SOLUTIONS, SECURITY & SERVICES

Cybersecurity Partner Challenges

Delaying projects and non-payments are impending cybersecurity partner business

AYSHWARIA LAKSHMI dqchannels@cybermedia.co.in

After layoffs during lockdown, the cybersecurity segment is faced with the crisis in hand– cutting expenses. This has led CIOs, CISOs and security leaders to come under pressure to do more for less. This in turn means that they are left with only a couple of choices – reduce budgets, delay projects and payments.

The majority of the Indian companies work for clients based in the US. For months now, companies in the US were laying off employees as they hired for growth that did not take place.

Decreased Business to India

Vallabha Desai, Founder, VAPT Consultants said that the companies have stopped opting for external consulting and certification due to the stress on the budgets. His own clients who were to go for ISO certification, for instance, have decided to defer it as it costs and opt to go for documentation and configuration.

Companies often adopt a cautious approach to managing their finances and mitigate potential risks at the sign of a recession or an economic downturn. Companies are generally adopting cost-cutting measures, reassessing budgets and optimising operational efficiency.

Workforce adjustments, strategic prioritisation and cash flow management are also common approaches. Additionally, companies are striving to remain



Companies are generally adopting cost-cutting measures, reassessing budgets and optimising operational efficiency.

—Vallabha Desai, Founder, VAPT Consultants

agile and adaptable by exploring new opportunities and embracing digital transformation. The severity and duration of the recession, as well as industry-specific factors, influence the specific actions taken by companies.

Vallabha added that the stress on financials has made the companies put aside cybersecurity projects.

"While this may not directly impact us, indirectly we are taking a hit, as the companies delay projects or payments. Some companies have even opted to step away from external consulting," he said.

Project delays and subsequent payment delays can occur due to unforeseen circumstances or misalignments in project scope and expectations.

Employee layoffs that are happening in the market are the cause of organisations resorting to employee layoffs as the first step without exploring other options, explaining that there has been mindless over-hiring which they are trying to correct using the present situation.

These factors can impact the timely delivery and commitment of providers, leading to payment delays. Additionally, external economic factors, such as market downturns or budget constraints, can contribute to project postponements and payment delays. Effective communication and proactive problem-solving between providers and clients are crucial in mitigating these challenges and finding mutually beneficial solutions.

"We are yet to see the impact to that level in the markets we are operating in.However, there is caution all around especially in the western markets compared to Asian markets," said Pradeep Menon, Cybersecurity Evangelist



Security risks exist across various industries, and other institutions should also prioritise security measures.

—Suresh Kumar, CEO, Skybertech

and Director, Cybersecurity NxxT and Zacco Digital Trust.

Does it Compromise Security?

Suresh Kumar, CEO of Skybertech says it would not."Institutions have traditionally maintained high-security standards due to the critical nature of their operations," explains Suresh. "However, it's important to note that security risks exist across various industries, and other institutions should also prioritise security measures."

He also added that failing to take security measures can leave them vulnerable to cyber threats and potential breaches. All organisations, regardless of industry, should strive to uphold robust security practices to safeguard their data, protect their stakeholders, and maintain trust in their operations.

Studies have also shown that Cybersecurity attacks escalate rapidly during economic downturns and recessions. Inadequate spending on security can lead to failure to protect against emerging threats leaving organisations highly vulnerable. Threat actors use fear and uncertainty as a tool to perpetrate more attacks.

For instance, areas such as SOCs (Security Operation Centres) would face lesser hiring or a reduction in workforce. It can also identify redundant cybersecurity tools that would overlap with functionality or add those that have a better Return of Income.

In reality, according to him, it's mostly a reduction in cybersecurity hiring or procurement is what the market is facing right now.

Arjun Venkat, an industry expert and IT consulting leader with one of the leading IT companies shares his thoughts, "The clients are not compromising on their expenditure related to security and compliance aspects, which remain



While there is a caution in the market, the companies understand the need for a strong cybersecurity system in place.

—SP Arya, Director, Technology, Biztek Advisor

the focus and key areas for clients globally. They are cautious on the expenditure towards any modernisations aspects."

Future to Normalcy

SP Arya, Director, Technology, Biztek Advisor, says that while there is a caution in the market, the companies understand the need for a strong cybersecurity system in place. Times like these are when ransomware attacks and risks rise.