

Most cyberattacks don't start with advanced hacking. They start with a series of small gaps that attackers string together. A phishing email leads to stolen credentials, a lack of multi-factor authentication allows access, and an unpatched system provides the opportunity to move further into the environment. Individually, these issues may seem manageable. Together, they can result in operational disruption, downtime, and significant business impact.

Phishing Email → Stolen Password → MFA Not Enabled → Unpatched System → Business Impact

Break any link in the chain, and you can stop the attack before it impacts your business.

1. Someone Trusts the Wrong Email

A purchasing manager receives a message that appears to be legitimate from a supplier. The logo looks right. The email address looks close enough. The request feels routine. Unaware, they click a link and enter their credentials.

What attackers are looking for:

- Supplier relationships
- Invoice approvals
- Shipping updates
- Purchase orders
- ERP login credentials

2. A Stolen Password Opens the Door

Once credentials are stolen, attackers attempt to sign in. If passwords are reused, shared, weak, or tied to multiple systems, one stolen credential can provide access to far more than expected.

Common Risks:

- Shared shop floor logins
- Generic operator accounts
- Vendor accounts that are never reviewed
- Former employee accounts that remain active

3. MFA Could Have Stopped the Attack

The attacker successfully logs in because Multi-Factor Authentication (MFA) isn't enabled. At this point, they look like a legitimate user.

No alarms.

No hacking tools

Just valid credentials.

Where MFA Matters Most:

- Email accounts
- ERP systems
- Remote access solutions
- VPN connections
- Administrative accounts
- Supplier portals

4. An Unpatched System Creates an Opening

Now inside the environment, the attacker looks for weaknesses.

One outdated server.

One unsupported application.

One missed security update.

That's often all it takes.

Common Manufacturing Targets:

- Legacy applications
- ERP integrations
- Vendor software
- Shared workstations
- Internet-facing systems
- Remote monitoring tools

**Reality Check:
Which of These
Exist Today?**

- | | |
|--|--|
| ☐ Shared passwords | ☐ Former employee accounts still active |
| ☐ VPN accounts without MFA | ☐ Unpatched systems waiting for downtime |
| ☐ Vendors with remote access | ☐ Employees reusing work passwords elsewhere |
| ☐ Users approving invoices from email alone | ☐ Supplier requests that are never independently verified |