Stopping ransomware in its tracks
CIO guide to building an integrated cybersecurity strategy

Ransomware is now one of the most significant threats to Australian organizations, with more than 500 incidents reported to the Australian Cyber Security Centre in the past year alone. Globally, it is a $400 billion criminal industry.

The Australian Government has now announced the Ransomware Action Plan in a bid to stem the problem. What do Australian CIOs need to know to align with the plan?

According to the 2021 IDG Security Priorities Study, 44% of security incidents are still caused by employees, despite 53% of IT leaders prioritising security training for employees in the past year. Unpatched software and security lapses follow as the second leading causes of incidents.

More concerning, the sudden shift to hybrid work arrangements due to the pandemic has added complexity to the task of securing data given employees now work on a wide array of unmanaged “BYOD” devices.

According to Leo Lynch, VP Sales for Data Protection and Business Continuity Solutions provider Arcserve, there are four key steps that Australian CIOs can immediately take to protect their organisation against the threat.

Prepare to be breached
It’s not “if” but “when” your business will be breached by ransomware, Arcserve’s Leo Lynch says. The Australian Government’s plan urges businesses to move beyond simply the ‘prepare and prevent’ phase to becoming ready to “respond and recover” and “disrupt and deter”.

“The longer businesses are down or without their data, it is costing money, so understanding how long it will take to recover your data will help you quantify what that will cost your business.

“Equally important, the recovery point you can get back to in terms the most recent good data can equate to a huge cost to the business if the restore process doesn’t produce up-to-date data.”

Leo recommends businesses test their recovery processes rigorously.
“Companies have invested a lot in security education for employees. But even so, staff will still click on links in emails and send documents to the wrong people. So it’s not a question of if, but when, there will be a ransomware breach. The challenge is to move beyond prevention to detection and be prepared for the recovery. Have you tested your data recovery system? When you really need it, will you actually be able to recover the data? Knowing the recovery time and reliability will be critical to understanding the cost to the business. Without this preparation, the business may not even survive.”

Leo Lynch, VP Sales for Data Protection and Business Continuity Solutions provider Arcserve

The importance of immutable storage

Immutable backups cannot be changed once they have initially been created. This means that once a backup is taken, data is never writeable again, with subsequent backups also unable to be changed.

The concept of immutable storage has become so important because ransomware attackers have developed a mode of operation of encrypting backups first, before even targeting live production systems, Leo explains. This means by the time a business discovers the intrusion – often more than 200 days later – the backups are no longer useful, pressuring desperate executives to pay the ransom.

The UK Government has now mandated that all its government departments use immutable storage as one of their backup strategies to guard against ransomware attacks.

One of Arcserve’s products, the OneXafe, is a powerful, yet simple, storage and backup appliance, measuring just a few inches across, which can be easily deployed to do immutable backup snapshots. It is coupled with OneSystem, a cloud-based management service.

Look for simplicity

When selecting a vendor for your data protection systems, make sure you are not introducing new complexity into your IT landscape.

Ask if your vendor can provide tier 1 security protection from an established antimalware vendor integrated across your disaster recovery and backup infrastructure so this doesn’t have to be separately sourced and implemented.

“Higher end Arcserve products come pre-loaded with Sophos, so you get one-touch support – there’s no finger pointing. We also have products with Nutenix integrated – we’re the only backup and recovery vendor worldwide that has that in the enterprise space,” comments Leo.

Don’t do business with criminals

Arcserve has worked with numerous clients to help them get their businesses back up and running after ransomware attacks and a clear learning out of this experience is not to pay the ransom.

“70-80% of customers who reported to us they had been breached also reported they’d paid the ransom, but they then found the intruders came back again for more, so it doesn’t solve the problem,” explains Leo.

“Additionally, you may not get all your information back after paying the ransom.

“On average, it’s 260 days before a business realises it has been breached. These are not burglars who break into your house, steal your TV and leave. These are burglars who come into your house and watch your family for months. They look at how money flows within your organisation and then they try to take manipulate and take advantage of that. They may stay there even after you pay a ransom,” he explains.