RANSOMWARE Q&A

1

How can a small business back up their cloud storage files and keep them offline so they cannot be encrypted?
The key to protecting the backup is setting up a system that pulls data from the primary servers. The primary servers must have no access to the backup server. Credentials shouldn't be reused between the two systems.

2

An automated backup solution would seem to be something that would mitigate the risk of a ransomware attack. Is that correct?
It can certainly help provide you with options during a ransomware attack. Two additional things to consider, however, are that at times a backup can be attacked, as well. First, current ransomware specifically looks for backup locations and tries to delete or encrypt them. If setup properly, the primary systems would not have access to the backups and would typically help to mitigate this risk. Second, new strands of ransomware are first taking your data prior to encrypting machines. This allows them to leverage the threat of releasing this data if you refuse to pay. In some cases, not only are attackers taking data and disclosing it, but they are also contacting a businesses customers to tell them that a company has ransomware. If you are interested, consider looking at news coverage of the RaceTrac & Washington DC Metro Police ransomware attacks.

3

Can you recommend affordable services to help us perform a security audit of our email and tech systems?
There are several options, but you may want to first consider what you need most. There are many options, such as vulnerability scanning, social engineering, technology audit, disaster recovery review etc. A great starting point is a conversation about your environment. It would help to walk through what is in place (hardware, software, backup, security) and what kind of information is being protected before knowing what services may be most beneficial. Let's connect and discuss briefly. Then, we should be able to help point you in the right direction. If you want to have a more direct conversation, send me an email to Jason.keith@saltmarshcpa.com

4

Does a 5-person company have to worry about ransomware?
Sadly, yes. If you use a computer and have information you want to protect, ransomware can find you. There are many examples of very small companies experiencing ransomware attacks. While the major attacks reported in the news were likely targeted persistently by hackers, most ransomware attacks are opportunistic. In most cases, emails and exploit kits are thrown at everything hoping that some will be successful. The good news is the smaller target you are the less likely someone is hunting specifically for you. Building in security, backup and recovery/insurance perspectives are still important but can be scaled to protecting a small company.

5

If the US gov't is successful in limiting the use of crypto for ransomware payments, what will be the alternative payment source?
To my knowledge, it is less about the use of crypto for ransomware payments and more about the end party receiving the payment. The US government is seeking to limit payments in any form (crypto or otherwise) for groups/individuals it has specifically identified on its OFAC list.

6

Is there a recommended backup platform for small businesses such as OneDrive, Google Drive, etc... that best mitigates the risk?
It is less about the specific platform and more about how you configure and utilize a backup system. Some strands of ransomware find backups and attempt to encrypt or delete those, as well. So, it becomes important to understand and manage how rights are assigned for backups. If you want to have a more direct conversation about this, send me an email to Jason.keith@saltmarshcpa.com

7

Ransomware preexisted bitcoin but it seems to be taking grief lately as the payment of choice. Is the criticism justified?
Crypto currency provides a nearly anonymous way of receiving payment. As probably the most dominant crypto currency, Bitcoin, gets the bad press. If money were forced to be moved through traditional banking systems, it would be easier to track and more likely to expose cyber criminals to heightened risks of being caught. Crypto currency was a key component to making ransomware pay. It is that ability to get paid which drives so many hackers into the space.