FTTH COUNCIL AFRICA

WHITE PAPER ON THEFT OF EQUIPMENT IN THE FIBRE INDUSTRY

Authors:

Chris Nel: Lambda Test Equipment

Zach Yacumakis: IC Logistix

Andrew Cole: Concilium Technologies

Niki Lankesar: Coral i

Juanita Clark: FTTH Council Africa

BACKGROUND

For some time now the fibre industry has been plagued by crime, theft and hijacking. Recently the incidents deteriorated, when people's lives were threatened and shots fired while performing day-to-day duties attending to maintenance issues next to public roads.

Based on similarities in the different incidents it would appear that there are syndicates at work, targeting very specific items used in the fibre industry. These attacks are well organised possibly with help from within the industry.

This document and project arises from the need to safeguard the people working in the fibre industry of which the FTTH Council and its members are an integral part.

Aim of the document

The main objectives of this document are to find ways to deter the theft of equipment and to empower owners of equipment to safeguard themselves and their employees from possible dangerous incidents. In this regard the members of the FTTH Council Africa joined forces to find ways of limiting, and hopefully in time eliminating the use of dubious equipment and contractors in the industry.

STEPS TO COMBAT THEFT

What the FTTH Council will do:

The organisation will dedicate a specific information page on its website where it will list the details of reported stolen equipment based on different categories. This information will be

available to the public allowing any person to easily reference equipment serial numbers against the FTTH Council Database of stolen equipment.

Whilst there is a genuine need for second-hand or used equipment (a second-hand or used instrument is one that is being purchased by or otherwise transferred to a second or later end user), it is often difficult to determine whether equipment on offer in the second-hand market has a legitimate background.

The online Database will empower purchasers to ensure that the equipment being considered for purchase is not listed as stolen goods.

It will also eliminate the value of stolen equipment as it will not be tolerated in the industry and companies and people dealing or who are found to be involved with stolen equipment will be blacklisted in the industry.

What our members must do:

1. When appointing a contractor, request a list of serial numbers of equipment and compare these against the list of serial numbers recorded in the Database on the FTTH Council Africa website.
2. Verify the validity of calibration certificates, service records whilst verifying serial numbers against the latest record of stolen equipment as listed in the Database on the FTTH Council website.
3. When appointing a contractor, request the original paperwork of the equipment to be used and verify its legitimacy against the Database (even if it is just randomly selected serial numbers).
4. Test results and documentation submitted for work completion with embedded information must be verified on a regular basis to ensure that the equipment used are compliant to specification and are been used legally.
5. Any company offering to service equipment and perform any associated remedial / repair or service procedure are requested to verify the authenticity and legal ownership of the equipment before offering any service or support on the equipment. Records must be kept on what procedures was done to validate ownership and also who submitted the equipment for repair or service to facilitate a traceable track record of items used in the industry.
6. Inform the FTTH Council Africa of any stolen goods in order for it to update its website.
    6.1 Prerequisite to registering stolen equipment requires official owner/s to provide an associated Official Police Case number or a sworn affidavit by owner/s confirming details of theft or loss to be submitted to the FTTH Council Africa. Details of Police case number or affidavit are for record purposes of the FTTH Council Africa only and will not be made accessible on the public domain.
    6.2 Owners are to ensure that the serial number/s are reflected in the police report or sworn affidavit as this ensures traceability once equipment is blacklisted.
7. Ensure that any suspected stolen equipment and or users / contractors are reported to the council.

Companies affected or who have lost equipment are requested to inform the FTTH Council Africa if any of the following equipment has been stolen:

Test Equipment:

Optical Light Source

Optical Power Meters

Optical Loss Test Sets

OTDR

Live Fibre Detectors

Fibre Dispersion Testers

Optical Spectrum Analysers

Transmission Test Instruments (SDH & Ethernet)

Fusion Splicers

Fibre Cleavers

Fibre Blowing Equipment

Compressors

*When reporting stolen equipment it is required to list the Make, Model and Serial number and to furnish proof or record of the claimed loss if so requested.

CRITICAL SUCCESS FACTORS

1. In order for this to be successful it will need a top down approach from the industry, starting with Members that must enforce it on primary contractors.
2. Primary Contractors to enforce it on their sub-contractors that the equipment they use is calibrated regularly and a valid certificate held, as required in ISO 9000.
3. Operators and companies that make use or service equipment used in the fibre industry are required to keep their asset registers up to date and have a written record of any and every instrument it handles or works on.
4. Vendors must immediately notify a Member if that Member's stolen equipment is received into their service centres.
5. Rightful owners to lay criminal charges in cases where equipment is identified.
6. When purchasing second-hand equipment – ask for the original paperwork and verify with the OEM or accredited agent what the history of that equipment is.
7. No person must work on, operate or buy any item of which the serial number was removed.
8. Spread the word on the website.

9. Each organisation should appoint a champion in their organisation to be responsible to supply updated information to this database on an ongoing basis.

CONCLUSION

The FTTH Council Africa is fully committed to protecting the stakeholders in the industry and will rely on its members to enforce the above guidelines going forward.

It is our belief that if we work together that we can eliminate this practise to a large degree.

For more information, or to make further suggestions to this document; please contact: admin@ftthcouncilafrica.com.