Deciding When & Why to Pay Ransom

Use this guide to help you decide whether to pay ransom in response to a ransomware incident This guide is intended to be used with the Ransomware Response Plan and Incident Response Plan.

WHAT YOU NEED TO KNOW

Statistics and facts regarding ransomware have a high amount of variation. Many organizations do not report ransomware attacks, and the attackers are continuously changing their tactics. It is becoming more frequent that attackers do not provide a workable key to unencrypt data once ransom is paid. Current studies report that victims are able to **unencrypt data 19-50%** of the time when ransom is paid. Federal Law Enforcement advises organizations not to pay ransoms in order to discourage the criminals.

A study by Trend Micro, Inc. found that most organizations end up paying the ransom. Currently the average ransom amount is $1,000 and usually payable in non-traceable currency such as bitcoin.

RANSOM PAYMENT ANALYSIS

- ☐ **Is the ransomware attack contained? Are you sure?**
  Some ransomware programs are designed to sit idle for a period of time before activating. A complete malware scan of all computer systems on the network should be performed. Isolate the compromised system(s) from all internal network connectivity until they are cleaned.
- ☐ **Have you identified the ransomware version?**
  Research the version.
- ☐ **Do you have the ransom note?**
- ☐ **Are the infected systems backed up?**
  Is the backup current?
- ☐ **Are the backups off-network?**
  Verify the ransomware files do not exist on the backup.
- ☐ **Some ransomware versions have a free solution to unencrypt the files.**
  Two sources of information which should be reviewed are: nomoreransom.org/crypto-sheriff.php and bleepingcomputer.com/forums/f/239/ransom-ware-help-tech-support/
- ☐ **Assign a value of the compromised data $ __________**
  (Cost to the business if the data is lost)
- ☐ **Initiate the Incident Response Plan**
  and contact the cyber insurance company.
- ☐ **Notify relevant stakeholders in the organization.**

The infected machine will need to be rebuilt even if the ransomware keys work. There may be bugs in the ransomware which impact system operation or even reinfect the machine.

If the above items have been completed, then there is enough information available to make a decision regarding paying the ransom. Paying the ransom is more of an operational decision then a technical decision. Does the cost to the organization in financial, reputational, lost business or the potential data lost exceed the price of the ransom? Will the loss be covered by insurance?

Time and the extent of a ransomware attack are significant factors which complicate the decision process. Typically, the ransom will give the victim a limited amount of time to pay before the ransom increases or the data is deleted.

LORICCA
HIPAA COMPLIANCE SPECIALISTS

Pay the Ransom Data Points

PRO: PAY THE RANSOM

- ☐ The business cost of data lost is significantly higher than the ransom
- ☐ Ransomware version history indicates success-ful access after payment
- ☐ Data backups are not good
- ☐ Ransomware is not contained/ significant im-pact to organization.
- ☐ All options for restoring the data have been unsuccessful

CON: DON'T PAY THE RANSOM

- ☐ At best, paying the ransom will provide a 50% chance of regaining access
- ☐ Clean data backups have been verified
- ☐ Ransomware has been contained
- ☐ Mitigation costs to clean the systems will be incurred regardless
- ☐ Is the version of ransomware reversible?
- ☐ Paying the ransom is likely to make the organization a larger future target

