Treasury and Trade Solutions

citi®

Beware of Ransomware

What is Ransomware?

Ransomware is a cyber-attack method. Malware which has been designed to encrypt files on a device is deployed, resulting in files and the systems that rely on them becoming inaccessible, or unusable. Cyber criminals then demand a ransom in exchange for decryption. Cyber criminals may also threaten to sell or leak the compromised data or authentication information if the ransom is not paid. Ransomware is becoming increasingly prevalent, and is often aimed at high-profile or high-value targets.

Ransomware in Numbers*

An estimated **€10.1 bl** was paid in ransoms in 2019 (€3.3 billion more than in 2018)

365% increase in detections in businesses in 2019

An estimated **45%** of attacked organizations paid the ransom

Best Practices

- Maintain reliable back-ups: Follow the 3-2-1 rule (Maintain at least 3 copies of important files in 2 different formats, keeping 1 copy offsite/offline). Regularly test back-ups
- Ensure your organization has a cyber incident response plan ready and that employees are aware and trained in the use of the response plan. Regularly test, update and train employees on the plan
- Undertake regular monitoring to identify vulnerabilities
- Use network segmentation, data encryption and access controls to protect data. Ensure segmentation between IT and OT networks
- Use appropriate and updated tools for ransomware protection
- Regularly patch and update software
- Undertake regular audits of remote desktop services
- Control external devices and port accessibility, ensure devices are correctly configured and that security features are enabled.
- Implement content filtering to filter out unwanted attachments and emails with malicious content
- Ensure antivirus and anti-malware software is up to date
- Ensure strong passwords are used

What to do if you have been the victim of a ransomware attack?

Isolate and Disconnect: Cyber criminals may monitor your organization's activity and/or communications after an initial attack to understand if their actions have been detected. Disconnect systems and use alternative communication methods such as phone calls, so that cyber criminals do not become aware that they have been discovered. If devices cannot be disconnected from the network, power them down to avoid further spread of the ransomware infection.

Identify critical systems: Work with your IT department to identify critical treasury systems. This should be done in advance of any attack, as part of your organization's cyber response planning. After an attack, treasury should work with IT to restore critical systems and identify those that have been compromised

Activate the Cyber Response Plan: Ensure that your organization has a Cyber Response Plan in place, and that it is regularly tested and updated. Employees should undertake regular training on the Cyber Response Plan, and be aware of their role in the event of an attack. In the event of a Ransomware attack, the Cyber Response Plan should be activated; including informing partners, such as banks, of the attack in a timely manner. Click here **to download a sample Cyber Response Planning Checklist**

Restore: Prioritize restoration and recovery based on a predefined critical asset list that identifies the systems critical for business continuation.

*ENISA Threat Landscape 2020 – Ransomware

For further information and resources please visit the Cybersecurity and Infrastructure Secuity Agency (CISA) website – www.cisa.gov/publication/ransomware-threat-to-ot

IRS Circular 230 Disclosure: Citigroup Inc. and its affiliates do not provide tax or legal advice. Any discussion of tax matters in these materials (i) is not intended or written to be used, and cannot be used or relied upon, by you for the purpose of avoiding any tax penalties and (ii) may have been written in connection with the "promotion or marketing" of any transaction contemplated hereby ("Transaction"). Accordingly, you should seek advice based on your particular circumstances from an independent tax advisor. This communication is provided for informational purposes only and may not represent the views or opinions of Citigroup Inc. or its affiliates (collectively, "Citi"), employees or officers. The information contained herein does not constitute and shall not be construed to constitute legal, tax and/or accounting advice by Citi. Citi makes no representation as to the accuracy, completeness or timeliness of such information. This communication and any documents provided pursuant hereto should not be used or relied upon by any person/entity (i) for the purpose of making regulatory decisions or (ii) to provide regulatory advice to another person/entity based on matter(s) discussed herein. Recipients of this communication should obtain guidance and/or advice, based on their own particular circumstances, from their own legal, tax or accounting advisor. Any terms set forth herein are intended for discussion purposes only and are subject to the final terms as set forth in separate definitive written agreements. This presentation is not a commitment or firm offer and does not obligate us to enter into such a commitment, nor are we acting as a fiduciary to you. By accepting this presentation, subject to applicable law or regulation, you agree to keep confidential the information contained herein and the existence of and proposed terms for any Transaction. We are required to obtain, verify and record certain information that identifies each entity that enters into a formal business relationship with us. We will ask for your complete name, street address, and taxpayer ID number. We may also request corporate formation documents, or other forms of identification, to verify information provided