RCPP

Redmond Channel Partner Profile

solarwinds msp

Security Survey Finds Perception Contradicts Reality: Creates Opportunity for MSPs

Q&A interview with Dave Sobel, SolarWinds MSP
Senior Director, Community & Field Marketing

Q What were the results of SolarWinds's recently completed security survey?

A The survey reveals that businesses are overly optimistic about their ability to deter and cope with malicious attacks, despite the majority experiencing a breach over the past year.

Q That's astounding! Can you share more details about the survey?

A Our survey, conducted by Sapio Research, covered cybersecurity preparedness, experiences, and failings of 400 SMBs and enterprises, split equally across the UK and the US. What we found was a contradiction between the confidence organizations have in their current security and the reality of their vulnerability. For example, while 87 percent of organizations have complete trust in their security techniques and technology—and 59 percent believe they are less vulnerable than they were 12 months previously—71 percent of those same organizations have been breached in the past 12 months. The belief that "it will never happen to us" simply doesn't hold true.

Q What impacts did those breaches have on the organizations?

A These breaches are significant and shouldn't be discounted. Of the businesses that have been breached and could identify an immediately traceable impact, 77 percent revealed that they had suffered a tangible loss, such as monetary impact, operational downtime, legal actions, or the loss of a customer or partner.

Q What can MSPs do to help their customers improve security and help avoid these kinds of loses?

A We have identified four key areas where MSPs have an opportunity to help their customers:

1. Offer cybersecurity training to your customers. Training can make a huge difference in your clients' security, so it's absolutely essential that you arm them with the knowledge they need to prevent breaches.
2. Make sure your own house is in order. MSPs need to make sure their own security practices are up to par. Does your security meet the current and future needs of the typical SMB or enterprise? Does it work well across on-premises, cloud, and hybrid environments? Can you serve clients in highly-regulated verticals?
3. Prepare with disaster drills. MSPs can also offer to stress test their clients' security via "war games." You can practice disaster events with your clients, both in terms of technology and processes, to discover weak points and make improvements.
4. Determine the partnerships or skillsets you'll need. Many security incidents require specialists to handle. You should either hire expertise in-house or partner with someone who can handle these incidents for you. You never want to have to build new skills in the middle of a crisis.

Q Do you have further information for MSPs who want to learn more about the survey results and the opportunities for helping their customers?

A Yes, we have a detailed report on the survey results and the opportunities. It is available for free at **http://pages.solarwindsmsp.com/lp-cybersecurity-survey-msps.html**

So, why is this disconnect occurring? Simply put, companies are overlooking seven basic security principles:

1. Security policies are inconsistently applied.
2. User training is massively under-prioritized.
3. Only basic technologies are being deployed.
4. Vulnerability reporting is often weak, or even nonexistent.
5. The majority of organizations make no changes to their technology or processes following a breach.
6. Widely accepted prevention techniques and processes remain overlooked.
7. Detection, response, and resolution times are all growing.

For more information, please visit **www.solarwinds.com**