Small Business Owners Suffer from False Sense of Cyber Security
Monday, October 24, 2011 12:49:41 PM (GMT)

Survey Reveals That More Than 8 in 10 U.S. Small Businesses Believe Their Firms Safe From Cyber Threats Yet Almost 80% Have No Formal Security Policies In Place

WASHINGTON, Oct. 24, 2011 /PRNewswire/ -- The majority of small business owners believe Internet security is critical to their success and that their companies are safe from ever increasing cyber security threats even as many fail to take fundamental precautions, according to a new survey of U.S. small businesses sponsored by Symantec and the National Cyber Security Alliance and conducted by Zogby International.

(Logo: http://photos.prnewswire.com/prnh/20110504/DC95016LOGO)

(Logo: http://photos.prnewswire.com/prnh/20111007/DC82477LOGO)

(Logo: http://photos.prnewswire.com/prnh/20101004/DC76016LOGO)

The survey found that two-thirds (67%) of U.S. small businesses have become more dependent on the Internet in the last year and 66% are dependent on the network for their day-to-day operations. What's more, 57% of firms say that a loss of Internet access for 48 hours would be disruptive to their business and 38% said it would be "extremely disruptive" and 76% say that most of their employees use the Internet daily.

The vast majority of small business owners think their company is cyber-secure as 85% of respondents said their company is safe from hackers, viruses, malware or a cyber-security breach and seven in ten (69%) believe Internet security critical to their business's success. Additionally, a majority (57%) of small businesses believe that having a strong cyber security and online safety posture is good for their company's brand.

Yet a closer look reveals that most small businesses lack sufficient cyber security policies and training. Seventy-seven percent said they do not have a formal written Internet security policy for employees and of those, 49% reported that they do not even have an informal policy. More small business owners also said they do not provide Internet safety training to their employees than said they do – to a tune of 45 versus 37%. And a majority of businesses (56%) do not have Internet usage policies that clarify what websites and web services employees can use and only 52% have a plan in place for keeping their business cyber-secure.

At the same time, small businesses may not understand how to respond to online threats or the danger they pose. For example, 40% of small businesses say that if their business suffered a data breach or loss of customer or employee information, credit card information or intellectual property, their business does not have a contingency plan outlining procedures for responding and reporting it. Two-fifths (43%) also say they do not let their customers and partners/suppliers know what they do to protect their information.

The respondents' sense of security is especially unwarranted given that 40% of all targeted cyber attacks are directed at companies with less than 500 employees, according to Symantec data (http://bit.ly/njTeMU). In 2010, the average annual cost of cyber attacks to small and medium sized business was $188,242. What's more, statistics show that roughly 60% of small businesses will close up within six months of a cyber attack (http://www.businessinsider.com/the-challenges-in-defending-against-malware-2011-9). According to the Norton Cybercrime Report, the total cost of cyber crime to consumers and small business owners alike, is greater than $114 billion annually (http://norton.com/cybercrimereport).

"We recognize that most small business owners are focused on running their businesses, and have limited resources and IT staff dedicated to managing their cyber security needs. Unfortunately, cyber criminals are increasingly making small businesses their targets, knowing they are likely to have fewer safeguards in place to protect themselves," said Cheri McGuire, Vice President of Global Government Affairs and Cybersecurity Policy at Symantec. "It's important for small businesses to educate their employees on the latest threats and what they can do to combat them. Education, combined with investment in reliable security solutions, provides small business owners with a well-rounded approach to protecting their businesses and managing cyber risk."

"The threats grow in number and complexity each day, but too many small business owners remain naively complacent," said NCSA Executive Director Michael Kaiser. "The stakes are high for individual businesses and the nation as a whole: a single malware attack or data breach can be fatal to a small enterprise but the collective vulnerability of all our businesses is a major economic security challenge."

The survey also found that 69% of their businesses handle customer data while about half (49%) handle financial records, one-third (34%) handle credit card information, one quarter (23%) have their own intellectual property, and one in five (18%) handled intellectual property belonging to others outside their company. When asked to rank the top concern of small business owners while their employees are on the Internet, 32% reported viruses, 17% spyware/malware and 10% reported loss of data. Yet only 8% are concerned about loss of customer information, 4% about loss of intellectual property and only 1% worry about loss of employee data, even though cyber security experts believe the loss of any of this kind of information would be devastating to a business.

Overall, cyber vulnerabilities and threats are steadily on the rise, according to the "Symantec Internet Security Threat Report, Trends for 2010," the latest version of the company's annual cyber security study. For example, the report found a 9% increase in web-based attacks (http://bit.ly/qGMNPO).

In addition to struggling with the basics, many small businesses are failing to keep up with the increasing adoption of mobile and social media platforms. Just 37% of U.S. small businesses have an employee policy or guidelines in place for remote use of company information on mobile devices and just over one in three (36%) maintains a policy for employees' use of social media.

Social networking platforms now provide hackers with the ability to easily research targets and develop powerful social engineering attacks. Smart phones and other mobile devices are also poised to play a large role with a sharp 42% rise last year in the number of reported security vulnerabilities, according to Symantec's 2010 report.

Experts say that strong password protections, protecting USB devices and wireless networks matter to a firm's security posture. Yet, a majority of firms (59%) do not use multifactor authentication (more than a password and logon) to access any of their networks. Only half (50%) reported they completely wipe data off their machines before they dispose of them and 21% never do. Two-thirds (67%) of U.S. small businesses allow the use of USB devices in the workplace.

The study was an online survey of 1,045 small business owners conducted by Zogby International from September 9-21, 2011. The survey had a margin of error of +/- 3.1 percentage points. For a full report on this survey please visit www.staysafeonline.org.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

About Norton from Symantec

Symantec's Norton products protect consumers from cybercrime with technologies like antivirus, anti-spyware and phishing protection-- while also being light on system resources. The company also provides services such as online backup and PC tuneup, and family online safety. More information about solutions available for businesses with ten or less PCs can be found at smallbusiness.norton.com.

About The National Cyber Security Alliance

The National Cyber Security Alliance is a non-profit organization. Through collaboration with the government, corporate, non-profit and academic sectors, the mission of the NCSA is to empower a digital citizenry to use the Internet securely and safely protecting themselves and the technology they use and the digital assets we all share. NCSA works to create a culture of cyber security and safety through education and awareness activities. NCSA board members include: ADP, AT&T, Bank of America, Cisco Systems, EMC Corporation, ESET, Facebook, General Dynamics Advanced Information Systems, Google, Intel, Lockheed Martin Information Systems & Global Services, McAfee, Microsoft, PayPal, Science Applications International

Corporation (SAIC), Symantec, Verizon and Visa. Visit www.staysafeonline.org for more information.

About National Cyber Security Awareness Month

National Cyber Security Awareness month now in its eighth year is a coordinated effort of the National Cyber Security Alliance, The Department of Homeland Security (DHS), and The Multi-State Information Sharing and Analysis Center (MSISAC).

About STOP. THINK. CONNECT.

The campaign was developed by the STOP. THINK. CONNECT. Messaging Convention, a public-private partnership established in 2009 and led by The Anti-Phishing Working Group (APWG) and National Cyber Security Alliance (NCSA) to develop and support a national cybersecurity awareness campaign. In October 2010 the White House, U.S. Department of Homeland Security and Messaging Convention launched the campaign. The Department of Homeland Security provides the Federal Government's leadership for the campaign. Industry, government, non-profits and education institutions participate in STOP. THINK. CONNECT. Learn how to get involved with the Stop. Think. Connect. Facebook page at https://www.facebook.com/STOPTHINKCONNECT. and the campaign website at www.stopthinkconnect.org.

SOURCE National Cyber Security Alliance

Contacts: Aimee Larsen Kirkpatrick, National Cyber Security Alliance, +1-202-570-7431, aimee@staysafeonline.org; or Krista Alestock, 463 Communications, +1-202-463-0013 x209, krista.alestock@463.com
Countries: United States
Industries: High Tech Security, Multimedia, Internet & Wireless Technology
Languages: English
Primary Identifiers: NLOK-US, 064C2X-E
Related Identifiers: NLOK-US, 064C2X-E