CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM (CTPAT)

Date April 6, 2021

U.S. Customs and Border Protection

Scope

- Understanding that the logistics industry is a prime target of APT (advanced persistent threat) groups, foreign state-sponsored hacking groups and others. Threat landscape is enormous and growing

- Communication/Oversight – improving communication between IT department and stakeholders within an organization

- Assessing risk internally, risk your organization poses to your supply chain partners and risk posed by your partners to your organization

Scope

- Training
- User Authentication (passwords/passphrases/2FA, etc)
- Patching
- Email Security – Implement Multi-factor authentication
- Back-ups – store remotely

Recent Notable Breaches

This is a very abbreviated list. The true list is alarming.

- Kia Motors/Hyundai
- Underwriters Laboratories-UL
- ATFS-Automatic Funds Transfer Services – used by many cities in California and Washington
- Bombardier
- University Hospital Newark New Jersey
- Baltimore County Schools
- Kroger
- 9 U.S. Government Agencies and possibly 100’s of companies (SolarWinds-ongoing and Microsoft Exchange Server)
- Solar Winds
- Microsoft Exchange Server

Recent Ransom Note

Appeared on screens of compromised v

March 2021

- February 202
- Ransomware
- Exfiltration o
- Hackers are
  Ransomware
  - Providing
    made to b
  - Offering c
    ransomwa
  - Conductin
    ransom pr

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[2]

Background on Ransomware Attacks

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, cyber actors threaten to publicly disclose victims' sensitive files. The cyber actors then demand a ransomware payment, usually through digital currency, in exchange for a key to decrypt the files and restore victims' access to systems or data.

In recent years, ransomware attacks have become more focused, sophisticated, costly, and numerous. According to the Federal Bureau of Investigation's 2018 and 2019 Internet Crime Reports, there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019.[3] While ransomware attacks are carried out against large corporations, many ransomware attacks also target small- and medium-sized

[1] This advisory is explanatory only and does not have the force of law. It does not modify statutory authorities, Executive Orders, or regulations. It is not intended to be, nor should it be interpreted as, comprehensive or as imposing requirements under U.S. law, or otherwise addressing any particular requirements under applicable law. Please see the legally binding provisions cited for relevant legal authorities.

[2] This advisory is limited to sanctions risks related to ransomware and is not intended to address issues related to information security practitioners' cyber threat intelligence-gathering efforts more broadly. For guidance related to those activities, see guidance from the U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, Cybersecurity Unit, *Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources* (February 2020), available at https://www.justice.gov/criminal-ccips/page/file/1252341/download.

[3] *Compare* Federal Bureau of Investigation, Internet Crime Complaint Center, *2018 Internet Crime Report*, at 19, 20, available at https://pdf.ic3.gov/2018_IC3Report.pdf, *with* Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report*, available at https://pdf.ic3.gov/2019_IC3Report.pdf.

1

Sectors Most Targeted

No sector is immune.

- Financial, healthcare and pharma sectors – most targeted/compromised in 2020
- Manufacturing sector - a close second
- Logistics/Transportation is third, and growing, due to their unique position and interaction with a wide variety of industry sectors,
  - Small operations with poor or no cybersecurity.

Communication

- A ‘good IT person’ does not equate with a cybersecurity professional.
- IT vs. Cybersecurity credentials, certifications – widespread
- Typical organizational structure does not include adequate oversight of IT Dept.
- Instances where IT Dept operates autonomously – common.
  - Without adequate auditing, oversight compared to other traditional departments, sections
  - Adherence to approved policies/procedures (MSC)
- Communication between IT Dept. and stakeholders is problematic - widespread

Communication

- *"No one in management was equipped to even understand where the weaknesses existed in IT and no one had oversight [of IT]".*
- We find that companies try to get as much out of their networking, traditional IT folks in lieu of hiring credentialed, certified cybersecurity personnel.
- *"Based upon your findings and our discussions today, I am going to hire a third-party in the interim and pay for our existing IT employees to take cybersecurity courses" - Owner of a medium-sized company in the IT sector*

Risk

- Third-party supply chain attacks
  - Software supply chain attacks
    - Solar Winds
    - Target, Inc.
- Hackers target weak parties in your network, supply chain, logistics chain, etc. Poor cybersecurity, password hygiene
- Collect intelligence to craft very convincing phishing emails
- Use connections to primary target company (portals, file transfer services, automated payment solutions, ERP, etc.) look for unpatched vulnerabilities,

Risk

- Assess overall cyber risk internally
- IT Dept should begin to coordinate with managers outside of department to assess their level of compliance with MSC
- Identify weaknesses
- Install an audit component
- Query IT personnel for issues of concern
- Assess risk posed by supply chain (vendors, clients, suppliers)
- Larger orgs may consider assisting smaller orgs based on a totality of risk

Yes, passwords are still a problem.

- P
- L
- U
- P
- IT
- P
- T
  p
- 2

S.No.	Password	S.No.	Password	S.No.	Password	S.No.	Password
1	1 2 3 4 5 6	26	654321	51	fuckyou	76	test
2	password	27	jordan23	52	nicole	77	hockey
3	12345678	28	password1	53	hunter	78	dallas
4	qwerty	29	1234	54	sunshine	79	password
5	1 2 3 4 5	30	robert	55	tigger	80	fuckyouasshole
6	123456789	31	matthew	56	1989	81	admin123
7	letmein	32	jordan	57	merlin	82	pussy
8	1234567	33	asshole	58	ranger	83	pass
9	football	34	daniel	59	solo	84	asdf
10	iloveyou	35	andrew	60	banana	85	william
11	admin	36	lakers	61	chelsea	86	soccer
12	welcome	37	andrea	62	summer	87	london
13	monkey	38	buster	63	1990	88	1q2w3e
14	login	39	joshwa	64	1991	89	1992
15	abc123	40	1qaz2wsx	65	phoenix	90	biteme
16	starwars	41	12341234	66	amanda	91	maggie
17	123123	42	ferrari	67	cookie	92	querty
18	dragon	43	cheese	68	ashley	93	rangers
19	passw0rd	44	computer	69	bandit	94	charlie
20	master's degree	45	corvette	70	killer	95	martin
21	hello	46	blahblah	71	meandyou	96	ginger
22	freedom	47	george	72	pepper	97	yankees
23	whatever	48	mercedes	73	jessica	98	thunder
24	qazwsx	49	121212	74	zaq1zaq1	99	Michelle
25	trustno1	50	maverick	75	jennifer	100	aaaaaa

User Authentication – MSC 4.8

The numbers speak for themselves – and these only represent what was found/reported

- 123456 (23.2m)
- 123456789 (7.7M)
- Qwerty (3.8)
- Password (3.6m)
- 11111111 (3.1m)
- 12345678 (2.9m)
- Abc123 (2.8m)
- 1234567 (2.5m)
- Password1 (2.4m)
- 12345 (2.3m)
- 1234567890 (2.2m)
- 123123 (2.2m)

Training: Phishing, Spoofing

How confident are you that employees in your organizations are properly trained? How about the same question posed to your business partners and their employees?

- Phishing emails
  - Which is a legitimate email?
    - jdoe@anderinger
    - jdoe@anderringer
    - jdoe@an.deringer
- Spoofed URL
  - Which web address is legit?
    - www.anderinger.com
    - www.anderringer.com
    - www.derringer.com
    - www.anderringer.org

Fileless attacks have risen exponentially over past 3 years

- Spoofed emails, links, photos, brand/company logos
- Spoofed website URL (website address)

Training: Phishing, Spoofing

The message on WhatsApp:

- Homograph – The ‘N’ in Nike is an international character which is recognized as a ‘dash’.
- Website spoofing - skimming

Training

Just about every credible list of cyber priorities starts with employee training

- In-person training highly recommended
- Frequent, recurring
- Use real-world scenarios (found to be effective)
- How to create a truly strong password
- Work with IT to convert to passphrases *(offer training)*
- Phishing

Training

- Insider threat
- Vishing – phishing over the phone (Twitter)
- Information Security
- Divulging company information and procedures

- Importance of reporting possible breaches in timely manner
- Streamlined reporting
- IT and the little antivirus icon can’t always do it alone

Patching – Network Defense MSC 4.2

- Important for POC* to have better understanding of patching (security updates)
- Hacker groups search for firms that have unpatched software
- Most successful way victim environments were accessed last year were by scanning and exploiting unpatched vulnerabilities
- Followed by phishing
- Understand difference between ‘critical’ or ‘high importance’ patch versus non-critical
- Timeliness of deploying patches, understanding process, auditing for compliance

Patching – Security Updates

All of these breaches – and many more – directly attributable to lack of patching.

- Equifax 143m,
- JPMorgan Chase 83m,
- Yahoo 1billion,
- Home Depot 56m,
- Uber 57m,
- Target 110m,
- Marriott 500m

- Network segregation and segmentation
  - Restrict lateral movement
- Files/data security – encrypting data/files
- Limiting access to files (a lot of companies say they restrict access to files based on need to know – but many recent breaches and audits say different)
- VPN*

Cloud

Operating in the cloud does not exempt your organization from implementing solid cybersecurity hygiene

- Company states they are exempt from cyber MSC – operate 100% in the cloud
  - Do you want your employees to disregard password rules and hygiene?
  - Clicking on phishing links
  - Accessing any files or data they choose
  - Allow anyone into your apps, software etc without any restriction?
  - IoT considerations
  - Insider threat
- Cloud can mean many things to many orgs – myriad variables
- Implement Encryption

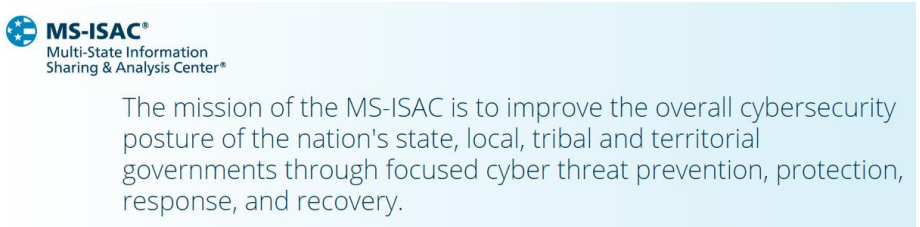
Cloud

- IAM – Identity Access Management
- Your org's are still responsible for configuring access restrictions to your data – no matter where it is stored
- If personnel don't follow user authentication protocols or click on malicious links – they could possibly allow hackers access to the data stored in the cloud.
- Apps that operate 100% online – ensure that they are updated, strong passwords (or better), ask for 2FA if offered.
- It is not the cloud vendor's responsibility to train your staff or ensure your IT staff sets the correct permissions

Sharing MSC 4.4

- MSC - Cybersecurity policies should address how a Member shares information on cybersecurity threats with the government and other business partners.

- Big problem is many SMB owners do not know where to start, lack resources
- MS-ISAC (Multi-State) designated by DHS as the cybersecurity ISAC for state, local, tribal governments. DHS provides operational-level coordination with MS-ICAC.



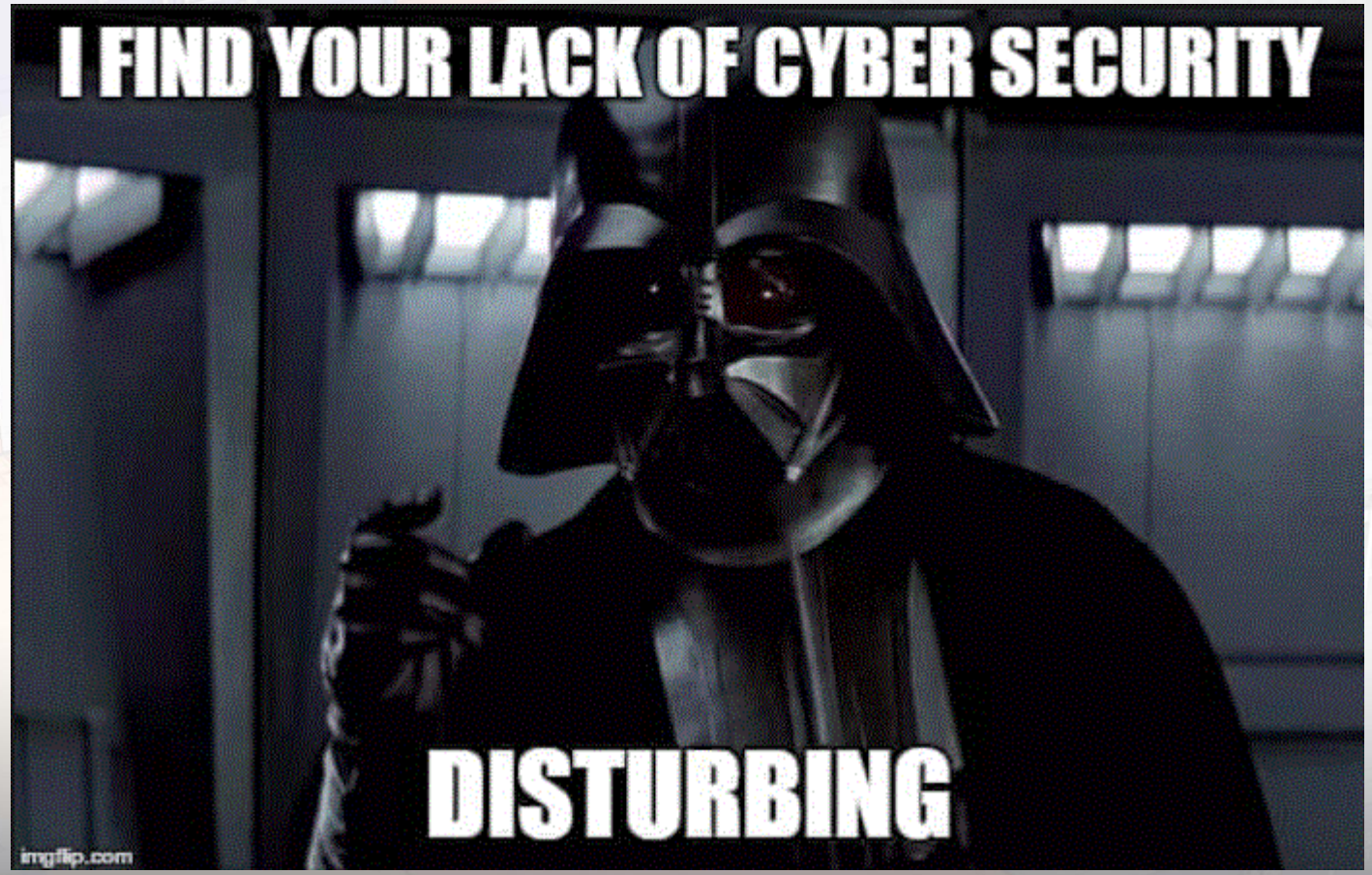
Other Considerations

- Join an ISAC
  - Based on geographic location or industry sector
- Rehearse response to a breach, continuation of operations plan, recovery plan
- Cyber MSC* is just as important as all other MSC
- Ensure there exists a strong audit component for cyber MSC

Additional Resources

- CISA.gov (DHS)
- FCC Cyber Security (Scroll Down)
- Small Business Administration
- Cyber.nj.gov **
- NIST Supply Chain Feb 2020
- Security Boulevard
- Krebs On Security
- CSO Online
- StaySafeOnline
- Lehigh University – Phishing Examples

CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.



U.S. Customs and Border Protection

CTPAT Q&A

Bryan Smith
SCSS
bryan.d.smith@cbp.dhs.gov

CTPAT
Office of Field Operations
U.S. Customs and Border Protection