CPA
Practice Advisor

accident) onto a business computer or network. The perpetrators of the scam then lock down the computers and threated to erase key data if the business doesn't pay a ransom.

Mar. 21, 2016

Cases of ransomware are on the rise in businesses of all sizes, according to a new

The new report by cloud IT services provider Intermedia surveyed nearly 300 expert IT consultants[1] for their perspectives on the scope and costs of this trending malware.

The experts’ opinions contradicted conventional wisdom regarding the threat associated with ransomware: Business downtime was ranked as a far bigger cost than the ransom itself. The survey also found that ransomware is affecting bigger businesses and multiple victims within each business.

Key Finding #1: Downtime is more detrimental than ransom costs
A ransomware outbreak creates two hard choices for businesses: Either spend multiple days recovering locked files from backups, or pay ransom to an organized crime syndicate.

In either scenario, though, businesses are likely to face significant user downtime that overshadows the cost of the ransom. 72 percent of infected business users could not access their data for at least two days following a ransomware outbreak, and 32 percent lost access for five days or more.

As a result, experts observed significant data recovery costs, reduced customer satisfaction, missed deadlines, lost sales and, in many cases, traumatized employees.

This widely observed downtime implies that few companies possess a business continuity solution for a ransomware outbreak. Such a solution enables users to remain productive during a ransomware outbreak. It offers the capabilities to instantly roll back an archive of files to their uninfected state and to immediately access those clean files from alternate devices.

Richard Walters, SVP of Security Products at Intermedia, stated, “In the age of ransomware, what matters is how quickly employees are able to get back to work. Traditional backup and file sharing solutions are increasingly inadequate when it comes to addressing this growing concern, putting businesses at risk. Modern

networks: 86 percent of outbreaks affected two or more employees, and 47 percent spread to more than 20 people.

Felix Yanko, President at Technology & Beyond, added, “The world is becoming more cyber-aware, but ransomware’s depravity keeps it three steps ahead. CryptoLocker, for instance, will take down multiple offices in one sweep, should it infect a shared server. A business that tries to restore from a ransomware attack off of traditional backup usually loses weeks of work due to lost files, plus a day or more of downtime while computers are wiped and reloaded. Companies must have measures in place to mitigate the devastation of ransomware.”

Key Finding #3: Ransomware is a growth industry
The threat of ransomware is rapidly growing. According to Intermedia’s report, 43 percent of IT consultants have had their customers fall victim to ransomware, 48 percent saw an increase in ransomware-related support inquiries and 59 percent expect the number of attacks to increase this year.

Walter Chamblee, Director of Information Technology at Signaturefd.com, said, “Ransomware attacks are on the rise and are growing in complexity. Without the right protection measures in place, ransomware can be majorly disruptive to a business. In these cases, it’s the user downtime and the hassle for IT that’s far costlier, even if you pay the ransom.”

Digital Currency • Security • Small Business • Technology

(NASBA) as a sponsor of continuing professional education on the National Registry of CPE