RT ProExec

Wiper vs. Ransomware:
Same Policy, Completely Different Claim

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

INTRODUCTION

Ransomware has dominated the cyber insurance conversation for years. It is the loss scenario carriers underwrite to, the risk policyholders fear most, and the event brokers build coverage around. But the March 2026 Iran-linked cyberattacks introduced a different kind of destructive event at Fortune 500 scale: the wiper attack. No ransom demand. No decryption key. No negotiation. Just destruction.

For cyber insurance policyholders, the distinction between a ransomware event and a wiper event is not academic. The same policy can respond very differently depending on which type of attack occurs. Different first-party coverage triggers activate, different sublimits may apply, and certain coverage grants that are central to a ransomware response may be entirely irrelevant in a wiper scenario.

This article is a companion to RT ProExec's recent publications on the Iran-linked cyberattacks, including "Iran, Cyber War, and Your Policy" (analyzing war exclusion frameworks) and "When the Management Tool Becomes the Weapon" (analyzing MDM weaponization and triggering event definitions). This piece addresses a third coverage question: when the attack is destructive rather than extortive, how does the first-party coverage architecture of a cyber policy respond?

1. Two Attacks, Side by Side

To understand how the coverage differs, it helps to see what actually happens in each scenario.

Ransomware
The attacker gains access to the insured's network, typically through phishing, credential theft, or exploitation of a vulnerability. Once inside, they deploy encryption malware across servers, workstations, and sometimes backups. The insured's data is locked but still exists, it is encrypted, not deleted. The attacker delivers a ransom note demanding payment, usually in cryptocurrency, in exchange for a decryption key. The insured faces a decision: pay the ransom and hope the decryption key works or refuse and attempt to restore from backups. Either way, the organization experiences business interruption during the period of encryption and restoration.

Wiper
The attacker gains access to the insured's network or, as seen in the March 2026 incident, to a cloud-based management platform. Instead of encrypting data, the attacker destroys it. Devices are factory reset, hard drives are overwritten, servers are wiped. There is no ransom note because the attacker's objective is destruction, not payment. The data does not exist in an encrypted state waiting to be unlocked, it is gone. Recovery depends entirely on the integrity and availability of offline backups. If backups were also compromised or connected to the wiped environment, the data loss may be permanent.

Both attacks cause business interruption. Both require forensic investigation. Both may trigger notification obligations. But the recovery path and the coverage triggers are fundamentally different.

2. How the Policy Responds Differently

The following table compares how key first-party coverage components typically respond to a ransomware event versus a wiper event. The specifics will vary by carrier and policy form, but the structural differences are consistent across most standalone cyber policies.

Coverage Component	Ransomware Response	Wiper Response
Cyber Extortion	Primary coverage trigger. Covers ransom payment, negotiation costs, and expenses associated with responding to the extortion demand. Often the largest single component of a ransomware claim.	Not triggered. There is no extortion demand and no ransom payment. The entire extortion coverage grant is irrelevant in a wiper scenario.
Data Recovery / Restoration	Triggered, but often secondary. The primary recovery mechanism is decryption via the ransom key. Data restoration from backups is the fallback if decryption fails or if the insured refuses to pay.	Primary coverage trigger. With no decryption option, the insured must rebuild, recreate, or restore all data from backups. If backups are compromised, the cost and complexity of data recreation can be substantial.
Business Interruption	Triggered during the period of encryption, negotiation, and restoration. The BI period typically begins when systems are encrypted and ends when operations are restored to pre-incident functionality.	Triggered, and potentially for a longer duration. Restoring 200,000 factory-reset devices, rebuilding server infrastructure, and recreating lost data may take significantly longer than decrypting systems with a valid key.
Hardware Replacement / Bricking	Rarely triggered. Ransomware encrypts data but generally does not damage hardware. The physical devices remain functional once decrypted or reimaged.	May be a significant component of the claim. Devices that have been factory reset or had their firmware corrupted may require reimaging, reconfiguration, or in some cases physical replacement. Not all policies include bricking coverage.
Forensic Investigation	Triggered. Investigators determine how the attacker gained access, what data was accessed or exfiltrated, and the scope of the encryption. The investigation informs both the extortion response and the notification analysis.	Triggered, with additional complexity. Investigators must determine the same access questions but also assess what data was exfiltrated prior to the wipe (since exfiltration often precedes destruction), and how the wipe was executed particularly, if legitimate administrative tools were used.
Notification and Regulatory	Triggered if data was accessed or exfiltrated. Many ransomware actors exfiltrate data before encrypting it as additional leverage. The notification analysis focuses on what data the attacker accessed.	Triggered if data was exfiltrated prior to the wipe. The challenge is that the destruction of systems may also destroy the forensic evidence needed to determine what was exfiltrated, complicating the notification analysis.
Ransom Payment	Available under most policies, subject to sublimit, carrier consent requirements, and OFAC sanctions screening.	Not applicable. There is no ransom demand and no payment to evaluate.

3. Key Implications for Policyholders

Extortion-Heavy Policies May Underperform
Many cyber policies are structured with significant capacity allocated to the extortion tower high sublimit for ransom payments, dedicated negotiation and response services, and pre-arranged relationships with ransomware response vendors. In a wiper scenario, that entire coverage architecture sits unused. If the policy's data recovery, business interruption, and hardware replacement sublimit are lower than its extortion sublimit, the policyholder may find that the coverage available for the actual loss is substantially less than the policy's headline limit would suggest.

Data Recovery Becomes the Central Battleground
In a ransomware event, the fastest path to recovery is often paying the ransom and obtaining the decryption key. Data recovery from backups is the fallback plan. In a wiper event, data recovery from backups is the only plan. The cost, complexity, and duration of that recovery particularly if backups were also compromised can be significantly greater than the cost of decrypting systems. Policies with standalone data recovery and restoration coverage are typically better positioned to respond. In contrast, where data recovery is treated as a sub-component of extortion coverage, the scope of recovery may be more constrained.

Business Interruption May Run Longer
Ransomware incidents can often be resolved in days or weeks once a decryption key is obtained or backups are deployed. A wiper event that destroys hundreds of thousands of devices may take significantly longer to remediate. Reimaging laptops, reconfiguring servers, re-enrolling mobile devices, and recreating lost data extends the business interruption period and the associated BI claim well beyond what a typical ransomware event would produce. Policyholders should understand their BI waiting period, the period of restoration definition, and any aggregate sublimit that could cap recovery.

Bricking Coverage Is No Longer Optional
When ransomware encrypts a device, the hardware is generally fine once it is decrypted or reimaged. When a wiper factory resets a device, the hardware may need to be physically recovered, reconfigured, or replaced. For organizations with large device fleets, this cost can be material. Carriers that include affirmative bricking or hardware replacement coverage provide a meaningful advantage in a wiper scenario. Carriers that exclude it or that limit first-party coverage to data restoration only may leave a significant portion of the loss uncovered.

Forensic Challenges Compound the Claim
In a ransomware event, the encrypted systems often preserve forensic evidence — investigators can analyze access logs, lateral movement, and exfiltration activity on the locked systems once they are decrypted or imaged. In a wiper event, the destruction of systems may also destroy the forensic evidence needed to answer critical questions: What data was accessed? What was exfiltrated? How did the attacker gain access? This can complicate both the forensic investigation and the notification analysis, potentially increasing costs and extending the claims process.

4. Broker Considerations

The shift from ransomware to wiper attacks introduces coverage considerations that may warrant review in connection with current and upcoming cyber placements:

1. Review Sublimit Architecture
Compare the sublimit for extortion, data recovery, business interruption, and hardware replacement. If the policy allocates significantly more capacity to extortion than to the other components, the coverage may be misaligned with the risk profile of a wiper event.

2. Confirm Standalone Data Recovery
Determine whether Data Recovery / Restoration is triggered independently or primarily in connection with extortion-related events. Policies that treat data recovery as a standalone coverage grant are better positioned for wiper scenarios.

3. Evaluate Bricking Coverage
Determine whether the policy affirmatively addresses the cost of restoring, reimaging, or replacing devices that have been factory reset or rendered inoperable. This coverage component can materially affect how the policy responds in a loss scenario.

4. Assess the BI Period of Restoration
Review how the policy defines the period of restoration for business interruption coverage. Wiper events may produce longer restoration periods than ransomware events, and policies with narrow restoration definitions or short time limits could cap recovery.

5. Consider Forensic Evidence Destruction
For clients in regulated industries with notification obligations, discuss the scenario where a wiper attack destroys the forensic evidence needed to determine what data was exfiltrated. The costs of conducting a notification analysis without intact forensic evidence can be substantial.

CONCLUSION

The cyber insurance market has spent years calibrating its products around ransomware. Extortion coverage, negotiation services, decryption support, and ransomware-specific incident response have become standard features. That calibration served the market well when ransomware was the dominant destructive threat.

The March 2026 wiper attack demonstrated that the threat landscape has expanded. State-aligned actors with geopolitical objectives are not seeking payment — they are seeking destruction. A single coverage approach may not address both scenarios, as the frameworks that respond to ransomware events do not necessarily apply to wiper-type incidents in the same way.

Retail brokers who understand this distinction and can evaluate their clients' policies through both lenses — extortion and destruction — are better positioned to add value as the threat environment evolves. The question is no longer just "are you covered for ransomware?" It is "are you covered for what comes after ransomware?"

For further analysis of the broader insurance implications of the Iran-linked cyberattacks, see RT ProExec's companion articles: "Iran, Cyber War, and Your Policy: War Exclusions, Coverage Implications, and What Policyholders Need to Know Now" and "When the Management Tool Becomes the Weapon: MDM Weaponization and the Cyber Coverage Question."

SOURCES AND CITATIONS

The factual assertions in this article are based on the following publicly available sources and the author's analysis of cyber insurance coverage structures.

Krebs, Brian. "Iran-Backed Hackers Claim Wiper Attack on Medtech Firm." KrebsOnSecurity. March 12, 2026. https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/

Cimpanu, Catalin. "Medtech Giant Offline After Iran-Linked Wiper Malware Attack." BleepingComputer. March 11, 2026. https://www.bleepingcomputer.com/news/security/medtech-giant-stryker-offline-after-iran-linked-wiper-malware-attack/

Collier, Kevin. "Iran Appears to Have Conducted a Significant Cyberattack Against a U.S. Company." NBC News. March 11, 2026. https://www.nbcnews.com/world/iran/iran-appears-conducted-significant-cyberattack-us-company-first-war-st-rcna263084

Kovacs, Eduard. "Iran-Linked Hacker Attack Disrupted Manufacturing and Shipping." SecurityWeek. March 13, 2026. https://www.securityweek.com/iran-linked-hacker-attack-on-stryker-disrupted-manufacturing-and-shipping/

"The Attack: Enterprise Resiliency Plans Can't Ignore UEM." Forrester Research. March 2026. https://www.forrester.com/blogs/the-stryker-attack-enterprise-resiliency-plans-cant-ignore-uem/

"Stryker Attack Raises Concerns About Role of Device Management Tool." Cybersecurity Dive. March 2026. https://www.cybersecuritydive.com/news/stryker-attack-device-management-microsoft-iran/814816/

Otto, Emily. "Shamoon to Stryker: Iran Wields Wiper Attacks." Center for European Policy Analysis (CEPA). March 16, 2026. https://cepa.org/article/shamoon-strikes-stryker-iran-wields-wiper-attacks/

Zetter, Kim. "Iranian Hacktivists Strike Medical Device Maker in 'Severe' Attack that Wiped Systems." Zero Day (Substack). March 11, 2026. https://www.zetter-zeroday.com/iranian-hacktivists-strike-medical-device-maker-stryker-in-severe-attack-that-wiped-systems/

Palo Alto Networks, Unit 42. "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran." March 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/

Mula, James. "Iran, Cyber War, and Your Policy: War Exclusions, Coverage Implications, and What Policyholders Need to Know Now." RT ProExec. March 2026. https://blog.ryanspecialty.com/iran-cyber-war-and-your-policy

All sources were accessed between March 11 and April 2, 2026. This article does not reproduce copyrighted material; all factual claims are paraphrased from the cited sources.