April 21, 2016

Paychex Urges Businesses to Make Online Security a Priority Year-Round

ROCHESTER, N.Y.--(BUSINESS WIRE)-- Small businesses are just as vulnerable to data breaches and cyber thefts as large corporations, perhaps even more so because they often lack the technology expertise to adequately safeguard data. Paychex, Inc, a leading provider of integrated human capital management solutions for payroll, HR, retirement, and insurance services, urges employers to protect their valuable data by proactively boosting online security now and remaining vigilant year-round as new threats continue to arise.

“With access to significant amounts of sensitive data, including the personally identifiable information of employees, small businesses make an attractive target for hackers,” said Todd Colvin, security director at Paychex. “Small businesses can significantly reduce the risk of a breach or attack any time of the year by creating a cyber security culture that makes protecting online data a top priority.”

Cyber Theft by the Numbers

Statistics compiled by the National Cyber Security Alliance and Mandiant, a cyber security authority, paint a disturbing portrait of business vulnerability:

- Almost 50 percent of small businesses have experienced a cyber attack.
- More than 70 percent of attacks target small businesses.
- 69 percent of businesses learn of a breach from an outside entity such as law enforcement.
- On average, attackers have access to breached systems for 205 days before being detected.

Tips to Stay Ahead of Cyber Criminals

When it comes to keeping your secure data safe, a multi-faceted approach is best. Consider the following tips to improve data security at your business:

- **Start with training.** Employees often make critical cyber security mistakes, such as clicking on a fraudulent link included in a phishing scam, because they lack the knowledge and training to recognize warning signs. The most cost-effective protection is a high level of employee awareness through information-security training. If employees encounter something suspicious online, they should feel empowered to say something. A comprehensive incident response plan stressing the need to immediately contact a manager or IT team may significantly curtail the effects of an attempted data breach.
- **Reward security-conscious behavior.** When an employee spots an intrusion attempt

and notifies the designated contact right away, salute that action in a public employee gathering or all-staff email. Consider a small rewards program for employees who regularly sign up for ongoing training (which reduces the "mandatory" nature for such training).

- **Strengthen and regularly change passwords.** A simple but effective step in thwarting online criminals is to strengthen and regularly change passwords and security questions that provide access to account information. Consider employing a layered defense that makes it more difficult for cyber-criminals to access sensitive information.
- **Review accounts regularly.** As an employer, if you don't make a habit of reviewing accounts regularly, rethink that practice. With cyber criminals often having access to stolen data for months on end, recognizing an account irregularity could be the first clue that something is amiss.
- **Limit access to personally identifiable information (PII) and protected health information (PHI).** A passive approach to internal controls around PII and PHI could have severe consequences for businesses. Only employees whose job responsibilities explicitly require access to PII and PHI should be granted it.

"Threats to business data are an unfortunate reality in today's marketplace," said Colvin. "Instilling a cyber security culture with proper training and reinforcement will go a long way toward protecting sensitive information--and preserve the integrity of your business."

Helpful Resources

In addition to making a concerted effort to constantly improve online security, Paychex offers these reminders and suggestions:

- The Internal Revenue Service (IRS) **does not** initiate contact with taxpayers by email or social media, and any unexpected call from someone claiming to be from the IRS threatening arrest for failure to pay immediately is a scam.
- The U.S. Department of Homeland Security has a website dedicated to online security with tip sheets, workplace materials, and planning guides at Stop. Think. Connect. Small Business Resources.
- A comprehensive list of identity theft protections and victim resources can be found on the IRS' official website, including online security pointers on the Tax Tips site.

Paychex Participates in IRS Pilot Program

Although employers are critical to protecting the confidential data of the business and its employees, they are not alone. As part of its efforts to advance the latest safeguards in protecting client data, Paychex participated in an IRS Pilot Program this tax season to test verification codes on Forms W-2 for select clients. The code is based on select data elements on each Form W-2 and a unique IRS algorithm. This may potentially help reduce Form W-2 tax fraud in the future, which has escalated to billions of dollars annually.

"Leaving your business data exposed to cyber attacks is simply too great a risk to ignore," said Colvin. "The best defensive strategy is creating a cyber security culture in the workplace

and taking specific actions and precautions during periods when the threat of cybercrime is higher than usual."

About Paychex

Paychex, Inc. (NASDAQ: PAYX) is a leading provider of integrated human capital management solutions for payroll, HR, retirement, and insurance services. By combining its innovative software-as-a-service technology and mobility platform with dedicated, personal service, Paychex empowers small- and medium-sized business owners to focus on the growth and management of their business. Backed by more than 40 years of industry expertise, Paychex serves approximately 590,000 payroll clients across 100 locations and pays one out of every 15 American private sector employees. Learn more about Paychex by visiting www.paychex.com, and stay connected on Twitter and LinkedIn.

View source version on businesswire.com:
http://www.businesswire.com/news/home/20160421006105/en/

Media:
Paychex, Inc.
Lisa Fleming, 585-387-6402
lfleming@paychex.com
@PaychexNews
or
Eric Mower + Associates
Danielle Gerhart, 315-413-4258
dgerhart@mower.com

Source: Paychex, Inc.