

IT Analysis – Securing the physical link

By Fran Howarth, Principal analyst, Quocirca Ltd

There is no shortage of government activity in the area of cybersecurity. In the US, President Obama has ordered a review to be completed, leading to the provision of US\$335 million of public money to address improved resilience in both the public and private sectors. In Europe, the EU has recently unveiled a new strategy aimed at preparing the region to act in the case of major attacks or disruptions to its critical information infrastructure. Around the world, private and public sector organisations spend heavily on securing their networks—and that spending is continuing, even as the economy falters.

At the same time, investments are continuing to be made in high-speed connectivity, helped by advances in technology that have allowed faster, more scalable communications and that enable high volumes of data to be transmitted. The widespread availability of fibre optic gigabit Ethernet technology, and the 10GbE standard that allows for high levels of efficiency in the speed of transmission, allows for more efficient services that can combine voice, data and video traffic over high bandwidth. In particular, it is particularly useful for high-speed, inter-network connectivity, such as for point-to-point or site-to-site connectivity.

Because of its performance and lower cost than the alternatives, fibre optic gigabit Ethernet technology is replacing dedicated leased lines, frame relay and asynchronous transfer mode technologies for use in wide area networks. As a result, organisations ranging from telecommunications providers and internet service providers, to financial sector organisations and government agencies are entrusting their inter-office data communications to optical Ethernet carriers. One example in the news this week is the use being made by Icelandic telecommunications operator Siminn, which is using fibre optics links developed by UK Geo Networks Ltd to provide a dedicated fibre connexion between two of its data centres in

London. Geo Networks also operates Geo.TradeNet, which links financial services organisations directly to trading venues in London.

According to security vendor SafeNet, the use of fibre optic cabling across wide area and metropolitan networks has become the de facto choice for data and voice communications. It states that one of the key reasons for this is that fibre optic cables are widely believed to be impervious to physical tapping. That, however, is a fallacy and wiretapping of fibre optic cables has been occurring for decades among government and military communities. It is known, for example, that North Korea has intercepted communications of US military build-up activities by tapping fibre optic cables, as has Al Qaeda for communications between the US and its embassies abroad.

In the commercial world, one of the best known cases is the tapping of fibre optic cables directly outside the offices of Verizon in New York City for the purposes of brand damage just before it was about to release its quarterly earnings. Another case involved the Hannaford grocery concern, which was forced to admit that credit card numbers for 4.2 million customers had been stolen by hackers who tapped into the fibre optic cable connecting its network to its internet service provider. This occurred even though auditors had confirmed that Hannaford had achieved compliance with the Payment Card Industry (PCI) regulation.

Some years ago, hacking into fibre optic networks required substantial resources. It also used to be a challenge to avoid being detected when tapping into such cables or to process the information that was picked up owing to the large volumes of data involved. Today, hacking into fibre optic networks is a relatively easy task and equipment is available on the market for less than US\$1,000, ranging from machines that can splice fibre optic cables, split them or even tap light rays in a non-obtrusive manner without

Comment Article

even having to touch the cables. Since new fibre optic communication lines run at speed of up to 10Gb, a great deal of information can be compromised in seconds and downloaded for analysis. Any organisation sharing sensitive data over an unprotected or shared fibre optic transport link runs the risk of substantial data loss. And it is easier than many assume to find out where those optical links are as many optical Ethernet providers publish maps of their cables and the same is true for many of the metropolitan area networks that have sprung up recently. One example of this is the city of San Diego in the US.

In reality, there is only one way of ensuring that data travelling over such networks is secure, and that is to encrypt it. Many of the regulations faced by organisations today provide a "safe harbour", meaning that they do not have to notify the public of a data breach if the data lost was encrypted. And recent updates to PCI specify that credit card information must be encrypted when transmitted across public networks.

There are two main encryption options in such situations—encryption at the network layer or at the data link layer (layers 3 and 2, respectively, of the OSI model that defines the seven layers of functions that take place at each end of a communication). Layer 3 performs network routing functions, the best known example of which is IP; layer 2 refers to the means of transferring data between network entities, largely in point-to-point or point-to-multipoint connexions characteristic of a wide area network. At the network layer, encryption is usually performed using the IPSec protocol on network routers, but this generally introduces latency and slows down performance. At the data link layer, standalone encryption devices are generally used, which introduce minimal latency and are designed for high-speed networks.

Data link layer encryption has long been used by governments and the military throughout the world, and now the use of such approaches is becoming more used in the rest of the commercial world. According to Infoguard, which is the commercial arm of Crypto AG, set up in 1952 to provide cryptographic solutions for

government, military and intelligence communities, take up is growing fast among organisations that transport sensitive information over public networks, among them financial institutions and healthcare concerns. Concerns over data breaches are increasing awareness fast, with interest spreading to outsourcers and service providers. Given the current interest in cybersecurity and the fact that so many organisations today rely on fibre optic networks, this is something that should be applauded.

Comment Article

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at
<http://www.quocirca.com>