Enterprises Risk All in Massive IoT and OT Security Compliance Time Bomb

November 8, 2017

SAN JOSE, CA -- (Marketwired) -- 11/08/17 -- ForeScout Technologies (NASDAQ: FSCT)

- *Line-of-business (LoB) leaders and IT are anxious about IoT/OT security due to concern about negative outcomes of a security breach*
- *Enterprises are not confident that they can pass an audit as 82 percent cannot identify all of their IoT/OT devices*
- *IT and LoB leaders are not aligned on IoT/OT security management*

ForeScout Technologies (NASDAQ: FSCT), a leading Internet of Things (IoT) security company, today revealed new findings about the impact IoT and operational technology (OT) are having on organizations and the cybersecurity dilemmas they are causing within security and LoB teams. The commissioned survey, conducted by leading independent analyst firm Forrester Consulting on behalf of ForeScout, unveiled that security and LoB leaders are experiencing high levels of anxiety due to IoT/OT security concerns, largely due to the negative business ramifications a security failure can have on critical business operations. Furthermore, the majority of these organizations (82%) struggle to identify all of their network-connected devices, and when asked who is primarily responsible for securing IoT, IT and LoB leaders did not have a clear answer or delineation of ownership.

"The survey results demonstrate a dynamic shift in the way organizations are starting to think about security and risk as it relates to IoT. Each new device that comes online represents another attack vector for enterprises and it only takes one device to compromise an entire network and disrupt business operations, which can impact the bottom line," said Michael DeCesare, president and CEO at ForeScout. "Securing IoT is not just a cybersecurity issue, it is a business issue and operating at any risk level is too much. Enterprises need full visibility."

According to the survey results collected from over 600 global enterprise businesses, 77 percent of companies agree that the increased usage of connected devices creates significant security challenges. As a result, 76 percent of respondents said IoT-related anxieties are forcing them to rethink their IT and LoB security strategies.

"Businesses can already see the benefits of connecting devices to the network that were not traditionally connected to improve their business processes and functions," according to the commissioned Forrester Consulting study, Fail To Plan, Plan To Fail. "Technological advancements have given rise to a deluge of new types of connected devices -- i.e., Internet of Things (IoT) -- which, in turn, introduce new security threats that enterprises are ill-equipped to combat and even recognize. With increased funding and a new security strategy focused on visibility and compliance, companies can begin taking strides forward to reduce their anxiety about IoT and regain confidence that their networks are secure."

Key findings include:

IoT Anxiety is Consuming Security Professionals
IoT is causing a new level of complexity and the potential for negative business impacts if a security failure occurs. Survey results show that over half of the respondents (54%) stated that they have anxiety due to IoT security, with LoB leaders having higher amounts (58%) compared to their IT counterparts (51%). Understanding the magnitude that a breach can have on enterprise operations and not receiving high-level assurances from IT that their devices are secure, can cause higher levels of anxiety in LoB leaders than IT. In addition, overall distress is due to added costs and time needed to manage these devices as well as a lack of security skills.

Barriers and Compliance Complications are Leading to Risk
IT and LoB respondents cited budget constraints (IT 45%; LoB 43%) as the greatest barrier to investing in IoT security, followed by senior leadership skepticism. Without the added investment, security professionals continue to rely on their traditional security approach to protect IoT/OT (40%). This strategy prevents organizations from being able to identify all network-connected devices, which opens the door for greater security risk and potential compliance complications. In fact, if audited, 82 percent said they could not identify 100 percent of the devices connected to their network. Additionally, over half of respondents (59%) cited that they are willing to tolerate a medium to high risk level in relation to compliance requirements for IoT security. A true concern as 90 percent of companies are expecting to see their volume of connected devices increase over the next few years.

IoT/OT Triggers Need for a New Symb-IoT-ic Relationship Across Business Leadership
The study supports a clear disconnect between IT and LoB leaders, highlighting potential ownership issues around securing process-specific IoT/OT devices. When asked who is primarily responsible for securing IoT/OT devices on an enterprise network, 44 percent of IT respondents versus 36 percent of LoB respondents stated security operations center (SOC) professionals. However, LoB respondents were more likely than IT to prefer a dedicated LoB IT staff or LoB practitioner to be responsible. While most companies tend to keep security under the purview of IT, it is becoming more critical for collaboration amongst asset managers, LoB teams and the network teams that are adopting and deploying these connected devices. This is important for enterprises as they consider their IoT security strategy, including managing default security configurations and enabling proper visibility of all devices.

Tackling IoT/OT Security Challenges: Taking the Right Steps Forward
The survey shows that a combination of top-down executive support, proper security tools and audits instill greater confidence in device visibility. In fact, 48 percent of all respondents stated that improving awareness and visibility of IoT devices is a top priority for improving IoT security and 82 percent of respondents expect their IoT/OT security spend to increase over the next one to two years. When considering the adoption of IoT security solutions, more than half of the respondents (55%) said integration with existing security systems was the most important criteria.

Survey Methodology

Commissioned by ForeScout, Forrester surveyed 603 IT and LoB decision-makers that are directly involved in their organization's network, data and endpoint security processes. Participants were asked about challenges with IoT security and overall awareness of devices on their network. Organizations were located the US, UK, Germany, France, Australia and New Zealand, and had employee counts of 2,500 or more.

Additional Resources:

- Forrester Consulting Study: Fail To Plan, Plan To Fail
- Blog: Part 1: Why OT Gives Security Professionals Anxiety by Ryan Brichant, VP, CTO Critical Infrastructure and OT Security at ForeScout
- Follow ForeScout online: Facebook | Twitter | LinkedIn | Blog
- ForeScout corporate brochure: https://forescout.com/forescout-company-brochure-pr/

About ForeScout
ForeScout Technologies, Inc. helps make the invisible visible. Our company provides Global 2000 enterprises and government agencies with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology integrates with disparate security tools to help organizations accelerate incident response, break down silos, automate workflows and optimize existing investments. Learn more at www.forescout.com.

Media Relations Contact:
Andria Leaf
ForeScout Technologies, Inc.
(408) 538-0870
andria.leaf@forescout.com

Source: ForeScout