BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

Why Cyber-resilience is Crucial

02 October 2024 | Opinion | By Sathish Murthy, Senior Systems Engineering Lead, Cohesity ASEAN & India

In recent years, ransomware attacks have become more regular, stealthy, and expensive. They have also been developing swiftly. Even for those lacking experience, new ransomware-as-a-service (RaaS) models provide pre-made avenues for financial gain for would-be threat actors. Attackers are also reinventing traditional strategies at the same time. Some are combining data theft and encryption into double extortion, increasing the strain on their victims. Some have invented "encryption-less" attacks, concentrating only on the possibility of a leak. Traditional ways of decrypting and recovering files are becoming less practical as new techniques develop.

Over $1.1 billion - that's how much ransomware gangs raked in last year, according to blockchain analyst Chainalysis. Does this astronomical figure say more about the sophistication of the adversary, or is it an indictment of our overall resilience to cyberattacks? Realistically, it’s a bit of both.

The healthcare sector exemplifies this reality. While healthcare facilities must continually ramp up cybersecurity efforts , the high value of personal health information (PHI) has made them an attractive target for cyber attackers. According to the Singapore Ministry of Health, PHI is 50 times more valuable on the black market than financial data because of its immutable nature, as it follows one throughout their lifespan, and can be exploited for identity theft to make fraudulent insurance claims or gain illegal access to prescriptions; among other nefarious purposes.

In the past few months alone, cyberattacks have disrupted operations in numerous hospitals across the world. One of these attacks disrupted operations at major US healthcare network Ascension and forced hospitals to incur significant debt due to their inability to connect with insurance providers to get reimbursement. Several London hospitals have also experienced disruptions in services related to blood transfusions following a ransomware attack on a provider responsible for managing medical testing services and lab operations, causing delays to surgery plans.

In Singapore, medical records must be safely and securely accessible across various settings and providers. The National Electronic Health Record (NEHR) system supports this by centralising patient medical summaries, enabling licenced healthcare providers, including family doctors, hospitals, and nursing homes, to share information seamlessly. As smart hospitals, data sharing and artificial intelligence (AI) become increasingly integrated into daily operations, the attack surface for cyber threats expands because increased data footprints mean there is more critical data that can be targeted - particularly when it is PHI data.

This data security risk threatens not only operations, but also patient data security, financial stability, and organisational reputation, especially given cyberattacks are a ‘when’ not ‘if’ likelihood. In healthcare, such cyber incidents can escalate to life-or-death scenarios, underscoring the necessity of cyber resilience. Cyber resilience ensures healthcare providers can sustain operational continuity, in an industry where every minute or hour counts, even amidst cyberattacks or IT system failures, which is essential for safeguarding patients.

Although paying a ransom is considered an action of last resort, a concerning revelation emerged from Cohesity’s Data Security Report 2024 (Singapore and Malaysia data): 82 per cent of the respondents said their organisation would pay a ransom to recover data and restore business processes. Close to 3 in 5 (59 per cent) Singaporean respondents and almost 3 in 4 (74 per cent) Malaysian respondents said their company would be willing to pay over $1 million to recover data and restore business processes, with 16 per cent and 22 per cent respectively saying their company would be willing to pay over $5 million.

Ruthless scams ramp up pressure

Unfortunately, paying the ransom does not guarantee business-as-usual. Ransomware gangs often blackmail their victims four times over: first, the victim's data is encrypted and if they don’t pay the ransom to decrypt it, then the data is exfiltrated from the company network and they’re threatened again that it will be published online.

Cyber criminals have also found novel ways to put even more pressure on victims via triple blackmail. Here, the data is not only encrypted and threatened with publication but in a third attempt to extract payment the criminals target everyone whose data has been stolen and harass them to exert even more pressure on the targeted organisation.

The hackers used stolen patient data to threaten these people with “swatting” - a ploy that begins by subjecting an individual to a report of a serious crime, which results in them being raided at their home by elite SWAT (Special Weapons and Tactics) teams or other law enforcement groups. Some of these incidents in the US have been fatal.

Ransomware attacks are also growing in sophistication and severity, with quadruple attacks now occurring whereby cyber criminals are now even threatening to involve authorities, as part of their blackmail and attack techniques. After the data is encrypted, then exfiltrated and published, the ransomware gang involved has harassed the victim organisation’s customers and also threatened to expose the victim organisation to the industry regulatory authority for not reporting the cyber-attack.

Holistic Cyber Security Strategy

Fuelling a vicious cycle, the increasingly damaging consequences of a cyber-attack have turbocharged demand for cybersecurity employees, exacerbating the shortfall in this field. For many organisations, maximising the efficiency of their understaffed cybersecurity teams comes down to people, processes and technology.

One way to foster a skilled workforce equipped to detect and respond to threats effectively is to organise realistic tabletop exercises simulating ransomware attacks, which can help organisations find out where their cybersecurity gaps are and rehearse the best ways to respond. These processes, coupled with employee education and training, will enable the organisation to keep pace with the rising sophistication of cyber-attacks.

When it comes to technology, below are a few key ways that organisations can prevent attacks:

- Immutable backup snapshots – these unmodifiable backup snapshots provide a secure data copy for recovery, forensic analysis, compliance and maintaining data integrity.
- Access controls – such as AI-enabled multi-factor authentication (MFA) add extra security layers to ensure only authorised users can access sensitive information, extend the capability to include authentication to data risk levels, and automatically block users for abnormal access behaviour.
- Quorum - which requires at least two parties to confirm major changes or access; and
- Role Based Access Control (RBAC) – which helps stop unauthorised access and limits access to role-specific activities.

Organisations need a combination of tools to detect, protect and recover from ransomware attacks - and most importantly remain cyber resilient. As threat actors look to gain any advantage they can to hit pay dirt through ransom payments, healthcare facilities need to remain vigilant in their data security prowess and establish or maintain cyber resilience.

Sathish Murthy, Senior Systems Engineering Lead, Cohesity ASEAN & India