How cyber-ready is the Indian physical security industry?

Source: asmag

Last month, someone working for an international security solutions provider asked me how the Indian market reacted to the Verkada breach incident. Many Western markets had found this issue troubling, and they probably expected Indian systems integrators and customers to be equally concerned.

Except that most systems integrators I talked to didn't even know that there was a breach at Verkada. Some didn't know Verkada at all, which is not surprising because of their lack of market presence here. But this naturally led me to the next question. How much of a concern is cybersecurity for Indian physical security professionals and customers?

"There is definitely more awareness than before, and there are tenders that we have come across where cyber-hardening is a separate section that is at least half of the cost of the entire project," says Kunal Bhogal, Chief Design and Technology Officer at IIRIS Consulting. "But this is often limited to efforts from large organizations. I'm surprised that many of the government city surveillance projects don't include cyber-readiness or cyber-hardening as requirements."

Lack of concern despite recent incidents

One reason for Indian customers not being too concerned about cybersecurity is that no significant data breach through physical security devices has been reported. In fact, even when there occurs an incident where an organization does come under a hacking attack, the news is forgotten as quickly as it surfaces.

The Verkada incident happened too far away for anyone in India to feel concerned. But in February, a large power plant in Mumbai suffered an outage. According to a New York Times report that quoted a company that tracks internet activities, this was part of a Chinese state-sponsored cyberattack plan. Following this, an outage at India's National Stock Exchange also came under the radar for being caused by external factors.

These are just the large-scale incidents that we hear about. There are announcements of investigations and then nothing. We don't know if any state really sponsored these attacks. We probably will never know. And precisely because of this lack of follow-up, the average customer of the Indian market does not consider cybersecurity a concern. They are still worried about physical security alone.

Even some of the efforts made to create awareness remain a formality. Pramoud Rao, MD of Zicom Electronic Security Systems, says that although there are events like seminars and webinars on the importance of cybersecurity in this domain, they remain limited to discussions.

Lack of focus on the right issue

All this is not to say that India's average physical security customer hasn't come across the concept of cybersecurity in the recent past. They have heard of it as the "issue with Chinese brands." Recent reports of certain Chinese brands being vulnerable and banned in countries like the US have prompted customers to reconsider their use. The Indian government has also imposed restrictions on the use of security products not made in India for public projects.

"When we go to meet a customer, he doesn't spend much time thinking about cybersecurity," Rao says. "And as a sales pitch, we tell the customer that there are certain Chinese brands that are banned, along with press releases and information to support this. That is the time they get interested in this matter. Left to themselves, the customer here is still not bothered about cybersecurity."

What's missing here is that the customer appears to remain unaware that any IP camera from any brand can potentially be hacked. The vulnerabilities could be different, including insider threats, but the result is the same. But for most Indian customers, in the contest between cybersecurity concerns and costs, the latter always wins.

"If you talk to the top-notch companies, the likes of multinational tech companies and BPOs, they are aware of the risks involved," Rao continued. "The CIOs of these companies are knowledgeable about this, and they spend considerable time on it."

What about systems integrators?

That end customers are not bothered about cybersecurity is not necessarily a surprise. After all, not all of them are tech-savvy. But Rao points out that the systems integrators themselves are not prepared for cybersecurity.

"When you further knock it down to the system integrators, I think while there is an interest in cybersecurity, there is no keenness," Rao added. "The reason is lack of education among the system integrators about cybersecurity. There is a lack of awareness about damage control because nobody is experiencing great cybersecurity challenges. So, there is a lack of knowledge, lack of application, and lack of customer demand."

A ticking timebomb

But Indian systems integrators may need to pay more attention to this aspect as there is a change in the nature of cyberattacks. Bhogal says that unlike before, where large companies were the target of hackers, now even small companies and startups that hold valuable data are vulnerable.

"These are less of attacks that converts into a ransomware or converts into siphoning of money or movement of money and primarily more targeted at the theft of information," Bhogal said, adding that often large companies have the infrastructure to protect themselves, while smaller companies don't.

In short, the negligence of cybersecurity is a ticking timebomb. If we wait for something to happen before taking action, it may be too late. a&s