Ransomware-how much is your data worth?

By Bob Goldberg
RSPA General Counsel

We all have heard about the attorney who dies without a will, but what about the reseller that fails to backup its systems or keep its antivirus software or firewall up to date? The call was urgent, anxiety high, and the need for guidance immediate. A pop-up message appeared on the owner's desktop computer advising that his computer had been locked and unless he paid money to the entity within thirty-six hours he would not have access to the data on his device again.

The reseller was a victim of Locker Ransomware that locks the user interface, denying access to computing resources. Unlike Crypto Ransomware, the reseller's underlying system and files were not encrypted or touched. Through the assistance of another RSPA member, a technician was able to remove the Locker Ransomware and restore the owner's access to all his files, financial information and records. A good result in a situation that could have been devastating.

As indicated, Crypto Ransomware is malware designed to find and encrypt valuable data stored on the computer, making the data useless without a decryption key. A key that will be provided only if the demanded amount is paid. Without a regular backup schedule, the loss of files could be permanent. Consider what the cost would be to your business if your data were no longer available. Ransomware is becoming a greater threat each day.

Ransomware may enter your computer in several ways, although the actual method is not always clear. A common method is through redirected traffic from one web site to another. Often the redirected traffic originates from an adult content related website. Malicious advertisements, known as "malvertisements" can also release malware if clicked upon. Spam email has always been a source for malware, especially opening attachments in unfamiliar emails. Criminals pose as potential customers in order to gain attention to their email. Some emails will even employ capabilities to spread to all your contacts and seek to infect them as well. Downloaded infected software may also be a source.

Ransomware is not limited to personal computers and may also infect servers and mobile devices. Criminals seeking to extort money update their malware and techniques on a daily basis. Are you doing the same in terms of prevention? Do you have backup and disaster recovery plans? Often these plans do not extend to individual end users who may operate the most vulnerable equipment. Does the developer of your ERP software have safeguards in place? Is the data backed-up automatically? Is it stored safely in the cloud? If you are a victim of Crypto or Locker Ransomware, can your ERP provider have you up and running immediately without paying the criminal? Have you tested your plans to see if they operate as envisioned?

Ransom paid averages $300.00, however the demands are usually far greater. Amounts have been negotiated. Criminals often release a few files to demonstrate their control and ability to do so. Payment must be anonymous and is typically in Bitcoins or Litecoins. Although many ransoms are not reported, a study found that Ransomware had infected 68,000 computers a month.

As the industry moves to become "Trusted Advisors," security and Ransomware are excellent areas on which to counsel your customers. However, that is the second step. The first is to secure your own devices and systems. Create backup and disaster recovery plans and test them regularly. Avoid clicking malicious links or attachments, and patch exploitable software vulnerabilities. There are numerous tools available to remove Ransomware, but it is more important to prevent it in the first place. **c**