Browse our categories

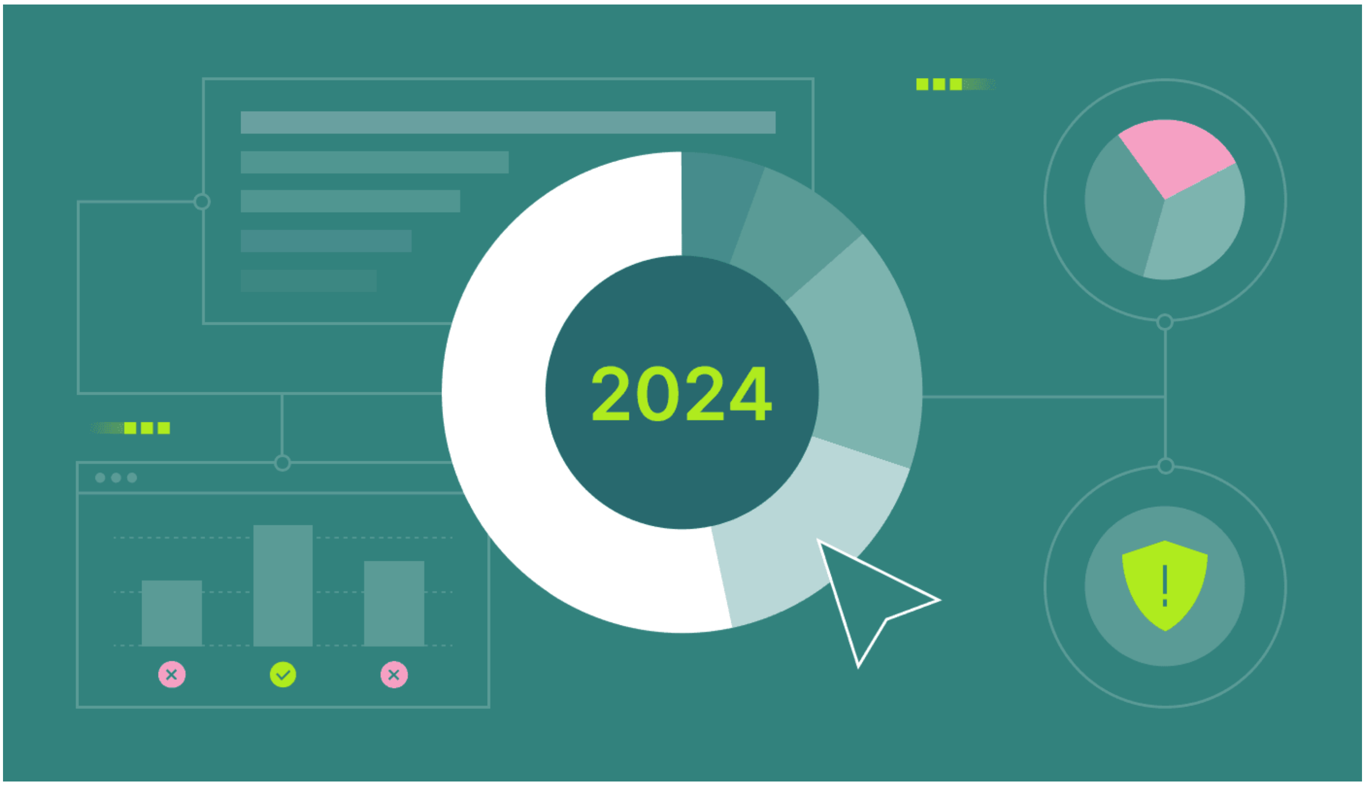
Blog / Trends & statistics

TRENDS & STATISTICS

Cybersecurity statistics 2024: key insights and numbers

Anastasiya Novikava

Dec 10, 2024 15 min read



> ***Summary:*** *Ransomware and cyber warfare surged in 2024. Learn which industries were targeted and how to protect your business moving forward.*

Each year, experts say it was the worst year for the cybersecurity industry and that it won't get better next time. It's true again for 2024.

One reason for this is the **National Public Data** breach— the second largest in history. It stole 2.9 billion records from people in the US, UK, and Canada. These records included full names, addresses, Social Security numbers, dates of birth, and phone numbers.

Another reason is the massive attack on **Change Healthcare**, the biggest healthcare data breach to date.

Finally, global cyber-attacks are now often called **cyber warfare**. Officials are even discussing whether it's time for the US to create a Cyber Force.

Even though there were no foreign cyber influences in the US elections this year that significantly affected the results, 2024 was still a tough year. It caused major damage to key sectors. Let's take a closer look at the details.

- **More cyber-attacks overall.** Amazon now tracks hundreds of millions more potential cyber threats daily. It went **from 100 million to 750 million threats per day** in just six or seven months. (The Wall Street Journal)

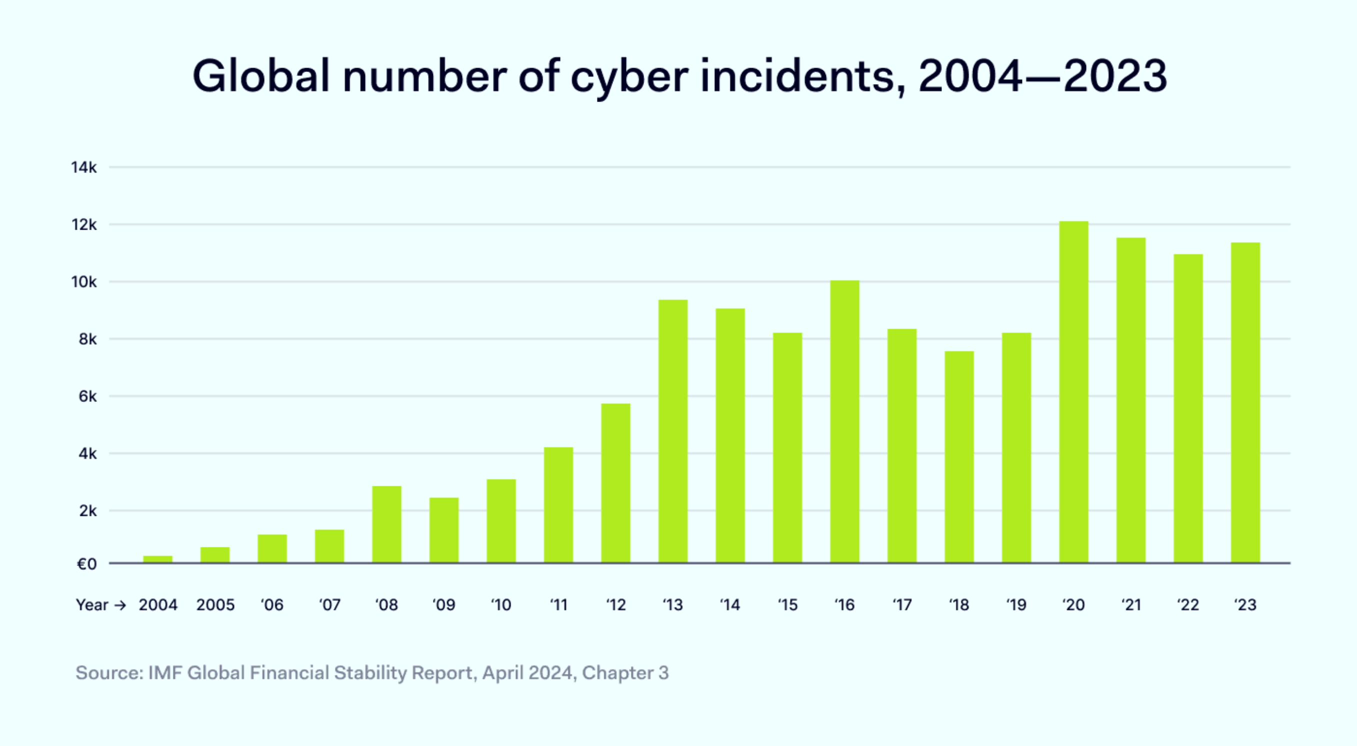
- **More DDoS attacks.** Distributed Denial of Service (DDoS) attacks rose by **46%** in the first half of 2024 compared to last year. Gaming and tech were hit the hardest. (Gcore Radar Q1–Q2 2024)

- **More ransomware attacks.** Major ransomware attacks are now much more common. In 2011, there were five big attacks a year. In 2024, there are **20 to 25 major ransomware attacks every day**. (The New York Times)

- **More election interference.** Cyber threats now pose a bigger risk to national security. There is more foreign influence on elections than ever before. Cyber-attacks aim to disrupt voting and elections. (Wired)

- **More financial impact.** Financial losses from cyber incidents have quadrupled since 2017. While most cyber-attack losses are small (around $0.5 million), major incidents can lead to huge damage. Once every 10 years, a company can lose up to $2.5 billion from a severe cyber-attack. (International Monetary Fund)

- **More regulations.** In 2023 and 2024, over **170 data protection laws** were introduced to fight data breaches. Companies are taking data security more seriously than ever. (MIT Sloan)


Global number of cyber incidents, 2004—2023

Source: IMF Global Financial Stability Report, April 2024, Chapter 3

In this article, we'll discuss in more detail the most targeted industries of 2024, the top cyber incidents, and key cybersecurity actions for 2025.

Most targeted industries in 2024

Some industries face more cyber-attacks because of the valuable data they hold. In 2024, healthcare and telecommunications stood out as prime targets for cyber threats.

Healthcare organizations

Healthcare organizations are prime targets because of sensitive data like patient records. According to Rebecca Wright, a cybersecurity professor at Barnard College, hospitals are particularly vulnerable to ransomware because they are hard to secure and rely on a mix of systems and third-party vendors.

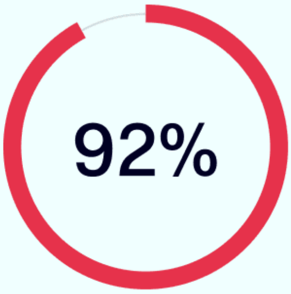
What's most concerning is that attackers often don't aim to steal data. Instead, **they aim to disrupt services to force hospitals to pay ransoms**.

Here's why healthcare stood out as a target in 2024:

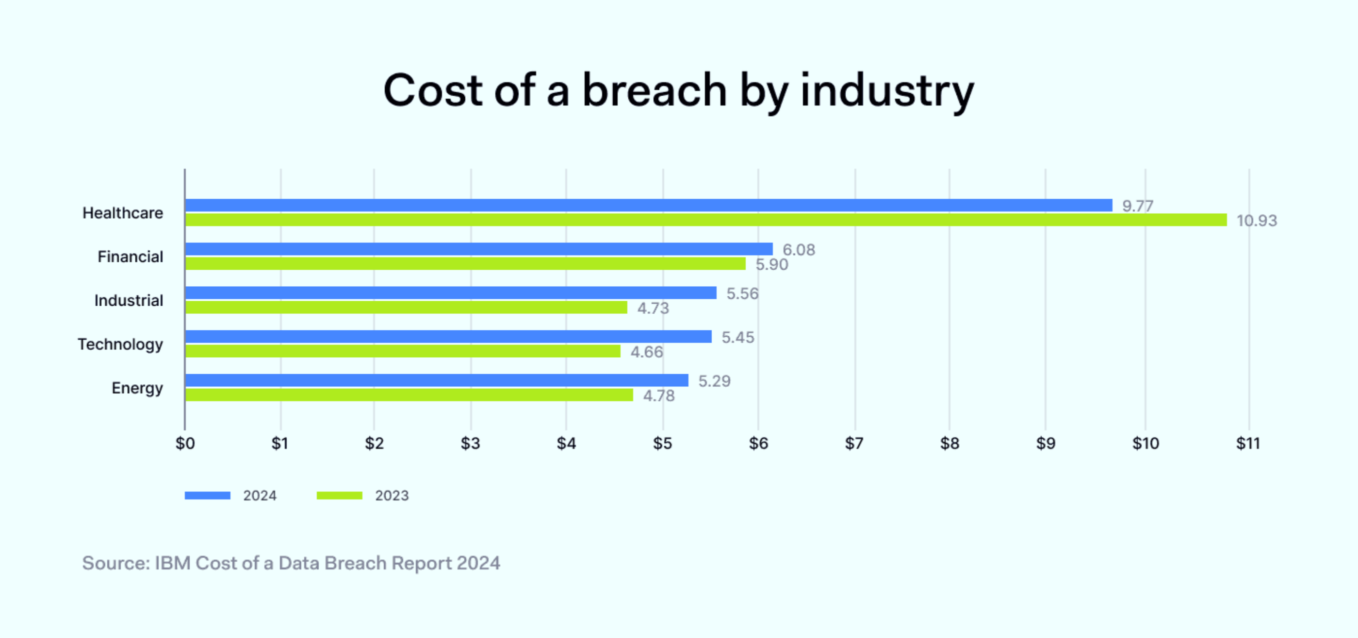
- **Impact on services.** A cyber-attack on **Change Healthcare** in February 2024 disrupted millions of prescriptions. This led to delays in medication and care. Cyber-attacks caused surgeries to be canceled and treatments delayed. Many medical practices faced closure due to lost revenue, risking patient care (The Lancet)
- Ransomware attacks:
  - Hospitals faced ransomware attacks that crippled systems. For example, Ascension Hospitals experienced delays in patient care (The New York Times).
  - **59%** of healthcare IT professional respondents said they had experienced at least one **ransomware attack** in the past 2 years, with an average of 4 ransomware attacks in the past 2 years. (Ponemon Institute Report)
  - The average ransom payment in 2024 was more than **$1 million** (Ponemon Institute Report)

92% of IT security professionals in U.S. healthcare faced a cyber-attack last year. This is up from 88% in 2023.

The HIPAA Journal



- More attacks:
  - **92%** of IT security professionals at U.S. healthcare organizations reported at least one cyber-attack last year, up from 88% in 2023 (The HIPAA Journal)
  - From January to September 2024, the *global* average number of attacks per healthcare organization was 2,018 per week. This marked a **32% increase** from 2023. (IndustrialCyber)
  - North America's healthcare sector saw a **20% year-on-year rise in weekly attacks**. It remains a top target because of valuable patient data and strong digital infrastructure (IndustrialCyber)
- Data breaches:
  - Breaches exposed sensitive data used for **espionage**. In August 2024, Iranian cyber actors accessed U.S. healthcare networks for espionage and helped Russian-affiliated attackers profit from ransomware (American Hospital Association)
  - The cost of a data breach in healthcare is the highest across industries (IBM Cost of a Data Breach Report 2024)



Cost of a breach by industry

Source: IBM Cost of a Data Breach Report 2024

Telecommunications industry

The telecommunications industry was a prime target in 2024. Known as **Salt Typhoon**, the Chinese hacking campaign targeted telecom networks for espionage.

In **February** 2024, CISA issued a warning. It stated that China-backed cybercriminals were setting up for potential cyber-attacks against U.S. critical infrastructure during a crisis or conflict.

Later in 2024, Chinese attackers infiltrated networks of major companies like **Verizon**, **AT&T**, and **T-Mobile**. These attacks targeted national security data.

In the case of T-Mobile, bad actors linked to Chinese intelligence accessed U.S. and international telecom networks. They aimed to spy on the phone communications of high-value intelligence targets'.

The attackers **retrieved audio files of calls and text content** from some victims. Many victims work in government or politics.

Despite months of investigation, as of December 2024, **the full scale of the attack is still unknown**. Authorities are unsure of how many victims were affected or if criminals still have access. In December 2024, U.S. federal authorities urged telecom companies to improve security.

Main cyber incidents of 2024

We already talked about some big data breaches, but let’s list some more.

1. Change Healthcare ransomware attack

In March 2024, a ransomware attack hit Change Healthcare, a UnitedHealth Group subsidiary. Change Healthcare supports over 100 essential healthcare functions, including claims processing and prescription management.

> **The Change Healthcare attack compromised the health information of at least 100 million people. This is nearly one-third of the U.S. population.**
>
> The HIPAA Journal

The attack disrupted critical healthcare services nationwide, making it the most impactful cyber-attack in U.S. healthcare history.

- **Patient care disruptions.** The shutdown delayed patient care and prescription access, affecting millions nationwide
- **Financial chaos.** The attack halted billions of dollars in payments to providers, crippling hospital finances
- **Protected health information compromised.** At least 100 million people had their health data exposed, nearly one-third of Americans
- **National security concerns.** The attack raised alarms about the security of healthcare financial systems
- **Emergency provider support.** UnitedHealth Group issued $8.5 billion in loans to assist providers. As of October 2024, $3.2 billion was repaid

UnitedHealth Group set up a program to support providers hit by the ransomware attack. They paid about $8.5 billion in loans. As of October 2024, $3.2 billion has been repaid.

The HIPAA Journal

2. Ascension Hospitals ransomware attack

Ascension, one of the largest U.S. health systems, operates about 140 hospitals in 19 states. In May 2024, Ascension Hospitals suffered a major cyberattack. For over two weeks, staff had to use manual methods because their computer systems were down.

This attack was similar to the one on Change Healthcare, which disrupted the nation's largest healthcare payment system. Ascension, like Change, was hit by ransomware.

The attack seems to have been carried out by a group called Black Basta, possibly linked to Russian-speaking cybercriminals.

The data breach happened after an employee accidentally downloaded a malicious file. Ascension called it an "honest mistake" as the file seemed legitimate.

- **Impact on patient care.** Doctors and nurses had to rely on paper and fax instead of digital records
- **Cause of the attack.** An employee downloaded a harmful file, leading to the ransomware attack
- **Emerging threats.** Human error continues to be a significant cyber risk in healthcare

3. Cyber-attacks on London hospitals cause major disruptions

In June 2024, a ransomware cyber-attack hit Synnovis, an organization that handles blood transfusions in London. According to Ciaran Martin, a former head of British cybersecurity, a Russian cybercriminal group, Qilin, was likely behind the attack.

Over 800 operations and 700 outpatient appointments were rescheduled after the Synnovis attack. This included 97 cancer treatments.

NHS

The attack led to the rescheduling of over 800 operations and 700 outpatient appointments, including 97 cancer treatments. Hospitals had to delay blood transfusions and reroute patients.

- **Pathology disruption.** Pathology services ran at just 10% capacity after the attack
- **Manual processes.** Medical staff had to use pen and paper for test results
- **Delayed emergency care.** Reduced capacity for blood tests affected emergency surgery operations

"It's not surprising that it happened, it's not surprising it was being reported as a Russian group, and it's not surprising it's healthcare related," said Joe Devanny, a lecturer at King's College London who focuses on the cybersecurity industry.

4. China's Salt Typhoon hacks target telecommunications

In 2024, China-linked hacking group Salt Typhoon attacked major U.S. telecom companies. The group targeted **Verizon, AT&T, T-Mobile,** and others. Authorities are investigating the data breaches, which may have impacted national security.

- **Targeted companies.** Verizon, AT&T, T-Mobile, and Lumen Technologies were affected
- **Espionage focus.** Threat actors aimed to steal sensitive national security data
- **Advanced techniques.** AI and machine learning were used to enhance the attacks
- **Compromised systems.** Cybercriminals accessed telecom infrastructure via Cisco router vulnerabilities

- **Government impact.** The data breach affected senior U.S. officials and political figures

5. Election-related cyber threats

In 2024, cyber attacks targeted U.S. elections. Foreign actors, including Iran, attempted to breach campaigns. Georgia's absentee ballot website was attacked but defended successfully.

- **Targeted systems.** Georgia's absentee ballot website faced a cyber-attack
- **Attack method.** Cyber-attackers tried to overwhelm the website with a surge in traffic
- **Cybersecurity response.** State officials quickly blocked the attack, preventing disruptions
- **National security risk.** The attacks raised concerns about election integrity and safety
- **Previous incidents.** Georgia has faced similar threats before, including in 2022 and earlier in 2024.

6. CrowdStrike update failure caused global IT meltdown

In July 2024, a flawed CrowdStrike update triggered a worldwide IT meltdown. This issue affected airports, banks, stock exchanges, and other businesses. The error stemmed from a small file in an update.

- **Industry context.** CrowdStrike is the second-largest endpoint protection software provider, controlling 18% of the $12.6 billion cybersecurity market
- **Cause of the issue.** A file called "C-00000291*.sys" in the Falcon sensor update caused Windows errors, leading to a "blue screen of death"
- **Global impact.** Millions of computers became inoperable, disrupting critical industries worldwide, including transportation and financial institutions
- **The scale of damage.** CrowdStrike, serving 29,000 organizations, impacted systems globally, requiring weeks of manual repairs

- **Multibillion losses.** The outage caused $5.4 billion in direct losses. Healthcare, again, took the biggest hit and lost $1.9 billion, followed by banking with $1.4 billion. On average, companies in each sector lost $43.6 million.

7. Ticketmaster breach exposes the personal data of millions

In May 2024, Ticketmaster experienced a breach, compromising the data of 560 million customers. Emails were sent to customers in North America, warning them about potential identity theft and fraud. The company has not explained the delay in notifying victims.

- **Scope of the data breach.** Cybercriminals stole personal details of 560 million customers worldwide, including names and contact info
- **Security concerns.** Encrypted credit card details were stolen, but no details on encryption security were provided
- **Notification process.** Ticketmaster sent emails to customers in Canada, the US, and Mexico, urging vigilance
- **Response to the data breach.** The attackers attempted to sell the stolen data online before Ticketmaster issued a shareholder notice

Essential cybersecurity actions for 2025

As we saw, in 2024, cyber threats and cyber-attacks surged. To improve data security and protect sensitive information, organizations must improve their cybersecurity posture in 2025. Here are essential actions to take:

Action 1. Use multi-factor authentication (MFA)

More than 99.9% of compromised accounts don't have MFA. MFA is essential because it cuts the risk of compromise by 99.22% overall and by 98.56% with leaked credentials.

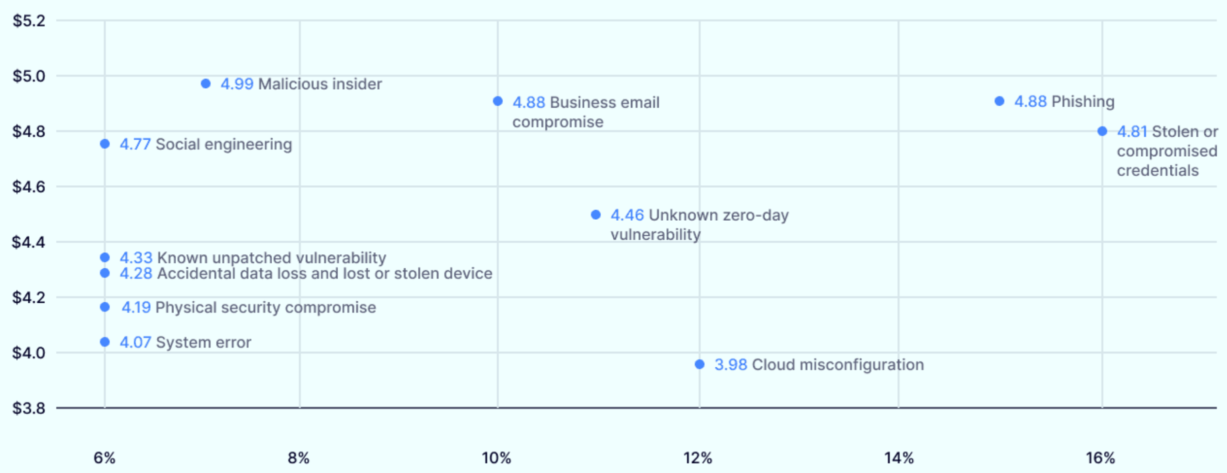
- **Reduce data breach risk.** Add another layer of security with MFA

- **Enable MFA for all users.** Make sure all accounts use MFA. NordLayer dashboards show how many employees have enabled it.

Action 2. Train all staff to detect phishing attacks

Phishing attacks remain one of the major cybersecurity risks. Employees must know how to recognize and report them.

Cost and frequency of data breaches by attack vector



Source: IBM Cost of a Data Breach Report 2024

- Regular training. Teach staff to spot phishing emails and websites
- **Test employees.** Run simulated phishing attacks to find weaknesses
- **Use anti-phishing tools.** Block malicious websites and email addresses

Action 3. Assign minimal user privileges in line with Zero Trust principles

Zero Trust limits access to sensitive data, reducing the attack surface.

- **Limit user access.** Grant only necessary permissions for each role
- **Monitor user activities.** Watch for unusual behavior or access patterns

- **Segment your network.** Implement network segmentation to protect sensitive data

Action 4. Use a password manager for strong passwords

Password managers store complex, unique passwords securely, simplifying management.

- **Generate strong passwords.** Use long, random passwords for each account
- **Store securely.** Use a password manager to store login details safely
- **Share securely.** Share passwords safely with trusted team members

Action 5. Secure remote devices with VPNs

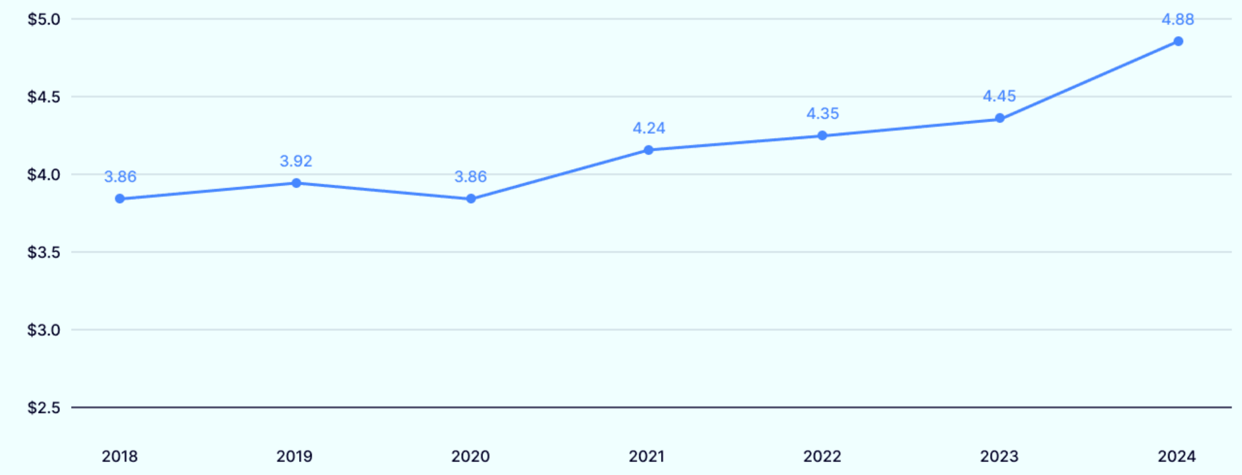
Remote devices are vulnerable to cybersecurity threats. Use a VPN to encrypt data and secure connections.

- **Use a Remote Access VPN.** Protect devices accessing your network remotely
- **Limit VPN access.** Allow only authorized devices to connect via VPN

Action 6. Use data loss prevention (DLP) tools

DLP tools protect sensitive data and prevent leaks or theft.

- **Monitor sensitive data.** Track where sensitive information is stored and used
- **Block unauthorized sharing.** Prevent sensitive data from being shared with untrusted sources
- **Detect insider threats.** Use DLP tools to flag unusual activities



Global average total cost of a data breach

Source: IBM Cost of a Data Breach Report 2024

Action 7. Encrypt your sensitive data

Encryption ensures data is unreadable to unauthorized users, protecting it from theft.

- **Encrypt data at rest.** Use encryption to protect stored data
- **Encrypt data in transit.** Secure data as it moves across networks
- **Encrypt all sensitive data.** Apply encryption to critical business data

Action 8. Use Threat Prevention solutions

NordLayer and NordStellar work together to protect against cybersecurity threats.

- **Protect the network perimeter.** NordLayer secures your network from unauthorized access and data interception
- **Detect threats early.** NordStellar monitors for data leaks and infrastructure vulnerabilities in real time
- **Respond quickly.** In case of a breach, act swiftly to limit the damage and contain threats

Action 9. Back up data regularly

Backups ensure you can recover from cyber incidents, such as ransomware attacks.

- **Automate backups.** Set up automatic backups for critical data
- **Store backups securely.** Use encrypted storage for sensitive data backups
- **Test recovery.** Regularly test backups to ensure they work during an incident

Action 10. Risk assess core threats and create response plans

Risk assessments help identify cyber threats and improve risk management strategies.

- **Assess vulnerabilities.** Identify and address gaps in security
- **Develop response plans.** Create clear action steps for cyber incidents
- **Update regularly.** Review and adjust risk assessments as threats evolve

Wrapping up 2024's key cyber insights

2024 was a rough year for cybersecurity. We saw more attacks, more data breaches, and bigger losses. The trends from 2024 show that the cyber threat landscape is getting worse. As we move into 2025, these threats will only grow. Here are some of the key cybersecurity trends that will matter in the coming year.

The rise of ransomware attacks

Ransomware attacks increased sharply in 2024. Cybercriminals used more sophisticated tactics to target businesses. They are now focusing on weaker links in the supply chain, like vendors and third-party contractors. This makes it harder for companies to protect themselves. In 2025, this trend will continue, and businesses will need stronger cybersecurity, especially when it comes to third-party access.

State-sponsored cyber warfare

In 2024, we saw state-sponsored cyber-attacks on a scale we've never seen before. Cyber-attacks from state actors have surged, with government-backed hackers targeting critical infrastructure and sensitive data.

The US and other countries are also facing rising threats from China. These attacks are not just about espionage anymore. Hackers are now using more disruptive tactics, like "living off the land" methods, where they silently infiltrate systems and wait for the right moment to strike. This will be a major issue in 2025 as nation-state actors continue to target critical sectors.

Quantum computing threats

Quantum computing has been a hot topic for years, but 2024 marked a turning point. Governments and businesses are starting to realize that current encryption methods may not hold up against the power of quantum computers.

With the rise of quantum technology, it’s only a matter of time before today’s encryption methods are cracked. In 2024, companies began preparing by integrating new cryptographic algorithms designed to protect against quantum hacks. This will become crucial in 2025 as more businesses transition to quantum-resistant encryption methods.

More complex attack vectors

2024 also saw cybercriminals become **more creative** with their attack methods. Phishing, social engineering, and malware attacks have all gotten more advanced. Attackers are using a mix of tactics, including AI, to exploit vulnerabilities. They’re targeting employees and systems that are not properly protected.

As a result, it’s harder for companies to spot these threats before they cause damage. In 2025, businesses will need to adopt smarter defenses that use machine learning and AI to detect these complex attacks before it’s too late.

About NordLayer

NordLayer helps businesses stay protected with a comprehensive suite of security features. The Business VPN ensures secure, encrypted connections for remote teams. It supports multiple VPN protocols, including NordLynx, OpenVPN TCP, and OpenVPN UDP.

AES-256 and ChaCha20 encryption keep all traffic secure. This protects data in transit, no matter where employees are working.

Zero Trust Network Access (ZTNA) solutions ensure that only authorized users and devices can access network resources. **MFA** adds extra protection during login. Device Posture Security checks devices for compliance before granting network access. Cloud Firewall helps organizations implement their network segmentation strategy and control what resources users can access.

NordLayer integrates with identity providers like **Okta**, **OneLogin**, and **Google** for easy SSO and user provisioning. These integrations make user management simple and secure.

Pricing starts at $7 per user per month, making NordLayer affordable. It provides businesses with security, flexibility, and control over their network.

Anastasiya Novikava

Copywriter

Anastasiya believes cybersecurity should be easy to understand. She is particularly interested in studying nation-state cyber-attacks. Outside of work, she enjoys history, 1930s screwball comedies, and Eurodance music.

Share this post

f 𝕏 in 🔗

Related Articles

← →