The alarming systems are also able to plug into infrastructure management software (IMS) that provide automation and a dashboard that allows remote monitoring of the events and alarms and the overall health of the network. The software can issue incident reports when alarms exceed the configured threshold.

One of the big challenges remaining after detection and alerting have been addressed is disconnecting or redirecting the data onto a backup network to limit the data exfiltration damage caused by the cyber criminal. Fiber-optic circuit switches have been used by several agencies to handle this task.

These switches are inserted between the network packet switch and the fiber-optic backbone cables. In normal operation, the switches pass the data straight through to the backbone network with very low latency.

But in the event of a breach, they are able to redirect this traffic instantly to a backup fiber network. If no backup is configured, the switch can instantly stop the data transfer. Optical taps can also be used on the circuit to passively copy the data to a networking monitoring system. In the event of a data breach, the network manager can go back to this stored data to determine the severity of the breach.

With the addition of several new technologies, security can be dramatically improved while also improving the chances of stopping data before it gets into the hands of data thieves. ●

A.K. Sharma
Sr. Vice President
Savitri Telecom Services

Industry Speak

Security Concerns with Optical Fiber Network – Thinking Ahead

In India, spread of optical fiber telecom network is taking place at a fast pace. Not only telecom operators but government of India is also pumping huge money to achieve the spread of this network throughout the country even to the remote panchayats and villages.

This spread will help better connectivity but at the same time secured network has to be provided in the area of defense and other vital sectors. Optical fiber networks were touted as one of the most secure infrastructure options. But recent perception is different from this notion. Vulnerability of OFC network has been established by experts. In the last couple of years, it has been suggested that fiber is almost as easy to tap as copper.

National security agencies are working simultaneously to secure OFC networks. Today, there are millions of miles of fiber cable spanning across the globe. There is an unimaginable amount of data being transmitted across these cables daily including sensitive government data, personal, financial, and others. If cable is laid in a public access space, this data may be compromised. Tighter access control to cabling needs to be implemented. More companies need to employ physical layer security systems in conjunction with their existing data layer security systems. Physical layer security systems are more able to detect and deal with intrusions to the cables that do not involve an easily measurable amount of data interruption. Also, it may not be completely advantageous to post optical fiber communication infrastructures on the Internet. This can provide a roadmap and bring attention to optical fiber communications vulnerabilities. Once an intruder has gained access to the cable, the actual tap is believed to be easier to accomplish than once thought. To do a virtually undetected tap, it is almost certain that intruders would only need available commercial items, such as a laptop, optical tap, packet-sniffer software, and an optical/electrical converter.

When a successful tap is made, the packet-sniffer software can filter through the packet headers only. This means that filters can be applied to the data allowing specified IP addresses, MAC addresses, or DNS information to be gathered, and then stored or forwarded to the intruding parties various tools and mechanisms, including other optical connections, links, wireless, another wavelength, or other resources. If an intruder is successful in using an unobtrusive method to retrieve data directly from the optical fiber cable, then the intruder does not need access to the company's network. Thus, there are no worries on how to get around firewalls, most IDS, or IPS.

It is being suggested that if the company is encrypting their transmitted data, this may provide a stumbling block for the intruder. Depending on the encryption methods used, it may still only be a matter of time before the intruder breaks the encryption and has their desired data. ■