CYBERARK®
The Identity Security Company

2023 Identity Security Threat Landscape Report

Cyber debt builds while AI tools, employee churn and economic pressures fuel the identity attack surface.

Table of Contents

Executive Summary

Levels of cyber debt — where investment in digital and cloud initiatives outpaces cybersecurity investment — in organizations around the world are at risk of compounding, driven by an economic squeeze, elevated levels of staff turnover, a consumer spend downturn and an uncertain global environment.

With business leaders continuing to drive digital acceleration to unlock greater efficiencies, it is a precarious position to be in. Cybersecurity professionals must grapple with highly complex IT environments and exponential — but often insecure — identity growth.

Our new report examines how the interplay of all these factors will result in increased attacker opportunity. Indeed, as adversaries embrace artificial intelligence (AI) to enhance and scale their identity-based attacks, security teams are being asked to do more with less as budget cuts widen existing skills and resource gaps.

The results from our global survey of 2,300 security decision makers demonstrates the longtail effect of today's cybersecurity decisions on future business outcomes, offering data-driven insights to help inform prioritization strategies and amplify security impact.

We believe that by placing identity at the heart of a Zero Trust cybersecurity approach, following a risk-based strategy to secure critical assets and leaning on the expertise of trusted partners, organizations will be best positioned to weather the current storm, minimize risks and face the future with confidence. The question of who and what to trust is now at the forefront of preventing cyber debt compounding. Stakes are high and because of this we see customer-driven initiatives to consolidate trust, where organizations aim to focus operations with a smaller set of partners to build long term resilience.

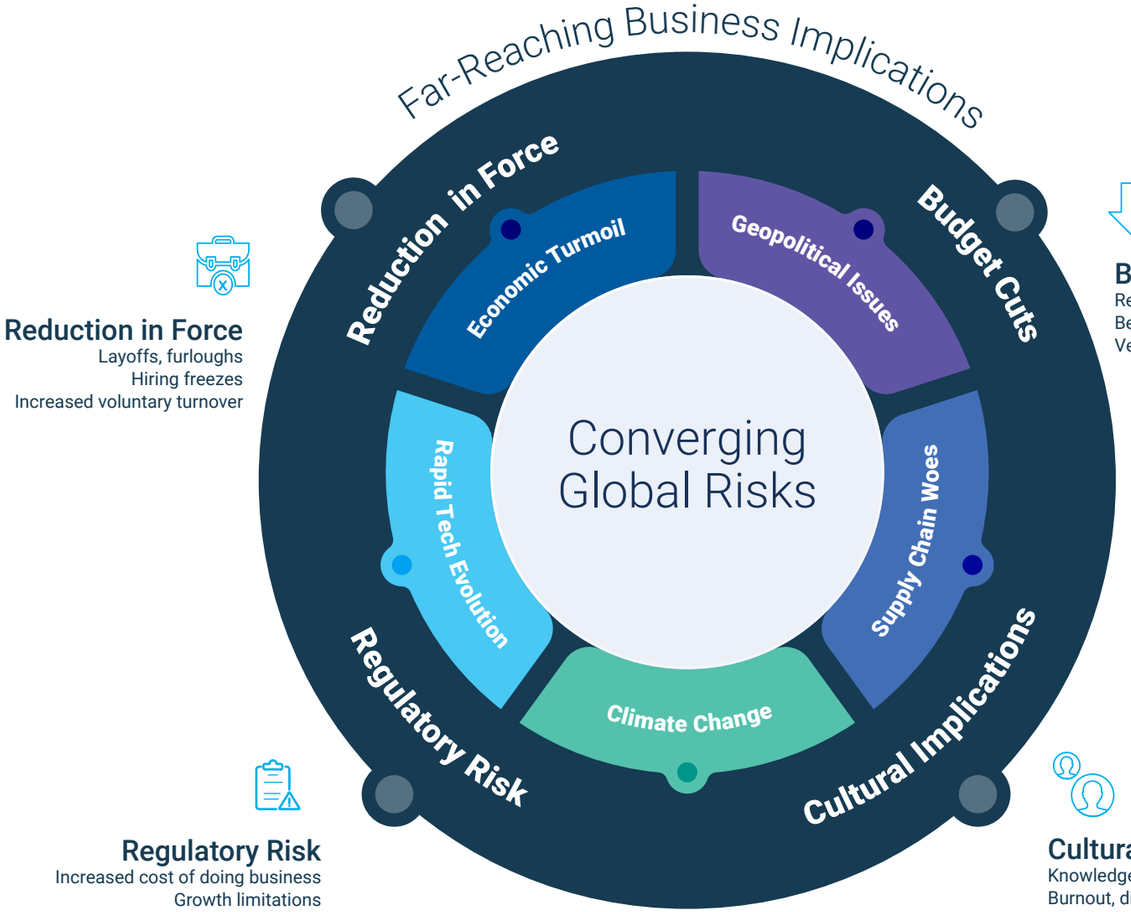
Clarence Hinton
Chief Strategy Officer, CyberArk

Virtually all (99%) respondents agree that they'll face an identity-related compromise in the year ahead. 58% say this will happen as part of a digital transformation initiative such as cloud adoption or legacy app migration.

Digital or Die

After COVID-19 compressed years of digital transformation into a few months, many organizations kept their foot on the gas. Digital and cloud investments continued to outpace cybersecurity spend despite a surge in new identities, new environments and new AI-fueled attack methods that increased risk and burdened security teams.

Now, reality is sinking in as converging global events force a sharp decline in consumer spending and a business reset of everything from strategy to staffing.



Reduction in Force
Layoffs, furloughs
Hiring freezes
Increased voluntary turnover

Budget Cuts
Reduced goods, services, inventory
Behavior changes
Vendor negotiation

Regulatory Risk
Increased cost of doing business
Growth limitations
Profit losses, weakened ROI

Cultural Implications
Knowledge loss
Burnout, disengagement
Innovation lag

Technology adoption continues at pace. In 2023 alone, this will drive:

2.4x

growth in human & machine identities

68%

increase in SaaS tools deployed

Q: Over the next 12 months, we expect the total number of identities (i.e., both human and machine identities) under management to approximately (banded options, 2,300 respondents)

Q: Approximately how many Software as a Service providers does your organization leverage today and in the next 12 months (2,300 respondents)

Enterprise Technology Adoption Persists

Despite cutbacks, IT initiatives involving cloud services and tools, automation and DevOps remain priorities as leaders seek to unlock new efficiencies from the front office to the back.

Every new SaaS app deployment, third-party service or cloud-based initiative creates new digital interaction points between people, applications and processes. An identity is required at each of these steps to authenticate the human user or machine involved. The sustained pace of digitization means respondents expect identities to more than double in 2023 and — per our 2022 report – there are 45 machine identities for every human identity. Respondents say that nearly half (45%) of these machine identities will have access to corporate sensitive data and any identity — human or machine — could be compromised and used to unlock higher levels of privileges to access critical assets.

Respondents say that their organizations use 75 SaaS applications on average today. In the next 12 months, they expect this number to increase by 68%. In many cases, legacy applications that only support password-based authentication will remain in the mix. Without a critical multi-factor authentication (MFA) layer, these applications are easy ingress points for attackers on the hunt for identities, and 75% of respondents say they are faced with significant levels of risk from apps in their environment that only support password-based authentication.

Identity Security Cracks Begin to Show

As rapid identity growth continues, cracks are beginning to show. Sixty-three percent of security decision-makers admit that the highest-sensitivity access for employees in their organization, such as IT admins and other privileged user accounts, is not adequately secured today. Organizational turmoil in the shape of sudden and widespread layoffs may exacerbate this problem.

Is it possible for cybersecurity teams to keep up as unaddressed risks push organizations further into cyber debt? The data suggest that without a major course correction, that is unlikely.

68% expect layoffs and workforce churn to create new security issues, while nearly **one-third say cybersecurity skills gaps hinder security** defences.

63% admit that highest-sensitivity access for employees is **not adequately secured**.

Q: Which of the following is true for your organisation in 2023? (2,300 respondents)

Q: To what extent do you agree or disagree with the following statements? (2,300 respondents)

Identity: The Heart of It All

Modern IT environments are dynamic and unconstrained. Instead of rigid network perimeters, identities are the first and last line of defense against malicious actors and unauthorized access.

But it's a demanding job to manage an ever-growing identity portfolio — across physical and virtual endpoints, devices, cloud workflows and SaaS solutions — while making sure users can securely access resources at the right time, no matter where they are or what devices they use.

Often understaffed, under-resourced and charged with protecting a rapidly growing identity portfolio, security decision-makers cite growing challenges across six distinct areas of identity security risk:

74% of respondents are **concerned about confidential information loss** stemming from employees, ex-employees and third-party vendors.

1. People

Humans are always a security wildcard. Add in flexible work, increased churn and recession-driven outsourcing, and the "people problem" becomes even more pronounced. Seventy-four percent of respondents are concerned about confidential information loss stemming from employees, ex-employees and third-party vendors. They point to third parties (partners, consultants and service providers) as the riskiest human identities that security teams have to deal with.

2. Workforce upheaval

Sixty-eight percent of respondents say layoffs and higher levels of employee churn will create new security issues. For example, 58% report instances of exiting users saving sensitive or confidential work documents outside of policy. Every time an employee leaves, the IT team must remove access permissions from the various applications they used. Malicious actors (sometimes former disgruntled employees) count on things slipping through the cracks during manual offboarding processes. One wrongly provisioned, overprivileged or orphaned account is all they need.

62% of **security teams** operate with **limited visibility** across their environment.

No.1

Business-critical applications top the list of at-risk systems.

3. Machine identities

Due to increasing IT complexity, 62% of security teams operate with limited visibility across their environment. This makes it difficult to understand not only who is accessing sensitive data and assets but also what they are accessing. Last year, we learned machine identities outnumber human ones 45:1. There's a pressing need to secure them all and secure them fast, yet doing so without impacting users is a tricky balancing act. Forty-two percent of respondents agree that managing and securing both human and machine identity types is equally difficult. This may be why 65% either took steps to protect machine identities last year or plan to do so in the next 12 months.

4. Business systems

When considering the IT environments where unmanaged and unsecured access is most prevalent, 42% of respondents say business-critical applications top their list of at-risk systems. Yet more than half of all respondents admit that identities are unmanaged and unprotected in revenue-generating customer-facing applications, enterprise resource planning (ERP), customer relationship management (CRM) and financial management software. This isn't even the worst-protected environment: only 25% of respondents say sensitive access to bots and robotic process automation (RPA) is secured. Since more than half of all identities have sensitive access to high-value data or services, often through SaaS applications and automated processes, these findings are particularly concerning.

5. Software development

With a need for speed and flexibility, software developers are often given more access than required — especially in lean times when rapid innovation is key to survival. Perhaps security teams don't have bandwidth to handle continuous access requests or developers are applying extra pressure. Regardless, 77% of respondents say developers have too many privileges — making these human identities highly attractive targets. Thirty-eight percent say the development realm is where unknown, unmanaged identities create the most risk.

6. Identity security toolsets

Security professionals' jobs are further complicated by a patchwork of heterogeneous tools from various vendors, creating identity security gaps in some areas and inefficient overlaps in others. Sixty-seven percent of respondents say they currently use tools from up to 40 different identity security vendors — underscoring a need for greater interoperability and vendor consolidation.

77% of respondents say developers have too many privileges — making these human identities highly attractive targets.

The 2023 Attack Surface Reflects Unaddressed Identity Risks

Security decision-makers' top concerns and recent experiences reflect the turbulent times. They also suggest that unaddressed (and fast-accumulating) cyber debt, where security investment lags behind broader business initiatives, is starting to catch up with organizations.

Credential theft has always been an attractive target for adversaries. Rapid digitization makes credential compromise even more alluring by creating a virtually endless supply of identities to target.

Stealing or abusing credentials to compromise identities (via phishing, social engineering or other tactics) is how most breaches begin and where cybersecurity professionals struggle the most. It's also one of the areas of risk that AI will heighten in 2023 (via chatbot security vulnerabilities or AI-powered credential compromise), according to respondents.

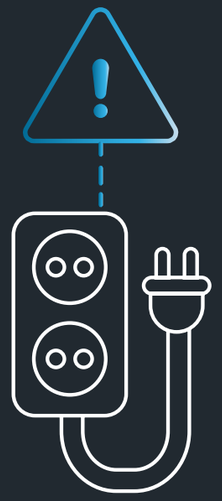
Poor password practices — from consolidating SaaS app logins in browsers to hard coding credentials — aggravate this problem and expose sensitive data. Even if users' credentials are managed, it doesn't necessarily mean they're secure. The vast majority of respondents — eighty-five percent — are growing increasingly concerned about the risk of security incidents involving standalone password managers. A string of high-profile breaches affecting these tools likely influenced the 87% who plan to explore enterprise-focused alternatives in the next 12 months.

No.1

Credential theft remains the number one concern for cybersecurity professionals.

89%

indicate their organizations were **targeted by at least one ransomware attack in the last 12 months** (97% for healthcare, the most-targeted sector).



59%

say they **would not be able to protect against an attack stemming from a successful compromise of a software supply chain provider**. The energy and utilities sector — which is often critical infrastructure — is the vertical most "at-risk," with 67% saying they could not stop an attack of this type.

Financial hardship, uncertainty and inadequate cybersecurity investment create a perfect storm for ransomware.

Our last report found that organizations experienced two successful ransomware attacks on average in the previous year. This year, we focused on responses to successful attacks. Nearly three-quarters of organizations paid ransoms at least once in the last 12 months, suggesting that attackers are turning up the heat and signaling that firms were likely victims of double extortion campaigns.

Consider the impact on insurability: 42% of organizations got a 2023 cyber insurance policy at a higher premium than last year.

In our software-led world, supply chains are increasingly intertwined, making it feasible for attackers to compromise multiple supply chains in their entirety to increase ROI.

In 2023, threat researchers definitively identified a cascading supply chain attack for the first time. Still, 56% of organizations have not taken steps to further secure their software supply chain in the last year as they are still in the designing or refining stage of their DevSecOps journey.

The report found that AI will be a double-edged sword in 2023. On one hand, the prospect of AI-enabled threats are top-of-mind for security professionals in 2023, with better than nine out of ten expecting AI to drive negative cyber impact in 2023. But nearly all are making use of AI to bolster cyber defenses in their organization as well.

In addition to the threat of AI-enabled malware (the perceived number one threat), 62% say company employees use unapproved AI-enabled tools that can increase security risk. It's on security teams to deal with exposure while ensuring they're not seen as barriers to innovation.

Generative AI tools, which have opened a Pandora's box of unprecedented technological possibilities across industries, are a particular security concern. Cybersecurity researchers have demonstrated numerous ways AI could be used maliciously, such as creating polymorphic malware or writing highly convincing phishing emails at scale.

93%

expect **negative cyber impacts** from AI tools in 2023.

98% of cybersecurity professionals use AI in some capacity.

Automation/ flexibility	47%
Breach detection/ prevention	43%
Skills/resource shortages	41%

The Path Forward

Not all is doom and gloom. Our survey also uncovered reasons for optimism. Sixty-nine percent of organizations are moving ahead with planned cybersecurity initiatives in 2023, a testament to their leaders. They realize the short-term cost savings provided by reduced cybersecurity spending will likely be eclipsed by breach-related damages and soaring insurance costs that ultimately hinder growth. They know that when facing inevitable tradeoffs, focus mastery can amplify the positive impact of security tools and strategy. They understand that by concentrating on mitigating identity-centric risk today, they're addressing their enterprise's largest attack surface head-on and paying down their cyber debt.

According to our research, several crucial identity security initiatives remain on priority lists, highly valued for addressing both security and operational requirements of:

Attack Surface Reduction

Identity misconfigurations abound in hybrid and multi-cloud environments, and periods of workforce turnover make this problem even worse. Fortunately, most organizations are automating access provisioning and deprovisioning to shrink the attack surface, clean up misconfigured and unused access permissions and reduce risk exposure.

28%

automated access provisioning/ deprovisioning in 2022 and 31% plan to this year.

Zero Trust Alignment

Identity security is critical for a robust Zero Trust implementation. To protect a broader range of human and machine identities and move forward with a "trust nothing, verify everything" approach, surveyed organizations either expanded the following privilege controls last year or plan to this year:

- **Least privilege access** on infrastructure that runs business-critical applications (31% did so in 2022, 32% plan to in 2023)
- **Just-in-time access** for operations that don't require credentials with 24/7 access permissions (32% in 2022 and 32% in 2023)
- **Local admin removal** on endpoints to prevent privilege escalation (32% in 2022 and 28% in 2023) and block ransomware and other threats
- **Standing access removal** across third-party vendors (29% in 2022 and 28% in 2023) and in their public cloud environments (29% in 2022 and 28% in 2023)

High-value Asset Protection

It's encouraging to see so many companies making extra strides to safeguard sensitive data and systems, but there's still room for growth. Only 47% use risk management-based considerations when evaluating asset sensitivity today. Because security teams can't tackle every threat at once, a risk-based approach is crucial for driving better decisions and outcomes.

Consolidation of Trust

Cybersecurity can't be done in a vacuum – it's a team game. Outside perspectives can help validate and strengthen strategies during times of change, while helping organizations create winning roadmaps for the long run. Further, many respondents (42%) intend on consolidating cybersecurity efforts with existing partners in 2023, extending what they have versus adopting new point solutions.

Identity management (79%) and **endpoint security/device trust (78%)** are "critical" or "important" to supporting Zero Trust.

51% look to trusted cybersecurity vendors to help forecast and design solutions for future cyber risk.

Conclusion

Despite the current challenges, there is a secure and surmountable path forward for forward-looking organizations. By focusing on the most critical areas of risk and acting now versus pushing things further down the line, organizations can avoid levels of cyber debt compounding and move forward with confidence.

About The Report

The CyberArk 2023 Identity Security Threat Landscape Report represents the findings of a worldwide survey across private and public sector organizations of 500 employees and above. It was conducted by market researchers Vanson Bourne amongst 2,300 identity security decision makers. Respondents were based in Brazil, Canada, Mexico, the US, France, Germany, Italy, the Netherlands, Spain, the UK, Australia, India, Israel, Japan, Singapore and Taiwan.

The CyberArk 2023 Identity Security Threat Landscape Report

www.cyberark.com

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow us on Twitter via @CyberArk, LinkedIn or Facebook.

U.S., 06.23 Doc: TSK-4110

CYBERARK®
The Identity Security Company