2023 Cybersecurity Year in Review:

SEC ruling, AI and ransomware raise security stakes

Sponsored by

RSAConference™

CRA Business Intelligence
A CRA Resource

SC Media
A CRA Resource

Contents

Introduction

The year 2023 saw three significant events that raised the stakes for cybersecurity professionals:

1 **In July, the U.S. Securities and Exchange Commission adopted new rules that require publicly traded companies to notify regulators within four days of a meaningful system compromise, and to give details about their cybersecurity risk governance in annual public filings.**

The rules are being phased in from December 2023 to July 2024, but have met with some flak in Congress, where a bill in both chambers seeks to defang the new rules.

Meanwhile, a ransomware group used the new regulations in November to "report" an alleged victim to the SEC, despite the rules not yet being in effect. Some security experts worry that such criminal reporting could become a standard extortion tactic, and another argues that the new SEC rules help investors rather than companies or CISOs.

2 **The world became transfixed by the potential power of ChatGPT and artificial intelligence, and it wasn't long before practically anyone could use ChatGPT to write phishing emails and rudimentary malware.**

By November 2023, it became clear that the best way to fight AI-powered adversaries was to use AI in defense. The White House issued an AI executive order increasing federal oversight of rapidly expanding AI systems and promoting the safety and security of AI development to reduce its risks for consumers and national security. The U.S. and the U.K. also issued joint AI security guidelines that were endorsed by 16 additional countries.

3 **Ransomware set new records for monthly incidents and nearly topped previous yearly payouts. The resurgence was accompanied by a breakdown in international cooperation to fight cybercrime, as tensions rose over the stalled but ongoing Russian invasion of Ukraine and U.S.-China relations deteriorated.**

The Russian foreign intelligence service's Cozy Bear threat actor, aka APT29, increased its espionage activities and the head of the FBI said that Chinese economic cyberespionage and theft of intellectual property posed an "unprecedented threat" to innovation.

In response to these threats, cybersecurity buyers, vendors, influencers and decision makers worked to improve their practices around ransomware prevention, privacy and third-party risk, vulnerability management, cloud security, and identity and access management. However, respondents in several CyberRisk Alliance Business Intelligence surveys reported more than a few challenges in meeting these goals.

The SEC's rule change and the AI executive order signaled greater U.S. government involvement in private-sector cybersecurity. The SEC also brought fraud charges against SolarWinds over the 2020 supply-chain hack of its Orion network-management software, and the Federal Trade Commission more zealously enforced its privacy-breach rules, both of which we examine in more detail in the following pages.

The potential power of AI looms over all aspects of cybersecurity. While its impact upon both attackers and defenders was more theoretical than actual in 2023, the upcoming year may see real-life examples of AI-augmented threats and protective measures, especially with regard to ransomware and vulnerability management, as explored below.

Ransomware surges, despite aggressive defenses

After a downturn in attacks and payouts in the previous year, ransomware roared back in 2023, with a near-record haul of $450 million midway through the year and an all-time monthly high of 514 reported incidents in September.

The highest-profile ransomware incident of the year was the September attack on MGM Resorts, which reportedly encrypted more than 100 hypervisors and forced the company to shut down its nationwide computer network, incurring an estimated $100 million loss.

The same attackers, the Scattered Spider group, also hit rival gaming giant Caesars Entertainment, which chose to pay a $15 million ransom. As of mid-November, the FBI was catching heat for not making any arrests despite apparently knowing the identities of the attackers, who seemed to be mostly English speakers living in Western countries.

A trend with greater impact was the continuous onslaught upon health-care providers, which had no respite from ransomware attacks. Attackers became crueler in 2023, hitting cancer centers, threatening to release patient information, knocking the Prospect Medical Holdings hospital system offline nationwide and hitting 30 hospitals across six states on Thanksgiving weekend. A new report showed what health-care providers have long feared: Ransomware attacks slow the pace of patient treatment and lead to hospital overcrowding, increasing risks for patients with time-sensitive emergencies such as strokes and heart attacks.

An October 2023 CyberRisk Alliance Business Intelligence survey of 218 North American security and IT leaders found that 19% had suffered a ransomware attack on their organizations within the previous 24 months. However, none said they had paid the ransoms. A third of the non-payers said backups saved their data, 24% said the lost data wasn't important, and another 24% said they resolved the issues on their own.

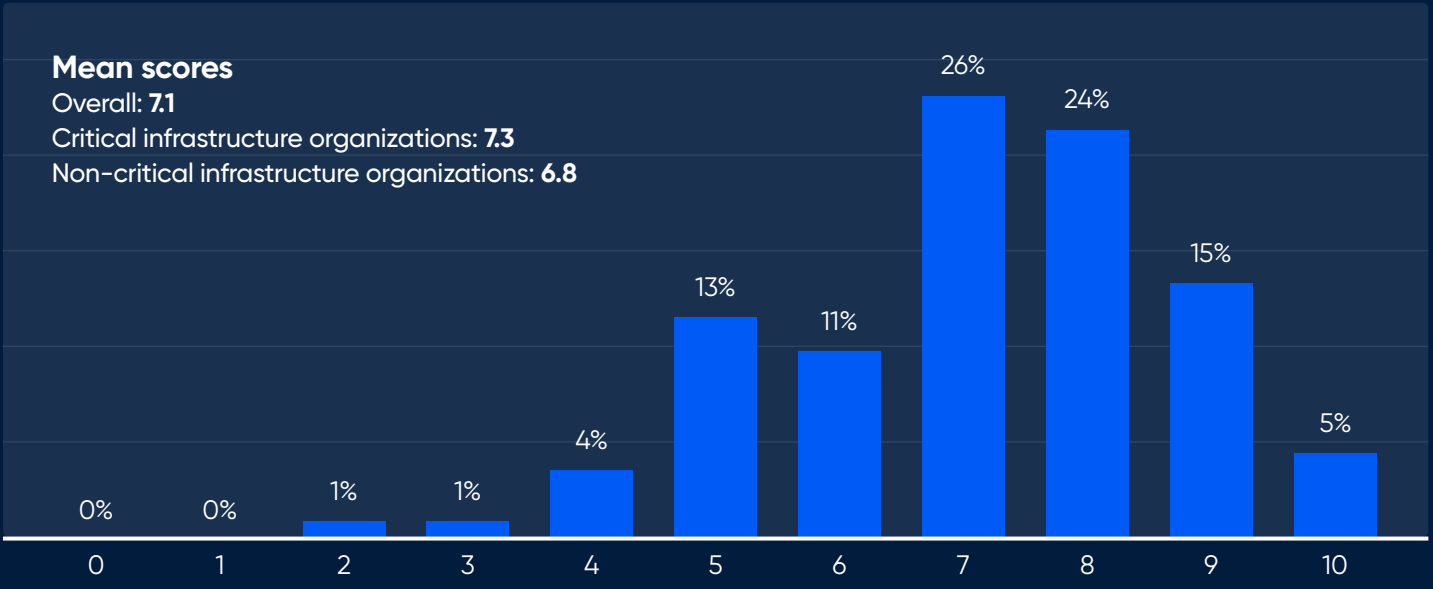
Overall, organizations have growing confidence in their ability to respond to ransomware attacks. Seventy percent of survey respondents had "moderate to high levels of confidence" in their companies' abilities to handle ransomware attacks, and 79% said they had mostly or fully completed secure backups of critical data.

"We implemented ransomware protection tools from third-party vendors, and we have a dedicated team to monitor threats regularly," said one survey respondent. "Our confidence level is high based on the precautionary measures we take."

> "We never missed an order. We never missed a delivery. Customer data was not compromised. … Probably 95% of the organization had no idea that we were under attack."
>
> *— Brian Balzer, EVP of Digital Technology & Business Transformation, G&J Pepsi-Cola Drink Bottlers, Inc.*

Ransomware detection and response confidence score

Overall, what is your confidence that your organization can detect/respond to a ransomware attack before it's too late?



Base: All respondents (n=218).
Note: Respondents were asked to select a rating on a scale of 0 to 10, where 0 is 'Not at all confident' and 10 is 'Extremely confident.'
Source: CyberRisk Alliance Business Intelligence (CRA BI), Ransomware Survey, October 2023.

That confidence may be essential if and when the SEC's new four-day reporting rule goes into effect. Publicly traded companies will need to prepare incident-response strategies and templates that enable quick information-gathering and report generation to meet the SEC deadline.

Unfortunately, organizations in sectors hit hardest by ransomware, such as healthcare and education, often have ineffective security safeguards. Few educational institutions are publicly traded companies, but we may see a record number of breach-related SEC penalties levied against healthcare providers in 2024.

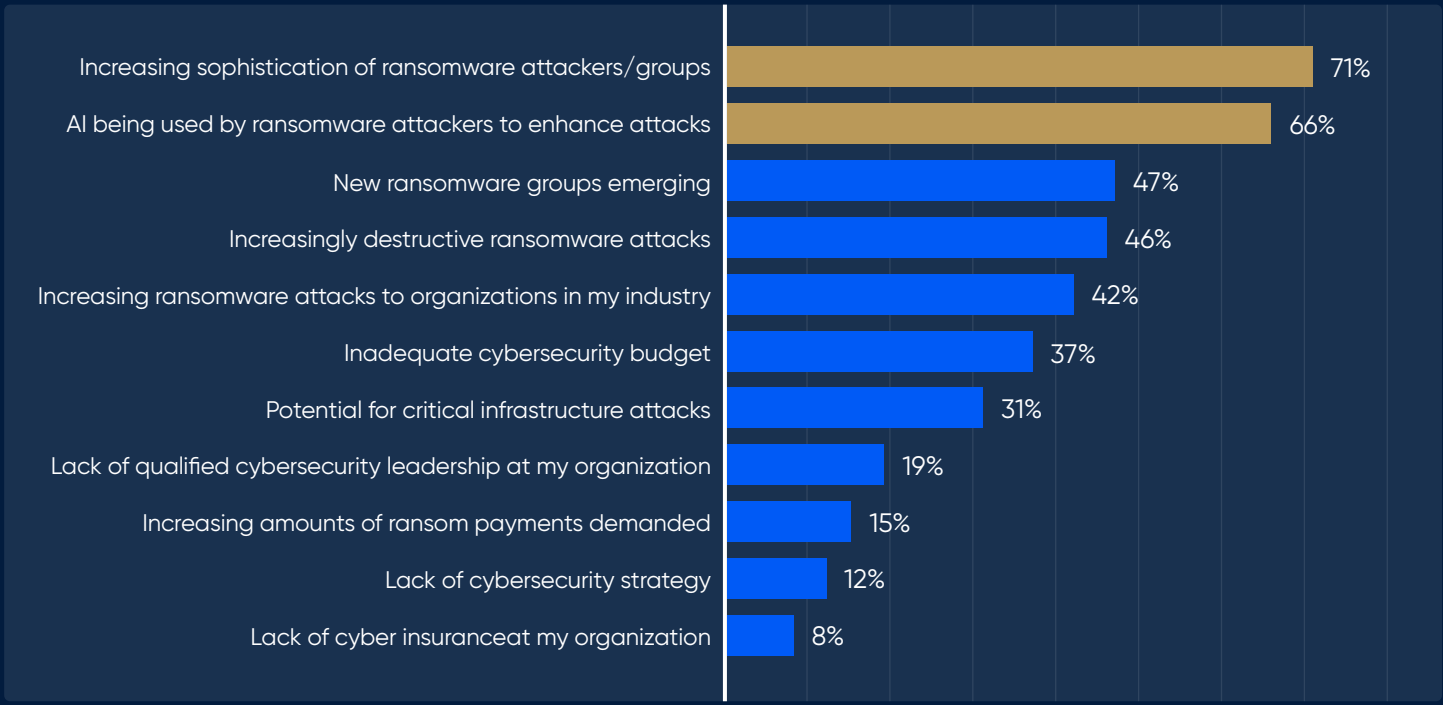
Weekly backups, cloud deployment and strong executive support were what let an Ohio bottling company recover from a ransomware attack in only seven hours, its security chief told a Cybersecurity Collaboration Forum CyberRisk Leadership Exchange conference in Cincinnati in June 2023.

"We never missed an order. We never missed a delivery. Customer data was not compromised," said Brian Balzer, Executive VP of Digital Technology & Business Transformation at G&J Pepsi-Cola Drink Bottlers, Inc. "I'd say probably 95% of the organization had no idea that we were under attack."

Rapid developments in AI may shift the high ground back to attackers, however. In the CRA survey, fully 66% of respondents listed AI aiding attackers as one of their top five ransomware concerns. When asked specifically about AI, 83% were moderately or very concerned that AI might enhance ransomware attacks, although 71% thought that AI might help defend systems, too.

Top concerns about potential ransomware attacks

Overall, what are your top concerns related to the potential for ransomware attacks to your organization in the next 12 months?



Base: All respondents (n=218).
Note: Respondents were asked to select up to 5 choices.
Source: CyberRisk Alliance Business Intelligence (CRA BI), Ransomware Survey, October 2023.

2024 to-do list:

- Develop a plan for AI's impact on ransomware, including both how to counter AI-assisted attacks and how to incorporate AI into your defenses.
- Develop rapid-response procedures to enable quick SEC reporting following a ransomware incident.
- Healthcare organizations should put more resources toward cybersecurity.
- Educational institutions should take advantage of cybersecurity-improvement programs such as the U.S. Department of Education's K-12 Digital Infrastructure Brief and free offerings from Amazon, Cloudflare and Google.

Third-party apps and other privacy threats

The health-care sector also dominated the bad news about third-party applications in 2023, as breaches of patient information made headlines, U.S. federal regulators beefed up enforcement and legislators took notice.

The Federal Trade Commission fined digital-health provider BetterHealth $7.8 million, online-prescription service GoodRx $1.5 million, and fertility app Premom $100,000 for sharing patient information with Facebook, Google and other advertisers.

U.S. senators questioned three other telehealth providers about similar allegations, and one, Cerebral, admitted sharing the data of about 3.2 million patients with third parties. Along similar lines, the FTC moved in June to update its Health Breach Notification Rule so that developers of healthcare applications would be required to post notifications of data breaches.

But the breaches kept coming. In July, data of 11 million patients was stolen from HCA Healthcare after email-formatting software was compromised. In October, medical transcription service provider Perry Johnson & Associates said 9 million patients had had their information compromised.

A study found that 99% of hospital websites used tracking code that funnels patient data to third parties, and the U.S. Department of Health and Human Services said many health-care organizations were still struggling to comply with HIPAA's Security Rule, despite the fact that the rule went into effect 17 years earlier.

The SolarWinds supply-chain hack of 2020, which led the SEC to charge the company CISO with fraud in October, seems to have inspired North Korean state-sponsored hackers. Over the course of 2023, Pyongyang was tied to supply-chain hacks of 3CX VoIP software, of the JumpCloud cloud-directory-provider, of the Zoho ManageEngine ServiceDesk, of VMConnect, and of CyberLink media-playing software.

Ironically, SolarWinds' quick SEC notification about the hack would likely have met the four-day reporting deadline had the attack taken place in 2024. Publicly traded companies such as HCA Healthcare will need to keep the new SEC reporting rules, along with the more stringently enforced FTC regulations, in mind going forward.

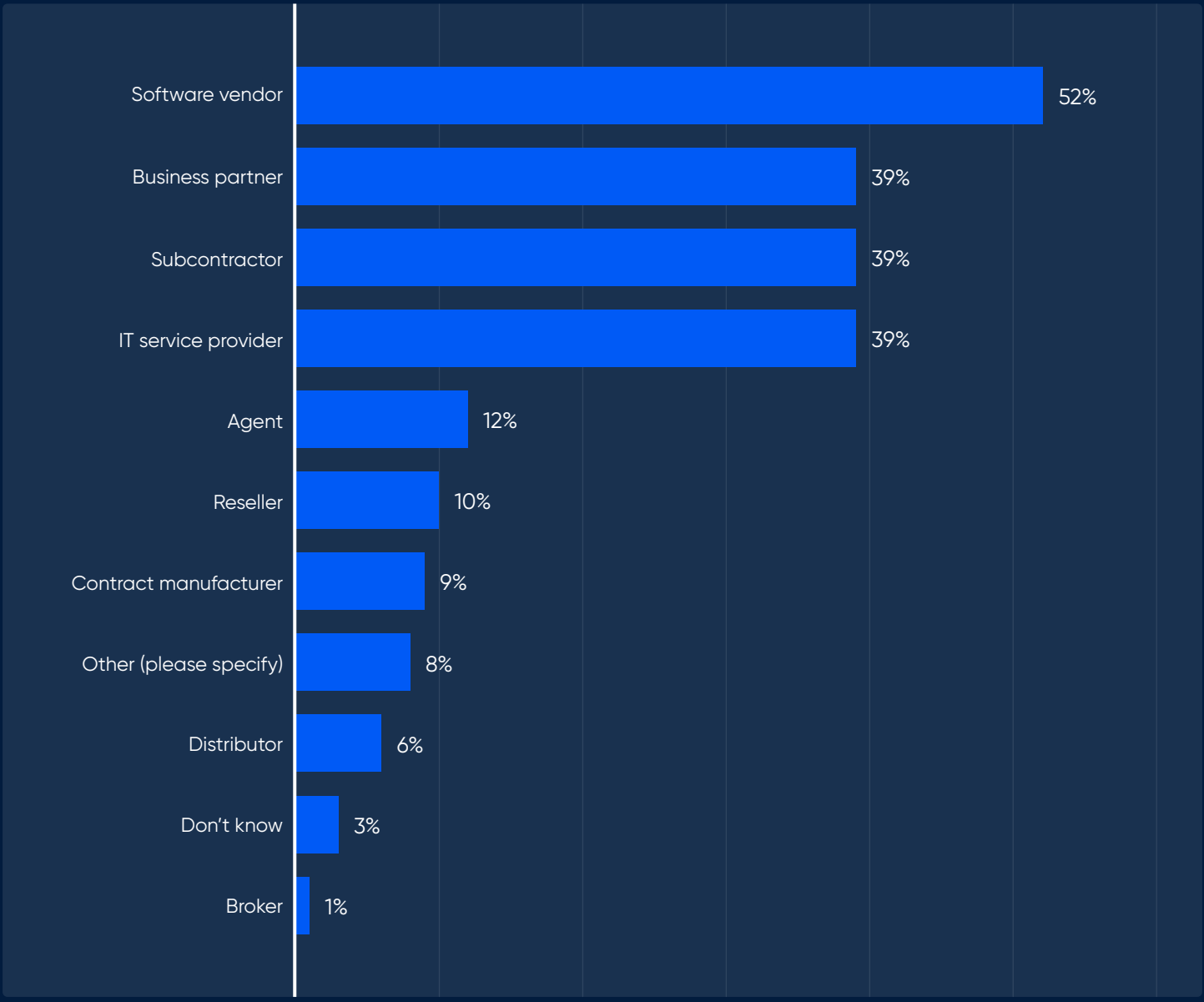
The CyberLink supply-chain attack was made possible by malicious Python packages placed in the online repository PyPI, one of several such supply-chain attacks involving open-source software. In February, 15,000 phishing packages were found in the NPM repository, and so many spam packages were uploaded to NPM in April that the repository briefly went offline. Supply-chain attacks on GitHub involved "repojacking," or taking over abandoned usernames, along with old-fashioned typosquatting to lure users to deceptively named tools. Fake vulnerability exploits and fake proofs of concept on GitHub spread malware to security researchers and wannabe black-hats alike.

The widespread availability of code-writing AI tools like Microsoft's Copilot, already part of GitHub, raises the stakes of third-party software security. AI can "hallucinate" the existence of imaginary code libraries in public software repositories, creating blank slates into which attackers can sneak malicious code through "hallucination squatting."

Fifty-seven percent of all respondents to a January 2023 CRA Business Intelligence survey of 209 IT and security professionals in the U.S. said that their organizations had suffered a security incident or data breach related to a third-party partner in the previous 24 months, and 52% of those said that the attack stemmed from a software vendor.

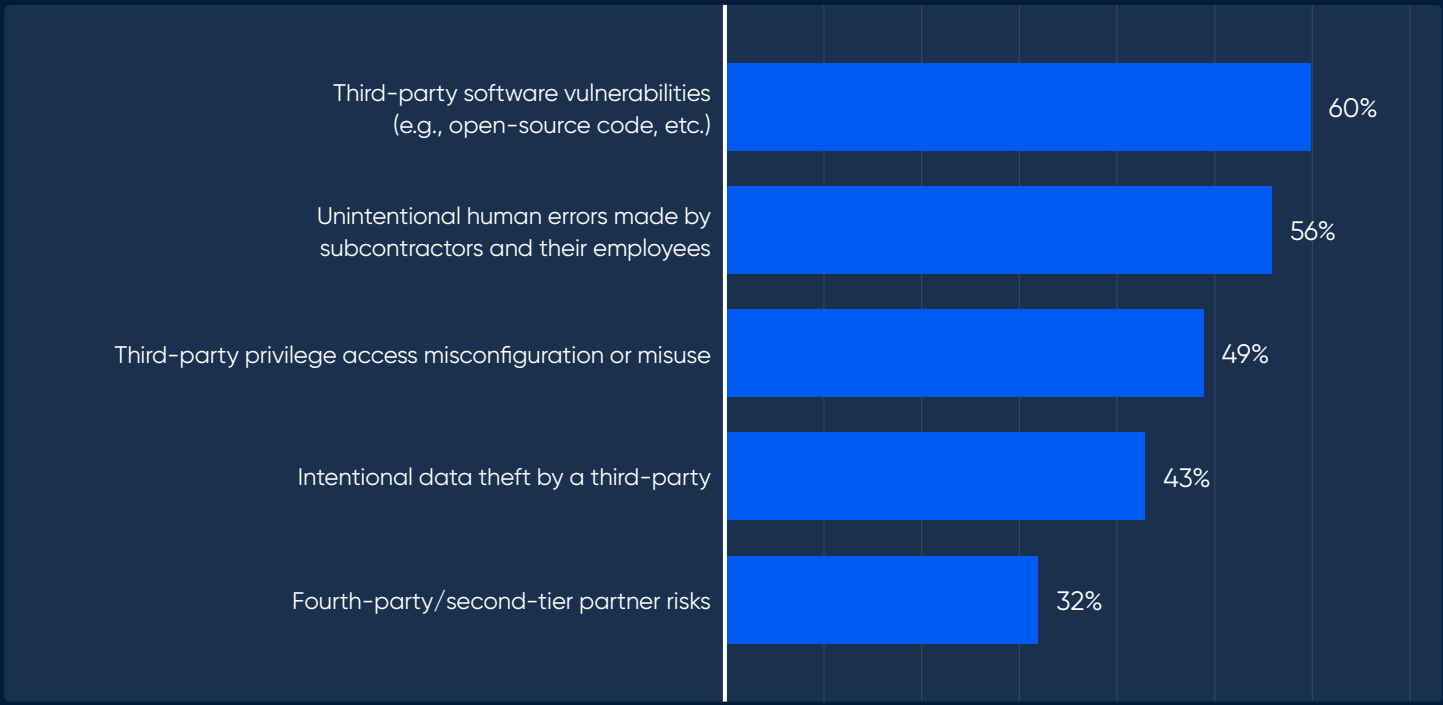
Which of the following were the source(s) of these attacks or breaches?

Select all that apply



High-risk incidents

How much of a risk does each of the following pose to your organization?



Third-party software vulnerabilities were seen as the gravest threat posed by third-party relationships, with 60% of respondents rating them between 5 and 7 on a 1-7 scale of potential risk.

"The third-party ecosystem has become complex, and the open-source software system has been attacked and is an easy target," said one survey respondent. "Without having clear visibility into the remediation process, it poses a big risk."

2024 to-do list:

- If you're a for-profit healthcare provider, plan for tougher FTC enforcement of data-breach rules (non-profit providers are regulated at the state level).
- Perform risk assessments of third-party software and third-party vendor relationships.
- Consider using a software bill of materials (SBOM) to keep track of third-party components.

Vulnerability management remains a moving target

Vulnerabilities were not limited to third parties, of course. Hundreds of organizations using MOVEit file-transfer software learned that the hard way when a zero-day flaw was disclosed in early June along with a patch.

The Cl0p ransomware group, which had earlier in the year targeted flaws in Fortra GoAnywhere MFT and PaperCut software, quickly exploited the patch lag among MOVEit customers. The group was apparently so successful with MOVEit that it abandoned its old business model and moved to old-fashioned blackmail without encrypting any data.

"They use the stolen files and information as leverage against the victims, with the threat of having customer PHI/PII or other details publicly published online being enough of a risk for organizations to pay," a Huntress researcher told SC Media.

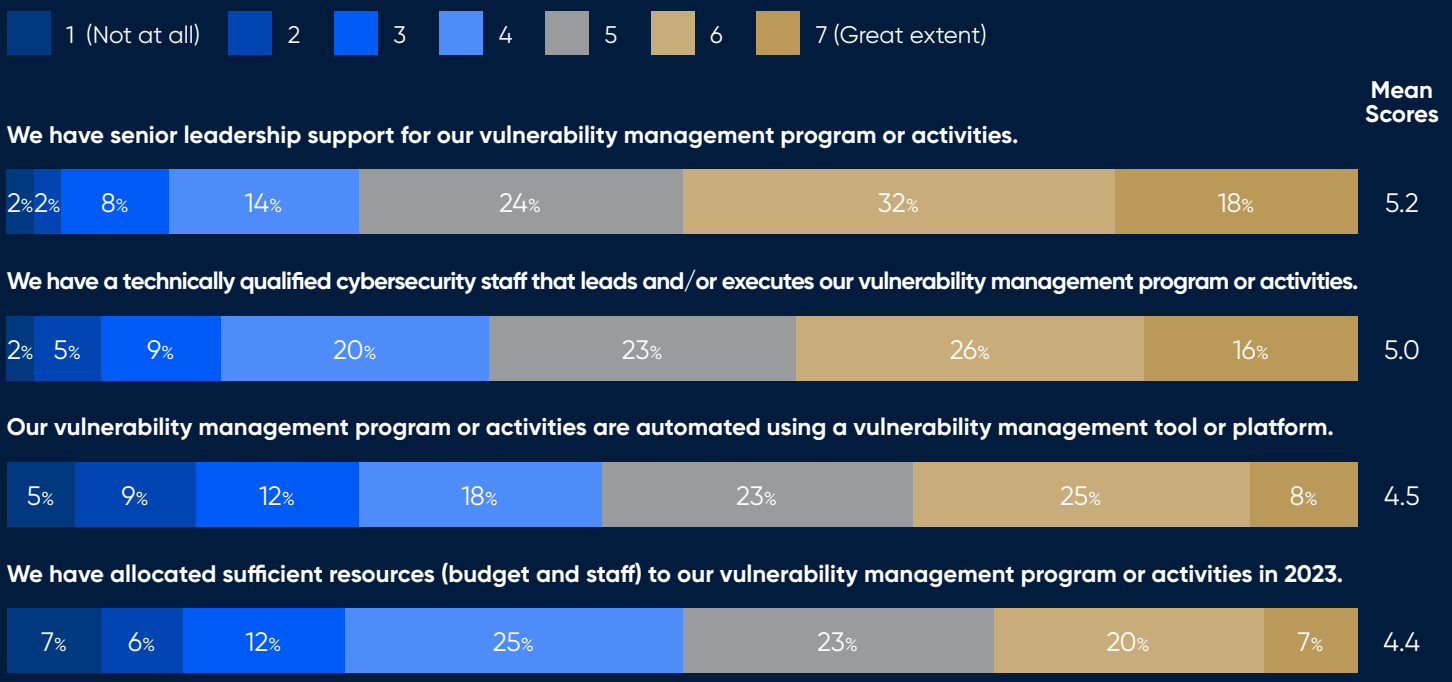
Cl0p hit at least 369 MOVEit clients, including Siemens Energy, UCLA, U.S. government contractor Maximus and several U.S. government agencies. In June, MOVEit maker Progress Software was hit with the first of several class-action lawsuits, although the CEO later said most customers were "really happy" with the company's handling of the vulnerability. By November, Cl0p had moved on to targeting a zero-day flaw in SysAid servers.

Less well noticed were a clutch of severe software flaws in Microsoft Azure disclosed in January and March, and an exploited zero-day critical vulnerability in Cisco's IOS XE software in October that may have affected tens of thousands of networking devices.

In an ideal world, all these flaws would have been patched immediately by all software users. But the reality is that many organizations can't quickly fix even the most severe vulnerabilities due to legacy technology, incomplete inventory of assets, lack of a formal vulnerability-management program, or insufficient budget, staffing or support from management.

In an April 2023 survey carried out by CyberRisk Alliance Business Intelligence, only half of 210 IT and security professionals said their organizations' vulnerability-management programs had strong leadership support. Only 27% strongly felt that their VM programs had enough budgeting and dedicated personnel to do an effective job.

Vulnerability management resources



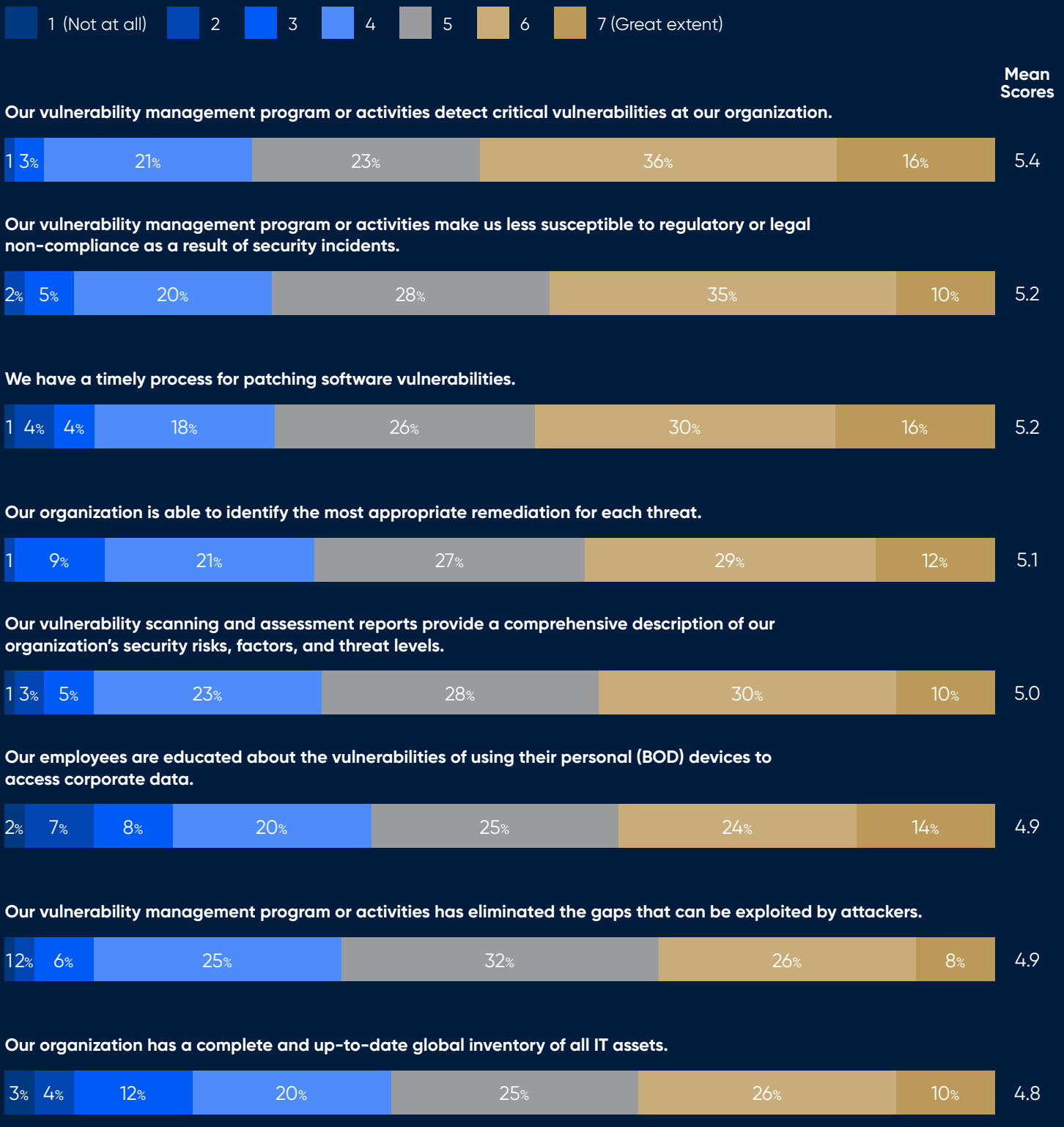
Note: Respondents were asked to rate each on a 7-point scale where 1 is "Not at all" and 7 is "To a great extent."
Chart shows percentage of respondents who provided each rating from 1 to 7; not all totals sum to 100% due to rounding.
Base: All respondents (n=210).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Vulnerability Management Survey, April 2023.

"We don't have the time, money or staff for these activities, and leadership is not supportive," said one survey respondent.

Likewise, only 36% of respondents strongly felt that their organizations had a complete inventory of IT assets, and only 34% believed that their VM programs had eliminated gaps that could be exploited.

> "Staying ahead of the constantly changing threat environment is by far the most difficult aspect of our cybersecurity management, even with the advanced tool set that we have."
>
> *— CyberRisk Alliance Business Intelligence survey respondent*

Vulnerability management outcome or results



Note: Respondents were asked to rate each on a 7-point scale where 1 is "Not at all" and 7 is "To a great extent."
Chart shows percentage of respondents who provided each rating from 1 to 7; not all totals sum to 100% due to rounding.
Base: All respondents (n=210).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Vulnerability Management Survey, April 2023.

"Staying ahead of the constantly changing threat environment is by far the most difficult aspect of our cybersecurity management, even with the advanced tool set that we have," said a survey respondent.

In-depth interviews with a CISO and a CTO from two different organizations revealed concerns about legacy technology and automating vulnerability management, as well as how 2021's Log4j supply-chain vulnerability led to better planning about patch lag time.

"Where we're still struggling, and I think a lot of companies are struggling, is automating vulnerability management to pair up with the business value or materiality or context," the CISO noted.

But one of the interviewees added, "within any vulnerability management program — no matter how close you're automating — there's still a limit to how many changes engineering teams want to have to their production systems in a short period of time."

Vulnerability-management software should become more rapid and efficient as its automation is augmented by AI and machine learning. But those features may not be immediately affordable to security teams with limited budgets.

For in-house software development, AI is well suited to help detect vulnerabilities, such as in static or dynamic application-security testing (SAST and DAST). But it is less reliable when writing code from scratch, and often creates software vulnerabilities on its own.

It's worth noting that the SEC's fraud charges against SolarWinds, mentioned earlier, involve vulnerability management. They allege that while SolarWinds portrayed itself as a security-minded company, it knew of internal risks and vulnerabilities that were not being properly addressed. Compliance with the SEC's new four-day reporting rule would not have changed that perception.

2024 to-do list:

Includes guidance from the Cybersecurity Collaborative's Task Force on vulnerability management:

Look into getting vulnerability-management software that uses AI/ML or incorporate those features into your existing VM tools.

Incorporate AI and machine learning into application-security tools wherever possible.

Develop procedures to apply critical software updates quickly. The Cl0p group exploited the MOVEit flaw just a couple of days after its disclosure.

Organizations behind on cloud security, even as cloud investments surge

In 2023, adversaries attacked assets and used the cloud for their own nefarious purposes, sometimes doing both at once.

January began with a report that threat actors were developing cloud skills more rapidly than the legitimate enterprises they targeted, and another that the number of cloud apps delivering malware had tripled in the previous year.

That observation was quickly borne out in April, as the Legion malware hijacked misconfigured cloud-based email servers, then attacked the Amazon Web Services monitoring tool AWS CloudWatch. Another group, TeamTNT, deployed a worm to go after Docker containers, first on AWS but then on Google Cloud Platform and Microsoft Azure as well.

An unnamed threat actor chained together Salesforce and Facebook flaws to pump out phishing emails, and a cloud-based command-and-control provider called Cloudzy hosted instances for several state-sponsored APT groups, even those from rival countries like India and Pakistan, as well as known criminal gangs.

Some of Cloudzy's APT customers were North Koreans, who needed no assistance in launching the supply-chain attack on JumpCloud, likely with the aim of hitting JumpCloud's cryptocurrency-using clients. Pyongyang's notorious Lazarus Group was also spotted midyear hijacking cloud-based Microsft IIS servers to spread malware.

After all that, the incident in which an attacker hijacked an abandoned AWS S3 bucket to spew malware seemed almost quaint by comparison.

Old-fashioned cloud security problems didn't go away, of course. Salesforce and a dating app both spilled sensitive data due to cloud misconfigurations, and ServiceNow was just lucky that its own misconfiguration went unexploited.

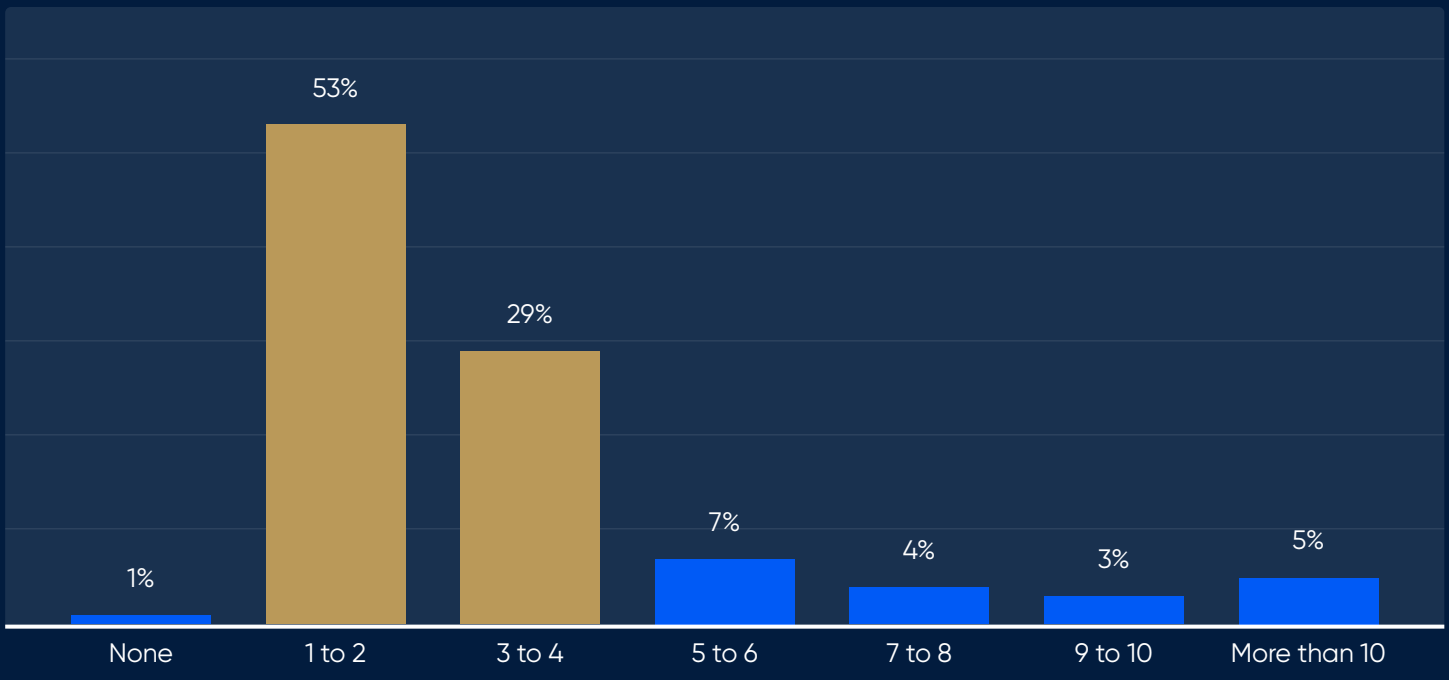
Organizations lost track of or just plain forgot about cloud assets, including in Salesforce communities and Azure Active Directory. It perhaps shouldn't have been surprising that 30% of 13 billion files stored in the public cloud were found to contain personally identifiable information.

Put together the cloud-related skills and knowledge gap between attackers and defenders with the advent of AI-driven attacks, and we might see a perfect storm of cloud-based and cloud-targeting threats in 2024. Threat actors might use AI to rapidly catalogue an organization's cloud assets and probe them for weaknesses, gaining visibility that the targeted organization lacks. Defenders of cloud assets may have to adopt AI-driven monitoring and response tools just to keep up.

An August 2023 CRA Business Intelligence survey of 200 IT and security managers in North America found that cloud adoption was widespread, with 43% of respondents saying that their organizations had moved at least half their workloads into the cloud. Forty-eight percent said they used three or more cloud providers, while only 1% said they didn't use the cloud at all.

Number of cloud providers

How many cloud providers does your organization currently use?



Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, August 2023.

Respondents generally felt comfortable with the security of their cloud platforms, with 56% of respondents rating their confidence levels at 7 or more on a scale of 1 to 10, even though 22% of Amazon Web Services and Microsoft Azure customers each said their platforms had been compromised in the previous 12 months. Two-thirds (66%) said they used the security services offered by their cloud platform providers.

Yet a sizeable fraction of survey respondents had doubts about their own abilities to manage, secure and gain visibility into their own cloud assets. One-quarter (25%) said they lacked the skills or expertise to properly secure the cloud, 14% said they didn't have the staff to manage the cloud, 13% said they lacked the required experience and 8% said they lacked visibility. Fifteen percent feared they wouldn't be able to handle adversarial attacks on their cloud assets, and 10% felt they needed more resources to manage the cloud.

Please describe the challenges or barriers your organization faces in implementing effective cloud security.

Top topics	% mentions	Respondent comments
Price	25%	"A fixation on cutting corners to save money and slow implementation."
Skills / expertise	25%	"I don't think we know enough about cloud security to effectively secure our connection/data."
Staff / dedicated team	14%	"We lack a dedicated team to oversee cloud operations and security."
Cloud experience	13%	"We are still working on our cloud security. We currently have very little in the cloud as we are still discovering what makes sense for us."
Users / employees	8%	"Understanding the complexity that the cloud can introduce. Trouble with training and maintaining employees that can stay current with the latest cloud technologies."
Visibility / insight / data sprawl	8%	"Lack of visibility and control over cloud workloads."
Tools	6%	"Utilizing cloud native versus existing security tool sets."
Vendors	6%	"Dealing with so many vendors and alerts."
Mostly on prem / little cloud	5%	"It's only a small part of our overall network and as such it doesn't command much attention. That will change as we push more workloads to the cloud."
Settings / configuration	5%	"Security settings/configuration relays on the vendor site."
Management support	3%	"Doesn't really seem to have the full backing of upper management, including settling on a single provider."
No strategy	3%	"Still developing strategies."
Monitoring cloud providers	2%	"There are so many different cloud provider and it's tough to monitor them all."

Note: Percentages represent % of mentions. Base: n= 64; Respondents who rated their confidence in their organization's cloud security 1, 2, 3, 4, or 5 (low confidence).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Cloud Security Survey, August 2023.

> "We're struggling to understand the complexity that the cloud can introduce and have trouble training and maintaining employees that can stay current with the latest cloud technologies."
>
> *— CyberRisk Alliance Business Intelligence survey respondent*

"We're struggling to understand the complexity that the cloud can introduce and have trouble training and maintaining employees that can stay current with the latest cloud technologies," said one respondent.

Such lack of confidence in organizations' abilities to manage, track and protect cloud assets doesn't bode well for compliance with the SEC's new breach-notification rules. Publicly traded companies may have to devote more resources to improving cloud visibility and security, and to create new procedures and templates that would speed up incident reporting.

2024 to-do list:

Includes guidance from the Cybersecurity Collaborative's Task Force on vulnerability management:

Prioritize additional cloud training for IT and security personnel.

Make sure new or recently added cloud-management tools include AI/ML, especially for asset inventory and misconfiguration and vulnerability detection.

Develop rapid cloud-breach reporting procedures to comply with SEC rules.

When IAM security conflicts with user experience

Many of the top identity and access management stories of 2023 involved Okta, and not in a good way. The widely used cloud-based IAM provider revealed in November that attackers had in September compromised an employee's Google account, letting them steal credentials to an Okta service account, which in turn let the attackers obtain administrative session cookies for Okta clients including BeyondTrust, Cloudflare and 1Password and possibly the contact information for every user of Okta's main customer-support system.

You never want your own company to become the focus of an Enterprise Security Weekly podcast with a title like "Five Lessons Learned From Okta's Customer Support System Breach."

Earlier in September, Okta clients found themselves targeted by a social-engineering campaign, attributed to the Scattered Spider aka Oktapus ransomware crew, that tried to cajole service-desk technicians into resetting MFA settings of Okta super-administrator accounts. This wasn't Okta's fault, and few of its clients fell for the ruse, but two very big ones did: gambling-industry giants MGM Resorts International and Caesars Entertainment.

The MGM hackers used the telephone as an avenue of attack. Social-engineering attacks in 2024 may use AI to rapidly mount and manage phishing, vishing and business email compromise campaigns. It won't be long before AI bots can keep potential victims on the hook with extended email, instant-messaging or even voice-based conversations.

The drip-drip-drip of revelations stemming from a single Okta breach incident might not fly well with an SEC seeking to enforce its new four-day reporting rule. Clients of IAM providers should look into stopgap solutions should their providers be similarly compromised and be ready to quickly report their own potential resulting breaches to the SEC if they are publicly traded. If it's any consolation to Okta, Microsoft in September had 38 terabytes' worth of its private GitHub data exposed, thanks to an abused shared access signature (SAS) token. The compromised data included 30,000 Teams messages, capping a summer of woe for Microsoft's messaging platform.

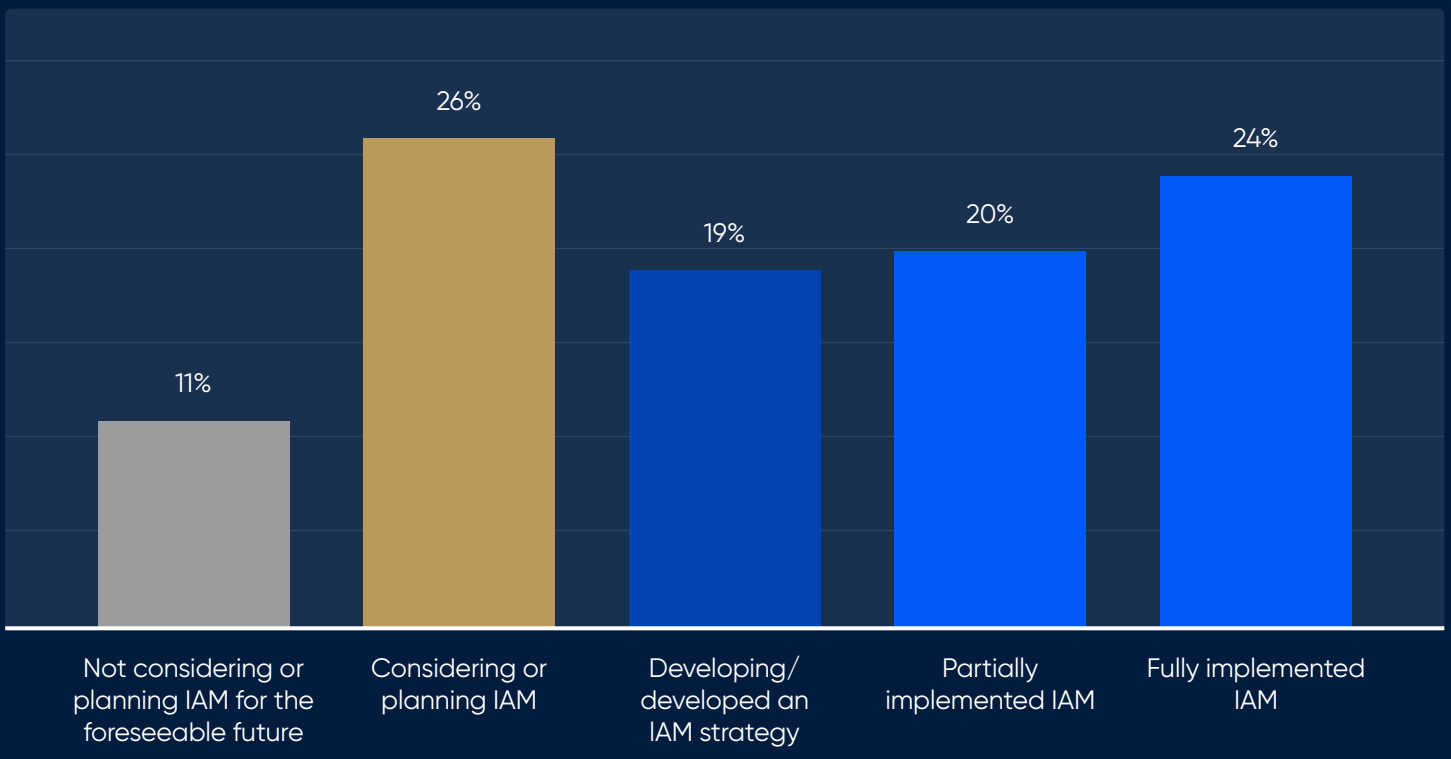
It began with the July release of a red-teaming tool called TeamsPhisher, which lets you send files directly to a Teams user from outside the user's organization's network, exploiting a vulnerability that Microsoft said it doesn't plan to patch. That led to a spate of phishing attacks on Teams users.

Teams was also hit hard by the Russian state-sponsored attackers Cozy Bear, the DarkGate malware crew and a broader Microsoft-services attack by Chinese state-sponsored hackers who had found a private encryption key in a crash-dump file stored on a Microsoft engineer's computer. None of those attackers seemed to be using TeamsPhisher.

For a bit of good news, the passwordless "passkey" system developed by Apple, Google and Microsoft became widely available in 2023 and was the hot topic at Identiverse 2023. In May, Google made passkeys an option for user accounts and then for enterprise users; by the autumn, GitHub, 1Password and WhatsApp had followed suit. In a CyberRisk Alliance Business Intelligence survey of 203 security and IT managers in North America, conducted in December 2022 and January 2023, 44% of respondents said that their organizations had at least partly implemented IAM solutions, and 26% were considering one. Of those who had moved ahead with IAM, roughly equal numbers went with on-premises, cloud-based or hybrid deployments.

Current IAM adoption

What is your organization's status in implementing an IAM program?



Base: All respondents (n=203).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Identity and Access Management Survey, December 2022/January 2023.

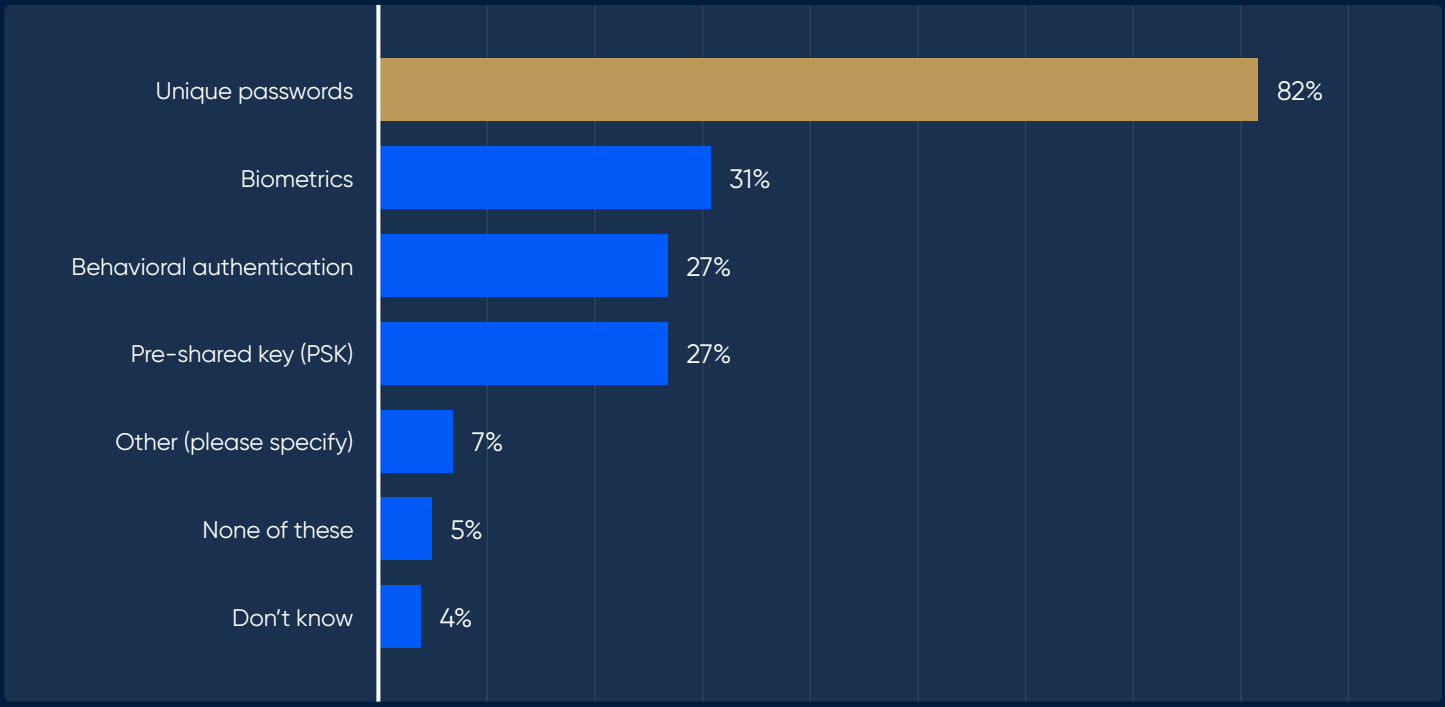
However, along with endpoint security and remote access, IAM implementers were concerned about the user experience, a constant worry with IAM deployments. Fifty-six percent of survey respondents said they were "currently focused" on the user experience, and another 32% said they were planning to focus on it.

Hesitation to take users into unfamiliar territory may explain why while 82% of respondents said their IAM programs enforced unique user passwords, more advanced authentication methods such as biometrics, pre-shared keys and behaviors were each used by slightly less than one-third of respondents.

> "Who wants to spend hours in understanding a product that always requires additional expertise to handle when its objective is to provide efficiency?"
>
> *— CyberRisk Alliance Business Intelligence survey respondent*

Included in IAM strategy or implementation to provide digital authentication

Which of the following methods are included in your organization's IAM strategy or program to provide digital authentication?



Note: Respondents were asked to select all that apply.
Base: Current IAM adopters (i.e., "Developed/developing IAM strategy," "Partially implemented IAM," or "Fully implemented IAM") (n= 128).
Source: CyberRisk Alliance Business Intelligence (CRA BI), Identity and Access Management Survey, December 2022/January 2023

"Who wants to spend hours in understanding a product that always requires additional expertise to handle when its objective is to provide efficiency?" asked one respondent. Another noted that "not disrupting the end user is difficult and requires more people than we currently have devoted to the project."

2024 to-do list:

- Look into mandating the use of passkeys for high-privilege administrative personnel and executives.
- Create internal "fail closed" procedures in case your external IAM provider is compromised.
- Always keep the user experience in mind when implementing new IAM procedures.

Conclusion: The point of it all

A common theme among most of the survey respondents was lack of information, skills and resources. Cloud-platform clients worry that they don't have the skills to manage their cloud assets; both cloud and vulnerability-management users worry they don't have visibility into all their assets; IAM clients worry that their employees won't be able to effectively use new systems; and all sorts of organizations worry that they can't see into their third-party partners' security practices, putting themselves at risk.

The only silver lining, ironically, lay in the ransomware survey, in which surprisingly high numbers of respondents felt confident in their ability to handle attacks and none admitted paying any ransom in the previous 24 months. That may be due to the extraordinarily high number of resources that were committed to combatting ransomware in the past several years.

If so, then that's a quiet victory that should be celebrated, and it may point the way toward defeating other major cybersecurity challenges.

Until AI changes the playing field, that is.

Report methodology

Each CyberRisk Alliance Business Intelligence survey was conducted online and involved roughly 200 IT and security leaders and executives, practitioners, administrators, and compliance professionals based in North America.

Roughly three-quarters of respondents were directors, managers or administrators; a bit less than 20% were C-suite executives or VPs. Two-thirds of respondents worked for medium-sized (100-999 employees) or large (1,000-9,999 employees) organizations, and about a quarter for enterprises (10,000 or more employees). Roughly two-thirds worked in the education, financial services, healthcare, high-tech, or manufacturing sectors.

CyberRisk Alliance Business Intelligence 2023 reports

1. Tough on Ransomware: Organizations fighting ransomware with continuous monitoring, IR playbooks, backups, and user education (November 2023)
2. Cloud security: Gaps in skillsets and lack of visibility leaves many organizations flying blind (October 2023)
3. Easy Prey: The Danger of Vulnerable Endpoint and Devices (September 2023)
4. Threat Intelligence: Eyes on the Enemy (August 2023)
5. Vulnerability Management: A Maelstrom of Moving Targets (June 2023)
6. Controlling the Chaos: The Key to Effective Incident Response (May 2023)
7. Identity and Access Management: Can Security Go Hand-in-Hand with User Experience? (April 2023)
8. Finding the Way to Zero Trust (March 2023)
9. Wanted: A Few Good Threat Hunters (February 2023)
10. Third-Party Risk: More Third Parties + Limited SupplyChain Visibility = Big Risks for Organizations (January 2023)

RSAConference™

About RSA Conference

RSA Conference is the premier series of global events and year-round learning for the cybersecurity community. RSAC is where the security industry converges to discuss current and future concerns and have access to the experts, unbiased content and ideas that help enable individuals and companies to advance their cybersecurity posture and build stronger and smarter teams. Both in-person and online, RSAC brings the cybersecurity industry together and empowers the collective "we" to stand against cyberthreats around the world. RSAC is the ultimate marketplace for the latest technologies and hands-on educational opportunities that help industry professionals discover how to make their companies more secure while showcasing the most enterprising, influential, and thought-provoking thinkers and leaders in cybersecurity today.

For the most up-to-date news pertaining to the cybersecurity industry visit www.rsaconference.com.
Where the world talks security.

CyberRisk ALLIANCE

About CyberRisk Alliance

CyberRisk Alliance provides business intelligence that helps the cybersecurity ecosystem connect, share knowledge, accelerate careers, and make smarter and faster decisions. Through our trusted information brands, network of experts, and innovative events we provide cybersecurity professionals with actionable insights and act as a powerful extension of cybersecurity marketing teams. Our brands include SC Media, the Official Cybersecurity Summits, TECHEXPO Top Secret, Security Weekly, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, Cybersecurity Collaborative, ChannelE2E, MSSP Alert, and LaunchTech Communications.

Learn more at www.cyberriskalliance.com.

RSAConference™ | Where the World Talks Security™

HOW TOP CISOS ARE TRANSFORMING THIRD-PARTY RISK MANAGEMENT

For CISOs and all cybersecurity professionals RSA Conference provides year-round insights and resources to help better secure your organization. Our second CISO Perspectives report is available: **How Top CISOs Are Transforming Third-Party Risk Management**.

The RSAC Executive Security Action Forum (ESAF) Program Committee tapped into the world's foremost enterprise security leaders from multiple industries to create this comprehensive report examining vital information CISOs share on addressing third-party risk.

Download the report at **RSAConference.com/CISOreport2023**.

REGISTER FOR RSAC 2024—THE ART OF POSSIBLE

In an ever-changing cybersecurity world, innovation and creativity are key. Join RSAC 2024 and discover **The Art of Possible** as we collectively create works that will change our perspective on what we can accomplish. Let's celebrate limitless opportunities, challenge the status quo, and explore new horizons together.

Learn more and register at RSAConference.com/cyberrisk2024.