



We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Data Breaches & Ransomware: Are You Prepared?

Randy Romes, CISSP, CRISC, CISA, MCP, PCI-QSA

Principal – Cybersecurity

612.397.3114

Randy.Romes@CLAconnect.com

October 2026



The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Today's Presenter



Randy Romes
Principal

Randy is a principal and cybersecurity consultant with CLA's National Digital group, specializing in cybersecurity risk assessment and governance. With 28+ years of hands-on experience leading penetration tests, vulnerability assessments, and social engineering engagements, he advises organizations across a diverse range of industries on strengthening digital defenses.

Randy's technical expertise spans advanced hacking and testing techniques — from network penetration and email phishing to bypassing firewalls and assessing the human element through social engineering. He also brings extensive project management experience in complex security initiatives and he leads CLA's PCI QSA credit card security practice.

He holds a Bachelor's Degree in Education from the University of Wisconsin and Masters Degree in Education from the University of St. Thomas. Randy maintains the following certifications: CISSP, CRISC, CISA, MCP, and PCI-QSA.

A sought-after national speaker, Randy has been an instructor at the Graduate School of Banking at the University of Colorado – Boulder, the CUNA Management School at UW-Madison and is a frequent speaker for FGFOA and a variety of national associations.





AGENDA

Threat Landscape

Initial Access

Privilege Escalation

Data Theft

Ransomware

Case Study

Controls & Response



LEARNING OBJECTIVES

- Identify common causes of cyber incidents that lead to data breaches or ransomware outbreaks
- Recognize leading practices to mitigate data breaches
- Review the incident response process and walk through key components of an incident response plan





THREAT LANDSCAPE



Cyber Trends

Cyber claims by event type

31%

BUSINESS EMAIL
COMPROMISE

27%

FUNDS
TRANSFER FRAUD

21%

RANSOMWARE



Cyber Trends – Email and Funds



58% of claims were Business Email Compromise (BEC) or Funds Transfer Fraud (FTF)

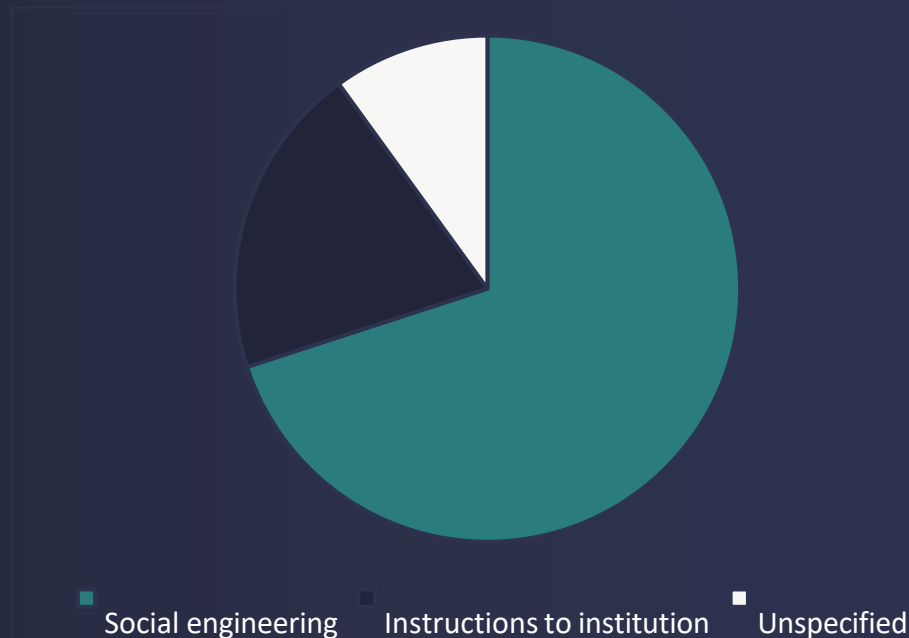


52% of FTF claims originated as BEC with an average loss of \$112k



71% of FTF claims resulted from social engineering

FTF claims by tactic



Cyber Trends – Ransomware



70% of ransomware claims involved both encryption and data exfiltration



47% surge in ransom demand to an average of over \$1m



86% of victims refused to pay

Top ransomware threat actors

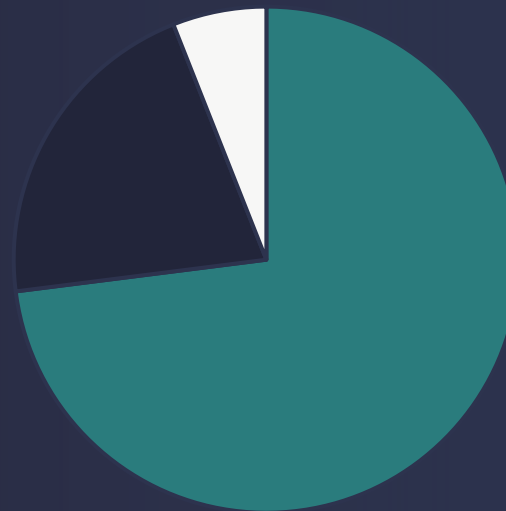
Threat actor	Average	Median	Minimum	Maximum
Akira	\$925k	\$670k	\$150k	\$4.9m
Qilin	\$1.2m	\$175k	\$15k	\$10m
RansomHub	\$2.3m	\$525k	\$70k	\$9m

Cyber Trends – AI & Breaches



\$6m – cost of “Model Inversion” where sensitive data is extracted from an AI model in 2026

Incident Involving AI



■ Did not involve AI ■ Involved AI ■ Unknown

The numbers your board should know

44%

of confirmed breaches involved ransomware (Verizon DBIR 2025)

\$6.29M

average cost of a financial-services breach (IBM Cost of a Data Breach 2026)

30%

of breaches involved a third party - double the prior year (Verizon DBIR 2025)

247

median days to identify and contain a breach globally (IBM Cost of a Data Breach 2026)



What changed: credential abuse (22%) and edge/VPN vulnerability exploitation (20%) now drive most intrusions, and ransomware crews increasingly skip encryption entirely in favor of pure data-theft extortion.



INITIAL ACCESS



Four common entry points



1. Phishing & social engineering

Credential-harvesting pages, malicious attachments, MFA-fatigue push bombing, and voice phishing of your help desk.



2. Stolen credentials / Remote Access / Weak MFA

Infostealer malware and password reuse hand attackers a valid login. Attackers use legitimate remote access services for institution. 22% of breaches start here — no exploit required.



3. Internet-facing vulnerabilities

Unpatched VPNs, firewalls, and file-transfer appliances. Edge-device exploitation grew nearly eight-fold.



4. Third parties & vendors

Core processors, MSPs, and fintech partners hold your data and your network access. 30% of breaches now involve a third party.



Phishing in 2026 doesn't look like phishing

What's changed

- ❖ Generative AI cut phishing email creation from hours to minutes - no more spelling-error tells
- ❖ MFA-bypass kits proxy the real login page and steal the session token
- ❖ Push-bombing wears the user down until they approve
- ❖ Attackers call the help desk impersonating an employee to reset MFA
- ❖ QR codes and cloud file-share links evade email filtering



Info Stealers

Imported At	Email/Username	Password	Source
2026-07-21	lce[REDACTED]s.com	layns[REDACTED]	Combolists
2026-07-21	nl[REDACTED]s.com	NAB[REDACTED]	Phishing Kits Credentials
2026-07-21	n[REDACTED]s.com	Nikki[REDACTED]	Phishing Kits Credentials
2026-07-21	n[REDACTED]s.com	4519[REDACTED]	Phishing Kits Credentials
2026-07-21	n[REDACTED]s.com	Salva[REDACTED]	Phishing Kits Credentials
2026-07-19	je[REDACTED]s.com	aGer[REDACTED]	URL Login Pass
2026-07-18	v[REDACTED]s.com	chan[REDACTED]	URL Login Pass
2026-07-18	ia[REDACTED]s.com	ajf6s[REDACTED]	URL Login Pass
2026-07-18	ik[REDACTED]s.com	(dory[REDACTED]	URL Login Pass
2026-07-15	l[REDACTED]S...	(TI@f[REDACTED]	Stealer Logs
2026-07-15	l[REDACTED]S...	AJf6[REDACTED]	Stealer Logs



Exploitation of Internet-Facing Devices

Check Point VPN Certificate Bypass (2026)

CVE-2026-85102 (CVSS: 9.8)

An improper certificate validation flaw in the VPN negotiation flow. It grants unauthenticated remote attackers the ability to execute arbitrary code (RCE) on Check Point Security Gateways.

Palo Alto GlobalProtect Flaws (2026)

CVE-2026-0257 (CVSS: 7.8)

An authentication bypass vulnerability affecting Palo Alto VPN portals and gateways. Attackers discovered they could bypass security restrictions to open unauthorized VPN connections directly into corporate networks.

Cisco Secure Firewall Zero-Days (2026)

CVE-2026-20131 (CVSS: 10.0)

An insecure deserialization flaw in the Cisco Secure Firewall Management Center (FMC). It allows unauthenticated threat actors to execute arbitrary Java code as root.

SonicWall VPN Authentication Bypass (2024)

CVE-2024-40766 (CVSS: 9.3)

An improper access control flaw impacting SonicOS firewalls. Allowed attackers to completely bypass Multi-Factor Authentication (MFA), hijacking active SSL VPN sessions to gain the exact permissions of the internal network.



Third-Party Data Breaches - MOVEit



What

SQL injection flaw in MOVEit web application



When

May – November 2023



How

Public webpage was vulnerable to SQL injection, allowing attackers to upload web shell

Impact

- ❖ Hackers uploaded web shell to MOVEit servers and exfiltrated data
- ❖ Hacker groups demanded payment, and disclosed sensitive data for organizations that did not pay
- ❖ Impacted over 2,550 organizations and 66 million individuals





PRIVILEGE ESCALATION



Why escalation succeeds in institutions

Default Vendor Passwords

FinTech Applications and
Databases coming with known,
default passwords

Insecure Network Protocols

Windows systems have default,
insecure protocols enabled by
default

Weak Account Passwords

User accounts and service
accounts that can have their
password cracked

Flat internal networks

Nothing separates the teller
workstation from the core.

Insecure File Shares

File shares that provide access to
sensitive PII or configuration files
with passwords

Lack of Server Hardening

Critical servers (Domain Controllers /
Certificate Authorities) with default,
insecure configurations





DATA THEFT



© 2026 CliftonLarsonAllen LLP



How your data actually leaves



Step 1 — Find it

Attackers search file shares, SharePoint, and mailboxes for keywords: SSN, loan, wire, account, payroll, board



Step 2 — Stage it

Data is compressed into archives, often split into pieces and hidden in ordinary-looking folders on a server you already trust



Step 3 — Move it

Uploaded to legitimate cloud services (AWS, OneDrive, Google Drive) or over encrypted tunnels - blending into normal traffic

Why this matters more than encryption

- ❖ A clean restore from backup does not undo a data breach - the consumer and regulatory impact remain
- ❖ For financial institutions, this triggers requirements to notify regulators
- ❖ Increased opportunity for fraud when account-holder data stolen





RANSOMWARE



© 2026 CliftonLarsonAllen LLP



The deployment playbook

1

Neutralize recovery

Backups deleted or encrypted, shadow copies removed, backup servers targeted first.

2

Disable defenses

EDR and antivirus stopped or uninstalled using stolen admin credentials.

3

Push the payload

Distributed by Group Policy, remote management tooling, or scripted deployment - organization-wide in minutes.

4

Detonate off-hours

Friday night, holiday weekend, or 2 a.m. - when your team is least likely to notice.

5

Double extortion

Ransom for the decryption key plus a second demand to not publish the stolen data on a leak site.



What it costs when it happens to you

21+

average days of material
operational disruption

\$1.5M

typical recovery spend,
separate from any ransom

69%

of victims refuse to pay
the ransom demand

Costs your cyber policy may not cover

- ❖ Consumer attrition after notification
- ❖ Regulatory examination findings
- ❖ Manual processing and overtime during outage
- ❖ Reputational damage in a relationship business





CASE STUDY



© 2026 CliftonLarsonAllen LLP



Executive Summary

A financial institution suffered a ransomware attack that disabled their operations.

7

ATTACK PHASES

1

EXPOSED SERVICE

< 24h

TIME TO FULL
COMPROMISE

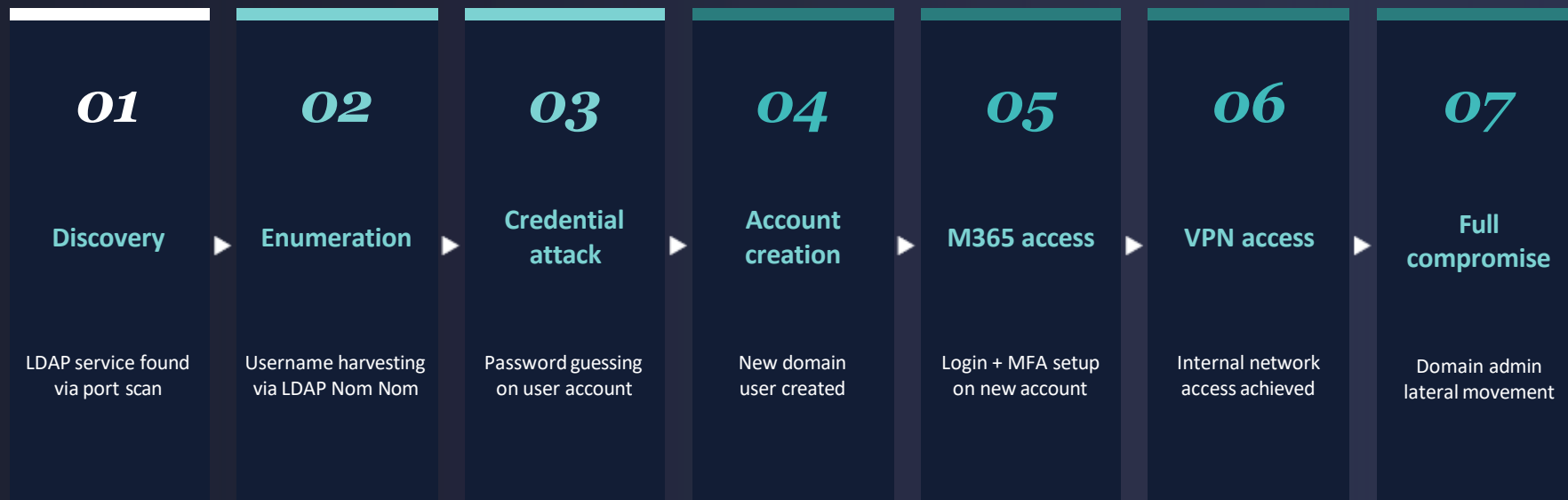
100%

NETWORK CONTROL
ACHIEVED



Attack Chain Overview

Kill chain progression from external reconnaissance to full domain control

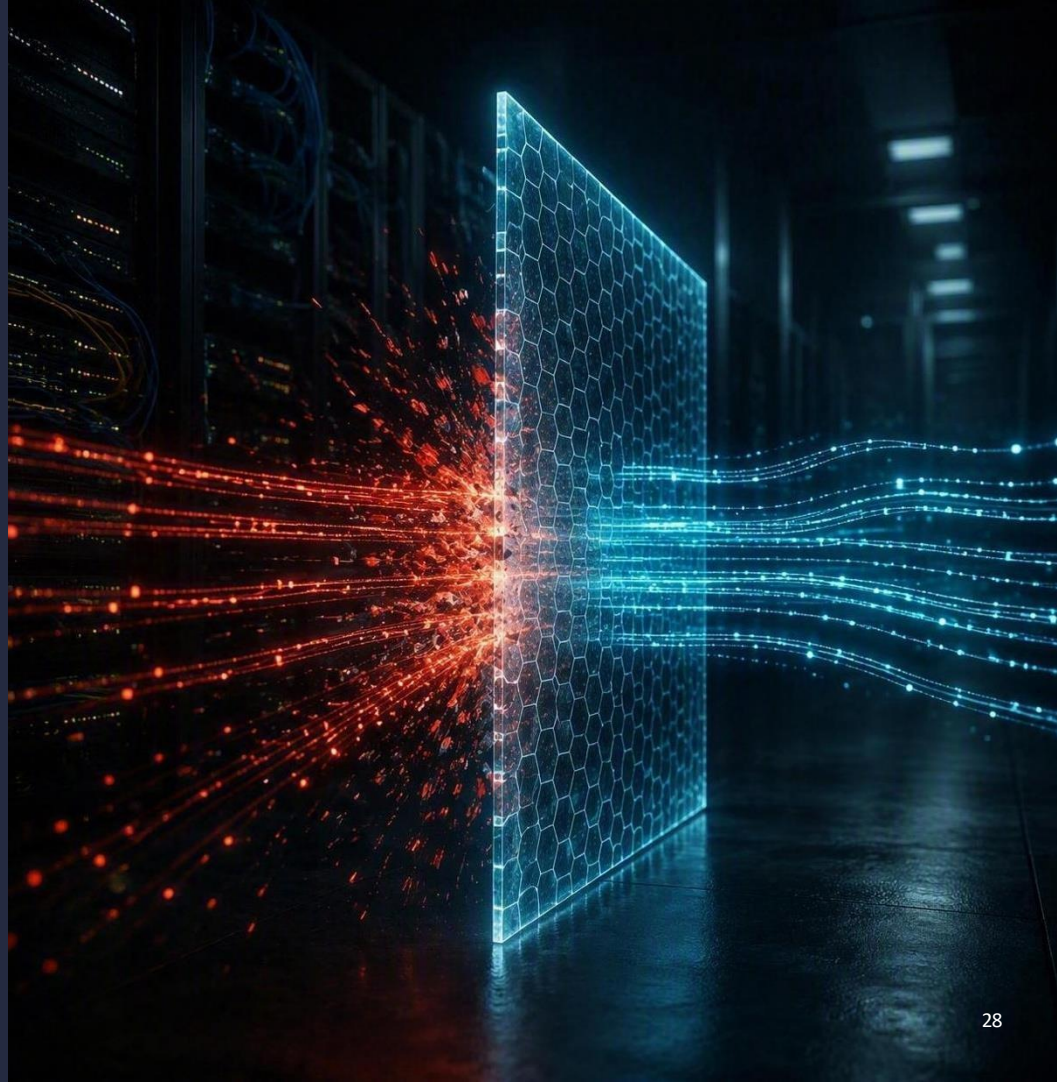


PHASE 01

External Service Discovery

Goal

Identify what ports and services
are exposed to the Internet



Issue: LDAP Service Exposed to Internet

The organization had LDAPS (Lightweight Directory Access Protocol over SSL/TLS) exposed directly to the internet on port 636. This service, which is normally used for internal directory lookups against Active Directory, was discoverable through basic port scanning.

TECHNICAL DETAILS

Protocol: LDAPS (port TCP/636)

Exposure: No firewall rules restricting inbound access

Discovery Method: Internet-wide port scanning (Shodan, Masscan, Nmap)

Risk: LDAP exposes directory structure, usernames, group memberships, and supports authentication

```
L-$ sudo nmap -Pn -n -p 636 -v -sV -A 5
Starting Nmap 7.98 ( https://nmap.org ) at 2026-05-01 13:38 +0000
Scanning 5 [1 port]
Discovered open port 636/tcp on 5
Initiating Service scan at 13:38
Scanning 1 service on 5
Nmap scan report for 5
Host is up (0.058s latency).

PORT      STATE SERVICE VERSION
636/tcp   open  ssl/ldap Microsoft Windows Active Directory LDAP (Domain: , Site: Default-First-Site-Name)
|_ssl-date: 2026-05-01T13:38:42+00:00; 0s from scanner time.
|_ssl-cert: Subject: commonName=
| Subject Alternative Name: DNS: , DNS: autodiscover.
| , DNS: , DNS:
|_ Issuer: commonName=Sectigo Public Server Authentication CA DV R36
/organizationName=
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2025-11-23T00:00:00
| Not valid after: 2026-12-23T23:59:59
```



PHASE 02

Username Enumeration

Goal

Identify valid usernames for
the organization



Issue: LDAP Username Enumeration

LDAP Nom Nom Attack

WHAT HAPPENED

The attacker used **LDAP Nom Nom**, a purpose-built tool for high-speed Active Directory username enumeration.

This tool exploits LDAP responses to determine whether a username is valid without triggering standard Windows authentication audit logs.

WHY IT MATTERS

Evades detection

- Does not generate Windows Security Event logs (4625, 4771)

High-speed enumeration

- Can test thousands of usernames per minute

Reveals org structure

- Confirms naming conventions (first.last, etc.)

RESULT: Attacker obtained a list of valid domain usernames including service accounts and administrators.



Issue: LDAP Username Enumeration

LDAP Nom Nom Attack

```
09/26 08:54:53 > ~/tools/ldapnomnom/ldapnomnom -dnsdomain [REDACTED].local -input /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
2025/09/26 08:54:53 LDAP Nom Nom - anonymously bruteforce your way to Active Directory usernames
2025/09/26 08:54:54 Auto-detected DNS domain as [REDACTED].local
2025/09/26 08:54:54 Detected [SERVER.[REDACTED].local server.[REDACTED].local [REDACTED].local] Domain Controllers for [REDACTED].local
2025/09/26 08:54:54 Using SERVER.[REDACTED].local, server.[REDACTED].local, [REDACTED].local as target servers
2025/09/26 08:54:54 Using these servers: SERVER.[REDACTED].local, server.[REDACTED].local, [REDACTED].local
Progress 99% | [REDACTED] | (42572 it/s) [3m17s:0s]
```



```
09/26 08:58:36 > cat ldapnomnom.txt
info
kevin
nicholas
office
jamie
manager
chief
Kevin
INFO
Jamie
```

**List of 10 million
common usernames**

**Usernames
validated per
second**

Total time

**Enumerated valid
usernames**

Password Guessing

Goal

Identify valid passwords for the usernames discovered



Issue: Weak Password

Using the enumerated usernames, the attacker performed targeted password guessing against the LDAP service. A help desk account was found to have a weak, easily guessable password.

ATTACK METHOD

- Targeted password guessing against known usernames
- Common passwords, seasonal patterns, org-specific terms
- LDAP bind requests used to validate credentials
- Low-and-slow approach to avoid lockouts

CRITICAL FINDING

Helpdesk User

Account compromised with a weak password

IMPACT: Attacker now possessed valid Helpdesk User credentials.



+ symbol
represents
successful login

Rogue Account Creation

With helpdesk privileges, the attacker created a new user account in Active Directory. This provided a persistent, less suspicious identity for continued access.

TECHNIQUE

- Used compromised helpdesk credentials
- Created new user via LDAP modify operations
- Added to VPN groups

PERSISTENCE

- Separate identity from compromised account
- Less likely to trigger alerts
- Survives password resets of original account
- Can be used across multiple services

STEALTH

- Account named to blend with naming conventions
- Added to existing groups, not new ones
- No email notifications generated
- Minimal audit trail if not monitored

PHASE 04

Rogue Account Creation

```
L$ ldap_shell [REDACTED].local/ch[REDACTED] : [REDACTED] ' -dc-ip [REDACTED] [REDACTED] -use-ldaps
[INFO] Starting interactive shell
# add user cl[REDACTED]
[INFO] User cl[REDACTED] added successfully to CN=cl[REDACTED],CN=Users,DC=[REDACTED],DC=local! Password: "[REDACTED]"
```

Adding new user to domain



M365 Access and MFA Enrollment

The attacker logged into Microsoft 365 with the newly created account and enrolled their own MFA device, establishing legitimate-appearing access to applications.

1

LOGIN TO M365

Used new account credentials synced from on-prem AD to Entra

2

MFA REGISTRATION

Enrolled attacker-controlled device as MFA factor (first-time setup)

3

ACCESS GRANTED

Access to M365 cloud resources

4

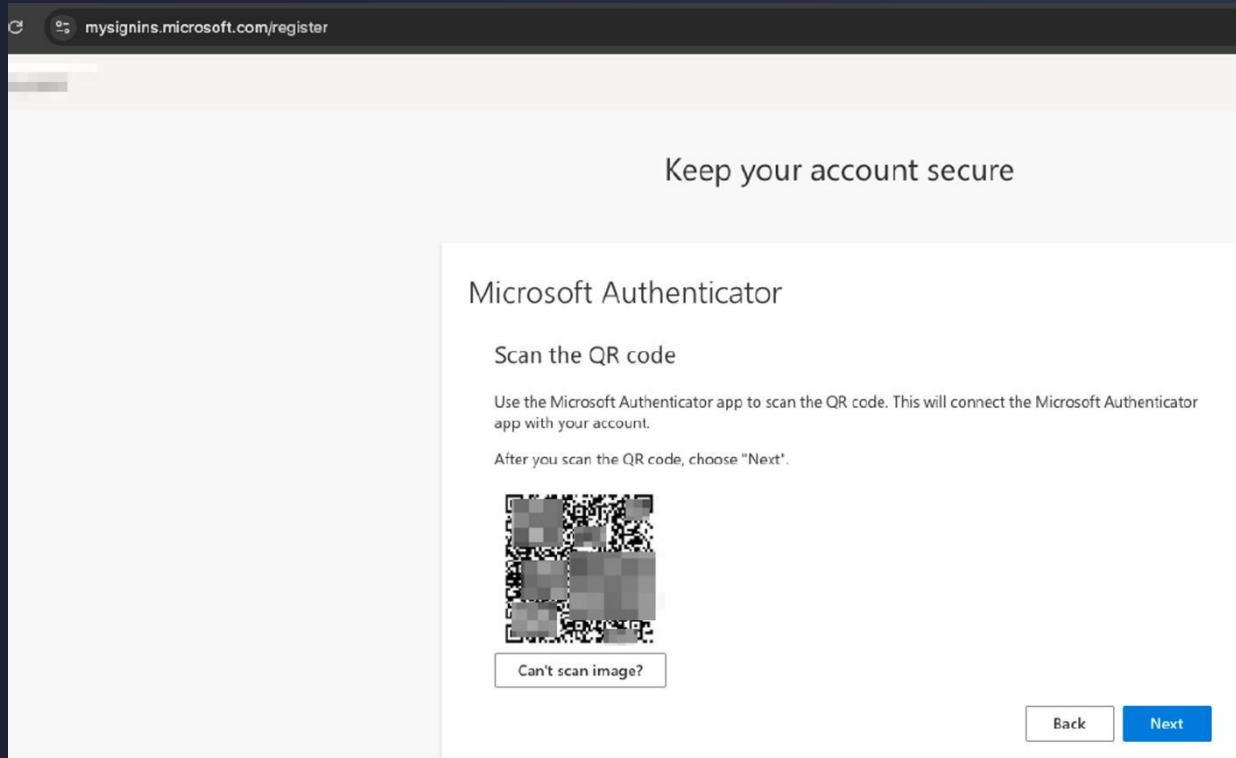
LEGITIMIZED

Account now appears as a normal user with proper MFA compliance

KEY ISSUE: No Conditional Access policies restricted MFA enrollment to trusted networks or required admin approval for new accounts.



Issue: No M365 Controls Restricting MFA Registration



VPN Access to Internal Network

With a fully enrolled M365 account and valid domain credentials, the attacker connected to the organization's VPN, gaining direct access to the internal network.

VPN ACCESS CHAIN

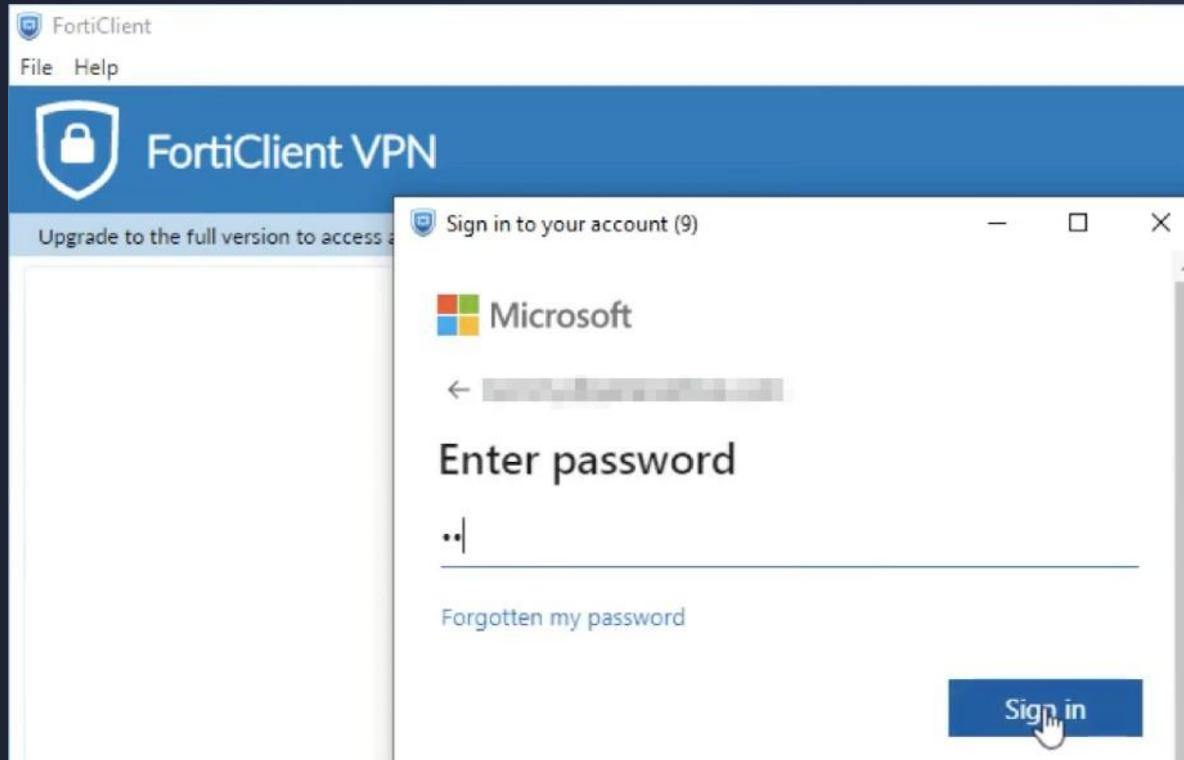
- Valid AD credentials from new account
- MFA verification via attacker-enrolled device
- VPN authenticated against Active Directory
- No device certificate or compliance check required
- **Full internal network access granted**

NETWORK ACCESS

- Domain controllers
- File servers
- Database servers
- Core systems
- Data stores
- Internal applications
- Backup infrastructure



Issue: No VPN Monitoring



PHASE 07

Full Network Compromise

Once on the internal network via VPN, the attacker leveraged the compromised helpdesk account to gain complete control of the entire Active Directory environment.

LATERAL MOVEMENT AND PRIVILEGE ESCALATION

- Identified default vendor passwords
- Exploited misconfigured certificate (ADCS)
- Accessed administrator Kerberos Ticket
- Identified backup systems and schedules



Issue: Default Vendor Credentials

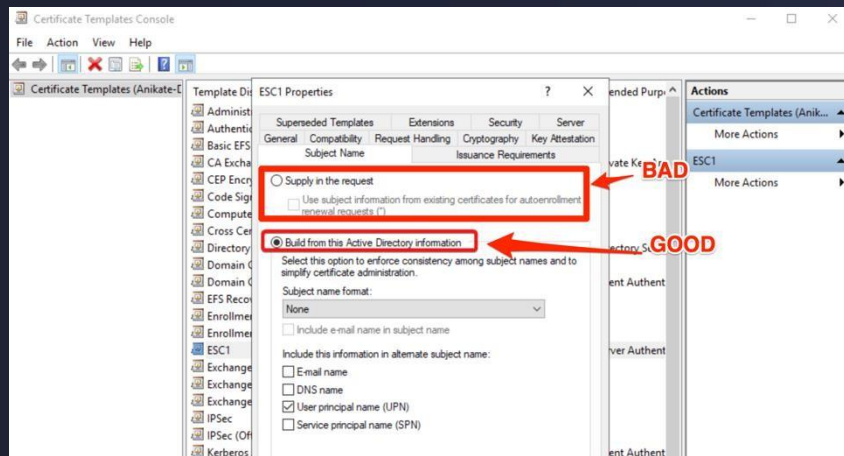
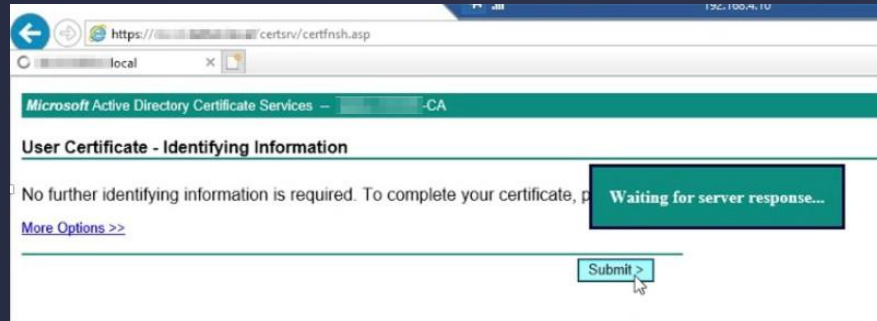
Default credentials were discovered on an application database. This allowed the attacker to obtain full control of the database server.

```
[T08:12:23-0800][root@RIVA83:~]# grep '[+]' bruteforcing/brute-msf-mssql-login.txt | grep -v 'NTLM::SendSPN'
[+] [-22:40:17] 172.16.1.1433 - 172.16.1.1433 - Login Successful: WORKSTATION\TemenosSQLUser:2
[+] [-22:40:17] 10.2.1.1433 - 10.2.1.1433 - Login Successful: WORKSTATION\Syn:$
[+] [-22:40:17] 10.2.1.1433 - 10.2.1.1433 - Login Successful: WORKSTATION\Syn:$
```

PHASE 07

Issue: Misconfigured ADCS Server

Active Directory Certificate Services (ADCS) server had misconfigured certificate templates. It was possible to use the SQL database computer account to request a certificate for a domain administrator.



Impact Assessment

OPERATIONAL

CRITICAL

- Complete AD domain compromise
- All systems accessible to attacker
- Backup infrastructure exposed
- Critical systems inaccessible

DATA

CRITICAL

- PII exfiltrated
- Financial data accessible
- Reporting obligations
- Notification required

FINANCIAL

HIGH

- Incident response costs
- Potential regulatory fines
- Notification expenses
- Cyber insurance implications

REPUTATIONAL

HIGH

- Consumer trust impact
- Board reporting
- Competitive disadvantage





CONTROLS & RESPONSE



Ten controls that break the attack chain



Phishing-resistant MFA

Everywhere: email, VPN, remote access, admin, cloud



Aggressive edge patching

VPN, firewall, and file transfer within days, not months



Privileged access management

No daily-driver admin accounts; check-out, rotate, log



Endpoint detection & response

24/7 monitored EDR — tooling without eyes is not a control



Immutable, offline backups

Tested restores; backups outside the production domain



Network segmentation

Separate core, cardholder, and backup environments



Email & web filtering

Block unknown websites, newly registered domains, and lookalikes



Least privilege & access reviews

Regular reviews; remove stale accounts fast



Centralized logging & alerting

Alert on new admins, EDR tampering, and bulk data access



Vendor risk management

Contractual notification terms, SOC 2 review, scoped access





REMEDIATION

Social Engineering

What to do about it

- ❖ Move to phishing-resistant MFA (FIDO2 / passkeys) for admins and remote access
- ❖ Require callback verification and manager approval for help-desk MFA resets
- ❖ Simulate testing and measure reporting rate, not just click rate
- ❖ Block newly registered domains and auto-quarantine lookalikes
- ❖ Disable legacy email protocols that bypass MFA



REMEDIATION

Network and Access Controls



Block unnecessary services (E.G., External LDAP)

Immediately restrict port TCP 636 at the perimeter firewall. LDAP should never be internet-facing. Use VPN or Zero Trust Network Access for remote directory queries.



Network segmentation

Implement network segmentation to isolate critical systems (DCs, databases, backups). Apply micro-segmentation between tiers.



Remote access hardening

Require device certificates, enforce compliance checks, implement Zero Trust architecture for remote access.



Incident Response Lifecycle



Preparation

Plan, roles, tooling, training, retainers, and contact lists maintained offline.



Detection & analysis

Triage the alert, confirm scope, classify severity, and start the timeline log.



Containment

Isolate hosts, disable accounts, block C2, preserve evidence before wiping.



Eradication & recovery

Remove persistence, rebuild clean, restore in a validated, staged order.



Post-incident review

Root cause, lessons learned, control gaps closed, plan updated.

Preparation is the only phase you control on your own schedule - and it determines how the other four go.



Key components of a usable IR plan

01

Scope & severity definitions

What counts as an incident and what triggers escalation

02

Roles & the incident commander

One named decision-maker, with a designated backup

03

Contact tree

Staff, executives, counsel, insurer, forensics, regulators

04

Detection & reporting paths

How staff report; how alerts reach the responder on call

05

Containment authority

Who may disconnect systems — pre-authorized, in writing

06

Evidence & documentation

Timeline log, chain of custody, forensic imaging standards

07

Communications plan

Internal, consumers, media, and board messaging

08

Legal & regulatory obligations

Regulatory notification, state laws, contractual notice terms

09

Recovery & restoration order

Which systems come back first, and who validates them

10

Testing & maintenance

Annual tabletop, post-incident updates, version control



Tabletop scenario: “Friday, 11:40 p.m.”

The scenario

Your core server is unreachable. An employee reports a ransom note on a shared drive. Your backup console shows all jobs failed at 11:02 p.m. A leak site posts your institution's name with a 5 GB sample of loan files.

Inject: at 6 a.m. a local reporter calls the branch manager for comment.



Run this in 60 minutes with executives in the room.

Questions to answer

- ❖ Who declares the incident, and who is called first?
- ❖ Who has authority to take the network offline?
- ❖ Where is the plan if the file server is encrypted?
- ❖ How do you operate branches without core access?
- ❖ When does the notification clock start?
- ❖ Who speaks to the reporter — and who does not?
- ❖ What do you tell consumers Monday morning?



OPEN DISCUSSION



Thank you!

Randy Romes, CISSP, CRISC, CISA, MCP, PCI-QSA

Principal, Cybersecurity

Randy.Romes@claconnect.com

612-397-3114



CLAconnect.com



CPAs | CONSULTANTS | WEALTH ADVISORS

© 2026 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See [CLAGlobal.com/disclaimer](https://claglobal.com/disclaimer).

Securities and investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor, member FINRA/SIPC.