



2025

The Big Book of Breaches

The year's most devastating attacks, how they happened, and what you can do about them



INTRODUCTION

Every day, a deluge of cybercrime threatens organizations around the world.

They span every industry. And they pervade every corner of the globe.

And as most security leaders know all too well, it's getting harder and harder to keep them all out. Attackers have grown too adept at exploiting mistakes, human frailties, and technical flaws. And worse, they're evolving by the day.

This e-book reviews the most notable breaches of the last year. But the events outlined here are not isolated cases. They reflect a global shift. Attacks are now a daily reality, a financial drain, and a political weapon. Cybercrime gangs and state-sponsored actors are skilled, focused, and well-funded. They exploit critical systems. They steal valuable corporate data. And they compromise government assets.

This collection of high-profile attacks provides a snapshot of the wide-ranging effects of cyber breaches. From ransomware attacks on healthcare providers to digital spying campaigns, they underscore the urgent need for fast, effective breach containment. And each serves as a vivid reminder: cyber resilience is no longer a nice-to-have — it's essential.

Change Healthcare ransomware attack

INDUSTRY

Healthcare

LOCATION

U.S.

DAMAGES

Early estimates exceed \$100 million

BREACH NO. 1

Critical condition

In healthcare, security isn’t about protecting just data. It’s about saving lives. The stakes couldn’t be higher — and neither could the cost of failure.

In February 2024, Change Healthcare, a critical player in U.S. healthcare technology, faced a massive ransomware attack by the ALPHV/BlackCat ransomware group. Hitting everything from prescription processing to insurance claims, the attack set off a cascade of chaos across the U.S. healthcare system.

Attackers had breached Change Healthcare’s network through unpatched flaws in key systems. They deployed ransomware that quickly spread across connected services. It targeted vital systems that support patient data and billing processes. Many healthcare processes across the U.S. ground to a halt.

The hackers encrypted vital data and threatened to leak sensitive patient data unless Change Healthcare paid a large ransom. The attackers knew the stakes: healthcare is a life-and-death matter, and providers rely on quick access to these systems to care for patients.

VERIFIED MITRE TTPS

Initial access:

- Unknown

Exfiltration:

- [T1059] Command and Scripting Interpreter
- [T1204] User Execution

Persistence:

- [T1486] Data Encrypted for Impact
- [T1490] Inhibit System Recovery

KEY IMPACTS

60K⁺ pharmacies hit



Millions of insurance claims delayed



Healthcare providers forced to switch to paper prescriptions



Many smaller medical practices faced severe cash flow issues



UnitedHealth Group released emergency funding to prevent healthcare disruptions



Recovery was slow going for many healthcare providers

OUTCOME

Change Healthcare worked with security experts to isolate affected systems.

From there, it tried to recover the encrypted data and harden its defenses. The attack prompted calls for stronger cyber defenses across healthcare networks.

KEY MICROSEGMENTATION STRATEGIES THAT COULD HAVE HELPED:

- Strictly segment pharmacy, payment, and claims processing systems
- Segment critical healthcare applications
- Create separate security zones for different types of healthcare data with granular access controls
- Set up real-time monitoring of inter-segment traffic to detect ransomware spread
- Define healthcare-specific protocol rules within segments to prevent unsanctioned data access
- Deploy segmentation to prevent attackers from spreading through the environment after initial compromise (lateral movement)

FURTHER READING

[“How the ransomware attack at Change Healthcare went down: A timeline”](#) (TechCrunch)

[“Change Healthcare cyberattack fallout continues”](#) (TechTarget)

[“Change Healthcare cyberattack was due to a lack of multifactor authentication, UnitedHealth CEO says”](#) (Associated Press)

CDK Global
ransomware attack

INDUSTRY
Automotive Technology

LOCATION
North America

DAMAGES
Estimated in hundreds of millions (exact figure undisclosed)

BREACH NO. 2

Ransomware
sticker shock

When hackers struck CDK Global in December 2023, they didn’t just breach another company. They threw sand into the gears of America’s car-selling machine. The firm provides crucial software services to about 15,000 car dealerships. It faced a system-wide outage that stalled auto sales across many parts of the country.

Attackers breached CDK Global’s network using phishing emails, gaining access to customer data systems. Once inside, they deployed ransomware that encrypted dealership and customer data. Parts of CDK’s operations failed, hitting dealers across the country. The attackers demanded a reported \$25 million to restore access.

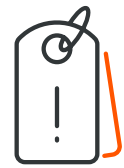
VERIFIED MITRE TTPS

Unknown or not publicly disclosed

KEY IMPACTS



Thousands of dealerships lost access to inventory management systems



Vehicle sales processing severely hit



Parts ordering systems crippled



Customer information systems not accessible



Dealerships forced to use manual processes for weeks



Massive revenue loss during the crucial end-of-year sales period

OUTCOME

CDK Global largely shut down in late June, bringing systems back online in phases through early July. It worked with law enforcement and security experts to strengthen its defenses.

KEY MICROSEGMENTATION STRATEGIES THAT COULD HAVE HELPED:

- Segment each dealership to prevent cross-dealership infection
- Segment dealer management software to protect vital business functions
- Deploy identity-based access controls to restrict system access based on role and location
- Set up separate security zones for inventory, sales, and customer data systems
- Enable dynamic security policies to instantly isolate breached systems
- Monitor inter-segment traffic for abnormal behavior

FURTHER READING

[“The CDK Global outage: Explaining how it happened”](#) (TechTarget)

[“How did the auto dealer outage end? CDK almost certainly paid a \\$25 million ransom”](#) (CNN)

[“Car dealerships in North America revert to pens and paper after cyberattacks on software provider”](#) (Associated Press)

Microsoft executive email breach

INDUSTRY
Technology

LOCATION
Global

DAMAGES
Undisclosed financial impact, significant reputational damage

BREACH NO. 3

Administrator access not required

Cybersecurity can be a challenge for even the largest tech companies. In January 2024, Microsoft disclosed that Russian state-sponsored hackers accessed senior leaders’ email accounts.

The attackers employed a technique called password spraying. Hackers methodically tried a list of frequently used passwords across multiple accounts. They successfully compromised an account on an old test system. From this breach, the hackers discovered and gained control of an outdated testing tool that had special access permissions within Microsoft’s corporate systems. It was like finding an old employee badge that still worked to open doors throughout the building.

The attack was ascribed to Midnight Blizzard (also known as Nobelium). It’s a case study in the constant threat of state-sponsored cyber spying — and why stopping lateral movement is critical. Modern attacks often succeed through a chain of seemingly minor actions rather than a single dramatic breach.

When even a tech leader like Microsoft can be breached, it’s time for everyone to take note.

VERIFIED MITRE TTPS

Initial access:

- [T1110.003] Password Spraying

Exfiltration:

- [T1030] Data Transfer Size Limits

Persistence:

- [T1078] Valid Accounts


Discovery:

- [T1087] Account Discovery
- [T1083] File and Directory Discovery

Collection:

- [T1114] Email Collection
- [T1213] Data from Information Repositories


KEY IMPACTS


- 

Compromised emails of senior leadership team
- 

Exposed internal emails about security practices
- 

Showed attackers Microsoft’s response to past security incidents
- 

Forced Microsoft to speed up security overhaul efforts
- 

Led to broader industry debates about legacy system risks
- 

Triggered regulatory probes

OUTCOME

Microsoft fully disclosed the attack and pledged to apply modern security standards to its legacy systems and internal business processes — even if that meant some short-term headaches. It was one of several incidents that spurred CEO Satya Nadella to ask his board of directors to cut his annual bonus.

KEY MICROSEGMENTATION STRATEGIES THAT COULD HAVE HELPED:

- Strictly segment your test and production systems to prevent credential abuse
- Set up executive-specific security segments with enhanced monitoring and access controls
- Create application-layer controls for email systems and sensitive email
- Deploy identity-based segmentation for sensitive data access
- Enable real-time policy enforcement to block unauthorized access
- Monitor segment-to-segment traffic for unusual patterns

FURTHER READING

- [“Microsoft explains how Russian hackers spied on its executives”](#) (TheVerge)
- [“Microsoft Executives’ Emails Hacked by Group Tied to Russian Intelligence”](#) (The New York Times)
- [“A Microsoft under attack from government and tech rivals after ‘preventable’ hack ties executive pay to cyberthreats”](#) (CNBC)

Espionage on U.S. telecommunications

INDUSTRY
Telecommunications

LOCATION
Global

DAMAGES
Classified (estimated in billions given national security implications)

BREACH NO. 4

Direct dial to Beijing

Sometimes the biggest threats aren't the ones making noise. They're the ones quietly listening in.

An advanced spying campaign ascribed to China's Salt Typhoon group breached critical U.S. telecom systems throughout 2024. The state-sponsored group set its sights on core network systems with strikingly advanced techniques.

As part of a long-term campaign, the attackers exploited unpatched software flaws. From there, they could listen in on calls and texts between public agencies and private contractors. The assumed goal: extract intel that could be used to hijack telecom systems during a crisis.

VERIFIED MITRE TTPS

- Initial access:
- [T1190] Exploited Public-Facing Applications
- Persistence:
- [T1136] Create Account
 - [T1078] Valid Accounts
- Defense evasion:
- [T1036] Masquerading
 - [T1070] Indicator Removal
- Command and control:
- [T1090] Proxy
 - [T1571] Non-Standard Port

KEY IMPACTS



Breached multiple tier-1 telecom providers



Potential access to sensitive communications data



Exposed critical system weaknesses



Triggered national security concerns



Led to emergency directive from CISA



Sparked major infrastructure review across the sector

OUTCOME

U.S. federal agencies worked with telecom providers to close security gaps, protect critical systems, and bolster surveillance measures.

KEY MICROSEGMENTATION STRATEGIES THAT COULD HAVE HELPED:

- Segment and isolate critical telecom systems
- Create separate security zones for different types of telecom system components
- Segment network management systems
- Set up strict control policies for inter-segment traffic
- Enable real-time monitoring of segmented environments to reveal APT activity
- Enforce Zero Trust principles within each segment to prevent unneeded lateral movement

FURTHER READING

[“What to know about string of US hacks blamed on China”](#) (BBC)

[“A 9th telecoms firm has been hit by a massive Chinese espionage campaign, the White House says”](#) (Associated Press)

[“White House urges crackdown on US telecoms after massive Chinese hack”](#) (USA Today)

North Korean cyberespionage campaign

INDUSTRY
Multiple (defense, research, government)

LOCATION
Global

DAMAGES
Classified, estimated over \$500 million in stolen intellectual property (IP)

BREACH NO. 5

An asymmetric advantage

Call it “alternative R&D.” A nation that can’t provide a constant flow of electricity to its citizens pulled off some of the most complex cyber operations ever over the summer.

A campaign blamed on North Korean threat actor Lazarus Group targeted defense contractors and research centers in several countries. The state-sponsored group used advanced social engineering and custom malware — to devastating effect.

The attackers breached networks of defense contractors, government agencies, and large multinationals. Once inside, the attackers gathered intel on other nations’ advanced knowhow. Stolen data included defense technology and strategic defense plans. The likely goal: advance the regime’s military and nuclear programs.

With over \$500 million in stolen IP (that we know about), the campaign wasn’t just a fruitful heist. It was a strike at the heart of Western tech dominance.

VERIFIED MITRE TTPS

- Initial access:
- [T1566.001] Spear Phishing Attachments
- Defense evasion:
- [T1027] Obfuscated Files or Information

KEY IMPACTS

- 

Theft of sensitive defense research data
- 

Compromise of intellectual property
- 

Exposure of classified defense projects
- 

Affected entities in U.S., South Korea, and Japan
- 

Triggered diplomatic tensions

OUTCOME

In response, governments around the world heightened their security protocols and conducted internal investigations. Some also imposed new sanctions on North Korean entities involved.

KEY MICROSEGMENTATION STRATEGIES THAT COULD HAVE HELPED:

- Segment and isolating sensitive research data
- Create separate security zones for different research disciplines and projects
- Impose strict controls on data transfer between segments to prevent data theft
- Segment specific research tools and systems
- Use identity-based segmentation to prevent credential abuse
- Watch inter-segment data transfers for unusual patterns

FURTHER READING

- [“NSA Joins FBI and Others to Warn of North Korea Cyber Espionage Campaign”](#) (NSA)
- [“North Korean hackers stealing military secrets, say US and allies”](#) (Reuters)
- [“North Korean Hackers Target Critical Infrastructure for Military Gain”](#) (Infosecurity Magazine)

Transport for London (TfL) cyberattack

INDUSTRY
Public transportation

LOCATION
UK

DAMAGES
£10+ million direct costs, broader economic impact assessed at £50+ million

BREACH NO. 6

Mind the security gap

Transport for London’s early 2024 ransomware attack brought to light the risk to critical urban infrastructure. The incident hit multiple systems and hampered London’s public transit system.

The attack targeted TfL’s OT systems with ransomware. Under a cascade of system failures, the agency struggled to manage transit schedules, payments, maintenance alerts, and real-time service data. As a result, passengers faced delays; some were stranded.

TfL’s normal service updates turned into a complex web of manual workarounds and best-guess estimates. Controllers were forced to manage one of the world’s busiest transit systems with about as much real-time information as a Victorian-era station master.

Police arrested a 17-year-old from English midlands a few days later in connection to the attack. Still, it remains a stark reminder that modern transport networks are only as robust as the digital systems that power them.

VERIFIED MITRE TTPS

Unknown or not publicly disclosed

KEY IMPACTS



Disrupted payment systems across London transport



Prevented sales of student and elderly travel passes



Affected real-time travel information displays



Breached internal communication systems



Forced manual operations for critical services



Millions of commuters affected



Required extensive system rebuilding

OUTCOME

TfL swiftly engaged security teams to regain control over its systems. It has since invested in new security measures.

KEY MICROSEGMENTATION STRATEGIES THAT COULD HAVE HELPED:

- Create separate microsegments for payment and operational systems
- Set up contractor-specific security zones with limited access rights
- Deploy application-level segmentation for transportation management systems
- Enforce identity-based access controls between segments
- Enable real-time monitoring of inter-segment traffic patterns
- Enforce Zero Trust principles for contractor access system

FURTHER READING

- “[TfL cyber attack: What you need to know](#)” (BBC)
- “[Fallout from TfL cyber-attack is slow burning and potentially costly](#)” (The Guardian)
- “[Cyber Attack Leaves a Sickly Canary in London’s Underground](#)” (Bloomberg)

Ivanti VPN attacks

INDUSTRY

Multiple

LOCATION

Global

DAMAGES

Estimated hundreds of millions in remediation costs

BREACH NO. 7

When good security tools go bad

What happens when security tools themselves become vectors for attack?

Ivanti customers found out the hard way during a campaign targeting the tech firm’s VPN products. The advanced supply chain attack turned products meant for protecting networks into virtual back doors into them.

Attackers exploited known flaws in the company’s Connect Secure and Policy Secure gateways. It let attackers in, where they could steal data, spy on network traffic, and disrupt business around the globe. Worse, the exploit also blocked the devices from detecting breaches in victims’ systems.

Notable victims included the U.S. Cybersecurity and Infrastructure Security Agency (CISA); that’s the agency charged with helping protect critical U.S. systems.

VERIFIED MITRE TTPS

Initial access:

- [T1190] Exploit Public-Facing Application

Execution:

- [T1203] Exploitation for Client Execution
- [T1059.001] PowerShell

Persistence:

- [T1505.003] Web Shell Installation
- [T1136] Create Account

Defense evasion:

- [T1027] Obfuscated Files or Information
- [T1070.004] File Deletion

Command and control:

- [T1071.001] Web Protocols
- [T1090] Proxy

KEY IMPACTS

1,700+ VPN devices breached globally



Affected critical infrastructure organizations



Required emergency patches and system rebuilds



Exposed sensitive corporate networks



Triggered widespread security audits



Led to regulatory investigations

OUTCOME

Ivanti quickly released patches. Customers updated their systems and reviewed security protocols for VPNs.

KEY MICROSEGMENTATION STRATEGIES THAT COULD HAVE HELPED:

- Deploy VPN-specific security segments with enhanced monitoring
- Set up application-level segmentation for remote access systems
- Create identity-based access controls within segments
- Enable real-time policy enforcement for VPN traffic
- Monitor segment-to-segment traffic for abnormal patterns

FURTHER READING

[“CISA Takedown of Ivanti Systems Is a Wake-up Call”](#) (Dark Reading)

[“Governments Urge Organizations to Hunt for Ivanti VPN Attacks”](#) (SecurityWeek)

[“US Agencies Must Disconnect Ivanti VPN Devices Amid ‘Substantial Threat’: CISA”](#) (CRN)

AT&T compromise

INDUSTRY
Telecommunications

LOCATION
U.S.

DAMAGES
Initial estimates exceed \$100 million

BREACH NO. 8

Breach out and touch someone

In an awkward twist on the company’s old ad jingle, a massive AT&T data breach exposed sensitive data of 73 million current and former customers in April. It marked one of the largest telecom breaches in history.

Hackers breached AT&T’s network, accessing a database with customer names, Social Security numbers, and account information. This breach is believed to have involved an insider who let the hackers bypass security controls and download a huge volume of data.

The attack highlighted the downside of traditional parameter security measures: they can fail when the threat comes from within.


VERIFIED MITRE TTPS


Unknown or not publicly disclosed

KEY IMPACTS

73 million customers affected

 Exposed names, addresses, and Social Security numbers

 Required extensive identity protection services

 Triggered multiple class-action lawsuits

 Led to regulatory investigations

 Damaged customer trust significantly

OUTCOME

AT&T strengthened internal security controls, deployed new authentication requirements, and advised customers to monitor for any signs of fraud.

KEY MICROSEGMENTATION STRATEGIES THAT COULD HAVE HELPED:

- Use data-specific segmentation for customer information
- Create separate security zones for different types of customer data
- Deploy application-level controls for database access
- Set up strict data transfer controls between segments
- Enable real-time monitoring of data access patterns
- Adopt Zero Trust principles for database access

FURTHER READING

[“Massive AT&T hack compromises phone, text records of “nearly all” customers”](#) (Axios)

[“AT&T data breach update: Call and text records compromised in massive hack impacting nearly all wireless customers”](#) (FastCompany)

[“After massive AT&T data breach, can users do anything?”](#) (USA Today)

Ticketmaster breach

INDUSTRY
Entertainment and Ticketing

LOCATION
Global

DAMAGES
Exact cost not yet disclosed; class-action lawsuit seeks \$5 million in damages

BREACH NO. 9

Reputation
(ShinyHunters’
Version)

As Ticketmaster learned in May 2024, sometimes the hottest tickets in town are database credentials. In an attack that would make scalpers blush, hackers accessed 560 million customer records for sale on the dark web.

The attackers used stolen credentials to get access to a third-party cloud database, believed to be managed by Snowflake. The breach compromised personal information of about 560 million customers. Exposed data includes names, addresses, email addresses, phone numbers, and partial payment card data. The hacker group ShinyHunters claimed responsibility. It offered 1.3 terabytes of stolen data for \$500,000.

The breach exposed millions of customers to identity theft and financial fraud. ShinyHunters claimed to have obtained and leaked barcodes for more than 170,000 tickets to Taylor Swift’s Eras Tour. But Ticketmaster’s rotating bar-code systems meant the codes couldn’t be used.

VERIFIED MITRE TTPS

Unknown or not publicly disclosed

KEY IMPACTS

560 million customers’ sensitive data exposed



Financial losses



Reputational damage



Additional regulatory scrutiny

OUTCOME

Parent company Live Nation filed a report with the SEC and let stakeholders know about the incident. It is working with experts to investigate the breach and enhance its defenses. Ticketmaster also told affected customers that it is working with authorities to ensure compliance with data protection rules.

KEY MICROSEGMENTATION STRATEGIES THAT COULD HAVE HELPED:

- Enforce strict segmentation to separate customer-facing applications (such as the Ticketmaster platform) from internal databases holding sensitive customer data.
- Use identity-based segmentation policies to control access for individual users and devices, applying the principle of least privilege.
- Use segmentation to control east-west traffic within the cloud environment, where attackers often move laterally. This is especially relevant in cloud storage settings and third-party-managed environments such as Snowflake.
- Apply segmentation to separate third-party systems (such as cloud databases or integrated vendor solutions) from core Ticketmaster and Live Nation systems.
- Deploy a policy-driven, adaptive segmentation model that monitors and adjusts access based on real-time risk signals.

FURTHER READING

“[Ticketmaster Confirms Data Breach. Here’s What to Know.](#)” (The New York Times)

“[Hackers Detail How They Allegedly Stole Ticketmaster Data From Snowflake.](#)” (Wired)

“[Hacking group claims it breached Ticketmaster and stole data for 560 million customers](#)” (CBS News)

Iran Trump campaign breach

INDUSTRY
Political

LOCATION
U.S.

DAMAGES
Undisclosed, estimated in millions

BREACH NO. 10

Iran’s Electoral espionage

In the digital age, campaign trail security is more than just physical protection. It’s about safeguarding the entire digital infrastructure that powers modern politics.

Iranian state-sponsored actors breached Donald Trump’s 2024 campaign accounts, raising concerns about election security. The attack shows how state-sponsored actors are targeting political campaigns as a matter of course in broader influence plays.

The hackers used phishing and credential stuffing against email accounts and cloud services linked to the Trump campaign. The hackers stole private campaign information and tried to hand it off to journalists and campaign staffers for President Joe Biden. Few bit; many staffers dismissed the emails as a phishing attempt.

Still, the attack risked exposing campaign strategies. It also weakened security confidence, highlighting weaknesses in political campaigns.

VERIFIED MITRE TTPS

Initial access:

- [T1566] Phishing
- [T1078] Valid Accounts

Exfiltration:

- [T1041] Exfiltration Over C2 Channel

KEY IMPACTS

- 

Campaign strategy documents exposed
- 

Donor information potentially exposed
- 

Required campaign email rebuild
- 

Triggered FBI investigation
- 

Raised election security concerns
- 

Led to enhanced campaign security measures

OUTCOME

The campaign bolstered its security, engaging security firms for help. It also began enforcing strict email and data protection protocols.

KEY MICROSEGMENTATION STRATEGIES THAT COULD HAVE HELPED:

- Create campaign data segmentation with enhanced security controls
- Implement separate security zones for different campaign operations
- Deploy application-level controls for campaign systems
- Establish strict data access controls between segments
- Enable real-time monitoring of access patterns
- Apply Zero Trust principles for sensitive campaign data

FURTHER READING

- [“Trump campaign hack traced to three Iranians seeking to disrupt election, DOJ says”](#) (NPR)
- [“Iranian hackers sent stolen Trump campaign information to people associated with Biden campaign”](#) (CNN)
- [“FBI says Iranian hackers tried but failed to interest Biden campaign in stolen Trump info”](#) (PBS News)

Conclusion

For security leaders, the world may never have felt so fraught. Preventing breaches has long been a losing game. Each new incident is a clear reminder that no amount of technology, spending or talent can keep attackers out forever.

But there's hope. The breaches laid out in this e-book are real, but they are also manageable. A Zero Trust strategy grounded in microsegmentation can shift the playing field, stopping cyberattacks where they start. Security teams can regain the upper hand. Organizations can build true resilience.

While cyber threats will persist, leaders who embrace new approaches such as Zero Trust and microsegmentation are better poised than ever to contain, detect, and resolve attacks. Because the future of security isn't about building higher and higher walls to keep every attacker out. It's about creating smart, adaptive defenses that can protect critical assets when attackers get in.

Breaches are inevitable. Disasters are optional.

To learn more about how Illumio Segmentation can help you stop breaches where they start, visit illumio.com/illumio-segmentation.

About Illumio

Illumio is the leader in breach and ransomware containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments – stopping the spread of attacks before they become disasters.

Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.

Copyright © 2025 Illumio, Inc. All rights reserved. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.

