BakerHostetler

Cybersecurity Risks in Trade Compliance

Guidance and Risk Management Strategies for Customs and Trade

Matthew Caligur
Kimberly Gordy

February 6, 2025

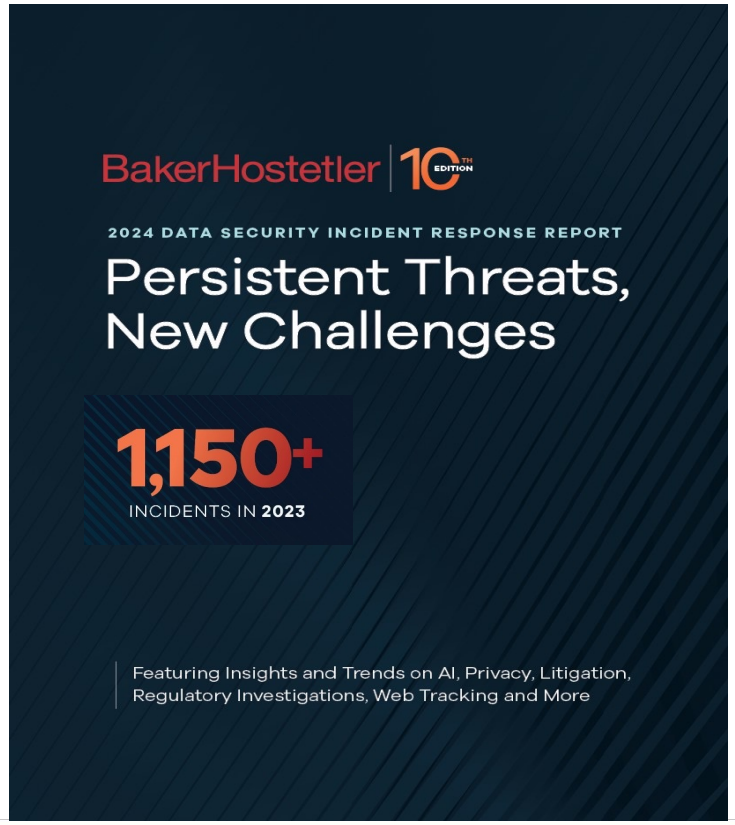
Agenda

BakerHostetler

- Overview of Data Breaches
- Summary of CBP Cybersecurity Guidance
- Indicators of Compromise
- Downtime and Business Continuity Considerations
- CBP Cybersecurity Incident Reporting Process

Overview of Data Breaches

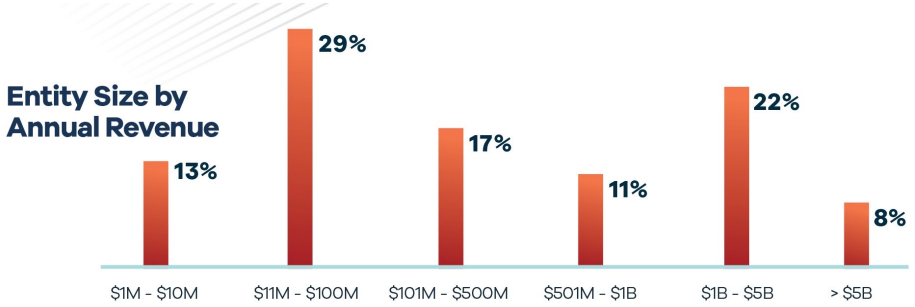
Overview

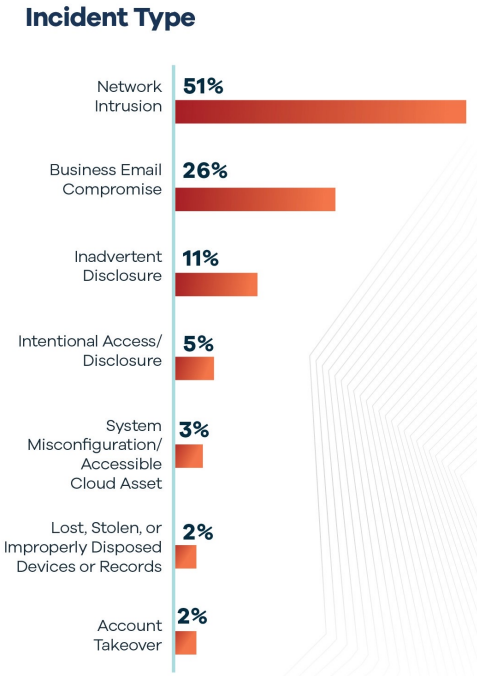


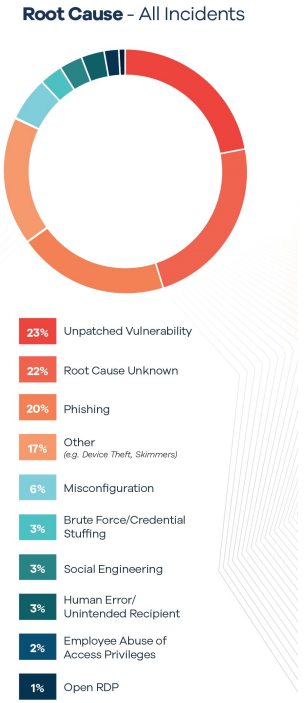
There is no "silver bullet" for preventing network intrusions and attack vectors including phishing, social engineering, and vulnerabilities in remote access tools such as VPN and SFTP systems continue to plague organizations.

Overview: The Numbers

- 1,150+ incidents in 2023
- 10th Annual Data Security Incident Response Report

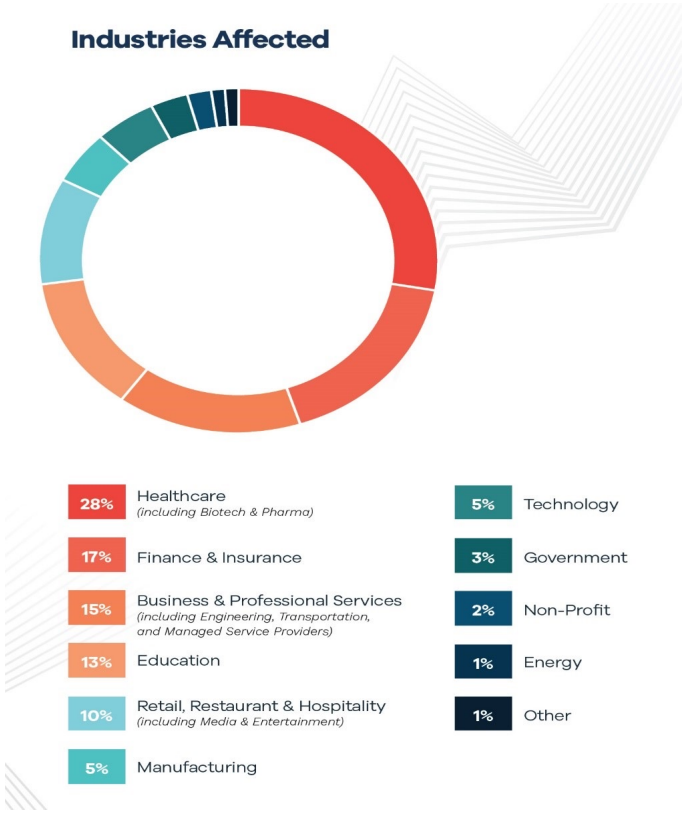






Source: BAKERHOSTETLER, 2024 DATA SECURITY INCIDENT RESPONSE REPORT: PERSISTENT THREATS, NEW CHALLENGES (2024) (reporting on 2023 security incidents for which BakerHostetler was counsel).

Overview: Industries Affected



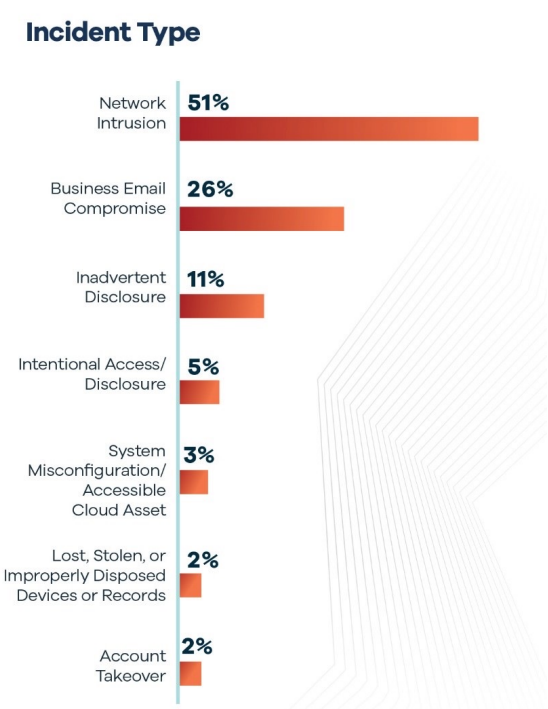
Industries Affected

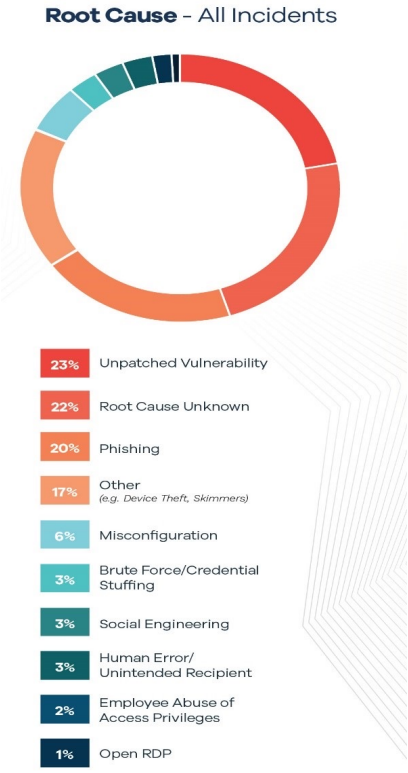
Average Median

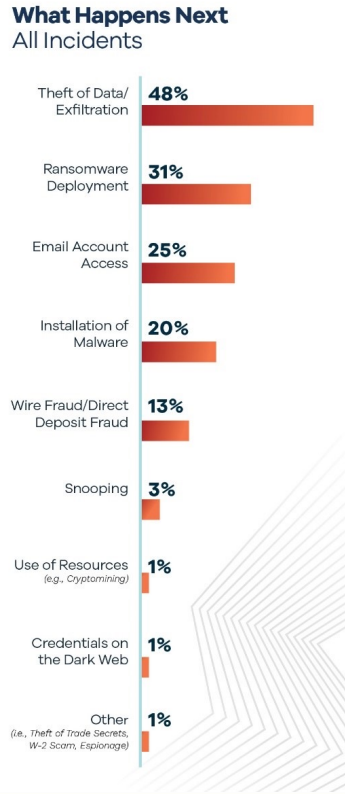
Industries Affected	Initial Ransom Demand	Ransom Paid	Days to Acceptable Restoration	Forensic Investigation Cost	Individuals Notified
RETAIL, RESTAURANT & HOSPITALITY	$5,701,509 ($1,000,000)	$150,000 ($150,000)	11.4 (8)	$60,520 ($26,000)	96,107 (770)
ENERGY & TECHNOLOGY	$5,400,854 ($917,000)	$1,468,800 ($220,000)	11.3 (11)	$68,542 ($37,063)	34,828 (351)
FINANCE & INSURANCE	$3,913,000 ($500,000)	$4,033,333 ($2,000,000)	9.8 (10)	$37,153 ($14,500)	28,039 (412)
HEALTHCARE	$3,492,434 ($2,000,000)	$857,933 ($420,000)	13.4 (9)	$63,993 ($30,390)	158,362 (1,440)
MANUFACTURING	$3,356,186 ($1,175,000)	$361,000 ($400,000)	11.7 (8.5)	$48,486 ($28,350)	99,931 (1,018)
GOVERNMENT	$1,584,742 ($250,000)	$15,490 ($15,490)	19.8 (14)	$43,618 ($29,706)	390,717 (541)
BUSINESS & PROFESSIONAL SERVICES	$1,133,835 ($690,000)	$523,465 ($206,000)	15.1 (6)	$38,678 ($20,000)	20,057 (310)
EDUCATION	$967,507 ($800,000)	$166,330 ($175,000)	19.6 (5)	$55,528 ($40,650)	155,156 (4,112)
NON-PROFIT	$101,667 ($100,000)	$5,000 ($5,000)	6.4 (10)	$23,769 ($14,500)	698 (371)

Overview: What Happens After Access?

BakerHostetler







Overview: The Ransomware Epidemic Key Metrics

BakerHostetler

Largest Ransom Demand in 2023:
$30+ Million
($90+ Million in 2022)

Largest Ransom Paid in 2023:
$10+ Million
($8+ Million in 2022)

Average Ransom Paid in 2023:
$747,651
($600,688 in 2022)

Average Forensic Investigation Costs

$50,125
All Incidents

$354,474
20 Largest Network Intrusion Incidents

$78,138
Network Intrusion Incidents

Average Ransom Demand & Payment

$2,644,647
Ransom Demand
(All Industries)

$747,651
Ransom Payment
(When Paid) (All Industries)

27% of organizations that experienced a ransomware or data extortion incident paid a ransom. The primary reasons for payment break down are as follows:

- **41%** of the time, payment was made primarily for buying a decryptor;
- **37%** of the time, payment was made primarily to prevent publication of the stolen data on the ransomware group's disclosure site; and
- **22%** of the time, payment was made for both a decryptor and nonpublication.

63% of the time, an organization restored from backup without paying a ransom.

85% of organizations found evidence of data exfiltration when there was a claim of data theft in the ransom note.

76% of incidents involved theft of data resulting in notice to individuals.

Historical Average Ransom Demands

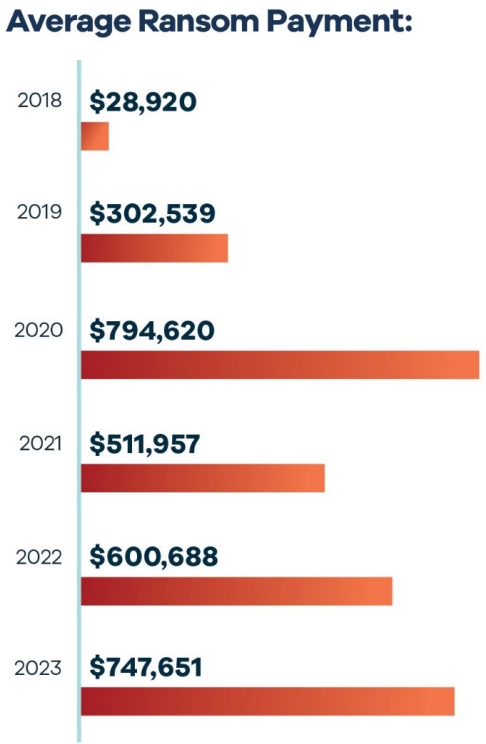
BakerHostetler

Ransom Payments Increased Again

The average ransom paid in 2023 was

$747,651

nearly returning to the average payment in 2020 during the height of the ransomware epidemic.



BakerHostetler

Incident Response Timeline *(in Days)*

	Detection Occurrence to Discovery	Containment Discovery to Containment	Analysis Time to Complete Forensic Investigation	Notification Discovery to Notification
Median All Incidents	**2**	**0**	**33**	**60**
Average All Incidents	**42**	**4**	**39**	**75**
Average Network Intrusions	**36**	**5**	**35**	**65**


CBP Cybersecurity Guidance for
Customs Brokers

Purpose of the Guidance

BakerHostetler

- Provides best practices to enhance preparedness for a cyber incident on a licensed customs broker data system.
- Applies to companies transmitting data to Automated Commercial Environment (ACE) directly or indirectly.
- Also applies to any web-based Applications such as ACE or CTPAT portals.

Key Elements of CBP Guidance for Cyber Incident Preparedness & Response

BakerHostetler

1. Prevent & Protect

2. Communicate

3. Respond

4. Recover

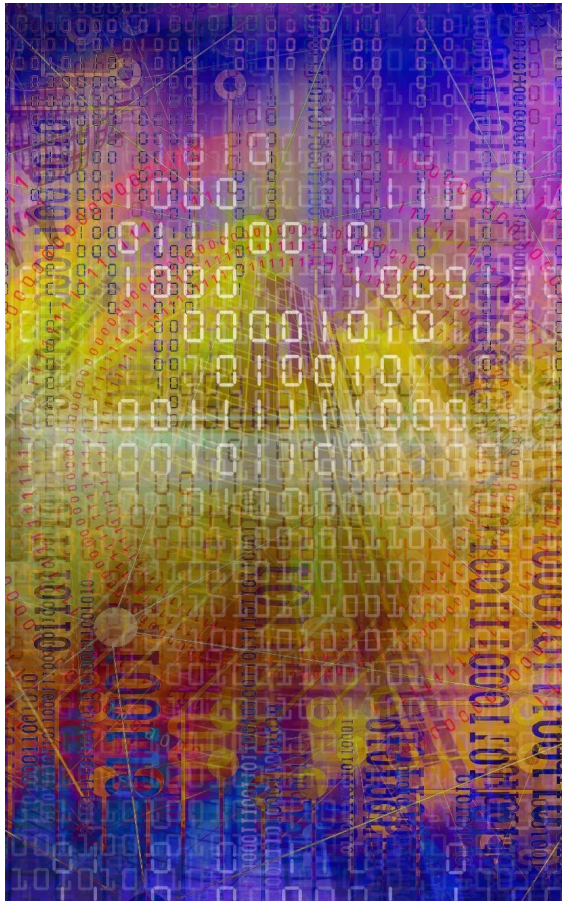
13

BakerHostetler

Prevent & Protect:

Cybersecurity Planning & Risk Management

- Purpose is to partner with trade entities with data connections to CBP to identify and disrupt future cyberattacks through the collection of cyberattack Indicators of Compromise.
- Provides a systematic and repeatable process for reporting the right information in the event of an active cyberattack on private industry.
- Applies to companies that transmit data to ACE, directly, or indirectly, using a service provider.
- Also applies to accessing any web-based applications, such as ACE or CTPAT portals.



Prevent & Protect:

Written Cybersecurity Program

BakerHostetler

Include **written policies and procedures** to protect IT systems

Follow protocol based on **recognized industry standards** like NIST CSF

Frequently review the written program for necessary updates

Submit **up-to-date ISAs** every 3 years if transmitting data directly to ACE

Prevent & Protect:

IT Controls

Utilize updated firewall, anti-virus, and anti-spyware software

Regularly test IT infrastructure with vulnerability scans

Exercise due diligence to ensure IT service providers have security measures in place

Prevent & Protect:

Cybersecurity Planning & Risk Management

- Maintain up to date Interconnection Security Agreements (ISA):
- If directly transmitting data to ACE, submit an updated ISA at least every three years.
- Data Protection:
  - Frequently back up data and store all sensitive and confidential data in an encrypted format.
  - Keep backup devices physically offsite (or in the cloud) and connect backup devices to a different network.
  - Maintain originals of records, including records stored in electronic formats, within the customs territory of the U.S. in accordance with 19 CFR 111.

BakerHostetler

Prevent & Protect:

Cybersecurity Planning & Risk Management

- Develop a plan for communicating with stakeholders about cybersecurity incidents that identifies:
  - WHO to notify, including current contact information, for CBP and Partner Governmental Agency (PGA) contacts;
  - WHEN to reach out to importer clients, system vendors, CBP, and PGA contacts; and
  - WHAT information to share at each stage of a cyber incident.

BakerHostetler

Prevent & Protect:

Cybersecurity Planning & Risk Management

- Account for supply chain risks—threats to national security, trade compliance, and PGA requirements—in business continuity plans, and identify how to manage these risks without system access.
  - Have a risk-based process for screening new business partners and for monitoring current partners.
  - **TIP**: Refer to CTPAT Five Step Risk Assessment Process for basic tools, resources, and examples to consider when conducting a supply chain risk assessment.
- PGA Requirements: Have a plan to verify client's PGA requirements absent system access.
  - ACE reports and reporting from PGAs may help.

BakerHostetler

Communicate:

Initial Notification & Ongoing Stakeholder Coordination

- Immediate Notification: CBP's Office of Information Technology Security Operations Center (SOC).
- Brokers must report any breach of records relating to Customs business no later than 72 hours as required under 119 CFR 11.21(b).
- Stakeholder Communication: Communicate with CBP client representatives and relevant PGAs.

BakerHostetler

Communicate:
Messaging Goals & Risks

Goals

- Comply with all applicable laws and regulations
- Be thorough and descriptive without causing unnecessary concern.
- Provide reassurance without overpromising
- Strive for openness and transparency without creating unnecessary risk

Risks

- Complaints
- Negligence, Invasion of Privacy Lawsuits
- Class Action Lawsuits
- Regulatory Action
- Damage to Brand and Trust

BakerHostetler

Communicate:
A note on the word “breach”

BREACH

- Legal Significance.
- Suggests something bad happened or is going to happen.
- Use it too frequently and it can make individuals and regulators think you are subject to numerous breaches.

Other Ways to Describe it?

- Incident.
- Event.

BakerHostetler

Communicate:
Don’ts and more Don'ts

- Don’t speak too early and/or “on the fly”
- Don’t use a misleading initial holding statement
- Don’t fall victim to saying too much or being too reassuring
- Don’t assume you have to answer all media inquiries
- Don’t over-apologize
- Don’t leave out helpful evidence
- Don’t call yourself a victim
- Don’t overstate the security measures you had in place
- Don’t overstate new security measures
- Don’t ignore regulators

BakerHostetler

Respond:

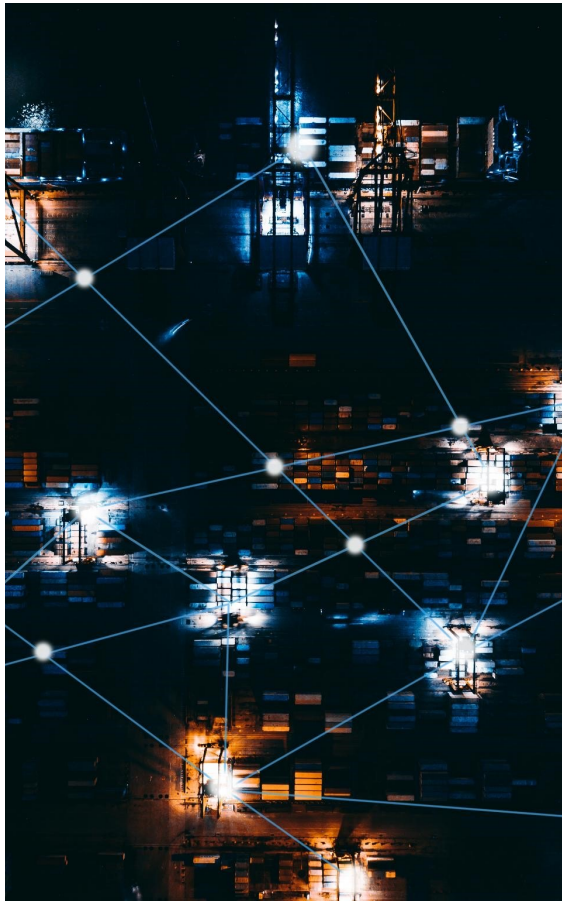
Maintain Movement of Lawful Cargo While Managing Risk

- CBP may be able to work with you to implement downtime procedures, providing flexibility to maintain the facilitation of lawful trade and release of cargo while systems are down.
- Contact CBP OFO: Reach out to headquarters level to request assistance and ensure broker's downtime procedures are compliance with CBP requirements.
- Downtime Letter: Provide downtime letter documenting each entry with entry numbers and other required data.
- Documents: Be prepared to provide copies of appropriate documents for manual review.

BakerHostetler

Recover:
Reconnect Systems, Work to Resume Business

- System Safety Validation:
  - Must provide evidence of system remediation before CBP will authorize reconnection to ACE.
- Retroactive Data Entry:
  - Must keep a full accounting of entries during cyber incidents and input that data into ACE for CBP processing.



Incident Preparedness

BakerHostetler

- Incident response plan review & development
- Incident response training & tabletop exercise
- Cybersecurity roadmap assessment
- Reasonable security measures and risk assessments
- Written information security programs

Incident Preparedness

BakerHostetler

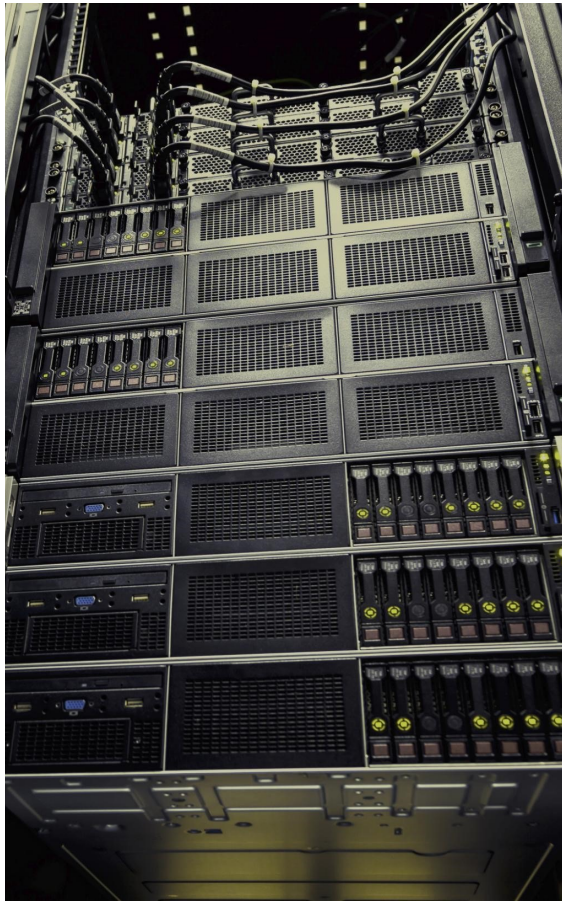
- Vendor risk management (cybersecurity supply chain risk management)
- Technology contract review and template building
- Privacy compliance
- Privacy governance
- Marketing, Advertising, and Digital Media


Reporting Cyber Incidents and Sharing
Indicators of Compromise

BakerHostetler

What are Indicators of Compromise?

- An Indicator of Compromise (IOC) is forensic evidence on a computer (host) or network that indicates the security of the network has been accessed without authorization.
- IOCs act as flags that cybersecurity to uses to detect unusual activity that is evidence of or can lead to a future attack.
- Also act as clues that may indicate actor intent and attribution and can help provide correlation of possible future attacks.

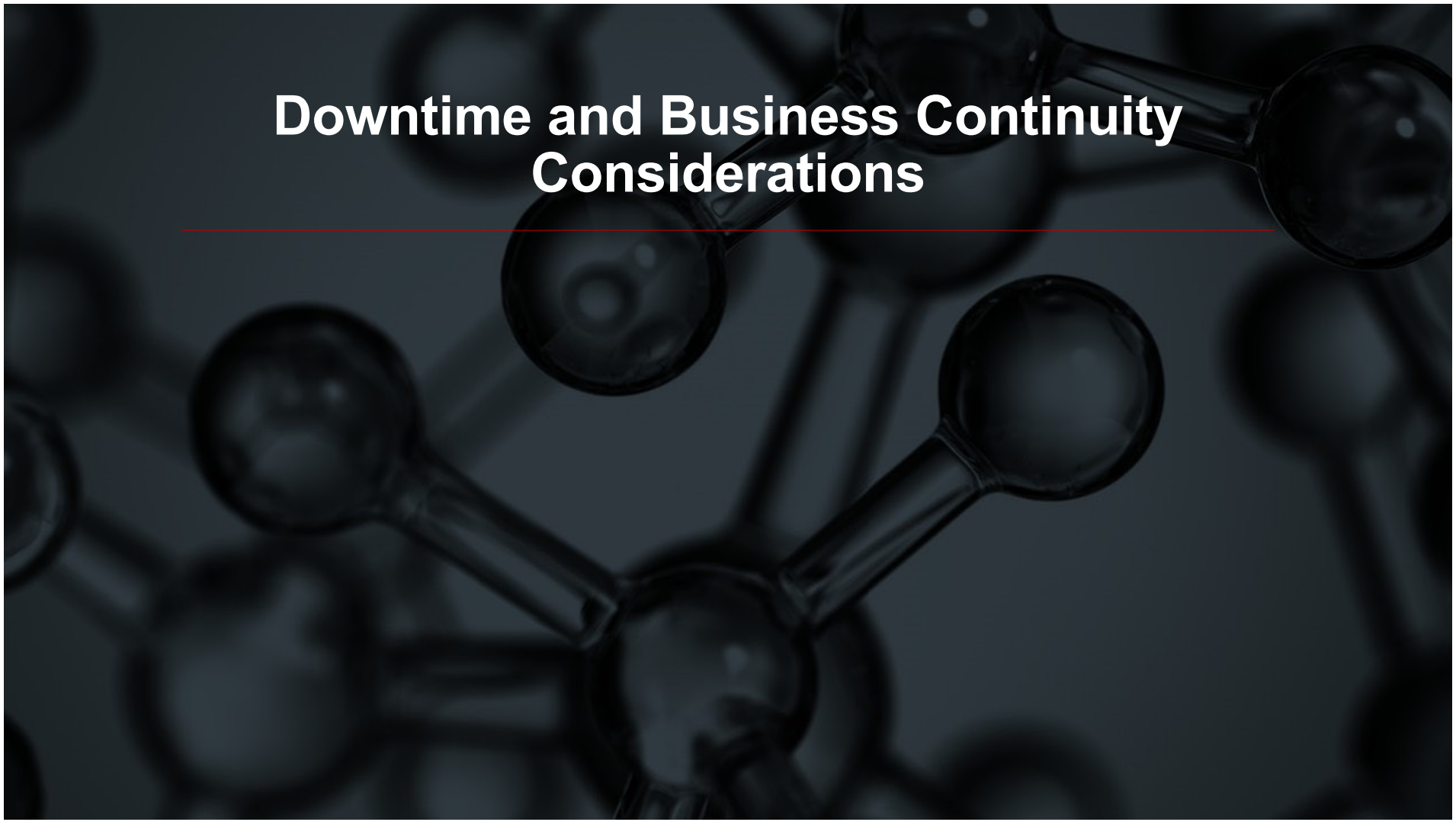


BakerHostetler

Common IOCs and Suspicious Activities

Section 2: Common IOCs and Suspicious Activities	
Unusual inbound or outbound network traffic	If inbound or outbound traffic patterns are unusual, this can be indicative of a potential attack.
Anomalies in privileged user account activity	If user account anomalies are identified, this could indicate a user trying to escalate privileges of a particular account or using the account to access others with more privileges.
Geographical irregularities	If network activity occurs outside of regular geographic locations, this can be evidence of a cyber threat actor in another country trying to penetrate the system.
Other login red flags	If an existing user - or an account that should not exist - has multiple login attempts, this may indicate an attempt to penetrate the system by a threat actor.
Increase in database read volume	If an attacker tries to extract your data, their efforts may result in a swell in read volume.
HTML response sizes (web/Internet)	If HTML data results are usually small, but you notice a far larger response size, it may indicate that data has been extracted.
Multiple requests for same file	If multiple requests to access the same file are detected, this may indicate threat actors are trying to steal files.
Mismatched port-application traffic	If an unusual port is being used, this can indicate an attacker attempting to penetrate the network through the application.

Downtime and Business Continuity Considerations



Key Concept: “Downtime”

- If cyber event affects brokers ability to submit required information to ACE, “downtime” provides an alternative process to release cargo.
- Authorized on case-by-case basis by Office of Field Operations (OFO).
- Broker must submit a “downtime letter” and required supporting documentation by email to a designated CBP official.
- No waiver or extension of filing deadlines.
- No waiver of Partner Government Agency (PGA) requirements.
- **Entries released through downtime processing must be resubmitted through ACE once access is restored**.

Key Concept: “Fully Up and Running”

- Fully up and running system:
  - Is safe and secure for a broker to reconnect to ACE after a cybersecurity incident; and
  - Broker’s systems can transmit required documents and information to CBP through ABI/ACE.
- Determination is made by CBP’s Office of Information and Technology (OIT).
- Prerequisites: broker must review patterns in technical processing, conducted human investigations, etc.

Key Concept: “Enforcement Discretion”

- CBP may provide discretion for post-release transactions to broker after a cyber event.
- Broker may submit voluntary tender(s) on behalf of importer clients to resolve interest debt on affected entries.
  - No obligation to do so.
  - Aggregate reconciliation can by calculated entry by entry or using midpoint calculation.
- Identify that the payment is for additional interest on entries submitted.
  - Include the affected broker’s name and identify the dates of the cyber event.
- Payment should be collected on a cash receipt.

Key Concept:
Reporting Affected Transactions

BakerHostetler

- Brokers are responsible for identifying and post-release transactions affected by the cyber event.
- Brokers must provide daily report of entries released during downtime with the cargo release information below (ACE date added once entry is put into ACE).
  - Send to cyberincident@cbp.dhs.gov, as well as appropriate Port Directors/Center Directors.
  - Include certified statement that all affected transactions are included in the report and have been transmitted to ACE within five business days after end of CBP enforcement discretion.

Cargo Release					
Entry Number	Port of Entry (POE)	Released on Downtime? (y/n)	Date of Entry (Date of Submission of Complete Information for Release)	Date of Release	Date Input in ACE

Downtime Tips & Best Practices

BakerHostetler

- Have an offline continuity plan, including a reserve of entry numbers.
- Plan to fulfill PGA requirements.
  - Hard copies of forms, invoices, and documentation may assist.
- Communicate appropriately with stakeholders.
- Remember that clearance of merchandise can be provisional in nature.
  - Requests for redelivery are possible.

Business Continuity Planning

- **Business Continuity Plan ≠ Disaster Recovery Plan**
  - DRP: Restore normalcy, get back to work
- **Business Continuity Plan ≠ Incident Response Plan**
  - IRP: Assess and handle incident
- **BCP: Keep business running while systems are down**
  - Including during restoration and recovery
- **Cyber event restoration: 1–3 weeks**

Industries Affected

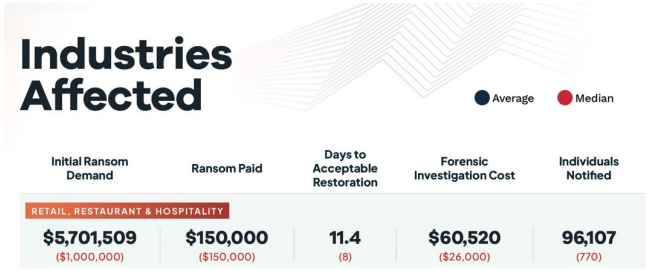
Average Median

Industries Affected	Initial Ransom Demand	Ransom Paid	Days to Acceptable Restoration	Forensic Investigation Cost	Individuals Notified
RETAIL, RESTAURANT & HOSPITALITY	$5,701,509 ($1,000,000)	$150,000 ($150,000)	11.4 (8)	$60,520 ($26,000)	96,107 (770)
ENERGY & TECHNOLOGY	$5,400,854 ($917,000)	$1,468,800 ($220,000)	11.3 (11)	$68,542 ($37,063)	34,828 (351)
FINANCE & INSURANCE	$3,913,000 ($500,000)	$4,033,333 ($2,000,000)	9.8 (10)	$37,153 ($14,500)	28,039 (412)
HEALTHCARE	$3,492,434 ($2,000,000)	$857,933 ($420,000)	13.4 (9)	$63,993 ($30,390)	158,362 (1,440)
MANUFACTURING	$3,356,186 ($1,175,000)	$361,000 ($400,000)	11.7 (8.5)	$48,486 ($28,350)	99,931 (1,018)
GOVERNMENT	$1,584,742 ($250,000)	$15,490 ($15,490)	19.8 (14)	$43,618 ($29,706)	390,717 (541)
BUSINESS & PROFESSIONAL SERVICES	$1,133,835 ($690,000)	$523,465 ($206,000)	15.1 (6)	$38,678 ($20,000)	20,057 (310)
EDUCATION	$967,507 ($800,000)	$166,330 ($175,000)	19.6 (5)	$55,528 ($40,650)	155,156 (4,112)
NON-PROFIT	$101,667 ($100,000)	$5,000 ($5,000)	6.4 (10)	$23,769 ($14,500)	698 (371)

Source: BAKERHOSTETLER, 2024 DATA SECURITY INCIDENT RESPONSE REPORT: PERSISTENT THREATS, NEW CHALLENGES (2024) (reporting on 2023 security incidents for which BakerHostetler was counsel).

Business Continuity Considerations

- **What business operations would be disrupted?**
  - Manufacturing/production?
  - Transportation/shipping?
  - Scheduling/delivery?
  - Accounting processes (e.g., payables and receivables)
- **How immediate is the impact?**
- **What are the failovers/workarounds?**
  - Have they been tested?
  - Who is responsible for implementation?
  - What is the implementation timing and timeline?



Business Continuity Considerations

- **How are you coordinating among locations and teams?**
- **How are you communicating with employees? Customers? Vendors? Other stakeholders?**
- **Implementing Business Continuity Measures**
  - Roles and responsibilities
  - Reasonable security measures and risk assessments
  - Testing Your procedures


CBP Cybersecurity Incident
Reporting Process

Reporting a Cybersecurity Incident

BakerHostetler

- **What to report:** Any "…breach of physical or electronic records relating to customs business…"
- **When to report it:** ASAP, but no later than 72 hours after discovery
- **Who to report it to:** CBP OIT Security Operations Center (SOC)
  - Telephone: 703-921-6507 or
  - Email: cbpsoc@cbp.dhs.gov **and** cyberincident@cbp.dhs.gov
- Broker must also inform impacted PGAs of outage to get guidance on admissibility clearance
  - CBP Office of Trade Headquarters can provide PGA point of contact
- CBP encourages brokers to notify their importer clients

What To Expect After Reporting A Cybersecurity Incident

BakerHostetler

- The CBP OIT SOC will follow up with questions and understands that all information may not be available.
- Questions that may be asked:
  - What is the root cause of the incident?
  - What is the nature of the cyber intrusion?
  - What are the attack vectors?
  - What systems/applications are impacted?
  - How does the cyber incident impact ACE?
  - Do you have a direct connection to ACE, or do you use a service center?

What To Expect After Reporting A Cybersecurity Incident

BakerHostetler

- More questions that may be asked:
  - What are the Indicators of Compromise?
  - What is the scale of the outage (local, national, global)?
  - What is the length of the outage (hours, days, weeks)?
  - What mitigation procedures are being performed by the broker?
  - What is the estimated timeline to resolution?
  - Any additional follow-up questions as needed.

Adding a Cybersecurity Point of Contact

Cybersecurity Technical Point of Contact

BakerHostetler

- CBP encourages having a Technical Point of Contact for Cybersecurity associated with ACE portal accounts.
- CBP can use contact if a legitimate cybersecurity threat is identified.
- Several benefits:
  - Reducing doubt about the legitimacy of both the cyberattack and the notification from a CBP official.
  - Providing CBP the correct person to contact for technical and cybersecurity related information.
  - Expediting collaborative efforts to intercept and/or mitigate the impacts of an identified threat.


Cybersecurity Requirements for CTPAT Compliance

CTPAT Cybersecurity Requirements

BakerHostetler

- Comprehensive written cybersecurity policies and procedures
- Sufficient hardware/software protection
- Regularly test security of IT infrastructure
- Plan for sharing information about cybersecurity threats
- System to identify unauthorized access to IT systems
- Frequent review of policies and procedures
- Restrict user access based on job description or assigned duties

CTPAT Cybersecurity Requirements

BakerHostetler

- Individually assigned accounts for IT system access
- Secure technologies for remote access connections
- Policies for personal devices
- Prevent use of counterfeit or improperly licensed products
- Backup data at frequent intervals
- Recurring inventories of data and equipment containing sensitive data

Contact Us 24/7/365

Matthew W. Caligur
Partner
mcaligur@bakerlaw.com
T +1.713.646.1355

Kimberly C. Gordy
Partner
kgordy@bakerlaw.com
T +1.713.646.1360

Toll-Free, 24-Hour
Data Breach Hotline
+1.855.217.5204
DataBreach@bakerlaw.com

BakerHostetler

bakerlaw.com

Atlanta | Austin | Chicago | Cincinnati | Cleveland | Columbus | Dallas

Denver | Houston | Los Angeles | New York | Orange County | Orlando

Philadelphia | San Francisco | Seattle | Washington, D.C. | Wilmington