IT Ops vs. IT Security: New Survey Reveals Organizations Lack Basic IT Security Hygiene

Devolutions

> “THERE’S A LACK OF COHESION, AND A DISPARITY IN OBJECTIVES IT SECURITY“

If you have a sneaking suspicion — or if you’ve clearly concluded — that the level of basic IT security hygiene in your organization is somewhere between troubled or terrible, then you are not alone. In fact, you are in the majority.

This is because a new survey of 600 IT decision-makers, sponsored by endpoint security management company IE, has revealed that 67 % of respondents do not believe that their IT Operations teams and IT Security teams work in a cohesive manner to secure the organization against internal and external threats and risks. What’s more, 97 % — which is virtually all of them — felt that their organization would significantly benefit from tighter and better collaboration between IT Operations and IT Security.

Disparity in Objectives

This systemic disconnect between IT Operations and IT Security is making it surprisingly easy for hackers to exploit oversights in basic IT security hygiene. Simply put, IT Operations assumes that IT Security has ownership of these maintenance tasks, and IT Security assumes that IT Operations has ownership of these maintenance tasks.

Microsoft MVP Jason Sandys, who was part of an expert panel that discussed the survey's findings, summarized the daily on-the-ground tension between the tribes: "There's a lack of cohesion, and a disparity in objectives. IT security thinks it's seen as the enemy – the blocker to productivity. IT operations will push ahead with a project, but it'll be inhibited by the IT security team, which naturally has to be cautious. It scuppers collaboration."

Chilling Lack of Visibility

It is certainly worrying that 67 % of IT decision-makers do not believe their IT Operations teams and IT Security teams work in a cohesive manner to secure the organization. However, this was not the survey's most chilling revelation.

This dubious distinction lies in the fact that only 64 % of IT decision-makers have visibility across the entire software portfolio, and only 66 % of their software is current. In other words, organizations lack control over 34 % — or roughly one-third — of their machines, and have no idea if they are vulnerable, infected or outright compromised by malware. Commented 1E's CEO Sumir Karayi: "CIOs have the challenge of explaining the pivotal need for areas like patching, which can feel mundane. But without this hygiene, companies must constantly defend against new vulnerabilities or risk a major breach."

From the Desk of Our CSO, Martin Lemay:

Lack of upper management commitment and bad reporting lines are non-negligible obstacles to a successful security program. Security must be everyone's concern from project management to operations. Good reporting lines will bring agility by allowing governance to make quicker and more accurate decisions regarding cybersecurity risks. With upper management support and an increased budget, collaboration between traditional IT Ops and IT Security should increase, resulting in better overall IT security hygiene.

What Is Your Experience?

Have you experienced a disconnect — or maybe a huge chasm — between IT Operations and IT Security? If so, what were some of the consequences and issues? Please also share any recommendations for closing the gap and improving basic security hygiene.