What 2024 Taught Us About Cybercrime

& What Leaders Need to Focus on Next

2024 delivered a striking mix of cyber chaos & clarity.

Three of the most respected threat intelligence sources - the FBI's IC3 Report, Verizon's DBIR, & Mandiant's M-Trends - paint a picture that's as predictable as it is sobering: **Attackers are faster, more focused, & increasingly enabled by automation & credential theft.**

Here's what stood out… & where **you need to pay attention**.

Exploits & Credentials Now Rule the Front Door

All three reports show a sharp pivot away from phishing & toward vulnerability exploitation & credential abuse.

Mandiant observed that 33% of intrusions began with an exploit, & another 16% involved stolen credentials, overtaking phishing as the #2 vector.

IC3 similarly flagged a rise in credential-driven fraud, especially among older victims.

DBIR quantified this precisely: stolen credentials accounted for 31% of breaches, while vulnerability exploitation rose 34% year-over-year.

Translation

- MFA fatigue, patch lag, & shadow IT are now risk accelerants.
- If your identity & asset management programs aren't equally mature, you're exposed.

Ransomware Didn’t Go Away - It Just Rebranded

Ransomware & extortion remain dominant.

The FBI reported $12.4 million in ransomware losses - a significant undercount due to non-reporting - while Mandiant found ransomware involved in 21% of all intrusions, often paired with data theft.

The LockBit takedown (Operation Cronos) made headlines, but new players like RANSOMHUB & Akira quickly filled the void.

What’s new

Ransomware actors increasingly skip encryption & jump straight to extortion. They target cloud workloads, SaaS accounts, & even exfiltrated HR data - especially if you’ve already lost the element of surprise.

Elder Fraud & Call Center Scams Are Surging

IC3's report emphasized one overlooked frontier: the elderly.

Victims over 60 lost $4.8 billion in 2024, with romance scams, tech support fraud, & investment schemes driving most of the damage.

Fraud operations often relied on phone-based social engineering, physical couriers, or fake crypto exchanges.

Message to CISOs

Not all threat surfaces are digital. Elderly customers, donors, or board members can become cyber liabilities, so they deserve protection strategies.

Cloud & SaaS Are Your Riskiest Blind Spots

39% of cloud intrusions began with phishing, but 35% involved credential theft or abuse, usually paired with SSO abuse & SaaS data exfiltration.*

In one case, attackers used customer support calls to reset MFA and spun up VMs for lateral movement.

If you haven't already…

- Review all support desk workflows.
- Disable legacy authentication.
- Enforce MFA registration change alerts.
- Start logging your SaaS tools.

*Mandiant

Dwell Time Shrinks, But Attackers Still Win

Median global dwell time dropped to 11 days in 2024*, with ransomware actors notifying victims within 5 days on average - via ransom note.

While this shows progress in detection, it also reflects attackers' accelerated tactics. They want to be seen quickly to start negotiations.

The fix

- Fast detection is good, but preemptive blocking is better.
- If you don't already have use-case driven threat hunting & alert triage plans mapped to MITRE ATT&CK, start now.

*In 2023, median global dwell time was 10 days, in 2022 it was 16 days, & in 2014 - as a long-term reference - was 205 days.

Third Parties Are Now Prime Targets

Attackers are increasingly abusing the trust placed in vendors whether they host your data, connect to your systems, or supply your software.

30% of breaches in the DBIR involved a third party. That's double the previous year.

The Snowflake and MOVEit events highlight how stolen credentials, poor vendor hygiene, or unpatched tools can become enterprise-wide disasters.

Mandiant echoed the concern: supply chain compromise, SaaS credential abuse, & even fraudulent job applicants (e.g., DPRK IT workers) created serious risk.

IC3 reported similar trends via Business Email Compromise (BEC) and tech support scams targeting vendor relationships

Risk reality check

- Third-party questionnaires are not enough. You need visibility into vendors' access, controls, & defaults.
- Focus on identity, not just connectivity. Stolen vendor credentials caused major incidents in 2024*.
- Not all vendor risk is tech. Fraud, impersonation, & workforce exploitation are now in scope.

*Hundreds of customer environments were compromised via stolen credentials from Snowflake clients. Change Healthcare was breached in 2024 via stolen remote access credentials lacking MFA, leading to ransomware deployment and widespread disruption across the U.S. healthcare system.

Where Perspectives Collide | Detection & Response Optimism

Mandiant is cautiously optimistic, noting that median dwell time remains historically low (11 days), & nearly half of intrusions are caught within a week.

DBIR, in contrast, emphasizes that detection is still slow in many industries & that breach-to-discovery timelines often exceed attack timelines, especially in sectors like public administration or manufacturing

Disagreement

Whether detection is genuinely improving across the board, or only among the most mature organizations.

Where Perspectives Collide | Phishing vs Exploits vs Credentials

Mandiant downplays phishing slightly, showing a decline in phishing as an initial infection vector (from 17% to 14%), with exploits and stolen credentials dominating instead.

DBIR still shows phishing as the top human-related attack pattern and suggests it's tightly coupled with credential theft but notes that exploitation is rising sharply.

IC3 says phishing is one of the most common complaint types but doesn't always distinguish it as an initial access method.

Disagreement

Which attack vector leads & whether credential theft should be counted separately or as a byproduct of phishing.

Where Perspectives Collide | Ransomware Loss Estimates

IC3 reports $12.4 million in ransomware losses which is a tiny fraction of what's estimated elsewhere. This is because IC3 data only includes losses reported through their complaint system.

Mandiant treats ransomware as a major threat that is involved in 21% of all incidents, & almost always paired with data theft or extortion.*

DBIR acknowledges that ransomware volume has plateaued, but impact is growing, especially when it hits operational or third-party systems.*

Disagreement

How much damage is ransomware actually causing, and whether current reporting reflects the true scale.

*Mandiant does not estimate total losses. DBIR does not quantify ransomware losses but notes rising impact from operational disruption; median BEC loss was $50K.

The 2025 threat landscape is all about trust

Attackers are exploiting human trust (admin calls, fake recruiters, phishing), technical trust (SSO tokens, unpatched appliances), & institutional trust (call centers, cryptocurrency hype).

The most resilient organizations will be those that re-align identity, vulnerability, & fraud strategies & treat resilience as a leadership challenge.

Want to stay ahead of tomorrow's threats?

Let's talk about how your organization can reduce risk, outpace evolving threats, and build smarter defenses for what's next

ResilientTech Advisors
inquiries@resilienttechadvisors.com