# Forescout Study Reveals Cybersecurity Concerns on the Rise Amid M&A Activity

June 24, 2019

- *Global research survey discovers that 65% of respondents experience buyers' remorse after closing an M&A deal due to cybersecurity concerns*
- *Among IT Decision Makers (ITDMs), 53% say they find unaccounted IoT and OT devices after completing the integration of a new acquisition*

SAN JOSE, Calif., June 24, 2019 (GLOBE NEWSWIRE) -- Forescout Technologies, Inc. (NASDAQ: FSCT), the leader in device visibility and control, today announced the results of its global mergers and acquisitions (M&A) cybersecurity risk survey. The study, *The Role of Cybersecurity in M&A Diligence*, surveyed more than 2,700 IT and business decision makers across the United States, France, United Kingdom, Germany, Australia, Singapore and India to examine the growing concern of cyber risks and the importance of cyber assessment during M&A and the subsequent integration process.

According to the survey, 53% report their organization has encountered a critical cybersecurity issue or incident during a M&A deal that put the deal into jeopardy. Cybersecurity concerns discovered after consummation of the deal often present costly risks that would have been factored into the deal negotiations and/or may have led to the dissolution of the deal. After closing the acquisition, 65% experienced buyers' remorse, regretting the deal due to cybersecurity concerns.

"M&A activity can be a game-changing moment in a company's history, but recent breaches shine the spotlight on cybersecurity issues and make one thing abundantly clear: you don't just acquire a company, but you also acquire its cybersecurity posture and a potential trojan horse," said Julie Cullivan, chief technology and people officer, Forescout. "Cybersecurity assessments need to play a greater role in M&A due diligence to avoid 'buying a breach.' It's nearly impossible to assess every asset before signing a deal, but it's important to perform cyber due diligence prior to the acquisition and continually throughout the integration process."

"Acquiring a company without proper cybersecurity due diligence is like buying a used car and taking the seller's word it is in good condition," said Joe Cardamone, senior information security analyst and NA privacy officer, Haworth. "A company should not automatically trust the hygiene of IT assets. It's critical to have full visibility into all connected devices and determine whether they are patched, configured properly, and free of malware."

The survey highlights the following findings:

- **Proper cybersecurity evaluation takes time, but acquisitions often run on fast track.** Many deals face a race to get across the finish line. Only 36% of respondents strongly agree that their IT team is given adequate time to review a targets' cybersecurity standards, processes and protocols before completing an acquisition.

- **More focus on cybersecurity risk during M&A is needed.** Eighty-one percent of IT decision makers (ITDMs) and business decision makers (BDMs) agree that they are putting more focus on an acquisition target's cybersecurity posture than in the past, highlighting that cyber is a top priority.

- **Connected devices and human error put organizations at risk.** When asked what makes organizations most at risk during the IT process, two answers stood out: human error and configuration weakness (51%) and connected devices (50%). Devices often get overlooked and missed during integration as over half (53%) of ITDMs say they find unaccounted devices, including IoT and OT devices, after completing the integration of a new acquisition.

- **Prevalence of cybersecurity issues.** More than half (53%) of survey respondents report their organization has encountered a critical cybersecurity issue or incident during an M&A deal that put the deal into jeopardy. Further demonstrating the potential consequence of a security incident, undisclosed data breaches have become a deal breaker for most companies. Seventy-three percent of respondents agreed that a company with an undisclosed data breach is an immediate deal breaker in their company's M&A strategy.

- **Internal IT teams may lack the skills to conduct cybersecurity assessments.** Among ITDMs, only 37% strongly agree that their IT team has the skills necessary to conduct a cybersecurity assessment for an acquisition. Due to lack of resources, organizations must allocate outside resources to their cybersecurity assessments and/or may not be able to complete a robust assessment.

For additional information, read the full *TheRole of Cybersecurity in M&A Diligence* report here or a blog by Julie Cullivan, Forescout's chief technology and people officer here.

**About the Study**
Forescout's Report, "The Role of Cybersecurity in M&A Diligence," is based upon a survey conducted from February 20 through March 10, 2019 commissioned by Forescout Technologies with respondents sourced from Quest Mindshare. Results were based on a total of 2,779 respondents of IT

decision makers and business decision makers across industries from the U.S., France, U.K., Germany, Australia, Singapore and India. The data was weighted to evenly represent audiences and regions. To qualify, respondents had to be employed full-time, senior manager level or higher, and the primary decision maker for IT purchasing decisions or involved in M&A strategy.

**About Forescout**
Forescout Technologies, Inc. provides security at first sight. Our company delivers device visibility and control to enable enterprises and government agencies to gain complete situational awareness of their environment and orchestrate action. Learn more at www.forescout.com.



**Media Relations Contact:**
Katie Beck
Forescout Technologies, Inc.
650-314-8705
katie.beck@forescout.com

**Investor Relations Contact:**
Michelle Spolver
Forescout Technologies, Inc.
408-721-5884
michelle.spolver@forescout.com

FSCT-O

Source: ForeScout Technologies, Inc.