MIND THE GAP

Chris Newton-Smith *examines the disparity between in cyber security confidence and reality*

As much as 60 percent of surveyed UK and US cyber security leaders now admit that security risks originating from third parties and supply chain partners are: "innumerable and unmanageable". This is according to the latest The State of Information Security report from IO, which reveals a growing disparity between cyber security confidence and reality.

A surprising 97 percent of cyber security leaders said they were confident in their breach response, with 61 percent describing themselves as: "very confident". Yet, that confidence contrasts drastically with 61 percent of leaders who noted their organisation had suffered a third-party or supply chain attack in the past 12 months. This further exemplifies the widening 'confidence gap', as business leaders back their resilience while supply chain compromises continue to cause widespread damage.

Recent high-profile incidents, such as the Jaguar Land Rover attack, which disrupted production across multiple manufacturing plants, and the Collins Aerospace attack on its MUSE software, which saw several European airports grind to a halt, highlight how supply chain compromises can quickly cascade far beyond their initial target.

Among those who suffered a third-party or supply chain attack, 38 percent resulted in customer, employee or partner data breaches, 35 percent suffered financial losses or unplanned costs (eg: remediation, fines, legal fees) and 33 percent faced temporary system outage or operational disruption. More than a third (36 percent) of organisations that suffered a customer data breach said they had experienced customer or partner churn or loss of trust as a result, while 28 percent faced heightened scrutiny from partners or suppliers.

Cyber security leaders clearly recognise the importance of supply chain security, but many still underestimate how complex and interdependent modern supply networks have become. This confidence needs to be matched by continuous action to avoid the domino effect across networks, impacting customer trust, finances, and operations.

Despite the growing risk, only 23 percent of all respondents ranked supply chain compromise among their top emerging threats, placing it below AI misuse, misinformation and phishing. This suggests that while investment is rising, supply chain risk is still underestimated relative to its potential impact. While this year's report focuses on the broader supply chain, it still underscores the disproportionate vulnerability of small and mid-sized businesses. Of those cyber security leaders within SMEs with up to 49 employees, 28 percent reported supply chain disruption or cascading partner issues following a customer data breach, compared with 21 percent of large enterprises. This suggests smaller firms are less able to contain the fallout of third-party incidents, often due to limited resources, smaller security teams and fewer formal risk processes.

The Collins Aerospace attack on its MUSE software brought several European airports to a standstill

Attackers increasingly see smaller suppliers as soft entry points into larger targets. They may not be the ultimate prize, but they're often the route into the larger organisations. Securing the entire supply chain is essential for national and commercial resilience. However, the research does demonstrate that investment in third-party and supply chain security is growing, as 64 percent of organisations plan to increase spending in this area over the next year. This number drops to 45 percent among smaller SMEs, who say budgets and investment will remain the same. Smaller firms are generally less likely to have a clear and well-communicated information security strategy, to invest in awareness training or to strengthen crisis management and incident response capabilities, all key components of an effective resilience plan.

Encouragingly, 80 percent of organisations have strengthened third-party and vendor risk management practices in the last 12 months or longer than 12 months, with a further 17 percent planning to do so in the next year. Meanwhile, 21 percent of leaders list strengthening vendor and third-party risk management among their top cyber security priorities for the next 12 months, reflecting a clear shift toward long-term resilience planning.

Supply chain resilience is now one of the top security priorities for the year ahead, but this needs to be embedded within the organisation. To close the confidence gap, leaders must focus on people and process, putting strategies in place to ensure compliance and build a culture of security and resilience across the chain to avoid any weak links ●

Chris Newton-Smith is CEO of IO.