The Ugly Truth About Ransomware

by Steve Brown

Some of you may have seen Ransom, the 1996 crime thriller directed by Ron Howard. For those unfamiliar with the plot, the film stars Mel Gibson as a multi-millionaire airline owner whose son is kidnapped and held for a $2mm ransom. Against advice, the distraught dad prepares to pay the money, but the drop-off plan gets fouled up and the enraged patriarch takes matters into his own hands.

For those who haven't seen the movie, we won't give away the ending. But, we're sure the subject of ransom is one that resonates with many of our banks as for many companies today, ransomware is rampant. Ransomware is when cyber thieves send a link to employees and someone clicks, leading it to install malware that encrypts the computer. The thieves then demand money to unlock it. This attack approach is becoming an all-too-familiar theme. In recent months, attacks involving ransomware have surged so much that the FBI has issued new guidance and yet another alert about the threat.

According to a recent article by CNNMoney, the FBI has declared that the use of ransomware has reached an all-time high. In the first three months of 2016 alone, cybercriminals have reportedly raked in $209mm by extorting businesses and institutions to unlock computer servers. At that rate, ransomware will be a more than $1B a year criminal industry this year. In 2015 ransomware reportedly cost people and large companies at least $24mm, according to the FBI. That is a sizable chunk of change, but nowhere near what's expected for this year.

No company, large or small, for-profit or not-for-profit, is immune from attack. That is why bankers need to inform customers to stay abreast of the latest developments, including ways to prevent and respond to these egregious attacks. In the past, attacks were typically directed at individual computers, but that may be changing. Consider that the FBI is also reportedly looking into a new strain of ransomware known as MSIL/Samas. The agency said this strain seeks to encrypt data on entire networks, a disquieting development from thieves' typical modus operandi.

For companies who are ransomware victims, there's a lot of controversy mired around whether to pay or not to pay. For its part, the FBI does not publically want companies to pay. Meanwhile, an FBI agent at a security conference in Boston last year caused a stir after he was quoted as suggesting the FBI tells some victims to just pay the ransom. In the wake of the media firestorm he sparked, the FBI came out strongly stating that the agency doesn't advise victims whether or not to pay any ransom. However, in March of this year, a unit chief in the FBI's cyber division, speaking on an FBI podcast and radio show, advised against paying a ransom. The argument goes that it encourages more attacks and since you are dealing with crooks, they may not unfreeze your computer even if you do pay.

To ward off attack, the FBI advises individuals and businesses to keep their anti-virus software active and up-to-date. Next, the agency also advises patching operating systems and applications promptly. Third, is to be suspicious of unsolicited emails, no matter how pertinent they may seem. Fourth, do not open attachments or click on links in emails, especially if they are unexpected. Fifth, make regular

backups, and keeping at least one backup offline. Finally, if you do become a victim of ransomware, immediately call your local FBI office.

Ransomware isn't going away, but you can mitigate risk by taking these suggested precautions. If criminals still manage to worm their way in and hold your data hostage, exercise extreme caution when taking matters into your own hands. Unlike the movies, real life doesn't always produce the happily-ever-after.

BANK NEWS

M&A Activity

1) Coastal Carolina National Bank ($176mm, SC) will acquire VistaBank ($110mm, SC) for about $12.2mm in cash (25%) and stock (75%) or roughly 1.01x tangible book.

Freelance Jobs

Research by Deloitte of thousands of business and HR leaders worldwide on human capital finds that today about 33% of US workers are freelancers (think Uber and Airbnb), a number expected to reach 40% by 2020.

IRS Hiring

The IRS is reportedly hiring 700 enforcement employees as it seeks to fill enforcement gaps and address attrition.

Car Crash

Fitch Ratings reports the rate of seriously delinquent subprime car loans jumped above 5% in Feb, the highest level in 20Ys.

Not Retiring

The Bureau of Labor Statistics reports nearly 20% of Americans 65 or older are currently working, the highest level since the 1960s.

Spending Reality

Research by the EBRI on retirement finds the actual amount of money retirees spend compared to what they expected to spend is: about the same (38%); somewhat higher (20%); much higher (18%); somewhat lower (13%); and much lower (8%).