CARBONITE

The rise of ransomware

The rise of ransomware

Small business owners have enough on their plates, such as wearing many different hats and managing the critical day-to-day elements of their businesses. Security can easily become a low priority. Many brush off high-profile cyber-attacks frequently reported in the media as they assume most are happening to large, global brands, governments or celebrities.

But there's a new and growing threat targeting small and midsize business owners directly.

Business owners are coming into work only to be locked out of their own computers and systems. Their essential data is being held for literal ransom, with payment as the only foreseeable way to recover their valuable information.

Between January and September 2016, the Justice Department reported 4,000 attacks of ransomware, which is a type of malware that prevents users from accessing their data until they pay a fee. This is quadruple the amount of such attacks from the previous year. New data from an anonymous source suggests ransomware criminals raked in $1 billion in 2016 from ransomware attacks.

Despite the uptick of ransomware attacks, small and midsize businesses are not taking sufficient measures to combat ransomware.

Unfortunately, ransomware is lucrative and hard to trace.

Since the inception of ransomware, hackers have become increasingly more sophisticated in their attempts and strategies to collect valuable data from companies of all sizes. It's challenging to find the criminals behind the attacks because most often attackers are being paid in untraceable virtual currency, like Bitcoin. Even those with little hacking experience can get involved through ransomware as a service (RaaS), which provides novice hackers with everything they need to launch an attack. Attackers are sophisticated enough to also have "customer service" representatives to help their victims "navigate payments," answering FAQs and more.

A new report from Carbonite and the independent research group The Ponemon Institute captures the increasing risks U.S. small and midsize businesses face from ransomware. From this research, businesses will gain new insights into how cybercriminals continue to profit, as well as the security measures to put in place that will help mitigate ransomware threats and secure their most valuable asset—their data.

The following report details the findings from a study of 618 individuals in small to midsize organizations who have responsibility for containing ransomware infections within their organization.

The rise of ransomware

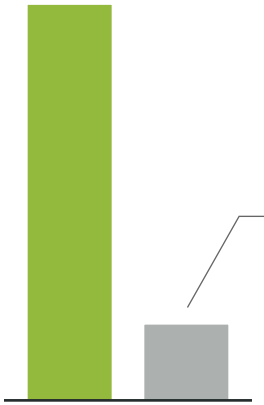
The preparation gap

More than half of companies surveyed believe they are too small to be a target for ransomware. These misperceptions can have costly affects when preparing for and investing in ransomware prevention procedures and technologies. In fact, the reality is that the severity and volume of ransomware infections have increased over the past 12 months.

However, when pressed about their vulnerability, 68% of survey respondents believe their company is "very vulnerable" or "vulnerable" to a ransomware attack.

This minimal preparation can largely be credited to a lack of confidence in existing technology systems or not having the right technology in place to combat these threats in the first place.

Many companies claim they don't have the appropriate technology in place to detect ransomware infections, putting their company at a great risk. Only 27% of respondents are confident their current antivirus software will protect their company from ransomware. Even more alarming, many infections are going unnoticed. One or more ransomware infections go undetected per month and are able to bypass the organization's IPS and/or AV systems (according to 44% of respondents).



66%

of respondents rate the threat of ransomware as "very serious."

13%

of those surveyed rate their company's preparedness to prevent ransomware as "high."

48%

of companies paid the ransom demanded.

42 hours

on average, was spent dealing with and containing a ransomware incident.

60%

of respondents would prefer to go without Wi-Fi for a week than deal with a ransomware attack.

The rise of ransomware

How are companies affected by ransomware?

Ransomware is no longer something that is a distant or unlikely risk. In fact, more than half of companies represented in this research (51%) experienced a ransomware attack. This trend is only continuing and 2017 is hailed to be the year of ransomware.

But how exactly are companies affected by ransomware attacks? How devastating can it be for small and midsize businesses? The results are astounding:

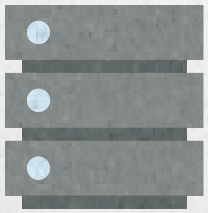
Financial loss

The top consequence of a ransomware attack is financial. Companies surveyed experienced an average of four ransomware attacks and paid an average of $2,500 per attack. And attackers didn't provide much time. Just under half of respondents said their attackers demanded payment in fewer than two days. Due to lack of preparation, many companies pay this ransom when faced with such a threat. According to the research, 48% of companies paid the ransom demanded.

Extended consequences

Beyond the significant financial consequences, businesses needed to invest in new technologies, they lost customers, and they lost money due to downtime. Moreover, nearly half of respondents believe one ransomware incident can make a company more vulnerable to future attacks.

The rise of ransomware



33%
needed new technologies

32%
lost customers

32%
lost money

Data exfiltration

Often, data exfiltration occurred from devices —meaning unauthorized transfer of data from a computer or server.

Reputational risk

Even given the great financial and business hardships, companies were reluctant to report ransomware incidents to law enforcement because of concerns of negative publicity.

In 2016, several high-profile ransomware attacks demonstrated the severity of this threat—from the San Francisco Municipal Transportation attack, a costly $73,000 demand, to the multitude of hospitals attacked.

More than half of companies represented in this research experienced a ransomware attack. This trend is only continuing and 2017 is hailed to be the year of ransomware.

The rise of ransomware

How do you protect against ransomware?

The question is no longer "if" but "when" a ransomware attack will happen against your company. So how can you be prepared when the ransom for your essential data is demanded?

According to this research, if a company didn't pay ransom, it was because it had full and accurate backup. Respondents noted that full and accurate backup is the best defense against ransomware.

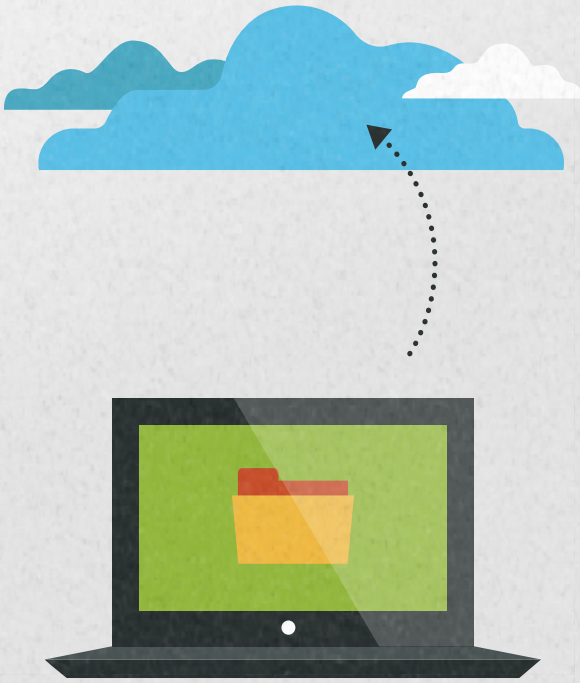
68% of respondents in companies that experienced a ransomware incident say it is "essential" or "very important" to have full and accurate backup as a defense for future ransomware incidents.

Further, employee education is critical. The most common way ransomware is unleashed is through phishing/social engineering and unsecure websites. If employees are properly trained to spot these tactics, companies will be less likely to experience a ransomware attack.

29% of respondents are confident their employees can detect risky links or sites that could result in a ransomware attack.

The bottom line is this: The threat isn't going away as long as ransoms continue to get paid and hackers are making money. Understanding this reality and prioritizing investments in training and education for employees as well as investing in backup with versioning capabilities is the first—and strongest—line of defense in the fight against ransomware.

For more information, download our free ransomware preparedness guide today.



Full and accurate backup is the best defense against ransomware.

Learn more

Phone: 800-683-4667
Email: DataProtectionSales@carbonite.com
www.carbonite.com

Survey methodology

This study was conducted by Ponemon Institute on behalf of Carbonite between September 5 and 19, 2016, among 618 individuals in U.S. small to midsize organizations who have responsibility for containing ransomware infections within their organization.

About Carbonite

Carbonite (Nasdaq: CARB) is a leading provider of cloud backup and restore solutions for small and midsize businesses. Together with our partners, we protect millions of devices and their valuable data for businesses and individuals around the world who rely on us to ensure their important data is secure, available and useful.

About Ponemon Institute

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. The firm's mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.