DARKREADING

DECEMBER 2023

The State of Passwordless Authentication: Security and Convenience Drive the Change

opentext™

Executive Summary

As cyber incident rates continue to surge, industry professionals worry about the constant threat of security breaches. When even sophisticated organizations fall prey to advanced social engineering attacks, it's clear that conventional security measures lag behind malicious capabilities. And according to IT and cybersecurity leaders, the gap is significant.

Identity verification is foundational to security as it helps organizations protect their systems, data, networks, websites, and applications from attacks. It also helps individuals keep their personal data confidential, empowering them to conduct business, such as banking or investing, online with less risk.

Any given data transaction increasingly utilizes cloud services, third-party apps, and personal devices, which gives rise to an indeterminate perimeter. Since passwords are easy to hack, they can be the weakest link in the security chain. According to Crowdstrike, 80% of all breaches use compromised identities and can take up to 250 days to identify. For these reasons, passwordless authentication options are growing in popularity to protect access where it matters most—at the end-user level.

This new survey from Dark Reading on behalf of Opentext indicates that industry professionals understand the urgency to move beyond passwords, to varying degrees. IT and security leaders were surveyed regarding their insights, opinions, and concerns about security and passwordless technology. Respondents clearly expressed their overarching goal to minimize the impact of rising threats that traditional identity authentication methods fail to mitigate.

Certain obstacles currently hinder widespread passwordless adoption, such as competing IT interests and concerns about security and business impact. Notably, the research reveals that most organizations plan to move forward with passwordless authentication precisely due to its distinct security advantages and business benefits.

The study results indicate that passwordless methods will continue to rise in acceptance as a core component of identity and access security—with the added advantage of user and customer convenience. Although the report reveals an industry experiencing tension, the anticipation of a more secure future remains intact.

Key findings

Phishing attacks top concern: Of the 140 IT and security professionals polled, 90% said they were concerned about phishing attacks or stolen/hacked credentials. Phishing and spear phishing continue to be leading attack vectors as threat actors enjoy a high level of success exploiting human-based errors.

Prioritizing passwordless: Respondents recognize the value of passwordless technology, with 64% stating it's important for their organizations to move to a fully passwordless authentication model. And 59% felt that passwordless is important when used as the primary credential or part of a multi-factor implementation as it relates to allowing their organization to offer more services to consumers.

Shared secrets identified as key risk: Nearly 80% of IT and security leaders polled said it was important for their organization to eliminate shared secrets, such as passwords and PINs. Shared secrets are risky since they are easy to steal and are typically stored in a single place.

Worrisome incident rates: Over half of respondents stated they were aware of their organization being targeted with a credential-based attack within the last six months. And more than one-third have fallen victim to successful credential-based attacks in the past year. These negative experiences drive the desire to move beyond password-based security.

Good for business: Passwordless technology was also recognized as having a positive impact on a business's bottom line, according to 63% of respondents. This is likely due to advantages such as improved user experience and customer satisfaction. Passwordless technology provides frictionless identity authentication for smoother transactional experiences.

Dissatisfaction with the status quo

"We Use Passwords and Authenticate constantly over and over and over again!!!!!"

Social engineering, phishing, and spear phishing attacks threaten essentially anyone active online. For the everyday internet user, government entities, critical infrastructure, large enterprises, and beyond, these incidents place every password-protected account at risk. Verizon's 2023 Data Breach Investigations Report (DBIR) revealed that a whopping 74% of breaches involved the human element, which includes social engineering attacks, errors, or misuse.

Due to the high rate of credential-based attacks, industry professionals fully grasp the need to move beyond passwords. What motivates respondents to move forward to passwordless options? It's the real-world pain experienced at the hands of nefarious aggressors. Participants in this survey confirmed the stark reality that was exposed in the DBIR.

"90% are concerned about phishing attacks or stolen/hacked credentials."

Figure 1

Real-World Attack Experience

What is the timeframe for each of the following?

	Past week	Past month	Past 3 months	Past 6 months	Past year	Past 2 years	Never
The last time that you were aware of your organization being targeted with a credential-based attack	13%	19%	13%	8%	15%	12%	20%
The last time a credential-based attack was successful against your organization	4%	5%	7%	7%	13%	14%	50%

Data: Dark Reading survey of 140 IT and cybersecurity professionals, October 2023

Among respondents, 53% had been targeted with a credential-based attack within the last six months. And over one-third were victims of a successful credential-based attack in the past year (Figure 1). Unsurprisingly, among surveyed professionals, 90% are concerned about phishing attacks or stolen/hacked credentials (Figure 2).

Figure 2

Top Security Threats

Please rate how concerned your organization is about the following security threats.

	Very concerned	Somewhat concerned	Neutral	Not very concerned	Not at all concerned
Phishing attack	67%	23%	8%	2%	0%
Stolen or hacked credentials	61%	29%	6%	4%	0%
A security misconfiguration of a datastore or server holding sensitive information	51%	36%	7%	6%	0%
Social engineering – the improper sharing of credentials	47%	40%	8%	2%	3%
Failure to patch the system holding sensitive information	46%	36%	13%	3%	2%
Data breach from a lost or stolen device	45%	29%	15%	8%	3%
Cloud security misconfiguration	43%	42%	8%	7%	0%
Malicious insider	43%	33%	14%	9%	1%
Unknown zero-day vulnerability	40%	41%	17%	2%	0%
Company email server	39%	34%	15%	9%	3%

Data: Dark Reading survey of 140 IT and cybersecurity professionals, October 2023

Social engineering hacks negatively impact even organizations with the best security teams and robust cybersecurity defenses. The problem resides in how we use the internet today.

Structured and unstructured private data is increasingly stored and accessed from the cloud. The data center has receded in its role as the host of corporate services. And the routing of traffic through the data center has been dramatically reduced. As we move towards a fully fluid perimeter, typical firewall security methods become irrelevant.

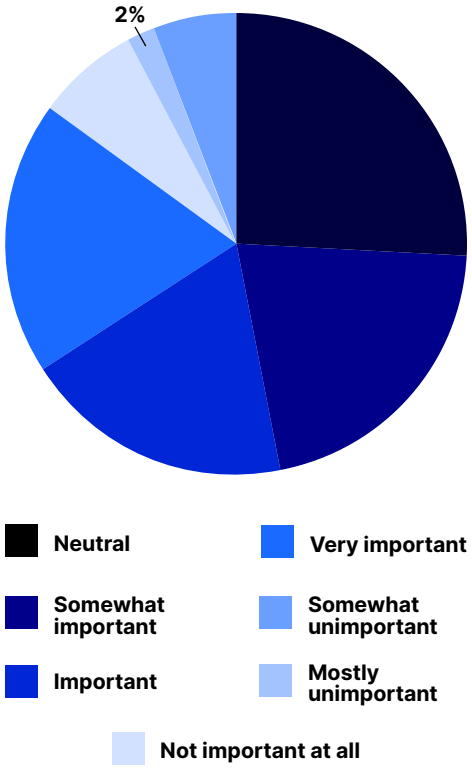
For these reasons, 59% of respondents felt that passwordless authentication is important, whether used as the primary credential or part of a multi-factor implementation, to allow their organization to offer more services to their consumers (Figure 3). Furthermore, 64% feel it's important to move to a fully passwordless authentication model (Figure 4).

"64% of respondents feel it's important to move to a fully passwordless authentication model."

Figure 3

Importance of Passwordless Authentication

How important has passwordless authentication technology been as it relates to allowing your organization to offer more services to your consumers?



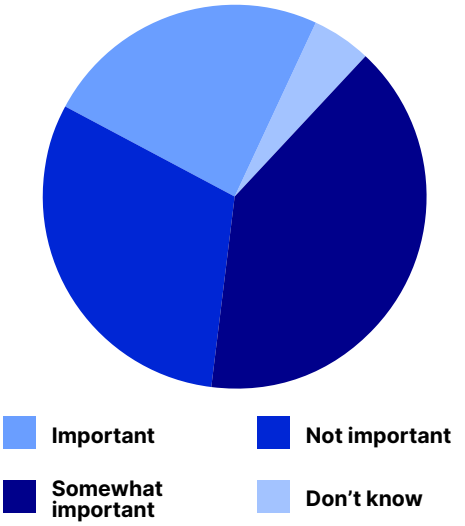
Data: Dark Reading survey of 140 IT and cybersecurity professionals, October 2023

Additionally, it's clear that shared secrets are disliked by IT and security teams. Nearly 80% of respondents feel it's important to eliminate shared secrets such as passwords (Figure 5). The problem with shared secrets is that they are easy to hack and tend to be stored all in one place. Even worse, shared secrets can be purchased in bulk on the dark web.

Figure 4

Moving to Passwordless Authentication Model

How important is it for your organization to move to a fully passwordless authentication model?

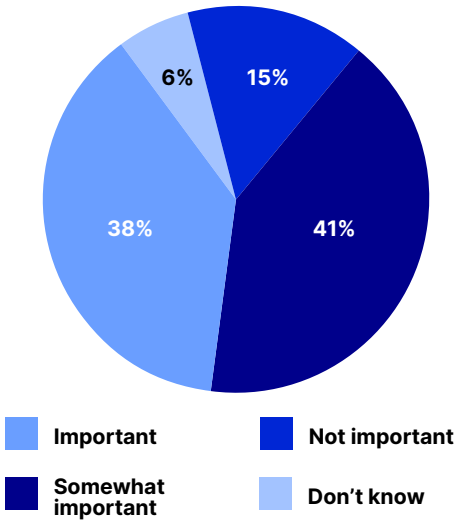


Data: Dark Reading survey of 140 IT and cybersecurity professionals, October 2023

Figure 5

Eliminating Passwords

How important is it for your organization to eliminate shared secrets such as passwords?



Data: Dark Reading survey of 140 IT and cybersecurity professionals, October 2023

What organizations think about passwordless tech

Passwordless technology continues gaining traction as a core response to the security challenges organizations face today. Additional business benefits also attract organizations to make the shift to passwordless.

"The main drivers behind an organization's efforts to adopt passwordless technology are stronger security, enhanced user experience, less IT work and improved productivity."

IT leaders are accustomed to leveraging any given technology for multiple advantages. In this manner, passwordless authentication is no different as it provides both improved security and more convenience for the end user. According to the respondents in this study, the main drivers behind an organization's efforts to adopt passwordless technology are improved security, improved user experience, less IT work, and improved productivity (Figure 6).

Figure 6

Driving Adoption to Passwordless Technology

Please rank the following reasons from most important to least important in how they drive your organization's adoption of passwordless technology.

	Overall rank	Score
Improved security	1	949
Improved user experience	2	636
Reduced IT burden	3	563
Improved productivity	4	563
Leadership priority	5	450
Government mandates	6	428
Customer impact	7	424
Employee demand	8	307

Note: Rank is based on a weighted score. Responses are weighted, and scores represent the sum of all weighted counts.

Data: Dark Reading survey of 140 IT and cybersecurity professionals, October 2023

As expected, improved security ranks highest among the reasons to adopt passwordless authentication. But beyond security, business-centric forces predominate among the motives driving passwordless adoption.

In today's digital reality, security and business benefits increasingly overlap. When organizations can manage risk better in engagements with digital partners and customers, the natural outcome is more efficient and meaningful interactions under various circumstances.

For **healthcare**, this means providers can deliver improved remote care with the added benefit of more robust security. Simplified yet secure access can greatly help impaired patients who might have difficulty navigating complex authentication schemes.

For **finance**, passwordless technology enables banks and lenders to provide fast and secure client access. The result is a simultaneous improvement in account security and customer satisfaction.

eCommerce is a favorite target of social engineering and phishing attacks. Passwordless authentication allows online retailers to not only ensure the security of their customers but also makes for a more streamlined shopping experience, which can boost sales.

In **education**, FIDO (Fast Identity Online) has quickly become the industry standard for access security. Students, staff, and faculty can plug their small portable FIDO devices into computers via Bluetooth for fast access to secured resources. These passwordless phishing-resistant methods frustrate attackers who quickly move on to easier targets.

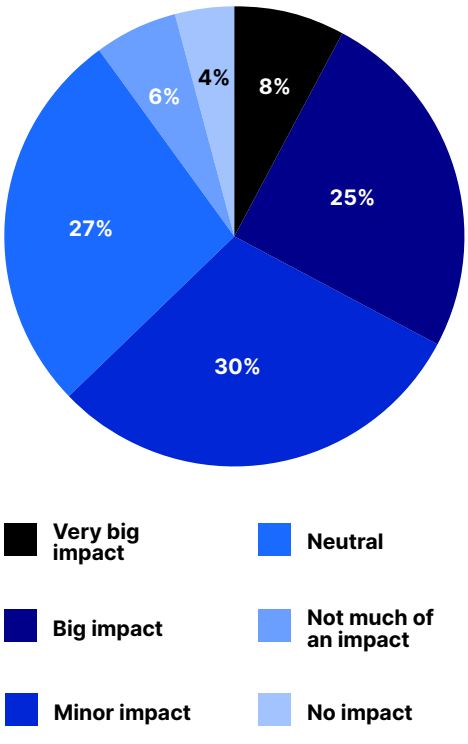
What about IT burden?

It might seem counterintuitive that passwordless would reduce IT burden, since initial deployment would require implementing specific tools and training. However, the long-tail benefits of a streamlined, passwordless UX can translate into less work for tech teams busily maintaining password-based access structures. Security teams would also be relieved of the burden of investigating and remediating credential-based incidents.

Figure 7

Impact of Passwordless Technologies on Bottom Line

How much of a positive impact do you expect that the adoption of passwordless technologies would have on your business's bottom line?



Data: Dark Reading survey of 140 IT and cybersecurity professionals, October 2023

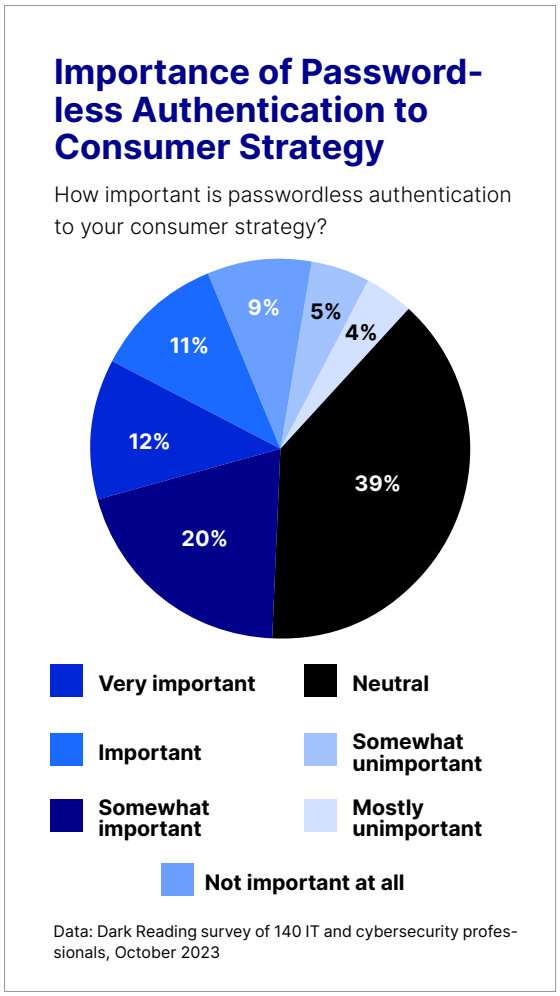
Positive impact on business

Decision makers quickly grasp the full benefit of passwordless solutions, which can be leveraged into a clear business advantage. And 63% of respondents said that passwordless would have a positive impact on the bottom line. A third of those interviewed stated that the impact would be "big" or "very big" (Figure 7).

"A third of those interviewed stated that the business impact of passwordless technology would be 'big' or 'very big'."

Given its ease of use, it's unsurprising that organizational leaders seek to adopt passwordless technology. It's clearly given weight in consumer strategy decision-making, with 43% of respondents confirming its importance (Figure 8).

Figure 8



Long-established options remain popular

Despite respondents' desire—driven by security and business benefits—to move to passwordless, many organizations are still stuck with traditional identification methods. The resistance to pivot to passwordless includes competing technological priorities, concerns about business impact, and lack of leadership support (Figure 9).

When asked about the current and future use of authentication technologies, nothing besides passwords and PINs has an adoption rate of over 40%—and the planned adoption rate isn't very high for any of the alternatives either.

Even though no single passwordless technology rises to the top, only two respondents said they neither use nor plan to purchase any of the passwordless options listed. In other words, 99% of respondents either already use or plan to purchase one of the passwordless technologies listed in Figure 10.

Figure 9

Obstacles to Passwordless Adoption

Please rank the following reasons from high to low based on how much of a factor they have been in preventing your organization from reaching your full passwordless goals.

	Overall rank	Score
Competing technological priorities	1	695

Note: Rank is based on a weighted score. Responses are weighted, and scores represent the sum of all weighted counts.

Data: Dark Reading survey of 140 IT and cybersecurity professionals, October 2023

Figure 10

Authentication Technologies In Use and Planned For Purchase

Which of these authentication technologies does your organization currently use, and which do you intend to purchase in the next 12 months?

	Currently use	Plan to implement	Neither use nor plan to implement
Traditional username and password	95%	4%	1%
Mobile SMS - one-time PIN	69%	14%	17%
Authentication card (PKI, RFID, NFC, etc.)	39%	7%	54%
Out-of-band push to mobile app	39%	11%	50%
Fingerprint	37%	16%	47%
Challenge-response authentication	30%	13%	57%
Nonmobile OTP	28%	10%	62%
Facial recognition	23%	15%	62%
Smart card	18%	9%	73%
Geo-fencing (passive)	15%	13%	72%
FIDO U2F	9%	15%	76%
FIDO UAF	6%	13%	81%
Bluetooth (passive)	3%	12%	85%
Voice recognition	2%	8%	90%

Data: Dark Reading survey of 140 IT and cybersecurity professionals, October 2023

Obstacles to passwordless implementation

While obstacles to passwordless adoption cannot be ignored, there are ways to navigate around them. Here are some of the most common objections to the technology (Figure 9) and the corresponding counter-arguments that support passwordless solutions.

Competing technological priorities/ limited IT resources

There's no lack of potential tech solutions available for a wide variety of organizational needs. How should priorities be established? Stemming the tide of social engineering/phishing attacks remains paramount. The FBI's most recent Internet Crime Complaint Center (IC3) report stated that phishing schemes were the number one type of cybercrime reported. These attacks can lead to millions of dollars in damage.

While other technologies may improve your security posture, few directly address the Achilles' heel of access: the password. One of the main reasons phishing attacks are so successful is because shared secrets, like passwords, exist. Remove the password, and you remove the risk.

Concerns about impacts to business and security

Business leaders must always evaluate the business and security impact of any new technology. Passwordless can benefit both. Passwordless authentication eliminates the need to store passwords, which can be vulnerable to a wide range of threats, including software supply chain attacks. Furthermore, security teams can focus on other tasks instead of trying to detect and prevent password leaks.

On the business side, by removing the need to remember or type passwords, passwordless creates a better user experience and customer experience. Companies also avoid spending on password storage, management, and resets. It's inevitable that employees will occasionally forget their passwords, such as for SaaS tool access. While they wait for IT to resolve account lockout, work is put on hold and productivity suffers. For larger enterprises, this repeated pattern can lead to significant losses over time. By definition, passwordless removes the resource drain caused by password based security.

Reluctant leadership

Executive buy-in is essential for any initiative. Risk reduction and cost benefits must be clearly demonstrated. All this can then be backed up by the business advantages outlined in this report. Eliminating centrally managed passwords leads to better security, fewer breaches, lower support costs, and enhanced user experience.

A unifying thread to all these obstacles may be lack of awareness and education. Many users are not familiar with passwordless authentication and may be hesitant to try it. While it will take time to educate leadership, it's worth the effort given the long term business and security benefits. One way to introduce the value of passwordless is to share data about phishing attempts and attacks with executives. Then explain how passwordless works to thwart those attacks.

The future of passwordless

Can we identify a favored method of all the passwordless authentication options? Our respondents named authentication cards, fingerprint, out-of-band push-to-app, facial recognition, and smart cards as favorites for internal and external users (Figures 11 & 12).

Traditional usernames and passwords were perceived as the most convenient access method, typical for a status quo option. However, 45% of the total respondents plan to purchase passwordless authentication technologies in the next 12 months, and those who plan to purchase indicated they would purchase an average of three different solutions. We can see IT and security leadership handling a time of change, with widespread adoption likely coming in the near future.

Figure 11

Preferred Passwordless Technologies for Internal Use

Please rank the level of convenience/confidence that you believe each of these passwordless technologies offers your internal employees or contractors from high to low.

	Overall rank	Score
Traditional username and password	1	1217
Mobile SMS - one-time PIN	2	1202
Authentication card (PKI, RFID, NFC, etc.)	3	1148
Fingerprint	4	1138
Out-of-band push to mobile app	5	983
Facial recognition	6	960
Smart card	7	952
Challenge-response authentication	8	786
Nonmobile OTP	9	747
FIDO U2F	10	620
Voice recognition	11	601
FIDO UAF	12	546
Geo-fencing (passive)	13	518
Bluetooth (passive)	14	496

Note: Rank is based on a weighted score. Responses are weighted, and scores represent the sum of all weighted counts.

Data: Dark Reading survey of 140 IT and cybersecurity professionals, October 2023

Figure 12

Preferred Passwordless Technologies for Consumers or Partners

Rank the level of convenience/confidence that you believe each of these passwordless technologies offers your consumers or partners.

	Overall rank	Score
Traditional username and password	1	1199
Mobile SMS - one-time PIN	2	1193
Fingerprint	3	1011
Authentication card (PKI, RFID, NFC, etc.)	4	958
Facial recognition	5	874
Out-of-band push to mobile app	6	872
Smart card	7	803
Nonmobile OTP	8	793
Challenge-response authentication	9	709
Voice recognition	10	653
FIDO U2F	11	549
Bluetooth (passive)	12	518
Geo-fencing (passive)	13	500
FIDO UAF	14	489

Note: Rank is based on a weighted score. Responses are weighted, and scores represent the sum of all weighted counts.

Data: Dark Reading survey of 140 IT and cybersecurity professionals, October 2023

Favorite passwordless technologies

Authentication card (PKI, RFID, NFC, etc.): Authentication cards are physical devices that store digital certificates and private keys. They use Public Key Infrastructure (PKI) to authenticate users. RFID (Radio Frequency Identification) and NFC (Near Field Communication) are wireless communication technologies that can be used to transmit data between the authentication card and the reader.

Fingerprint: Fingerprint authentication uses biometric technology to verify a user's identity. It captures the unique pattern of ridges and valleys on a person's fingertip and compares it to a stored template to authenticate the user.

Out-of-band push to mobile app: Out-of-band push authentication sends a push notification to a user's mobile device when they attempt to log in. The user approves the request with a single button tap on their mobile app.

Facial recognition: Facial recognition uses biometric technology to verify a user's identity by analyzing their facial features. It captures an image of the user's face and compares it to a stored template to authenticate the user.

Smart card: A smart card is a physical device that stores digital certificates and private keys. It can be used for authentication by requiring the user to insert the card into a reader and enter a PIN.

One of the reasons for lagging adoption rates might be the lack of awareness surrounding passwordless technology along with the lack of a single predominant solution. A basket of tools might make it more challenging to educate and convince stakeholders to embrace new technology. While this makes the transition more complicated, it can also be an advantage as companies can choose the method that works best for their business.

Just like multi-factor authentication continues to gain user acceptance over time, passwordless will likely follow suit. Modern-day users are increasingly tech-friendly. Smartphones have played a huge role in getting people comfortable with passwordless technologies (such as fingerprint and facial recognition). Meanwhile, Intel and Microsoft's biometric tools have also widened public acceptance of passwordless methods. Since the final result is enhanced security and improved convenience, passwordless acceptance levels are expected to rise.

Conclusion

Given the relentless pace of attacks and the high cost of incident response, cybersecurity has assumed a core role in business decision-making. Social engineering attacks, like phishing, dominate the worry wall for IT and security teams. Security and identity and access management (IAM) leaders know that passwords are the obvious weak link in cyber defense.

By nature, passwordless authentication eliminates the problem of using weak passwords. It also offers distinct business advantages to users and organizations. For users, passwordless streamlines the user experience. Companies no longer need to store and protect passwords, which leads to better security, fewer breaches, and lower support costs.

Research confirms that organizations prioritize assessing and implementing robust passwordless authentication methods. Stronger security and enhanced user convenience will continue to drive this change forward.

About

opentext™

OpenText helps organizations tackle the most complex digital transformation programs with confidence. With the world's most complete and integrated Information Management platform, OpenText empowers their customers to organize, integrate and protect data and content as it flows through business processes inside and outside their organization.

Survey Methodology

OpenText commissioned Dark Reading to research the current state of passwordless (biometrics) and other authentication technologies, and what's driving the adoption of said technologies. The survey collected responses from 140 IT and cybersecurity professionals on their organization's usage and impact of passwordless technologies to their users.

The survey was conducted online in October 2023. Respondents were recruited via emailed invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database. Informa is the parent company of Dark Reading. Informa Tech was responsible for all survey design, administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

Respondents worked at companies of all sizes. Twenty-six percent of respondents were at large companies with 5,000 or more employees; 24% at companies with 500 to 4,999; 28% with 50 to 499 employees; and 22% from organizations with fewer than 50 employees.

The final data set includes job titles from executive level to staff. Eighteen percent held IT executive job titles (CIO/CTO or VP), and 6% were cybersecurity executives (CSO/CISO). Other titles included IT head/director/manager (19%), cybersecurity head/director/manager (9%), and IT or cybersecurity staff (17%). Other titles included corporate management (8%), network/system administrator (8%), engineer (7%), and software developer (4%).

Respondents' organizations represent more than 21 vertical industries including technology, banking and financial services, consulting, education, government, healthcare, and manufacturing.