ICAT
logistics, inc.

C-TPAT
Customs-Trade
Partnership Against Terrorism

# Security Awareness Training

# What IS C-TPAT and WHY is it important?

C-TPAT stands for Customs – Trade Partnership Against Terrorism.

C-TPAT is a voluntary partnership program between U.S. Customs and Border Protection and the trade industry. The purpose of the program is to strengthen and protect the supply chain.

ICAT has been a member of C-TPAT since 2006. Compliance with the security requirements of the program is of utmost importance to our company. This commitment to C-TPAT extends to promoting awareness and training not only internally but with our partners on an ongoing basis.

Below is a link to a short introduction on C-TPAT!

C-TPAT Introduction Video: CTPAT Introduction Video | U.S. Customs and Border Protection (cbp.gov)

# HOW does this affect you?

C-TPAT affects not only all aspects of the supply chain, but all persons and entities involved in it. Each person and company in the chain is key to maintaining a robust secure supply chain.

Security and Threat Awareness is an important link in the chain. Everyone involved in the transport process should be an active participant in keeping vigilant and making sure that their part of the supply chain stays strong.

## Keys to achieving this include:

# Policies, Procedures, Processes

Protocols for recognizing, stopping, and reporting issues such as unauthorized persons, compromised equipment, or internal conspiracies.

There should be protocols in place for recognizing, stopping, and reporting issues. All employees should be aware of the policies, and they should be communicated to employees on a regular consistent basis.

Below are tips to recognize, avoid, and correct potential situations.

| Unauthorized persons | Compromised seals and containers | Internal conspiracies | Suspicious packaging and paperwork |
|---|---|---|---|
| Badges for Visitors and Employees.<br><br>Visitor badges should be easily identifiable. Bright Colored badges for example.<br><br>There should be Initial, recurrent annual training, and regular reminders on how to identify an unauthorized person and whom to report to should be ongoing. | Containers that do not pass inspection Must be refused.<br><br>Seals that show signs of tampering or have a different number should be reported to company management, authorities, and ICAT.<br><br>Containers not stored in secure locations should be halted and reported to management, authorities, and ICAT. | Employees must be encouraged to report suspicious behavior among coworkers or supervisors.<br><br>There must be an established way of reporting such suspicious behavior anonymously.<br><br>Signs of internal conspiracies may include sudden unexplained wealth, an insistence on always working with the same person or in the same area of the warehouse, etc. | Suspicious signs may include:<br><br>Paperwork that looks like it has been erased and over written.<br><br>Piece counts or weights that are different then expected.<br><br>Packages that smell different, feel different, show signs of leaking, wetness, or protrusions. |

# Security Training and Threat Awareness Training

The purpose of security training and threat awareness training is to train employees to recognize and be aware of the threat posed by terrorists at each point in the supply chain.

Training should include:

Employees must know how to report situations that may compromise security (who, what, when).

Employees must be aware of emergency procedures the company has in place.

- evacuation procedures

Employees should know how to inspect containers and security seals, as well as how containers and seals should be stored.

Employees must be aware of emergency procedures the company has in place.

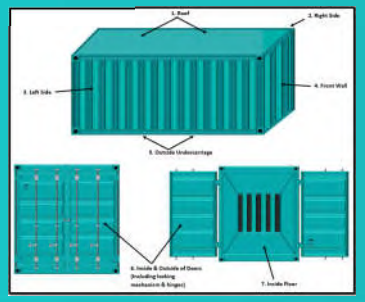
- evacuation procedures

Containers and seal security and inspection are key aspects of the C-TPAT program and of ensuring a safer supply chain. The 7 / 17-point inspection checklists must be used on all Full Container/ Full Trailer shipments. Below are the links to three excellent videos that show how to inspect containers and verify seals.

- CTPAT MSC Container Inspection - https://youtu.be/qFNshSZfNK8
  *Credit to: ASCSEG Servicios de Seguridad

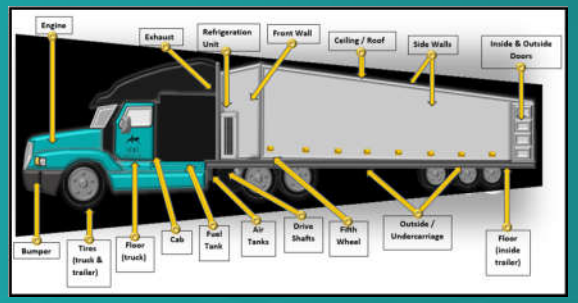
- Seal and container door inspection part 1: https://youtu.be/2x-S7v-5Cdk
  *Credit to: Andrew Ciccarone

- Seal and container door inspection part 2: https://youtu.be/Hu-rA2epsC4
  *Credit to: Andrew Ciccarone



Other key aspects include:

Have written seal control and usage procedures in place.
Use high quality ISO17712 seals.
Have proper reporting procedure to local authorities



# Physical Deterrents & Security

Facilities should utilize physical deterrents and security to assist in securing the supply chain.

Examples of this are:

- Fencing in active use around international shipping and receiving areas
- Door and gate locks used and functioning properly.
- Camera surveillance equipment in place and in working order.
- Adequate lighting.

****The following should be reported and investigated by management/authorities immediately:

Defective locking devices
Signs of tampering
Damage to exterior fencing, gates, building structures, or lighting.
Missing badges and access cards OR the use of badges and cards by unauthorized personnel;
Damage to the alarm or video systems

# Physical Access Controls

Physical Access Controls are an **IMPORTANT AREA OF EMPLOYEE PARTICIPATION**

– Employees should recognize fellow co-workers and challenge unauthorized personnel to identify themselves when seen on the premises.

– Employees should notify Security or their supervisor about ANY unauthorized personnel on premises.

– Employees should immediately report if terminated employees try to access the facility premises.

# Important Procedural Security

Employees in the receiving department must:

– Verify that cargo specifications match paperwork
– Verify seal numbers
– Check for exterior signs of tampering
– After unloading, check interior for tampering
– Report any signs of tampering or suspicious activity
– Make sure container/trailer is properly reloaded or stored
– Follow all written procedures: keep all logs updated

Management's responsibility is to:

– Quickly segregate suspect cartons or identify a and isolate suspicious persons.
– Advise of necessary evacuations
– Act on reports of suspicious activities
– Remove all keys, badges, and entry points of terminated employees.
– Ensure that all employees are instructed and aware of all required actions during a security threat. This can be achieved through safety talks, threat awareness training and emergency action-planning.

# What are some of the signs of a security threat?

Boxes that look "out of place" or have no labeling.

Sagging or loose shrink wrap.

Shipments missing boxes or containing too many boxes.

Excessive securing material such as tape or string.

Pallets or Packages that show signs of tampering.

Smells, Wires, Leaking, etc.

Protruding wires, stains, misspelled common words. Unusual marks.

# What are the steps is a package IS Suspicious?

Handle it with care!

Do not shake, bump, or drop.

Isolate it.

Don’t open it or smell it.

Immediately call authorities, security,
ICAT, and company management.

# Cyber Security

Cyber security is one of the most prevalent dangers in the supply chain today. As more companies use computers to transmit data more opportunity to commit fraud and terrorism occur. Every single day new threats appear. It's estimated that in 2020 alone 300,000 thousand new pieces of malware were created everyday and Ransomware attacks accounted for over $20 billion dollars of loss.

Every 40 seconds, a new cyber attack starts.

In 2020 there were nearly 550,000 cyber attacks per day involving ransomware. The average amount demanded was nearly a quarter of a million dollars.

Over 65% of organizations worldwide have had at least one cyber attack against them.

43% of all cyber attacks are made on small businesses.

25% of all data breaches are motivated by espionage or stealing commercial information.

**Email is responsible for propagating 95% of all malware.**

70% of all data breaches globally are financially motivated.

63% of all data breaches in organizations are caused by compromised usernames and passwords.

**Ransomware attacks are increasing at a rate of 400% year on year.**

# Phishing Attacks

**Phishing** is one of the most common types of cyber attacks. It's a deceptive and fraudulent attempt to obtain sensitive information from someone and usually happens via email.

The four main types of phishing are:

**Clone phishing -** involves sending legitimate-looking copies of emails from what LOOKS like a credible source (like a bank or a mortgage company) to get people into sharing private information. This type of phishing is  a type of "net" fishing as it usually targets large groups of people.

**Spear phishing**, like clone phishing, attempts to replicate legitimate correspondence. The difference is spear phishing uses more personalized information to target specific individuals or companies. These emails appear to originate from coworkers, family members or associated companies.

**Whale phishing** is the most specific type of phishing. The "whale" in this scenario typically is high-profile, wealthy or powerful individuals, like heads of companies.

**Tech support phishing** attacks are correspondence that pretends to come from a tech company like Microsoft or Apple. They warn that a virus or malicious program has infected a user's computer and that they need immediate updates, often for a fee.

# Malware

**Malware** is a malicious software attack. This may include ransomware, spyware, Trojans, and viruses. These types of attacks focus on not only retrieving information but often destroys information and wreaks havoc on computers or computer networks.

Common Malwares:

**Ransomware-** is a type of software that blocks access to a computer or network until a sum of money is paid. Hence the "ransom". It's basically a cyber kidnapping and hostage situation.

**Spyware** – is a type of software that enables the cyber criminal to obtain covert information about the user's computer activities.

**Trojans –** this type of software is often disguised as legitimate software. A "Trojan Horse" so to speak. Trojans are often employed by cyber-thieves and hackers to gain access to a user's system.

**Viruses –** are pieces of computer code capable of copying itself and infecting computers and networks. Typically, this type of code has a detrimental affect such as destroying systems and corrupting data.

**Password Attacks –** this type of attack is an attempt to obtain users' passwords for personal gain or illegal activities. Hackers use multiple types of attacks to do this. An example of this type of attack includes Brute Force attacks. This type of attack is where a computer program is used to enter password after password until successful. Another example would be credential stuffing.

# Cyber Attack Signs

Cyberattacks can be tough to spot. However, there are several signs to look for when you're on the receiving end of a suspicious email:

- Unsolicited emails asking for sensitive information
- Obvious grammar and spelling errors
- Clickable links to unsecured websites within the email
- Links that direct you to another country or website

When in doubt, don't act! It's better to check with your IT department before responding to any suspicious-looking email.

# Cyber Attack Signs & Survival Tips

**Expect and prepare for crises -** Protect your business against cyberattacks by keeping backups and having an emergency recovery plan in place. This can prevent against catastrophic data losses. Make sure this includes "who" is responsible for different actions in an emergency.

**Manage Critical Software Patches -** Missing critical software patches endangers your entire IT environment. and could affect basic features users depend on.

**Protect your passwords** – Use strong passwords or pass phrases. Don't use the same password on multiple sites. Keep passwords in a secure location (password management tools can be a great option!)

**Limit user access –** Only allow users to have access to programs required for their job functions and impose email restrictions as needed.

**Update polices regularly –** Have a cyber checklist and use it regularly to check your processes.

**Train employees on cyber security requirements and protocols –** Have a cyber checklist and use it regularly to check your processes.

**Firewalls, spam filters, and anti-virus programs -** Use software that can assist with securing your fire-wall or preventing viruses.

# Cyber Security Summary

Knowing what strategies cyber criminals use is only half the battle. Having a game plan and implementing steps to stop attacks is crucial to not only survival – but success.

Each of us is ultimately responsible for securing the supply chain, however by working together, having set and defined processes we can build a safer more reliant global infrastructure!