Nine out of Ten Critical Infrastructure Security Professionals Say Their Environments Have Been Damaged by a Cyberattack in the Last Two Years

April 5, 2019 | Columbia, MD

Report by Ponemon Institute for Tenable finds 62% of respondents said their organizations have suffered multiple attacks

Tenable®, Inc., the Cyber Exposure company, today released the 'Cybersecurity in Operational Technology: 7 Insights You Need to Know' report, an independent study by the Ponemon Institute. The study identifies the true extent of cyberattacks experienced by critical infrastructure operators — professionals in industries using industrial control systems (ICS) and operational technology (OT). It found that 90% of respondents stated their environments had been damaged by at least one cyberattack over the past two years, with 62% experiencing two or more attacks.

Key highlights from the study include:

- **Insufficient Visibility Into the Attack Surface:** 80% of respondents cited lack of visibility into the attack surface, knowing what systems are part of their IT environments, as the number one issue in their inability to prevent business-impacting cyberattacks.

- **Inadequate Staffing and Manual Processes Limit Vulnerability Management:** Lack of personnel and a reliance on manual processes were cited by 61% and 55% of respondents respectively as major obstacles in their ability to assess and remediate vulnerabilities.

- **C-Suite Buy-In Is Key:** 70% of respondents view increasing communication with executives and board members as one of their governance priorities for 2019.

The convergence of IT and OT is a reality in today's digital era. But this convergence has connected once-isolated OT systems to a variety of attack paths. This Ponemon study, based entirely on the self-reported experiences and observations of ICS and OT experts themselves, confirms that the threats to critical infrastructure are real, severe and ongoing.

"OT professionals have spoken — the people who manage critical systems such as manufacturing plants and transportation almost unanimously state that they are fighting off cyberattacks on a regular basis," said Eitan Goldstein, senior director of strategic initiatives, Tenable. "Organizations need visibility into their converged IT/OT environments to not only identify where vulnerabilities exist but also prioritize which to remediate first. The converged IT/OT cyber problem is one that cybersecurity and Critical Infrastructure teams must face together."

For more information, read the full **Cybersecurity in Operational Technology: 7 Insights You Need to Know** report.

Notes to Editors:

- The original study was conducted by Ponemon Institute - **Measuring & Managing the Cyber Risks to Business Operations**

- This report is based on its analysis of a subset of 701 respondents from organizations that fall into the Critical Infrastructure sector—defined as organizations dependent upon industrial control systems (ICSs) and other operational technology:
  - Energy & utilities; health & pharma; industrial & manufacturing; and transportation.

- All respondents are involved in their organizations' evaluation and/or management of investments in IT and/or OT cybersecurity solutions.

- An infographic to support this release is available on request.

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 25 percent of the Global 2000 and large government agencies. Learn more at **www.tenable.com**.

Contact Information: Dulcie McLerie | **tenablepr@tenable.com**