opentext™ Cybersecurity

2025

OpenText Cybersecurity Threat Report

opentext Cybersecurity

Table of Contents

Foreword

The cybersecurity landscape in 2024 continued to show worrying trends, and even seemingly good news carried ominous overtones. Rapidly advancing AI capabilities enabled ever more sophisticated attacker tactics. Mainland Europe became one of the riskiest regions in the world as geopolitical conflict carried over into cyberspace. Meanwhile, notable law enforcement success against LockBit only underscored the limitations of such measures against an affiliate-based ransomware industry.

The ongoing war between Russia and Ukraine heavily influenced 2024 cyberattack patterns well beyond the immediate conflict zone. European businesses and government institutions found themselves in the crosshairs of threat actors linked to Russia. As the Kremlin's cyber tactics grew more aggressive, the EU cybersecurity agency reported a twofold rise in disruptive attacks in recent months. "This is part of the Russian war of aggression," an EU official warned, "fought digitally across Europe."

Pro-Russian hacktivist groups played a prominent part in this activity. These loosely organized independent threat actors conduct DDoS attacks, defacements, and data leaks in support of Moscow's agenda. One such group has claimed over 6,600 attacks since the war began in 2022, 96% against European targets including government websites, airports, media outlets, and companies. Meanwhile, state-sponsored Russian hacking groups continued their campaigns of espionage and sabotage. Western security agencies disclosed that Russian intelligence units have "substantially dialed up" their cyber operations against NATO members since the Ukraine invasion.

Numerous high-profile breaches and ransom incidents have made it clear that Russia has removed any remaining constraints on third-party attacks against the West while launching more state-directed and ideologically motivated attacks of its own. This convergence of criminal and state-sponsored threats—often blurred—made 2024 an extremely challenging year for Europe's cybersecurity. In fact, the infection rate in Europe is now 3 – 4 times higher than in the U.S.

Law enforcement did notch a notable success with the February 2024 takedown of LockBit's servers, including its dark web leak site and affiliate infrastructure. Officials obtained roughly 1,000 decryption keys and made several arrests. While the group remained operational throughout 2024, it was clearly weakened by the joint FBI-Europol operation. But celebrations were muted. As ransomware continues to grow unchecked, gangs rely on an underground ecosystem of affiliates to carry out attacks in exchange for a share of the payment. It's these lower-level associates who take the risk. If they're caught, the leadership simply lays low on the beach for a few weeks, rebrands under a new name, and goes right back into business.

Meanwhile, the impact of ransomware attacks has grown more dire. In the past, gangs would restrain or reprimand affiliates who hit humanitarian targets such as hospitals or charities, and in some cases even provide decryption keys to the victim. This is no longer the case. As tensions rise, both state-sponsored and independent ransomware gangs are wreaking havoc indiscriminately.

We'll explore these trends in more depth in this year's report. As organizations of all sizes face intensifying threats, our aim is to empower you with knowledge—together with comprehensive security solutions—to build smarter defenses and stronger cyber resilience.

> *Cybersecurity is no longer just an IT concern, it's a geopolitical imperative. As digital threats cross borders and motives blur, organizations must rethink what readiness truly means."*

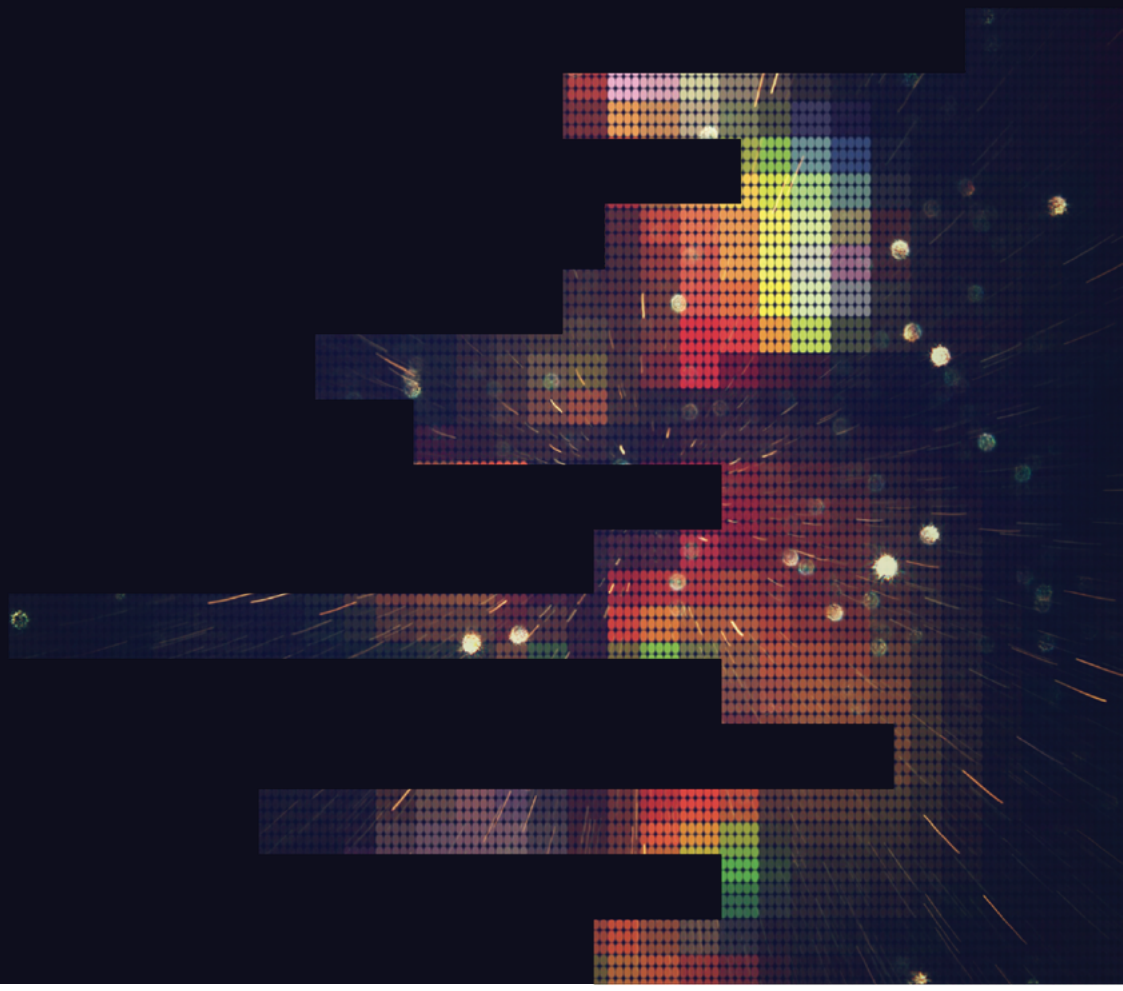
Muhi Majzoub
Executive VP,
Security Products

opentext Cybersecurity

Threat Intelligence Overview

This report is based on threat intelligence data collected from tens of millions of endpoints across the massive OpenText real-time file sensor network. We analyze files, email messages, and communications with malicious websites.

These endpoints encounter hundreds of thousands of never-before-seen application files every day. We classify these files by source, with business PCs seeing 73.8% of all new files, and consumer devices encountering only 26.2%.



Malware

2024 was a bad year for business PCs. The malware infection rate on these devices rose more than 28% to 2.39%, the highest since 2020. In 2023, we reported a slight uptick following a four-year decline. The latest data shows that this was no blip, but rather the beginning of a concerning upward trend.

Consumers weren't spared from rising infections. Following a similar curve, their rate had seen yearly declines from 8.68% in 2020 to 2.94% in 2022 before bouncing back to 3.01% last year's report. In 2024, the rate edged further upward to 3.07%—not exactly a spike, but still moving in the wrong direction.

It's hard to pin down the exact reason for this trend, but it's safe to assume that tools like generative AI have played a key role. Phishing attacks and social engineering schemes are becoming both easier to create and harder for users to recognize. We'll explore the latest phishing tactics later in this report, but it's clear that businesses have begun losing ground in the battle against these attacks. Renewed focus and effort will be essential to slow this trend.

While infection rates are rising, the prevalence of unique variants in these attacks has plateaued in recent years, ranging from a low of 86.2% in 2019 to a high of 87.5% in 2022, coming in this year at 86.5%. This tactic is here to stay, and for good reason. By versioning their malware on a per-infection basis, attackers can evade signature-based defenses. For businesses, this makes it especially important to implement antivirus protection with per-endpoint telemetry. By capturing a wide range of data from each device, such as process creation, network connections, and registry modifications, organizations can detect and block novel malware variants not seen before.

The percentage of malware variants seen on only a handful of PCs has remained consistent as well, with 2024's rate of 11.6% hovering within the range of previous years. Infections seen more frequently on 11 – 100 endpoints are relatively rare at 1.7%, also firmly in the middle of the recent trend.

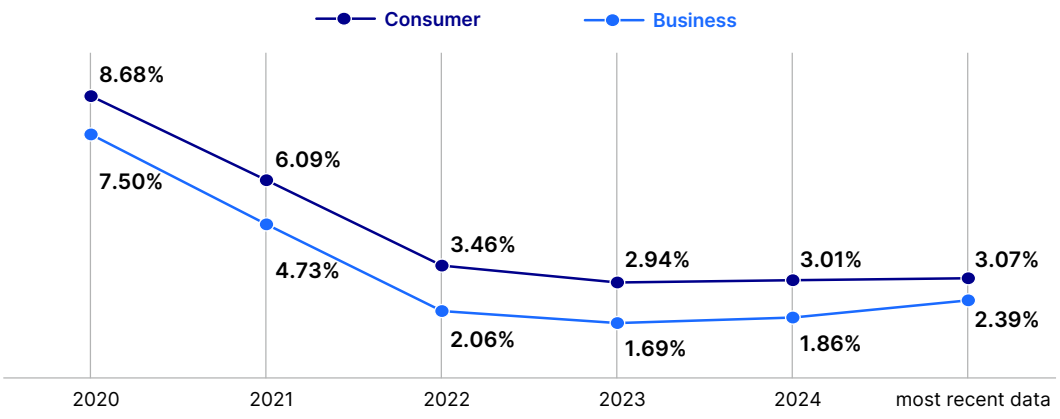


Figure 1: Malware infection rates: Consumer vs. business PCs, 2020-2024

The importance of a multi-layered approach for cyber resilience

Security experts have long advised that multiple layers of protection are essential to reduce malware infections, and the data continues to bear this out.

OpenText customers who implement security awareness training in conjunction with endpoint protection see 7.3% fewer infections than those who rely on endpoint protection alone.

OpenText customers who combine DNS protection with endpoint protection see 19.4% fewer malware infections than those who use just endpoint protection.

Infection rates: Consumer vs. business PCs

Business PCs traditionally see a much lower infection rate than consumer PCs. That's understandable, as cybersecurity teams leverage both expertise and resources that few private individuals could muster. The gap narrowed dramatically in 2024, however—perhaps due to greater attacker success in undermining user training efforts with more sophisticated delivery tactics.

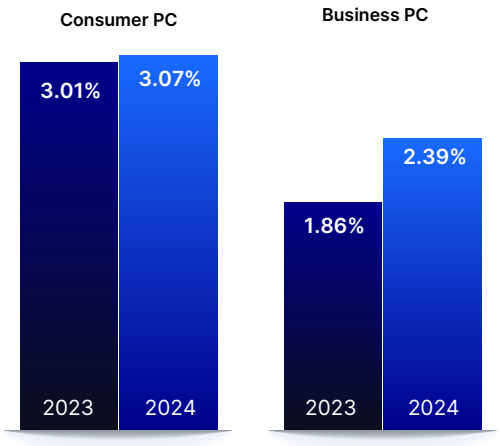


Figure 2: Infection rates: Consumer vs. business PCs, 2023-2024

For consumers, the overall infection rate increased slightly last year from 3.01% to 3.07%, a negligible 1.99% rise. Businesses, on the other hand, spiked by an alarming 28.49% from 1.86% to 2.39%. That's still significantly behind the consumer rate, but the idea that attackers are eroding the effectiveness of established cybersecurity teams should give business leaders pause.

In a glimmer of good news for businesses, re-infection rates were somewhat lower on these endpoints than on their consumer counterparts. Of all the consumer endpoints encountering an infection in 2024, 56% saw an additional infection over the course of the year. Businesses were more successful in preventing a recurrence with only 43% of infected endpoints seeing an additional infection in 2024. This underscores the importance of post-compromise user education. A malware incident can be a valuable opportunity to make an impression on those affected—and inspire greater vigilance with improved hygiene moving forward.

> *Given the continuous advancements in AI and the fact that all great innovative technologies are used for both good and nefarious reasons, I expect 2025's infection rate trend to continue in the wrong direction."*

Grayson Milbourne
Security Intelligence Director

Malware

Malware can lodge nearly anywhere in an endpoint filesystem, or even be fileless in some cases. But the overwhelming majority—81.8%—hides in just a few locations. Among businesses, the distribution across these locations saw moderate shifts in 2024: 21.4% in the Temp folder, down from 22.7% in 2023; 26.6% in AppData, up from 22.6%: 11.8% in Downloads, down from 15.2%; and 9.6% in Desktop, up from 8.0%. Business paths accounted for about 8% of the total, broken out into 7.6% for %WinDir% and 9.8% for %ProgramFiles%.

For consumers, on the other hand, the story of 2024 was a huge increase in the share of malware hiding in the Downloads folder, from 23.5% in 2023 to 37.6% in 2024—a more than 50% jump. With malware on the desktop rising from 12.1% to 13.0%, we now find more than half of consumer malware in the two most common locations for email attachments to end up. As we'll explore later in this report, threat actors are becoming increasingly adept at using AI tools to create more convincing phishing campaigns. Consumers are clearly taking the bait.

The operating system version you're on can have a significant impact on infections. Upgrading to the latest release can decrease malware risks, especially from a version that is no longer supported. In that light, it's good news that we're continuing to see rising rates of adoption for Windows 11 as Windows 10 prepares to follow Windows 7 into end-of-life this October. Among consumers, Windows 11—included on all new PCs sold—now accounts for 26.7% of all endpoints, compared with 44.1% for Windows 10. Businesses are lagging somewhat, with 64.7% still on Windows 10 and just 25.4% on Windows 11.

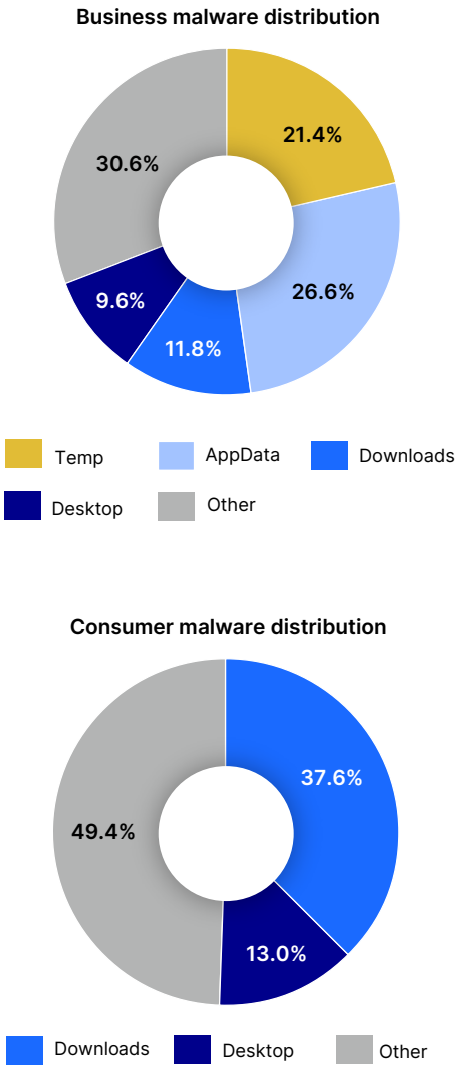


Figure 3: Malware distribution across business and consumer PCs in 2024

Infection rates by business size

The correlation of business size to infection rate remained largely unchanged in 2024. Simply put, smaller organizations are attacked less often and see fewer infections each time. Larger organizations are a more appealing target for attackers, often having both a broader attack surface and a bigger bank account to fund ransom payments.

But this isn't to say that small businesses are at less risk. The number of infections they see may be smaller in absolute terms, but they account for a far larger proportion of their organization. A half-dozen infections in a 20-headcount office is a far more serious matter than a 50-device infection in a 10,000-employee enterprise.

At the small end of the scale, 4.6% of businesses globally with 20 or fewer licensed PCs experienced an infection, with an average of 4.9 PCs impacted. Larger businesses ranging from 21 to 100 licensed PCs had a 27.8% infection rate with an average of 6.7 PCs affected. Moving up the scale, those with 101 to 500 licensed PCs experienced a 58.7% infection rate, with an average of 14.6 PCs affected. In each of these cases, the infection rate was slightly lower than in 2023, while the number of affected devices rose. The largest businesses with more than 500 licensed PCs saw an overall infection rate of 85.0%, with 40.1 PCs impacted on average, both slightly lower than last year.

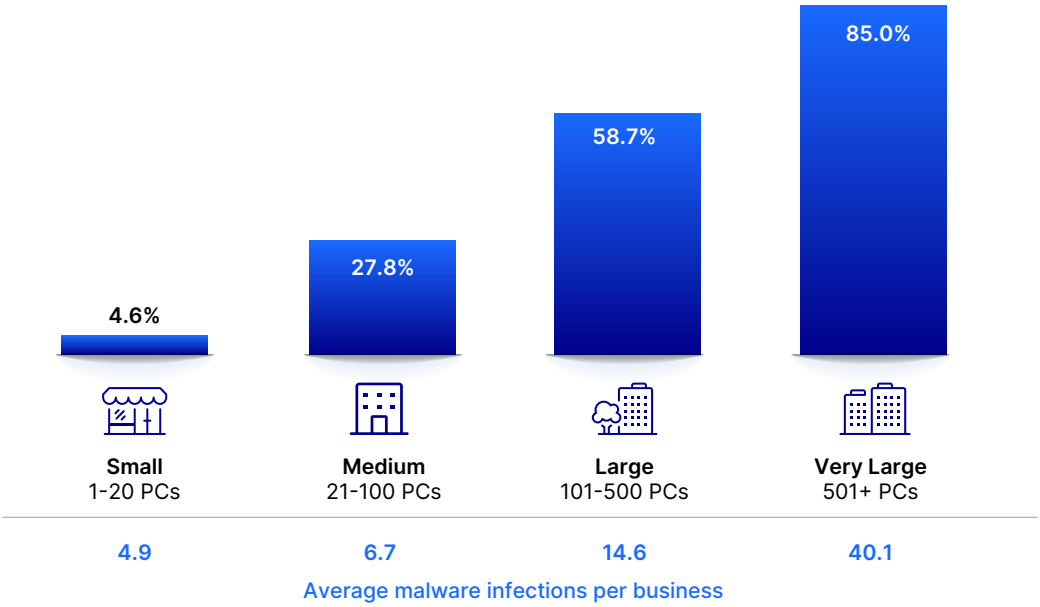


Figure 4: Malware infection rates by business size, 2024

Infection rates by region

Europe's bad year shows up clearly in our 2024 infection rate heat map. In the past, the region's relatively low malware incidence has traditionally placed it in the "less risky" grouping alongside Australia, New Zealand, Japan, North America, and the UK. However, Europe's rate has now overtaken that of South America, 2.3% to 2.1%. As a result, we've had to shift the continent to the "more risky" group with South America, Asia, Africa, and the Middle East.

The differences between these two groups are stark. "More risky" regions collectively see six times the overall infection rate of "less risky" regions, 7% vs 1.18%. Among consumers, the disparity is 6.6% to 2.2%, a threefold difference. Among businesses, the gulf is even wider, with a 5.1% infection rate for riskier regions compared with 0.9% for those less at risk.

As discussed earlier, the rising geopolitical tensions surrounding the Ukraine-Russia war are having a clear impact on the threat landscape across the continent. Ransomware gangs based in Russia or Russian-occupied territories have felt emboldened to hit European companies and critical services without fear of punishment by Russian authorities. In fact, Europe emerged as the top target region for many financially motivated groups as well, second only to North America in total cyber extortion cases.

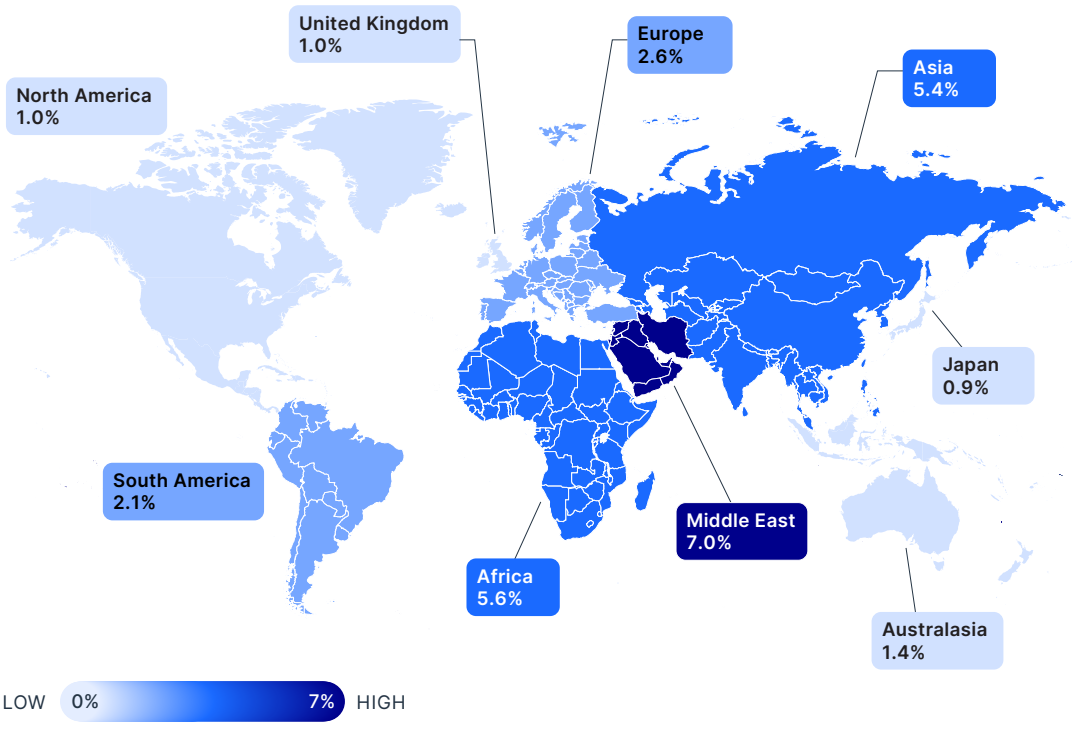


Figure 5: Malware infection rates by geographic region, 2024

Infection rates by industry

Survey respondents have the option of sharing which industry vertical they're in, and just under half did so. Among these, we noted sharp increases in several sectors:

Manufacturing

On an organization-wide level, these businesses were 42.4% more likely to see infected workstations than the overall average, up from 32.9% last year.

Information

38.4% more likely to see infected workstations, up from 23.5% last year—the largest increase reported in this year's survey.

Management of companies and enterprises

28.3% more likely to see infected workstations, up from 18.2% last year.

Public administration

27.3% more likely to see infected workstations, up from 14.8% last year.

On the other hand, after jumping into the second-highest slot last year with a 23.8% higher than average infection rate, educational services declined slightly to 23.2% this year. That's still enough to be the fifth most victimized sector, but these companies have managed to escape the surging infections elsewhere on the top-five list.

Meanwhile, last year's fifth most infected sector, mining, quarrying, and oil & gas extraction, has eased from a 15.5% higher infection rate to just 12.1% this year.

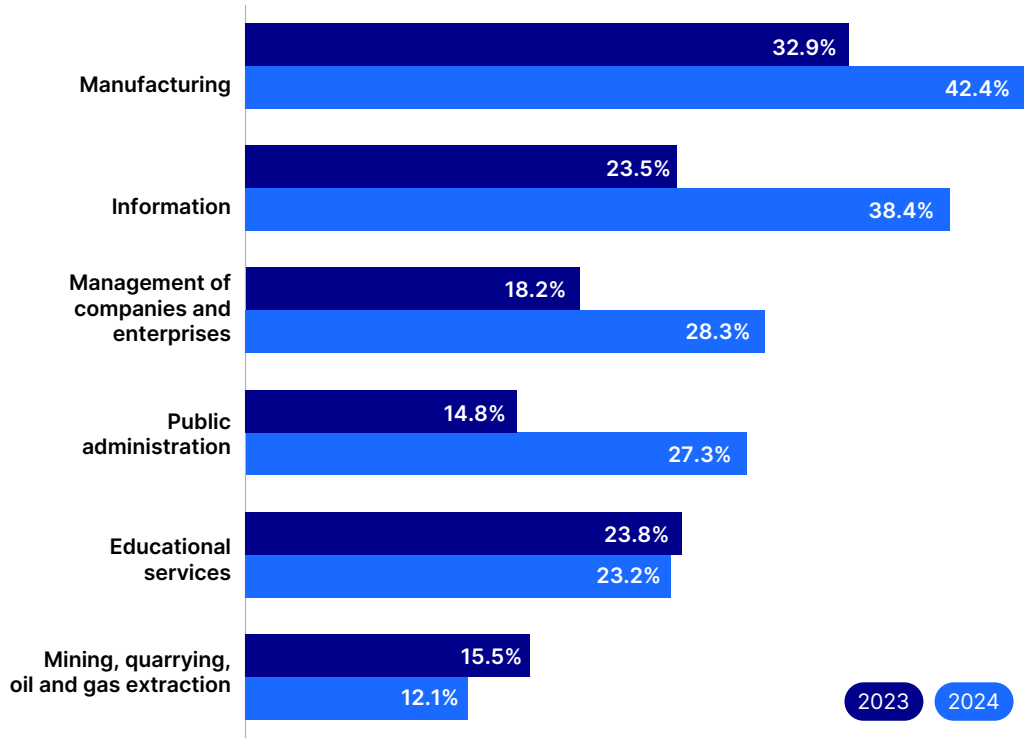


Figure 6: Malware infection rates by industry, 2023-2024

opentext Cybersecurity

Ransomware

As the ransomware threat continues to evolve and intensify, OpenText Cybersecurity launched its third annual survey of C-level executives, IT directors, and security professionals from businesses of all sizes in the U.S., UK, France, Germany, Australia and India. The 2024 report explored current cybersecurity sentiment and security postures, views on AI-powered cyber threats, and the impact of software supply chain attacks.

The survey captures a snapshot of ransomware running rampant. Almost half of respondents (48%) reported that their company has previously experienced a ransomware attack, a large majority of them within the previous year. Multimillion-dollar demands are now common, with 31% of payments falling between $1 million and $5 million. Smaller businesses may offer lower yields for attackers, but that doesn't keep them out of the line of fire. In fact, SMBs in our survey reported more ransomware attacks than large enterprises. But the news isn't all bad. With a majority of companies testing their recovery plans at least twice yearly, almost all respondents (97%) were able to successfully restore their organization's data using either backups or a decryption key provided by the attacker.

48%

of respondents reported that their company has experienced a ransomware attack.

Among the most recent ransomware victims, 46% made the demanded payment. This is notable in light of that 97% overall success rate for restoring data. If so many organizations are getting their data back without paying for decryption, why do so many continue to give in to attackers? Modern techniques like air gapping and immutability, combined with well-established best practices for testing, offer a high level of confidence in resilience.

But maybe decryption isn't the whole story. Attackers now commonly add a layer of extortion to their tactics, threatening to sell or publicize sensitive data that could subject the victim to humiliation, compromised trust, or damaged business relationships. In early 2024, Dark Angels used an extortion-only approach to extort $75 million from a Fortune 50 victim. As long as victims fear public shame, ransomware will remain a profitable business. The only solution is to remove this stigma. Breaches are inevitable; no organization is immune. If we can ease the shame, we can reduce attackers' leverage.

Ransomware

The rise of extortion-only attacks is a wake-up call: resilience can't stop at recovery. If your data has value, you're a target and reputational damage is the new ransom."

Tyler Moffitt
Senior Security Analyst

Companies are increasingly focused on the security of their supply chains—and rightly so. Even when you're doing everything right, a lapse by a connected third party can invite a breach. A full 91% of respondents were concerned about supply chain ransomware attacks, almost half (49%) to the point of considering changing vendors. 62% of the respondents who reported a ransomware attack in the previous year noted that it had originated from a software supply chain partner. In response, security collaboration and audits are becoming routine. Two-thirds of respondents planned to work with their software suppliers to improve security, and almost three-quarters assess vendor security at least yearly. On the vendor side, it's important to be able to respond effectively to collaboration requests and audits with clear information about your current security practices—backed up with the data needed to build customer and partner confidence.

While the need for better supply chain security speaks for itself, amplification can help. For 37% of respondents, regulatory compliance or cyber insurance requirements are the primary drivers for increasing ransomware defense investment within the software supply chain.

The OpenText survey also captured the impact of widespread AI adoption by threat actors. 55% of respondents believed that this trend puts their companies at greater risk of a ransomware attack. 45% of respondents saw an increase in phishing attacks due to AI's proliferation, including 69% of those who had experienced a ransomware attack. This rise makes user education more critical than ever. 91% of respondents require employees to participate in security awareness or phishing training, and 88% consider these measures very or somewhat effective.

Major developments in ransomware

Exfiltration-only attacks on the rise

A major shift in ransomware tactics throughout 2024 was the increasing reliance on data exfiltration-only attacks, often referred to as extortionware or ransomware without encryption. Traditionally, ransomware groups have encrypted victim files and demanded payment for decryption keys. However, many organizations have improved their backup and recovery strategies, reducing the effectiveness of encryption-based attacks. In response, cybercriminals are bypassing encryption altogether, instead focusing on stealing sensitive data and threatening to leak or sell it unless a ransom is paid.

This shift in tactics has several advantages for attackers:

- **Faster execution**
  Encrypting an entire network takes time, whereas exfiltrating data can be done stealthily over days or weeks.
- **Increased pressure**
  Victims face reputational damage, legal liability, and compliance fines if sensitive information is leaked.
- **Broader range of targets**
  Even organizations with strong backup solutions remain vulnerable to extortion.

In 2024, numerous ransomware groups embraced this approach, with BlackCat (ALPHV), RansomHub, and 8Base among the most active in pure data exfiltration extortion schemes. As long as companies store valuable information, the threat of data leaks will remain a powerful source of leverage for cybercriminals.

LockBit crackdown—a developer arrested, but the group lives on

While the February 2024 Operation Cronos law enforcement takedown weakened LockBit, the group continues to operate. One of the biggest developments came later in the year when a LockBit developer was arrested in Israel and extradited to the U.S. The unnamed individual is believed to have played a key role in the development and refinement of LockBit's encryption malware.

Despite this arrest, LockBit remains one of the most active ransomware groups. Its affiliate-based model ensures that attacks continue even when leadership is disrupted. The group's leader, known as "LockBitSupp," remains at large and has openly mocked law enforcement efforts. The group's resilience highlights a key challenge in combating ransomware: even after infrastructure seizures and high-profile arrests, the decentralized nature of ransomware-as-a-service (RaaS) means new affiliates and revised malware variants keep operations running.

While LockBit continues to operate under the same name following the crackdown—perhaps to flaunt its supposed invulnerability—it's one of the few RaaS gangs to do so. More often, groups subjected to law enforcement pressure adopt a lower profile until the heat dies down, and then resume operations under a new brand. As ringleaders evade arrest, authorities increasingly target their affiliates in hopes of undermining the trust that the relationship hinges on. A similar approach was used in the 2023 takedown of Genesis Market, in which customers of the marketplace's stolen access credentials faced jail time. Lower-level criminals may be more easily intimidated or deterred by such operations than masterminds like LockBitSupp.

Ransomware

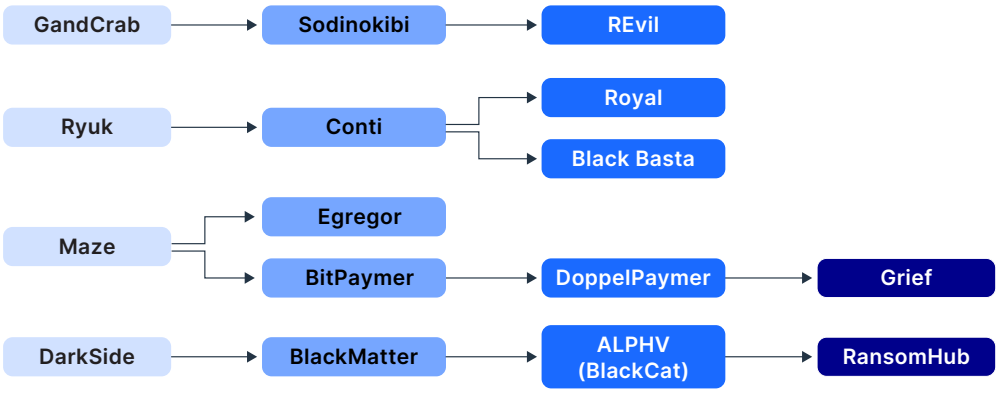


Figure 7: Rebranded ransomware identities

Exploiting unpatched systems—the role of ESXi, firewalls, and misconfigurations

Many of the most devastating ransomware attacks in 2024 had nothing to do with sophisticated exploits or zero-days. Instead, they were the result of unpatched systems and insecure configurations. Several ransomware groups focused on widely known yet often ignored vulnerabilities in enterprise environments, in particular:

ESXi virtual machines (VMs)

Attackers exploited vulnerabilities in outdated ESXi hypervisors to gain access to entire virtualized infrastructures.

Firewall and VPN weaknesses

Unpatched Fortinet, SonicWall, and Palo Alto Networks devices were frequently compromised, allowing attackers to pivot into corporate networks.

Default credentials and open management ports

Many victims failed to secure remote access tools, leaving RDP, SSH, or VNC exposed to the internet.

The lesson from 2024 is clear: Many ransomware attacks aren't sophisticated—they're preventable. Cybercriminals are increasingly using automated tools to scan for vulnerable systems, so any delay in patching or hardening defenses is an open invitation for attack. Organizations must prioritize vulnerability management, continuous monitoring, and network segmentation to reduce their exposure.

Other key trends from 2024

Double and triple extortion become standard

Many ransomware groups now combine encryption, data theft, and direct pressure tactics (e.g., contacting customers, partners, or regulators to force a ransom payment). This escalation increases pressure on victims and raises reputational risk.

Ransomware-as-a-Service (RaaS) grows more professionalized

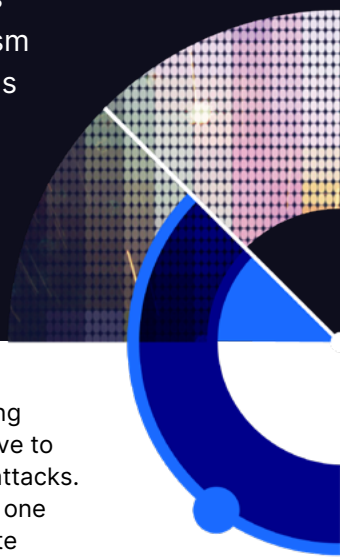
Some groups are moving toward a franchise-style model with customized playbooks, affiliate dashboards, and even customer support channels to manage negotiations.

New attack surfaces: cloud and identity attacks

Instead of targeting endpoints, attackers are breaching cloud environments, stealing API keys, or abusing identity services like Okta & Azure AD to bypass MFA. Cloud ransomware incidents saw a surge in 2024 due to poor identity and access management (IAM) controls.

Phishing

Phishing attacks continued to become much more targeted, customized and precise in 2024. Generative AI has made it much simpler to customize messages at massive scale as well as to improve the fluency of their wording and the realism of their branding, eliminating many of the errors that users count on to flag bogus emails. Attackers are evolving from generalized spray-and-pray tactics to more personalized campaigns that can achieve higher open and click-through rates. Routine phishing looks more like sophisticated spearphishing every day.



Phishing volume peaked in the fourth quarter of 2024 as the holiday season approached, followed by May, when many SMBs are working to meet deadlines for income tax extensions. The prevalence of spearphishing tactics trended upward throughout the year, often correlating with higher overall volume. In the peak month of November, 56.56% of total phishing attacks were spearphishing, the year's highest rate. This emphasizes the increasing ease of personalization: attackers don't have to sacrifice volume to deliver more targeted attacks. That's a highly worrying development, and one that underscores the vital role of up-to-date awareness training. Savvy users can be at risk of complacency, thinking that they know what to look for but oblivious to the latest attacker capabilities.

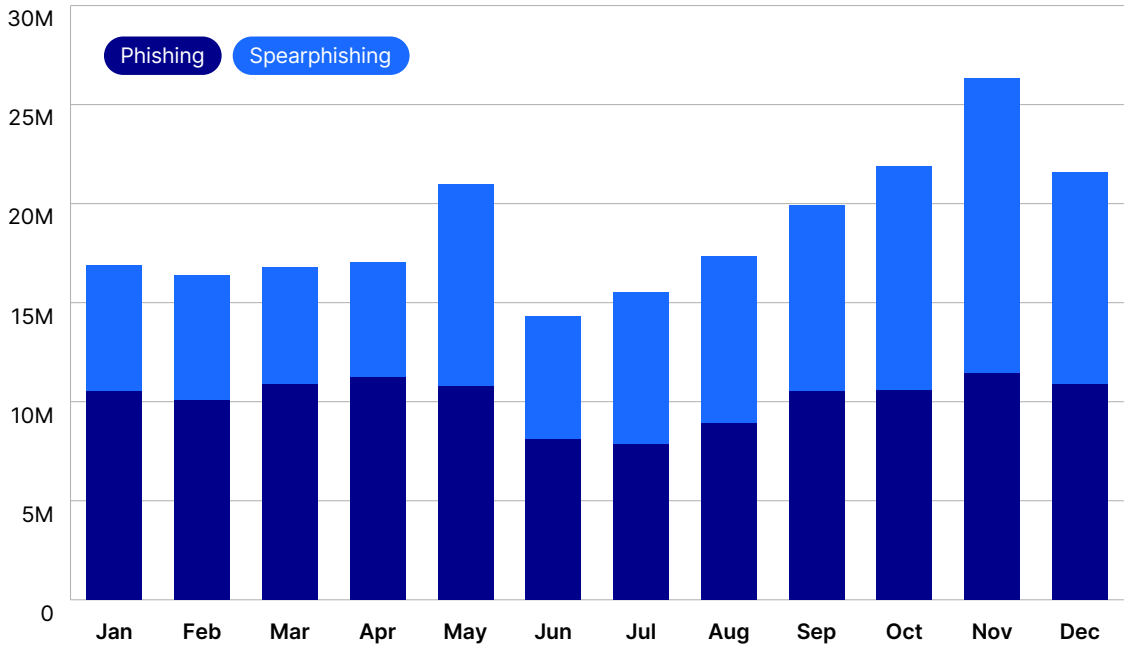


Figure 8: Phishing and spearphishing attacks in 2024

Malware and attachments

Throughout 2024 we quarantined over 235 million emails with malware attachments. Of these, roughly a quarter originated in the US—understandably, given the geographic distribution of our customer base. Next in prevalence, an uptick in malware attacks originating in Kazakhstan brought that country to second place and bumped Netherlands down to third, followed by Uzbekistan, China, and Russia. The share of all email traffic containing malware ranged from a low of 0.42% during the slow summer month of August to peaks of 2.50% in April and 1.92% in October.

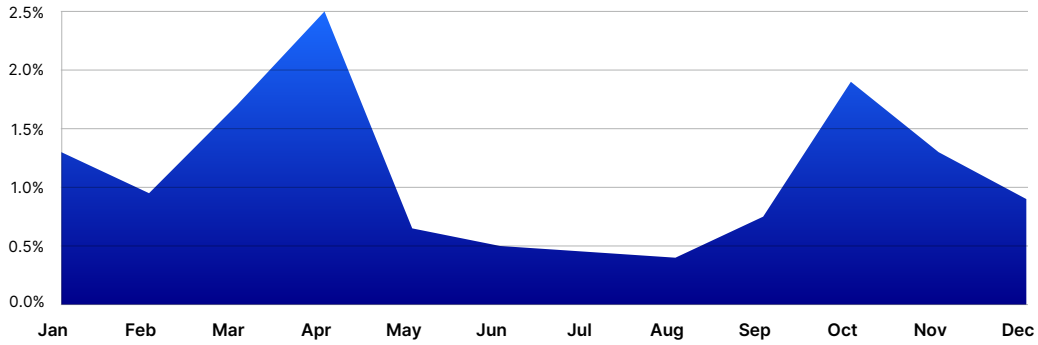


Figure 9: Malware attacks as a percentage of total email traffic, 2024

Last year saw a dramatic change in attacker tactics. While email attachments remain a popular malware delivery method, the majority—53%—now take the form of .zip files, followed by 20% using .htm, formerly the most popular format, 7.5% using pdf, and 5.6% each for .doc/x 5.6% and .rar 5.6%. Instead of relying on documents that run scripts or direct to an .htm script, attackers are placing malware directly in the .zip folder. In our view, the reasons for the surging popularity of .zip are twofold. Years ago, the occurrence of malicious internet-bound macros in Microsoft documents led that company to remove such macros from attachments by default. In response, attackers pivoted to delivering .htm files with a link inviting prospective victims to download a file. As users have grown more wary of this approach, .zip has come into favor as a type of format that is commonly used for attachments, very difficult to sanitize, and less associated with malware in recent years.

.zip also offers an advantage in terms of social manipulation. These files often arrive password-protected, with the password provided in the body of the email. This can trick the user into thinking that the file is both legitimate and secure—and they end up running the malware as a result.

> *Phishing attacks are shifting away from traditional "spray and pray" tactics, with a notable decline in URL and text-based email threats. This trend suggests that cybercriminals are moving toward more sophisticated, highly targeted attacks rather than mass-distributed schemes."*

Troy Gill
Sr. Manager,
Threat Research

Obfuscation tactics

As users become more wary, threat actors become more creative in concealing their attacks. Recent innovations include QR codes opening links to malicious websites, or quishing; more convincing telephone-oriented attack delivery (TOAD), in which cleverly branded email messages urge the recipients to call a number regarding an overdue account or other serious matter; and the use of legitimate services to conduct phishing attacks. This last tactic, known as "living off the land" (LotL) phishing, has become especially popular over the last year.

In LotL phishing, threat actors use the URL of a legitimate service to redirect users to a malicious site, or to host the phishing payload itself. Because the service is also used for legitimate business purposes, it can't be blocklisted, leaving users at the mercy of a link they have every reason to believe is genuine. While the 171.1 million instances of this tactic in 2024 represent a decrease of 14.3% from 2023, we also noted sharp increases in the abuse of several services, including Amazon AWS, which rose 22.5% to over 13.4 million. New entrants to our "Top 10 Abused Services" list for 2024 included List-manage (Mailchimp), Canva, and Cloudflare IPFS. Google APIs took the top spot at over 75 million, and a separate entry for Google Docs made an appearance as well with over 2 million occurrences.

Email threats can hide in endless ways, including many URL and text-based scams. In 2024 we quarantined around 7.3 billion of these, a slight decrease from the previous year. Volumes remain relatively flat as threat actors focus on maximizing efficacy and efficiency through attention to detail, as explored in our earlier discussion of spearphishing.

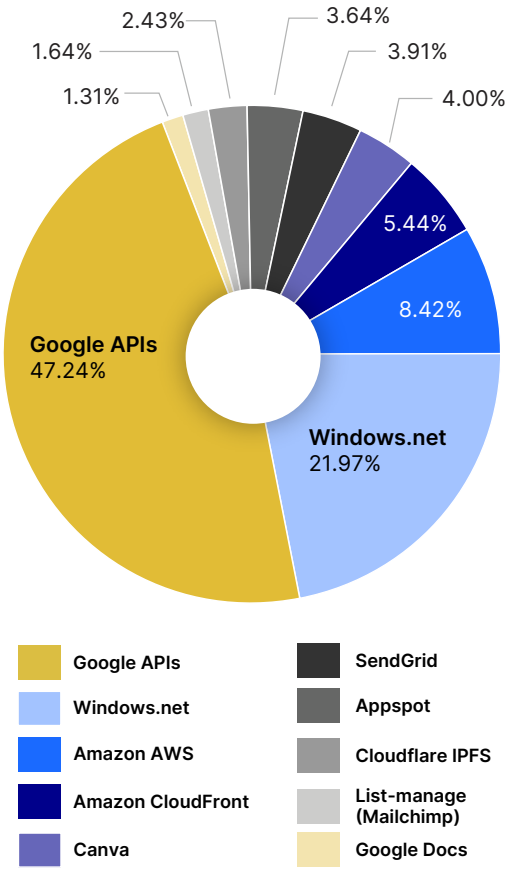


Figure 10: Top ten abused services in 2024

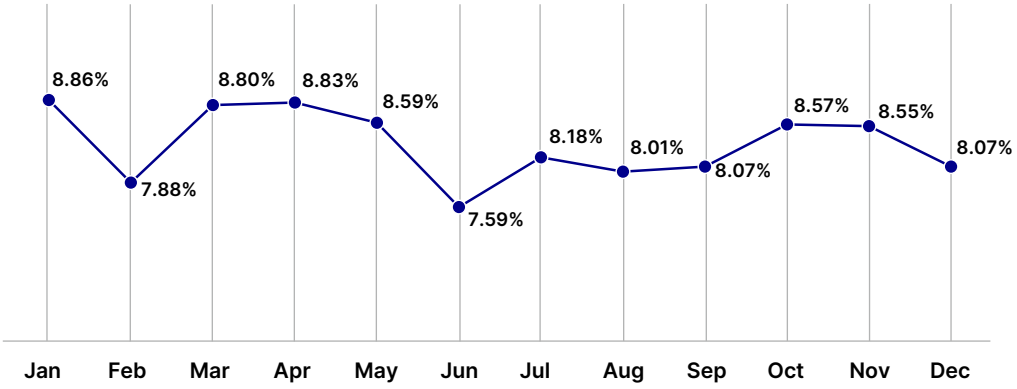
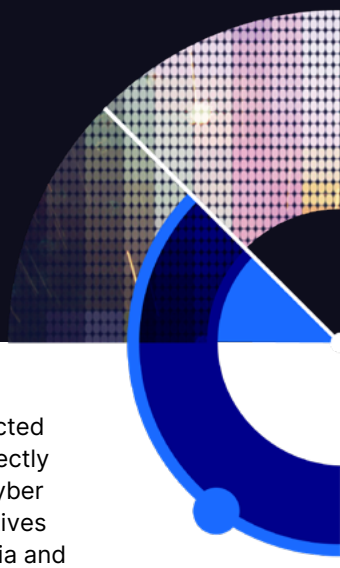


Figure 11: 2024 Monthly share of URL and text-based threats, including spam and phishing

Cybersecurity outlook for 2025

Looking ahead to 2025, experts anticipate that both political changes and threat actor adaptations will shape the cyber landscape. A significant wildcard is the potential return of a Trump administration in the U.S. and how it might alter international cybersecurity efforts—especially regarding Russia.



Under President Biden, the U.S. led a strong international stance against ransomware and state cyber threats, forging alliances such as the 60-nation Counter Ransomware Initiative and pressuring adversaries like Russia with sanctions and offensive operations. In contrast, President Trump's "America First" approach could shift priorities in ways that worry cyber defenders.

As 2024 turned to 2025, we saw signs that the new administration might scale back efforts to confront Russia in cyberspace. Reports emerged that U.S. Cyber Command had been ordered to pause or dial down planned cyber offensives against Russia. A leaked DHS memo also suggested that CISA's analysts were being directed to focus less on Russian threats and more on other adversaries, sparking concern that Washington might deemphasize the Kremlin's cyber activities. Homeland Security officials subsequently rebuked this notion, insisting that there's been "no change" and that Russia remains on the radar. Even so, the perception of a policy shift exists. Such a stance would represent a dramatic pivot: U.S. leadership in global cyber crackdowns could wane if combating Russian hackers is no longer a top priority.

Indeed, Western European allies are uneasy. Cyber chiefs of NATO members warned that a retreat by the U.S. would leave a vacuum in the fight against ransomware and cyber-espionage at a critical moment. The past year showed Russia's cyber aggression is still on the rise, so any easing of pressure might embolden threat actors. There is also the question of support for Ukraine's cyber defense: the Trump administration is expected to reduce aid to Ukraine, which could indirectly benefit Russian operations. International cyber capacity-building programs and joint initiatives (like those that helped countries like Albania and Costa Rica recover from attacks) may be scaled back as foreign cybersecurity aid budgets are slashed. All of this points to a potential strategic shift in 2025—one where Russia and its criminal proxies might feel less constrained by U.S. actions, even as Europe and others try to keep collaborative enforcement efforts alive.

On the threat side, cybercriminals will undoubtedly evolve tactics in response to 2024's successes by law enforcement. Ransomware groups may change their business models or techniques. For instance, gangs could further reduce their reliance on encrypting files, which draws immediate attention, and focus on pure data theft and extortion, or on destructive attacks masked as something else.

Some criminals are already diversifying, targeting smaller businesses (which saw a 2024 surge in incidents) or exploiting third-party supply chains to indirectly breach bigger targets. Such supply-chain threats loom large in 2025: After the high-profile MOVEit file-transfer hack in 2023 and others, attackers learned that compromising one software vendor can unlock dozens of victims. We expect more such exploits aimed at software providers or managed service firms, allowing ransomware or espionage to propagate widely.

Within 72 hours of CrowdStrike's July 2024 outage, our Analysts detected over 400 lookalike domains linked to the ensuing social engineering campaign. Attackers mimicked legitimate CrowdStrike resources to offer fake support and spread malware disguised as remediation tools. These opportunistic attacks are a growing threat, exploiting urgency as businesses face increasingly crippling outage costs."

Serena Peruzzi
Sr. Manager,
Web Analysis

Cybercriminal marketplaces for initial access are also likely to stay busy. Infostealer malware infections continue to feed credentials to the underground, enabling a rash of account takeover and network intrusions. New infostealers will pose ongoing issues, and RedLine could resurge in some form given that its source remains at large.

The weaponization of AI has been relentless and will continue to be so. In 2024, hackers used generative AI for phishing and misinformation. In 2025, this could escalate to AI-driven attack automation, conversational phishing bots, or more convincing deepfake scams.

Nation-state actors might up the ante as well. For example, U.S. experts predict that China will intensify its cyber-espionage, quietly planting backdoors in critical U.S. infrastructure as geopolitical tensions simmer. If the U.S. shifts focus to countering China, we could see even more China-origin attacks (and potentially fewer restraints on Russian hacking as mentioned). Back in 2018, a Chinese computer manufacturer was reported to have installed a spy chip on the motherboards of computers sold to several major U.S. companies, a leading cloud vendor, and the U.S. Department of Defense. In March 2025, the Chinese-made Bluetooth chip used in over a billion devices worldwide, including the majority of IoT devices, was found to contain undocumented commands that could be used in attacks. The capability for a major offensive operation is likely in place. The question is whether or when one might take place.

For defenders and law enforcement, 2025 will demand adaptability. Cyber agencies may need to adopt more aggressive pre-emptive operations, similar to those conducted against TrickBot and QakBot, to take down threats before they spread. Such operations require global cooperation. With a possible change in U.S. posture, other countries and transnational alliances such as the EU and Interpol might step up leadership in coordinating takedowns of ransomware infrastructure or sanctioning cybercriminals' crypto flows. However, we also anticipate a continued blurring of the line between criminal and state-sponsored attacks, which can complicate the government's response through law enforcement and national security agencies. And as long as certain countries (like Russia) provide safe havens, the "Whac-a-Mole" game will continue.

Ultimately, while the law enforcement efforts of 2024 achieved real progress, the cybercriminal ecosystem is already regrouping. The trajectory for the coming year will hinge on whether the international community can maintain collective pressure against threat actors—or whether shifts in geopolitical priorities will give those actors an opening to regain strength. Either way, organizations should brace for an evolving threat landscape in 2025, armed with the hard-won lessons from a tumultuous 2024.

opentext Cybersecurity

Recommendations to maintain cyber resilience

Attackers never rest—and neither can their potential victims. As ransomware gangs continue to diversify their techniques, infections can arrive through many vectors and execute schemes in multiple ways. Even the strongest preventive measures can't offer complete protection, as human error, zero day vulnerabilities, and other entry points inevitably leave organizations of all sizes at risk. It's not a question of whether you'll be breached, but when, how, and what you'll do next. Prevention remains essential to mitigate risk, but to ensure cyber resilience, it must be complemented with rapid recovery.

Ransomware attackers are capable of breaching each layer of your environment individually, so no single defensive measure can block every threat. On the other hand, it's much more challenging to breach every layer at the same time—making multi-layered, defense-in-depth strategies far more effective. By adopting comprehensive security technologies and best practices from the endpoint to the network gateway to the data center, and everywhere in between, you can greatly reduce your exposure to attack. User training provides an essential additional layer of vigilance.

As you're working to prevent breaches, you must also prepare to respond to them. Security teams need to be able to detect infections early, act quickly to stop their spread, identify and neutralize the threat, and prevent similar incidents in the future. A rapid recovery capability is critical to restore the data and applications your organization depends on. Don't underestimate the time factor. When your systems are down, so is your business. Frequent testing for backup and restore operations will help you assess your readiness to meet SLAs for restore point objective (RPO) and restore time objective (RTO). True cyber resilience means being able to get back to work quickly no matter what happens. This strategy will not prevent all ransomware infections. Cyber resilience also entails preparing your organization to respond to ransomware attacks that slip through the cracks. This means maintaining robust incident response capabilities, so that security teams can act quickly to stop an initial infection from spreading. It also means testing your backup systems so that you can be confident that you could restore critical systems and data in time to protect the continuity of your operations, should the worst-case scenario occur. Finally, you should re-evaluate your cyber resilience plan on a regular basis to ensure that it has been updated to reflect the most prevalent current threats.

Recommendations to maintain cyber resilience

Your cyber resilience checklist includes:

- The ability to detect and quarantine malicious email attachments to block incoming threats.
- Timely, risk-prioritized vulnerability management across all servers and PCs.
- Antivirus and endpoint protection on every device on the network and in the organization.
- Multi-factor authentication (MFA) for all organizational accounts and resources
- Supply chain security collaboration and audits with software vendors and partners.
- Frequent, immutable, airgapped backups for critical files and systems.
- A disaster recovery plan that includes regular backup and restore testing as well as tabletop exercises for key stakeholders.
- Ongoing re-evaluation of your cyber resilience plan to ensure that it reflects current threats.
- Frequent and comprehensive security awareness training for employees, including updated guidance on the latest phishing tactics.

Given the scope of this list, it can be difficult for organizations to keep up with even baseline best practices for security. In that light, it's understandable that managed security service provider (MSSP) offerings are growing in popularity. By offering cybersecurity services on a subscription basis, such as monitoring, threat detection, and incident response, MSSPs can help businesses maintain more consistent, standards-based protection.

Whether you choose to work with an MSSP or address your cybersecurity needs in-house, the urgency of the situation is clear. As threats grow in sophistication amid uncertain global enforcement efforts, every organization must take responsibility for its own protection. The list above is a baseline—not an aspiration. When your business is at stake, comprehensive security is non-negotiable.

opentext™ Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.