THE ECONOMIC TIMES

NEUTRALISING
THE CYBER THREAT SPIKE

SOPHOS

CONSUMER CONNECT INITIATIVE

WIDENING THE SECURITY NET

2020 made organisations realise the criticality of cybersecurity. Going forward, it's role will only get more crucial

Malvika Chandan

The critical role that cybersecurity plays in protecting our privacy, rights, freedom, and our physical safety will continue even after the pandemic has long gone. Covid-19 saw cyber-attacks reaching a new high – the FBI said its cyber division received 400 per cent more complaints of cyber-attacks than before the pandemic. That's not it. According to a Microsoft report, COVID-themed phishing and social engineering attacks climbed to 20,000-30,000 per day in the US. Things were no better in India where a report by Indian Computer Emergency Response Team (CERT-In) confirmed that there were close to 7 lakh cyber-attacks till August 2020.

For cyber criminals, the Covid-19 proved to be an opportunity to exploit and conquer. But for some smart cybersecurity solutions by some companies, the damage done by the ever-rising cyber-attacks could have been irreversible.

A lot of things which employees click on accidently such as phishing emails would not even come to them if they were sitting in the enterprise

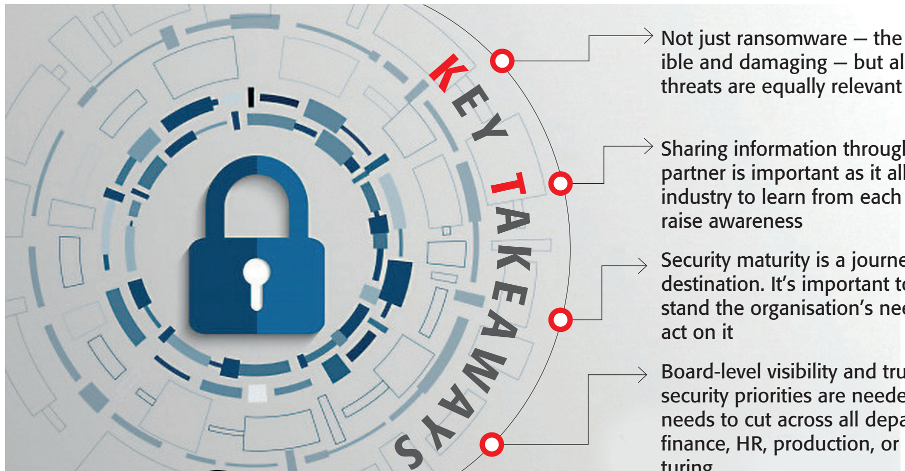
ANKUSH TIWARI
VP and Head-Digital Services
QuEST Global

For database authentication, not having a two-factor set up is an example of an issue with the Cloud. It's important to understand Cloud architecture and the way it is configured

DURGA PRASAD SWAMINATHAN, CIO
Cholamandalam Investment and Finance Company

So, has the cybersecurity paradigm changed forever? Are we as much at risk now as in the beginning of the pandemic? The cloud has emerged as a saviour towards ensuring business continuity, but is it safe enough? A virtual roundtable of leading CIOs and security professionals around 'Neutralising the Cyber Threat Spike' organised by ET and Sophos, tried to find some answers.

The leaders acknowledged that 2020 upended greater risk than any IT team had planned for. According to a ransomware survey conducted by Sophos, globally, 51 per cent organisations were hit with ransomware and 73 per cent of those had their data encrypted. In India, that toll was even higher – 82 per cent of the organisations Sophos surveyed were hit with ransomware in 2020 and 92 per cent of them were encrypted. "Ransomware has got a lot nastier. The payments are over a million dollars now with the highest I've seen being in the $30-34 million range," said John Shier, Senior Security Advisor at Sophos. Another Sophos survey reveals the average global threat detection time to be five days or 120 hours. It means that an attacker will be in your network for an average of five days before you are able to detect it. Unfortunately, in India, the same is 228 hours or 9.5 days.



KEY TAKEAWAYS

Not just ransomware – the most visible and damaging – but all security threats are equally relevant

Sharing information through a trusted partner is important as it allows the industry to learn from each other and raise awareness

Security maturity is a journey not a destination. It's important to understand the organisation's need and act on it

Board-level visibility and trust on security priorities are needed. Security needs to cut across all departments – finance, HR, production, or manufacturing

Because of the pandemic, a whole new set of systems such as Cloud collaboration tools – which were not well tested and unfamiliar to colleagues – had to be adopted

PRIYANK KOTHARI
Head-Information Security, **Tesco Business Service**

Quite obviously, security needs to gain boardroom importance to safeguard organisations against possible threats. For that, Prateek Bhajanka, Senior Principal Analyst, Gartner believes, "Security professionals need to speak in a language that the board of directors understand, namely, cost, revenue and risk. All security related investments, outcomes and operations and initiatives need to be explained in these three words." Empowering workforces is equally critical. "It's important that they imbibe the culture of 'you see something; you say something'."

According to Gartner's 2020 Board of Directors survey, cybersecurity related risk is the second highest risk for the enterprise, followed by regulatory and compliance risk

PRATEEK BHAJANKA
Senior Principal Analyst
Gartner

Some organisations, such as Cholamandalam Investment and Finance Company, sent out continuous messages to their users to remain aware. "A niche area we explored was behavioural authentication.

Partnerships, whether with SaaS providers or other businesses, should go through a solid vendor security assessment as they are also susceptible to attackers

ZAK MURAD
Chief Information Officer, **CRISIL**

The pandemic is an opportunity to upgrade your security programs and look at a zero-trust approach to stay safer as an organisation

JOHN SHIER
Senior Security Advisor
Sophos

So, if someone's credentials are trapped through a key log, there are ways for us to go back and authenticate it," said Durga Prasad Swaminathan, its CIO. But what should be the priority areas in terms of security management? "Protecting applications and services on the cloud landscape; factor authentication controls – to differentiate between an employee and a hacker; web-based controls – not just of corporate devices but also of personal devices; and regularising and increasing the number of phishing simulations," said Priyank Kothari, Head-Information Security, Tesco Business Service.

Having a zero trust approach and zeroing on all possible entry points of attacks are critical to a robust security strategy, echoed the panel. "Employee awareness is very significant. Designing campaigns internal to the corporate and sending dummy phishing emails to understand how much aware are your employees are very important," said Zak Murad, Chief Information Officer, CRISIL.

Underling the importance of the Cloud by calling it the great enabler which gives faster scale, Ankush Tiwari, VP and Head-Digital Services, QuEST Global, cautioned that depending on a single, major cloud provider, may prove to be a problem if it is not present in other geographies required by the enterprise. "It's important keeping decentralisation in mind."

How many organisations are using Extended Detection and Response (EDR) protection on their endpoint? Less than 1 to 2 percent

SUNIL SHARMA
Managing Director-Sales
(India & SAARC), **Sophos**

In the current scenario, with people working from diverse locations, security will continue to be a challenge for organisations. While organisations are giving security risk more credence, said Sunil Sharma, Managing Director-Sales (India & SAARC), Sophos, "The reality is that a lot more focused and regular engagement at a senior level is needed towards security management."

Send feedback to etgreycell@timesgroup.com