April 1, 2026

Subject: Blackswan Cybersecurity Response to Recent CISA Guidance on Microsoft 365 Administrative Controls

CISA alert issued on March 18, 2026, following the cyberattack on Stryker Corporation.

Blackswan Cybersecurity specializes in **cybersecurity monitoring and response**. While we may not have administrative access to your Microsoft 365 tenant, we are well-positioned to serve as a trusted advisor to your IT team. We can provide targeted guidance, help identify gaps, and significantly enhance detection capabilities for privileged account activity and related anomalies in your existing environment.

Our Assessment of the Guidance

CISA recommendations are timely and directly address the Stryker incident, where attackers compromised a single Intune administrator account and used legitimate Microsoft tools to cause widespread disruption. The key safeguards highlighted least-privilege access, strong phishing-resistant multi-factor authentication (MFA) for privileged accounts, and multi-admin approval (two-person rule) for high-impact changes. These are excellent practices that align with both CISA guidance and the CIS Microsoft 365 Foundations Benchmark v6.0.0.

These controls are particularly important for regulated organizations like credit unions, as they help limit the blast radius of a potential compromise and support NCUA expectations around strong governance.

How Blackswan Can Support Your Team

We recommend the following proactive steps, which your IT team can implement while we enhance monitoring and detection on our end:

1. **Privileged Access Review**
    - Conduct an immediate inventory of all Global Administrators, Privileged Role Admins, Intune Administrators, and other elevated roles.
    - Reduce permanent assignments and move toward just-in-time access using Entra ID Privileged Identity Management (PIM).

2. **Strengthen Authentication Controls**
    - Enforce phishing-resistant MFA (e.g., FIDO2 security keys or certificate-based authentication) for all privileged accounts.
    - Review and tighten Conditional Access policies specifically for administrative sign-ins.
3. **Implement Multi-Admin Approval**
    - Enable Intune Multi-Admin Approval (MAA) access policies for high-impact actions, including device wipes, script deployments, RBAC changes, and major configuration modifications. This directly addresses the attack vector seen in the Stryker incident.
4. **Ongoing Governance**
    - Schedule regular privileged access reviews (monthly recommended).
    - Establish break-glass emergency accounts with strict monitoring.

Blackswan to Enhanced Monitoring and Response Detections

Blackswan has strengthened detections in the following areas:

- Anomalous privileged role activations or creations (e.g., new Global Admin accounts).
- Admin sign-in anomalies (impossible travel, unusual locations, or risky sign-ins).
- High-impact administrative actions in Entra ID, Microsoft 365, and Intune (even if approval workflows are in place).
- Configuration drift or unexpected changes to policies and roles.

We will tune our Monitoring and Detection platform with specific correlation rules and alerts tailored to your environment, enabling faster identification and response to any suspicious activity involving administrator accounts. We can also assist with developing response playbooks for privileged account incidents.

Next Steps

We are available to meet with your IT team to:

- Review your current privileged access posture (based on any data you can safely share).

- Prioritize the recommendations above.
- Confirm and optimize the current data sources and update to include any gaps (e.g., Entra ID, Microsoft 365 audit logs, and Intune activity).

Please let us know your availability, or feel free to reply with any specific questions. We are committed to helping your credit union meet these enhanced expectations efficiently while maintaining strong detection and response capabilities through our partnership.

Thank you again for the opportunity to support you on this important initiative.

Best regards,

Dr. Mike Saylor, DBA, CISM, CISA
Msaylor@blackswancybersecurity.com
www.blackswancybersecurity.com
855-BLK-SWAN