CARBONITE

January 24, 2017

Carbonite Research: Majority of U.S. Businesses Unprepared to Handle a Ransomware Attack

Sixty-six percent of IT professionals identify ransomware as a serious threat, yet only 13 percent say their company is prepared to handle it

BOSTON, Jan. 24, 2017 (GLOBE NEWSWIRE) -- Businesses consider ransomware a very serious threat; however, most are ill prepared to handle a ransomware attack, according to a new study released today by Carbonite (NASDAQ:CARB). The research report, The Rise of Ransomware, which was conducted by The Ponemon Institute, details the malicious software's cause and effect chain and offers solutions to mitigate ransomware risks.

The data represents insights from those responsible for containing ransomware infections within their organizations, including IT professionals and IT managers, who primarily report to the Chief Information Officer (CIO). According to these respondents, current technologies aren't considered sufficient to prevent ransomware infections, leading many companies (48 percent) to pay the ransom.

The majority of IT professionals believe that backup is critical to their ransomware protection strategy. Sixty-eight percent of IT professionals in companies that experienced a ransomware incident say it is essential (30 percent) or very important (38 percent) to have full and accurate backup as a defense against future ransomware incidents.

"This study reveals a startling prevention gap: most businesses are either underprepared for an attack — or even worse — underestimate the risk ransomware places on their broader organizations," said Dr. Larry Ponemon, chairman and founder of the Ponemon Institute.

According to the data, ransomware risks are significant. The primary losses businesses suffer include:

- **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 time is of the essence: 46 percent of respondents said their attackers demanded payment in fewer than two days.
- **Extended consequences:** Beyond the significant financial consequences, businesses needed to invest in new technologies (33 percent), lost customers (32 percent) and lost money (32 percent) due to downtime.
- **Data exfiltration:** Often, data exfiltration occurred from devices — meaning unauthorized transfer of data from a computer or server. On average, 42 hours were spent dealing with and containing a ransomware incident.
- **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.

"Ransomware will continue to outpace the rate at which businesses can defend against it," said Norman Guadagno, chief evangelist at Carbonite. "If businesses take one insight away from this research, it is that you are not alone in feeling vulnerable to ransomware attacks. Now is the time to act: educate staff on simple measures you can take to avoid an attack and update your data protection measures now, before it's too late."

Resources
Get the entire report of survey results by joining a webinar hosted by Carbonite and The Ponemon Institute. Join here: http://get.evault.com/webinar-the-rise-of-ransomware.html

To learn more about how to protect your company against cybersecurity threats visit: https://www.carbonite.com/en/cloud-backup/business/resources/small-business-data/what-is-ransomware/

For the latest news, tips and tricks on ransomware visit FightRansomware.com and follow @FightRansomware on Twitter.

Learn why backup software is essential for business, and get best practices to manage and protect small business data by visiting Carbonite's suite of resources:

- Subscribe to the Carbonite blog
- Follow Carbonite on Twitter
- Follow Carbonite on LinkedIn

Survey Methodology
This study was conducted by Ponemon Institute on behalf of Carbonite between September 5 and 19, 2016 among 618 individuals in small to midsized organizations in the U.S. 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.

Media Contacts:
Sarah King, Carbonite
617-421-5601
media@carbonite.com

Kelsey Shively, Weber Shandwick (for Carbonite)
425-306-2090
wswnacarbonite@webershandwick.com