No Malware. No Ransomware.

Identity Lessons from the Stryker Cyberattack

Adam Clifford

Chief Information Officer, Miron Construction

InfraGard Wisconsin Webinar

March 11, 2026

2:14 a.m.

Stryker, March 11, 2026

How the press coverage and the technical reality lined up

Sources

- Stryker SEC 8-K filing
- Stryker customer message page
- CISA Advisory (March 18, 2026)
- DOJ press release / FBI seizure
- BleepingComputer reporting
- KrebsOnSecurity
- Ars Technica (Dan Goodin)

No malware. No CVE. No zero-day.

Every preventive control was working. None of them mattered.

What they didn't use

- No exploit
- No malware payload
- No vulnerability
- Stryker confirmed: a malicious file ran commands but was not capable of spreading

What they did use

- A phished Windows admin password
- A new Global Administrator role assignment in Entra
- Microsoft Intune's built-in bulk wipe command

Why this matters

- Every preventive control was working as designed
- Compliance was passing, audits were clean
- The attack used the platform exactly as Microsoft built it
- This is living off the cloud control plane

About me

Adam Clifford

Chief Information Officer

Miron Construction

ABOUT MIRON CONSTRUCTION

Wisconsin general contractor. 1,700 people. Over $2B in annual revenue.

BACKGROUND

8 years consulting on Microsoft identity, endpoint, and security architecture. Clients ranged from small shops to Fortune 100s, including DOD. CIO at Miron since fall 2025.

WHY I'M HERE

The architecture I'll walk through is the playbook I've built and delivered with clients for years. Stryker is why I'm bringing it to Miron now, and why I think every M365 tenant should be having this conversation.

Microsoft Certifications

Active. Relevant. Backing the architecture you're about to see.

Cybersecurity Architect

EXPERT

Identity & Access Admin

ASSOCIATE

Endpoint Administrator

ASSOCIATE

Security Operations Analyst

ASSOCIATE

M365 Administrator Expert

Azure Administrator Associate

7 active Microsoft certifications across identity, endpoint, security, and cloud.

CISA's response guidance, March 18

Three recommendations published a week after the attack.

1

Least Privilege

for administrative accounts via Intune RBAC.

2

Phishing-resistant MFA

for privileged users via Conditional Access.

3

Multi-Admin Approval

for sensitive Intune actions like device wipes.

Source: CISA Advisory, March 18, 2026

Good start. Falls short.

Tracing CISA's recs against the Stryker kill chain.

WHAT IT CATCHES

- Casual credential theft (phishing-resistant MFA blocks it at sign-in)
- Single-admin destructive actions where MAA is configured (a small list of Intune resources)

WHAT IT MISSES

- Attackers never had to bypass MAA. They created a NEW Global Admin and used it.
- Role assignment is not in Microsoft's Protected Actions permission set today.
- MAA only protects a small list of Intune resources. The broader Entra control plane is not covered.
- Nothing in the recs requires a hardened admin workstation.
- Nothing in the recs requires step-up at the moment of high-impact action.

Think of your tenant like an operating room

Stryker builds the tools. We're going to borrow their world.

OR DISCIPLINE	IDENTITY ARCHITECTURE
Sterile field	→ Managed, compliant, hardened devices only
Scrubbing in	→ Phishing-resistant authentication and PAW entry
Surgical time-out	→ Step-up at the moment of high-impact action
Instrument count	→ Access reviews — what's been used, what's been left behind
Crash team	→ Break-glass and emergency access — intentional, rehearsed

Tiered admin accounts: Green, Yellow, Red

And inside the tiers — Always-on or PIM-eligible?

TIERS

GREEN

Routine ops

Helpdesk, password reset, reads.
Mix of always-on and PIM-eligible.

YELLOW

Service / workload

Non-interactive. IP and app constrained.
No interactive sign-in.

RED

Control plane

Global Admin, CA Admin, Security, Exchange, SharePoint, Teams admin.
Always PIM. Always PAW.

ALWAYS-ON vs PIM-ELIGIBLE

Always-on is for:

- Read-mostly roles
- Roles where activation friction creates fatigue without proportionate security benefit

PIM-eligible is for:

- Writes affecting security posture
- Identity, user, group, device, or data exposure changes
- Regardless of how routine the change feels

Default: PIM-eligible. Make always-on earn its place.

Phishing-resistant MFA. And step-up at the moment of risk.

PHISHING-RESISTANT MFA

FIDO2 keys. Passkeys. Windows Hello for Business.

Not SMS. Not number-matched push. Not OTP codes.

Those are still phishable through attacker-in-the-middle frameworks.

Microsoft doesn't use passwords internally — at all.

Their admin tier is fully passwordless. There's no reason yours should be different.

For legacy form-auth apps without OAuth or SAML, use a password vault with SSO to Entra. Stop typing passwords into browsers.

AUTHENTICATION CONTEXTS

Step-up tied to actions, not to sign-in.

Fresh phishing-resistant MFA, compliant device, PIM activation —

all required at the moment of risk.

Less friction at sign-in. More security at the action.

Privileged Access Workstations: a spectrum

Right answer depends on your risk profile, not someone else's reference architecture.

WHERE WE LANDED

Virtualized PAW — Windows 365 Cloud PCs

Strong isolation without a hardware program. Separate Azure VNet. No inbound. Egress allow-listed through Cisco Umbrella. Destroyed and rebuilt on a regular cadence.

Protected Actions: gating the verbs that matter

WHAT'S IN THE PERMISSION SET TODAY

- Conditional Access policy create / update / delete
- Cross-tenant access policy changes
- Named locations create / update / delete
- Hard delete of Entra directory objects
- Authentication Context binding changes

HONEST GAP

Role assignment isn't on the list.

The Stryker kill chain went through role assignment. The attack still hits the wall — just one stage later, when the attacker tries to weaken CA policies blocking the wipe.

PARALLEL ATTACK SURFACE

Workload identities.

Same kill chain works through an app registration with Graph permissions like RoleManagement.ReadWrite.Directory. App consent governance is the parallel program.

Continuous Access Evaluation + risk-based access

Two controls that work together. One is foundational. The other is the most expensive thing in your E5 license.

CONTINUOUS ACCESS EVALUATION

Re-evaluates access decisions in near real time after sign-in.

Triggers on:

- Password reset
- Account disable
- Risk score change
- Policy change
- Network change

Foundational. Tenant-wide. Most of you already have it.

RISK-BASED ACCESS

Risky Users + Risky Sign-ins feed CA policies.

Risky Users (aggregate signal):

Leaked credentials. Anomalous behavior. Malware association.

Risky Sign-ins (per-event):

Anonymous IP. Atypical travel. Unfamiliar device.

Locked behind Entra ID P2 / E5. Should be foundational. If you're paying for it and not using it, you're leaving the most expensive thing on the table.

LIVE DEMO

The Wall

Imagine an attacker has phished an admin's password and MFA. Valid session. Standard MFA. The kind of credential a phishing kit produces every day. They've signed into Azure. They want to weaken the Conditional Access posture before pivoting.

Watch what happens.

What just happened

1. The attacker had a valid credential. Sign-in succeeded. They got into the admin portal.

2. They tried to do the thing the Stryker attacker did — weaken the CA posture. They hit a wall. Not at sign-in. At the action.

3. The wall was a single Conditional Access policy targeting an Authentication Context, attached to the verbs the attacker needed. Phishing-resistant MFA and a compliant managed device were required. They had neither.

What this doesn't fully solve

An honesty slide. Identity controls limit blast radius. They don't eliminate it.

DETECTION ISN'T PREVENTION

You still need a SOC layer.

Even strong identity controls assume some breaches succeed. Sentinel, Defender for Identity, audit alerting on every Protected Action and PIM activation. Watch the slow, careful attacker.

WORKLOAD IDENTITIES

App registrations are the parallel surface.

Service principals can run the same kill chain through Graph permissions. App consent governance, app permission reviews, app authentication policies. Most orgs aren't watching it.

POST-AUTH TOKEN THEFT

Compliant device + CAE help. Residual risk remains.

Token protection (preview) will help more — binds session tokens to the issuing device. Limited M365 ecosystem support today. Track it. Don't assume it's solved yet.

Where the leverage actually is

After 8 years of consulting — controls I see most orgs leave on the table.

1

Compliant device requirement

Criminally underused. One of the best defenses against session token theft. Available in Entra ID P1 — most of you already have it.

2

Risk-based access + compliant device

Massive force multiplier. Rarely fully implemented. Locked behind Entra ID P2 / E5 — should be foundational, but isn't.

3

Passwordless + phishing-resistant

Microsoft doesn't use passwords internally. Use a password vault with SSO to Entra for the legacy form-auth gap.

4

Token protection (preview)

Next step against session token theft. Limited M365 ecosystem support today. App developers must implement. Watch this space.

This is a framework. Not a prescription.

Adapt to your context.

- Risk profile and threat model
- Regulatory and contractual obligations
- Organizational maturity and change tolerance
- Existing investments and skills

The shape of the architecture is what matters. The specifics will look different in your tenant.

Where to start. Where to go.

NEXT 90 DAYS

- Inventory your admin accounts. Tier them.
- Block legacy authentication tenant-wide if you haven't.
- Require phishing-resistant MFA for the Red tier.
- Stand up an Authentication Context for Protected Actions.
- Map at least one Protected Action to the new context.

NEXT 12 MONTHS

- PAW for the Red tier — pick your spectrum point.
- PIM-eligible for everything that isn't read-mostly.
- Compliant device + risk-based access on every CA policy that touches sensitive data.
- Workload identity program — app consent governance, app permission reviews.
- Detection coverage on Protected Actions and PIM activations.

This is dollars per admin per day, not a capital project. For a 1,700-person org, low five figures annually.

One last thing.

5,000 people in Cork didn't get a vote that morning.
79 countries didn't get a vote.

The vote you have is happening in your
next budget cycle.
Your next architecture review.
Your next conversation with your CEO.

Don't wait for your version of March 11.

Resources

Q&A

HARDENING BASELINES

OpenIntuneBaseline

github.com/SkipToTheEndpoint/OpenIntuneBaseline

Community-driven, CIS-aligned Intune hardening. If you do one thing — start here.

VENDOR GUIDANCE

Microsoft — Best practices for securing Microsoft Intune

techcommunity.microsoft.com (March 14, 2026)

Microsoft Learn — Authentication Contexts, Protected Actions, Token Protection

INCIDENT REFERENCES

CISA Advisory (March 18, 2026)
DOJ press release / FBI seizure (March 19, 2026)
KrebsOnSecurity (March 11, 2026)
BleepingComputer coverage (March 11–19, 2026)
Ars Technica — Dan Goodin

CONTACT

Adam Clifford

Chief Information Officer, Miron Construction

LinkedIn: /in/adamclifford

Questions?