# Improve your network security

As the World Wide Web evolves and company networks become bigger and better, network security has become crucial to protecting businesses' most valuable intellectual property and data.

"By improving network security, companies can lower the risk of many different types of attacks, such as identity theft, spoofing, data theft and suchlike," said Jayson O'Reilly, Director of Sales and Innovation of DRS.

He said that there are several steps that businesses can take to boost their network security. "Firstly, remember that technology can only take you so far - at the end of the day, it's about people. Many of the measures we have in place are aimed at finding out what errors people have made and remediating against them. Because of this, education and training are of key importance. Teach your employees to make clever choices that lower any security risks. Prevention is, after all, much better than cure."

Next, O'Reilly advised to assess which assets are most crucial to the business, in particular which data is most valuable. "It is important not only to know what you are protecting, but ensure that security efforts focus on the most critical assets first. Knowing that your most precious assets are being appropriately defended will give peace of mind, as you are not leaving them open to attack."

**Buffer zones**

Thirdly, he said that companies should implement network zoning to delineate between ranks of assets and communication between them, creating buffer zones to help prevent and deflect attacks. "Establishing isolated security zones within the enterprise network is an excellent way of lowering many different types of risk, particularly when you think that today's networks are more permeable than ever before. Perimeter defences are just not good enough on their own any longer."

Following on from network zoning, O'Reilly said that the business then needs to be crystal clear about who is allowed access to which zones, who should be denied access, and who is allowed access under certain circumstances.

"Understand what access needs to be available, and what access is strictly prohibited. For example, the chances are that you will wish to forbid any outside links to your network."

Finally, once all these aspects of network security have been defined and put in place, it is vital to employ automation to ensure that the network properly implements it all. "Too often networks simply do not do what is intended, and this is almost always due to errors in configurations that allow unexpected access and other untended consequences. The network today is so vast, and so interconnected, that it can result in possible paths that circumvent controls under unlikely circumstances."

Network security should be a top priority due to the growing threat from cyber criminals, saboteurs and even hacktivists. "Network security is vital to protecting businesses' most valuable data, and preventing industry sabotage and espionage. These threats can affect all businesses, and while there are no silver bullets, following these simple steps can go a long way towards lessening any risk."