VANGUARD LOGISTICS

Vanguard Logistics
5000 Airport Plaza Drive
Suite 200
Long Beach, CA 90815
U.S.A

communications@vanguardlogistics.com
vanguardlogistics.com

Date 27th October 2021
Subject Network Security Incident

Attention DB Schenker

NETWORK SECURITY INCIDENT - Customer Update

Dear Dominik,

Thank you for your patience and support as the Vanguard team works through the impact of our Network Security Incident. We continue to make progress in our milestones to reinstate core systems with some systems already up, and our business continuity plans are in action. However, this process must be completed diligently and with the utmost precaution for the security of ours and our customers' businesses and data. Therefore, we greatly appreciate your patience over the coming days.

We are now in a position to answer a few of your questions, which we have received regarding how we are managing the processes and our ability to support your shipping operations.

We must also state that our IT team is 100% focused on the safe and rapid reinstatement of our operating systems. They continue to working closely with specialized experts on the required forensics and analytics to ensure the safety and integrity of our systems and data - which is an ongoing process. As such, we will only be able to answer more technical and regulatory questions as information is reliably available.

Please refer to the Q&A below for current updates. If you have other questions please contact us at **communications@vanguardlogistics.com** and we will add answers where information is available.

On Behalf of the Vanguard Leadership Team
Vanguard Communications

FAQ

Q: What is the nature of the cyber security incident?
A: It is a ransomware attack that involved the encryption of data on certain computers in our network

Q: Which systems are affected?
A: Initially, all systems were taken down to contain the incursion and avoid propagation of the malicious code to systems that were not initially infected. As per standard protocol, all systems will need to be checked and cleared prior to being placed back on line. We are currently focused on our operating systems and devices, which is hampering the ability of our teams to access our core applications.

Q: What is the impact of the incident and how long do you think it will take?
A: Currently we are cycling through a clear plan and already achieved a number of milestones. We are working to a timeframe of between a week to 2 weeks for platforms to be fully available, although probably at reduced capacity.

Q: Which countries are affected and can we get a status report by country?
A: All locations are somewhat impacted as we have taken down all systems and re-introduce as possible. As we are incrementally bringing locations back up, we are also prioritizing systems that support all our regions to give global coverage albeit at a lower capacity.

Q: Have you activated your business continuity plans and how do they look like?
A: Yes our BCPs are activated including manual processes, fall back support offices, prioritizing systems for certain processes, finance controls and payments, shipment visibility and communications across our network.

Q: Have you shut down any direct network connection to third parties?
A: Yes, our EDI and API capabilities and other direct network connections have been shut down as a precaution and as is standard protocol.

Q: When do you plan to recover sending EDI messages?
A: At this moment we are not able to confirm. For reasons of diligence, prudence and security of our customers' data, we expect EDI to be one of our later milestones. We are however able to accept bookings via other methods and to provide visibility through our website.

Q: Did you identify impact to PII / personal data?
A: At this stage forensics and analysis are ongoing and when we have specifics, we will share any relevant findings as they become available.

Q: Is there any risk to customer systems?
A: Our network and systems are isolated, and while forensics and analytics remain ongoing, based on our current analysis and model of integrations, we strongly believe that there has not been risk to customer systems.

Q: Can you give us contact with your IT organization?
A: Our IT team is 100% focused on reestablishing systems for our operations with diligence and care, while also completing the necessary forensics and analysis to ensure the security of our business and data. As we have specifics and any pertinent updates, we will provide through our communications team.