CYBERARK®
The Identity Security Company

iSMG
INFORMATION SECURITY
MEDIA GROUP

Critical Gaps in Securing Identities

2023 Survey Results

INTRODUCTION

TONY MORBIN
Executive News Editor, EU
Information Security
Media Group

Welcome to the report summarizing the survey: Critical Gaps in Securing Identities.

Enterprises today rely on hundreds of applications to achieve their business and operational goals. Most of these apps integrate with single sign-on and multifactor authentication tools as the first line of defense against attacks that leverage compromised credentials, but some business apps require users to log in with usernames and passwords that are different from their corporate credentials.

This introduces security and usability challenges. To stay productive, employees need to access all business applications seamlessly and securely from any device and at any time. In addition, since some business apps contain high-value, privileged information, additional protections must be considered to control how employees use web applications and handle sensitive data.

In Q1 2023, we surveyed 214 senior cybersecurity professionals to identify:

- The top organizational challenges in securing non-SSO integrated apps;
- How organizations monitor and audit user activity within high-value applications;
- Benchmarking best practices;
- Where the biggest gaps/pain points are, how they're being addressed, and the rate of adoption of these new approaches in 2023.

More than just survey results, this report offers expert analysis of what organizations perceive to be the main challenges around identifying and remediating critical gaps in securing identities. This report intends to benchmark what your competitors are doing so that you can use these results to help enhance your own defenses.

Tony Morbin
Executive News Editor, EU
Information Security Media Group
tmorbin@ismg.io

TABLE OF CONTENTS

About this survey:

This survey was conducted in spring 2023. It attracted 214 responses from senior cybersecurity professionals in the NA, APAC, UKI and EU regions.

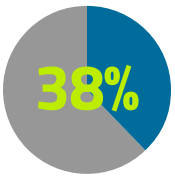
ABOUT CYBERARK:

Learn more at: www.cyberark.com

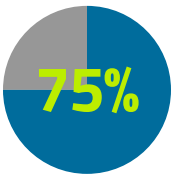
CYBERARK®
The Identity Security Company

BY THE NUMBERS

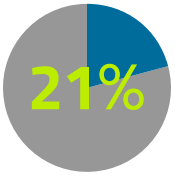
STATISTICS THAT JUMP OUT FROM THIS STUDY ON GAPS IN ID SECURITY:



38% of respondents say that their approach to handling credentials for apps not integrated with SSO is to leave it to the discretion of users.



75% of respondents say end-to-end encryption of usernames and passwords is the most important feature when selecting a password manager.



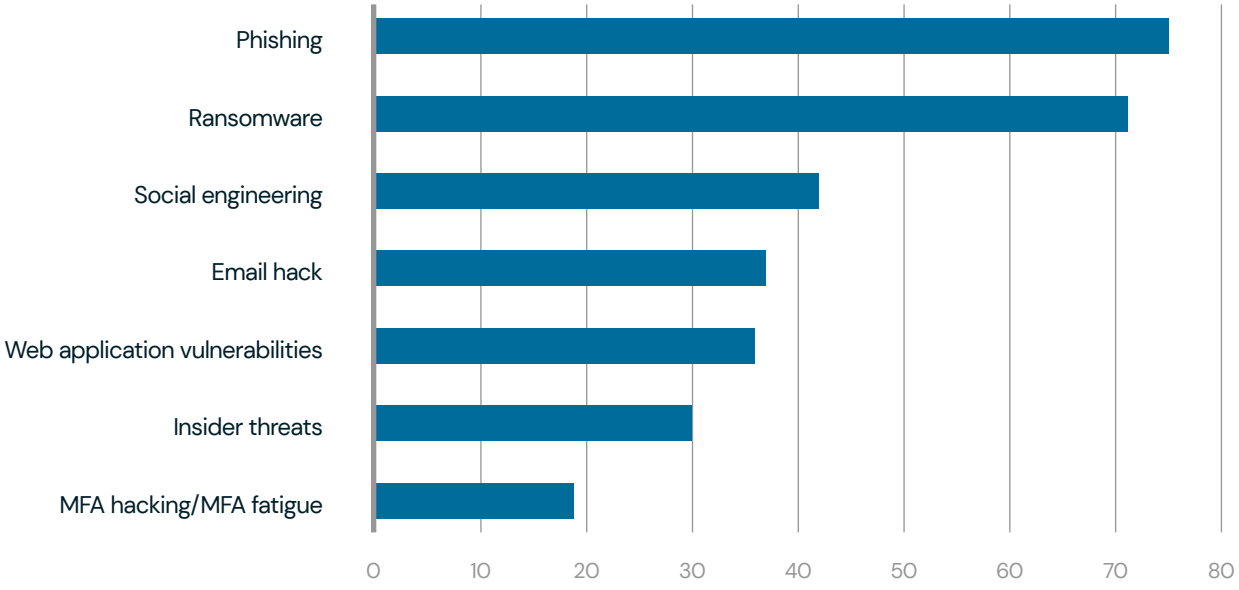
21% of respondents say it takes up to a week or more to gain full understanding of a reported incident.

EXECUTIVE SUMMARY

The respondents are frank and open about where their identity security gaps are, to the extent that the concerning practices they identify go beyond what one would expect any CISO to report to their board – particularly the high number leaving it to the discretion of users to handle credentials for apps not integrated with SSO.

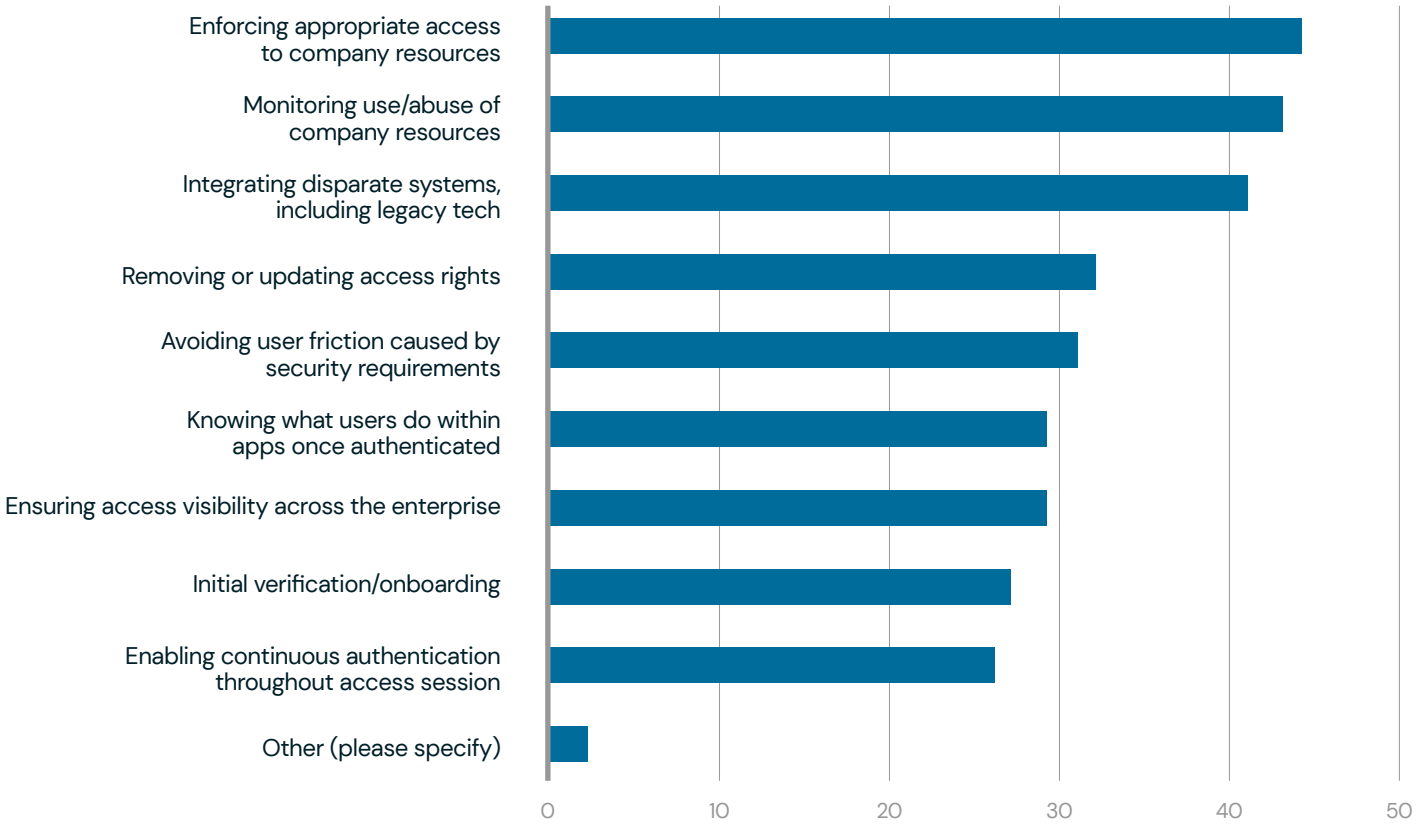
SURVEY RESULTS

Of the attack vectors that could affect your business in 2023, which are you most concerned about?



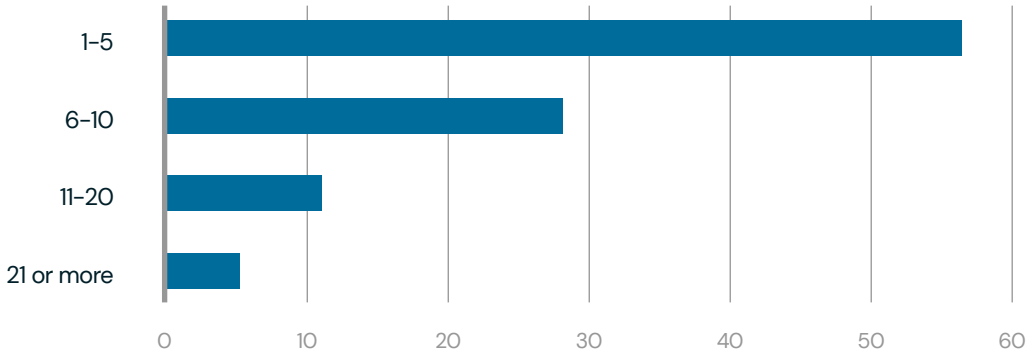
It is not a huge surprise that phishing and ransomware are the top attack concerns, cited by 74% and 70% respectively. Maybe more of a surprise is that 18% are now concerned about MFA hacking and fatigue.

What are the most challenging elements of delivering secure access management in your organization?



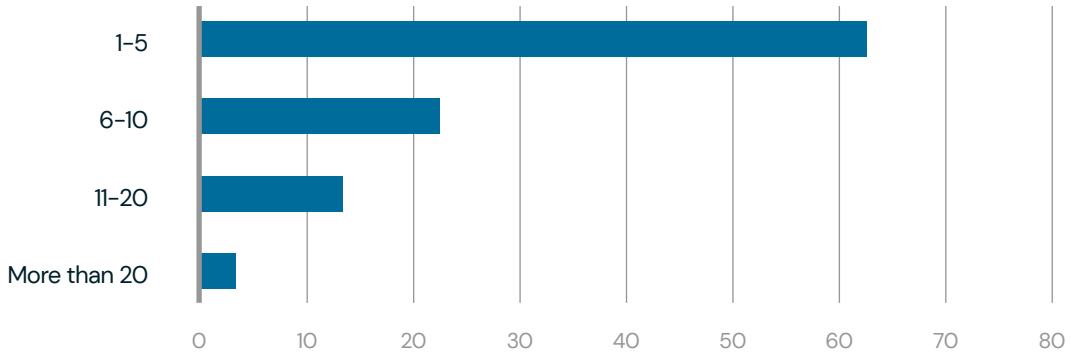
The most challenging aspect of securing access is enforcing appropriate access to company resources at 44% – and while that can include cash, it's mostly data. Next is what is done with that access – monitoring abuse is close behind on 43%. The issue of integrating systems including legacy also figures highly at 41%. Knowing what users do within apps once authenticated is a top-three concern for 29%.

How many business applications that you use hold business-critical or highly sensitive information?



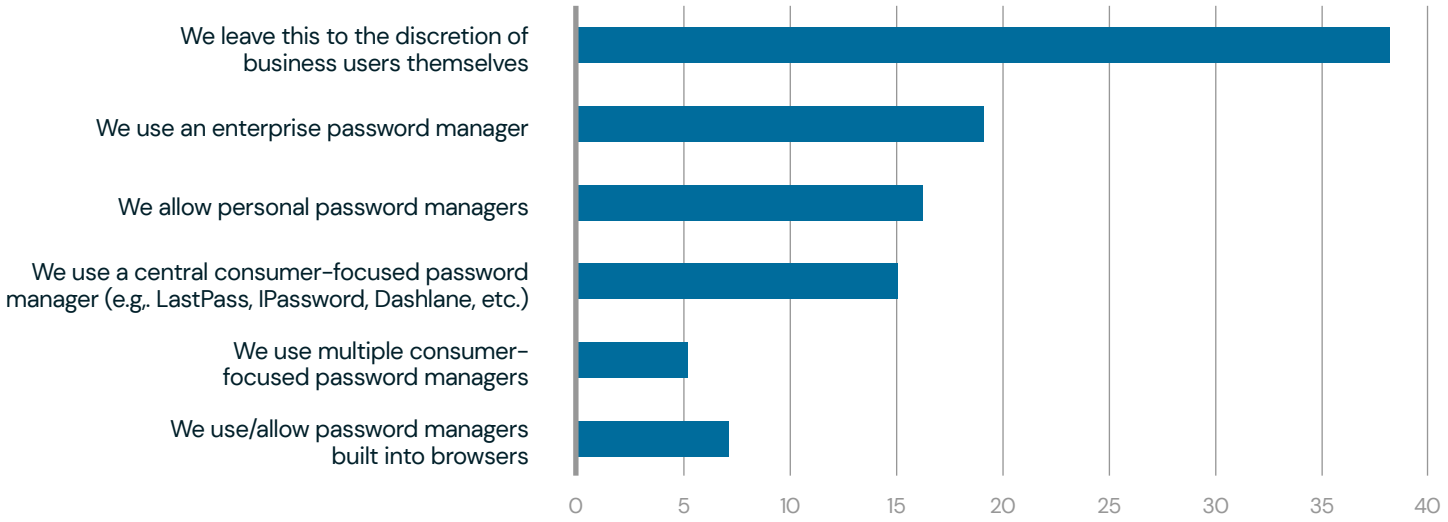
For 44% of respondents, more than six of the apps they access carry critical data – and more than 10 apps do so for 16% of respondents.

How many business applications that can't be integrated with an SSO solution does an average employee have? (e.g., social media apps, banking websites, shipping company portals, etc.)



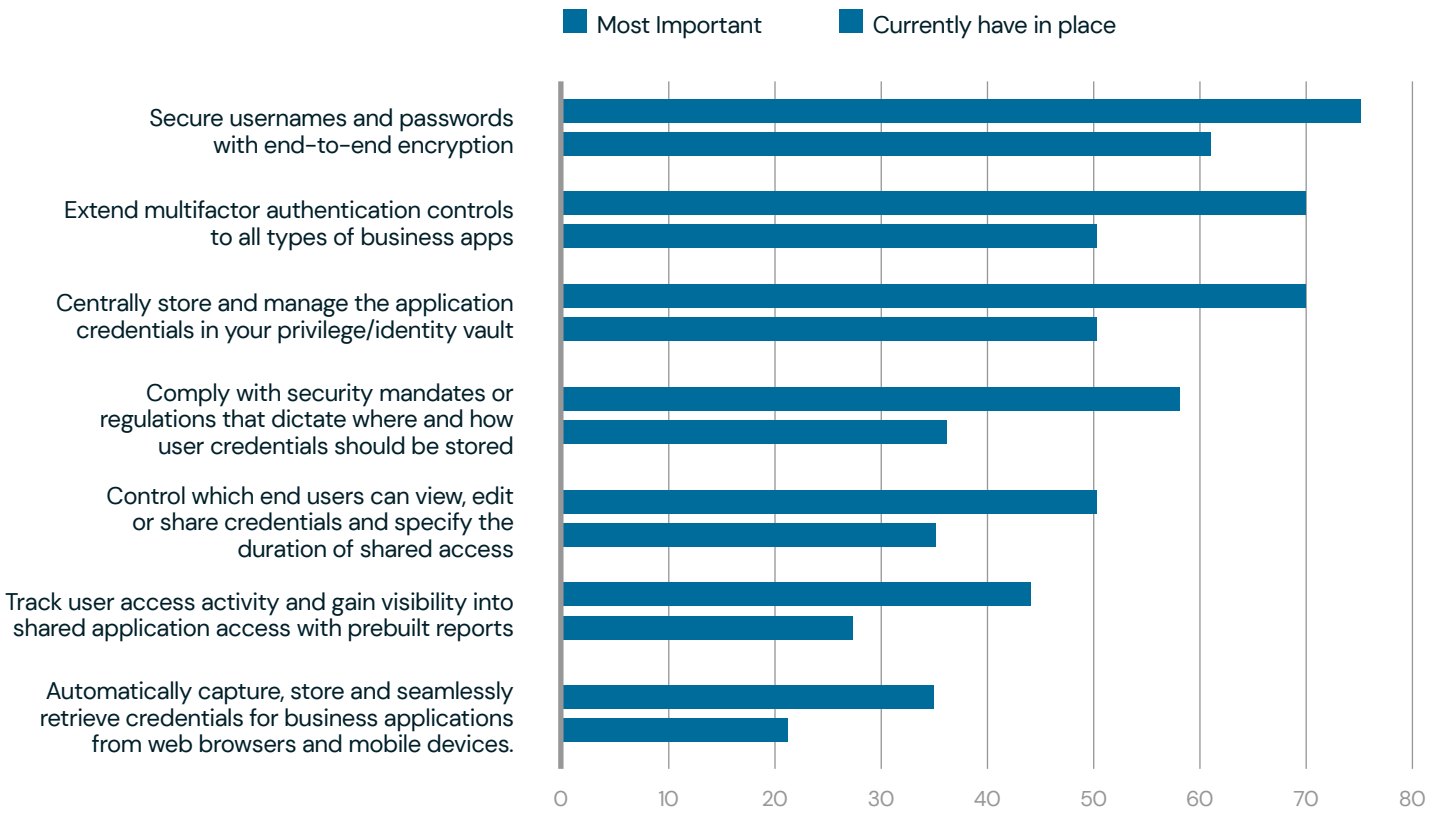
Thirty-eight percent of respondents report that six or more of their apps can't be integrated with SSO.

How do you store, manage, and share credentials for applications that can't be integrated with an SSO solution?



The most frequent approach to handling credentials for those apps not integrated with SSO – 38% – is to leave it to the discretion of users.

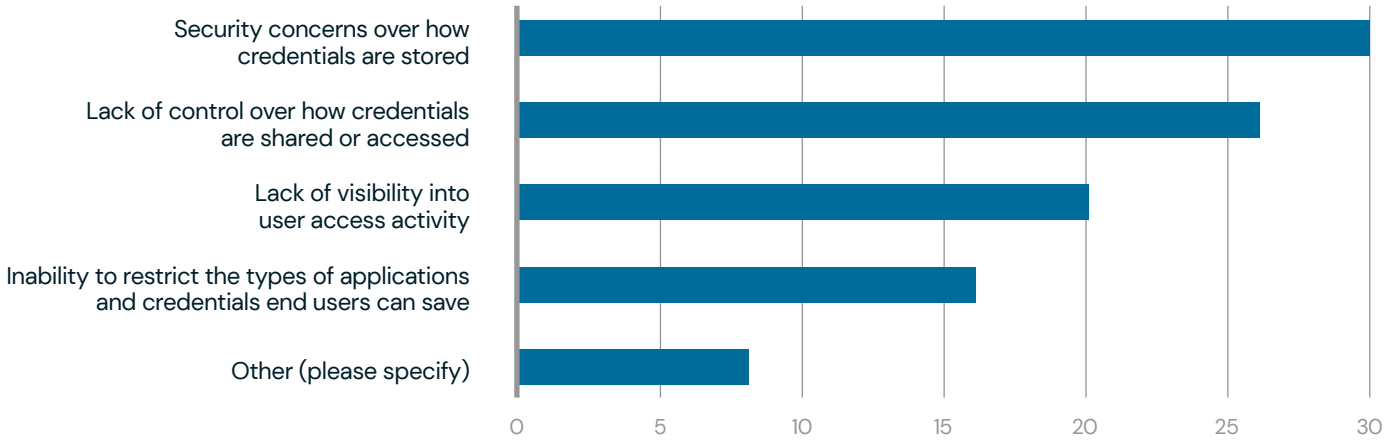
A: What's most important to you when selecting a password management tool?
B: Out of the following capabilities for password management, which do you currently have in place?



When selecting a password manager, end-to-end encryption of usernames and passwords is the most important feature at 75%, followed by extending MFA controls and central store and management of app credentials in privilege vault, both at 70%.

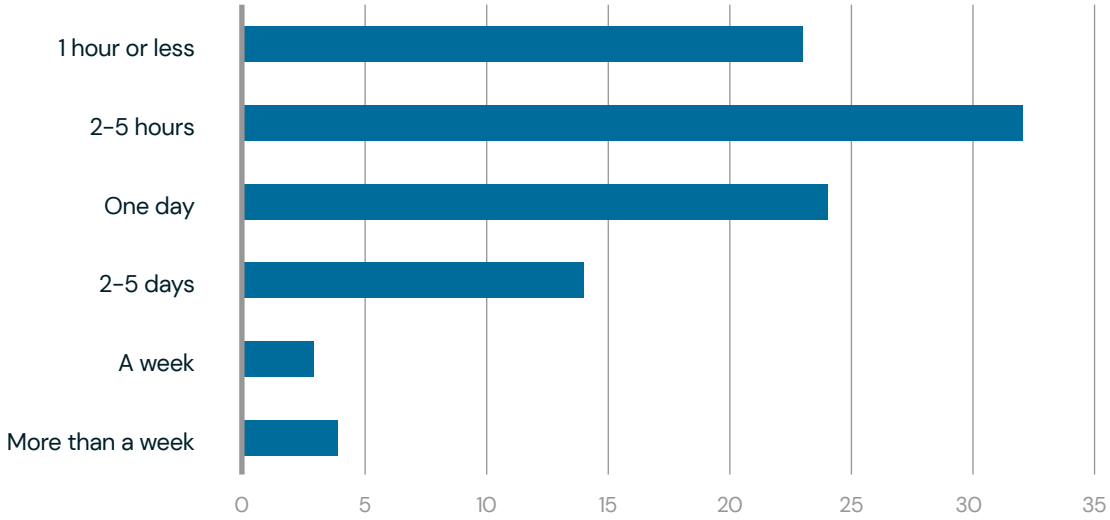
The most important features desired reflect the features in place, but desire for features is higher than actual implementation. End-to-end encryption of usernames and passwords tops the list at 61%, followed by extending MFA controls and central storage and management of app credentials in privilege vault, both at 50%.

What is your greatest challenge with the password management capabilities you have in place?



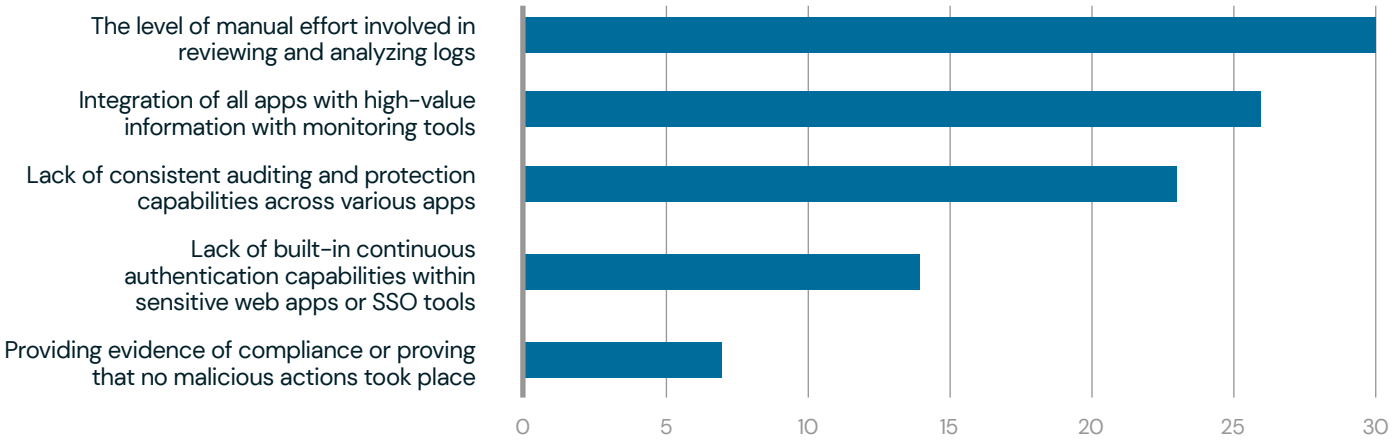
The top password management challenge is concern about how credentials are stored at 30%, followed by control over how they are shared or accessed at 26%.

How long does it typically take to determine exactly what transpired once a security incident or anomalous activity is discovered?



Seventy-nine percent of respondents say they fully understand a reported incident within a day, but 21% report up to a week or more to gain full understanding.

What is your greatest challenge with auditing and protecting web sessions you have today?



The level of manual effort involved is users' greatest challenge in audit at 30%, followed by integration of all apps with high-value information with monitoring tools at 26% and lack of consistent auditing and protection at 23%.

CONCLUSION

POOR PASSWORD MANAGEMENT

Passwords and credential management leap out as being poorly protected in many organizations, even in banking. The situation may have been exacerbated by the pandemic and working from home, but there is widespread use of consumer-grade protections in the enterprise, which can result in no visibility, control or policy enforcement.

LACK OF VISIBILITY

Lack of visibility includes both the likely extent of apps accessing critical information, and a failure to continuously monitor what is happening within those apps.

NEED FOR STRONGER CONTROLS

It is not that security professionals are unaware of the need for stronger controls, as their ranking of and wish list of features to implement is greater than the extent of controls in place. This suggests the issue is organizational prioritization and budgets.

It may be that the critical security role of passwords and credential management is not fully understood by the board, or there is complacency about current implementations. But if the security message has not got through, then given the foundational role of identity in establishing zero trust networks, perhaps CISOs should be making the board more aware of how the current gaps in their identity security might be compromising their compliance.

EXPERT ANALYSIS

KHIZAR SALTAN

Based on Interview with Khizar Sultan, senior director, IAM product and GTM strategy, CyberArk

BACKGROUND ON THE SURVEY

TONY MORBIN: Can you explain the background to the Securing Identity survey? Who were you targeting and what were you hoping to discover?

KHIZAR SULTAN: When we put the survey together, we were very much focused on hearing from enterprise IT professionals or IT professionals from different backgrounds all over the globe. Ultimately, we wanted to understand the risk as it pertains to things like workforce users' passwords, because we talk a lot about that here at CyberArk, and also about sessions within those workforce users' applications. Customers are asking us a lot about the new workplace and workforce scenarios that we have because a lot of people are working from home. There also have been significant changes in the way people interact with their day-to-day applications and their co-workers. The survey incorporates a lot of those questions that we have for those professionals.

STAND-OUT SURVEY RESULTS

MORBIN: The results are in now. What particularly stood out for you, and why do you think we saw that result?

SULTAN: The first thing that stood out to me was that passwords, credentials and secured items for a workforce user were definitely blind spots. Survey and freeform answers showed us that not only are passwords and credentials not being secured in the same way that we would secure something like a privileged user's credential, but in a very high percentage of cases, they are not being secured at all.

"Not only are passwords and credentials not being secured in the same way that we would secure something like a privileged user's credential, but in a very high percentage of cases, they are not being secured at all."

"One question was: How do you store and manage credentials for applications that don't integrate with something like an SSO application or an SSO tool? And the number one response was: We leave it to the discretion of the user."

I hope it was a wake-up call for those professionals. I was happy to see the honesty in their answers, but it definitely showed there were blind spots. We also saw surprising results about sessions and authentication for applications downstream for the workforce user.

SURPRISING SURVEY RESULTS

MORBIN: What did surprise you? Was there anything that you didn't expect to see?

SULTAN: I didn't expect to see the honesty. People are not saying they have all these protections and tools in place. One question was: How do you store and manage credentials for applications that don't integrate with an SSO application or tool? And the number one response was: We leave it to the discretion of the user. I can't imagine any security professional saying that out loud and letting users' hygiene and best practices be at play. We make sure our customers recognize that these products are not just nice to have but that they should have or must have them to make sure that they're protected as an organization.

PROBLEMS OF UNSECURED APPS

MORBIN: What conclusions do you draw about the number of unsecured apps that people have, and is that in line with what you see from your clients?

SULTAN: Based on the results – and this was in line with what we see in our usual conversations – more than half of respondents said that up to 10 applications are authenticated. People log into those applications via a password or a credential that they maintain. Good examples of these are social media accounts that the marketing team maintains, like Twitter, Facebook and LinkedIn. These don't plug into your SSO tool or integrate with the identity provider you have in place. Your marketing team not only maintains these credentials, but they also share them among each other because companies have social media teams.

There also are examples on the finance and operation sides. On the finance side, you would think that when it comes to a business's authentication into banking websites, they're completely logged in, using credentials. And I would hope that they're also leveraging multifactor authentication. But ultimately, the weak point in that authentication is the fact that the credential needs to be managed and secured. So, if organizations today are self-identifying that there are up to 10 applications like that, I can guarantee you that it's probably three or four times as many than what they have visibility into. You would imagine someone who works in IT doesn't have full visibility into everything that marketing is doing or everything that finance is doing. So 10 is really just the tip of the iceberg. That's something you need to start paying attention to.

CONSEQUENCES OF LOW VISIBILITY

MORBIN: Less than 20% said they had full visibility into web apps used, and 14% said they had none or almost none. Is that sustainable today? What are the likely consequences for those without visibility?

SULTAN: The term "visibility" can be defined in a variety of ways. It is generally assumed and understood that if I have purchased or I am using an enterprise-grade application for my business – it could be a CRM or a tool that you use in marketing for email campaigns – the visibility that application gives you is in the form of reporting and event logs. They'll let you know what actions a user took as they were within their session. But the amount of actions and activity that's not represented in that event log is enormous, and we can show you that sensitive or privileged actions oftentimes don't show up in the activity log.

Second, there are homegrown applications in the average organization stack. They're custom-built and used by the workforce. They oftentimes are operational applications that run the business. Think about a large retailer that has a warehousing application that they've built internally. That scenario exists across hundreds of businesses. The applications that were built internally oftentimes have no reporting. And if they have reporting, it's just administrative actions. It's not things that the user or the workforce user did. So visibility is a fallacy. You think that there's visibility there, but ultimately the user can use that application to conduct a variety of different actions and only a little bit of it is recorded. You think that you can go back and look at the logs to see what the user did, but oftentimes the logs are pretty bare.

NEED FOR CONTINUOUS AUTHENTICATION

MORBIN: Continuous authentication was an issue for most of the respondents, and they seem to find it pretty difficult. What problems can occur when people don't have continuous authentication?

SULTAN: Those who are working from home oftentimes don't respect the same type of IT perimeters. I don't lock my computer when I go to the bathroom because there's no one else here; it's just me. This type of bad hygiene starts getting developed at home. Eventually, many of us will go back to an office, but the things that we were taught when we were working in an office have evaporated in the grand scheme of things. Continuous authentication and zero trust – everyone has been promoting those policies inside of your organization for many years. You have to protect the user when they're not thinking about ways in which they should be protecting themselves. That's the number one thing.

Continuous authentication is there to make sure that someone locks that machine and reauthenticates that user. And that someone is essentially the vendor in place, the security solution. It's someone who is there to look for risky behavior and scenarios where a machine has been left untouched. If there's a session that's open and that's privileged or sensitive, that person will block access for anyone that might be walking by. That's the basics of it, but continuous authentication goes way beyond that too. You can block copy and paste or downloads from taking place, and you can challenge the user for a multifactor prompt.

Little bits of security go much farther than a bunch of security upfront. It's important to stay involved in the user session throughout the day versus just

"Little bits of security go much farther than a bunch of security upfront. It's important to stay involved in the user session throughout the day versus just making the user do a bunch of steps to get into their machine and then keeping it open from there on."

making the user do a bunch of steps to get into their machine and then keeping it open from there on. Oftentimes, it's easier for the user to consume because it's happening in little bites versus trying to change everything about the user's behavior at the get-go.

UNMANAGEABLE PASSWORD MANAGERS

MORBIN: Only 14% of respondents said they used a third party, enterprise-grade password manager. Is that a cause for concern? Or maybe the variety of circumstances means that there are alternative valid options being used?

SULTAN: There were two things that stood out in that question. One was that the biggest response answer was that they leave it to the discretion of the users. The other responses were more centered around whether they have a solution in place or allow users to use something. That tells me that either they've purchased a solution and rolled it out to their end users or they allow the end users to bring tools from home, which is the most common scenario. Things like password managers from home use get brought into work and all the lines get blurred. Everything is kept in one location. A lot of times there's password reuse, which is the biggest threat to a lot of organizations when it comes to passwords.

The passwords that I use at home become the passwords that I use at work because one strong password is about as much as a user can memorize, but that one strong password could easily be compromised in a personal, consumer-oriented breach. And that trickles down to your work scenario. So personal password managers are good, but it would be great if they were sanctioned and rolled out by the organization itself. The survey results show that that only about 20% of organizations have something like that in place. And they may not even have visibility into who else is using it.

What also stood out to me was that respondents openly said that they were using consumer-grade solutions for their enterprise passwords. That means that they have no visibility, control or policy enforcement. It's not plugged into their SSO, identity provider or directory. And you know what? Workforce users, like employees, leave companies eventually. Not everybody works at one place forever. And if I leave, I take those passwords and all the folders of credentials with me. I also don't get offboarded in a succinct manner. These scenarios add up to the larger threat. We try to make sure that our customers can take action on the things that will have the biggest impact over time.

SURVEY TAKEAWAYS

MORBIN: What is your key takeaway from the survey as a whole?

"Think about users that have access to sensitive information and ... then think about protecting their passwords and credentials. As they access applications, see what those applications are. Then look at some ways in which you can protect the user session."

SULTAN: The amount of discovery that questions like these can open up for an organization is important. So, if you are being asked about passwords and credentials for the first time, it's certainly been a blind spot for you. And it goes beyond just the IT department and the security teams, who oftentimes already have tools and solutions in place for privilege credentials or their developers and what they consider to be high-value individuals and applications. Those are typically always covered by IAM solutions and other solutions that exist for secrets management.

Privilege is everywhere. We can look at customer information. I work closely with the sales team, so I have access to our CRM, which allows me to see the contract for every customer globally. If we acknowledge that we have privilege, then we can think about ways to add protection into our day-to-day use of applications and resources. We don't necessarily have to put every single user into a tool. Think about users that have access to sensitive information and high-value data and then think about protecting their passwords and credentials. As they access applications, see what those applications are, what type of reporting is available to you, and if and when you need to do an audit. Then look at ways in which you can protect the user session, get more visibility, and have better tracking and strong authentication along the way.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center Princeton, NJ 08540 www.ismg.io