Written by Marco Attard
02 June 2017

An IDC survey sponsored by operational intelligence platform provider Splunk reveals organisations are "constantly under attack," so much so they often fail to "effectively protect themselves."

The survey involves 600 senior security professionals across Germany, France, Sweden, the Netherlands, the UK and the US. It shows 47% of security teams gather enough information about incidents to enable appropriate or decisive action, but only 27% think they are coping comfortably with the workload, which consists of an average of 40 actionable incidents per week (with the number rising to 77 for finance and 124 for telco).

Around one third (33%) describe themselves as "struggling" or "constantly firefighting," while 53% of respondents claim the biggest limitation to improving security is resourced tied up on routine operations and incident investigation. As for the frequency of attacks, 62% of firms are attacked "at least" weekly, 30% suffer daily attacks and 10% hourly or "continuously." In addition, 45% face a rise in security threats.

Making things worse is firms surfacing a breach to the board at the last possible moment. The top incident reported to the board is sensitive data breach (66%), followed by compromised customer data (57%) and mandated notification to a regulator (52%). Only 35% of firms have breach reporting to the board built into the defined incident response process.

“It’s time to change how we approach incident response,” Splunk remarks. “As attacks become more advanced, frequent, and take advantage of IT complexity, we must become proactive in our approach to security-- how else will we know we have been breached? As demonstrated by the swift, global spread of WannaCry, it has never been more important for organisations to proactively monitor, analyse and investigate to verify whether there are real threats, then

prioritize and remediate the most critical."

Go Investigation or Exasperation? The State of Security Operations