≥ QUICK GUIDE

STEP 1:

Disconnect everything and evaluate

❑ Do not turn the computer off. The message on the screen may be required to determine the ransomware type

❑ Verify that an incident actually occurred and determine the incident type (*e.g. denial of service, malware, inappropriate use*)

❑ Assign initial priority rating (*e.g. Urgent, High, Medium, Low*)

❑ If the CISO is not yet aware of the incident, notify the CISO

❑ Activate SIRT Team

❑ Set up Command Center and Contacts Notification of Staff

❑ Remember Chain of Custody Processes

❑ Unplug the computer from the network via the Ethernet cable

❑ Turn off any wireless functionality: Wi-Fi, Bluetooth, NFC

❑ Disconnect all external storage: memory sticks, attached phones/cameras, external hard drives, and USB drives

❑ Report the ransomware incident

❑ Contact Insurance

❑ Contact Legal or Security Consultants

❑ Consider limiting or ceasing nonessential services

❑ Notify community partners in accordance with local policies and procedures (*e.g., consider local Emergency Operations Center, other area hospitals, local emergency medical services*)

❑ Containment and Eradication procedures. BCP plan and IRP procedures

STEP 2:

Determine the scope of the infection and check the following for signs of encryption from a known good, uninfected computer

❑ Mapped or shared drives

❑ Mapped or shared folders from other computers

❑ Network storage devices of any kind

❑ External hard drives

❑ USB storage devices of any kind (*e.g. USB sticks, memory sticks, attached phones/cameras*)

❑ Cloud-based storage: DropBox, Google Drive, OneDrive, etc.

❑ Backups

STEP 3:

Determine the ransomware strain. This is important because there are multiple strains of ransomware and how you respond can be decided depending on the strain

❑ With support determine what strain or type of ransomware. (*e.g. CryptoWall, Teslacrypt, etc.*)

❑ https://labs.bitdefender.com/2017/09/bitdefender-ransomware-recognition-tool/

❑ https://id-ransomware.malwarehunterteam.com/

❑ Look for available descriptors

❑ https://labs.bitdefender.com/2017/09/bitdefender-ransomware-recognition-tool/

❑ https://www.nomoreransom.org/

❑ https://www.nomoreransom.org/en/decryptiontools.html

STEP 4:

Determine Response. Now that you know the scope of your encrypted files and the ransomware strain you are dealing with, you can make a more informed decision about what to do next

RESPONSE I
Restore Your Files From Backup

❑ Locate your backups

❑ Ensure all the files you need are there

❑ Verify integrity of backups

❑ Check for Shadow Copies if possible

❑ Check for any previous versions of files that may be stored on cloud storage (*e.g. DropBox, Google Drive, OneDrive*)

❑ A good practice is to back up the encrypted files in case a decryptor becomes available

❑ Rebuild the system from known good sources

❑ Restore your files from backups

❑ All credentials stored anywhere on the local network (including those saved inside Web browsers and password managers) could be compromised and need to be changed

❑ Many ransomware cases are the result of phishing. Look for phishing messages and corrupt downloads and permanently delete to avoid reinfection

RESPONSE II
Try to Decrypt

If you determined the strain and version of the ransomware, find out if there is a decryptor available. A good practice is to back up the encrypted files. In case the decryptor does not work, continue the following steps:

❑ Attach any storage media that contains encrypted files (hard drives, USB sticks, etc.)

❑ Backup the newly decrypted files for reloading

❑ Rebuild the system from known reliable sources. Do not trust antivirus programs to completely remove all malware from a system. Install all patches to avoid reinfection from network transmitted malware

❑ Many ransomware cases are the result of phishing. Look for phishing messages and corrupt downloads and permanently delete them to avoid reinfection

❑ All credentials stored anyw here on the local network (including those saved inside Web browsers and password managers) could becompromised and need to be changed

RESPONSE III
Do nothing and lose files

❑ Back up the encrypted files in case a decryptor becomes available

❑ Rebuild the system from known sources. Do not trust antivirus programs to completely remove all malware from a system. Install all patches to avoid reinfection from network transmitted malware

❑ Many ransomware cases are the result of phishing. Look for phishing messages and corrupt downloads and permanently delete them to avoid reinfection

❑ All credentials stored anywhere on the local network (including those saved inside Web browsers and password managers) could be compromised and need to be changed

RESPONSE IV
Negotiate and/or Pay the Ransom

This is not recommended and if considering this option, it is imperative to consult with the Legal and Insurance for proper guidance. After consultation, if you choose to proceed, follow these steps:

❑ Back up the encrypted files in case the decryptor provided by the criminals does not work

❑ Decrypt files as instructed

❑ Back up all files

❑ Rebuild the system from known good sources. Do not trust antivirus programs to completely remove all malware from a system. Install all patches to avoidreinfection from network transmitted malware

❑ Restore your files from your backup

❑ All credentials stored anywhere on the local network (including those saved inside Web browsers and password managers) could be compromised and need to be changed

❑ Many ransomware cases are the result of phishing. Look for phishing messages and corrupt downloads and permanently delete them to avoid reinfection

WWW.OBSGLOBAL.COM

HEALTH CYBERSECURITY SERVICES

❑ HIPAA Security Risk Assessment

❑ Technical Virtual CISO

❑ Training and Webinars

❑ Policy Development

❑ Tabletop Exercises, IRP Plan

≥ ASK US ANYTHING

Shelby Kobes – skobes@obsglobal.com

Adam Kehler – akehler@obsglobal.com

≥ RANSOMWARE PLAYBOOK