CARLTON FIELDS

Should Your Company Purchase Bitcoin to Pay a Cyber Ransom?

December 22, 2016

In recent years, businesses have witnessed the proliferation of cyber attacks, hacking, and other digital threats. One common threat is ransomware. In a ransomware attack, a company may lose access to critical systems and information until it pays a ransom or otherwise manages to defeat the malicious software affecting its operations. Due to their ability to help conceal the identities of the transacting parties, cryptocurrencies—and, in particular, bitcoin—have become a favorite medium of exchange for ransomware attackers. Opinions differ as to whether it is advisable to pay the ransom in the event of such an attack. Recent FBI guidance suggests that implementing prevention efforts and creating a business continuity plan are preferable solutions. Nevertheless, companies insufficiently prepared for a ransomware attack may find themselves with no choice but to pay the ransom. Companies at risk of a ransomware attack should understand how to obtain cryptocurrencies and how they work. Bitcoin, for example, may be purchased on numerous online exchanges such as Gemini (United States), GDAX (United States), Bitfinex (Hong Kong), Bitstamp (United States), Kraken (United States), Huobi (Hong Kong), and OKCoin (China). While exchanges are typically used by day traders, other sources of bitcoin such as Coinbase and Circle offer similar services, but are not designed for speculative trading. In addition, services such as LocalBitcoins offer users the ability to meet face to face to transact in bitcoin. Companies seeking to acquire cryptocurrency should carefully vet the purchase source before initiating a transaction. Most cryptocurrencies are stored in a digital wallet. To send a transaction from a wallet, the owner of that wallet must control the wallet's private key. Private keys can be stored in a variety of ways, each with its own inherent risks. For instance, if the key is stored on a vulnerable system, there is a risk the wallet could become sequestered when the ransomware attack begins, preventing the company from accessing its bitcoin. Alternatively, if the bitcoin is stored on an online exchange, the company must entrust its private key to a third-party, in which case the company risks losing access to its bitcoins if the third-party is compromised. Although such risks are generally less concerning to companies that intend to purchase bitcoin only as needed, given the ever-increasing threat of cyber attacks, companies may wish to include in their preparedness policies plans for acquiring bitcoin should the need arise. Companies that wish to implement such a plan should work carefully with

their management, IT department, and attorneys to ensure that risks, such as those mentioned above, are considered.

Authored By

Edmund J. Zaharewicz

Related Practices

Blockchain and Digital Currency
Consumer Finance
Cybersecurity and Privacy
Intellectual Property
Technology

Related Industries

Technology