Ticked, filed, breached: Closing Malaysia's cyber compliance gap

By ARIVINDRAN SAIDOO

LATE on the night of Nov 6, a government-linked bank found its website defaced. The attacker left a message calling it a "security assessment" of the bank, and for several hours the altered pages remained visible in Google search results.

The bank said the problem lay with a third-party service provider and that customer funds, data and banking systems were not affected. I have no reason to doubt that. But a customer who searched for the bank that night would not have known, or cared, which server the page sat on.

The following day, the National Security Council (NSC) said the National Cyber Security Agency (NACSA) was aware of cyber incidents and system disruptions at several financial institutions and was monitoring the situation with those involved.

NACSA recorded 5,110 cybersecurity incidents from January to September this year. Bukit Aman received 16 reports of cybersecurity threats between Oct 10 and 31, with losses of about RM79mil. Computer crime cases from January to October rose to 1,297, up from 1,174 in the same period last year, although total losses were lower.

On Nov 14, the prime minister said Malaysia faces thousands of attempted cyberattacks every month.

These figures raise broader questions about the state of cybersecurity preparedness among organisations. Cybersecurity has featured regularly in conferences, industry briefings and boardroom discussions.

I have also been invited to speak on the subject at several industry sessions before. Yet, the more important question is whether this awareness is translating into effective controls, timely remediation and tested recovery capabilities.

On Nov 4, NACSA raised the National Cyber Security Threat Level from low to medium. The NSC described it as a precaution considering current security developments, and NACSA has said the move is meant to enhance preparedness and should not be read as a national cyber crisis.

In my opinion, it was the right call.

For most organisations, the practical change is modest. Those designated as National Critical Information Infrastructure (NCII) now have nine preparedness actions to carry out, including round-the-clock monitoring, patching, multi-factor authentication (MFA) and updated service continuity plans. Sector leads must also send NACSA a weekly threat status report.

Organisations outside the Cyber Security Act 2024 have been given guidelines with 12 priority actions. Companies that are not on the NCII list should not take this as a reason to relax since theexposure to cyber threats does not depend on their regulatory status.

Boards and senior management in Malaysia have heard the message many times. Cyber risk is on most corporate risk registers and phishing training is routine.

The challenge now is to ensure this recognition translates into sustained action across day-to-day operation.

None of these measures are new. Monitoring, patching, MFA and continuity planning are fundamental cybersecurity practices, and they are where most of the organisations continue to fall short. The heightened threat level is a timely reminder to ensure these measures are in place, and working effectively to manage cyber risks.

The gap is in follow-through. NACSA chief executive Megat Zuhairy Megat Tajuddin recently noted that many attacks still exploit basic weaknesses such as unpatched systems, weak passwords and holes in suppliers and third parties. These are familiar cybersecurity risks, but many organisations continue to overlook them, leaving the door open to cyber threats.

Most awareness effort also goes to the wrong audience. We train employees not to click on suspicious links, which is useful, but the decisions that carry the most risk are made in management meetings: delaying a patch to avoid downtime, say, or offering website hosting to the lowest bidder.

These decisions involve legitimate commercial and operational trade-offs. They are weighing it against other priorities, and the answer I hear most often is "kena submit paper untuk budget dulu".

This tension is particularly relevant to operational technology (OT), the systems that run plants, utilities and transport. Many operators still think of these systems as cut off from the outside world, long after remote access and links to office IT changed that.

On industrial sites I still find flat plant networks where one infected computer can reach almost everything, and contractors plugging laptops straight into control networks because the job had to be done that day.

The engineers rarely need convincing; most can point out the weak spots before you ask. Getting management to fund the fix is the hard part, and in the meantime the exposure stays where it is.

Box-ticking compliance-led approach worries me even more. In too many organisations the aim is to "pass the audit, cukup makan" – treated as a one-off task rather than a means of strengthening security.

It is not for lack of rules. Bank Negara Malaysia's Risk Management in Technology (RMiT) policy is one of the stricter regimes in the region, and the Cyber Security Act 2024 requires NCII organisations to follow codes of practice, conduct risk assessments, audits and exercises, and report incidents.

But as Megat has said, laws on their own are not enough, their effectiveness depends on how well organisations put them into practice. That is where we come up short. An approved policy does not prove a control works, and a yearly penetration test shows how things looked on the day it was done.

> SEE PAGE 8

Cyber preparedness is judged by how well protections work

> FROM PAGE 4

A crisis drill run to the same script every year tells you very little about how people will react to something new. Assessments, including the ones firms like mine carry out, achieve little if nothing happens after the report is handed over.

Closing an audit finding should therefore involve more than completing the required paperwork. If the underlying cause remains unresolved, the weakness can recur in a different form. Regulators have noticed, and enforcement under RMiT is no longer theoretical.

Third-party risk is where the limitations of a documentation-led approach become particularly apparent. Vendor due diligence is often reduced to a questionnaire filled in when the contract is signed and rarely looked at again. In March, several Malaysian stockbrokers had trading disrupted for days in two separate incidents, both reportedly linked to weaknesses in third-party trading systems.

Then, in early November, Malaysia's national carrier joined several other Asian airlines in warning that passenger booking data may have been exposed, through a breach at the reservation system provider they share rather than in their own systems.

These incidents illustrate why supplier assurance needs to extend beyond initial onboarding.

A breach of a service provider can still disrupt an organisation's operations and affect its customers, even when its own systems have not been compromised.

The priority is not necessarily another framework, but stronger oversight of the outcomes existing frameworks are intended to achieve. Boards will get further by asking for results rather than documents: how long it takes to apply a critical patch, whether every admin account has MFA, and how quickly we would know if someone got in tonight.

Those answers say far more than a note that a policy was approved last quarter.

Testing should also be closer to the real-world conditions. Run unannounced exercises, and every so often point the ethical hackers at your weakest supplier instead of your best-defended system.

On suppliers, organisations should identify which vendors can access your critical systems or customer data, ask them for evidence rather than self-assessments, and write breach notification and audit rights into the contract.

Recovery needs more attention than it gets. Restore plans often look fine until someone asks how long a full restore would actually take.

Plan based on the assumption that a breach will happen, and practise bringing key services back from clean backups with a stopwatch running.

Plant operators should include OT in this, which starts with knowing what is on the plant network, separating it from office IT and controlling remote access. All of this needs people with the time and skills to do it. I have seen organisations spend heavily on security tools, only to leave them poorly configured and underused due to lack of time and resources.

The threat level may well drop back to low in a few months, but the risk behind it isn't going anywhere.

Speaking in Parliament in November, the prime minister said Malaysia's growing digital infrastructure and its position on international issues make it a potential target, and our push to become a regional hub for data centres will make the resilience of that infrastructure even more important.

Conferences and industry discussions have played an important role in building awareness. What I would like to see is these conferences go beyond discussions and end with clear, measurable commitments that organisations can revisit a year later. This means tracking progress, looking at what has improved and identifying gaps that still need to be addressed. At next year's conferences, we should be able to show what has changed, rather than simply have the same conversations again.

Malaysia's cyber preparedness should be judged not by the volume of discussion or the completeness of compliance records, but by the effectiveness of the protections behind them.

Compliance provides an essential foundation. Resilience depends on whether those requirements translate into sustained action before, during and after an incident.

Arivindran Saidoo is partner – technology, risk and cyber security advisory at KPMG in Malaysia. The views expressed here are the writer's own.