COMMON CYBER ATTACKS FACING DISTRIBUTORS

American Supply Association – Cybersecurity Task Group
Foundational Awareness Resource – Version 2 | January 19, 2026

Cyber-attacks often sound abstract until they show up inside normal, everyday business activity. This document explains the most common cyber-attacks facing distributors in plain language, using familiar scenarios.

It is intended to build baseline awareness, not create fear, assign blame, or prescribe specific tools. These examples help explain why cybersecurity controls exist and how real-world attacks typically unfold.

This resource is designed to be used **in conjunction with ASA's Cybersecurity Checklist**. The attack scenarios below describe *what can happen*. The checklist outlines *the controls and practices organizations use to reduce risk across increasing maturity levels*.

PHISHING & CREDENTIAL THEFT

What it is
Phishing occurs when an attacker tricks someone into clicking a link, opening a file, or entering login credentials into a fake site that looks legitimate. The goal is usually to steal usernames and passwords so the attacker can access systems as a trusted user.

How it usually shows up
This often looks like a routine email asking you to review an invoice, confirm a shipment, reset a password, or open a shared document. The message may appear to come from a vendor, customer, or familiar service like Microsoft or a shipping carrier.

Why distributors are targeted
Distributors rely heavily on email, shared files, and many different systems across sales, purchasing, accounting, and operations.

What this puts at risk
Stolen credentials can give attackers access to email, ERP systems, shared files, and cloud tools.

Related Checklist Controls

- Multi-Factor Authentication (MFA)
- Basic Phishing Awareness Training
- Strong password standards
- Centralized logging
- Monthly phishing simulations

BUSINESS EMAIL COMPROMISE (BEC)

What it is
Business Email Compromise occurs when an attacker gains access to a real email account or convincingly impersonates a trusted contact to manipulate financial or operational transactions.

How it usually shows up
Emails requesting wiring changes, invoice payment updates, or urgent approvals appearing to come from executives, vendors, or colleagues.

Why distributors are targeted
High volumes of invoices, payments, and routine trust-based workflows.

What this puts at risk
Direct financial loss, delayed shipments, and strained vendor relationships.

Related Checklist Controls

- Multi-Factor Authentication (MFA)
- Vendor risk assessment process
- Privileged access management (PAM)
- Centralized logging
- Role-based recovery playbooks
- **Tabletop exercise**

RANSOMWARE

What it is
Ransomware encrypts systems or data and demands payment to restore access, often after data is stolen.

How it usually shows up
Introduced through phishing, compromised credentials, or unpatched systems before rapidly spreading.

Why distributors are targeted
Operational dependence on system availability for order processing, inventory, and logistics.

What this puts at risk
Extended downtime, revenue loss, and exposure of sensitive data.

Related Checklist Controls

- Regular patching / automated patching program
- Daily backups with periodic test restores
- Immutable/offline backups
- Documented incident response plan
- Managed Detection & Response (MDR)
- **Tabletop exercise**

MALWARE VIA ATTACHMENTS OR DOWNLOADS

What it is
Malware installs itself to steal data, monitor activity, or maintain attacker access.

How it usually shows up
Email attachments or downloads disguised as invoices, spreadsheets, or shipping documents.

Why distributors are targeted
High volume of file exchanges with vendors, customers, and internal teams.

What this puts at risk
Credential theft, monitoring, and persistent system access.

Related Checklist Controls

- Antivirus / Endpoint Detection & Response (EDR)
- Web filtering enabled
- Centralized logging
- Basic SIEM or log-monitoring capability
- **Inventory of devices and applications**

DATA LEAKAGE VIA CLOUD, FILE SHARING, OR AI TOOLS

What it is
Unintentional exposure of sensitive information outside approved systems.

How it usually shows up
Misconfigured file sharing, data uploaded to cloud or AI tools, or sensitive data sent via collaboration platforms.

Why distributors are targeted
Distributed data across pricing, customer, contract, and operational systems.

What this puts at risk
Exposure of sensitive information and erosion of customer trust.

Related Checklist Controls

- Data Loss Prevention (DLP)
- Inventory of devices and applications
- Vendor risk assessment process
- Zero Trust architecture components

COMPROMISED VENDORS OR THIRD PARTIES

What it is
Attackers exploit trusted vendors or partners to gain indirect access.

How it usually shows up
Malicious links from vendor accounts, compromised updates, or abused shared credentials.

Why distributors are targeted
Reliance on many external partners for software, logistics, and services.

What this puts at risk
Malware introduction, data exposure, and operational disruption.

RELATED CHECKLIST CONTROLS

- Vendor risk assessment process
- Privileged access management (PAM)
- Network segmentation
- Centralized logging
- Inventory of devices and applications

STOLEN, REUSED, OR WEAK CREDENTIALS

What it is
Use of weak, reused, or previously exposed passwords.

How it usually shows up
Credentials reused across systems, shared internally, or obtained via phishing.

Why distributors are targeted
Multiple systems and legacy access models.

What this puts at risk
Unauthorized access, impersonation, and attack escalation.

Related Checklist Controls

- Strong password standards
- Multi-Factor Authentication (MFA)
- Privileged access management (PAM)
- Centralized logging

COMPANION USE NOTE

This document is intended to raise awareness of common cyber threats facing distributors. Organizations should use the **ASA Cybersecurity Checklist** to assess which controls are in place today and identify the next practical steps for reducing exposure to the risks described above.