

CASE STUDY · JUNE 2023

From Ransomware Paralysis to Full Operations in 72 Hours

A project case study of how Massive IT neutralized a ProxyLogon/Hafnium ransomware attack against a Michigan college and restored 40+ servers over a single weekend.



Conceptual illustration only; not the customer's production environment.

Incident snapshot

Detail	Summary
Organization	Public community college, Western Michigan
Enrollment	Approx. 1,300 students; faculty and staff across multiple locations
Environment	Microsoft 365 / Exchange Online (production) plus legacy on-premises Exchange Server
Attack vector	ProxyLogon / Hafnium exploit — CVE-2021-26855 and related vulnerabilities
Endpoint protection	Legacy, consumer-grade antivirus
Servers encrypted	40+ servers — Active Directory, SQL, file, print, application
Systems down	All production systems, student management, email, workstation login
Operational impact	Full faculty and staff dismissal; classes and payments suspended
Call to Massive IT	Thursday, 9:00 AM EST
Operations restored	Monday morning — faculty and students back on schedule

The environment: a forgotten server, a wide-open door

Like many educational institutions moving to cloud services, this Michigan community college had recently migrated from its on-premises Microsoft Exchange Server to Microsoft 365 and Exchange Online. Email was running in the cloud, users were productive, and the IT team moved on.

But the legacy Exchange Server wasn't decommissioned. It remained online, exposed to the public internet and integrated with Active Directory, because its interface was convenient for hybrid identity and user provisioning. It no longer handled production email, so it wasn't on anyone's patching radar: no critical security updates, no service packs, no monitoring. From an attacker's perspective, it was a perfect target.

The ProxyLogon / Hafnium vulnerability (CVE-2021-26855)

ProxyLogon is a critical pre-authentication remote code execution vulnerability in Microsoft Exchange Server, weaponized by the Hafnium threat actor group and rapidly adopted by ransomware operators. An unpatched, internet-facing Exchange Server requires no user interaction and no credentials to exploit — a crafted HTTP request grants SYSTEM-level control. From that foothold, lateral movement through Active Directory is systematic and fast.

The attackers used ProxyLogon to take control of the Exchange Server, moved laterally through Active Directory, escalated privileges, and deployed ransomware across the network. The college's consumer-grade antivirus did not detect or stop the intrusion.

The scope of the attack: 40+ servers, zero access

Impact	Result
Servers encrypted	40+
Domain controllers compromised	100%
SQL and application servers	All down
Workstation login	Not possible

- All Active Directory domain controllers were encrypted, making workstation authentication impossible campus-wide.
- All SQL database servers were encrypted, taking down the Student Management System (SMS) that processes payments, enrollment, and curriculum changes.
- All file and print servers were encrypted, eliminating access to shared documents and printing.
- All application servers were encrypted, taking down every line-of-business application.

All faculty and staff were dismissed, classes were suspended, and student services were unavailable. The campus was, in every meaningful sense, offline.

Thursday, 9:00 AM: the call to Massive IT

The college's IT team contacted Massive IT on Thursday morning requesting emergency incident response. Massive IT engaged immediately, focusing the first hours on three objectives:

- **Root cause identification** — confirming ProxyLogon/Hafnium as the initial access vector and tracing the lateral movement path through Active Directory.

– **Command-and-control isolation** — severing the attacker's access and C2 channels to stop further exfiltration or encryption.

– **Damage assessment** — inventorying affected systems, identifying survivors, and locating viable backups.

Key finding: offline backups of the Active Directory environment were intact and recoverable. The entire recovery plan was built around them.

The recovery timeline: Thursday to Monday

When	Milestone
Thursday, 9 AM – EOD	Engage, diagnose, contain. Root cause confirmed via the unpatched legacy Exchange Server. Attacker C2 channels severed, scope assessed, recovery plan formed around the offline AD backup, and the legacy Exchange Server isolated and taken offline.
Friday, all day	Active Directory recovery begins. Offline backup validated, domain controller restoration initiated, and rebuild priorities set: domain controllers first, then the production application stack.
Saturday, by evening	Active Directory functional. Domain reconstituted from offline backup, new domain controllers promoted, workstation logins confirmed, and domain integrity validated across all locations.
Sunday, all day	Production server stack restored. File, print, SQL, and application servers rebuilt or restored; the Student Management System brought back online; integrations tested and final checks completed.
Monday morning	Full operations resume. Faculty and students returned to normal schedules. Remaining peripheral integrations were flagged for follow-up remediation.

The outcome: a campus back online in 72 hours

From the Thursday morning call to Monday morning operations, Massive IT and the college IT team recovered a fully encrypted 40+ server environment in under 72 hours of active work, without paying the ransom and without losing the academic calendar.

Result	Outcome
Time to restored operations	72 hours
Servers recovered	40+
Ransom paid	\$0
Classes	Faculty and students back on schedule Monday

The Student Management System was back online before the week began, so payments, enrollment changes, and curriculum access resumed without a billing cycle disruption. Active Directory was reconstituted from backup rather than rebuilt from scratch, preserving years of user, group, and policy configuration.

In the following days and weeks, Massive IT remained engaged on-site and remotely to resolve the remaining application integrations, peripheral configurations, and compatibility items. Every outstanding item was tracked, documented, and closed.

These outcomes describe this specific incident, not a guarantee for future engagements.

Post-recovery: securing the baseline

- The legacy Exchange Server was fully decommissioned, and hybrid identity management moved to modern tooling with no on-premises Exchange footprint.
- All remaining on-premises servers were audited and patched, with a documented patching cadence for ongoing maintenance.
- The legacy antivirus was replaced with enterprise-grade endpoint detection and response (EDR) providing behavioral threat detection.
- The internet-facing attack surface was reduced: unnecessary public services and ports closed and firewall policies tightened.
- Backup architecture was hardened with offline and offsite copies for all critical systems and routine integrity validation.
- Incident response protocols and escalation paths were documented and shared with the college IT team.

Security outcome: the college emerged with a stronger security posture than before the attack — a reduced attack surface, modernized endpoint protection, and backups validated under real-world recovery conditions.

Why Massive IT

- **Immediate response** — engaged within hours of the call, with no intake delay or queue.
- **Deep Active Directory expertise** — recovery centered on offline AD backup reconstitution, executed precisely under time pressure.
- **Structured incident methodology** — diagnose, contain, assess, plan, recover, with clear communication to IT leadership at every step.
- **Side-by-side partnership** — working directly with the college's IT team to preserve institutional knowledge and build internal capability.
- **Recovery-to-security continuity** — staying engaged through hardening so the restored environment was stronger than the one compromised.

Facing an active incident or want to test your readiness? Schedule a consultation or call (813) 518-5454.