The Stryker "Wiper" Incident

March 2026

AutoTableTop™ 2.0 Facilitator Guide

Subject:	Cyber-Sabotage, Administrative Tool Weaponization, and Geopolitical Retaliation
Target Audience:	Incident Response Teams (IRT), C-Suite Executives, IT Operations (ITOps), Identity & Access Management (IAM), Legal/Compliance, Supply Chain Risk Managers, Crisis Communications
Classification:	CONFIDENTIAL — For Facilitator Use Only
Version:	2.0 — April 7, 2026

Prepared by Derezzed Inc. d/b/a ThreatGEN
For use with AutoTableTop™ 2.0 AI-Powered Tabletop Exercise Platform

Table of Contents

1. Executive Summary

In March 2026, Stryker Corporation, a Fortune 500 medical technology leader with $25.1 billion in annual revenue and operations across 79 countries, suffered one of the most consequential cyberattacks in corporate history. This was not a ransomware attack for financial gain. It was a state-aligned destructive operation designed to cause maximum organizational damage with zero expectation of payment.

The threat actor, **Handala** (assessed by multiple intelligence firms as a front for **Void Manticore**, a destructive operations unit within Iran's Ministry of Intelligence and Security), weaponized Stryker's own Microsoft Intune endpoint management console to issue a mass factory-reset command. Approximately **80,000 to 200,000 devices** were wiped across 79 countries between 05:00 and 08:00 UTC on March 11, 2026. No ransomware or traditional malware was deployed. The attack used purely legitimate administrative tooling—a textbook *Living-off-the-Land (LotL)* operation that rendered endpoint detection and response (EDR) solutions blind.

This case study represents a structural shift in the cyber threat landscape. It demonstrates that the most dangerous attack surface in a modern enterprise is not the endpoint—it is the identity and administrative control plane. When an attacker gains Global Administrator privileges in Microsoft Entra ID, they hold a kill-switch for every enrolled device in the organization, and every command they issue is treated as a legitimate administrative action.

This facilitator guide provides everything needed to run a comprehensive tabletop exercise using the AutoTableTop™ 2.0 platform based on this incident. It includes the granular attack timeline, expanded exercise injects, facilitator questions, scoring criteria, and the technical and organizational context required to drive meaningful participant decision-making.

2. Incident Background & Context

2.1 Geopolitical Trigger

The Stryker attack was explicitly framed by Handala as retaliation for the February 28, 2026, joint U.S.-Israeli military strikes in Tehran (designated “Operation Epic Fury”). Iranian officials subsequently stated that Tehran would expand its targeting to include economic centers, banks, and companies with ties to the U.S. military or Israel. Stryker was identified as a target due to its significant U.S. military medical device contracts and its ownership of OrthoSpace Ltd., an orthopedic device subsidiary based in Israel.

2.2 Why This Attack Matters

- **Paradigm shift from ransomware to destruction:** The attacker’s goal was not financial. There was no ransom demand, no negotiation channel, and no decryption key. Recovery required rebuilding from scratch—not paying a fee.
- **Control-plane compromise, not endpoint compromise:** The attack succeeded without deploying a single piece of malware. EDR, antivirus, and endpoint hardening were irrelevant because the attack operated through the legitimate administrative control plane.
- **Living-off-the-Land at enterprise scale:** Every destructive action was a signed, authorized command from Microsoft Intune’s own cloud service. From the platform’s perspective, every wipe was a legitimate administrative action.
- **Identity = infrastructure:** A single compromised administrator account, elevated to Global Administrator, was sufficient to destroy the operational capacity of a $25 billion company across 79 countries.
- **Medical supply chain impact:** While connected medical devices were architecturally isolated and unaffected, the disruption to ordering, manufacturing, and shipping systems had direct downstream effects on patient care, including delayed surgeries and offline emergency medical telemetry systems.

2.3 What This Is Not

This is not a ransomware scenario. Facilitators should actively redirect participants who default to ransomware-oriented responses (e.g., “should we pay the ransom?” or “contact the attacker for a decryption key”). There is no ransom. There is no decryption. The data is gone. The devices are wiped. The only path forward is restoration from backups—and verification that the environment is clean before restoration begins.

3. Threat Actor Profile: Handala (Void Manticore / Storm-1084)

Handala is an Iranian-linked cyber persona that blurs the boundary between hacktivism and state-sponsored sabotage. Multiple independent threat intelligence firms—including Check Point Research, CrowdStrike, Microsoft, and Palo Alto Networks Unit 42—assess Handala as one of several online personas operated by Void Manticore, a destructive operations unit directed by Iran's Ministry of Intelligence and Security (MOIS). Microsoft tracks this activity cluster as Storm-1084.

Attribute	Detail
Aliases	Handala, Void Manticore, Storm-1084, DEV-1084
State Sponsor	Iran — Ministry of Intelligence and Security (MOIS)
Operational Doctrine	Combined "Hack-and-Leak" and "Wiper" operations. Goal: psychological impact and degradation of Western critical infrastructure. Not financially motivated.
Geopolitical Trigger	Feb 28, 2026 joint U.S.-Israeli "Operation Epic Fury" strikes in Tehran. Handala called Stryker "a Zionist-rooted corporation."
Tool Overlap	Code analysis links Handala to other Iranian units (MuddyWater/Void Manticore), suggesting they are a front-end persona for more sophisticated state capabilities.
Historical Precedent	Iran has conducted some of the most destructive wiper attacks in history: Saudi Aramco (Shamoon, 2012), Sands Casino (2014), Albanian government systems (2022). The Stryker attack continues this doctrine.
Claimed Impact	Wipe of 200,000+ devices, exfiltration of 50 TB of corporate data, screenshots of Rubrik Secure Vault and vSphere control panels published on Telegram.
Post-Attack Actions	U.S. DOJ seized four websites used by Iran's MOIS to spread threats and claim responsibility for hacking operations.

4. Technical Deep Dive: The Intune Kill-Switch

The attack succeeded because it exploited the administrative control plane rather than the endpoint. Understanding this distinction is essential for facilitators—participants trained in ransomware response will need to be guided toward a fundamentally different mental model.

4.1 Initial Access: Adversary-in-the-Middle (AiTM) Phishing

The attackers did not guess a password or brute-force MFA. They deployed an Adversary-in-the-Middle (AiTM) phishing attack—likely using a phishing-as-a-service platform such as Tycoon 2FA—that perfectly replicated Stryker's branded Microsoft login screen. The attack works as follows:

1. **Targeted phishing email:** A convincing email (likely a Microsoft 365 notification or SharePoint document share) was sent to a senior systems administrator.
2. **Reverse proxy interception:** The link directed the victim to an attacker-controlled server running a reverse proxy positioned between the victim and the real Microsoft Entra ID login page. All traffic was forwarded transparently in both directions.
3. **Session token theft:** The victim authenticated normally—including completing MFA—but the reverse proxy captured the resulting authenticated session token (cookie). This is not a password theft; it is a complete session hijack that renders MFA irrelevant.
4. **Token replay:** The attackers replayed the stolen session token to access Microsoft Entra ID as the authenticated administrator, with full privileges, without triggering any additional authentication challenges.

4.2 Privilege Escalation: Ghost Admin Creation

Using the hijacked administrator session, the attackers accessed Microsoft Entra ID and created a new account with Global Administrator privileges—a "Ghost Admin" that was not associated with any known employee and was not subject to existing monitoring or access reviews. This new account served as the primary execution identity for the wipe operation, ensuring persistence even if the original compromised account was detected and disabled.

4.3 Execution: The Intune Mass Wipe

Microsoft Intune is a cloud-based unified endpoint management (UEM) platform that manages corporate device fleets from a single web console. When a device is enrolled in Intune (whether a corporate laptop or a personal phone through BYOD), it trusts Intune as an authority. If Intune sends a factory reset command, the device executes it immediately ***without further verification***. Between approximately 05:00 and 08:00 UTC on March 11, 2026, the Ghost Admin account issued remote wipe commands to all enrolled devices simultaneously. The wipe affected:

- Corporate Windows workstations and laptops
- Windows servers with Intune enrollment
- Corporate mobile phones
- Personal BYOD devices enrolled through Intune's Work Profile
- **Note:** On some older OS versions, a bug in the Work Profile isolation caused a full device wipe of personal phones, destroying employees' personal data (photos, messages, apps) in addition to corporate data.

4.4 Why EDR Was Blind

This is the critical insight for exercise participants: Endpoint Detection and Response (EDR) solutions are designed to detect malicious software, anomalous processes, and suspicious file activity on the endpoint.

The Intune wipe command is none of these things. It is a signed, legitimate administrative instruction issued from Microsoft's own cloud infrastructure. From the EDR's perspective, it was an authorized administrative action—indistinguishable from a legitimate IT operation. There was nothing to detect, nothing to block, and nothing to alert on at the endpoint level.

4.5 Persistence & Additional Actions

- **Web shells:** The attackers established multiple persistent entry points to ensure continued access even if one was discovered.
- **Multiple admin accounts:** Additional administrative accounts were created to ensure the wipe operation would continue even if the Ghost Admin was detected and disabled mid-execution.
- **Data exfiltration claim:** Handala claimed to have exfiltrated 50 TB of data prior to the wipe, publishing screenshots of Rubrik Secure Vault and VMware vSphere control panels as proof of access depth.
- **Concealment:** A malicious file was used to run commands while hiding activity from Stryker's threat detection solutions during the pre-detonation reconnaissance and data exfiltration phases.

5. Target Organization Profile: Stryker Corporation

Attribute	Detail
Full Name	Stryker Corporation (NYSE: SYK)
Headquarters	Portage, Michigan, USA
Revenue (2025)	$25.1 billion
Employees	~56,000 globally across 79 countries
Industry	Medical Technology / Medical Devices & Equipment
Business Divisions	Orthopaedics; MedSurg & Neurotechnology; Spine
Key Products	Mako robotic surgical system, LIFEPAK defibrillators, Airo TruCT mobile imaging, Vocera communications, care.ai ambient monitoring, SurgiCount surgical safety, orthopedic implants
Israeli Subsidiary	OrthoSpace Ltd. (acquired 2019) — cited by Handala as targeting justification
CISO	Dave Nathans
CEO	Kevin Lobo
IT Environment	Microsoft-centric: Entra ID, Intune (UEM/MDM), Microsoft 365, Azure cloud. Hybrid with on-premises Active Directory. Key enterprise apps: DELMIA Apriso (MES), Mainsaver (CMMS), SolidWorks (CAD). BYOD program with Intune enrollment.
Product Architecture	Connected medical products operate on isolated, architecturally independent networks. Vocera Ease on AWS. SurgiCount in dedicated isolated cloud. Mako, LIFEPAK, Airo TruCT on independent product networks with no standard pathway to corporate IT.

6. Granular Incident Timeline (MSEL)

The following Master Scenario Events List (MSEL) provides the granular timeline that drives the AutoTableTop™ 2.0 exercise. All times are Eastern Standard Time (EST) unless otherwise noted.

Time (EST)	Phase	Event Description
T−24 hrs	**Reconnaissance**	Handala conducts pre-attack reconnaissance of Stryker's Microsoft environment. Attacker identifies senior systems administrators with Intune privileges through LinkedIn OSINT and credential-stuffing attempts. AiTM phishing campaign is staged using a phishing-as-a-service platform (e.g., Tycoon 2FA) that replicates Stryker's branded Microsoft login page. A malicious file is prepared to conceal post-compromise activity from threat detection.
02:00 AM	**Initial Access**	Attackers bypass MFA using session hijacking (AiTM). A valid session token for a senior systems administrator is captured via the reverse proxy and replayed to access Microsoft Entra ID. The attacker is now authenticated as a trusted administrator.
02:15 AM	**Concealment**	A malicious file is deployed to run commands while hiding activity from Stryker's threat detection solutions. This file does not have the ability to spread (confirmed by Unit 42 forensics) but provides operational concealment during the pre-detonation phase.
02:30 AM	**Data Staging**	Attackers begin exfiltration operations. Handala later claims 50 TB of corporate data was stolen, publishing screenshots of Rubrik Secure Vault and VMware vSphere control panels as proof of deep infrastructure access.
03:15 AM	**Escalation**	Using the hijacked session, attackers access Microsoft Entra ID and create a "Ghost Admin" account with Global Administrator privileges. Additional admin accounts are created as backup persistence mechanisms. Web shells are established for alternative re-entry.
04:00 AM	**Detonation**	**The mass "Wipe" command is triggered via Microsoft Intune using the Ghost Admin account.** Unlike a malware payload, this is a native UEM function—a signed, legitimate administrative command that is trusted implicitly by every enrolled device. The command is issued to all enrolled endpoints simultaneously across 79 countries.
04:05 AM	**Mass Impact**	Mass "Blue Screen" events begin globally. Laptops, Windows servers, and personal BYOD phones begin unrecoverable factory resets across 79 countries. Employees discover devices wiping in real-time. Some employees urgently uninstall Intune and Company Portal from personal devices to halt the wipe. Login screens on some devices are replaced with Handala's logo.
05:00 AM	**Containment**	Stryker's cybersecurity team detects the mass wipe and activates the incident response plan. Systems are isolated. External advisors and forensic experts are engaged. Microsoft's Detection and

		Response Team (DART) is notified. The immediate priority is stopping the ongoing wipe and revoking the Ghost Admin accounts.
06:00 AM	**Communications Blackout**	Internal communications (Outlook, Teams) are confirmed offline. Corporate email is unavailable. Employees in multiple countries are sent home. In Ireland, 5,500 employees across Stryker's hub are told not to come in. Out-of-band communication (phone, personal email) becomes the only coordination method.
09:00 AM	**Regulatory Filing**	Stryker files an 8-K with the SEC disclosing the cybersecurity incident. A second 8-K is filed the following day (March 12). CEO Kevin Lobo posts a letter to employees on LinkedIn. CISO Dave Nathans begins direct outreach to key customers and cybersecurity community members.
Day 1–3	**Triage & Assessment**	Palo Alto Networks Unit 42 is engaged for digital forensics and incident response (DFIR). Coordination begins with FBI, CISA, White House National Cyber Director, DHA, HHS, and H-ISAC. Electronic ordering systems remain offline; manual ordering through sales representatives is activated as fallback. Maryland EMS reports LIFENET ECG transmission system is offline statewide.
Day 3	**Secondary Claims**	Handala posts on Telegram claiming exfiltration of 50 TB of data. Screenshots of Rubrik Secure Vault and vSphere control panels are released. Handala states the attack is "only the beginning of a new chapter in cyber warfare." Iranian officials announce expanded targeting of U.S. economic centers.
Day 4	**CISA Alert**	CISA issues public alert urging all U.S. organizations to harden endpoint management system configurations. Microsoft publishes best practices for securing Intune. CISA recommends Multi Admin Approval, phishing-resistant MFA, and Privileged Identity Management (PIM) deployment.
Day 5	**Assurance Letter**	Palo Alto Networks Unit 42 issues an assurance letter confirming: no evidence of unauthorized activity since March 11; malicious file confirmed unable to spread; incident contained to internal Microsoft environment; no evidence of customer, supplier, vendor, or partner system compromise.
Day 7–14	**Restoration**	Primary manufacturing lines begin returning to operation. Core transactional systems (ordering, shipping, distribution) are progressively restored. Personalized implant orders begin processing. Some patient-specific surgical cases that were rescheduled during the disruption are rebooked. Recovery cost estimated in the hundreds of millions. At least 6 employee lawsuits filed over stolen personal data.
Day 21+	**Full Recovery**	Stryker announces it is fully operational across its manufacturing network and moving rapidly toward peak production capacity. Commercial, ordering, and distribution systems fully restored. DOJ seizes four websites used by Iran's MOIS. Product supply remains healthy with strong availability across most product lines.

7. Expanded Exercise Injects

The following injects are designed to be introduced sequentially during the exercise to escalate pressure, force trade-off decisions, and test different functional areas of the participant organization. Each inject includes a trigger time, scenario description, pressure point, and facilitator guidance.

Inject #1: The Personal Privacy Crisis (Legal/HR)

Trigger	T+30 minutes after initial detection
Scenario	The Intune factory reset hit the “Work Profile” on personal BYOD phones, but a bug in older Android/iOS versions caused a Full Device Wipe on a subset of enrolled devices. Thousands of employees have lost personal photos, messages, financial apps, and personal data. Employee social media posts are going viral. An employee in Ireland posts: “Stryker just wiped my kid’s photos off my personal phone. Every single one.”
Pressure Point	Legal counsel warns that “Hold Harmless” clauses in the BYOD enrollment agreement may not cover “Gross Negligence” if the company failed to implement reasonable safeguards on the Intune admin console (e.g., Multi Admin Approval, phishing-resistant MFA). HR is fielding hundreds of calls from distraught employees. At least 6 lawsuits will eventually be filed.
Facilitator Guidance	This inject forces a conversation about BYOD risk that most organizations avoid until it’s too late. Key questions: Does your BYOD policy explicitly address what happens when the MDM platform itself is compromised? Does your enrollment agreement cover company liability for destructive attacks? Should BYOD devices be enrolled in the same Intune tenant as corporate-owned devices, or should they be segmented?

Inject #2: The Clean Room Lockout (Facilities/Operations)

Trigger	T+1 hour
Scenario	Badge readers and IoT HVAC control systems in Stryker’s implant manufacturing “Clean Rooms” authenticate through Entra ID. With the identity provider disrupted, these systems have defaulted to a “Fail-Secure” (locked) state. No one can badge into the clean rooms, and the HVAC environmental controls are no longer maintaining the required temperature, humidity, and particulate levels.
Pressure Point	If the HVAC environmental controls remain offline for more than 4 hours, the current $50 million batch of custom orthopedic implants in production is considered contaminated under FDA manufacturing standards and must be destroyed. Facilities is asking: do we physically override the badge locks (violating physical security protocols during an active attack) or do we let the batch be destroyed?
Facilitator Guidance	This inject exposes the IT/OT convergence risk. Key question: Do your manufacturing environmental controls depend on the same identity provider as your corporate IT? If so, a corporate IT compromise can cascade into manufacturing disruption—even if the OT network itself is technically

	"segmented." This forces participants to confront the difference between network segmentation and identity dependency.

Inject #3: The Ghost in the Machine (Trust/Security)

Trigger	T+2 hours
Scenario	The recovery team begins restoring servers from Rubrik backups. Thirty minutes later, Handala posts a message on Telegram: "We saw you restoring the Finance DB. Thank you for doing the work for us. We've updated the admin password again." The message includes a screenshot showing a timestamp from Stryker's internal Rubrik console taken after the wipe was supposed to have been contained.
Pressure Point	How do you verify the integrity of your "clean" restoration environment when the attackers may still have access to the identity provider? Do you trust your backups if the attacker had access to Rubrik? Do you bring systems back online knowing the attacker is watching, or do you delay restoration (and manufacturing) by days to perform a complete identity provider rebuild?
Facilitator Guidance	This is the highest-stress inject in the exercise. It tests whether the team understands that you cannot restore from backups into a compromised identity environment. The correct response involves building a clean Entra ID tenant, revoking all existing session tokens, disabling all admin accounts, and rebuilding identity infrastructure before restoring application workloads. Most teams will want to "just restore and monitor"—the facilitator should push back hard on this impulse.

Inject #4: The Surgical Supply Crisis (Supply Chain/PR)

Trigger	T+4 hours
Scenario	Major trauma centers report that Stryker "Personalized Implants" (custom-manufactured for specific patients based on pre-operative imaging) are stuck in a wiped shipping/logistics system. Surgeons at three Level 1 trauma centers are threatening to cancel life-saving operations scheduled for this week. Separately, Maryland EMS reports that Stryker's LIFENET ECG transmission system—used by paramedics to transmit cardiac data to hospitals en route—is offline across most of the state. Paramedics are falling back to radio consultations.
Pressure Point	Prioritization dilemma: Do you allocate recovery resources to restoring the public website (to control the media narrative and reassure investors) or the logistics/shipping SQL servers (to get implants to patients)? What is the communication strategy to hospitals and surgeons? How do you handle the EMS system going offline—is this a patient safety issue that requires a separate FDA notification?
Facilitator Guidance	This inject tests crisis prioritization. Participants must weigh reputational damage against patient safety. The "right" answer depends on the organization's values—but participants who prioritize PR over patient-facing

	systems should be challenged. This also forces a discussion about regulatory notification obligations: when a medical device's supporting infrastructure goes offline, at what point does it become an FDA-reportable event?

Inject #5: The Insider Doubt (HR/Security)

Trigger	T+6 hours
Scenario	The forensic team identifies that the compromised administrator account belongs to a senior IT employee who recently returned from a vacation in a country with known Iranian intelligence operations. Security leadership asks: is this an insider threat, or was this employee simply phished? HR wants to suspend the employee immediately. Legal warns that premature action could constitute wrongful termination and trigger additional litigation.
Pressure Point	How do you handle the human element during a nation-state investigation? Do you isolate the employee without accusation? Do you involve law enforcement immediately? What if the employee is innocent and your actions destroy their career and reputation? What if they are complicit and your delay allows them to destroy evidence?
Facilitator Guidance	This inject introduces the human dimension that is often absent from technical tabletop exercises. The correct approach involves coordinating with legal counsel and law enforcement (FBI) before taking any employment action, preserving forensic evidence from the employee's workspace and accounts, and conducting the investigation without prejudging the outcome. Facilitate discussion about the difference between account compromise (victim) and insider threat (perpetrator).

Inject #6: The Media Firestorm (Communications/Executive)

Trigger	T+8 hours
Scenario	NBC News breaks a story identifying the attack as the first significant Iranian cyberattack against a U.S. company since the war started. The White House issues a statement. Congressional leaders demand a briefing. Stryker's stock drops 4% in pre-market trading. A major healthcare system (representing 8% of Stryker's annual revenue) calls the CEO directly to ask whether they should begin sourcing implants from a competitor "as a precaution."
Pressure Point	Who speaks publicly? What do they say? How do you balance transparency (the SEC requires material disclosure) with operational security (revealing recovery details could help the attacker)? How do you reassure the major healthcare system without making promises you cannot keep about restoration timelines?
Facilitator Guidance	This inject tests executive-level crisis communications under combined cybersecurity, geopolitical, financial, and regulatory pressure. The real Stryker response included an 8-K filing, CEO LinkedIn letter, CISO direct outreach, and coordinated government engagement. Facilitate discussion about pre-drafted

	holding statements, designated spokespersons, and the tension between SEC disclosure requirements and the desire to control the narrative.

8. Facilitator Pressure-Cooker Questions

The following questions are designed to be deployed at the facilitator's discretion throughout the exercise to deepen discussion, challenge assumptions, and expose gaps in organizational preparedness. They are organized by theme.

8.1 Identity & Administrative Controls

1. Do we have "Wipe Protection" thresholds set in our UEM/MDM to pause or alert if more than 100 devices are wiped within an hour?
2. How long do our admin session tokens last? Could a stolen session cookie be used 24 hours later? Do we enforce session duration limits for privileged accounts?
3. If Entra ID is compromised, do we have a secondary, out-of-band method to verify the identity of our own IT staff? How do we know the person on the phone claiming to be our sysadmin is actually our sysadmin?
4. Are we using phishing-resistant MFA (FIDO2/YubiKeys) for all privileged accounts, or are we still relying on push notifications that are vulnerable to MFA fatigue and AiTM session hijacking?
5. Do we have Multi Admin Approval configured for high-impact Intune actions (device wipe, bulk policy deployment, compliance policy changes)?
6. Is Privileged Identity Management (PIM) deployed with just-in-time access elevation, or do admin accounts hold standing privileges 24/7?

8.2 Detection & Response

1. Our EDR was blind to this attack because the wipe command was a legitimate administrative action. What additional telemetry or detection logic would catch a mass wipe in progress?
2. Do we monitor Entra ID audit logs for new Global Administrator account creation in real-time, or would we discover it during a post-incident review days later?
3. If our corporate email (Exchange Online) and Teams are offline, what is our out-of-band incident communication plan? Have we tested it?
4. How quickly can we revoke all active session tokens for all admin accounts across the entire Entra ID tenant?

8.3 Recovery & Restoration

1. Can we rebuild our Entra ID tenant from scratch? How long would it take? Do we have the configuration documented offline?
2. Are our backups stored in a system (e.g., Rubrik) that authenticates through the same Entra ID tenant that was compromised? If so, can we trust them?
3. What is our estimated time to recover 80,000 wiped devices? Do we have the imaging infrastructure, network bandwidth, and staff to do it?
4. Can our manufacturing operations sustain a 2-week system outage? What is the financial impact per day of manufacturing downtime?

8.4 Organizational & Legal

1. Does our BYOD policy explicitly address company liability when the MDM platform itself is weaponized against enrolled personal devices?
2. At what point does a disruption to medical device supporting infrastructure (e.g., LIFENET ECG transmission going offline) trigger FDA reporting obligations?

3. Who has pre-authorization to communicate publicly during a cybersecurity incident? Is the CEO's LinkedIn a sanctioned communication channel?
4. Do we have pre-established relationships with FBI, CISA, and our sector-specific ISAC (H-ISAC for healthcare)? Or would we be making cold calls during the crisis?

8.5 Geopolitical & Threat Intelligence

1. Do we monitor geopolitical threat intelligence that could signal increased risk of nation-state targeting? Would the February 28 strikes in Tehran have triggered an elevated alert posture for us?
2. Do we have an Israel-based subsidiary, U.S. military contracts, or other attributes that would make us a geopolitically motivated target? Have we assessed this risk?
3. How would our response differ if this were a ransomware attack with a ransom demand versus a destructive wiper with no path to recovery?

9. Win/Loss Conditions & Scoring Rubric

9.1 Win Conditions (Indicators of Effective Response)

- Team identifies the attack as a wiper (not ransomware) within the first decision round and adjusts response strategy accordingly.
- Team prioritizes identity provider containment (revoking sessions, disabling admin accounts, isolating Entra ID) before attempting system restoration.
- Team activates out-of-band communications and does not rely solely on corporate email/Teams for incident coordination.
- Team explicitly addresses the BYOD personal device impact and initiates legal/HR coordination.
- Team prioritizes patient-facing logistics/shipping systems over public website restoration.
- Team engages appropriate government agencies (FBI, CISA) and industry partners (H-ISAC) early in the response.
- Team demonstrates awareness that backups restored into a compromised identity environment are not trustworthy.
- Team develops coordinated external communications (SEC filing, customer updates, media holding statement) within the first 4 hours.

9.2 Loss Conditions (Indicators of Ineffective Response)

- **Team treats the incident as ransomware** and wastes time looking for a ransom note, negotiation channel, or decryption key.
- **Team begins restoring systems from backups without first verifying the identity provider is clean** and without revoking all compromised admin sessions.
- **Team fails to address the BYOD personal device wipe** and does not coordinate with Legal/HR on employee communications and liability.
- **Team prioritizes public image (website, press release) over patient-facing systems** (logistics, shipping, EMS telemetry).
- **Team does not activate out-of-band communications** and attempts to coordinate the response using the compromised corporate email/Teams environment.
- **Team does not engage law enforcement or government agencies** within the first 8 hours of detection.
- **Team takes premature employment action** against the compromised administrator without legal coordination.

10. Participant Roles & Responsibilities

The following roles should be represented during the exercise. Depending on group size, participants may cover multiple roles.

Role	Exercise Responsibilities
CISO / Security Lead	Overall incident command. Drives containment and eradication decisions. Coordinates with forensic teams and government agencies. Authorizes identity provider rebuild.
CIO / IT Operations Lead	Manages system restoration priority and sequencing. Coordinates device re-imaging. Oversees backup integrity verification. Manages Intune/Entra ID recovery.
CEO / Executive Sponsor	Authorizes public statements and SEC filings. Manages board communications. Makes final prioritization calls on recovery sequencing (PR vs. patient systems).
General Counsel / Legal	Advises on SEC disclosure timing and content. Assesses BYOD liability exposure. Coordinates with law enforcement. Manages litigation risk from employee lawsuits.
VP Supply Chain / Logistics	Manages manual ordering fallback process. Prioritizes personalized implant orders. Coordinates with hospitals and surgeons on delayed deliveries. Assesses manufacturing batch contamination risk.
VP Communications / PR	Drafts customer updates, media holding statements, and employee communications. Manages social media monitoring. Coordinates with IR team on what can be disclosed.
IAM / Identity Engineer	Executes session revocation and admin account disablement. Leads Entra ID tenant rebuild. Verifies identity provider integrity before restoration begins.
HR Representative	Manages employee communications about personal device loss. Coordinates with Legal on the compromised administrator situation. Handles employee wellbeing concerns.

11. Key Takeaways & Lessons Learned

The following takeaways should be reinforced during the exercise debrief, regardless of how well participants performed during the exercise itself.

1. **Identity is the new perimeter.** The Stryker attack succeeded without malware, without exploiting a software vulnerability, and without bypassing endpoint security. It succeeded because a single privileged identity was compromised. Organizations must treat their identity provider (Entra ID, Okta, etc.) as critical infrastructure—not just an IT service.
2. **Endpoint management platforms are high-value targets.** Any platform with the authority to issue remote wipe, deploy software, or modify device configurations at scale is a potential weapon. Intune, JAMF, Workspace ONE, SCCM—all of these hold the same destructive potential if administrative access is compromised.
3. **Phishing-resistant MFA is not optional.** Push-based MFA and SMS-based MFA are both vulnerable to AiTM session hijacking. Only hardware-bound, phishing-resistant MFA (FIDO2/WebAuthn/passkeys) prevents the specific initial access technique used in this attack.
4. **Multi Admin Approval is a critical safeguard.** The ability for a single administrator to wipe 80,000 devices without any secondary approval is a catastrophic single point of failure. Requiring a second authorized administrator to approve destructive actions would have stopped this attack.
5. **Wiper response is fundamentally different from ransomware response.** Ransomware is a financial negotiation. A wiper attack is a total loss event. There is no decryption key. The only path forward is clean rebuilding—starting with the identity infrastructure, then the management platforms, then the application workloads.
6. **Out-of-band communications must be pre-planned and tested.** When corporate email and Teams are down, organizations that have not pre-established alternative communication channels (Signal groups, satellite phones, personal email distribution lists) are blind and deaf during the most critical hours of the response.
7. **BYOD enrollment in corporate MDM creates shared-fate risk.** When personal devices are enrolled in the same management platform as corporate devices, a compromise of that platform affects both. Organizations must assess whether the productivity benefits of BYOD enrollment outweigh the risk of shared-fate destruction.
8. **Geopolitical threat intelligence is an operational input.** The Stryker attack was predictable in the sense that Iranian retaliatory cyber operations were widely anticipated following the February 28 strikes. Organizations with geopolitical exposure (military contracts, Israeli subsidiaries, critical infrastructure designation) should elevate their security posture in response to escalating geopolitical tensions.

12. References & Source Attribution

The following sources informed the development of this facilitator guide:

- Stryker Corporation, “Customer Updates: Stryker Network Disruption,” March 2026 (stryker.com)
- Stryker Corporation, SEC Form 8-K filings, March 11–12, 2026
- CISA, “CISA Urges Endpoint Management System Hardening After Cyberattack Against US Organization,” March 18, 2026
- Palo Alto Networks Unit 42, DFIR Assurance Letter to Stryker Corporation, March 2026
- Cybersecurity Dive, “Stryker attack raises concerns about role of device management tool,” March 2026
- Cybersecurity Dive, “Stryker confirms cyberattack is contained and restoration underway,” March 2026
- NBC News, “Iran appears to have conducted a significant cyberattack against a U.S. company,” March 2026
- HIPAA Journal, “Stryker Fully Operational After March Cyberattack,” April 2026
- Sygnia, “Stryker Incident: Entra ID & Intune as Attack Vectors,” March 2026
- Glueckkanja, “The Stryker Attack: How a Compromised Admin Account Wiped 80,000 Devices via Intune,” March 2026
- Forrester, “The Stryker Attack: Enterprise Resiliency Plans Can’t Ignore UEM,” March 2026
- Lumos, “The Stryker Hack: How One Compromised Admin Account Wiped 80,000 Devices,” March 2026
- SecurityAffairs, “Attack on Stryker’s Microsoft environment wiped employee devices without malware,” March 2026
- CBIA, “When the Goal Is Destruction: What the Stryker Cyber Attack Means,” April 2026
- Arctic Wolf, “Stryker Systems Disrupted in Cyber Attack; Handala Group Claims Responsibility,” March 2026

End of Facilitator Guide
AutoTableTop™ 2.0 — Derezzed Inc. d/b/a ThreatGEN
threatgen.com | sales@threatgen.com