CTPAT™

YOUR SUPPLY CHAIN'S STRONGEST LINK.

Cybersecurity

U.S. Customs and Border Protection

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

How does cybersecurity affect trade?

CBP facilitates more than $2.4 trillion dollars in business revenue each year.

An inadequate cyber system can have significant security implications for businesses.

$1 trillion dollars

Worldwide losses in 2018 due to cybercrime, including criminal gains and the cost of recovery and defense

Cyber threats will continue to increase.

"…In 2013, cyberattacks bumped terrorism out of the top spot on our list of national threats … and cyber threats have led our report every year since then."

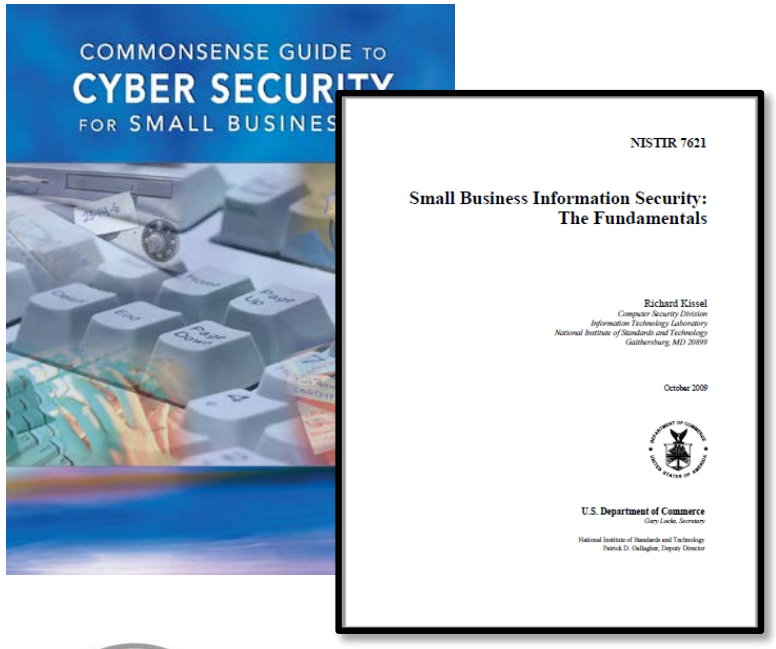
- James Clapper, Director of National Intelligence

U.S. Customs and Border Protection

Cybersecurity

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

- Common sense criteria based on industry recommendations.
- Extend to your business partners.
- The key to safeguarding a company's most valuable assets: intellectual property, customer information, financial and business data, and employee records.



National Cyber Security Alliance USA - 60% of small businesses cannot maintain their business for more than six months after a cyberattack. Often, they simply don't have the resources.

NIST Interagency Report (NISTIR) 7621 - Small Business Information Security: Bottom Line - Because small businesses generally don't invest in information security in the same way that large companies do, many cybersecurity criminals see them as easy targets.

U.S. Customs and Border Protection

Cybersecurity

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

1 Identify

Identify and control who has access to your business information.
Conduct employee investigations.
Get user accounts for each employee.
Create policies and procedures for cybersecurity.

5 Recover

Make backup copies of important business information and data.
Continue scheduling incremental backups.
Consider cyber insurance.
Make improvements in processes, procedures, and technologies.

2 Protect

Limit employee access to data and information.
Install surge protectors and uninterruptible power supplies (UPS).
Routinely patch your operating systems and applications.
Install and activate software and hardware firewalls on all your business networks.
Secure your wireless access point and your networks.
Configure network ad filters for emails.
Encrypt confidential business information.
Dispose old computers and devices safely.
Train your employees.

4 Respond

Develop a plan for disasters and security incidents of your systems.

3 Detect

Install and update antivirus, antispyware, and other anti-malware programs.
Maintain and monitor records.

The US National Cyber Security Alliance says the cost of recovering after an attack for a small to medium-sized business can range from $690,000 to more than $1 million.

U.S. Customs and Border Protection

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.1 Core -Written Procedures

- CTPAT members MUST have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems.
- The written IT policy, as a minimum, MUST cover all individual Cybersecurity criteria.

Attention: https://www.nist.gov/topics/cybersecurity

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.1 Core - Implementation Guide

- Members are encouraged to follow cybersecurity protocols that are based on industry-recognized frameworks/standards.
- The National Institute of Standards and Technology's (NIST) Cyber Security Framework(https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf) offers voluntary guidance based on existing standards, guidelines, and practices to help manage and reduce cybersecurity risks both internally and externally.
- It can be used to help identify and prioritize actions for reducing cybersecurity risk.

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.1 Core - Implementation Guide

- It is a tool for aligning policy, business, and technology focuses to manage that risk.
- The framework complements an organization's risk management process and cybersecurity program. Alternatively, an organization without an existing cybersecurity program can use the framework as a reference to establish one.
- NIST is currently the developer of technology standards for the US Federal government.

4.2 Core - Software/Hardware Protection

- To protect systems against common cyber threats, a company MUST install sufficient software/hardware to protect against malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewall) on its information systems.
- Members MUST ensure that their security software is up-to-date and receives regular security updates.
- Members MUST have policies and procedures to prevent attacks via social engineering.
- If a data breach or other event occurs that results in the loss of data and/or equipment, procedures MUST include recovery (or replacement) of IT systems and/or data.

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

Consider:

- Social Engineering Attack - the attacker uses human interaction to obtain or manipulate information about an organization or its systems.
- Aggressor - May appear modest and respectable, possibly claiming to be a new hire, technician, investigator, and may even offer credentials to support that identity. However, by asking questions, they can collect enough information to infiltrate an organization's network.
- Phishing: A type of social engineering, email, or website requesting personal information by posing as a trusted organization.

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

Tips

- Be suspicious of unsolicited phone calls, visits, or emails from people asking about employees or inside information.
- Do not respond to requests for personal or financial information, especially links sent in an email.
- Before providing any information, call and verify with the company that they were in fact the ones who sent the email.
- Pay attention to the website's URL. Malicious websites may look identical to a legitimate site, but the URL may use a spelling variation or a different domain.
- Deactivate the option to automatically download attachments.

4.3 Core - Put the System to the Test

- CTPAT members using network systems MUST regularly test their infrastructure security.
- If vulnerabilities are found, corrective actions MUS implemented as soon as possible.

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.3 - Implementation Guide

A secure network is of the utmost importance to a business and ensuring that it is protected requires periodic testing. This can be done by:

- Scheduling vulnerability scans.
  - A vulnerability scan identifies the openings on your computers (open ports and IP addresses), operating systems, and the software through which a hacker could gain access to your network.
  - The vulnerability scan does this by comparing the results of its analysis against a database of known vulnerabilities and produces a correction report for the company to act on.
  - There are many free and commercial versions of vulnerability scanners available.
- The frequency of testing will depend on several factors, including the company's business model and level of risk. For example:
  - They should run these tests when there are changes in the company's network infrastructure.
  - Cyberattacks are on the rise in companies of all sizes, and this should be considered when designing a testing plan.

Cybersecurity

4.4 Core

- Cybersecurity policies MUST address how a CTPAT member shares information about cybersecurity threats with the government and other business partners.

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.5 Core

- A system MUST be in place to identify unauthorized access to IT systems/data or abuse of policies and procedures, including inappropriate access to internal systems or external websites and tampering or altering of business data by employees or contractors.
- All violators MUST be subject to appropriate disciplinary action.

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

System access control practices:

- Deny undefined users or anonymous accounts access to systems.
- Limit and monitor the administrator use and other powerful accounts.
- Suspend or delay access ability after a specified number of failed login attempts.
- Delete outdated user accounts as soon as the user leaves the company.
- Suspend inactive accounts after 30 to 60 days.
- Enforce strict access criteria.
- Apply 'need-to-know' and 'minimum-privilege' practices.
- Override account default password settings.
- Make sure that login IDs are not descriptive of the job role.
- Enforce password requirements (length, content, lifetime, distribution, storage, and transmission).
- Audit the system, user events, and actions, and review the reports periodically.

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

Disciplinary Actions - Establish Procedure

- Employees and contractors sign a "Behavior Rules" or "Code of Conduct" to confirm their understanding and adherence to company cyber policies.
- Employees receive training on cybersecurity policies.
- Employees are informed of the consequences for not following behavior rules.
- Failure = Consequences (Infractions) Chart

U.S. Customs and Border Protection

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.6 Core

- Cybersecurity policies and procedures MUST be reviewed annually, or more frequently, depending on risk or circumstances.
- After review, policies and procedures MUST be updated if necessary.

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.7 Core

- User access MUST be restricted based on job description or assigned duties.
- Authorized access MUST be periodically reviewed to ensure access to sensitive systems is based on job requirements.
- Computer/device and network access MUST be eliminated upon employee separation.

  Example: Access to business data systems (ACE, AMS, ABI) must be limited to those employees who need to process import/export data.

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.8 Core

- People with system access MUST use individually-assigned accounts.
- System access MUST be protected against infiltration via the use of strong passwords, passphrases, or other forms of authentication, and user access to systems MUST be protected.

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.8 IndividualAccounts/passwords/Passphrases

Guide based on NIST recommendations

- Authentication: 2FA or MFA preferred
- Use of long, easy-to-remember phrases preferred over passwords
  - Eliminate periodic password change requirements
  - Eliminate password complexity requirements
- Require new password detection (commonly used or compromised passwords)

4.8 Implementation Guide

- In order to protect systems, user access must be protected through an authentication process. Complex passwords or passphrases, biometric technologies, and electronic identification cards are three different types of authentication processes.

- Processes that use more than one measure are preferred:
  - Two-factor authentication (2FA) or multi-factor authentication (MFA).
  - MFA is the most the secure because the user is required to present two or more forms of proof (credentials) to verify their identity during the login process.
  - MFAs can help block network intrusions that are exploited by weak passwords or stolen credentials.
  - How? By requiring users to strengthen their passwords or passphrases with something they have like a "token", or one of their physical characteristics: a biometric.

- If you use passwords, they must be complex. Instead of using words with special characters, the National Institute of Standards and Technology (NIST) recommends the use of long phrases up to 64 characters that are easy to remember. These longer passphrases are considered more difficult to crack.

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.9 Core

- Members who allow their users to remotely connect to their network MUST employ secure technologies, such as virtual private networks (VPNs), to allow employees to securely access the company's intranet when they are away from the office.
- Members MUST also have procedures designed to prevent remote access by unauthorized users.

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.10 Core

If members allow employees to use personal devices to perform company work, all such devices MUST adhere to company cybersecurity policies and procedures, including making regular security updates and a method to securely access the company network.

- More than 50% of the US workforce is currently working from home.
- 25% to 30% of the US workforce will work from home with some frequency after COVID-19.
- 43% of cyberattacks target small businesses.
- 22% of jobs in Mexico can be done from home.

Cybersecurity

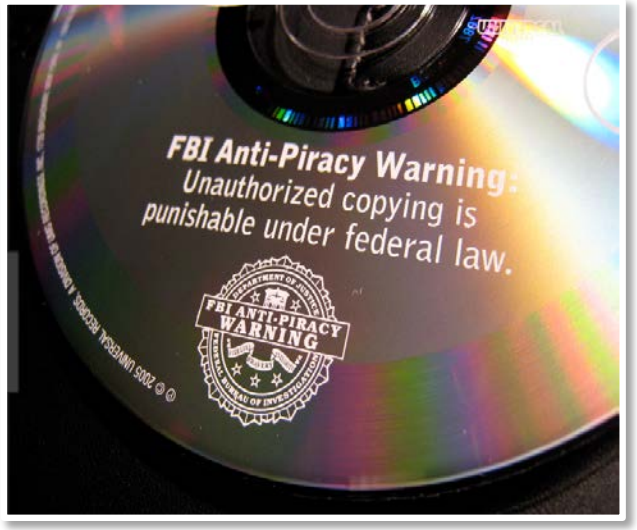
4.10 Implementation Guide

Personal devices include storage media such as CDs, DVDs, and USBs. Caution is required if you let your employees connect these personal storage devices to company computers, since these data storage devices can be infected with malware that could spread across the company network.

Cybersecurity

4.11 Core

- Cybersecurity policies and procedures MUST include measures to prevent the use of counterfeit or improperly licensed technology products.



Say NO - to the use of counterfeit or improperly licensed products

- May not update properly
- May contain malware
- No warranties or technical support
- Legal consequences: civil penalties and/or criminal prosecution

U.S. Customs and Border Protection

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.12 Core - Backups

- The data MUST be backed up once a week or as appropriate.
- All confidential data MUST be stored in an encrypted format.

External Location, Cloud Copy, Internal Hard Drive, Removable Storage Devices

The 3-2-1 rule:

3 - Keep 3 copies of any important files: 1 primary and 2 backups

2 - Keep files on 2 types of media

1- Store 1 copy outside your facilities

4.12 Implementation Guide

- Daily backups may be needed due to the effect that data loss can have on some employees if shared or production servers are compromised/lost. Individual systems may require less frequent backups, depending on the type of information involved.

- Storage devices used to store backups should preferably be stored in an external facility. These devices should not be on the same network as the primary. Data backup to the cloud is acceptable as an off-site installation.

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

4.13 Core

- All devices, hardware, or other equipment containing confidential information about the import or export process MUST be accounted for through periodic inventories.
- When disposed, they MUST be properly sanitized or destroyed per National Institute of Standards and Technology (NIST) guidelines covering these standards or other appropriate industry guidelines.

4.13 Implementation Guide

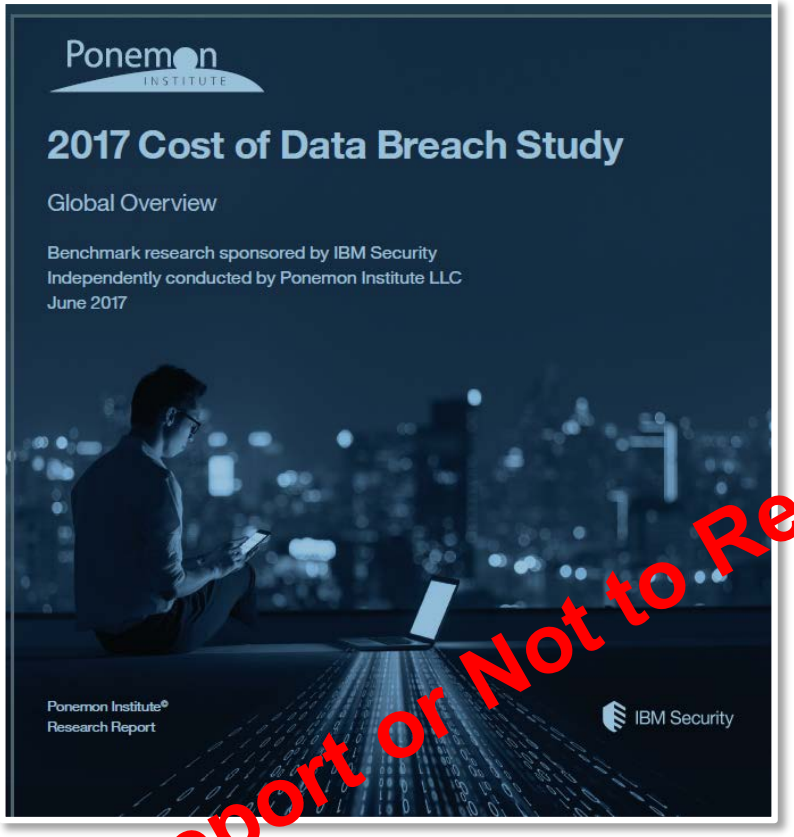
- Computer media types are: hard drives, removable drives, CD-ROM or CD-R discs, DVD or USB drives.
- The National Institute of Systems and Technology (NIST) has developed US government storage device destruction standards. CTPAT members would benefit from consulting the NIST standards regarding device cleaning and destruction.
- Hard Drive Destruction:
  - http://ewastesecurity.com/nist-800-88-hard-drive-destruction/
- Sanitation:
  - https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization

Cybersecurity

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

Study IBM by Ponemon Institute - 2019

- Cost per cyberattack:
  - Up to $8.19 million, depending on the country.
  - The global average is $3.19 million
- 24% of attacks are caused by human error.
- Small companies suffer greater damage: $3,500 per employee per attack (Companies with 500 to 1000 employees).



To Report or Not to Report?

U.S. Customs and Border Protection


CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.
U.S. Customs and
Border Protection