Issued 1/18/17

Ransomware: Should You Pay Up?

If you're a victim of ransomware, cybercriminals will encrypt your data and documents and demand a fee for them to unlock it. Once your data is locked, you face a tough choice: whether or not to pay. If you pay, will you really get your data back anyway? Here, we look at some tips on what to do if it happens to you.

The amount of the ransom will depend on the size of your organization, how much data is affected, and how likely, historically, it is that people in a similar position have paid. Easy targets with deep pockets are likely to get higher bills; whereas those who don't pay are typically less likely to be targeted, and therefore the ransom amounts will be closer to a nuisance fee, not something that's higher than a house payment.

Many ransomware campaigns use phishing emails as an entry point, and while user training makes it easier to spot these, the emails can be very convincing. For this reason, upstream email gateways, or even on the endpoint (depending on your environment) can spot rogue emails before they get a chance to act. As long as it's profitable, ransomware will continue to flourish. By taking these steps, we all can help reduce the likelihood of a payout, and defund the scammers. As soon as the money stops, they will too.