White Paper

halcyon

Cyberfort
Expert-led. Security Driven.

The Guide to Ransomware Resilience

Five Ransomware Attacks That Changed Everything, and Lessons Learned

Wake-Up Calls That Shaped Security

The most critical lessons learned are through the toughest trials. The cybersecurity industry is no stranger to this concept. Global headlines often confirm that the defenders' dilemma, which demands perfect accuracy, isn't a foolproof principle. Historically, when threat actors have succeeded with devastating breaches, the fallout has contributed to pivotal moments in history. The valuable lessons learned from these moments often pave the way for future technological innovation that changes how we look at security. What follows are five pivotal moments, and the lessons they taught us.

01 | Boeing's Unexpected Cyber Detour

What Happened:

Two days into November 2023, Boeing self-reported what would be one of the most impactful breaches to date. During the closing week of October 27th, Lockbit, also known as ALPHV/BlackCat, exploited a Citrix Bleed vulnerability (CVE-2023-4966), which was among the top 15 most exploited vulnerabilities as of November 2024, leveraging an array of tools to gain access. This resulted in a leak of 43GB worth of sensitive data and a $200 million ransom demand. Data from Citrix appliances and email backups, provisioning services, audits, security controls, aircraft production details, contracts, and IT management configurations were included in the breach.

Business Impact:

CyberScoop reported that the ransom demand was so outrageous that Boeing ultimately refused to pay it. This quickly led to the stolen data being published on Lockbit's Tor site, exposing several other vulnerabilities to secondary threat actors. While Boeing's team detected and restored disrupted services within weeks, the damage caused by the stolen data impacted Boeing's public image and reputation.

While Boeing's team detected and restored disrupted services within weeks, the damage caused by the stolen data impacted Boeing's public image and reputation.

Key Takeaways:

Catching the intrusion can mitigate further risk; however, an early warning system capable of detecting data exfiltration could have done more. Ransomware data exfiltration in 2025 has become the norm. Extortion attempts quickly dive into chaos: pay up or watch your data leaked publicly. Spoiler: neither option is great. Halcyon identifies discovery of exfiltration attempts in two ways: Nefarious Peer Detection and Volumetric Detection. Halcyon uses Nefarious Peer Detection to isolate and identify malicious methods commonly used in exfiltration attempts, such as unauthorized file-sharing services, FTP/SFTP, Rclone usage, or RDP abuse. Volumetric Detection allows customizable data movement thresholds that trigger alerts when they detect rogue exfiltration activity. Using these two techniques, Halcyon addresses the need to rapidly identify exfiltration attempts and prevent your business from taking a costly detour.

Checklist:

☐ Block Nefarious Peers

Quickly detect nefarious peers and generate alerts on restricted connection usage to prevent data exfiltration.

☐ Cap Data Volumes

Enforce thresholds in data migration volumes and transfer volumes.

☐ Secure Backups

Protect Volume Shadow Copy (VSS) and shield shadow copies from corruption.

Ransomware by the Numbers

$813M

estimated total payments to threat actors in 2024.

Chainalysis

180%

increase in the exploitation of vulnerabilities as an initial breach method, fueled by zero-day exploits used in ransomware attacks.

Verizon's Insights Report 2024

25%

of ransomware victims lost existing customers; the same proportion lost new business opportunities.

Ransomware Insights Report 2025

02 | Change Healthcare's Ransom Code Blue

What Happened:

Lockbit, targeting the medical industry, struck again, causing the most significant healthcare data breach to Change Healthcare in American history to date. On February 21st, 2024, Lockbit compromised a Citrix remote access portal lacking multi-factor authentication, which proved to be the perfect entry point. Armed with stolen credentials, Lockbit spent roughly nine days exfiltrating between 4 and 6 TB of data before encrypting all systems. The result? Approximately 70,000 pharmacies, 8,000 healthcare facilities, and 5,500 hospitals lost complete access to prescription claims, processing, and authorization. To make matters worse, 94% of providers had negative financial impacts, and 60% experienced daily revenue shortfalls exceeding $1 million, as reported by CNBC.

Business Impact:

Unfortunately, the impact was felt beyond the providers. It's estimated that 192.7 million individuals (or 1 in 3 Americans) were exposed to the attack. Included in those exposures was an array of PHI data consisting of names, addresses, Social Security numbers, clinical data, and payment details, all of which became accessible on the dark web. A total of $22 million was paid for the ransom, and this was promptly followed by a second data extortion payment demand, which was refused. Impacted systems would not be restored for nine months. Congressional hearings on pure negligence swiftly followed suit.

Armed with stolen credentials, Lockbit spent roughly nine days exfiltrating between 4–6 TBs of data before encrypting all systems.

Key Takeaways:

Dwell time, or the time it takes to discover an attacker is in the network, is a hard lesson to learn on the job. Security solutions like SIEM and EDR help lessen the discovery time, but may not always be enough. Today's attacks require deeper insight than traditional discovery tools provide. Behavioral analytics, which look at Living off the Land (LoTL) attacks, can mean the difference between rapid discovery and an extended dwell time. PowerShell, WMIC, and other tools native to your operating system can be leveraged against you, further deploying Bring Your Own Vulnerable Drivers (BYOVD) to create additional exploitation points. Halcyon's behavioral analytics leverage AI and Machine Learning to address this concern, drawing from past attacks. Rapid identification of exposure points and vulnerable tools can be the difference between a regular workday and an emergency.

Checklist:

☐ Thwart LoTL Tactics

Detect Living-off-the-Land techniques flagging malicious use of tools like PowerShell and WMIC through behavioral analytics.

☐ Slash Dwell Time

Monitor and spot threats faster, minimizing dwell time and preventing data encryption and theft with behavioral analysis and machine learning models designed exclusively for ransomware.

☐ Neutralize BYOVD Attacks

Halt unauthorized access and exfiltration attempts utilizing Bring-Your-Own-Vulnerable-Driver exploitation.

Ransomware by the Numbers

17%

of all ransomware attacks globally targeted healthcare, highlighting its position as a top target.

State of Healthcare 2025, PDF

$3.5M

is the average cost of a data breach for healthcare organizations.

State of Healthcare 2025

50%

of healthcare organizations lack confidence in detecting and resolving data breaches.

State of Healthcare 2025

03 | Ascension's Emergency Cyber Surgery

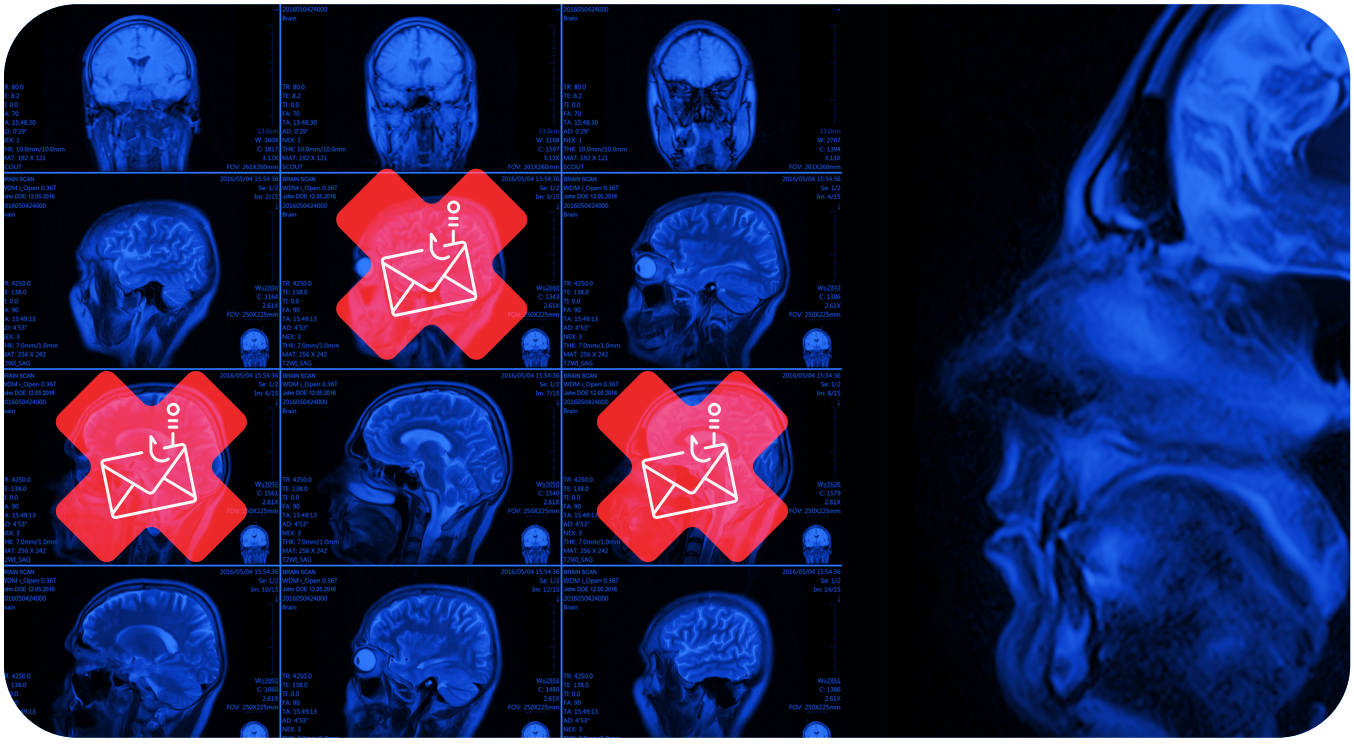
What Happened:

In May 2024, Ascension found itself in a similar scenario to Change Healthcare. Using a classic phishing email against an unsuspecting employee, the ransomware group Black Basta successfully infiltrated Ascension's critical systems. The threat actor wasted no time moving laterally across electronic health care (EHR), MyChart portals, and telephony servers. By May 8th, 2024, seven of the organization's 25,000 servers were compromised, and data exfiltration began. The problem? As reported by HealthCare IT News, all seven servers contained PHI and PII data. Here is the kicker: Ascension had all the right tools in place, including email filtering, EDR, and user training. One successful phishing attempt was all it took to bypass security measures.

Business Impact:

The attack brought down 140 hospitals across 19 different states, several emergency departments, and increased wait time for critical imaging results. Over 5.6 million people were affected by the breach, resulting in $1.1 billion in net loss for the fiscal year. Full recovery took roughly five weeks, and several class action lawsuits followed, alleging failure to adhere to industry HIPAA compliance standards.

The attack brought down 140 hospitals across 19 different states, several emergency departments, and increased wait time for critical imaging results.



Key Takeaways:

Security tools like email filtering and EDR are incredible advances in security. However, their generalist approach can be a detriment when they are required to find threats designed to bypass, blind, or disable tools like EDR. Threat actors have evolved to get around these tools first, giving them all the time they need to exfiltrate data, encrypt files, and leave behind a friendly reminder that payment in Bitcoin will suit just fine. Halcyon EDR Tamper Protection was designed to directly address the problem of EDR bypass. Tamper protection works in three ways: protecting against the use of vulnerable drivers to compromise your EDR, flagging when an EDR is tampered with, and lastly, protecting our own agent from compromise. Protect the tools that protect you.

Checklist:

☐ Fortify EDR Agents

Deploy EDR agent protection to prevent disablement or blindness, ensuring continuous malware detection.

☐ Flag Tampering Attempts

Rapidly detect neutralized defenses targeting EDR vulnerabilities and prevent kernel-level access.

☐ Secure Ransomware Agent

Ensure the self-protection of ransomware detection agents and establish breach-resistant ransomware barriers.

Ransomware by the Numbers

22%

of healthcare assets do not have active VSS protection even with EDR in place.

State of Healthcare 2025

60

seconds is the median time for users to fall victim to phishing emails.

Verizon Key Insights 2025

71%

of organizations that had experienced an email breach were also hit with ransomware.

2025 Ransomware Insights Report

04 | Digital Dashboard Lights Up Red At CDK

What Happened:

Even after two major breaches, 2024 was not finished. On June 18th, 2024, 15,000 car dealerships across the US were affected by the threat actor BlackSuit. CDK, a heavily utilized SaaS-based car dealer management system, was initially compromised when the threat actor gained access through a phishing attempt. Successful attempts led to CDK's files becoming encrypted and data being exfiltrated. Shortly after the breach, CDK attempted to restore services using backups to get dealerships back online. A day later, CDK was hit again, causing a complete shutdown of all online dealership services. Security professionals quickly criticized CDK for moving to restore operations too quickly, according to articles on BleepingComputer.

Dealership losses exceeded $1 billion in revenue, with sales dropping by as much as 50% and 100,000 fewer cars sold in June.

Business Impact:

This resulted in car sales, inventory searches, financing, and service requests all screeching to a halt, leaving everyone dusting off clipboards and rediscovering the ancient art of pen and paper sales. What made this breach even more dangerous was the "always-on" VPN tunnel connecting every dealership to CDK's data centers. Due to the VPN requirement, the risk for downstream exposure and encryption escalated for all 15,000 dealerships tied to CDK. BlackSuit gained access to use API keys or session IDs to potentially compromise dealerships using the VPN connection. Payment was sent by CDK on June 21st for roughly $25 million or 387 Bitcoin at that time. Dealership losses exceeded $1 billion in revenue, with sales dropping by as much as 50% and 100,000 fewer cars sold in June (a 7% decrease). Almost all dealerships were back up and running by July 4th, and 10 lawsuits were filed against CDK by dealership groups like Fowler Buick-GMC and Kinley Automotive Group.

Key Takeaways:

Loss of revenue from a ransomware attack is a tremendous risk to any organization. However, getting back online too quickly, especially with an always-on VPN, can be even riskier. Ransomware attacks are set apart. Requiring persistence, security tool tampering, and quick lateral movement, these tactics aren't always visible to organizations with a small or nonexistent security team. Often, behaviors and patterns can be misread or not seen at all without the proper expertise on hand. The Halcyon Ransomware Operations Center (ROC) is our response to this problem. Rapid identification of threats, behaviors, patterns, and open and exposed entry points is critical to discovery at the point of impact. Our ROC team does just that, providing that needed guidance, visibility, and quick reaction 24/7/365. Halcyon's ROC team catches what others miss, before an entire dealership is back to writing orders on sticky notes.

Checklist:

☐ Establish Guided Response

Gain access to clear, actionable alerts, isolation tools, and defined strategies that give SOC teams the visibility and guidance they need.

☐ Enhance Team Coverage

Automate monitoring with tamper-proof agents, bridging gaps and ensuring 24/7 SOC coverage, outsourcing as needed.

☐ Counter Blind Spots

Develop real-time insights into threats with defined threat intelligence against ransomware group Tactics, Techniques, and Procedures (TTPs).

Ransomware by the Numbers

69%

of organizations that paid ransom were attacked more than once.

2025 Ransomware Trends and Proactive Strategies

69%

of ransomware victims said they thought they were prepared before being attacked, but that confidence dropped by more than 20% post-attack.

Ransomware Trends 2025

46%

of internal SOC teams spend more time maintaining tools than defending threats.

State of Security 2025

05 | The Domino Effect of Blue Yonder's Supply Chains

What Happened:

Rounding out our top five attacks is a unique supply chain attack against Blue Yonder, a software company specializing in supply chain, logistics, retail, and commerce solutions for global brands. As 2024 ended, the threat actor group Termite launched an attack on November 21st, targeting Blue Yonder with a modified version of Babuk ransomware, whose source code had been publicly leaked. The attack on Blue Yonder's hosted environment disrupted inventory, demand forecasting, and warehouse management for 3,000 clients, including Starbucks, UK retailer Morrisons and Sainsbury's, Renault, Tesco, and Procter & Gamble.

Business Impact:

In the aftermath, over 11,000 Starbucks stores lost access to automated scheduling and payment systems, while UK retailers Morrisons and Sainsbury's had their warehouse management systems taken offline. Blue Yonder's server data was encrypted, but not before Termite exfiltrated 680 GB of data, which included sensitive information such as databases, email addresses, and over 200,000 insurance documents, according to a report by Cyberscoop. With one fell swoop, over 3,000 clients globally lost access to Blue Yonder without the ability to use backup systems in one of the largest ever supply chain attacks. By December, Blue Yonder successfully restored services to most of its clients.

In the aftermath, over 11,000 Starbucks stores lost access to automated scheduling and payment systems, while UK retailers Morrisons and Sainsbury's had their warehouse management systems taken offline.

Key Takeaways:

The interesting lesson from this attack is that the source code for the ransomware used, Babuk, was leaked. This meant that the potential for decryption was present if the means to reverse-engineer the key was available. While payment to ransomware groups only propagates future attacks, some organizations, due to a loss of backups or inability to decrypt, ultimately have little choice but to pay the ransom. Key Material Capture and decryption is one of the main ways Halcyon builds ransomware resiliency. When malicious encryption activities are detected, we attempt to capture the encryption key material generated. Coupled with our deep knowledge of ransomware attacks, we can accelerate decryption efforts. We snatch the symmetric key during encryption or reverse-engineer it afterward, so your supply chain keeps moving, and no ransom needs to be paid to get your files back.

Checklist:

☐ Enable Ransomware Decryption

Onboard decryption capabilities that recover data by analyzing ransomware behavior, restoring files without paying a ransom.

☐ Capture Key Material

Intercept key material during attacks, enabling rapid decryption in the event of a breach.

☐ Reverse-Engineer Encryption Keys

Establish or outsource ransomware data analysts to reverse-engineer post-breach ransomware encryption, unlocking encrypted data with precision.

Ransomware by the Numbers

62%

of organizations that reported a ransomware attack in the previous year noted that it had originated from a software supply chain.

2025 OpenText Cyber Report

91%

of respondents were concerned about supply chain ransomware attacks.

2025 OpenText Cyber Report

29%

of those who had data encrypted said they used “other means” to restore their data. This includes those who used decryption keys that had previously been made public.

Sophos State of Ransomware 2025

Defenses Built on Hard Lessons

These aren't just cautionary tales; they're grim reminders that the hard lessons surface during and after a crisis, when decisions carry real weight and visibility is clearest. Understanding what went wrong isn't about pointing fingers; it's about preparing smarter. Halcyon studied these attacks closely, using the insights to strengthen our approach and build solutions specifically designed to:

- Identify exfiltration attempts quickly
- Detect ransomware behaviors and patterns early
- Detect when attackers tamper with security tools
- Managed 24/7 by Ransomware Experts
- Decrypt your data, avoiding the ransom

In a connected world, where every minute offline is costly, resilience isn't built in the middle of an attack; it's built long before one ever begins. See how Halcyon stays one step ahead of ever-changing threats, and request a demo by emailing ***info@cyberfortgroup.com*** to discover the future of smarter protection.

halcyon Cyberfort Expert-led Security Driven.