U.S. Customs and Border Protection:

How CBP and Trade Partners Can Address Cybersecurity Threats

Shaun Khalfan, CISSP, CEH

CBP Chief Systems Security Officer

April 5-7, 2016

Washington, D.C.

How does cybersecurity impact trade?

Working directly with its trade partners, CBP facilitates approximately **$2.4 trillion** in trade revenue each year.

Weak cybersecurity can have significant implications for trading partners

$445B

Estimated losses to the global economy in 2013 due to cyber crimes, including both the gains to criminals and the cost of recovery and defense

456

Hours to restore one vessel's seaworthiness due to malware

90%

Percentage of world's goods on 400,000 ships left potentially vulnerable to GPS spoofing, jamming, or interception

Cyber threats will only continue to increase.

"In 2013, 'cyber' bumped 'terrorism' out of the top spot on our list of national threats… **And cyber has led our report every year since."**

– James Clapper, Director of National Intelligence
January 29, 2016

Who's targeting our networks?

Threat assessments show that CBP and its trade partners' networks are targeted by multiple threat actors that have both the capability and intent to mount sophisticated cyber attacks.

Organized Criminals: Cartels

- Organized criminal groups have a financial interest in breaching CBP networks to **facilitate drug and human trafficking**.
- These groups could exploit vulnerabilities in field technologies used by CBP field agents patrolling on the border to determine when and where to transfer illicit goods.

Nation States

- State-sponsored actors have been involved in several high profile government breaches **to steal national security and economic data**.
- CBP's networks are more likely to be targeted than other Federal agencies given its mission and the sensitive law enforcement and trade data it holds.

Organized Criminals: Black Market Entities

- Black market entities **anonymously sell counterfeit products or forged documents,** allowing criminals and terrorists to enter the country or pose as officials.
- Groups sell information on cybersecurity tools or vulnerabilities to other individuals that may compromise systems or networks, particularly databases that host valuable data.

Terrorists

- Terrorists are likely to target CBP field operations through cyber means **to advance ideology and undermine public security**.
- Terrorist organizations' cybersecurity capabilities continue to grow in sophistication and could exploit CBP data and infrastructure to further operationalize goals to traffic weapons and operatives into the United States.

How is CBP addressing these threats?

Data Protection

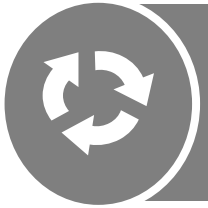
Personal identity verification (PIV) credentials physically and digitally match a user's identity to protect data confidentiality, integrity, and availability. By issuing PIV cards to CBP partners, it prevents and protects systems from unauthorized, potentially malicious actors.

Proactive Threat Identification and Monitoring

Cyber threat intelligence (CTI) is evidence-based knowledge about an existing or emerging cyber threat that is timely, accurate, relevant, and predictive. CBP is establishing a CTI program to identify and defend against external attacks on its most critical assets.

Enhanced Information Sharing

CBP is renewing its efforts to educate its partners on how it is incorporating cybersecurity and privacy protection measures into existing requirements and programs, which protect the integrity and privacy of personally identifiable information and trade data.



Continuous Cyber Hygiene

CBP routinely updates its server and endpoint operating systems and automated security programs as part of a comprehensive effort to drive continuous cyber hygiene. These efforts proactively mitigate new vulnerabilities and risks as they arise.

How do CBP's cybersecurity efforts support effective and lawful trade?

Cybersecurity efforts underpin CBP's customs and trade mission by enabling secure transactions, strengthening trade enforcement operations, and protecting companies' brand reputation.

 **Transaction Integrity**	CBP hardens its cyber infrastructure against a variety of threats to protect the confidentiality, integrity, and availability of data, systems, and equipment, such as ACE, non-intrusive screening equipment, and other manifest databases. This helps **ensure the integrity of transactions** and **prevents cargo from theft or compromise.**
 **Trade Enforcement**	Trade enforcement operations rely on secure IT support and database connectivity for field agents and officers to conduct enforcement against counterfeits, unsafe products, and trade agreement violators. In 2014 alone, CBP's enforcement operations seized counterfeits with an **estimated value of $1.2 billion.**
 **Brand Reputation**	CBP protects legitimate trade through secure, data-driven decision making that supports intellectual property rights, import safety monitoring, and privacy to **protect companies' brand reputation.**

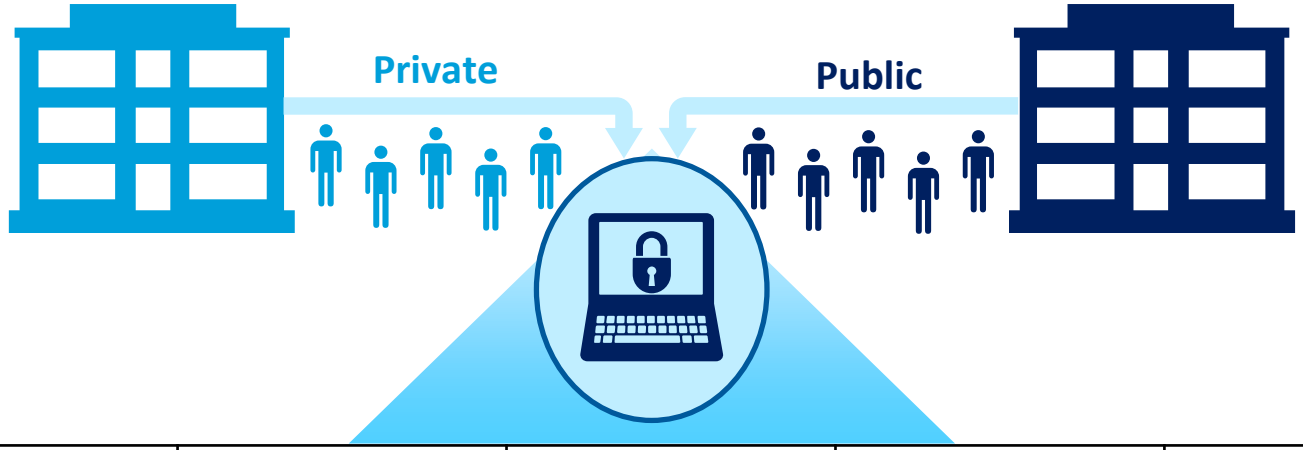
How can organizations enhance their cybersecurity posture?

While each industry and company are different, there are five common best practices that all organizations should take to set the foundation for a strong cybersecurity program. When implemented as part of a holistic risk management strategy, **these five practices can greatly increase an organization's resilience to cybersecurity threats**.

Asset Identification	Cybersecurity begins with an organization knowing what is connected to its network. Every piece of equipment has vulnerabilities and exposes an organization to risk; organizations can only protect assets they know exist.
Asset Protection	Organizations should ensure their most critical assets are protected by installing and anti-virus software, patching and updating operating systems and software regularly, and enabling a cyber-aware workforce.
Attack Detection	Understanding that a network has been compromised is the first step to attack response. Continuous monitoring and detection capabilities can provide insight into network anomalies.
Attack Response	Once an attack is detected, organizations should have a plan in place to quickly analyze the threat and take action. Organizations should also understand who to contact for help, if necessary.
Attack Recovery	Recovering from an attack includes resuming regular operations but also incorporating lessons learned into protection, detection, and response plans.

How can TSN and CBP collaborate on cybersecurity?

Recognizing the impact of cybersecurity on nearly every facet of society, the Federal Government offers a host of resources to help companies enhance their own cybersecurity posture. By leveraging these resources, **partners can help secure their systems, thereby decreasing the risk to CBP and other trading partners**.



National Institute of Standards and Technology Cybersecurity Framework http://www.nist.gov/cyberframework/	**Department of Homeland Security Critical Infrastructure Cyber Community Voluntary Program** https://www.dhs.gov/ccubedvp	**Department of Homeland Security *Stop.Think.Connect.* Campaign** https://www.dhs.gov/stopthinkconnect	**Federal Bureau of Investigation Malware Investigator** http://www.malwareinvestigator.gov/	**U.S. Industrial Control Systems Cyber Emergency Response Team Assessment Tool https://ics-cert.us-cert.gov/Assessments**