Preparing customers for new cyber security regulations

Organisations across the board are under pressure to secure their data, and act decisively and transparently should they suffer a security event. Slow responses to data breaches, translate into massive fines from regulators, and more damagingly, loss of reputation and customer confidence.

Chris Buchanan, client solutions director at Dell EMC South Africa

However, on average, it takes organisations over 100 days to discover a data breach, meaning that cybercriminals have had months to go through a business's systems.

"No wonder some of them have decided ransomware isn't worth it, it's easier to just come and steal an organisation's data."

These are the words of Chris Buchanan, client solutions director at Dell EMC South Africa, who was speaking at Pinnacle Techscape, recently held in Mauritius.

Making matters worse, he says 93% of data breaches occur at the endpoint. "If you as an organisation are trying to do something to protect yourself against threats and attacks and you haven't looked at the endpoint, you're completely missing the point."

"Think about it. How many of your customers have laptops stolen? How many of them recover that data? How many of them are even interested in recovering that data? None. They don't care. After using a laptop for two weeks, the data on the device becomes more valuable than the device itself.”

Buchanan says no one is interested in recovering that data but asks how critical would it be if someone else got hold of that data. “Now we’re taking a reputational risk. That is incredibly serious. So what are you going to do about it?”

We’ve all heard of POPI, GDPR, and the new Cybercrimes Bill which will finally become law about eight years later, says Buchanan, adding that preparing customers for this is crucial.

Many think encrypting the data is the answer, using one or another solution, he explains. “However, the challenge with that, is if you have a device stolen, or you lose a device, you are going to have to prove what on that device was encrypted and when last it was encrypted. With many solutions, it not always possible to tell when it was encrypted and which device was encrypted. You can’t run an audit on it, you need some type of management tool to manage that side of it.”

He says Dell has a few security solutions to meet these challenges, which includes Dell Data Protection and Encryption, that enables the enterprise to detect data security risks on desktops, laptops and external media, and protect data on these devices by enforcing access control policies, authentication and encryption of sensitive data. It doesn’t encrypt the whole drive, this just isn’t necessary.

Another is an advanced threat protection solution that is cloud-deployed, and picks up 98.7% of threats out there, by continually monitoring endpoints, analysing data, detecting threats and containing attacks without impacting on workflow.

An increasingly mobile workforce means more risk, he says. “Our approach to data protection with Dell Data Guardian is unique, as it will safeguard data wherever it goes and irrespective of how it is shared. The solution ensures that data is encrypted beyond the boundaries of the organisation, usage is controlled and monitored, and visibility of data activity and location is accessible and easy.”

Finally, a ‘safe screen’ option is being introduced and will prevent other users from seeing what is on a user’s screen.