November 13, 2017

After Equifax: New Survey Shows Security Professionals Expect the Worst and Claim They Are Prepared

Nearly 50% of IT pros are bracing for a cyberattack, yet 89% profess confidence in their cybersecurity stance

NEW YORK, Nov. 13, 2017 (GLOBE NEWSWIRE) -- Varonis Systems, Inc. (NASDAQ:VRNS), a leading provider of software solutions that protect data from insider threats and cyberattacks, today released findings from an independent survey exploring security practices and expectations in the wake of the massive Equifax breach. The survey, which polled 500 IT decision makers in the UK, Germany, France and U.S., highlights an alarming disconnect between security expectations and reality.

An infographic accompanying this announcement is available at http://www.globenewswire.com/NewsRoom/AttachmentNg/ff245771-0c7f-4d17-824b-d63826f690d3

The vast majority (89%) express confidence in their cybersecurity stance and feel that their organization is in a good position to protect themselves from attack. Yet in the months after WannaCry, 4 in 10 organizations are not taking critical steps to lock down sensitive information, putting them at risk from data loss, data theft and the next ransomware attack.

Nearly half of respondents (45%) believe their organization will face a major, disruptive attack in the next 12 months.

Looking ahead to 2018, data theft and data loss were cited as top concerns for organizations. Other notable findings include:

- 25% reported their organization was hit by ransomware in the past two years.
- 26% reported their organization experienced the loss or theft of company data in the past two years.
- 8 out of 10 respondents are confident that hackers are not currently on their network.
- 85% have changed or plan to change their security policies and procedures in the wake of widespread cyberattacks like WannaCry.

"It is encouraging that IT professionals are understanding that it's a matter of when, not if, their organization will be hit with a damaging cyberattack. However, their level of confidence when it comes to security is inconsistent with what we see in practice," said John Carlin, former Assistant Attorney General for the U.S. Department of Justice's National Security Division and currently chair of Morrison & Foerster's global risk & crisis management practice. "The reality is that businesses are consistently failing to restrict access to sensitive information and are regularly experiencing issues such as data loss, data theft and extortion in the form of ransomware."

The survey also showed major differences on cybersecurity policies and tendencies by country. Key findings in this area include:

- Only 66% of U.S. organizations and 51% of EU-based organizations surveyed fully restrict access to sensitive information on a "need-to-know" basis. Organizations in Germany are the least likely to restrict access (38%).
- A majority (67%) of respondents reported their organizations have cybersecurity insurance policies. They are least prevalent in the U.S. (62%) and most common in France (75%).
- German organizations have been hit particularly hard by ransomware, with 34% affected in the past 2 years.

"Attackers are upping their game, using more sophisticated, blended attacks like WannaCry and NotPetya that make use of multiple attack vectors," said Varonis CMO David Gibson. "At the same time, valuable data remains vulnerable to attacks that require little to no sophistication, like disgruntled employees snooping through overly accessible folders. While it's heartening that major security incidents are inspiring preparedness, if the past year is any indication, it is unlikely the actual security of these organizations aligns with perception."

The independent survey on top concerns, approaches and experiences of IT professionals involved in cybersecurity was commissioned by Varonis and conducted by Survey Sampling International. Respondents were 500 IT decision makers from the United Kingdom, France, Germany and the United States from organizations with 1,000+ employees. The survey was conducted from September 28 - October 6, 2017.

Additional Resources

- Read the full survey findings: https://www.varonis.com/learn/cybersecurity-expectations-vs-reality-survey/
- For more information on Varonis' solution portfolio, please visit www.varonis.com
- Visit our blog, and join the conversation on Facebook, Twitter, LinkedIn and YouTube.

About Varonis
Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Through an innovative software platform, Varonis allows organizations to analyze, secure, manage, and migrate their volumes of unstructured data. Varonis specializes in file and email systems that store valuable spreadsheets, word processing documents, presentations, audio and video files, emails, and text. This rapidly growing data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property, and confidential employee, customer or patient records. IT and business personnel deploy Varonis software for a variety of use cases, including data security, governance and compliance, user behavior analytics, archiving, search, and file synchronization and sharing. With offices and partners worldwide, Varonis had approximately 5,950 customers as of September 30, 2017, spanning leading firms in financial services, healthcare, public, industrial, insurance, energy and utilities, media and entertainment, consumer and retail, technology and education sectors.

News Media Contacts:
Rachel Hunt
Varonis Systems, Inc.
877-292-8767 (ext. 4247)
Email: rhunt@varonis.com

Mia Damiano
Merritt Group
703-390-1502
Email: damiano@merrittgrp.com

Investor Relations Contact:
Yun Kim
Varonis Systems, Inc.
646-640-2149
Email: kimy@varonis.com