DON'T WAIT FOR THE STATE

Richard Massey *says businesses should take steps to protect themselves now as Governments mull mandatory ransomware-readiness*

Ransomware attacks are a topline concern for businesses everywhere. In 2022, organisations worldwide detected 493.33 million attacks. According to the latest data from IBM, the average cost of these was $4.54 million.

Those are astounding numbers. And in response, governments are taking action. One suggestion is forbidding payments to ransomware gangs. Recently, the US and UK announced sanctions, including a payment ban to Russia's Trickbot ransomware gang.

Another action governments are mulling is a legal requirement that companies be ransomware-ready. In a recent survey by Arcserve, respondents were evenly split as to whether this is a good idea. They were similarly divided as to whether companies that do pay a ransom should face penalties. Those supporting penalties argue that paying perpetuates the problem. Those against say paying the ransom is often the only way to recover lost data and so penalises victims twice.

These findings highlight the complexity of the issue and the challenges that governments and businesses face. For example, legally requiring companies to be ransomware-ready will have myriad benefits and drawbacks. On the benefit side, such laws could improve cyber security, limit attacks and reduce financial impact on companies.

However, such laws can increase compliance costs, regulatory complexity and a false sense of security. Plus establishing a baseline standard for cyber security will be a challenge for many small and medium-sized enterprises.

Before deciding on any regulations, assessing the potential benefits and drawbacks is essential. Let's start with the benefits. One of the most significant potential benefits of government-mandated rules is that they will establish a baseline for cyber security, leading to a higher level of preparedness in the business community overall.

If more robust measures are mandated, the thinking goes, companies will be better equipped to detect, prevent and recover from ransomware attacks. These measures, in turn, will reduce ransomware attacks, which will benefit companies and society at large. Companies prepared for ransomware attacks will inspire confidence in consumers, who can trust that their data and financial information are safe.

Now for the drawbacks. The biggest is cost. Companies will have to spend to comply with regulations mandated by governments and the expense will be particularly onerous for small businesses. As a remedy, governments could provide tax breaks for companies that comply with a ransomware-readiness requirement.

A reliable backup system is one of the best ways to guard against a ransomware attack. This system should include storing backups offline or in a secure, isolated environment and testing those backups regularly to ensure they work correctly. There should also be a consistent backup schedule, which enables organisations to seamlessly restore any compromised systems or data.

Picture credit: Adobestock

Encrypting your sensitive data is also highly recommended. That way, if ransomware attackers gain access to your critical assets, they won't be able to extort you. Organisations should look for a data storage solution that safeguards information continuously by taking snapshots every 90 seconds so that even if ransomware does sneak through and criminals overwrite your data, your information will still be easily recoverable to a recent point in time. Because the backup snapshots are immutable, you'll have several recovery points to restore your data intact.

Large and small businesses should also understand that not all of their data is created equal, so they should consider data tiering. This is a system in which less frequently used, less vital data is moved to lower-level storage, which may be less available and recoverable but less costly. The idea is that because not all data is created equal, the 'less important' data doesn't need the Fort Knox treatment. Companies should have different policies for different data sets, depending on how quickly they need to access and recover it in case of a ransomware attack.

It will be crucial for governments and stakeholders to carefully evaluate all the potential benefits and drawbacks of ransomware regulations before implementing them. This approach will enable policymakers to determine rules that balance the benefits of improving security and the costs in complying. Regardless, companies that store and use data – which nowadays is just about all companies – should plan their steps to ensure it is safe, backed up and recoverable should a ransomware attack occur ●

There are both positives and negatives to legal requirements for being ransomware-ready

Richard Massey is Vice President of Sales, EMEA, at Arcserve