly mature their capabilities across this component of their identity security ecosystem. The changing cyberthreat environment around identities means that improved visibility isn't just a best practice, it's an essential one.

See Figure 13.

Figure 13
Maturity of systems and processes for visibility into identity security
Percentage of respondents



Source: Osterman Research (2024)

Many organizations lack mature systems and processes for providing visibility into identity security posture.

Conclusion

Threat actors want organizations to embrace the following playbook:

- **Use weak forms of MFA**
  Keep relying on weak forms of MFA that can be easily bypassed, such as one-time codes by any form, such as SMS or email. While these approaches provide a sense of security, ultimately it is a false one that can be turned against organizations for malicious gain.

- **Don't worry about visibility into identity security posture**
  Knowing who does and doesn't have MFA enabled, what MFA methods they are using, who has privileged access rights, and which identities have access to various systems and data is an overrated capability. Hope for the best. It will also save on fees for licensing new identity security solutions.

- **Don't monitor to ensure your employees credentials aren't compromised**
  Assume that your employees' credentials are safe without verifying their security status. Avoid implementing continuous monitoring or dark web scanning for compromised credentials—after all, what you don't know can't hurt you, right? This lack of vigilance could lead to a significant breach.

Now that you know, do the opposite.

Threat actors prefer organizations to keep relying on weak forms of MFA, forget about visibility into identity security posture, and not to bother about verifying the security status of identities.

Sponsored by Abnormal Security

Abnormal Security is the leading AI-native human behavior security platform, leveraging machine learning to stop sophisticated inbound attacks and detect compromised accounts across email and connected applications. The anomaly detection engine leverages identity and context to understand human behavior and analyze the risk of every cloud email event—detecting and stopping sophisticated, socially engineered attacks that target the human vulnerability.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly. Additional protection is available for Slack, Workday, Salesforce, ServiceNow, Zoom, Amazon Web Services and multiple other cloud applications.

abnormalsecurity.com

Abnormal

abnormalsecurity.com

@AbnormalSec

Methodology

This white paper is based on findings from a survey conducted by Osterman Research. One hundred twenty-six (126) respondents who are responsible for the management or maintenance of how their organization approaches identity security, uses MFA to protect identities, and plans for rethinking MFA protections in light of the rise of identity attacks were surveyed during July 26 to August 8, 2024. To qualify, respondents had to work at organizations with at least 500 employees. All surveys were conducted in the United States. The survey was cross-industry, and no industries were excluded or restricted.

JOB ROLE

Identity infrastructure manager	29.4%
IAM manager, director or head	22.2%
Cybersecurity manager	17.5%
Identity architect	15.9%
CISO	15.1%

ORGANIZATION SIZE

1000 to 4999 employees	85.7%
5000 to 9999 employees	9.5%
10,000 to 19,999 employees	2.4%
20,000 to 25,000 employees	2.4%

INDUSTRY

Agriculture, forestry or mining	1.6%
Computer hardware or computer software	4.8%
Data infrastructure or telecom	7.1%
Education	4.8%
Energy or utilities	6.3%
Financial services	10.3%
Government	3.2%
Healthcare	5.6%
Hospitality, food or leisure travel	4.8%
Industrials (manufacturing, construction, etc.)	6.3%
Information technology	2.4%
Life sciences or pharmaceuticals	6.3%
Media or creative industries	5.6%
Professional services (law, consulting, etc.)	11.1%
Public service or social service	5.6%
Retail or ecommerce	8.7%
Transport or logistics	5.6%

---

[1] IBM, X-Force Threat Intelligence Index 2024, February 2024, at https://www.ibm.com/reports/threat-intelligence

[2] Constella Intelligence, 2024 Identity Breach Report, August 2024, at https://constella.ai/wp-content/uploads/2024/08/Constella_IdentityBreachReport-2024.pdf

[3] Jai Vijayan, Threat Actor May Have Accessed Sensitive Info on CISA Chemical App, June 2024, at https://www.darkreading.com/cyberattacks-data-breaches/threat-actor-may-have-accessed-sensitive-info-on-cisa-chemical-app

[4] SlashNext, The State of Phishing 2024, May 2024, at https://slashnext.com/the-state-of-phishing-2024/

[5] CISA, FY22 Risk and Vulnerability Assessments (RVA) Results, July 2023, at https://www.cisa.gov/sites/default/files/2023-07/FY22%20RVA%20Infographic_508c.pdf

[6] Microsoft Security, Microsoft Digital Defense Report 2023, October 2023, at https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

[7] Google Blog, Making you safer with 2SV, February 2022, at https://blog.google/technology/safety-security/reducing-account-hijacking/

[8] FIDO Alliance, Google Case Study, January 2019, at https://fidoalliance.org/google-case-study/

[9] Richard Bortnick and Jonathan Meer, Practical Implications of Travelers v. ICS for Cyber Insurance Brokers, Carriers and Policyholders: Emerging Trends & Predictions –Takeaways from the Cyber Insurance Webinar, February 2023, at https://natlawreview.com/article/practical-implications-travelers-v-ics-cyber-insurance-brokers-carriers-and