AUTOMOTIVE AFTERMARKET SERVICES

NEWS ALERT

July 2023
Volume 5 | Issue 3

Risk Management

Preventing Warehouse and Factory Fires

ONE OF the biggest risks to warehouses and factories is fires, which can spread rapidly in these environments.

Facilities that are most at risk are those that have high ceilings, large footprints and hold large quantities of inventory that is stored close together.

If you don't have a fire prevention system in place, your inventory is at risk, as well as machinery and the building itself.

If you operate such a facility, you need to make sure that you reduce the risk of fires, and that you keep your inventory clear of any potential ignition sources.

To start, you need to understand what kind of ignition sources you have in your facility and how to identify hazards. Next, put together a fire protection plan.

Your plan will depend on the materials and inventory that you are storing and using.

For example, materials in corrugated cartons are much less combustible than plastic packaging. And inventory such as paint, oil and sawdust is extremely flammable.

Shelving

One of the first orders of business is to evaluate your current shelving design.

One factor is the height of your storage. The higher you stack inventory, the greater the fire suppression challenge. Sprinkler systems that run along the ceiling have to reach not only the top layers of your inventory, but also the bottom layers.

One solution is to install in-rack sprinklers.

Another issue to consider is solid versus open shelving.

Solid shelving increases the fire risk because it creates an enclosed area where the fire can burn more easily.

Fires to products on open shelving are easier to douse and they don't spread as easily.

Also, the warehouse should be neat and items properly stored. Failing to arrange storage can increase your risk because:

- Crowded aisles may block fire exits and make it harder for people to escape, and
- Fires spread more easily in cramped warehouses.

Dust danger

When accumulated dust particles are suspended in the air and contained in a confined space, all it takes is one small ignition source – like static electricity or metal-on-metal friction – to set off a chain reaction and a burst of fire.

When that happens it creates a rise in temperature and a rise in pressure.

That pressure will push outwards and if your building is not designed to contain that explosion and vent it safely, the result can be significant damage.

On top of that, the initial explosion may dislodge additional dust on horizontal surfaces, which will add to the fire, putting at risk your entire facility. ❖

DUST FIRE PREVENTION

Fires can be prevented via proper housekeeping and regular maintenance and upkeep of equipment, and the installation of vacuum-powered dust collectors on the outside of the warehouse.

STORAGE TIPS

- Keep electrical switchgear and heating equipment clear of storage.
- Never let goods sit within 18 inches of lighting.
- Allow enough clearance between sprinkler heads and stored goods to make sure that your sprinkler system can effectively douse the area.
- Segregate hazardous and non-hazardous materials.

AUTOMOTIVE AFTERMARKET SERVICES

Automotive Aftermarket Services

7777 Greenback Ln. #212
Citrus Heights, CA 95610

Phone: (888) 383-2274
Fax: (888) 383-2211
www.aasins.net

If you have questions about our services, please e-mail us at: info@aasins.net

Essentials of an OSHA-Approved First Aid Kit

DO YOU know what OSHA requires you to keep in the first aid kits at your place of business? The relevant Cal/OSHA Standard requires that "adequate first aid supplies shall be readily available."

You should put a staff member in charge of inspecting first aid kits on a regular basis to make sure they have all the items required under the ANSI standard, and that items have not expired.

Over-the-counter medicines are fine for inclusion in first aid kits, but you should avoid medications that could cause drowsiness – if a worker takes one of these and has an accident soon afterwards, the implication could be that you as the employer may be culpable.

If you do include over-the-counter medications, all meds should be wrapped in tamper-evident packaging as individual doses. You should not have any bottles. If you reasonably expect that workers treating other injured employees could come into contact with blood or other pathogens, you should also consider including personal protective equipment, such as latex gloves, masks, gowns and face shields. ❖

CAL/OSHA'S FIRST AID KIT REQUIREMENTS

A Class A kit must contain at least:

- 16 Adhesive Bandages: 1" x 3" (2.5 x 7.5 cm)
- 1 Adhesive Tape: 2.5 yd (2.3 m)
- 10 Antibiotic Applications: 1/7 oz (0.5 g)
- 10 Antiseptics: 1/7 oz (0.5 a)
- 1 Burn Dressing (gel soaked): 4" × 4" (10 x 10 cm)
- 10 Burn Treatments: 1/32 oz (0.9 g)
- 1 Cold Pack: 4" x 5" (10 x 12.5 cm)*
- 1 CPR Breathing Barrier
- 2 Eye Coverings with means of attachment: 2.9" sq (19 sq cm)
- 1 Eye/Skin Wash: 1 f1 oz total (29.6 ml)
- 1 First Aid Guide
- 1 Foil Blanket: 52" × 84" (132 x 213 cm)
- 10 Hand Sanitizers: 1/32 oz (0.9 g)
- 4 Medical Exam Gloves
- 1 Roller Bandage: 2" x 4 yd (5 cm x 3.66 m)
- 1 Scissors**
- 2 Sterile Pads: 3" × 3" (7.5 x 7.5 cm)
- 2 Trauma Pads: 5" x 9" (12.7 x 22.9 cm)
- 1 Triangular Bandage: 40" x 40 × 56" (101 x 101 x 142 cm)

Color-coding requirements

First aid kits should be color-coded in the following manner:

- Blue: Antiseptics
- Yellow: Bandages
- Red: Burn treatments
- Orange: Personal protective equipment
- Green: Miscellaneous

Tips on Tackling Employee Dishonesty

EMPLOYEE DISHONESTY that leads to some type of theft or embezzlement, be that of company funds, assets or vital company data, can be a serious threat to your bottom line.

There are ways you can mitigate the risk by sticking to proven hiring principles, and putting in place procedures and safeguards to reduce the likelihood of employee theft. Your strategy should also include securing employee dishonesty insurance coverage, just in case.

Small and mid-sized businesses suffer disproportionate losses from employee dishonesty because they typically have limited resources to devote to detecting fraud or theft, according to the Association of Certified Fraud Examiners . It recommends the following:

Hire wisely – Conduct pre-employment background checks of job applicants that include the following:

- Criminal history for crimes involving violence, theft and fraud.
- Civil history collections, restraining orders or fraud lawsuits.
- Driver's license check for numerous or serious violations.
- Education verification of any degrees the applicant claims.
- Calling former employers to verify the positions the applicant held, length of employment, and reasons for leaving.

Checks and balances – No employee should be responsible for both recording and processing transactions.

Control access – Restrict access to physical and financial assets and information to authorized employees only.

Authorization controls – Develop policies to determine how financial transactions are initiated, authorized, recorded and reviewed.

Keep staff posted – Educate employees on your policies a related to fraud, the internal controls you have set in place, as well as your company's ethics policy and how you will mete out discipline for violations. Have all of your employees sign a form verifying that they have read and understand your policy.

Hold an annual training session on fraud and theft prevention.

Anonymous reporting – To ensure that your staff can feel protected if they become aware of employee theft or other dishonest behavior, provide for a reporting system for employees, vendors and customers to anonymously report any violations of policies and procedures.

Take reports seriously and investigate thoroughly.

Audits – You should already be conducting regular audits. But you should also conduct unannounced audits, that give employees no time to cover their tracks if they've been stealing.

Probe reports – Investigate every incident and report, no matter how small. A thorough and prompt investigation of policy and procedure violations, allegations of fraud, or warning signs of fraud will give you the facts you need to make informed decisions and reduce potential losses.

Analyze bank statements – Review bank statements prior to passing them to the bookkeeper.

Expense procedures – Have a strict expense report documentation policy and audit reports prior to payment.

Check inventories – Conduct physical inventories often and reconcile inventory to sales.

Check rules – Limit the number of check signatories to a few trusted staff and keep blank checks in a secure location.

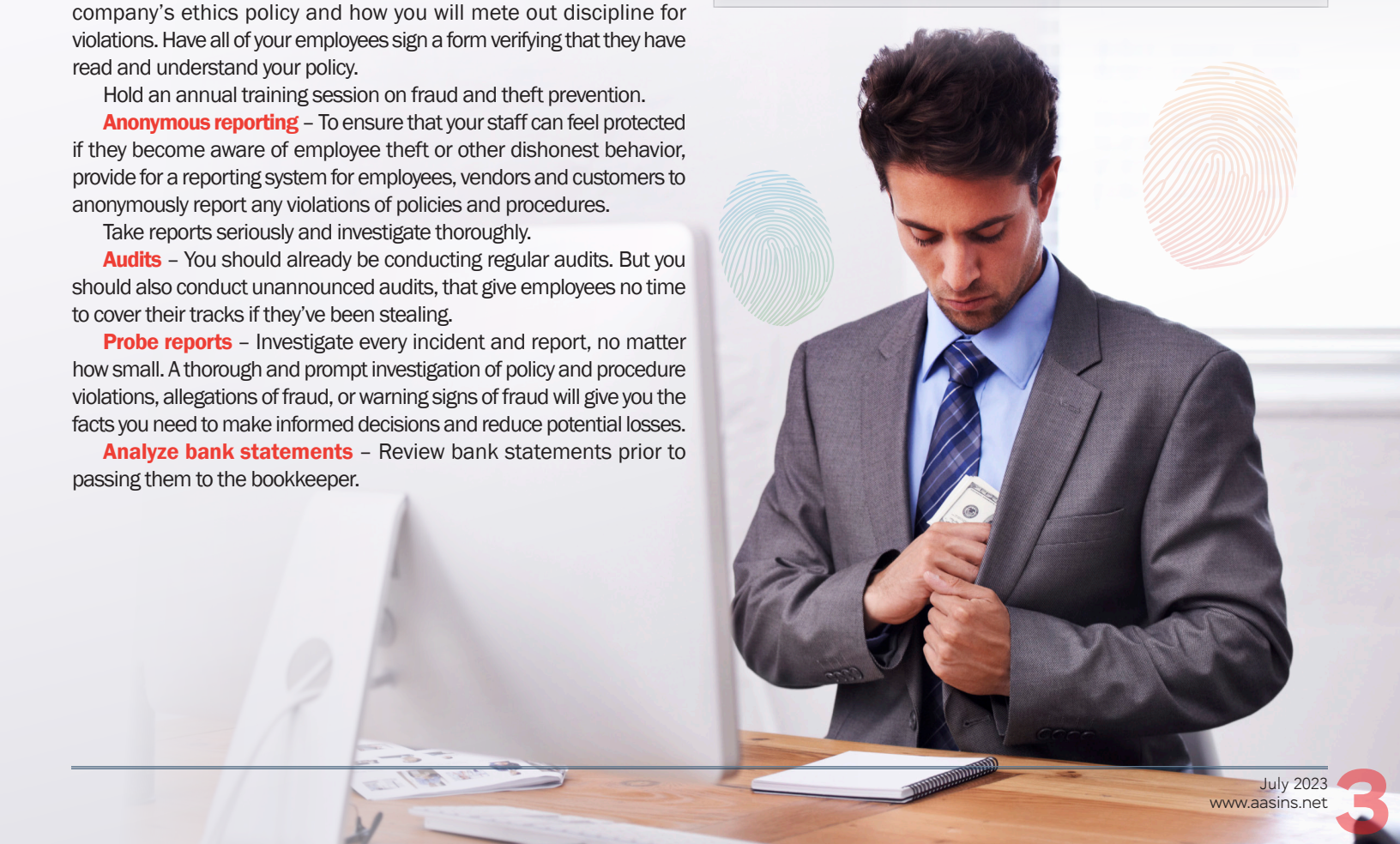
Lock the cash – Allow a limited number of employees the ability to disburse petty cash. Require a receipt for all petty cash disbursements.

Anti-theft devices – Buy security and fraud-resistant products such as special cash drawers that limit the ability to pilfer, tamper-resistant bank deposit bags, and clear-view employee bags that allow you to see the contents to avoid staff slipping company assets into their purses or bags.

INSURANCE

Finally, you can consider purchasing employee dishonesty insurance. A typical policy includes:

- Coverage for a loss involving money, securities and other property committed by the fraudulent act of any employee.
- Coverage of a client's property. Your business office package policy may not provide coverage if the theft is of your client's funds, or if the theft is by a third party (non-employee).
- Coverage for workers while working off-premises at a client.
- Automatic credit-card forgery coverage.
- Automatic Employee Retirement Income Security Act bond coverage is included on most policies, eliminating the need to maintain a stand-alone ERISA bond. ❖



Think Twice Before Scanning That QR Code

QR CODES – short for Quick Response codes – are everywhere these days, on the tables at restaurants, on posters, print and electronic advertising, and even during TV programming and commercials.

But now, even these are prone to misuse and if one of your employees scans a bogus one, the scammers can potentially steal funds and business or personal data. The FBI recently warned that criminals are using tampered codes to redirect people to malicious sites that could access your firm's sensitive data.

They can send the code through e-mail as promotion codes. They also may paste the fake code on the original one, such as on parking meters, flyers, or a restaurant table where the original code would bring up the menu. The FBI says criminals are using QR codes in two ways:

1. When scanned, the code takes you to an imposter phishing website trying to trick you into logging in, hoping that you will use an existing username and password, or share other personal or banking information.

The QR code releases malicious code – such as malware, ransomware and trojans – onto your phone, allowing criminals to track information from your phone and even lock you out of the device and only releasing it if you pay up.

2. The QR code can compose pre-written e-mails and send them from your account. These e-mails are often new phishing e-mails aimed at getting your contacts to open and click on malicious links. Scammers can also program the codes to open payment sites and follow social media accounts.

TRAIN YOUR STAFF

Cyber security firm Aura and news site *TechTarget* recommend training your staff to:

- **Avoid opening QR codes in mail** – Do not scan QR codes received in regular mail and e-mails. Delete the latter and notify the IT department.
- **Avoid log-in pages** – If a QR code takes you to a log-in page, do not enter your credentials.
- **Look for signs of tampering** – Scammers may place QR code stickers over legitimate ones. Check to see if the code is on a sticker above another one, or for signs it has been tampered with.
- **Preview the URL first** – The box that opens when you scan a QR code includes text identifying the site to which it will direct you. Beware of an URL that doesn't look complete or if you can't read it.
- **Check for signs it's not legit** – Clues a site is not legit include misspelled words or odd grammar. The design may be shoddy and the images low resolution.
- **Watch out for QR codes in public places** – These codes may have been placed there by a scammer.

IT department actions

Your IT and/or security team should also ensure that:

Security software is up to date – Make sure that users are running the latest security software on any mobile device that has access to corporate resources. The software should be able to protect against device takeover attacks, phishing attacks and other mobile device exploits.

MFA is implemented across the organization – Implement multifactor authentication requirements across your company as an interim measure, and then gradually work on adopting an authentication solution that does not rely on passwords.

Many QR code-based attacks are designed to trick users into entering their passwords so that cyber criminals can steal their credentials.

If you can eliminate the need for passwords, you can greatly reduce the success rate of these attacks. ❖