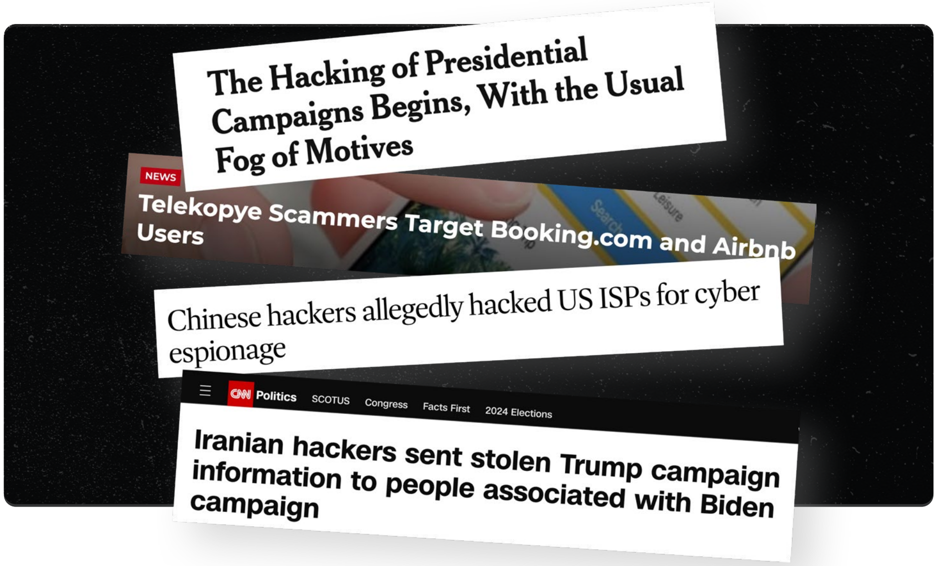
VARONIS

THE IDENTITY CRISIS

An in-depth report of cyberattacks in 2024

All it takes is an identity.

In 2024, nation-state attacks and massive IT outages dominated headlines. From state-sponsored attacks to election campaign hacks to new forms of ransomware, the threat landscape appears to be a minefield of sophisticated cyberattacks.



The Hacking of Presidential Campaigns Begins, With the Usual Fog of Motives

NEWS

Telekopye Scammers Target Booking.com and Airbnb Users

Chinese hackers allegedly hacked US ISPs for cyber espionage

Iranian hackers sent stolen Trump campaign information to people associated with Biden campaign

CNN Politics
SCOTUS
Congress
Facts First
2024 Elections

However, these headlines don't reflect reality.

The truth is most cyberattacks are far less flashy. All bad actors really need is an identity. In most cases, attackers use simple techniques like credential stuffing to steal an identity. Once they have legitimate credentials, they can dwell in an environment for months undetected, exploiting vulnerabilities and searching for sensitive data.

This report analyzes the occurrence of cyberattacks and provides practical guidance on preventing breaches.

METHODOLOGY

In December 2023, a **Securities and Exchange Commission (SEC) rule** requiring the disclosure of material cybersecurity incidents went into effect.

We reviewed 35 SEC Form 8-K filings disclosed between January and August 2024 and cross-referenced them with news sources and threat reports to better understand how cyberattacks occur.

Additionally, during the same period, we integrated insights from investigations conducted by Varonis' Managed Data Detection and Response (MDDR) team, which provides threat detection and response services for some of the world's largest companies.

Attackers don't hack in; they *log* in.

In examining these 35 cyberattacks, we found that bad actors typically don't hack in using sophisticated techniques or malware. Most often, they log in via credentials that have either already been stolen or use tried-and-true techniques to gain access, like phishing and password spraying. All it takes is one valid set of stolen credentials, and a hacker can access everything a user can.

57%

OF CYBERATTACKS START WITH COMPROMISED IDENTITY

HOW DO CYBERATTACKS OCCUR?

In more than half (57%) of the cyberattacks examined, attackers compromised an identity to gain access to the environment with techniques that include:

- Phishing
- Social engineering
- Password sprays
- Supply-chain attacks
- Data exposure
- Compromised accounts
- Compromised credentials
- Insider threats
- Privilege escalation

The most common cause of cyberattacks reported in SEC filings is "unauthorized third-party access." While this description tells us little, corroborating reports provided greater detail on many of the incidents. For example, an **8-K form filed in February,** Prudential Financial states that a "threat actor had gained unauthorized access to certain of our systems." While in a **March notification,** Prudential Financial added more detail and said that the breach was caused by "social engineering."

Alarmingly, the method of attack in more than 40% of publicly reported incidents is unknown. This suggests both a lack of information and a lack of self-reporting on the root cause of these cyberattacks.

How do attackers get in?

To further examine cyberattack methods, we categorized more than 60 incidents investigated by the **Varonis Managed Data Detection and Response (MDDR)** team in 2024. Their findings align with those in the SEC filings: eight of the nine most common attack methods addressed by the team involved compromised identity, with ransomware acting as the lone outlier not directly related to identity.

BRUTE FORCE

A brute-force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.

COMPROMISED ACCOUNT

An account is compromised when an unauthorized user gains access to an account's login details, such as a username and password.

COMPROMISED EMAIL

A compromised email account is an email account that has been accessed by an unauthorized user.

EXPOSED DEVICE

An exposed device is a device that has been compromised by a vulnerability or left unsecured, allowing attackers to access the device, network, or data.

HIGH-RISK PERMISSIONS

Permissions that allow users to access sensitive information that creates a security risk are considered high-risk.

INSIDER THREAT

An insider threat is a type of cyberattack originating from an individual who works for an organization or has authorized access to its networks or systems.

PHISHING

Phishing is a type of cyberattack that uses fraudulent emails, text messages, phone calls, or websites to trick people into sharing sensitive data, downloading malware, or otherwise exposing themselves to cybercrime.

RANSOMWARE

A ransomware attack is a type of malware attack that prevents a victim from accessing their device or data by encrypting files or locking the device.

UNAUTHORIZED LOGIN

An unauthorized login is when someone gains access to a system or account without permission or exceeds their authorized access.

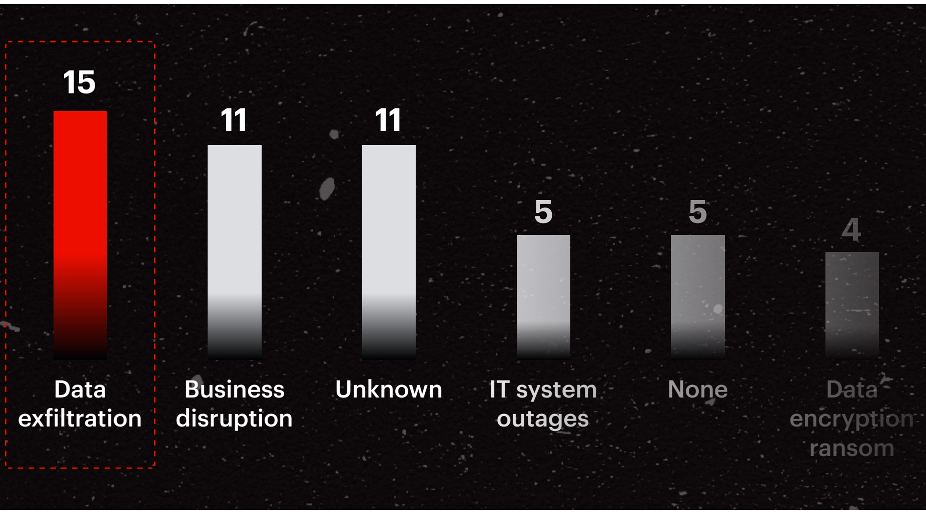
Data is the main target.

While attackers exploit weak identity security as a starting point, it's also important to understand what they do after they gain access. Examining the impact of these cyberattacks paints a clearer picture of what bad actors are targeting, and most of the time, it's data.

In our examination of SEC 8-K filings, "data exfiltration" was the most common consequence of cyberattacks, more prevalent even than "business disruption."

THE IMPACT OF CYBERATTACKS

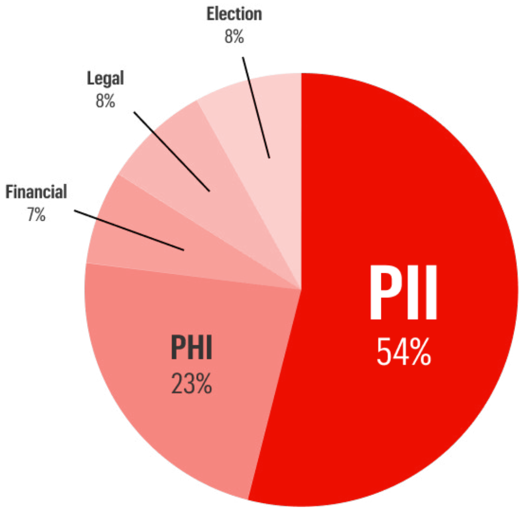
This analysis of cyberattack disclosures and investigations from the first half of 2024 illustrates how malicious actors purchase stolen credentials or employ established techniques to access systems and extract data.



While bad actors often target various data types, our research found that customer data was by far the most targeted type. In this instance, "customers" primarily refers to healthcare patients, financial service clients, and software application users.

When the data's sensitivity was disclosed, PII was the most affected type of sensitive data, followed by PHI.

WHAT TYPE OF DATA WAS TARGETED?

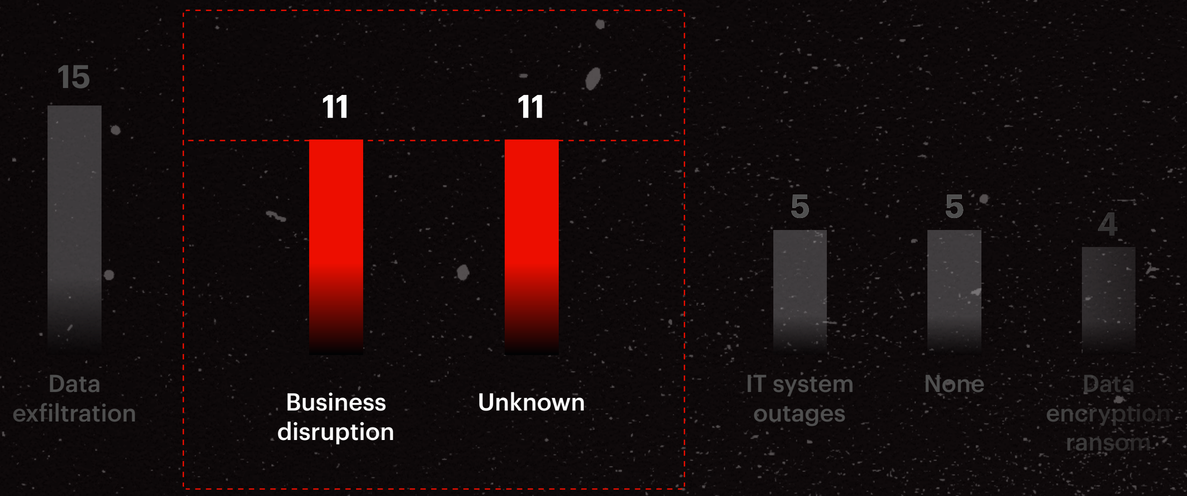


Unknown consequences

Surprisingly, “unknown” is tied with “business disruption” for the second most commonly reported impact, as many of these incidents are still under investigation. Of the incidents we examined, 85% were still under investigation.

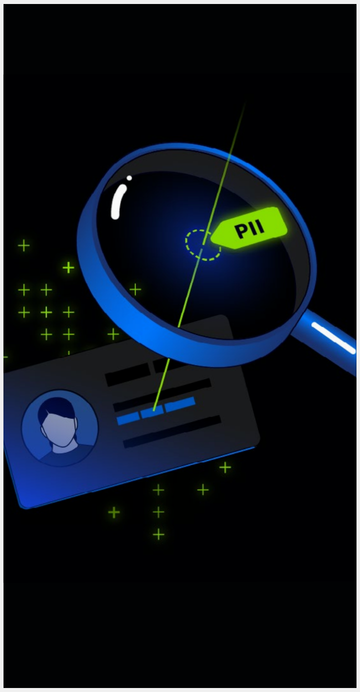
85% **OF CYBERATTACKS WERE STILL UNDER INVESTIGATION.**

This suggests that instances of data exfiltration might be even higher than 57%. Many organizations lack the visibility to accurately assess the consequences of a cyberattack.



“UKNOWN” IS TIED WITH “BUSINESS DISRUPTION” FOR THE SECOND MOST COMMONLY REPORTED IMPACT.

Case studies



National Public Data breach

While data exfiltration is the most common consequence of a breach, the extent of the data affected is often unknown until much later, as was the case with consumer data broker National Public Data (NPD).

An outsourced web development firm inadvertently published the passwords to NPD's back-end database in a file freely available from its homepage.

The impact of this security oversight wasn't known until a consumer used a theft protection service and found their information leaked on the **dark web.**

The March 2024 breach affected 2.9 billion people and exposed personal data, including social security numbers, addresses, and phone numbers. However, it wasn't discovered until July when a malicious actor was found selling the NPD data on the dark web for $3.5M. In August, NPD disclosed the breach to the SEC.

Exploiting Snowflake credentials

In May 2024, **a campaign against Snowflake customers** resulted in at least four cyberattacks. Reports indicate that attackers may have accessed roughly 165 companies' accounts.

The threat actors didn't use sophisticated techniques or malware, and there is no evidence of Snowflake product vulnerabilities or data exfiltration due to compromised employee credentials. Instead, bad actors used stolen or exposed credentials to log in.

In several cases, bad actors exploited poor security and permissions hygiene, such as missing MFA, to gain access to company accounts. Some credentials had been available on the dark web for years, indicating that those passwords had not been updated.

Three phases of a cyberattack

Our analysis explains how to defend against cyberattacks, which have three phases requiring security measures at each stage.

PHASE 1

Login with stolen credentials

Stop attackers before they get in.

Bad actors often access environments using credentials. Right-size permissions, unravel identities, and monitor data activity to detect credential misuse.

PHASE 2

Exploit the blast radius

Reduce the blast radius.

Bad actors move laterally within the system to find sensitive data and exploit weaknesses. According to **Verizon's Data Breach Investigations Report,** incidents involving stolen credentials have an average dwell time of 150 days before detection. Fixing exposure and misconfigurations is essential to ensure that your environment is secure.

PHASE 3

Steal and encrypt critical data

Detect attacks and encrypt critical data.

Attackers typically seek data to steal and sell or hold for ransom, often involving data exfiltration in ransomware attacks. According to **Symantec,** ransomware actors deploy a growing array of data-exfiltration tools in their attacks. Automated policies and threat detection resources help identify abnormal activity, critical for preventing data exfiltration.

The future of cyberattacks

The cloud and AI will increasingly complicate cybersecurity in the future.

Nearly two-thirds of organizations are now multi-cloud, and with the rise of generative AI, cloud data is expected to surge even more. This growth will result in more complex cloud environments, create additional attack vectors, and put more sensitive data at risk.

At the same time, gen AI has the potential to facilitate cyberattacks, making forms of attack like phishing and social engineering more effective and scalable.

With the cloud's trajectory and generative AI aiding bad actors, we can expect more identity-based attacks targeting sensitive information in the future.

Focusing on monitoring sensitive data, locking down identities, safeguarding credentials and permissions, and detecting abnormal behaviors will give security teams an advantage.

How can Varonis help?

Varonis helps security teams stay ahead of cyberattacks with our **unified Data Security Platform.** With Varonis, organizations can discover and secure sensitive data automatically at each phase of a cyberattack's lifecycle, including:

- **Safeguarding identity and right-sizing permissions:** View permission structures in a single interface and ensure only the right people have access to important files, folders, and mailboxes. Effortlessly eliminate stale users, excessive permissions, and misconfigured roles, groups, and policies that bad actors can exploit.
- **Detecting abnormal behavior and insider threats:** Correlate identity and data activity in real time. Pinpoint and track threats with a full forensics log of actions, including file access, email activity, permissions changes, and more. Varonis uses behavior-based detections to alert you to abnormal behaviors that indicate a bad actor is in your environment.
- **Securing data and preventing data exfiltration:** Varonis factors in entitlements, group memberships, sharing links, muting permissions, and more to give you the most accurate view of sensitive data risk. Automated remediation ensures your data becomes more secure, even as data volumes grow.

SOURCES

BankInfoSecurity. (2024, July). Millions Affected by Prudential Ransomware Hack in February.

BleepingComputer. (2024). Cencora data breach exposes US patient info from 11 drug companies.

Board Cybersecurity. (n.d.). Reports.

CNBC. (2024, July 12). Snowflake shares slip after AT&T says hackers accessed data.

CyberNews. (2024). LockBit breach: Kulicke and Soffa SEC 8-K filing.

Cybereason. (2024). Threat alert: INC ransomware.

Cybersecurity & Infrastructure Security Agency. (2023). Cybersecurity Advisories: AA23-165A.

Cybersecurity & Infrastructure Security Agency. (2024). Cybersecurity Advisories: AA24-242A.

Dark Reading. (2024). Midnight Blizzard breached HPE email before Microsoft hack.

Dropbox Sign Blog. (2024). A recent security incident involving Dropbox Sign.

Halcyon. (2024). Repligen Corporation hit by ransomware attack; 500GB data breach by INC Ransom.

Halcyon. (2024). Rhysida attacks MarineMax.

InfoSecurity Magazine. (2024). Cencora patient data stolen.

Malwarebytes. (2024, July). Affirm says Evolve Bank data breach also compromised some of its customers.

Microsoft Security Response Center. (2024, March). Update on Microsoft actions following attack by nation-state actor Midnight Blizzard.

PYMNTS. (2024). HealthyEquity says data breach isolated amid larger cyberattack wave.

SC Media. (2024). Cyberattack impacts Radiant Logistics Canada operations.

SC Media. (2024). More than 123k hit by MarineMax hack.

SOCRadar. (2024). Dark web profile: Red Ransomware.

TechCrunch. (2024, April 8). Targus says cyberattack causing operational outage.

The Verge. (2024, June 10). Frontier Communications hack cyberattack data breach ransom.

Top Class Actions. (2024). SouthState Bank class action claims data breach exposed customer data.

Wired. (2024). EPAM, Snowflake, Ticketmaster breach by ShinyHunters.

VARONIS

Ready to experience the Varonis difference?

Reduce your risk without taking any. Contact our team to learn what will be covered in your **free** Data Risk Assessment.

Get your assessment

ABOUT VARONIS

Varonis (Nasdaq: VRNS) is a leader in data security, fighting a different battle than conventional cybersecurity companies. Our cloud-native Data Security Platform continuously discovers and classifies critical data, removes exposures, and detects advanced threats with AI-powered automation.

Thousands of organizations worldwide trust Varonis to defend their data wherever it lives — across SaaS, IaaS, and hybrid cloud environments. Customers use Varonis to automate a wide range of security outcomes, including data security posture management (DSPM), data classification, data access governance (DAG), data detection and response (DDR), data loss prevention (DLP), and insider risk management.

Varonis protects data first, not last. Learn more at www.varonis.com.