Ransomware Resurgence

cyber security risk management pandemic

Summary: Ransomware has been a growing threat. But, the greater reliance on digital access from the pandemic has resulted in an alarming spike in attacks.

The film "All the Money in the World" depicts the real-life kidnapping of one-time-richest-man in-the-world J. Paul Getty's grandson -- and his controversial refusal to pay the ransom.

In the 50 years since this iconic story came to light, the issue of whether paying extortion is a good or bad idea has been hotly contested. Nowadays, extortion has moved to the digital realm. More hackers see ransomware schemes as a quick way to make cash, by gaining access to and locking up businesses' important data and systems, which they will release only when a ransom is paid.

Ransomware has been a growing threat for several years, for financial institutions (FIs) as well as businesses that have become the target of such attacks. With the onset of the pandemic and a sudden heightened reliance on digital access, a huge boom in ransomware has resulted.

Indeed such attacks on FIs increased more than 230% just between the beginning of February and the end of April of this year. One-quarter of victims said these hits caused significant damage, as well as generate a ransom payment, according to VMWare Carbon Black.

In late July, the FBI sent an alert warning of at least one ransomware variant, Netwalker. It had been gaining ground since June, and was "*taking advantage of the COVID-19 pandemic to compromise an increasing number of unsuspecting victims.*"

The reason for the leap in attacks is clear and multi-fold. Like all businesses right now, FIs are often working with a much more limited staff. They're still trying to provide open and easy access to customers who cannot go into a branch and they are experiencing much higher than normal demand on their online and mobile interfaces. So, what can community financial institutions do in the face of this increasing and expensive threat?

1. **Remind employees.** The most popular point of access is still the email attachment or hyperlink, clicked on by a naive employee. Remind staff members strongly and often that this could cause tremendous harm to the bank.
2. **Back up files.** Many bankers recommend the 3-2-1 method: make three copies of critical data; keep it backed up on two different types of storage; and keep at least one off-site copy. Any way you slice it, maintaining off-system copies limits the potential impact of ransomware threats.
3. **Update security features.** As more customers embrace digital banking access, it is incumbent on CFIs to make sure that their online and mobile operating systems are current and regularly updated.
4. **Keep track of privileged users.** Smart hackers know that if they can gain access to the credentials of a user with high-level access, they are more likely to gain access to the crown jewels of an institution's data. Hence privileged access should not only be limited, but security professionals should be more mindful of their own staff, bank executives, and anyone else who might have this level of access.

ASSESS PROFITABILITY THROUGH THE CRISIS

Profitability FIT is a profitability solution that measures performance on both a customer relationship and an account basis. With PPP and loan modifications, this is key. Contact us today for more information.